ONTAP 9 文件

ONTAP 9

NetApp
February 12, 2026

This PDF was generated from https://docs.netapp.com/zh-tw/ontap/index.html on February 12, 2026.
Always check docs.netapp.com for the latest.

目錄

ONTAP 9 文件 1
版本資訊 2
ONTAP 9 版本重點摘要 2
ONTAP 9.18.1 亮點 2
ONTAP 9.17.1 亮點 3
ONTAP 9.16.1 重點介紹 4
ONTAP 9.15.1 重點介紹 4
ONTAP 9.14.1 重點摘要 5
ONTAP 9.13.1 重點介紹 6
ONTAP 9.12.1 重點摘要 7
ONTAP 9.11.1 重點摘要 8
ONTAP 9.10.1 重點摘要 9
ONTAP 9.9.1 重點摘要 9
ONTAP 9.18.1 的新增功能 10
資料保護 10
網路 10
SAN 11
S3 物件儲存 11
安全性 11
儲存資源管理增強功能 12
ONTAP 9.17.1 的新增功能 12
資料保護 12
S3 物件儲存 13
安全性 13
儲存資源管理增強功能 14
ONTAP 9.16.1 的新增功能 14
資料保護 14
網路 15
S3 物件儲存 15
SAN 16
安全性 16
儲存效率 16
儲存資源管理增強功能 17
系統管理員 17
ONTAP 9.15.1 的新增功能 17
資料保護 18
安全性 18
儲存效率 19
儲存資源管理增強功能 19

系統管理員 20
升級 20
ONTAP 9.14.1 的新功能 20
資料保護 20
檔案存取通訊協定 21
S3 物件儲存 21
SAN 22
安全性 22
儲存效率 22
儲存資源管理增強功能 23
SVM 管理增強功能 23
系統管理員 23
ONTAP 9.13.1 的新功能 24
資料保護 24
檔案存取通訊協定 24
網路 25
S3 物件儲存 25
SAN 25
安全性 25
儲存效率 26
儲存資源管理增強功能 26
SVM 管理增強功能 27
系統管理員 27
ONTAP 9.12.1 的新功能 27
資料保護 27
檔案存取通訊協定 28
網路 28
S3 物件儲存 29
SAN 29
安全性 29
儲存效率 30
儲存資源管理增強功能 30
SVM 管理增強功能 30
系統管理員 31
ONTAP 9.11.1 的新功能 31
資料保護 32
檔案存取通訊協定 32
網路 33
S3 物件儲存 33
SAN 33
安全性 33

儲存效率 33
儲存資源管理增強功能 34
SVM 管理增強功能 34
系統管理員 34
ONTAP 9.10.1 的新功能 35
資料保護 35
檔案存取通訊協定 36
網路 36
S3 物件儲存 36
SAN 37
安全性 37
儲存效率 37
儲存資源管理增強功能 37
SVM 管理增強功能 38
系統管理員 38
ONTAP 9.9.1 的新功能 39
資料保護 39
檔案存取通訊協定 40
網路 40
S3 物件儲存 40
SAN 41
安全性 41
儲存效率 41
儲存資源管理增強功能 41
系統管理員 42
變更為 ONTAP 限制和預設值 43
變更為 ONTAP 預設值 43
ONTAP 限制變更 44
ONTAP 9 版本支援 46
支援層級 46
開始使用 48
瞭解 ONTAP 48
ONTAP 平台 48
ONTAP 使用者介面 49
將ONTAP系統管理器與NetApp控制台集成 50
叢集儲存設備 51
高可用度配對 52
AutoSupport 與數位顧問 53
網路架構 54
用戶端傳輸協定 57
磁碟和本機層 59

磁碟區、qtree、檔案和LUN 64
儲存虛擬化 65
路徑容錯移轉 69
ONTAP 中的負載平衡 71
複寫 73
儲存效率 79
安全性 89
ONTAP 和 VMware vSphere 95
FabricPool 96
ONTAP快速入門 97
設定 ONTAP 叢集 98
ONTAP 叢集設定工作流程摘要 98
收集資訊以設定 ONTAP 叢集 99
建立 ONTAP 叢集並加入節點 102
或者，也可以將 ONTAP 管理階層的生命從 IPv4 轉換為 IPv6 107
使用數位顧問 Config Advisor 檢查您的 ONTAP 叢集 108
在 ONTAP 叢集上同步處理系統時間 109
升級及還原 ONTAP 軟體與韌體 113
升級ONTAP 113
瞭解 ONTAP 升級 113
我應該何時升級 ONTAP ？ 113
在計畫性升級之前執行 ONTAP 自動升級前檢查 115
準備 ONTAP 升級 126
在升級之前下載 ONTAP 軟體映像 216
ONTAP 升級方法 217
ONTAP 升級後的處理方式 271
韌體，系統和安全性更新 286
ONTAP 中的韌體，系統和安全性更新總覽 286
如何排程自動更新以進行安裝 288
啟用自動更新 288
修改自動更新 290
管理建議的自動更新 291
手動更新韌體 292
還原ONTAP 295
我是否需要技術支援才能還原 ONTAP 叢集？ 295
支援的 ONTAP 還原路徑 296
ONTAP 回復問題和限制 297
準備 ONTAP 還原 298
下載並安裝ONTAP 更新版的軟體映像 316
還原ONTAP 整個叢集 318
ONTAP 還原後的處理方式 326

叢集管理 334
使用System Manager進行叢集管理 334
了解如何使用 ONTAP System Manager 進行叢集管理 334
使用 System Manager 存取 ONTAP 叢集 335
在 ONTAP 叢集上設定通訊協定 336
使用 ONTAP System Manager 新增許可證金鑰來啟用新功能 336
使用 ONTAP System Manager 下載叢集配置 337
使用 ONTAP 系統管理員為叢集指派標籤 337
使用 ONTAP 系統管理員檢視和提交支援案例 338
在 ONTAP 系統管理員中管理儲存虛擬機器的最大容量限制 339
在 ONTAP System Manager 中監控叢集，階層和 SVM 容量 340
查看硬體配置以確定 ONTAP 系統管理員的問題 343
使用 ONTAP 系統管理員管理節點 349
授權管理 351
ONTAP 授權總覽 351
從 NetApp 支援網站 下載 NetApp 授權檔案（ NLF ） 354
在 ONTAP 中安裝 NetApp 授權 355
管理ONTAP 不需購買的授權 356
授權類型與授權方法 359
用於管理 ONTAP 中授權的命令 360
使用CLI進行叢集管理 360
使用 ONTAP CLI 瞭解叢集管理 360
叢集與SVM管理員 361
使用CLI存取叢集（僅限叢集管理員） 362
使用ONTAP 指令行介面 373
錄製 ONTAP CLI 工作階段，並管理錄製的工作階段 386
叢集管理（僅限叢集管理員） 388
管理節點 392
設定SP/BMC網路 415
使用 SP/BMC 遠端管理節點 420
管理 ONTAP 叢集時間（僅限叢集管理員） 447
管理橫幅和MOTD 449
管理 ONTAP 工作和工作排程 458
備份及還原叢集組態（僅限叢集管理員） 461
管理 ONTAP 叢集的節點核心傾印（僅限叢集管理員） 469
磁碟與階層管理 471
磁碟與 ONTAP 本機層 471
管理本機層 472
管理磁碟 513
管理RAID組態 544
管理 Flash Pool 本機層 550

資料層管理FabricPool 564
瞭解 ONTAP FabricPool 的資料分層功能 564
使用 ONTAP FabricPool 的需求 565
利用 ONTAP FabricPool 原則有效分層資料 569
了解 ONTAP FabricPool 設定和管理任務 573
設定FabricPool 功能 573
管理FabricPool 590
管理FabricPool 鏡射 611
用於管理 FabricPool 資源的 ONTAP 指令 618
SVM資料移動性 621
了解ONTAP SVM 資料遷移 621
遷移ONTAP SVM 628
監控ONTAP卷遷移 630
暫停和恢復ONTAP SVM 遷移 631
取消ONTAP SVM 遷移 632
ONTAP SVM 遷移後手動切換客戶端 632
客戶端切換後手動移除來源ONTAP SVM 632
HA配對管理 633
了解 ONTAP 叢集中的 HA 對管理 633
了解 ONTAP 叢集中的硬體輔助接管 634
了解 ONTAP 叢集中的自動接管和交還 635
ONTAP 自動接管指令 638
ONTAP 自動交還指令 639
ONTAP 手動接管指令 641
ONTAP 手動交還命令 643
在 ONTAP 叢集中測試接管和交還 646
用於監控 HA 對的 ONTAP 指令 648
用於啟用和停用儲存故障轉移的 ONTAP 命令 652
在雙節點叢集中，無需啟動接管即可暫停或重新啟動 ONTAP 節點 652
配置ONTAP HA 流量的加密 655
使用 System Manager 進行 REST API 管理 656
使用 System Manager 進行 REST API 管理 656
存取REST API記錄 657
Volume管理 659
使用System Manager進行Volume與LUN管理 659
管理磁碟區 659
使用 ONTAP 系統管理員管理 LUN 665
使用 ONTAP 系統管理員擴充存儲 667
使用 ONTAP System Manager 進行壓縮、壓縮和重複資料刪除，節省儲存空間 669
使用 ONTAP 系統管理員移動 LUN 來平衡負載 669
使用 ONTAP 系統管理員將磁碟區移至另一層，從而平衡負載 670

使用 Ansible Playbooks 透過 ONTAP System Manager 新增或編輯磁碟區或 LUN 670
使用 ONTAP System Manager 管理儲存效率策略 672
使用 ONTAP System Manager 使用配額管理資源 673
使用 ONTAP System Manager 設定配額以限制資源使用 674
使用 ONTAP 系統管理器複製捲和 LUN 以進行測試 674
在 ONTAP 系統管理員中搜尋、篩選和排序資訊 676
使用CLI進行邏輯儲存管理 679
使用CLI進行邏輯儲存管理總覽 679
建立及管理磁碟區 679
移動及複製磁碟區 697
使用FlexClone Volume來建立FlexVol 有效複本的功能 705
使用FlexClone檔案和FlexClone LUN來建立有效率的檔案和LUN複本 710
使用qtree來分割FlexVol 您的等量磁碟區 718
磁碟區的邏輯空間報告與強制 723
使用配額來限制或追蹤資源使用量 730
使用重複資料刪除技術、資料壓縮及資料壓縮技術來提高儲存效率 770
將一個磁碟區從一個SVM重新裝載到另一個SVM 798
建議的Volume與檔案或LUN組態組合 805
變更檔案或目錄容量時的注意事項與考量 809
FlexClone 檔案和 FlexClone LUN 支援的功能 812
資料區管理FlexGroup 814
透過 CLI 瞭解 ONTAP FlexGroup Volume 管理 814
瞭解 ONTAP FlexGroup Volume 815
ONTAP FlexGroup 磁碟區支援和不支援的組態 816
設定流通量FlexGroup 820
管理FlexGroup 功能 829
資料保護FlexGroup 功能 865
管理FlexGroup 資料保護作業、以利執行不中斷的作業 883
將功能區轉換為FlexVol 功能區FlexGroup 899
資料區管理FlexCache 906
瞭解 ONTAP FlexCache Volume 906
ONTAP FlexCache Volume 支援和不支援的功能 907
ONTAP FlexCache Volume 規模調整準則 913
建立 ONTAP FlexCache Volume 914
FlexCache 回寫 919
FlexCache 二元性 934
管理 FlexCache Volume 941
用於熱點修復的 FlexCache 948
網路管理 960
開始使用 960
使用系統管理員視覺化 ONTAP 網路 960

瞭解 ONTAP 叢集的網路元件 961
ONTAP 網路纜線的最佳實務做法 963
判斷 ONTAP 網路中要使用的 LIF 容錯移轉原則 964
NAS 路徑容錯移轉工作流程 967
在 ONTAP 網路上設定 NAS 路徑容錯移轉 967
ONTAP 網路上的 NAS 路徑容錯移轉工作表 968
網路連接埠 974
瞭解 ONTAP 網路連接埠組態 974
設定網路連接埠 975
IPspaces 1001
瞭解 ONTAP IPspace 組態 1001
為 ONTAP 網路建立 IPspace 1004
檢視 ONTAP 網路上的 IPspace 1005
從 ONTAP 網路刪除 IPspace 1006
廣播網域 1007
瞭解 ONTAP 廣播網域 1007
建立 ONTAP 廣播網域 1008
從 ONTAP 廣播網域新增或移除連接埠 1011
修復 ONTAP 連接埠連線能力 1013
將 ONTAP 廣播網域移至 IPspace 1020
分割 ONTAP 廣播網域 1021
合併 ONTAP 廣播網域 1021
變更 ONTAP 廣播網域中連接埠的 MTU 值 1022
檢視 ONTAP 廣播網域 1024
刪除 ONTAP 廣播網域 1025
容錯移轉群組和原則 1026
瞭解 ONTAP 網路上的 LIF 容錯移轉 1026
建立 ONTAP 容錯移轉群組 1027
在 LIF 上設定 ONTAP 容錯移轉設定 1027
用於管理容錯移轉群組和原則的 ONTAP 命令 1029
子網路（僅限叢集管理員） 1030
瞭解 ONTAP 網路的子網路 1030
為 ONTAP 網路建立子網路 1030
從 ONTAP 網路的子網路新增或移除 IP 位址 1033
變更 ONTAP 網路的子網路內容 1035
檢視 ONTAP 網路的子網路 1037
從 ONTAP 網路刪除子網路 1037
為 ONTAP 網路建立 SVM 1038
邏輯介面（LIF） 1044
LIF 總覽 1044
管理生命 1053

設定 ONTAP 虛擬 IP （ VIP ）生命 1072
平衡網路負載 1079
使用 DNS 負載平衡最佳化 ONTAP 網路流量 1079
瞭解 ONTAP 網路的 DNS 負載平衡 1079
為 ONTAP 網路建立 DNS 負載平衡區域 1080
從負載平衡區域新增或移除 ONTAP LIF 1080
設定 ONTAP 網路的 DNS 服務 1081
設定 ONTAP 網路的動態 DNS 服務 1084
主機名稱解析 1085
瞭解 ONTAP 網路的主機名稱解析 1085
設定 DNS 以進行 ONTAP 網路的主機名稱解析 1085
用於管理 ONTAP Hosts 表的 ONTAP 命令 1087
保護您的網路安全 1087
使用 FIPS 為所有 SSL 連線設定 ONTAP 網路安全性 1087
設定 IPsec 在線上加密 1091
配置ONTAP後端集群網路加密 1099
在 ONTAP 網路中設定生命安全的防火牆原則 1100
管理防火牆服務和原則的 ONTAP 命令 1106
QoS 標記（僅限叢集管理員） 1106
瞭解 ONTAP 網路服務品質（ QoS ） 1107
修改 ONTAP 網路 QoS 標記值 1107
檢視 ONTAP 網路 QoS 標記值 1108
管理 SNMP （僅限叢集管理員） 1108
瞭解 ONTAP 網路上的 SNMP 1108
為 ONTAP 網路建立 SNMP 社群 1109
在 ONTAP 叢集中設定 SNMPv3 使用者 1112
在 ONTAP 網路上設定用於 SNMP 的 traphosts 1115
驗證 ONTAP 叢集中的 SNMP 輪詢 1116
用於管理 SNMP ，設陷和 traphosts 的 ONTAP 命令 1118
管理SVM中的路由 1120
瞭解 ONTAP 網路上的 SVM 路由 1120
為 ONTAP 網路建立靜態路由 1121
啟用 ONTAP 網路的多重路徑路由 1121
從 ONTAP 網路刪除靜態路由 1121
檢視 ONTAP 路由資訊 1122
從 ONTAP 網路的路由表中移除動態路由 1124
ONTAP 網路資訊 1125
檢視 ONTAP 網路資訊 1125
檢視 ONTAP 網路連接埠資訊 1125
檢視 ONTAP VLAN 資訊 1127
檢視 ONTAP 介面群組資訊 1128

檢視 ONTAP LIF 資訊 1129
檢視 ONTAP 網路的路由資訊 1132
檢視 ONTAP DNS 主機表格項目 1134
檢視 ONTAP DNS 網域組態資訊 1134
檢視 ONTAP 容錯移轉群組資訊 1135
檢視 ONTAP LIF 容錯移轉目標 1136
檢視負載平衡區域中的 ONTAP 生命負載 1137
檢視 ONTAP 叢集連線 1139
用於診斷網路問題的 ONTAP 命令 1145
檢視與鄰近探索通訊協定的網路連線 1146
NAS儲存管理 1158
使用System Manager管理NAS傳輸協定 1158
了解如何使用 ONTAP System Manager 進行 NAS 管理 1158
使用 ONTAP 系統管理員為 VMware 資料儲存庫配置 NFS 存儲 1158
使用 ONTAP 系統管理員為主目錄設定 NAS 存儲 1159
使用 ONTAP 系統管理器透過 NFS 為 Linux 伺服器設定 NAS 存儲 1160
使用 ONTAP System Manager 的匯出策略管理存取 1162
使用 ONTAP 系統管理員的 SMB 為 Windows 伺服器設定 NAS 存儲 1162
使用 ONTAP 系統管理器透過 NFS 和 SMB 為 Windows 和 Linux 配置 NAS 存儲 1164
使用 ONTAP 系統管理員透過 Kerberos 保護用戶端存取 1166
使用 ONTAP 系統管理員透過名稱服務提供用戶端訪問 1168
使用 ONTAP System Manager 管理目錄和文件 1168
使用 ONTAP System Manager 管理特定於主機的使用者和群組 1169
使用 ONTAP 系統管理員監控 NFS 活動用戶端 1172
啟用NAS儲存設備 1173
配置 NFS 1176
使用 ONTAP CLI 瞭解 NFS 組態 1176
了解 ONTAP NFS 設定工作流程 1177
準備 1178
設定SVM的NFS存取 1190
將儲存容量新增至啟用NFS的SVM 1222
在哪裡可以找到更多 ONTAP NFS 信息 1236
此功能與7-Mode匯出有何不同ONTAP 1237
管理 NFS 1241
了解 NFS 協定的 ONTAP 檔案訪問 1241
瞭解NAS檔案存取 1241
在NAS命名空間中建立及管理資料磁碟區 1248
設定安全樣式 1253
使用 NFS 設定檔案存取 1257
使用 NFS 管理檔案存取 1290
支援的NFS版本和用戶端 1340

並行 NFS 1344
NFS和SMB檔案及目錄命名相依性 1367
管理 NFS 主幹 1372
瞭解 ONTAP NFS 主幹 1372
設定新的 NFS 伺服器並匯出以進行主幹連線 1373
調整現有的 NFS 匯出以進行主幹連線 1378
透過RDMA管理NFS 1383
瞭解 ONTAP 中的 NFS over RDMA 1383
透過RDMA設定NFS的NIC 1385
透過RDMA設定NFS的LIF 1387
修改NFS組態 1389
使用 CLI 設定 SMB 1389
使用 ONTAP CLI 瞭解 SMB 組態 1389
ONTAP SMB 組態工作流程 1390
準備 1391
設定SMB存取SVM 1400
設定SMB用戶端存取共享儲存設備 1420
使用 CLI 管理 SMB 1429
瞭解 ONTAP SMB 1429
SMB伺服器支援 1429
管理SMB伺服器 1436
使用SMB設定檔案存取 1526
使用SMB管理檔案存取 1587
部署SMB用戶端型服務 1673
部署SMB伺服器型服務 1686
NFS和SMB檔案及目錄命名相依性 1749
提供S3用戶端對NAS資料的存取 1754
了解ONTAP S3 多協定支持 1754
了解ONTAP S3 用戶端存取的 NAS 資料需求 1757
在ONTAP SVM 上啟用 S3 協定存取 NAS 數據 1758
建立ONTAP S3 NAS 儲存桶 1760
啟用ONTAP S3 用戶端用戶 1762
Microsoft Hyper-V和SQL Server的SMB組態 1765
Microsoft Hyper-V與SQL Server的SMB組態總覽 1765
設定ONTAP 適用於Microsoft Hyper-V和SQL Server over SMB解決方案的支援功能 1765
不中斷營運：透過SMB執行Hyper-V和SQL Server 1766
使用遠端VSS進行共用型備份 1770
ODX複製卸載如何透過SMB共用搭配Hyper-V和SQL Server使用 1773
組態需求與考量 1774
SQL Server與Hyper-V over SMB組態的建議 1781
透過SMB組態規劃Hyper-V或SQL Server 1781

利用ONTAP Hyper-V和SQL Server、透過SMB建立不中斷營運的支援組態 1785
透過SMB組態管理Hyper-V和SQL Server 1798
使用統計資料、透過SMB監控Hyper-V和SQL Server活動 1801
驗證組態是否能夠不中斷營運 1805
SAN 儲存管理 1821
SAN概念 1821
使用iSCSI進行SAN資源配置 1821
iSCSI服務管理 1822
使用FC進行SAN資源配置 1828
採用NVMe的SAN資源配置 1829
SAN 磁碟區 1830
SAN 主機端空間管理 1834
關於igroup 1835
指定igroup的啟動器WWPN和iSCSI節點名稱 1836
使用虛擬化SAN環境的優點 1836
改善VMware VAAI的ESX主機效能 1837
SAN 複製卸載 1838
SAN管理 1841
SAN 資源配置 1841
NVMe資源配置 1851
管理LUN 1862
管理igroup和portSet 1874
管理iSCSI傳輸協定 1880
管理FC傳輸協定 1887
管理NVMe傳輸協定 1889
使用FC介面卡管理系統 1898
管理所有SAN傳輸協定的生命量 1905
啟用 SAN 通訊協定的 ONTAP 空間分配 1911
建議的Volume與檔案或LUN組態組合 1913
SAN 資料保護 1918
瞭解適用於 SAN 環境的 ONTAP 資料保護方法 1918
從 ONTAP 快照還原單一 LUN 1919
從 ONTAP 快照還原磁碟區中的所有 LUN 1921
使用 ONTAP FlexClone LUN 保護您的資料 1922
在SnapVault SAN環境中設定及使用靜態備份 1923
將主機備份系統連接至 ONTAP 的建議組態 1930
使用主機備份系統來保護 ONTAP 儲存系統上的 LUN 1931
SAN組態參考 1933
瞭解 ONTAP SAN 組態 1933
iSCSI 組態 1933
FC 組態 1936

FCoE 組態 1942
FC 和 FCoE 分區 1946
連線至 ONTAP 和非 NetApp 系統的 SAN 主機需求 1949
SAN組態MetroCluster 1949
ONTAP 支援 SAN 主機多重路徑功能 1952
組態限制 1953
S3物件儲存管理 1968
瞭解 ONTAP 9 中的 S3 支援 1968
瞭解 ONTAP S3 組態 1968
使用 FlexGroup Volume 的 ONTAP S3 架構 1969
ONTAP S3 主要使用案例 1971
規劃 1971
支援 S3 物件儲存的 ONTAP 版本與平台 1971
支援的動作ONTAP 1972
SS3互通性ONTAP 1981
經過驗證的 ONTAP 中使用 S3 的第三方解決方案 1983
設定 1983
關於S3組態程序 1983
設定S3對SVM的存取 1988
將儲存容量新增至啟用S3的SVM 2003
建立或修改存取原則聲明 2018
允許用戶端存取S3物件儲存設備 2032
ONTAP S3 儲存服務層級 2035
為 ONTAP S3 貯體設定跨來源資源共享（ CORS ） 2036
使用 SnapMirror S3 保護貯體 2041
瞭解 ONTAP SnapMirror S3 2041
遠端叢集上的鏡射與備份保護 2044
本機叢集上的鏡射與備份保護 2055
利用雲端目標提供備份保護 2066
修改 ONTAP SnapMirror S3 原則 2075
利用快照保護 S3 資料 2076
瞭解 ONTAP S3 快照 2076
建立 ONTAP S3 快照 2078
檢視及還原 ONTAP S3 快照 2080
刪除 ONTAP S3 快照 2082
稽核S3事件 2083
瞭解如何稽核 ONTAP S3 事件 2083
規劃 ONTAP S3 稽核組態 2086
建立並啟用 ONTAP S3 稽核組態 2088
選擇 ONTAP S3 稽核的儲存區 2090
修改 ONTAP S3 稽核組態 2090

顯示 ONTAP S3 稽核組態 2091
驗證與存取控制 2094
驗證與存取控制總覽 2094
用戶端驗證與授權 2094
系統管理員驗證與RBAC 2094
管理系統管理員驗證和 RBAC 2094
瞭解 ONTAP 中的系統管理員驗證和 RBAC 2094
ONTAP 系統管理員驗證和 RBAC 工作流程 2095
ONTAP 系統管理員驗證和 RBAC 設定工作表 2095
建立登入帳戶 2107
管理存取控制角色 2122
管理系統管理員帳戶 2134
管理多管理員驗證 2159
管理動態授權 2192
使用 OAuth 2.0 進行驗證與授權 2201
ONTAP OAuth 2.0 實作總覽 2201
概念 2204
設定與部署 2218
為遠端ONTAP用戶設定 SAML 身份驗證 2225
啟用SAML驗證 2225
停用SAML驗證 2229
配置第三方 IdP 2230
疑難排解SAML組態問題 2232
在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組 2234
如何識別群組 2234
使用名稱管理群組 2235
使用 UUID 管理群組 2236
使用 WebAuthn MFA 進行驗證與授權 2238
了解 ONTAP System Manager 使用者的 WebAuthn 多因素驗證 2238
為 ONTAP 系統管理員使用者或群組啟用 WebAuthn MFA 2238
停用 ONTAP System Manager 使用者的 WebAuthn MFA 2240
檢視 ONTAP WebAuthn MFA 設定並管理認證 2241
管理Web服務 2243
管理網路服務總覽 2243
管理對ONTAP Web 服務的訪問 2244
在 ONTAP 中管理網路傳輸協定引擎 2245
用於管理 Web 協定引擎的ONTAP指令 2246
配置對ONTAP Web 服務的存取 2247
用於管理 Web 服務的ONTAP命令 2248
用於管理ONTAP節點上的掛載點的命令 2249
在ONTAP中管理 SSL 2249

將 HSTS 用於ONTAP Web 服務 2250
解決ONTAP Web 服務存取問題 2252
使用憑證驗證遠端伺服器的身分 2254
了解如何在ONTAP中使用憑證驗證遠端伺服器的身份 2254
使用ONTAP中的 OCSP 驗證數位憑證是否有效 2254
查看ONTAP中基於 TLS 的應用程式的預設證書 2256
相互驗證叢集和 KMIP 伺服器 2257
相互驗證ONTAP叢集和 KMIP 伺服器概述 2257
在 ONTAP 中為叢集產生憑證簽署要求 2257
為ONTAP叢集安裝 CA 簽署的伺服器憑證 2258
在ONTAP中為 KMIP 伺服器安裝 CA 簽署的客戶端憑證 2259
安全性與資料加密 2261
自主勒索軟體保護 2261
瞭解 ONTAP 自主勒索軟體保護 2261
ONTAP 自主勒索軟體保護使用案例與考量 2267
啟用 ARP 2271
在學習期間之後，在 ONTAP ARP 中切換至作用中模式 2281
了解 SAN 磁碟區的ONTAP ARP 評估期 2283
暫停 ONTAP 自主勒索軟體保護，將工作負載事件排除在分析之外 2285
管理 ONTAP 自主勒索軟體保護攻擊偵測參數 2287
回應 ONTAP ARP 偵測到的異常活動 2291
在勒索軟體攻擊之後，從 ONTAP ARP 快照還原資料 2296
調整自動產生的 ARP 快照的設置 2299
使用 AI （ARP/AI ）更新 ONTAP 自主勒索軟體保護 2302
使用 VScan 保護病毒 2304
了解 ONTAP Vscan 的防毒配置 2304
關於NetApp防毒保護 2305
VScan伺服器安裝與組態 2311
設定掃描器資源池 2318
設定存取時掃描 2325
設定隨需掃描 2329
在 ONTAP Vscan 中配置機外防毒功能的最佳實踐 2335
在 SVM ONTAP Vscan 上啟用病毒掃描 2336
重設 ONTAP Vscan 掃描檔的狀態 2337
使用 ONTAP 檢視 VScan 事件記錄資訊 2337
監控並疑難排解連線問題 2338
稽核SVM上的NAS事件 2343
瞭解如何針對 SMB 和 NFS 傳輸協定使用 ONTAP 來稽核檔案存取 2343
稽核的運作方式 2344
ONTAP 稽核的必要條件 2346
限制 ONTAP 稽核記錄的暫存檔案大小 2347

瞭解 ONTAP 稽核事件記錄的支援格式 2348
檢視及處理 ONTAP 稽核事件記錄 2348
可稽核的SMB事件 2349
瞭解 ONTAP 對 NFS 檔案和目錄存取事件的稽核 2354
規劃 ONTAP VM 上的稽核組態 2355
在SVM上建立檔案和目錄稽核組態 2360
設定檔案和資料夾稽核原則 2363
顯示套用至檔案和目錄的稽核原則相關資訊 2367
可稽核的CLI變更事件 2373
管理稽核組態 2379
疑難排解 ONTAP 稽核和暫存磁碟區空間問題 2383
在SVM上使用FPolicy進行檔案監控與管理 2385
瞭解 FPolicy 2385
規劃FPolicy組態 2393
建立FPolicy組態 2426
管理 FPolicy 組態 2434
使用安全性追蹤來驗證存取 2442
了解 ONTAP 安全追蹤 2442
ONTAP SVM 上的存取檢查安全追蹤監視器的類型 2443
在 ONTAP SVM 上建立安全追蹤時的注意事項 2443
執行安全追蹤 2444
解釋 ONTAP 安全追蹤結果 2452
在哪裡可以找到有關 ONTAP SVM 的更多信息 2453
使用System Manager管理加密 2454
使用基於軟體的加密對ONTAP叢集中儲存的資料進行加密 2454
使用自加密磁碟機加密ONTAP叢集中儲存的數據 2454
使用CLI管理加密 2455
了解ONTAP資料加密 2455
配置NetApp捲和聚合加密 2455
設定NetApp硬體加密 2490
管理NetApp加密 2513
資料保護與災難恢復 2548
叢集與SVM對等關係 2548
瞭解 ONTAP 叢集和 SVM 對等關係 2548
準備叢集與SVM對等關係 2548
設定叢集間LIF 2551
設定對等關係 2564
啟用對等關係上的 ONTAP 叢集對等加密 2573
移除對等關係中的 ONTAP 叢集對等加密 2573
管理本機快照 2574
瞭解如何管理本機 ONTAP 快照 2575

了解ONTAP長期保留快照 2575
設定自訂快照原則 2575
手動管理快照 2579
管理快照保留 2582
從快照還原檔案 2586
SnapMirror Volume複寫 2591
瞭解 SnapMirror Volume 複寫 2592
設定 SnapMirror Volume 複寫 2617
管理SnapMirror Volume複寫 2637
管理SnapMirror SVM複寫 2666
瞭解 ONTAP SnapMirror SVM 複寫 2666
複寫SVM組態 2673
從 SnapMirror SVM DR 目的地提供資料 2685
重新啟動 SnapMirror 來源 SVM 2689
將 ONTAP SnapMirror Volume DR 關係轉換為 SVM DR 關係 2702
刪除 ONTAP SnapMirror SVM 複寫關係 2703
管理SnapMirror根Volume複寫 2704
瞭解 ONTAP SnapMirror 根磁碟區複寫 2704
建立並初始化 ONTAP 負載共用鏡射關係 2704
更新 ONTAP 負載共用鏡射關係 2706
升級 ONTAP 負載共用鏡像 2707
備份到雲端 2708
安裝 ONTAP SnapMirror 雲端授權 2708
使用 ONTAP SnapMirror 將資料備份到雲端 2709
使用NetApp備份和恢復備份數據 2711
利用SnapLock NetApp技術歸檔及法規遵循 2715
了解ONTAP SnapLock 2715
設定SnapLock 功能 2719
管理WORM檔案 2734
行動ONTAP SnapLock卷 2747
鎖定ONTAP快照以防止勒索軟體攻擊 2749
一致性群組 2756
了解ONTAP一致性組 2756
了解ONTAP一致性組限制 2761
配置單一ONTAP一致性組 2762
配置分層ONTAP一致性組 2766
保護ONTAP一致性組 2770
修改ONTAP一致性群組中的成員卷 2777
修改ONTAP一致性組幾何結構 2783
修改ONTAP一致性群組應用程式和元件標籤 2788
克隆ONTAP一致性組 2789

刪除ONTAP一致性組 2791
SnapMirror 主動同步 2792
簡介 2792
規劃 2804
設定 2812
管理 SnapMirror 主動同步並保護資料 2852
疑難排解 2868
適用於 MetroCluster 和 SnapMirror 主動同步的 ONTAP 調解器 2878
瞭解 ONTAP Mediator 2878
ONTAP Mediator 的新功能 2879
安裝或升級 2884
管理 ONTAP Mediator 2927
維護 ONTAP Mediator 的主機作業系統 2957
了解使用 ONTAP System Manager 進行 MetroCluster IP 網站管理 2961
使用磁帶備份來保護資料 2962
了解ONTAP FlexVol卷的磁帶備份 2962
ONTAP磁帶備份與復原工作流程 2962
ONTAP SMTape 和轉儲備份引擎的用例 2963
管理磁帶機 2963
關於磁帶機 2969
在儲存系統之間傳輸資料 2976
NDMP for FlexVol 需求 2980
了解ONTAP FlexGroup卷的 NDMP 支持 2997
了解帶有ONTAP SnapLock卷的 NDMP 2997
管理FlexVol 節點範圍的NDMP模式、以利實現不受限的功能 2997
管理SVM範圍內的FlexVol NDMP模式、以利不受限於功能區 2999
關於FlexVol 針對資料量的傾印引擎 3005
關於FlexVol 適用於資料量的SMTape引擎 3015
監控FlexVol 磁帶備份與還原功能、以利執行各項功能 3019
磁帶備份與FlexVol 還原的錯誤訊息 3023
NDMP 組態 3043
瞭解 ONTAP NDMP 組態 3043
了解 ONTAP NDMP 設定工作流程 3044
準備 ONTAP NDMP 配置 3045
驗證 ONTAP NDMP 磁帶設備連接 3047
為 ONTAP NDMP 備份作業啟用磁帶預留 3048
設定SVM範圍的NDMP 3049
設定節點範圍的NDMP 3058
為 ONTAP NDMP 配置配置備份應用程式 3063
在不同時複寫NetApp Element 功能的軟體與ONTAP 非本性概述之間 3063
事件、效能和健全狀況監控 3064

使用System Manager監控叢集效能 3064
使用 ONTAP 系統管理器監控叢集效能 3064
了解如何在 ONTAP System Manager 儀表板上查看叢集 3064
在 ONTAP 系統管理員中辨識熱捲和其他對象 3065
在 ONTAP 系統管理員中修改 QoS 3066
在 ONTAP 系統管理員中監控風險 3066
利用 ONTAP System Manager 洞察優化您的系統 3068
在 ONTAP 系統管理員中設定本機 FPolicy 3070
使用CLI監控及管理叢集效能 3070
ONTAP效能管理工作流程 3070
執行基礎架構檢查 3071
管理工作負載 3078
使用統一管理器監控和管理叢集效能 3097
使用 ONTAP Unified Manager 監控叢集效能 3097
了解ONTAP Active IQ Unified Manager效能監控與管理 3097
監控效能 3098
使用ONTAP Active IQ Digital Advisor檢視系統效能 3107
使用 ONTAP 資料基礎架構洞察監控叢集效能 3107
監控、疑難排解及最佳化所有資源 3107
稽核記錄 3108
瞭解 ONTAP 稽核記錄實作 3108
瞭解 ONTAP 稽核記錄的變更 3109
顯示 ONTAP 稽核記錄內容 3109
管理 ONTAP 稽核 Get 要求設定 3111
啟用ONTAP跨叢集審核 3111
管理 ONTAP 稽核記錄目的地 3113
AutoSupport 3114
瞭解 AutoSupport 3114
規劃 3127
設定 3133
使用 AutoSupport 上傳檔案 3135
疑難排解 3137
健全狀況監控 3143
瞭解 ONTAP 系統健全狀況監控 3143
瞭解 ONTAP 健全狀況監控元件 3144
瞭解 ONTAP 系統健全狀況警示回應 3144
瞭解 ONTAP 系統健全狀況警示自訂功能 3145
瞭解 ONTAP AutoSupport 健全狀況警示觸發程序 3145
瞭解可用的 ONTAP 叢集健全狀況監視器 3146
自動接收 ONTAP 系統健全狀況警示 3147
回應降級的 ONTAP 系統健全狀況 3147

瞭解如何回應降級的 ONTAP 系統健全狀況 3148
用於監控 ONTAP 系統健全狀況的命令 3151
檢視 ONTAP 環境資訊 3154
檔案系統分析 3154
瞭解 ONTAP 檔案系統分析 3154
啟用 ONTAP 檔案系統分析 3156
使用 FSA 查看 ONTAP 檔案系統活動 3159
使用 FSA 啟用 ONTAP 活動追蹤 3161
使用 FSA 啟用 ONTAP 使用情況分析 3163
根據 FSA 中的 ONTAP 分析採取糾正措施 3164
透過 ONTAP 檔案系統分析，以角色為基礎的存取控制 3165
ONTAP 檔案系統分析的考量事項 3167
EMS 組態 3169
瞭解 ONTAP EMS 組態 3169
使用系統管理員設定 ONTAP EMS 事件通知和篩選器 3169
使用CLI設定EMS事件通知 3172
更新過時的EMS事件對應 3178
指令參考資料ONTAP 3186
指令參考ONTAP 資料以取得有限支援版本的支援（僅PDF） 3186
CLI比較工具 3186
法律聲明 3187
版權 3187
商標 3187
專利 3187
隱私權政策 3187
開放原始碼 3187
ONTAP 3187
適用於 MetroCluster IP 組態的 ONTAP Mediator 3187

ONTAP 9 文件

版本資訊

ONTAP 9 版本重點摘要

每個 ONTAP 9 資料管理軟體版本都提供全新且增強的功能、可改善 ONTAP 的功能、管理能力、效能和安全性。

除了這些重點摘要之外、您還可以針對最新 ONTAP 版本中推出的所有新功能和增強功能、找到全方位的每個版本涵蓋範圍。

- 深入瞭解 "全新增強的 ONTAP MetroCluster 功能"。
- 了解 "適用於NetApp AFX 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "適用於NetApp ASA r2 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "對AFF 、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

若要升級至最新版的 ONTAP 、請參閱 升級至最新版的 ONTAP 和 我應該何時升級 ONTAP ？

ONTAP 9.18.1 亮點

ONTAP 9.18.1 在安全性、可擴充性和儲存管理方面提供了新的和增強的功能，以支援資料基礎架構現代化。這些增強功能可協助您擴展規模、提高營運效率並確保未來資料安全。如需查看所有新增功能和改進的完整列表，請參閱ONTAP 9.18.1 的新增功能。

- 後端叢集高可用性加密

  能夠使用 mTLS 對後端叢集網路進行加密。

- PQC對傳輸中資料的支持

  能夠使用後量子演算法處理傳輸中的資料。

- 支援 IPv6 IPSec 和硬體卸載

  支援使用 IPv6 位址進行硬體卸載的 IPSec。

- ARP/AI 支援FlexGroup卷

  NetApp FlexGroup磁碟區支援 ARP/AI，提供基於機器學習的進階勒索軟體偵測和保護。

- NVMe 的複製卸載

  透過將複製操作直接卸載到儲存設備來加速大數據傳輸，從而降低主機 CPU 和網路負載。

- 儲存驅動的 S3 儲存桶快照恢復

能夠恢復 S3 儲存桶中損壞的對象，或將整個儲存桶恢復到現有儲存桶之上。

ONTAP 9.17.1 亮點

ONTAP 9.17.1 在 AI 驅動的 SAN 自主勒索軟體防護方面提供了創新，並透過SnapMirror主動同步和一致性群組分層管理增加了 NVMe 前端主機支援。這些增強功能鞏固了 NetApp 在資料安全和網路彈性方面的領導地位，提高了ONTAP 的效能、可擴展性、效率和業務連續性。有關新功能和增強功能的完整列表，請參閱ONTAP 9.17.1 的新增功能 。

- 支援具有自主勒索軟體防護功能的 SAN

  ARP 支援基於加密的異常檢測功能，可支援 SAN 卷，引入用於詳細熵統計的新命令，並統一了系統管理器中先前專注於 NAS 的勒索軟體防護訊息傳遞。可配置的偵測閾值和更確定性的快照保留功能為各種工作負載提供了更大的靈活性。

- HTTP 嚴格傳輸安全性 (HSTS) 支持

  ONTAP 9.17.1 支援 Web 服務的 HTTP 嚴格傳輸安全，以便能夠在使用者瀏覽器和ONTAP之間實作安全的 HTTPS 通訊。

- 透過鏈路聚合組進行 IPsec 硬體卸載

  ONTAP 9.17.1 支援鏈路聚合組的 IPsec 硬體卸載，擴展了ONTAP 9.16.1 中引入的硬體卸載支援。

- IPsec 後量子預共享密鑰支持

  ONTAP支援 IPsec 的後量子預共用金鑰，以防止未來潛在的量子電腦攻擊。

- OpenStack Barbican 金鑰管理器支援

  ONTAP支援 OpenStack 的 Barbican 金鑰管理器用於NetApp磁碟區加密 (NVE) 金鑰。

- 即時 (JIT) 權限提升支持

  ONTAP支援基於角色的存取控制 (RBAC) 的 JIT 權限提升。使用者可以請求臨時提升到已配置的角色，從而按需存取特權命令。叢集管理員可以設定哪些人可以存取 JIT 權限提升，以及何時允許存取以及允許存取多長時間。

- 支援 Entra IdP 和 IdP 群組支援 SAML 身份驗證

  ONTAP支援使用 Microsoft Entra 作為 SAML 身分提供者。此外，IdP 提供的群組資訊可以對應到ONTAP角色。

- SnapMirror主動同步支援透過 NVMe 進行主機訪問

  SnapMirror主動同步功能新增了對 VMware 工作負載的 NVMe 存取支持，支援 NVMe/TCP 和 NVMe/FC 主機訪問，適用於雙節點ONTAP叢集。 VMware

- ONTAP Cloud Mediator 支援SnapMirror主動同步

  ONTAP Cloud Mediator 是ONTAP 9.17.1 中引入的新功能，支援SnapMirror主動同步關係。基於雲端的調解器（例如ONTAP Mediator）可充當SnapMirror主動同步關係的仲裁見證，確保透明的故障轉移，同時降低

維護和管理第三個站點的操作複雜性。

ONTAP 9.16.1 重點介紹

ONTAP 9 。 16.1 在安全管理，資料保護，網路， SAN 管理和儲存管理等領域提供全新且增強的功能。如需新功能與增強功能的完整清單，請參閱ONTAP 9.16.1 的新功能。

- 多重管理驗證（ MAV ）增強功能

  ONTAP 9 。 16.1 在 MAV 架構中新增更多命令，以進一步保護免於惡意內部人員的攻擊。這些增強功能包括許多一致性群組（ CG ）， VScan 和自主勒索軟體保護（ ARP ）管理，以及 NVMe 組態命令。

- 利用 AI 增強功能（ ARP/AI ）提供自主勒索軟體保護

  ARP 已升級為全新的 AI 功能，讓 IT 能夠偵測並回應勒索軟體攻擊，精確程度達 99% ，而且容易回收。由於 AI 受過全方位資料集的訓練，因此在 FlexVol 磁碟區上執行 ARP 不再需要學習一段時間，而且 ARP/AI 會立即以作用中模式啟動。ARP/AI 也推出自動更新功能，不受 ONTAP 升級影響，確保持續保護並抵禦最新威脅。

- 透過 TLS 1.3 的 NVMe / TCP

  透過簡化的組態和比 IPSec 更好的效能，保護通訊協定層的 NVMe / TCP 「無線傳輸」。

- IPsec 硬體卸載支援新的網路卡

  ONTAP 9.16.1 在最新一代的 AFF A 系列和 AFF C 系列系統平台中，將 IPSec 硬體卸載功能運用在卸載卡上，可提供更高的「有線」加密效能。

- 支援 NVMe 空間分配

  NVMe 命名空間現在支援空間釋放（也稱為「打洞」和「取消映射」）。當主機應用程式刪除資料時，空間釋放可協助精簡配置磁碟區和 NVMe 命名空間回收未使用的空間。這大大提高了整體儲存效率，特別是對於資料週轉率高的檔案系統。

- FlexGroup 磁碟區的進階容量平衡

  NetApp FlexGroup Volume 可選擇性地在多個後端組成磁碟區之間的單一檔案中等量資料，減少效能瓶頸，並在平衡後端組成磁碟區的容量時增加一致性。

- SVM 資料移動性支援，可移轉 MetroCluster 組態

  ONTAP 支援下列 MetroCluster SVM 移轉：

  - 在非 MetroCluster 組態和 MetroCluster IP 組態之間移轉 SVM
  - 在兩個 MetroCluster IP 組態之間移轉 SVM
  - 在 MetroCluster FC 組態和 MetroCluster IP 組態之間移轉 SVM

ONTAP 9.15.1 重點介紹

ONTAP 9.15.1 在安全管理、資料保護和 NAS 工作負載支援等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.15.1 的新功能。

- "支援全新 AFF A 系列系統、專為 AI 打造的儲存設備"

  ONTAP 9.15.1 支援全新的高效能 AFF A1K 、 AFF A90 和 AFF A70 系統、專為下一代商業工作負載所設計、例如 AI / ML 訓練和推論。這種新型系統的效能是現有 AFF A 系列產品的兩倍，並可「持續運作」提升儲存效率，而不會影響效能。

- 伺服器上的 Windows 備份應用程式和 Unix 風格的符號鏈接

  從 ONTAP 9.15.1 開始、您也可以選擇備份 symlink 本身、而非指向的資料。這可提供多項優點、包括改善備份應用程式的效能。您可以使用 ONTAP CLI 或 REST API 來啟用此功能。

- 動態授權

  ONTAP 9.15.1 引進動態授權的初始架構、這項安全功能可判斷系統管理員帳戶所發出的命令是否應遭到拒絕、是否提示進行額外驗證、或是否允許繼續。判斷是根據使用者帳戶的信任分數、並考量時間、位置、 IP 位址、信任的裝置使用量、以及使用者的驗證和授權記錄等因素。

- 擴大多管理驗證的影響範圍

  ONTAP 9.15.1 RC1 為 MAV 架構新增了超過一百個命令、以進一步保護免於惡意內部人員的攻擊。

- TLS 1.3 加密支援叢集對等關係等功能

  ONTAP 9.15.1 針對 S3 儲存、 FlexCache 、 SnapMirror 和叢集對等加密、推出 TLS 1.3 加密支援。FabricPool 、 Microsoft Azure Page Blobs 儲存設備和 SnapMirror Cloud 等應用程式在 9.15.1 版中持續使用 TLS 1.2 。

- 支援 TLS 上的 SMTP 流量

  透過支援 TLS 的電子郵件安全傳輸 AutoSupport 資料。

- SnapMirror 主動同步適用於對稱的主動 / 主動式組態

  這項新功能可提供同步雙向複寫、以利業務持續運作和災難恢復。透過跨多個故障網域同時讀取及寫入資料、保護關鍵 SAN 工作負載的資料存取、實現不中斷的作業、並將災難或系統故障期間的停機時間降至最低。

- FlexCache 回寫

  FlexCache 回寫功能可讓用戶端在本機寫入 FlexCache 磁碟區，相較於直接寫入原始磁碟區，可減少延遲並改善效能。新寫入的資料會以非同步方式複寫回原始磁碟區。

- NFSv3 over RDMA

  NFSv3 over RDMA 支援可透過 TCP 提供低延遲、高頻寬存取、協助您解決高效能需求。

ONTAP 9.14.1 重點摘要

ONTAP 9.14.1 在 FabricPool 、反勒索軟體保護、 OAuth 等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.14.1 的新功能。

- WAFL 保留減少

ONTAP 9.14.1 將 WAFL 保留空間減少至 30 TB 以上、可立即增加 5% 的 FAS 和 Cloud Volumes ONTAP 系統可用空間。

- FabricPool 增強功能

  FabricPool 提供更高的效益 讀取效能 並可直接寫入雲端、降低空間不足的風險、並將冷資料移至成本較低的儲存層、進而降低儲存成本。

- "支援 OAuth 2.0"

  ONTAP 支援 OAuth 2.0 架構、可透過系統管理員進行設定。有了 OAuth 2.0 、您就能安全地存取自動化架構的 ONTAP 、而無需建立或將使用者 ID 和密碼公開給純文字指令碼和執行手冊。

- "自主勒索軟體保護（ ARP ）增強功能"

  ARP 可讓您更有效地控制事件安全性、讓您調整建立警示的條件、並降低誤報的可能性。

- SnapMirror 災難恢復在 System Manager 中進行演練

  System Manager 提供簡單的工作流程、可在遠端位置輕鬆測試災難恢復、並在測試後進行清理。此功能可讓測試更輕鬆、更頻繁、並提高恢復時間目標的信心。

- S3 物件鎖定支援

  ONTAP S3 支援物件鎖定 API 命令、可讓您保護寫入 ONTAP S3 的資料、避免遭到刪除使用標準 S3 API 命令、並確保重要資料在適當的時間內受到保護。

- 叢集 和 Volume 標記

  將中繼資料標記新增至磁碟區和叢集、這些標記會隨著資料從內部部署移至雲端並進行反轉。

ONTAP 9.13.1 重點介紹

ONTAP 9.13.1 在防勒索軟體保護、一致性群組、服務品質、租戶容量管理等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.13.1 的新功能。

- 自主勒索軟體保護（ ARP ）增強功能：
  - 自動啟用

    有了 ONTAP 9.13.1 、 ARP 在擁有足夠的學習資料後、就會自動從訓練模式移轉至正式作業模式、免除管理員在 30 天之後啟用的需求。

  - 多重管理驗證支援

    多重管理驗證支援 ARP 停用命令、確保沒有單一管理員可以停用 ARP 、將資料暴露於可能的勒索軟體攻擊之中。

  - FlexGroup 支援

    從 ONTAP 9.13.1 開始， ARP 支援 FlexGroup 磁碟區。ARP 可以監控並保護橫跨叢集中多個磁碟區和節點的 FlexGroup 磁碟區，甚至是最大的資料集都能使用 ARP 來保護。

- 系統管理程式中一致性群組的效能與容量監控

  效能與容量監控可針對每個一致性群組提供詳細資料、讓您在應用程式層級快速識別及報告潛在問題、而不只是在資料物件層級。

- 租戶容量管理

  多租戶客戶和服務供應商可以設定每個 SVM 的容量限制、讓租戶能夠執行自助服務佈建、而不會有一個租戶在叢集上過度使用容量的風險。

- 服務品質的天花板和地板

  ONTAP 9.13.1 可讓您將磁碟區、 LUN 或檔案等物件分組、並指派 QoS 上限（最大 IOPs ）或最低 IOPs （最低 IOPs ）、以改善應用程式效能期望。

ONTAP 9.12.1 重點摘要

ONTAP 9.12.1 在安全強化、保留、效能等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.12.1 的新功能。

- 防竄改快照

  有了 SnapLock 技術，您就可以保護快照，避免在來源或目的地上遭到刪除。

  保護主要與次要儲存設備上的快照、避免勒索軟體攻擊者或惡意系統管理員刪除、進而保留更多恢復點。

- 自主勒索軟體保護（ ARP ）增強功能

  根據主要儲存設備已完成的篩選模式、立即在次要儲存設備上啟用智慧型自主勒索軟體保護。

  容錯移轉之後、立即識別二級儲存設備上可能發生的勒索軟體攻擊。系統會立即擷取開始受到影響的資料，並通知系統管理員，協助阻止攻擊並加強還原。

- FPolicy

  單鍵啟動 ONTAP FPolicy 可自動封鎖已知的惡意檔案簡化的啟動有助於防範使用一般已知副檔名的典型勒索軟體攻擊。

- 安全強化：防竄改保留記錄

  ONTAP 中的防竄改保留記錄可確保遭入侵的系統管理員帳戶不會隱藏惡意動作。如果系統不知情、就無法變更或刪除管理員和使用者歷程記錄。

  記錄並稽核所有管理動作、無論來源為何、都能保證擷取所有影響資料的動作。每當系統稽核記錄遭到竄改、以任何方式通知系統管理員變更時、就會產生警示。

- 安全強化：擴充的多因素驗證

  多重驗證（ MFA） for CLI （ SSH ）支援 Yib金 鑰實體硬體權杖裝置、確保攻擊者無法使用遭竊的認證或遭入侵的用戶端系統來存取 ONTAP 系統。採用 System Manager 的 MFA 支援 Cisco Duo 。

- 檔案物件雙重性（多重傳輸協定存取）

檔案物件雙重性可讓原生 S3 傳輸協定讀取和寫入相同資料來源的存取權、而該資料來源已具有 NAS 傳輸協定存取權。您可以將儲存設備同時存取為檔案或來自相同資料來源的物件、不需要複製資料來搭配不同的傳輸協定（ S3 或 NAS ）使用、例如使用物件資料的分析。

- 重新平衡FlexGroup

  如果 FlexGroup 成分變得不平衡、 FlexGroup 可以不中斷地從重新平衡和管理
  CLI 、 REST API 和 System Manager 。為了達到最佳效能、 FlexGroup 中的成員應平均分配其使用的容量。

- 儲存容量增強功能

  WAFL 空間保留空間已大幅減少，每個聚合最多可提供 40 TiB 更多可用容量。

ONTAP 9.11.1 重點摘要

ONTAP 9.11.1 在安全性、保留、效能等方面提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.11.1 的新功能。

- 多管理員驗證

  多重管理驗證（ MAV ）是業界首創的原生驗證方法，需要多項核准，才能執行敏感的管理工作，例如刪除快照或磁碟區。MAV 實作所需的核准可防止惡意攻擊和資料意外變更。

- 增強的自主勒索軟體保護功能

  自主勒索軟體保護（ ARP ）利用機器學習功能、以更精細的方式偵測勒索軟體威脅、讓您能夠快速識別威脅、並在發生資料外洩時加速恢復。

- SnapLock Compliance for FlexGroup Volumes

  透過 WORM 檔案鎖定保護資料、保護電子設計自動化、媒體與娛樂等工作負載的多 PB 資料集、讓資料無法變更或刪除。

- 非同步目錄刪除

  使用 ONTAP 9.11.1 時、檔案刪除會發生在 ONTAP 系統的背景中、讓您輕鬆刪除大型目錄、同時消除對主機 I/O 的效能和延遲影響

- S3 增強功能

  利用 ONTAP 簡化及擴充 S3 的物件資料管理功能、在儲存區層級提供額外的 API 端點和物件版本設定、讓物件的多個版本儲存在同一個儲存區中。

- System Manager增強功能

  System Manager 支援進階功能、可最佳化儲存資源並改善稽核管理。這些更新包括管理和設定儲存集合體的增強功能、增強系統分析的可見度、以及 FAS 系統的硬體視覺化。

ONTAP 9.10.1 重點摘要

ONTAP 9.10.1 在安全強化、效能分析、 NVMe 傳輸協定支援和物件儲存備份選項等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.10.1 的新功能。

- 自主勒索軟體保護

  自動勒索軟體保護會自動建立磁碟區快照，並在偵測到異常活動時向管理員發出警示，讓您能夠快速偵測勒索軟體攻擊並更快地恢復。

- System Manager增強功能

  系統管理器除了提供與Active IQ Digital Advisor （也稱為Digital Advisor）、 NetApp Console 和憑證管理的新整合外，還會自動下載磁碟、機架、服務處理器的韌體更新。這些增強功能簡化了管理並維持了業務連續性。

- 檔案系統分析增強功能

  檔案系統分析提供額外的遙測功能、可識別檔案共用中的重要檔案、目錄和使用者、讓您識別工作負載效能問題、以改善資源規劃和 QoS 實作。

- AFF 系統的 NVMe over TCP （ NVMe / TCP ）支援

  當您在現有的乙太網路上使用 NVMe / TCP 時、可在 AFF 系統上為企業 SAN 和現代工作負載達成高效能並降低 TCO 。

- NVMe over Fibre Channel （ NVMe / FC ）支援 NetApp FAS 系統

  在混合式陣列上使用 NVMe / FC 傳輸協定、即可統一移轉至 NVMe 。

- 物件儲存的原生混合雲備份

  您可以選擇物件儲存目標來保護 ONTAP S3 資料。使用 SnapMirror 複寫功能、將 StorageGRID 的內部部署儲存設備備份到 Amazon S3 的雲端、或是 NetApp AFF 和 FAS 系統上的另一個 ONTAP S3 儲存區。

- 使用 FlexCache 進行全域檔案鎖定

  使用 FlexCache 進行全域檔案鎖定、以確保在原始伺服器的來源檔案更新期間、快取位置的檔案一致性。這項增強功能可針對需要增強鎖定的工作負載、在原始伺服器對快取關係中啟用專屬的檔案讀取鎖定。

ONTAP 9.9.1 重點摘要

ONTAP 9.91.1 在儲存效率、多因素驗證、災難恢復等領域提供全新且增強的功能。如需新功能與增強功能的完整清單、請參閱 ONTAP 9.9.1 的新功能。

- 增強的 CLI 遠端存取管理安全性

  支援 SHA512 和 SSH A512 密碼雜湊功能、可保護系統管理員帳戶認證免受試圖取得系統存取權的惡意攻擊者攻擊。

- "MetroCluster IP 增強功能：支援 8 節點叢集"

新的上限是前一上限的兩倍、可支援 MetroCluster 組態、並可持續提供資料可用度。

- SnapMirror 主動同步

  針對 NAS 工作負載的大型資料容器、提供更多複寫選項以進行備份和災難恢復。

- 提高 SAN 效能

  為單一 LUN 應用程式（例如 VMware 資料存放區）提供高達四倍的 SAN 效能、讓您在 SAN 環境中達到高效能。

- 混合雲的全新物件儲存選項

  可將 StorageGRID 用作 NetApp Cloud Backup Service 的目的地、以簡化並自動化內部部署 ONTAP 資料的備份作業。

後續步驟

- 升級至最新版的 ONTAP
- 我應該何時升級 ONTAP ？

ONTAP 9.18.1 的新增功能

了解ONTAP 9.18.1 中提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "適用於NetApp AFX 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "適用於NetApp ASA r2 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱"準備升級 ONTAP"。

資料保護

更新	說明
SnapMirror 雲端支援 MetroCluster FlexGroup Volume	SnapMirror cloud 支援在 MetroCluster 組態中的 FlexGroup volume 進行備份與還原作業。

網路

更新	說明
IPsec 硬體卸載 IPv6 支持	IPsec硬體卸載支援已擴展到IPv6。
OpenSSL PQC 演算法	ONTAP支援用於 SSL 的後量子計算加密演算法。這些演算法可針對未來潛在的量子運算攻擊提供額外保護，並且在 SSL FIPS 模式停用時可用。
ONTAP後端叢集網路加密	您可以為ONTAP後端叢集網路上的傳輸中資料啟用 TLS 加密。
ONTAP HA 流量網路加密	您可以為高可用性 (HA) 對中的節點之間的流量啟用加密。

SAN

更新	說明
NVMe 複製卸載	NVMe 複製卸載功能可讓 NVMe 主機將複製作業從其 CPU 解除安裝至ONTAP儲存控制器的 CPU。主機可以將資料從一個 NVMe 命名空間複製到另一個 NVMe 命名空間，同時將其 CPU 資源保留給應用程式工作負載。

S3 物件儲存

更新	說明
支援恢復 S3 快照（時間點）	現在可以透過 ONTAP CLI 直接存取 S3 快照儲存貯體。此外，您還可以從 S3 快照在 S3 用戶端上還原單一物件、一組物件或整個儲存貯體。
支援在 FlexCache 磁碟區上建立 NAS 儲存桶	您可以在 FlexCache 磁碟區上建立 NAS 儲存桶，當叢集中的所有節點都使用 ONTAP 9.18.1 或更新版本時，應用程式可以使用 S3 協定存取 FlexCache 磁碟區上的資料。有關啟用對 NAS FlexCache 磁碟區的 S3 存取的詳細資訊，請參閱"啟用對 NAS FlexCache 磁碟區的 S3 存取"。

安全性

更新	說明
FlexGroup磁碟區支援 ARP/AI	NetApp FlexGroup磁碟區支援 ARP/AI，提供基於機器學習的進階勒索軟體偵測和保護。在ONTAP 9.17.1 及更早版本中， FlexGroup磁碟區僅支援第一代 ARP。從ONTAP 9.18.1 開始， FlexGroup磁碟區在本機ONTAP平台（AFF和FAS）和虛擬ONTAP部署（包括Cloud Volumes ONTAP和ONTAP Select ）上與FlexVol磁碟區具有同等功能。因此，ARP/AI 成為FlexVol和FlexGroup磁碟區的預設 ARP 技術。
在支援的系統上，新磁碟區預設會啟用 ARP/AI	建立新叢集或將叢集升級至 9.18.1 版本時，AFF A 系列、AFF C 系列、ASA 和 "ASA r2"系統的所有新磁碟區在 12 小時寬限期後預設自動啟用 ARP/AI。在此寬限期內，您可以選擇停用預設啟用。

儲存資源管理增強功能

更新	說明
支援在SVM和磁碟區上設定兩級嵌套的QoS策略群組	您可以同時為 SVM 和 SVM 下的磁碟區指派 QoS 策略。
在 SVM-DR 關係中建立來源磁碟區的 SVM FlexCache卷	您可以建立屬於 SVM-DR 關係的來源磁碟區的 SVM FlexCache磁碟區。
用於顯示空間使用資訊的命令	在 ONTAP 9.18.1 及更高版本中，`storage aggregate show-space`命令變更了邏輯引用容量和邏輯非引用容量的報告方式。邏輯引用容量報告所有物件中的引用區塊以及碎片化物件中的非引用區塊。邏輯非引用容量僅報告已超過容量飽和閾值且符合物件刪除和碎片整理條件的物件中的非引用區塊。 例如，當您使用 ONTAP S3 和 StorageGRID 的預設 Aggregate 完整度臨界值 40% 時，物件中 60% 的區塊必須未被引用，然後這些區塊才會被報告為未被引用的容量。 在 ONTAP 9.18.1 之前的版本中，「邏輯引用容量」會報告所有物件（包括已滿物件和碎片物件）中已引用的區塊。「邏輯未引用容量」會報告所有物件中未引用的區塊。

ONTAP 9.17.1 的新增功能

了解ONTAP 9.17.1 中提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "適用於NetApp AFX 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "適用於NetApp ASA r2 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱"準備升級 ONTAP"。

資料保護

更新	說明
SnapMirror主動同步支援透過 NVMe 進行主機訪問	SnapMirror主動同步功能新增了對 VMware 工作負載的 NVMe 存取支持，支援 NVMe/TCP 和 NVMe/FC 主機訪問，適用於雙節點ONTAP叢集。VMware工作負載對 NVMe/TCP 的支援取決於 VMware 漏洞的修復情況。

更新	說明
ONTAP Cloud Mediator 支援SnapMirror主動同步	ONTAP Cloud Mediator 是ONTAP 9.17.1 中引入的新功能，支援SnapMirror主動同步關係。基於雲端的調解器（例如ONTAP Mediator）可充當SnapMirror主動同步關係的仲裁見證，確保透明的故障轉移，同時降低維護和管理第三個站點的操作複雜性。

S3 物件儲存

更新	說明
ONTAP S3 NAS 儲存桶中的 CopyObject 操作支持	ONTAP S3 NAS 儲存桶支援 CopyObject 操作。
支援將 S3 NAS 儲存桶連結到連線路徑	使用ONTAP CLI 建立 S3 NAS 儲存桶時，您可以選擇將儲存桶連結到卷，而不是使用連線路徑。連結到磁碟區時，如果路徑發生變化（例如，卸載或掛載磁碟區時），連線路徑會自動更新。
S3 多協定支援標記和元數據	在多協定（S3 和 NAS）環境中，CreateMultipartUpload 操作支援標記和使用者元資料鍵/值對。

安全性

更新	說明
自主勒索軟體防護快照更新	ONTAP對 ARP 快照進行了多項更新。
HTTP 嚴格傳輸安全性 (HSTS) 支持	ONTAP支援 Web 服務的 HTTP 嚴格傳輸安全，因此能夠在使用者瀏覽器和ONTAP之間實作安全的 HTTPS 通訊。
透過鏈路聚合組進行 IPsec 硬體卸載	ONTAP支援鏈路聚合組的 IPsec 硬體卸載，擴展了 9.16.1 中引入的硬體卸載支援。
IPsec 後量子預共享密鑰支持	ONTAP支援 IPsec 的後量子預共用金鑰，以防止未來潛在的量子電腦攻擊。
OpenStack Barbican 金鑰管理器支援	ONTAP支援 OpenStack 的 Barbican 金鑰管理器用於NetApp磁碟區加密 (NVE) 金鑰。
即時 (JIT) 權限提升支持	ONTAP支援基於角色的存取控制 (RBAC) 的 JIT 權限提升。使用者可以請求臨時提升到已配置的角色，從而按需存取特權命令。叢集管理員可以設定哪些人可以存取 JIT 權限提升，以及何時允許存取以及允許存取多長時間。
支援 Entra IdP 和 IdP 群組支援 SAML 身份驗證	ONTAP支援使用 Microsoft Entra 作為 SAML 身分提供者。此外，IdP 提供的群組資訊可以對應到ONTAP角色。

更新	說明
跨集群請求審計	您可以在啟動來源叢集和目標（執行）叢集上配置並執行稽核作業。在先前的版本中，只有接收客戶端請求的叢集才會執行稽核。借助此功能，滿足跨群集請求的對等群集也會記錄該活動。這些審計操作可以啟用並擴展到在ONTAP中發起的任何 SET 或 GET 請求。
支援具有自主勒索軟體防護功能的 SAN	ARP 支援基於加密的異常檢測功能，可支援 SAN 卷，引入用於詳細熵統計的新命令，並統一了系統管理器中先前專注於 NAS 的勒索軟體防護訊息傳遞。可配置的偵測閾值和更確定性的快照保留功能為各種工作負載提供了更大的靈活性。

儲存資源管理增強功能

更新	說明
預設情況下，新磁碟區啟用 FSA	在ONTAP叢集上新建的 SVM 上建立的磁碟區（如果已指派 NAS 協定）預設啟用檔案系統分析 (FSA)。 FSA會在磁碟區建立後立即自動激活，無需額外配置即可提供即時分析功能。
增強了對查看FlexGroup磁碟區上的直接刪除進度的支持	ONTAP CLI 指令 `volume file async-delete show`已增強，包括從客戶端發出的非同步刪除作業。

ONTAP 9.16.1 的新增功能

瞭解 ONTAP 9.16.1 中提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "適用於NetApp ASA r2 儲存系統的全新增強型ONTAP軟體功能" 。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱"準備升級 ONTAP"。

資料保護

更新	說明
支援 SnapMirror 主動式同步的多節點模式	SnapMirror 主動式同步可從先前的雙節點限制擴充，支援四節點叢集，為較大型的工作負載提供資料複寫功能。

更新	說明
SnapMirror 雲端支援建立扇出關係	SnapMirror 雲端支援從相同來源 Volume 或 FlexGroup 到兩個不同物件存放區的扇出關係。扇出可以是兩個物件存放區，以及物件存放區中的一或兩個貯體。
支援從移轉的磁碟區進行 SnapMirror 雲端備份	SnapMirror 雲端支援使用現有的 ONTAP REST API 將移轉至雲端的磁碟區備份。這項新功能可支援從雲端中移轉的磁碟區到相同目的地物件儲存區端點的 SnapMirror 雲端備份，而無需執行重新基準化作業。支援 FlexVol 和 FlexGroup 磁碟區。

網路

更新	說明
BGP 對等群組的 MD5 驗證支援	ONTAP 支援 BGP 對等群組上的 MD5 驗證，以保護 BGP 工作階段。啟用 MD5 時， BGP 工作階段只能在獲授權的對等點之間建立和處理，防止攻擊者嘗試利用 BGP 更新將假路由資訊注入網路等攻擊。
IPsec 硬體卸載支援	IP 安全性（ IPsec ）是資料傳輸安全選項，可用來保護用戶端和 ONTAP 節點之間的所有 IP 流量。此傳輸協定最初是以 ONTAP 9 8 提供，並僅以軟體形式實作。從 ONTAP 9 · 16.1 開始，您可以選擇將某些運算密集的作業（例如加密和完整性檢查）卸載到儲存節點上安裝的支援網路介面控制器（ NIC ）卡。使用此硬體卸載選項可大幅改善受 IPsec 保護的網路流量的效能和處理量。

S3 物件儲存

更新	說明
多重傳輸協定 S3 貯體支援 S3 物件中繼資料和標記	從 ONTAP 9.16.1 開始， S3 物件標記從非多重傳輸協定 ONTAP S3 儲存區延伸至 NAS 和 S3 多重傳輸協定 ONTAP S3 儲存區。標籤只能在 S3 傳輸協定中看到。使用 S3 用戶端套用到 "標記和中繼資料" S3 物件，有助於定義儲存為 ONTAP 中物件或檔案之資料的生命週期，恢復收費，資料類別及自訂工作流程。當與 AWS 資料服務（例如 bedrock 或 Athena ）整合時，標記和中繼資料會成為這些服務所提供 Data Processing 的核心。 ONTAP 9.9.1 開始支援原生 S3 儲存區中的標記和使用者定義中繼資料。
多重傳輸協定 S3 貯體支援多重部分上傳	多部分上傳是一項核心 S3 功能，自一開始就適用於非多重傳輸協定的 ONTAP S3 儲存區。從 ONTAP 9.16.1 開始，這項核心功能已延伸至 NAS 和 S3 多重傳輸協定 ONTAP S3 儲存區。
支援 ONTAP S3 儲存區的跨來源資源共享（ CORS ）	透過跨來源資源共享（ CORS ），充分發揮網路應用程式的潛力。CORS 可讓用戶端應用程式在一個網域和另一個網域中的資源之間順暢互動。透過整合 CORS 支援，您可以透過選擇性的跨來源存取資源，讓 ONTAP S3 型網路應用程式更具能力。

更新	說明
ONTAP 支援拍攝 ONTAP S3 儲存區的快照	您可以為 ONTAP S3 儲存區產生唯讀的時間點快照。使用 S3 快照功能，您可以手動建立快照，或透過快照原則自動產生快照。此外，您可以檢視，瀏覽及刪除 S3 快照，並透過 S3 用戶端還原快照內容。

SAN

更新	說明
NVMe 空間取消分配預設為啟用	預設情況下，NVMe 命名空間啟用空間釋放（也稱為「打洞」和「取消映射」）。空間釋放允許主機從命名空間中釋放未使用的區塊以回收空間。這大大提高了整體儲存效率，特別是對於資料週轉率高的檔案系統。

安全性

更新	說明
符合資格的規則保護命令集已延伸、可進行多重管理驗證	系統管理員可以建立多重管理驗證規則來保護一致性群組，包括建立，刪除及修改作業，建立及刪除一致性群組快照及其他命令。
利用 AI 增強功能（ARP/AI）提供自主勒索軟體保護	ARP 已升級為全新的 AI 功能，讓 IT 能夠偵測並回應勒索軟體攻擊，精確程度達 99% ，而且容易回收。由於 AI 受過全方位資料集的訓練，因此在 FlexVol 磁碟區上執行 ARP 不再需要學習一段時間，而且 ARP/AI 會立即以作用中模式啟動。ARP/AI 也隨附自動更新功能，可確保持續提供保護並抵抗最新威脅。 ARP/AI 功能目前僅支援 NAS 。雖然自動更新功能會顯示系統管理員中部署的新安全檔案可用度，但這些更新僅適用於 NAS 工作負載保護。
透過 TLS 1.3 的 NVMe / TCP	透過簡化的組態和比 IPSec 更好的效能，保護通訊協定層的 NVMe / TCP 「無線傳輸」。
支援 FabricPool 物件存放區通訊的 TLS 1.3	ONTAP 支援 FabricPool 物件存放區通訊的 TLS 1.3 。
Microsoft Entra ID 的 OAuth 2.0	OAuth 2.0 支援是由 ONTAP 9 .14.1 首次推出，已經過強化，可支援採用標準 OAuth 2.0 宣告的 Microsoft Entra ID 授權伺服器（前身為 Azure AD ）。此外，新的群組和角色對應功能也支援以 UUID 樣式值為基礎的 Entra ID 標準群組宣告。我們也推出新的外部角色對應功能，此功能已經過 Entra ID 測試，但可搭配任何支援的授權伺服器使用。

儲存效率

更新	說明
延伸 qtree 效能監控，包括延遲指標和歷史統計資料	較早的 ONTAP 版本針對 qtree 使用量提供強大的即時指標，例如每秒 I/O 作業數，以及多個類別的處理量（包括讀取和寫入）。從 ONTAP 9 。 16.1 開始，您也可以存取即時延遲統計資料，以及檢視歸檔的歷史資料。這些新功能可讓 IT 儲存管理員更深入地瞭解系統效能，並能更長時間分析趨勢。如此一來，您就能針對資料中心和雲端儲存資源的營運與規劃，做出更明智且資料導向的決策。

儲存資源管理增強功能

更新	說明
在啟用儲存限制的 SVM 中支援資料保護磁碟區	已啟用儲存限制的 SVM 可包含資料保護磁碟區。支援非同步災難恢復關係中的 FlexVol Volume ，不含串聯，同步災難恢復關係和還原關係。 在 ONTAP 9.15.1 及更早版本中，無法針對任何包含資料保護磁碟區， SnapMirror 關係中的磁碟區或 MetroCluster 組態的 SVM 設定儲存限制。
支援 FlexGroup 進階容量分配	啟用時，進階容量平衡功能會在 FlexGroup 成員磁碟區之間的檔案內分散資料，如此一來，就能在一個成員磁碟區上大幅增加檔案並佔用空間。
SVM 資料移動性支援，可移轉 MetroCluster 組態	ONTAP 支援下列 MetroCluster SVM 移轉： • 在非 MetroCluster 組態和 MetroCluster IP 組態之間移轉 SVM • 在兩個 MetroCluster IP 組態之間移轉 SVM • 將 SVM 從 MetroCluster FC 組態移轉至 MetroCluster IP 組態

系統管理員

更新	說明
支援 System Manager 中的網路釣魚防護 WebAuthn 多重驗證	ONTAP 9 。 16.1 支援 WebAuthn MFA 登入，可讓您在登入系統管理員時使用硬體安全金鑰作為第二種驗證方法。

ONTAP 9.15.1 的新增功能

瞭解 ONTAP 9.15.1 提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF 、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。

- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱"準備升級 ONTAP"。

資料保護

更新	說明
伺服器上的 Windows 備份應用程式和 Unix 風格的符號鏈接	當 Windows 備份應用程式遇到 Unix 樣式的符號連結（ symlink ）時、連結就會跟隨、實際資料會由 ONTAP 傳回並備份。從 ONTAP 9.15.1 開始、您也可以選擇備份 symlink 本身、而非指向的資料。這可提供多項優點、包括改善備份應用程式的效能。您可以使用 ONTAP CLI 或 REST API 來啟用此功能。
SnapMirror 主動同步支援對稱式主動 / 主動式部署	SnapMirror 主動式同步（前身為 SnapMirror Business Continuity ）現在支援對稱式主動 / 主動式部署、可透過雙向同步複寫、從受保護 LUN 的兩個複本進行讀寫 I/O 作業。
使用 SnapMirror 非同步增加一致性群組中磁碟區的限制	使用 SnapMirror 非同步保護的一致性群組現在支援一致性群組中最多 80 個磁碟區。
支援系統管理權限層級、以使用一致性群組進行 REST API 和 CLI 作業	系統管理權限層級現在支援一致性群組的 CLI 和 REST API 作業。
使用 Windows Server 容錯移轉叢集持續保留 VMware 虛擬磁碟區	ONTAP 目前支援 VMware 虛擬磁碟區（ vVols ）、以及傳統 LUN 的持續保留。從 ONTAP 9.15.1 開始、您也可以使用 vVol 建立持續保留。ONTAP Tools for VMware vSphere 9 已實作此功能的支援。只有 Windows Server 容錯移轉叢集（ WSFC ）是一組叢集式 Windows 虛擬機器、才支援此功能。

安全性

更新	說明
簡化的 FPolicy 持續儲存區建立與組態	您可以使用建立 FPolicy 持續儲存區、並同時自動化其磁碟區建立與組態 `persistent-store create` 命令。 增強功能 `persistent-store create` 命令也允許使用 autosup-mode 參數、此參數可讓磁碟區根據使用的空間量來增加或縮小大小。
支援採用 RDMA 的 NFSv3	NFS over RDMA 組態現在支援 NFSv3 。
FPolicy 支援 NFS 4.1 傳輸協定	FPolicy 支援 NFS 4.1 傳輸協定。

更新	說明
FPolicy 的原型引擎格式支援	Prototbuf 是 Google 的語言中立機制、用於序列化結構化資料。它比 XML 更小、更快、更簡單、有助於改善 FPolicy 效能。 您可以使用 probuf 外部引擎格式。設為 probuf 時、通知訊息會使用 Google Prototbuf 以二進位格式編碼。在將外部引擎格式設定為 protobuf 之前、請確定 FPolicy 伺服器也支援 protobuf 反序列化。
SSH 連線的動態授權	ONTAP 9.15.1 提供動態授權的初始架構、可讓您指派安全性信任分數給系統管理員使用者、並在其活動看起來可疑時、透過額外的授權檢查來挑戰他們、以加強管理 ONTAP 系統的安全性。 您可以利用動態授權做為資料導向的 Zero Trust 安全架構的一部分。
支援用於 S3 儲存、 FlexCache 和叢集對等加密的 TLS 1.3	自 ONTAP 9.11.1 開始支援 TLS 1.3 進行管理存取、但 ONTAP 9.15.1 現在支援 S3 儲存、 FlexCache 和叢集對等加密。某些應用程式（例如 FabricPool 、 Microsoft Azure Page Blobs 儲存設備和 SnapMirror Cloud ）在 9.15.1 版中仍僅限使用 TLS 1.2 。
符合資格的規則保護命令集已延伸、可進行多重管理驗證	系統管理員可以建立多重管理驗證規則、以保護叢集組態、 LUN 刪除、系統組態、 IPsec 和 SAML 的安全組態、磁碟區快照作業、虛擬伺服器組態和其他命令。
使用含 TLS 的 SMTP 傳輸 AutoSupport 訊息	雖然建議將 AutoSupport 訊息傳輸至 NetApp 的是 HTTPS 、但未加密的 SMTP 也可以使用。有了 ONTAP 9.15.1 、客戶現在可以選擇將 TLS 與 SMTP 搭配使用。SMTPS 傳輸協定會加密電子郵件流量和選用的電子郵件伺服器認證、藉此建立安全的傳輸通道。使用明確的 TLS 、因此在建立 TCP 連線後會啟動 TLS 。如果訊息複本傳送至本機電子郵件地址、則會使用相同的組態。

儲存效率

更新	說明
磁碟區空間度量報告變更	我們引進了兩個新的計數器、僅顯示正在使用的中繼資料。此外、已調整數個現有計數器、以移除中繼資料並僅顯示使用者資料。這些變更共同提供更清楚的檢視、讓您瞭解分隔成兩種資料類型的度量。客戶可以使用這些計數器來實作更準確的計費模式、方法是從總計中扣除中繼資料、並僅考慮實際的使用者資料。
CPU 或專用卸載處理器的儲存效率	ONTAP 在 AFF A70 、 AFF A90 和 AFF A1K 平台上提供儲存效率和資料壓縮功能。視平台而定、壓縮是使用主 CPU 或專用卸載處理器來執行。儲存效率會自動啟用、無需組態。

儲存資源管理增強功能

更新	說明
FlexCache 回寫支援	在快取磁碟區上啟用回寫時，寫入要求會傳送至本機快取，而非原始磁碟區，為邊緣運算環境和具有大量寫入工作負載的快取提供更好的效能。
檔案系統分析的效能提升	ONTAP 強制規定、在啟用檔案系統分析時、必須釋放容量的 5-8% 、以減輕 Volume 和檔案系統分析的潛在效能問題。
FlexClone Volume 加密金鑰	FlexClone Volume 會被指派獨立於 FlexVol Volume （主機）加密金鑰的專用加密金鑰。

系統管理員

更新	說明
系統管理員支援設定 SnapLock 資料保險箱關係	當來源和目的地同時執行 ONTAP 9.15.1 或更新版本時、可使用系統管理員來設定 SnapLock 資料保險箱關係。
System Manager 儀表板的效能增強功能	System Manager 儀表板健全狀況、容量、網路和效能檢視上的資訊包括更完整的說明、包括效能指標的增強功能、可協助您識別並疑難排解延遲或效能問題。

升級

更新	說明
在自動不中斷升級期間、支援 LIF 移轉至 HA 合作夥伴節點	如果在自動不中斷升級期間、 LIF 移轉至其他批次群組失敗、則會將生命體移轉至同一個批次群組中的 HA 合作夥伴節點。

ONTAP 9.14.1 的新功能

瞭解 ONTAP 9.14.1 提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
SVM 根磁碟區支援 NVE	SVM 根磁碟區可以使用具有 NetApp Volume Encryption 的唯一金鑰來加密。
能夠在長期保留快照上設定快照鎖定和重新初始化 Compliance 時鐘	在具有 SnapLock 授權的叢集上，可為非 SnapLock SnapMirror 目的地磁碟區上建立的快照設定防竄改快照鎖定，而當沒有 SnapLock 磁碟區時，也可以初始化法規遵循時鐘。
SnapMirror Active Sync 支援 SCIS3 持續保留和 Windows 容錯移轉叢集	SCSI3 持續保留和 Window 容錯移轉叢集 for SnapMirror 主動式同步支援多個節點存取裝置、同時封鎖對其他節點的存取、確保不同應用程式環境的叢集作業保持一致且穩定。
使用一致性群組複製 Volume 精細的快照	您可以利用一致性群組，將非同步 SnapMirror 快照和磁碟區精細快照複寫到目的地一致性群組，以進行額外的災難恢復層。
在 SVM 災難恢復關係中支援一致性群組的非同步資料保護	如果 SVM 包含一致性群組、則為 SVM 災難恢復設定的 SVM 可將一致性群組資訊複寫到次要站台。
"SnapMirror 非同步支援 20 個扇出目標"	使用 ONTAP 9.14.1 時、 A700 及更高系統支援的 SnapMirror 非同步扇出目標數量從 16 個增加至 20 個。
從加密來源建立未加密的快取	從 ONTAP 9.14.0 開始、 FlexCache 支援從加密來源建立未加密的 FlexCache Volume 。在舊版 ONTAP 中、當快取來源已加密時、 FlexCache 建立失敗。
CLI 支援一致性群組	使用 ONTAP CLI 管理一致性群組。

檔案存取通訊協定

更新	說明
NFSv4.1 工作階段主幹	工作階段主幹可讓多個路徑通往匯出的資料存放區。如此可簡化管理、並隨著工作負載的擴充而提升效能。它特別適用於具有 VMware 工作負載的環境。

S3 物件儲存

更新	說明
S3 FlexGroup 磁碟區已啟用自動調整大小功能、以避免在磁碟區上建立儲存區時過度分配容量	在新的或現有的 FlexGroup 磁碟區上建立或刪除貯體時、會將這些磁碟區調整為所需的最小大小。所需的最小大小是 FlexGroup Volume 中所有 S3 儲存區的總大小。
S3 物件儲存支援鏡射和無鏡射的集合體	您可以在 MetroCluster IP 和 FC 組態中的鏡射或無鏡射集合體中、在 SVM 上啟用 S3 物件儲存伺服器。
根據使用者角色和鎖定保留期間鎖定物件	S3 儲存區中的物件可以鎖定、避免遭到覆寫或刪除。鎖定物件的能力取決於特定使用者或時間。
設定 LDAP 使用者群組的存取權限、以支援外部目錄服務、並新增存取和秘密金鑰的有效期間	ONTAP 系統管理員可以設定輕量型目錄存取傳輸協定（ LDAP ）或 Active Directory 使用者群組對 ONTAP S3 物件儲存設備的存取權、以便在 LDAP 快速繫結模式中啟用驗證。本機或網域群組或 LDAP 群組中的使用者可以為 S3 用戶端產生自己的存取和秘密金鑰。 您可以為 S3 使用者的存取金鑰和秘密金鑰定義有效期間。 ONTAP 支援如的變數 `$aws:username` 適用於庫位原則和群組原則。

SAN

更新	說明
NVMe / TCP 自動主機探索	根據預設、使用 NVMe / TCP 傳輸協定的控制器主機探索是自動化的。
NVMe / FC 主機端報告和疑難排解	根據預設、 ONTAP 支援 NVMe / FC 主機透過唯一識別碼來識別虛擬機器、並支援 NVMe / FC 主機監控虛擬機器資源使用率。這可強化主機端報告和疑難排解。
NVMe 主機優先順序	您可以設定 NVMe 子系統、以優先分配特定主機的資源。指派高優先順序的主機會分配較大的 I/O 佇列數和較大的佇列深度。

安全性

更新	說明
支援適用於 SSH 使用者的 Cisco 雙核心多因素驗證	SSH 使用者可在登入期間使用 Cisco Duo 進行驗證、作為驗證的第二個因素。
"OAuth 2.0 支援增強功能"	ONTAP 9.14.1 擴充了 ONTAP 9.14.0 最初提供的核心權杖型驗證和 OAuth 2.0 支援。您可以使用 Active Directory 或 LDAP 來設定授權、並進行群組對角色對應。也支援寄件者限制的存取權杖、並根據相互 TLS （ MTLS ）來保護其安全。除了 Auth0 和 Keycloak 之外、 Microsoft Windows Active Directory Federation Service （ ADFS ）也支援身分識別提供者（ IDP ）。
"OAuth 2.0 授權架構"	新增開放式授權（ OAuth 2.0 ）架構、並為 ONTAP REST API 用戶端提供權杖型驗證。這可利用以 REST API 指令碼或 Ansible 為基礎的自動化工作流程、更安全地管理 ONTAP 叢集。支援標準 OAuth 2.0 功能、包括發卡行、對象、本機驗證、遠端自我反省、 遠端使用者宣告及 Proxy 支援。用戶端授權可以使用獨立的 OAuth 2.0 範圍或對應本機 ONTAP 使用者來設定。支援的身分識別提供者（ IDP ）包括使用多個並行伺服器的驗證 0 和 Keycloak 。
可調警示、提供自動勒索軟體保護	設定「自動勒索軟體保護」，以便在偵測到新的副檔名或擷取 ARP 快照時接收通知，並收到可能發生勒索軟體事件的早期警告。
FPolicy 支援持續儲存區、以減少延遲	FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步和非同步強制組態。
FPolicy 支援 SMB 上的 FlexCache 磁碟區	FPolicy 支援 FlexCache Volume 搭配 NFS 或 SMB 。以前、 FlexCache Volume 不支援使用 SMB 的 FPolicy 。

儲存效率

更新	說明
檔案系統分析中的掃描追蹤	追蹤檔案系統分析初始化掃描、並即時深入瞭解進度和節流。
增加 FAS 平台上的可用 Aggregate 空間	對於 FAS 平台、大於 30TB 大小的 WAFL 保留區會從 10% 降至 5% 、進而增加聚合中的可用空間。

更新	說明
TSSE 磁碟區中實體使用空間的報告變更	在已啟用溫度敏感儲存效率（ TSSE ）的磁碟區上、用於報告磁碟區所用空間量的 ONTAP CLI 度量、包括因 TSSE 所節省的空間。此度量會反映在 Volume show -physical used 和 volume show-space -physical used 命令中。 對於 FabricPool 、的價值 `-physical-used` 是容量層和效能層的組合。 如需特定命令、請參閱 `volume show` 和連結： `volume show space`。

儲存資源管理增強功能

更新	說明
主動式 FlexGroup 重新平衡	FlexGroup Volume 支援自動將目錄中不斷成長的檔案移至遠端成員、以減少當地成員的 I/O 瓶頸。
FlexGroup 磁碟區中的快照標記	您可以在中新增，修改及刪除標記和標籤（註解），以協助識別快照，並避免意外刪除 FlexGroup 磁碟區中的快照。
使用 FabricPool 直接寫入雲端	FabricPool 新增了將資料寫入 FabricPool 中磁碟區的功能、因此它可以直接移至雲端、而無需等待分層掃描。
FabricPool 積極預先讀取	FabricPool 在其支援的所有平台中提供對卷檔案的積極預讀功能。

SVM 管理增強功能

更新	說明
SVM 資料移動性支援移轉包含使用者和群組配額及 qtree 的 SVM	SVM 資料移動性新增了移轉 SVM 的支援、其中包含使用者和群組配額及 qtree 。
每個 SVM 最多支援 400 個磁碟區、最多支援 12 個 HA 配對、而使用 SVM 資料移動功能的 pNFS 則支援 NFS 4.1	SVM 資料移動性支援的每個 SVM 磁碟區數量上限增加至 400 個、而支援的 HA 配對數則增加至 12 個。

系統管理員

更新	說明
SnapMirror 測試容錯移轉支援	您可以使用 System Manager 來執行 SnapMirror 測試容錯移轉排練、而不會中斷現有的 SnapMirror 關係。
廣播網域中的連接埠管理	您可以使用 System Manager 來編輯或刪除已指派給廣播網域的連接埠。
啟用 Mediator 輔助自動非計畫性切換（ MAUSO ）	執行 IP MetroCluster 切換和切換時、您可以使用系統管理員來啟用或停用 Mediator 輔助的自動非計畫性切換（ MAUSO ）。
叢集 和 Volume 標記	您可以使用 System Manager 使用標記、以不同方式分類叢集和磁碟區、例如依用途、擁有者或環境。當有許多物件屬於同一類型時、這項功能非常實用。使用者可以根據指派給它的標記、快速識別特定物件。
強化一致性群組監控支援	System Manager 會顯示一致性群組使用量的歷史資料。

更新	說明
NVMe 頻內驗證	您可以使用 System Manager 、使用 DH-HMAC-CHAP 驗證傳輸協定、透過 NVMe / TCP 和 NVMe / FC 傳輸協定、在 NVMe 主機和控制器之間設定安全、單向和雙向驗證。
支援將 S3 儲存區生命週期管理延伸至 System Manager	您可以使用 System Manager 來定義刪除貯體中特定物件的規則、並透過這些規則使這些貯體物件過期。

ONTAP 9.13.1 的新功能

瞭解 ONTAP 9.13.1 提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
"多管理員驗證"	叢集管理員可以在叢集上明確啟用多重管理驗證、以在執行某些 SnapLock 作業之前要求仲裁核准。
"增強了對管理一致性群組的支援、包括 Volume Move 和幾何"	您可以在一致性群組之間移動磁碟區、修改階層式一致性群組的幾何形狀、並將容量洞見納入一致性群組。System Manager 支援使用新的 NAS 磁碟區或 NVMe 命名空間來建立一致性群組。
"使用 SnapMirror Synchronous 進行 NDMP 還原"	SnapMirror 同步支援 NDMP 還原。
SnapMirror 主動同步增強功能	• "使用主動式 SnapMirror 主動式同步關係、以不中斷營運的方式將磁碟區新增至一致性群組。" • "使用 SnapMirror 主動式同步的 NDMP 還原"。
"利用單一一致性群組來支援非同步 SnapMirror"	一致性群組支援非同步 SnapMirror 組態、可為單一一致性群組儲存 SnapMirror 備份。

檔案存取通訊協定

更新	說明
"NFSv4.x storepool 支援"	少數用戶端使用過多的 NFSv4.x 儲存資源、導致其他 NFSv4.x 用戶端因為 NFSv4.x 儲存資源無法使用而遭到封鎖。您可以選擇啟用拒絕和封鎖在其環境中使用大量 NFSv4.x storepool 資源的用戶端。

網路

更新	說明
擴充硬體支援 RDMA 叢集互連	ONTAP 支援 AFF A900 、 ASA A900 和 FAS9500 系統、用於叢集互連 RDMA 與 X91153A 叢集 NIC 、有助於減少延遲、縮短容錯移轉時間、並加速節點之間的通訊。
增加資料 LIF 限制	ONTAP 為 HA 配對和叢集增加資料 LIF 擴充限制、提供更大的靈活度。
在 A800 和 FAS8700 平台上進行叢集設定時支援 IPv6	在 A800 和 FAS8700 平台上、您可以使用 ONTAP CLI 在僅 IPv6 的網路環境中建立和設定新叢集。

S3 物件儲存

更新	說明
S3 貯體生命週期管理	S3 物件到期動作定義貯體中的物件何時過期。這項功能可讓您管理物件版本、以符合保留要求、並有效管理整個 S3 物件儲存。

SAN

更新	說明
支援 AIX 主機上的 NVMe / FC	ONTAP 支援 AIX 主機上的 NVMe / FC 傳輸協定。請參閱 "NetApp 互通性工具" 適用於支援的組態。

安全性

功能	說明
自主勒索軟體保護	• 多管理驗證功能與自主勒索軟體保護 • 從學習模式自動轉換為使用中模式 • FlexGroup 支援包括分析及報告 FlexGroup 磁碟區和作業、包括擴充 FlexGroup 磁碟區、 FlexVol 至 FlexGroup 轉換、 FlexGroup 重新平衡。
使用 Active Directory 進行 SSH 公開金鑰驗證	您可以使用 SSH 公開金鑰做為 Active Directory （ AD ）使用者的主要驗證方法、也可以在 AD 使用者之後使用 SSH 公開金鑰做為次要驗證方法。
使用 SSH 公開金鑰的 X.509 憑證	ONTAP 可讓您將 X.509 憑證與帳戶的 SSH 公開金鑰建立關聯、讓您在登入 SSH 時、能夠更安全地進行憑證過期和撤銷檢查。
FPolicy 檔案存取失敗通知	FPolicy 支援存取遭拒事件的通知。由於缺乏權限而產生檔案作業的通知失敗，包括由於 NTFS 權限而失敗，由於 Unix 模式位元而失敗，以及 NFSv4 ACL 失敗。

功能	說明
採用 TOTP 的多因素驗證（時間型一次性密碼）	使用時間型一次性密碼（ TOTP ）設定具有多因素驗證的本機使用者帳戶。TOTP 永遠是第二種驗證方法。您可以使用 SSH 公開金鑰或使用者密碼做為主要驗證方法。

儲存效率

更新	說明
變更系統管理員的主要資料減量比率報告	System Manager 中顯示的主要資料減量比率不再包含計算中的快照空間節約。它僅描述已用邏輯空間和已用實體空間之間的比率。在舊版 ONTAP 中，主要資料減量比率包括快照的顯著空間減量效益。因此、當您升級至 ONTAP 9.13.1 時、您會發現回報的主要比率明顯降低。您仍可在「 容量」詳細資料檢視中查看含快照的資料減量比率。
對溫度敏感的儲存效率	對溫度敏感的儲存效率可增加連續實體區塊的連續包裝、以提高儲存效率。當系統升級至 ONTAP 9.13.1 時、已啟用溫度敏感儲存效率的磁碟區將會自動啟用連續封裝。
邏輯空間強制	SnapMirror 目的地支援邏輯空間強制執行。
儲存 VM 容量限制支援	您可以在儲存 VM （ SVM ）上設定容量限制、並在 SVM 接近百分比臨界值時啟用警示。

儲存資源管理增強功能

更新	說明
增加最大 inode 數量	ONTAP 將繼續自動新增 inode （以每 32 KB 磁碟區空間 1 inode 的速度）、即使磁碟區成長超過 680 GB 。ONTAP 將繼續新增 inode 、直到達到 2,040,109,451 上限為止。
支援在 FlexClone 建立期間指定 SnapLock 類型	在建立讀寫磁碟區的 FlexClone 時、您可以指定三種 SnapLock 類型之一、無論是法規遵循、企業或非 SnapLock 。
依預設啟用檔案系統分析	將檔案系統分析設為在新磁碟區上預設啟用。
SVM 災難恢復與 FlexGroup Volume 的扇出關係	移除具有 FlexGroup 磁碟區的 SVM DR 的移除限制。 SVM DR 搭配 FlexGroup 、可支援與八個站台之間的 SnapMirror 扇出關係。
單一 FlexGroup 重新平衡作業	您可以排程單一 FlexGroup 重新平衡作業、以便在您指定的未來日期和時間開始。
FabricPool 讀取效能	FabricPool 為單一和多串流工作負載提供更好的循序讀取效能、以利雲端駐留資料和分層處理量。這項改善可將較高的獲得和置入率傳送至後端物件存放區。如果您有內部部署物件存放區、則應考慮物件存放區服務的效能保留空間、並判斷是否需要限制 FabricPool 放置。
調適性 QoS 原則範本	Adaptive QoS 原則範本可讓您在 SVM 層級設定處理量層級。

SVM 管理增強功能

更新	說明
SVM資料移動性	增加移轉最多 200 個磁碟區的 SVM 的支援。

系統管理員

從ONTAP 9.12.1 開始，系統管理器與NetApp控制台整合。詳細了解System Manager 與NetApp Console 集成。

更新	說明
主要資料減量比率的報告變更	System Manager 中顯示的主要資料減量比率不再包含計算中的快照空間節約。它僅描述已用邏輯空間和已用實體空間之間的比率。在舊版 ONTAP 中，主要資料減量比率包括快照的顯著空間減量效益。因此、當您升級至 ONTAP 9.13.1 時、您會發現回報的主要比率明顯降低。您仍可在容量詳細資料檢視中，查看含快照的資料減量比率。
防竄改快照鎖定	您可以使用系統管理員鎖定非 SnapLock 磁碟區上的快照，以防止勒索軟體攻擊。
支援外部金鑰管理員	您可以使用 System Manager 來管理外部金鑰管理員、以儲存及管理驗證和加密金鑰。
疑難排解硬體問題	System Manager 使用者可以在「硬體」頁面中檢視其他硬體平台的視覺化說明、包括 ASA 平台和 AFF C 系列平台。 ONTAP 9.12.1 、 ONTAP 9.11.1 和 ONTAP 9.10.1 的最新修補版本也支援 AFF C 系列平台。 視覺化功能可識別平台的問題或疑慮、為使用者提供快速的硬體問題疑難排解方法。

ONTAP 9.12.1 的新功能

瞭解 ONTAP 9.12.1 提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
使用 SnapMirror Synchronous 支援較大的 FlexVol 磁碟區	SnapMirror 同步組態支援的 FlexVol 磁碟區大小上限、已從 100 TB 增加至 300 TB 。來源叢集和目的地叢集都必須執行 ONTAP 9.12.1P2 或更新版本 _ 。
SnapMirror Synchronous 支援較大的檔案和 LUN 大小	SnapMirror 同步組態支援的檔案和 LUN 大小上限、已從 16 TB 增加至 128 TB 。來源叢集和目的地叢集都必須執行 ONTAP 9.12.1 P2 或更新版本。
增強一致性群組的支援	• 您可以從一致性群組新增和移除磁碟區，複製一致性群組（包括從快照中）。 • 一致性群組支援應用程式標記、可簡化資料保護與管理程序。 • ONTAP REST API 支援使用 NFS/SMB 磁碟區或 NVMe 命名空間來設定一致性群組。
SnapMirror 同步 n	SnapMirror Synchronous 支援 HA 接管與恢復、 Volume 搬移及其他維護相關作業的不中斷作業（ n ）。此功能僅適用於 AFF/ASA 平台。
ONTAP Mediator 1.5 支援 SnapMirror 業務持續運作	ONTAP Mediator 1.5 可用於監控 SnapMirror 主動同步關係。
SnapMirror 主動同步持續性增強功能	SnapMirror 主動式同步支援從快照進行部分 LUN 還原。此外、 SnapMirror 主動式同步可將 QoS 延伸至非 SnapMirror 關係中的磁碟區。
SnapMirror 非同步的資料倉儲重建指標	SnapMirror 非同步提供指標、顯示資料倉儲在災難恢復排練後所需的重建時間、並顯示完成百分比。
SnapLock 選項可設定「未指定」絕對保留時間的最短保留時間	SnapLock 包含一個選項、可在絕對保留時間設定為「未指定」時、設定最短保留時間。
防竄改快照	您可以鎖定非 SnapLock 磁碟區上的快照，以防止勒索軟體攻擊。鎖定快照有助於確保不會意外或惡意刪除快照。

檔案存取通訊協定

更新	說明
使用 AES 加密配置基於 Kerberos 的通訊的安全性	新的 SMB 安全選項可讓您停用 RC4 和 DES 、而非進階加密標準（ AES ）加密類型、以便與 Active Directory （ AD ） KDC 進行 Kerberos 型通訊。
S3 用戶端存取 NAS 資料	S3 用戶端可以存取與 NFS 和 SMB 用戶端相同的 NAS 資料、而無需重新格式化、因此更容易為需要物件資料的 S3 應用程式提供服務。
NFS擴充屬性	啟用 NFSv4.2 的 NFS 伺服器可從支援 xattr 的用戶端儲存及擷取 NFS 擴充屬性（ xattrs ）。
NFSv4.2 稀疏檔案和空間保留支援	NFSv4.2 用戶端可為稀疏檔案保留空間。空間也可以從檔案取消分配和取消保留。

網路

更新	說明
LIF 服務	您可以使用 `management-log-forwarding` 用於控制將稽核記錄轉送到遠端 Syslog 服務的生命期的服務

S3 物件儲存

更新	說明
擴大支援 S3 行動	支援下列 Amazon S3 API 動作： • `CopyObject` • `UploadPartCopy` • `BucketPolicy` （取得、放置、刪除）

SAN

更新	說明
增加 AFF 和 FAS 平台的最大 LUN 大小	從 ONTAP 9.12.1P2 開始、 AFF 和 FAS 平台上支援的最大 LUN 大小從 16 TB 增加至 128 TB 。
"增加 NVMe 限制"	NVMe 傳輸協定支援下列項目： • 單一儲存 VM 和單一叢集中有 8K 個子系統 • 12 個節點叢集 NVMe / FC 支援每個連接埠 256 個控制器、而 NVMe / TCP 則支援每個節點 2K 控制器。
NVMe / TCP 支援安全驗證	NVMe 主機和控制器之間的安全、單向和雙向驗證、可透過使用 DHHMAC-CHAP 驗證傳輸協定的 NVMe / TCP 來支援。
MetroCluster IP 支援 NVMe	4 節點 MetroCluster IP 組態支援 NVMe / FC 傳輸協定。

安全性

在 2022 年 10 月、 NetApp 實施變更、以拒絕使用 Sv1.2 或安全 SMTP 的 HTTPS 所傳送的 AutoSupport 訊息傳輸。如需詳細資訊、請參閱 "SU484 ： NetApp 會拒絕傳輸安全性不足的 AutoSupport 訊息"。

功能	說明
自主勒索軟體保護互通性增強功能	以下組態提供自主勒索軟體保護： • 受SnapMirror保護的磁碟區 • SnapMirror保護SVM • 已啟用移轉的SVM（SVM資料移動性）

功能	說明
支援使用 FIDO2 和 PIV 的 SSH （兩者均由 Yibkeyy 使用）的多因素驗證（ MFA ）	SSH MFA 可以使用硬體輔助的公開 / 私密金鑰交換與使用者名稱和密碼。Yubibkey 是插入 SSH 用戶端的實體權杖裝置、可提高 MFA 的安全性。
防竄改記錄	根據預設、所有 ONTAP 內部記錄都是防竄改的、可確保遭入侵的系統管理員帳戶不會隱藏惡意動作。
事件的 TLS 傳輸	EMS 事件可以使用 TLS 通訊協定傳送至遠端 Syslog 伺服器、藉此加強有線保護、以進行中央外部稽核記錄。

儲存效率

更新	說明
對溫度敏感的儲存效率	在新的 AFF C250 、 AFF C400 、 AFF C800 平台和磁碟區上、預設會啟用對溫度敏感的儲存效率。在現有磁碟區上、 TSSE 預設不會啟用、但可以使用 ONTAP CLI 手動啟用。
增加可用的 Aggregate 空間	對於 All Flash FAS （ AFF ）和 FAS500f 平台、大於 30TB 的 WAFL 保留區會從 10% 降至 5% 、進而增加集合體的可用空間。
檔案系統分析：依大小而定的主要目錄	檔案系統分析現在可識別佔用空間最大的磁碟區目錄。

儲存資源管理增強功能

更新	說明
重新平衡FlexGroup	您可以啟用自動不中斷營運的 FlexGroup Volume 重新平衡功能、以便在 FlexGroup 元件之間重新分配檔案。 建議您不要在 FlexVol 轉 FlexGroup 之後使用自動 FlexGroup 重新平衡。您可以輸入命令，改用 ONTAP 9.10.1 及更新版本提供的具破壞性回溯性檔案移動功能 `volume rebalance file-move`。有關詳細資訊和命令語法，請參閱"《指令參考》ONTAP" 。
SnapLock for SnapVault 支援 FlexGroup Volume	SnapLock for SnapVault 支援 FlexGroup Volume

SVM 管理增強功能

更新	說明
SVM 資料移動性增強功能	叢集管理員可以使用 FAS 、 AFF 平台、在混合式集合體上、不中斷地將 SVM 從來源叢集重新定位到目的地叢集。 新增了對破壞性 SMB 傳輸協定和自主勒索軟體保護的支援。

系統管理員

從ONTAP 9.12.1 開始，系統管理器與NetApp控制台整合。透過控制台，管理員可以從單一控制平面管理混合多雲基礎設施，同時保留熟悉的系統管理器儀表板。登入系統管理員時，管理員可以選擇存取NetApp控制台中的系統管理器介面或直接存取系統管理員。詳細了解System Manager 與NetApp Console 集成 。

更新	說明
SnapLock 的系統管理員支援	系統管理員支援 SnapLock 作業、包括法規遵循時鐘初始化、 SnapLock Volume 建立及 WORM 檔案鏡射。
纜線的硬體視覺化	System Manager 使用者可以檢視叢集中硬體裝置之間纜線的連線資訊、以疑難排解連線問題。
登入 System Manager 時支援 Cisco 雙核心的多重驗證	您可以將 Cisco DuoTM 設定為 SAML 身分識別供應商（ IDP ）、讓使用者在登入 System Manager 時能夠使用 Cisco DuoTM 進行驗證。
System Manager網路增強功能	在建立網路介面期間、System Manager可更有效地控制子網路和主連接埠的選擇。System Manager 也支援透過 RDMA 連線設定 NFS 。
系統顯示佈景主題	System Manager 使用者可以選取明亮或暗色主題來顯示 System Manager 介面。他們也可以選擇預設為其作業系統或瀏覽器所使用的主題。此功能可讓使用者指定更適合讀取顯示器的設定。
改善本機層容量的詳細資料	System Manager 使用者可以檢視特定本機層的容量詳細資料、以判斷空間是否過度使用、這可能表示他們需要新增更多容量、以確保本機層不會用盡空間。
改善搜尋功能	System Manager 具備改良的搜尋功能、可讓使用者透過系統管理員介面、直接從 NetApp 支援網站 搜尋及存取相關且內容相關的支援資訊和系統管理員產品文件。這可讓使用者取得所需的資訊、無需在支援網站的不同位置進行搜尋、即可採取適當的行動。
Volume 資源配置的改善	儲存管理員可以在使用 System Manager 建立磁碟區時選擇快照原則，而非使用預設原則。
增加磁碟區的大小	儲存管理員可以在使用 System Manager 調整磁碟區大小時，檢視對資料空間和快照保留的影響。
儲存資源池 和 Flash Pool 管理	儲存管理員可以使用 System Manager 將 SSD 新增至 SSD 儲存池、使用 SSD 儲存池分配單元建立 Flash Pool 本機層（ Aggregate ）、以及使用實體 SSD 建立 Flash Pool 本機層。
System Manager 中的 NFS over RDMA 支援	System Manager 支援 NFS over RDMA 的網路介面組態、並識別具備 ROCE 功能的連接埠。

ONTAP 9.11.1 的新功能

瞭解 ONTAP 9.11.1 的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
叢集外部金鑰伺服器	為提供叢集式 KMIP 伺服器解決方案的 NetApp 合作夥伴新增叢集式外部金鑰管理伺服器支援。如此可新增主要和次要 KMIP 伺服器、避免加密金鑰資料重複。如需支援的合作夥伴、請參閱 "互通性對照表工具"。
System Manager 中的 SnapMirror 非同步原則	您可以使用 System Manager 來新增預先建立和自訂的鏡射和資料保險箱原則、顯示舊版原則、以及在保護磁碟區和儲存 VM 時、覆寫保護原則中定義的傳輸排程。您也可以使用 System Manager 來編輯 Volume 和儲存 VM 的保護關係。 如果您執行的是 ONTAP 9.8P12 或更新版本的 ONTAP 9.8 修補程式、已使用系統管理員設定 SnapMirror 、並計畫升級至 ONTAP 9.9.1 或 ONTAP 9.10.1 版本、請使用 ONTAP 9.9.9.1P13 或更新版本、以及 ONTAP 9.10.1P10 或更新版本的修補程式來進行升級。
SnapMirror Cloud 單一目錄還原	可讓叢集在管理權限層級進行管理、從雲端端點執行單一目錄還原作業。必須提供來源端點 UUID 、以識別您要從中還原的備份端點。因為多個備份可以使用相同的備份 `cloud_endpoint_name` 作為目的地、還原命令必須提供與備份相關的 UUID 。您可以使用 `snapmirror show` 取得的命令 `source_endpoint_uuid`。
增強了對 SnapMirror 主動同步的支持	• SnapMirror 主動同步支援 AIX 做為主機 • SnapMirror 主動式同步支援單一檔案 SnapRestore 、可讓您在 SnapMirror 主動式同步組態中還原個別 LUN 或一般檔案。
SVM 資料複寫快速重新同步	SVM 資料複寫快速重新同步功能可讓儲存管理員略過完整的資料倉儲重建作業、並從災難恢復排練中更快速地恢復。
支援 MetroCluster 的 SVM 資料複寫	MetroCluster 組態的兩端都支援 SVM-DR 來源。
建立兩階段一致性群組快照	在 REST API 中，一致性群組支援兩階段的快照程序，可讓您在提交快照之前進行預先檢查。

檔案存取通訊協定

更新	說明
支援 TLSv1.3	ONTAP 支援 TLS 1.3 for HTTPS 和 REST API 管理通訊協定。SP/BMC 或叢集對等加密不支援 TLS 1.3 。
LDAP 快速連結支援	如果 LDAP 伺服器支援、您可以使用 LDAP 快速繫結、快速簡單地驗證 ONTAP 管理員使用者。

網路

更新	說明
連結層探索傳輸協定（LLDP）	叢集網路支援LLDP、可讓ONTAP 支援不支援Cisco探索傳輸協定（CDP）的叢集交換器搭配使用。
LIF 服務	新的用戶端LIF服務可提供更多控制權、以控制哪些LIF用於傳出AD、DNS、LDAP及NIS要求。

S3 物件儲存

更新	說明
對 S3 物件動作的額外支援	ONTAP API 支援下列動作： `CreateBucket`、 `DeleteBucket`、 `DeleteObjects`。此外、 ONTAP S3 也支援物件版本設定、以及與相關的動作 `PutBucketVersioning`、 `GetBucketVersioning`、 `ListBucketVersions`。

SAN

更新	說明
iSCSI LIF 容錯移轉	新的iSCSI LIF容錯移轉功能可在SFO合作夥伴容錯移轉和本機容錯移轉中、支援iSCSI LIF的自動和手動移轉。iSCSI LIF 容錯移轉功能可在所有 SAN 陣列（ASA）平台上使用。
從 LUN 到 NVMe 命名空間、從 NVMe 命名空間到 LUN 的非破壞性移轉	使用 ONTAP CLI 就地轉換 現有 LUN 至 NVMe 命名空間 或是 現有 NVMe 命名空間至 LUN。

安全性

更新	說明
自主勒索軟體保護（ARP）增強功能	ARP 偵測演算法已增強、可偵測其他惡意軟體威脅。此外、新的授權金鑰也用於啟動自動勒索軟體保護。對於從 ONTAP 9.10.1 升級的 ONTAP 系統、先前的授權金鑰仍提供相同的功能。
多管理員驗證	啟用多重管理驗證時，某些作業（例如刪除磁碟區或快照）只能在獲得指定管理員的核准後執行。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。

儲存效率

更新	說明
檢視實體佔用空間的節約效益	當您在磁碟區上啟用對溫度敏感的儲存效率時、您可以使用 volume show-f佔地面積命令來顯示實體佔用空間的節約效益。
SnapLock 支援 FlexGroup Volume	SnapLock 支援儲存在 FlexGroup 磁碟區上的資料。FlexGroup Volume 支援適用於 SnapLock Compliance 和 SnapLock Enterprise 模式。

更新	說明
SVM資料移動性	將支援的 AFF 陣列數量增加到三個、並在來源和目的地同時執行 ONTAP 9.11.1 或更新版本時、新增對 SnapMirror 關係的支援。此外也推出外部金鑰管理（ KMIP ）、可用於雲端和內部部署安裝。

儲存資源管理增強功能

更新	說明
檔案系統分析中 SVM 層級的活動追蹤	活動追蹤會在 SVM 層級進行彙總、追蹤讀寫 IOPS 和流量、提供即時且可據以行動的資料洞見。
啟用檔案存取時間更新	啟用時、只有在目前存取時間的存留時間超過使用者指定的持續時間時、FlexCache 原始磁碟區的存取時間才會更新。
非同步目錄刪除	當儲存管理員授予 NFS 和 SMB 用戶端在磁碟區上的權限時、就可以使用非同步刪除功能。啟用非同步刪除時、 Linux 用戶端可以使用 mv 命令、Windows 用戶端可以使用 rename 命令來刪除目錄並將其移至隱藏位置 `.ontaptrashbin` 目錄。
SnapLock 支援 FlexGroup Volume	SnapLock 支援儲存在 FlexGroup 磁碟區上的資料。FlexGroup Volume 支援適用於 SnapLock Compliance 和 SnapLock Enterprise 模式。SnapLock 不支援在 FlexGroup 磁碟區上執行下列作業： SnapLock for SnapVault 、事件型保留和法定保留。

SVM 管理增強功能

更新	說明
SVM資料移動性	將支援的 AFF 陣列數量增加到三個、並在來源和目的地同時執行 ONTAP 9.11.1 或更新版本時、新增對 SnapMirror 關係的支援。此外、我們也推出外部金鑰管理（ KMIP ）、可用於雲端和內部部署安裝。

系統管理員

更新	說明
管理 SnapMirror 非同步原則	使用 System Manager 新增預先建立的自訂鏡射和資料保險箱原則、顯示舊版原則、以及在保護磁碟區和儲存 VM 時、覆寫保護原則中定義的傳輸排程。您也可以使用 System Manager 來編輯 Volume 和儲存 VM 的保護關係。 如果您使用的是 ONTAP 9.8P12 或更新版本的 ONTAP 9.8 修補程式版本、而且您使用系統管理員設定了 SnapMirror 、而且您打算升級至 ONTAP 9.9.1 或 ONTAP 9.10.1 版本、則應該使用 ONTAP 9.9.9.1P13 或更新版本、以及 ONTAP 9.10.1P10 或更新版本的修補程式來進行升級。
硬體視覺化	System Manager 中的硬體視覺化功能支援所有目前的 AFF 和 FAS 平台。
系統分析洞見	System Manager 會在 Insights 頁面上顯示額外的容量和安全洞見、以及叢集和儲存 VM 組態的新見解、協助您最佳化系統。

更新	說明
使用性增強功能	• 根據預設、新建立的磁碟區無法共用： 您可以指定預設存取權限、例如透過 NFS 匯出或透過 SMB/CIFS 共用、以及指定權限等級。 • SAN 簡化： 新增或編輯啟動器群組時、 System Manager 使用者可以檢視群組中啟動器的連線狀態、並確保群組中包含已連線的啟動器、以便存取 LUN 資料。
進階本機層（ Aggregate ）作業	如果系統管理員管理員不想接受系統管理員的建議，他們可以指定本機層的配置。此外，管理員還可以編輯現有本機層的 RAID 配置。 如果您使用的是 ONTAP 9.8P12 或更新版本的 ONTAP 9.8 修補程式版本、而且您使用系統管理員設定了 SnapMirror 、而且您打算升級至 ONTAP 9.9.1 或 ONTAP 9.10.1 版本、則應該使用 ONTAP 9.9.9.1P13 或更新版本、以及 ONTAP 9.10.1P10 或更新版本的修補程式來進行升級。
管理稽核記錄	您可以使用系統管理員來檢視和管理 ONTAP 稽核記錄。

相關資訊

- "SnapMirror 顯示"

ONTAP 9.10.1 的新功能

瞭解 ONTAP 9.10.1 中提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
將 SnapLock 保留期間設為 100 年	在早於 ONTAP 9.10.1 的版本中、支援的保留時間上限為 2071 年 1 月 19 日。從 ONTAP 9.10.1 SnapLock 企業與法規遵循開始、可支援截至 10 月 26 日、 3058 日的保留時間、以及最長 100 年的保留期間。當您延長保留日期時、會自動轉換較舊的原則。
能夠在同一個 Aggregate 上建立 SnapLock 和非 SnapLock Volume	從 ONTAP 9.10.1 開始、 SnapLock 和非 SnapLock 磁碟區可以存在於同一個 Aggregate 上、因此不再需要為 SnapLock 磁碟區建立個別的 SnapLock Aggregate 。

更新	說明
一致性群組	在一致性群組中組織磁碟區和 LUN 、以管理資料保護原則、並確保跨越多個儲存磁碟區的工作負載具有寫入順序的保真度。
使用公有雲進行歸檔備份	SnapMirror Cloud 支援 ONTAP 備份分層、可在 AWS 和 MS Azure 中降低公有雲物件儲存類別的成本、以便長期保留資料。
AES 支援安全的 Netlogon 通道通訊	如果您使用 Netlogon 驗證服務連線至 Windows 網域控制站、則可以使用進階加密標準（ AES ）進行安全通道通訊。
用於 SMB 網域通道驗證的 Kerberos	Kerberos 驗證可用於 ONTAP 管理的網域通道驗證、以及 NTLM 。如此一來、就能使用 Active Directory 認證、更安全地登入 ONTAP CLI 和系統管理員 GUI 。
通道繫結可提升 LDAP 通訊安全性	Active Directory 和名稱服務 LDAP 連線預設都支援 LDAP 通道繫結。這可提供更好的保護、防範攔截式攻擊。

檔案存取通訊協定

更新	說明
NFS over RDMA （僅 NVIDIA ）	NFS over RDMA採用RDMA介面卡、可在儲存系統記憶體與主機系統記憶體之間直接複製資料、避免CPU中斷與負荷。NFS over RDMA 可在支援 NVIDIA GPU 的主機上、使用 NVIDIA GPUDirect Storage 來處理 GPU 加速工作負載。

網路

更新	說明
RDMA叢集互連	有了 A400 或 ASA A400 儲存系統和 X1151A 叢集 NIC 、您就可以利用 RDMA 來加速多節點叢集內流量的高效能工作負載
在系統 SVM 中將 LIF 的狀態設定為「系統管理員」之前、必須先確認	如此可防止您意外中斷重要的生命、以確保叢集正常運作。如果您的指令碼在 CLI 中叫用此行為、則必須將其更新為帳戶、以進行確認步驟。
自動偵測及修復網路線路問題建議	當偵測到連接埠可連線性問題時、 ONTAP 系統管理員建議進行修復作業來解決問題。
網際網路傳輸協定安全性（ IPsec ）憑證	除了驗證憑證之外、 IPsec 原則還支援預先共用金鑰（ SDK ）。
LIF服務原則	防火牆原則已過時、並取代為 LIF 服務原則。此外、我們也新增了 NTP LIF 服務原則、以提供更多控制、讓您可以使用哪些生命來處理傳出的 NTP 要求。

S3 物件儲存

更新	說明
S3 物件資料保護、備份與災難恢復	SnapMirror S3 為 ONTAP S3 物件儲存提供資料保護服務，包括鏡射至 ONTAP S3 組態的儲存區，以及儲存區備份至 NetApp 和非 NetApp 目的地。

更新	說明
S3稽核	您可以稽核 ONTAP S3 環境中的資料和管理事件。S3稽核功能類似於現有的NAS稽核功能、S3和NAS稽核可共存於叢集內。

SAN

更新	說明
NVMe命名空間	您可以使用 ONTAP CLI 來增加或減少命名空間的大小。您可以使用 System Manager 來增加命名空間的大小。
TCP 的 NVMe 傳輸協定支援	非揮發性記憶體高速（ NVMe ）傳輸協定適用於透過 TCP 網路的 SAN 環境。

安全性

更新	說明
自主勒索軟體保護	在 NAS 環境中使用工作負載分析功能、「自主勒索軟體保護」會針對可能表示勒索軟體攻擊的異常活動發出警示。自動勒索軟體保護功能也會在偵測到攻擊時，建立自動快照備份，此外還會保護現有的定期快照保護功能。
加密金鑰管理	使用 Azure Key Vault 和 Google Cloud Platform Key Management Service 來儲存、保護和使用 ONTAP 金鑰、簡化金鑰管理和存取。

儲存效率

更新	說明
對溫度敏感的儲存效率	您可以在新的或現有的 AFF 磁碟區上、使用「預設」模式或「有效率」模式來啟用對溫度敏感的儲存效率。
能夠在叢集之間不中斷地移動 SVM	您可以在實體 AFF 叢集之間重新部署 SVM 、從來源移轉到目的地、以進行負載平衡、效能改善、設備升級和資料中心移轉。

儲存資源管理增強功能

更新	說明
使用檔案系統分析（ FSA ）追蹤 Hot 物件的活動	為了改善系統效能評估、 FSA 可以識別最大流量和處理量的 Hot 物件：檔案、目錄、使用者和用戶端。
全域檔案讀取鎖定	在所有快取和原始伺服器上的單一點啟用讀取鎖定；移轉中受影響的文章。
支援 FlexCache 的 NFSv4	FlexCache Volume 支援 NFSv4 傳輸協定。
從現有的 FlexGroup 磁碟區建立複本	您可以使用現有的 FlexGroup Volume 建立 FlexClone Volume 。
將 FlexVol Volume 轉換為 SVM 災難恢復來源中的 FlexGroup	您可以在 SVM 災難恢復來源中、將 FlexVol Volume 轉換為 FlexGroup Volume 。

SVM 管理增強功能

更新	說明
能夠在叢集之間不中斷地移動 SVM	您可以在實體 AFF 叢集之間重新部署 SVM 、從來源移轉到目的地、以進行負載平衡、效能改善、設備升級和資料中心移轉。

系統管理員

更新	說明
在 System Manager 記錄中啟用效能遙測記錄	如果系統管理員發生效能問題、系統管理員可以啟用遙測記錄、然後聯絡支援部門以分析問題。
NetApp 授權檔案	所有授權金鑰都會以 NetApp 授權檔案的形式提供、而非個別 28 個字元的授權金鑰、因此可以使用單一檔案來授權多項功能。
自動更新韌體	系統管理員可將 ONTAP 設定為自動更新韌體。
檢閱風險緩解建議、並瞭解 Digital Advisor 回報的風險	System Manager 使用者可以檢視 Digital Advisor 所報告的風險、並檢閱降低風險的建議。從 9.10.1 開始、使用者也能瞭解風險。
設定系統管理員接收 EMS 事件通知	System Manager 管理員可以設定事件管理系統（ EMS ）事件通知的傳送方式、以便在系統問題需要注意時通知他們。
管理憑證	系統管理員可以管理信任的憑證授權單位、用戶端 / 伺服器憑證、以及本機（內建）憑證授權單位。
使用 System Manager 檢視容量的歷史使用情況、並預測未來的容量需求	數位顧問與系統管理員之間的整合可讓系統管理員檢視叢集容量使用歷史趨勢的相關資料。
使用系統管理員、使用 Cloud Backup Service 將資料備份至 StorageGRID	身為 Cloud Backup Service 管理員、如果您在內部部署了 Cloud Manager 、則可以備份到 StorageGRID 。您也可以使用 Cloud Backup Service 搭配 AWS 或 Azure 來歸檔物件。

更新	說明
使用性增強功能	從 ONTAP 9.10.1 開始、您可以： • 將 QoS 原則指派給 LUN 、而非父磁碟區（ VMware 、 Linux 、 Windows ） • 編輯LUN QoS原則群組 • 移動LUN • 使LUN離線 • 執行滾動 ONTAP 映像升級 • 建立連接埠集、並將其繫結至 igroup • 自動偵測及修復網路線路問題建議 • 啟用或停用用戶端對 Snapshot 目錄的存取 • 刪除快照之前，請先計算可回收空間 • 存取 SMB 共用區中持續可用的欄位變更 • 使用更精確的顯示單位來檢視容量測量 • 管理 Windows 和 Linux 的主機專屬使用者和群組 • 管理 AutoSupport 設定 • 將磁碟區調整為獨立的動作

ONTAP 9.9.1 的新功能

瞭解 ONTAP 9.9.1 提供的新功能。

如需最新 ONTAP 9 版本中已知問題、限制和升級注意事項的詳細資訊、請參閱 "發行說明ONTAP"。您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

- 瞭解全新與增強功能 "ONTAP MetroCluster 功能"。
- 了解 "對AFF、 ASA和FAS系統以及支援的交換器的全新和增強支持" 。
- 瞭解的更新 "靜態API ONTAP"。

若要升級至最新版的 ONTAP ，請參閱準備升級 ONTAP。

資料保護

更新	說明
"SnapLock 磁碟區和集合體上的儲存效率支援"	SnapLock 磁碟區和集合體的儲存效率功能已擴充、包括資料壓縮、跨磁碟區重複資料刪除、調適式壓縮和 TSSE （溫度敏感儲存效率）、可為 WORM 資料節省更多空間。
"支援在 SVM DR 來源和目的地上設定不同的快照原則"	SVM DR 組態可使用 mirror 保存原則在來源和目的地上設定不同的快照原則，而目的地上的原則不會被來源上的原則覆寫。

更新	說明
"System Manager 支援 SnapMirror Cloud"	SnapMirror Cloud 現在在 System Manager 中受到支援。
稽核啟用的 SVM	叢集中支援的啟用稽核的 SVM 數量上限已從 50 個增加到 400 個。
SnapMirror同步	每個 HA 配對支援的 SnapMirror 同步端點數量上限從 80 增加至 160 。
FlexGroup SnapMirror 拓撲	FlexGroup Volume 支援兩個以上的扇出關係、例如 A → B 、 A → C與 FlexVol Volume 類似、 FlexGroup 扇出功能最多可支援 8 個扇出式支腳、並可串聯至兩個層級、例如 A → B → C

檔案存取通訊協定

更新	說明
"LDAP 參照追蹤增強功能"	LDAP 參照追蹤支援 LDAP 簽署與密封、加密 TLS 連線、以及 LDAPS 連接埠 636 上的通訊。
"任何連接埠都支援 LDAPS"	LDAPS 可在任何連接埠上設定、連接埠 636 則維持預設值。
"預設會啟用 NFSv4.x 版本"	預設會啟用 NFSv4.0 、 NFSv4.1 和 NFSv4.2 。
"標示為 NFSv4.2 支援"	啟用 NFSv4.2 時、支援標有 NFS 的強制存取控制（ MAC ）。有了這項功能、 ONTAP NFS 伺服器就能感知 MAC 、儲存及擷取 `sec_label` 用戶端傳送的屬性。

網路

更新	說明
"叢集恢復能力"	• 雙節點無交換器叢集的連接埠監控與避免（先前僅適用於交換式組態） • 當節點無法在其叢集網路上提供資料時、自動節點容錯移轉 • 顯示哪些叢集路徑發生封包遺失的新工具
"虛擬 IP （ VIP ） LIF 擴充"	• 邊界閘道傳輸協定（ BGP ）的自治系統編號（ ASN ）支援 4 位元組的非負整數。 • 多出口鑑別器（ MED ）可提供進階路由選擇、並支援路徑優先順序。Med 是 BGP 更新訊息中的選用屬性。 • VIP BGP使用BGP對等群組來提供預設路由自動化、以簡化組態。

S3 物件儲存

更新	說明
"S3 中繼資料與標籤支援"	ONTAP S3 伺服器可為 S3 用戶端和應用程式提供增強的自動化功能、並支援使用者定義的物件中繼資料和物件標記。

SAN

更新	說明
外部 LUN 匯入（ FLI ）	NetApp 支援網站 上的 SAN LUN 移轉應用程式可用於驗證 FLI 互通性對照表中未列出的外部陣列。
NVMe 遠端路徑存取	如果在容錯移轉中遺失直接路徑存取、遠端 I/O 可讓系統容錯移轉至遠端路徑並繼續資料存取。
支援 ASA 上的 12 節點叢集	AFF ASA 組態支援 12 節點叢集。ASA 叢集可以混合使用各種 ASA 系統類型。
ASA 上的 NVMe 協定	AFF ASA 系統也支援 NVMe 型傳輸協定。
igroup 的增強功能	• 您可以建立包含現有 igroup 的 igroup。 • 您可以將描述新增至做為 igroup 或主機啟動器別名的 igroup 或主機啟動器。 • 您可以同時將 igroup 對應至兩個或多個 LUN 。
單一 LUN 效能改善	AFF 的單一 LUN 效能大幅提升、是簡化虛擬環境部署的理想選擇。例如、A800 可提供高達 400% 的隨機讀取 IOP 。

安全性

更新	說明
登入 System Manager 時支援 Cisco 雙核心的多重驗證	從 ONTAP 9.9.1P3 開始、您可以將 Cisco 雙核心設定為 SAML 身分識別供應商（ IDP ）、讓使用者在登入系統管理員時能夠使用 Cisco 雙核心驗證。

儲存效率

更新	說明
"將磁碟區的檔案數量設為最大值"	使用 Volume 參數將檔案最大值自動化 `-files-set-maximum`，無需監控檔案限制。

儲存資源管理增強功能

更新	說明
System Manager 中的檔案系統分析（ FSA ）管理增強功能	FSA 提供額外的系統管理員功能、可用於搜尋和篩選、以及針對 FSA 建議採取行動。
支援負向查詢快取	在 FlexCache 磁碟區上快取「找不到檔案」錯誤、以減少因向來源伺服器呼叫而造成的網路流量。
FlexCache 災難恢復	提供用戶端從一個快取到另一個快取的不中斷移轉。
SnapMirror 串聯及展開支援 FlexGroup Volume	支援 FlexGroup 磁碟區的 SnapMirror 串聯和 SnapMirror 扇出關係。
FlexGroup Volume 的 SVM 災難恢復支援	SVM 對 FlexGroup 磁碟區的災難恢復支援使用 SnapMirror 來複寫和同步 SVM 的組態和資料、藉此提供備援功能。

更新	說明
FlexGroup Volume 的邏輯空間報告與強制支援	您可以顯示及限制 FlexGroup Volume 使用者所使用的邏輯空間量。
qtree 中的 SMB 存取支援	支援 SMB 存取 FlexVol 和啟用 SMB 的 FlexGroup 磁碟區中的 qtree 。

系統管理員

更新	說明
System Manager 會顯示 Digital Advisor 回報的風險	使用系統管理員連結至 Active IQ 數位顧問（也稱為數位顧問）、報告降低風險並改善儲存環境效能與效率的機會。
手動指派本機層	System Manager 使用者在建立和新增磁碟區和 LUN 時、可以手動指派本機層。
非同步目錄刪除	可以在 System Manager 中刪除具有低延遲非同步目錄刪除功能的目錄。
產生 Ansible 教戰手冊	System Manager 使用者可以從 UI 產生一些特定工作流程的 Ansible Playbook 、並可在自動化工具中使用這些手冊來重複新增或編輯磁碟區或 LUN 。
硬體視覺化	ONTAP 9.8 首次推出硬體視覺化功能、現在支援所有 AFF 平台。
數位顧問整合	System Manager 使用者可以檢視與叢集相關的支援案例、然後下載。他們也可以複製叢集詳細資料、以便在 NetApp 支援網站 上提交新的支援案例。System Manager 使用者可從 Digital Advisor 收到警示、通知他們有新韌體更新可用。然後、他們可以下載韌體映像、並使用 System Manager 上傳。
Cloud Manager 整合	System Manager 使用者可以設定保護功能、使用 Cloud Backup Service 將資料備份至公有雲端點。
資料保護資源配置工作流程增強功能	System Manager 使用者可在設定資料保護時手動命名 SnapMirror 目的地和 igroup 名稱。
增強的網路連接埠管理	「網路介面」頁面具有增強的功能、可在其主連接埠上顯示及管理介面。
系統管理增強功能	• 支援巢狀 igroup • 在單一工作中將多個 LUN 對應到一個 igroup 、並在程序期間使用 WWPN 別名進行篩選。 • 在建立 NVMe of LIF 期間、您不再需要在兩個控制器上選取相同的連接埠。 • 使用切換按鈕停用每個連接埠的 FC 連接埠。
系統管理員中的快照相關資訊強化顯示	• System Manager 使用者可以檢視快照大小和 SnapMirror 標籤。 • 如果禁用了快照，則快照保留將設置爲零。

更新	說明
系統管理員中的增強顯示功能、可顯示儲存層的容量和位置資訊	• 新的 **Tiers** 欄會識別每個磁碟區所在的本機層（集合體）。 • System Manager 會顯示實體使用容量、以及叢集層級和本機層級（ Aggregate ）層級的邏輯使用容量。 • 新的容量顯示欄位可讓您監控容量、追蹤容量接近或使用率偏低的磁碟區。
在系統管理員中顯示 EMS 緊急警示及其他錯誤和警告	24 小時內收到的 EMS 警示數量、以及其他錯誤和警告、都會顯示在 System Manager 的 Health Card 中。

變更為 ONTAP 限制和預設值

瞭解 ONTAP 9 版本中實作的一些限制和預設值變更。NetApp 致力於協助客戶瞭解每個 ONTAP 版本中最重要的預設值、並限制變更。

變更為 ONTAP 預設值

在升級至新的 ONTAP 版本之前、您應該注意 ONTAP 預設設定的任何變更、這些變更可能會影響您的自動化或業務營運。

功能	預設變更	版本變更...
自主勒索軟體保護（Arp）	在支援的平台上，所有新磁碟區在 12 小時寬限期後預設自動啟用 ARP/AI。	ONTAP 9.18.1
音量預設值	在為 NAS 協定指派的ONTAP叢集上新建立的 SVM 上建立的磁碟區預設啟用檔案系統分析 (FSA)。	ONTAP 9.17.1
HTTP 嚴格傳輸安全性 (HSTS)	HSTS 在 9.17.1 中預設為啟用。	ONTAP 9.17.1
NAS 稽核	和參數的上限 `file-session-io-grouping-count`和 `file-session-io-grouping-duration`參數已增加，因此您可以選擇性地選擇較少，更合併的 NAS 稽核事件通知。這項優點是 SVM 具備高 IO 率，可減少對目的地 Volume 的儲存影 響。nfs_file_Session_io_grouping_count_MAX ： 20000 至 120000 nfs_file_Session_io_grouping_dimal_MAX ： 600 至 3600	ONTAP 9.16.1.
FAS 系統每個節點的最大磁碟區數	對於每個控制器具有大於 200GB RAM 的 FAS 系統，每個節點所支援的磁碟區數量上限從 1000 個增加到 2500 個。在舊版 ONTAP 中，"資料保護最佳化（DPO）"需要授權，才能將 ONTAP FAS 系統支援從每個節點 1000 個磁碟區增加到 2500 個磁碟區。	ONTAP 9.16.1.
負載共享鏡像	建立負載共享鏡像關係時，SVM 不能啟用儲存限制。	ONTAP 9.16.1.

功能	預設變更	版本變更...
`vserver object-store-server user show` 命令	在 ONTAP 9.15.1 之前的版本中 `vserver object-store-server user show` 命令會傳回 S3 使用者的秘密金鑰。此命令將不再傳回 S3 使用者的秘密金鑰資料。	ONTAP 9.15.1.1
NAS 稽核	NAS 稽核組態可依預設保留所有稽核記錄。旋轉限制參數的修訂值可確保稽核記錄的大小適合支援它的磁碟區。	ONTAP 9.15.1.1
空間分配	根據預設、新建立的 LUN 會啟用空間分配。在舊版 ONTAP （ 9.14.1 及更早版本）中、空間分配預設為停用。	ONTAP 9.15.1.1
NVMe / TCP 自動主機探索	根據預設、使用 NVMe / TCP 傳輸協定的控制器主機探索是自動化的。	ONTAP 9.14.1.
用於 Kerberos 型通訊的 AES 加密	預設會針對與 SMB 伺服器的 Kerberos 型通訊啟用驗證的 AES 加密。如果您的環境不支援 AES 加密、您可以手動停用 AES 加密。	ONTAP 9.13.1.12.9.11.9.11.
RAID Aggregate	從 ONTAP 9.12.1 開始、如果任何 Aggregate 降級、系統控制器預設不會在 24 小時後關機。如果使用者變更 `raid.timeout` 選項、系統控制器將在到期後繼續關機 `raid.timeout` 小時。	ONTAP 9.12.1
TLS 1.1 預設為停用	ONTAP 的新安裝預設會停用 TLS 1.1 。升級至 ONTAP 9.12.0 及更新版本且已啟用 TLS 1.1 的系統不會受到影響、因為升級會將 TLS 1.1 保持在啟用狀態。不過、如果您要升級啟用 FIPS 的叢集、則從 ONTAP 9.11.1 開始、 FIPS 不支援 TLS 1.1 、因此 TLS 1.1 將會自動停用。依預設停用時、可視需要手動啟用 TLS 1.1 。	零件9.12.0 ONTAP
TLS 1.0 預設為停用	ONTAP 的新安裝預設會停用 TLS 1.0 。升級至 ONTAP 9.8 及更新版本、且已啟用 TLS 1.0 的系統不受影響、因為升級將使 TLS 1.0 保持啟用狀態。不過、如果您要升級已啟用 FIPS 的叢集、則 FIPS 1.0 不支援從 ONTAP 9.8 開始的 TLS 1.0 、因此 TLS 1.0 會自動停用。依預設停用時、可視需要手動啟用 TLS 1.0 。	部分9.8 ONTAP

ONTAP 限制變更

在升級至新的 ONTAP 版本之前、您應該注意 ONTAP 限制的任何變更、這些變更可能會影響您的自動化或業務營運。

功能	限制變更	版本變更...
qtree 延伸效能監控	您可以在單一 ONTAP 叢集中啟用最多 50,000 個 qtree 的延伸效能監控。	ONTAP 9.16.1.
SnapMirror 主動同步	SnapMirror Active Sync 支援一致性群組中的 80 個磁碟區	ONTAP 9.15.1.1
SnapMirror 非同步	使用 SnapMirror 非同步保護的一致性群組可在一致性群組中支援多達 80 個磁碟區。	ONTAP 9.15.1.1

功能	限制變更	版本變更...
檔案系統分析	為了減輕效能問題、 ONTAP 強制在啟用檔案系統分析時、必須釋放容量的 5-8% 。	ONTAP 9.15.1.1
SVM資料移動性	SVM 資料移動性支援的每個 SVM 磁碟區數量上限增加至 400 個、而支援的 HA 配對數則增加至 12 個。	ONTAP 9.14.1.
重新平衡FlexGroup	FlexGroup 重新平衡作業的可設定檔案大小下限從 4 KB 增加到 20 MB 。	• ONTAP 9.14.1. • ONTAP 9.13.1P1 • ONTAP 9.12.1P10
FlexVol 和 FlexGroup Volume 大小限制	AFF 和 FAS 平台上支援的 FlexVol 和 FlexGroup 磁碟區組成大小上限、從 100 TB 增加到 300 TB 。	ONTAP 9.12.1P2
LUN 大小限制	AFF 和 FAS 平台上支援的 LUN 大小上限從 16 TB 增加至 128 TB 。SnapMirror 組態中支援的 LUN 大小上限（同步與非同步）從 16 TB 增加至 128 TB 。	ONTAP 9.12.1P2
FlexVol Volume 大小限制	AFF 和 FAS 平台支援的最大磁碟區大小從 100 TB 增加至 300 TB 。SnapMirror 同步組態中支援的 FlexVol 磁碟區大小上限、從 100 TB 增加至 300 TB 。	ONTAP 9.12.1P2
檔案大小限制	AFF 和 FAS 平台上 NAS 檔案系統支援的檔案大小上限、從 16 TB 增加到 128 TB 。SnapMirror 同步組態中支援的檔案大小上限從 16 TB 增加至 128 TB 。	ONTAP 9.12.1P2
叢集磁碟區限制	提高控制器更充分利用 CPU 和記憶體的能力、並將叢集的最大磁碟區數從 15,000 增加至 30,000 。	ONTAP 9.12.1
FlexVol Volume 的 SVM-DR 關係	對於 FlexVol Volume 、 SVM-DR 關係的最大數量已從 64 個增加至 128 個（每個叢集 128 個 SVM ）。	零點9.11.1. ONTAP
SnapMirror 同步	每個 HA 配對允許的 SnapMirror 同步作業數量上限從 200 個增加到 400 個。	零點9.11.1. ONTAP
NAS FlexVol Volume	NAS FlexVol 磁碟區的叢集限制已從 12 、 000 個增加至 15 、 000 個。	零點9.10.1 ONTAP
SAN FlexVol 磁碟區	SAN FlexVol 磁碟區的叢集限制已從 12 、 000 個增加至 15 、 000 個。	零點9.10.1 ONTAP
FlexGroup Volume 的 SVM-DR	• FlexGroup 磁碟區最多支援 32 個 SVM-DR 關係。 • 單一 SVM 在 SVM-DR 關係中支援的最大磁碟區數量為 300 、其中包括 FlexVol 磁碟區和 FlexGroup 組成數量。 • FlexGroup 中的最大組成數不可超過 20 個。 • SVM-DR 磁碟區限制為每個節點 500 個、每個叢集 1000 個（包括 FlexVol 磁碟區和 FlexGroup 成分）。	零點9.10.1 ONTAP
稽核啟用的 SVM	叢集中支援的啟用稽核的 SVM 數量上限已從 50 個增加到 400 個。	部分9.9.1 ONTAP
SnapMirror 同步	每個 HA 配對支援的 SnapMirror 同步端點數量上限從 80 個增加至 160 個。	部分9.9.1 ONTAP

功能	限制變更	版本變更...
FlexGroup SnapMirror 拓撲	FlexGroup Volume 支援兩個或多個扇出關係、例如 A 至 B 、 A 至 C與 FlexVol Volume 類似、 FlexGroup 扇出功能最多可支援 8 個扇出式支腳、並可串聯至兩個層級、例如 A 至 B 至 C	部分9.9.1 ONTAP
SnapMirror 並行傳輸	非同步卷級並發傳輸的最大數量已從 100 增加到 200。高階系統上的SnapMirror雲端傳輸次數從 32 次增加到 100 次，低階系統上的SnapMirror傳輸次數從 6 次增加到 20 次。	部分9.8 ONTAP
FlexVol Volume 限制	FlexVol 磁碟區的空間已從 100 TB 增加至 300 TB 、適用於 ASA 平台。	部分9.8 ONTAP

ONTAP 9 版本支援

從 ONTAP 9.8 版本開始、 NetApp 每個日曆年度提供 ONTAP 版本兩次。雖然計畫可能會有所變更、但其目的是在每個日曆年度的第二季和第四季推出新的 ONTAP 版本。使用此資訊規劃升級的時間範圍、以充分利用最新的 ONTAP 版本。

版本	發行日期
9.18.1	2025年11月
9.17.1	2025年9月
9.16.1.	2025 年 1 月
9.15.1..	2024 年 7 月
9.14.1.	2024 年 1 月
9.13.1.12.9.12.9.	2023 年 6 月
9.12.1	2023 年 2 月
9.11.1.	2022 年 7 月
9.10.1	2022 年 1 月
9.9.1	2021 年 6 月

支援層級

特定 ONTAP 版本可用的支援層級會因軟體發行時間而異。

支援層級	完全支援			有限支援		自助服務支援		
年	1.	2.	3.	4.	5.	6.	7.	8.
存取線上文件	是的	是的	是的	是的	是的	是的	是的	是的
技術支援	是的	是的	是的	是的	是的			
根本原因分析	是的	是的	是的	是的	是的			
軟體下載	是的	是的	是的	是的	是的			
服務更新（修補程式版本 [P-版本] ）	是的	是的	是的					
有關弱點的警示	是的	是的	是的					

若要升級至最新版的 ONTAP 、請參閱 升級至最新版的 ONTAP 和 我應該何時升級 ONTAP ？

開始使用

瞭解 ONTAP

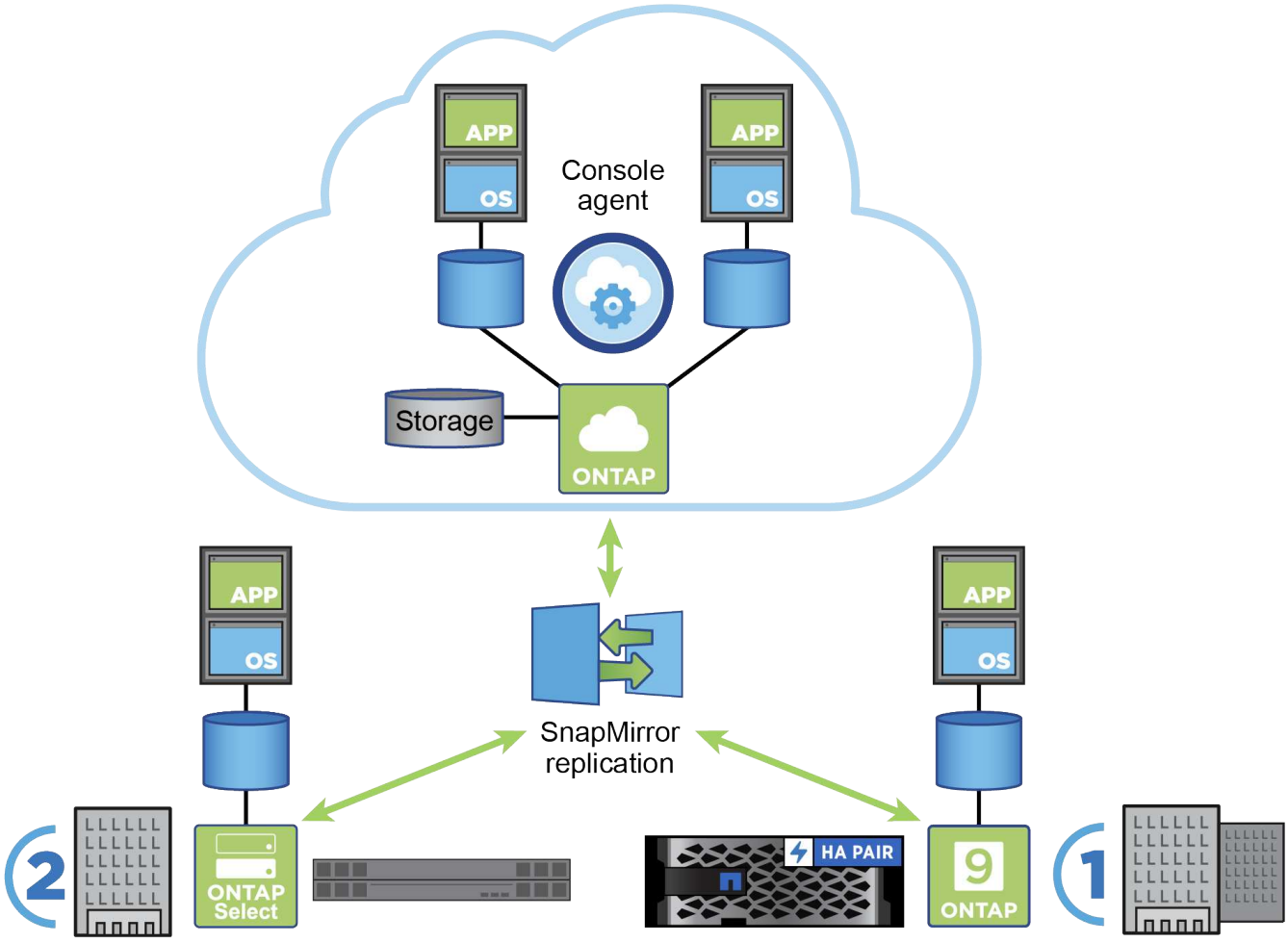
ONTAP 平台

ONTAP 資料管理軟體為讀寫區塊或檔案資料的應用程式提供統一化儲存設備。儲存組態中的選項包括高速 Flash 、價格較低的旋轉媒體、以及雲端型物件儲存。

ONTAP 實作可在下列環境中執行：

- * NetApp設計的系統*： "AFF、AFX、 ASA和FAS儲存系統"
- ONTAP儲存特性 "AFX 和ASA r2 儲存系統" 運行專用ONTAP特性，提供專注於特定協定的分解ONTAP儲存。
- * 商品硬體 * ： "ONTAP Select"
- 私有雲、公有雲或混合雲： "Cloud Volumes ONTAP" ， "Amazon FSX for NetApp ONTAP 產品" ， "Azure NetApp Files" ， 和 "Google Cloud NetApp Volumes"
- * 專業實作 * 、包括 "資料中心FlexPod"、提供同級最佳的融合式基礎架構

這些實作結合起來形成 _ 智慧型資料基礎架構 _ 的基本架構，並採用通用的軟體定義方法來管理資料，以及跨平台進行快速有效的複寫。



ONTAP 使用者介面

ONTAP 資料管理軟體提供多種介面、可用於管理 ONTAP 叢集。這些介面選項提供不同層級的存取和功能、並可根據您的環境、靈活地管理 ONTAP 叢集。

您可以使用任何這些介面來管理 ONTAP 叢集、並執行資料管理作業

系統管理程式ONTAP

ONTAP 系統管理員是一種網路型使用者介面、可提供簡化且直覺的方式來管理叢集。您可以管理一般作業、例如儲存組態、資料保護、網路設定與管理。System Manager 也提供風險與叢集效能監控與洞見、協助您因應叢集問題、並在問題發生前先行處理。 "深入瞭解"。

ONTAP 9.7 標誌著 ONTAP 系統管理員的重要關鍵時刻。在該版本中， NetApp 提供兩個版本的 ONTAP 系統管理員，推出重新設計，更精簡，更直覺化的版本，以及 ONTAP 9.7 之前的版本。在 ONTAP 9.7 之後，重新設計的版本將會延續為 ONTAP System Manager 及其前身，並重新命名為 System Manager Classic 。上次在 ONTAP 9.7 中更新 System Manager Classic 。如果您使用的是 System Manager Classic ，則可取得其說明文件 "另外"。

NetApp控制台

從ONTAP 9.12.1 開始，您可以使用NetApp Console 基於 Web 的介面從單一控制平面管理混合多雲基礎架構，

同時保留熟悉的系統管理器儀表板。透過控制台，您可以建立和管理雲端儲存（例如， NetApp備份和還原）、使用 NetApp 的資料服務（例如，雲端備份）以及控制許多內部部署和邊緣儲存設備。將本機ONTAP系統新增至控制台可讓您從單一介面管理所有儲存和資料資產。 "深入瞭解" 。

指令行介面**ONTAP**

。 "ONTAP 命令列介面（ CLI ）" 是一種文字型介面、可讓您使用與叢集、節點、 SVM 等進行互動 "命令" 。CLI 命令的可用依據為 "角色類型"。您可以透過 SSH 或主控台連線至叢集中的節點、來存取 ONTAP CLI 。

靜態**API ONTAP**

從 ONTAP 9.6 開始、您可以存取 RESTful API 、以程式設計方式管理及自動化叢集作業。使用 API 執行各種 ONTAP 管理工作，例如建立和管理磁碟區，快照和集合體，以及監控叢集效能。您可以使用 Curl 等公用程式或任何支援 REST 用戶端的程式設計語言（例如 Python ， PowerShell 和 Java ），直接存取 ONTAP REST API 。 "深入瞭解"。

ONTAPI 是ONTAP REST API 之前的專有ONTAP API。如果您正在使用 ONTAPI，則應規劃您的 "移轉至 ONTAP REST API" 。

NetApp 工具套件與架構

NetApp 針對特定開發語言和環境提供用戶端工具套件、可抽象化 ONTAP REST API 、並讓建立自動化程式碼變得更容易。
"深入瞭解"。

除了這些工具套件之外、您還可以使用架構來建立及部署自動化程式碼。 "深入瞭解"。

將**ONTAP**系統管理器與**NetApp**控制台集成

您可以使用NetApp控制台中的系統管理員管理ONTAP 9.10.1 及更高版本。透過這種集成，您可以使用統一的控制平面有效地監督混合多雲基礎設施，同時保留熟悉的系統管理器使用者介面。

透過控制台，您可以建立和管理雲端儲存（例如， Cloud Volumes ONTAP）、使用NetApp資料服務（例如，Cloud Backup）以及控制許多內部部署和邊緣儲存設備。

控制台提供了兩種發現和管理叢集的方法：

- 透過系統管理器直接發現並進行管理（ONTAP 9.12.1 及更高版本）
- 透過控制台代理發現。

控制台代理程式是安裝在您的環境中的軟體。這使您可以透過系統管理器存取管理功能，並存取提供資料複製、備份和復原、資料分類、資料分層等功能的NetApp雲端服務。

詳細了解"使用NetApp控制台進行本機ONTAP叢集管理" 。

步驟

1. 登入NetApp控制台。
    a. 如果您有控制台登錄，請使用它。

b. 如果這是您第一次，請選擇使用您的NetApp支援網站憑證登錄，然後在控制台登入頁面上輸入您的憑證。

2. 使用控制台代理程式或直接發現在控制台中發現您的本機叢集。了解更多有關連結的資訊：https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html [發現本地ONTAP集群^]。

   a. 了解如何"管理直接發現的集群" 。

   b. 了解如何"管理使用控制台代理發現的集群" 。

3. 使用系統管理員管理您的內部部署叢集。在我的工作環境系統頁面上，選擇集群，然後按一下服務清單中的系統管理員。

   a. 詳細了解"管理直接發現的集群" 。

   b. 了解如何"管理使用控制台代理發現的集群" 。

NetApp控制台和**ONTAP 9.12.1**

注意：如果您使用的是ONTAP 9.12.1，則會出現一則訊息提示您試用NetApp控制台。

+ 如果叢集已連線至NetApp控制台，則會顯示登入提示。

1. 按一下「繼續到NetApp控制台」** 以依照連結進入控制台。

   如果您的系統設定阻止了外部網絡，您將無法存取控制台。若要使用控制台存取系統管理員，您必須確保您的系統可以存取位址「cloudmanager.cloud.netapp.com」。否則，在提示字元下，您可以選擇使用隨ONTAP系統一起安裝的系統管理員版本。

2. 在控制台登入頁面上，選擇*使用您的NetApp支援網站憑證登入*並輸入您的憑證。

   如果您已經使用過控制台並使用電子郵件和密碼登錄，那麼您需要繼續使用該登入選項。

   "了解有關登入NetApp控制台的更多信息" 。

3. 如果出現提示，請輸入新的NetApp控制台帳號的名稱。

   大多數情況下，控制台會根據您的叢集資料自動為您建立帳戶。

4. 輸入叢集的叢集管理員認證。

結果

系統管理器顯示，您現在可以從控制台管理叢集。

了解有關**NetApp**控制台的更多信息

- "NetApp控制台概述"
- "透過NetApp控制台管理您的NetApp AFF和FAS系統"

叢集儲存設備

目前的功能性更新是ONTAP 專為NetApp橫向擴充_cluster儲存架構所開發。這是您在資料

中心實作ONTAP 過程中通常會發現的架構。因為這項實作運用了ONTAP的大部分功能、所以您可以從瞭解有關ONTAP 此技術的概念開始著手。

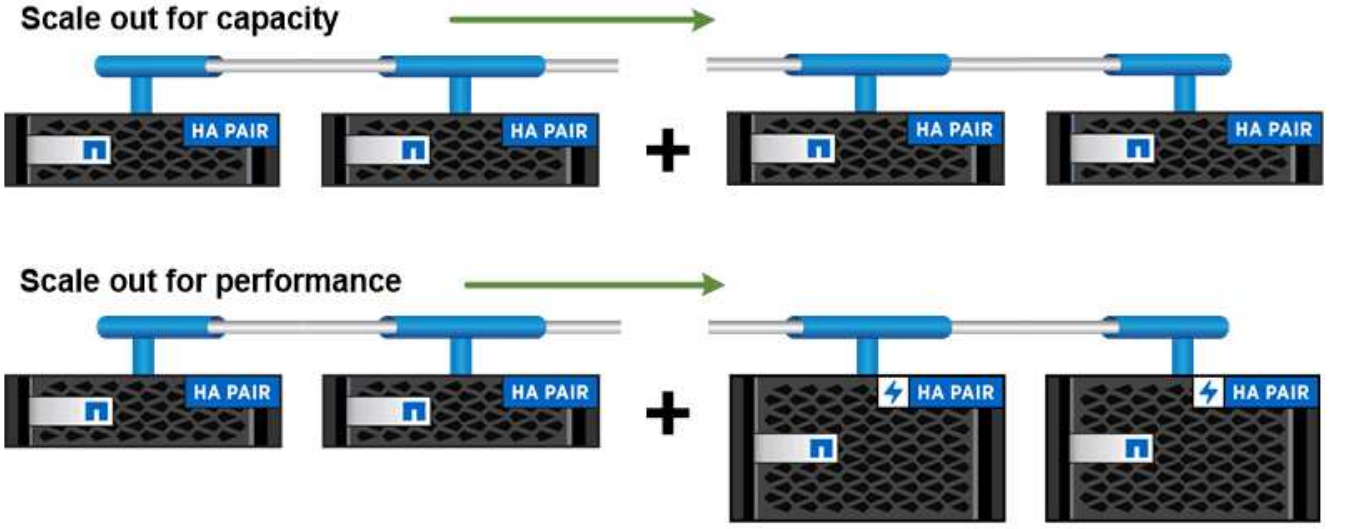
資料中心架構通常部署運行ONTAP資料管理軟體的專用AFF、 ASA或FAS系統。每個控制器、其儲存、網路連線以及在控制器上執行的ONTAP實例稱為一個「節點」。

節點已配對以提供高可用度（HA）。叢集由這些配對組成（SAN最多12個節點、NAS最多24個節點）。節點可透過專用的私有叢集互連、彼此通訊。

視控制器機型而定、節點儲存設備由Flash磁碟、容量磁碟機或兩者組成。控制器上的網路連接埠可存取資料。實體儲存設備和網路連線資源是虛擬化的、僅供叢集管理員查看、而非NAS用戶端或SAN主機。

HA配對中的節點必須使用相同的儲存陣列模式。否則您可以使用任何支援的控制器組合。您可以透過新增節點（例如儲存陣列機型）來橫向擴充容量、或是新增節點（使用較高階儲存陣列）來提升效能。

當然、您也可以透過所有傳統方式進行垂直擴充、視需要升級磁碟或控制器。ONTAP的虛擬化儲存基礎架構可讓您輕鬆地在不中斷營運的情況下搬移資料、也就是說、您可以垂直或水平擴充、而不需停機。



You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

高可用度配對

叢集節點是以_高可用度（HA）配對_設定、以提供容錯能力和不中斷營運。如果某個節點發生故障、或是您需要關閉節點以進行例行維護、其合作夥伴可以接管其儲存設備、並繼續從其中提供資料。當節點恢復連線時、合作夥伴 _ 會提供 Back_storage 。

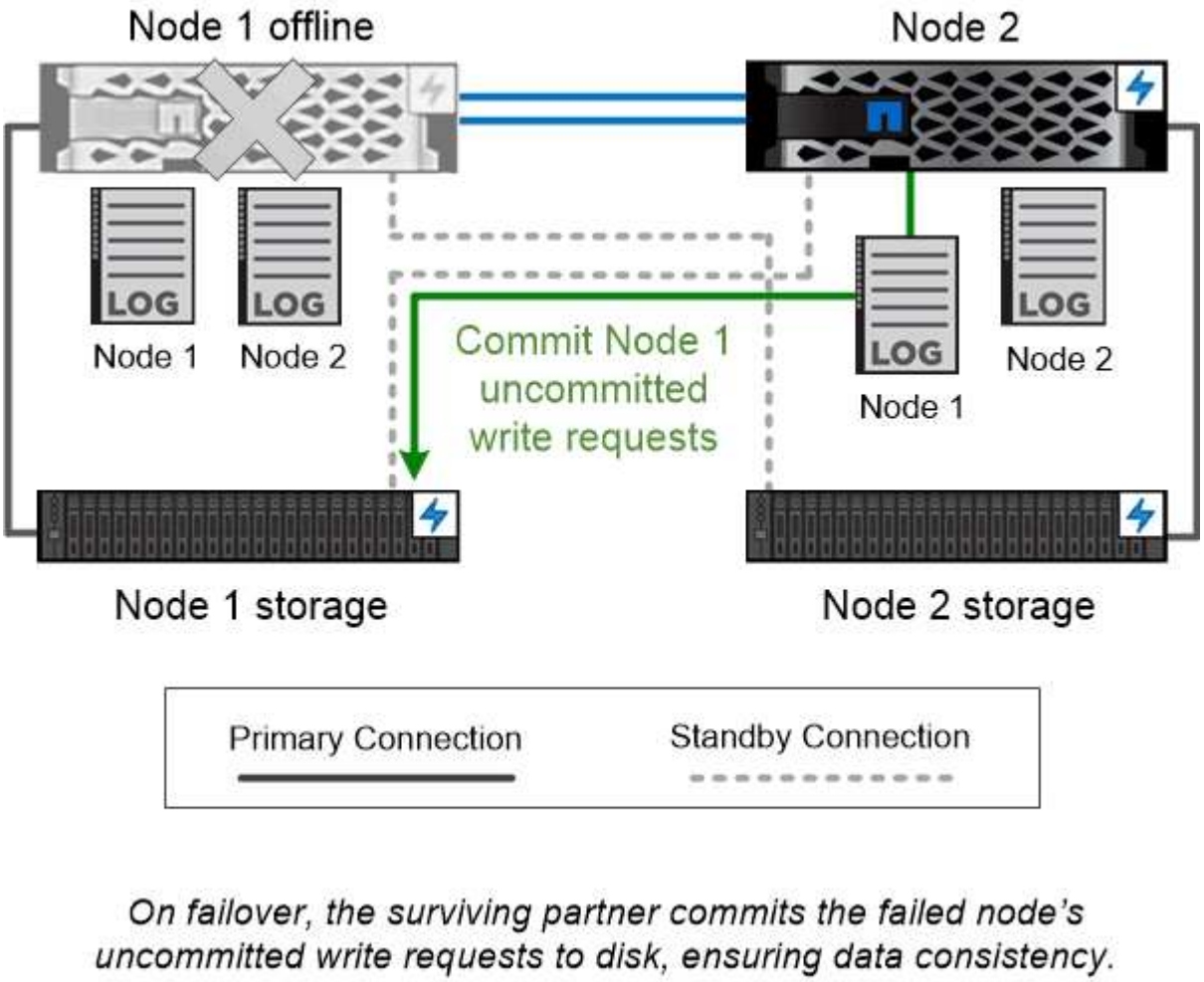
HA配對永遠由類似的控制器機型所組成。控制器通常位於具有備援電源供應器的同一個機箱中。

HA 對是容錯節點，可以以不同的方式相互通信，以允許每個節點不斷檢查其夥伴是否正常運行，並為對方的非揮發性記憶體鏡像日誌資料。當向節點發出寫入請求時，該請求會記錄在兩個節點的NVRAM中，然後再將回應傳送回客戶端或主機。在故障轉移時，倖存的夥伴將故障節點未提交的寫入請求提交到磁碟，確保資料一致性。倖存節點繼續將寫入記錄到NVRAM分區，該分區先前充當故障節點的NVRAM的鏡像。

連線至其他控制器的儲存媒體、可讓每個節點在接管時存取另一個節點的儲存設備。網路路徑容錯移轉機制可確

保用戶端和主機繼續與正常運作的節點通訊。

為確保可用度、您應將任一節點的效能容量使用率維持在50%、以因應容錯移轉案例中的額外工作負載。基於同樣的理由、您可能想要為節點設定不超過NAS虛擬網路介面數量上限的50%。



On failover, the surviving partner commits the failed node's uncommitted write requests to disk, ensuring data consistency.

接收並恢復虛擬**ONTAP** 化的功能

在虛擬化「無共享」 ONTAP實作（例如ONTAP Select）中，節點之間不共用儲存。當某個節點發生故障時，其配對節點將繼續透過該節點資料的同步鏡像副本提供資料。它不會接管該節點的存儲，而只接管其資料服務功能。

AutoSupport 與數位顧問

透過入口網站和行動應用程式、提供人工智慧導向的系統監控與報告功能。ONTAPONTAP 的 AutoSupport 元件會傳送由 Active IQ 數位顧問（也稱為數位顧問）分析的遙測。

Digital Advisor可透過雲端型入口網站和行動應用程式、提供可據以行動的預測分析和主動式支援、讓您在全球混合雲中最佳化資料基礎架構。所有擁有有效 SupportEdge 合約的 NetApp 客戶、都能從數位顧問獲得資料導向的洞見和建議（功能因產品和支援層而異）。

以下是數位顧問的一些功能：

- 規劃升級。數位顧問可識別環境中可透過升級至較新版本的 ONTAP 來解決的問題、而升級顧問元件則可協助您規劃成功的升級。
- 檢視系統健全狀況。數位顧問儀表板會回報任何健康問題、並協助您修正這些問題。監控系統容量、確保儲存空間永遠不會耗盡。
- 管理效能：Digital Advisor 顯示系統效能的時間比 System Manager 長。找出影響您效能的組態和系統問題。
- 最大化效率。檢視儲存效率指標、找出在更少空間中儲存更多資料的方法。
- 檢視庫存與組態。Digital Advisor 會顯示完整的庫存及軟體與硬體組態資訊。查看服務合約何時到期、以確保您享有保固。

相關資訊

"NetApp 文件：數位顧問"

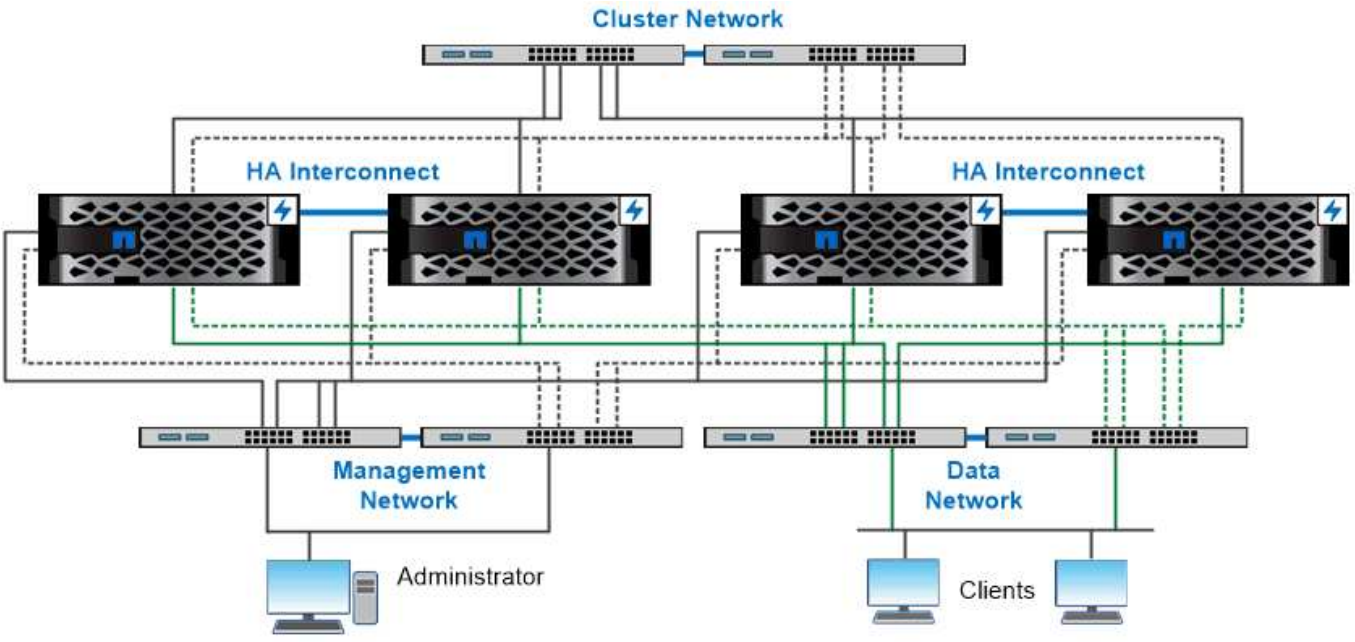
"啟動 Digital Advisor"

"部門服務SupportEdge"

網路架構

網路架構總覽

實作資料中心的網路架構ONTAP 通常包含叢集互連、叢集管理的管理網路、以及資料網路。NIC（網路介面卡）提供實體連接埠以供乙太網路連線使用。HBA（主機匯流排介面卡）提供實體連接埠以供FC連線使用。



The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network.

除了每個節點上提供的實體連接埠之外、您也可以使用_logical連接埠_來管理網路流量。邏輯連接埠是介面群組或VLAN。

介面群組

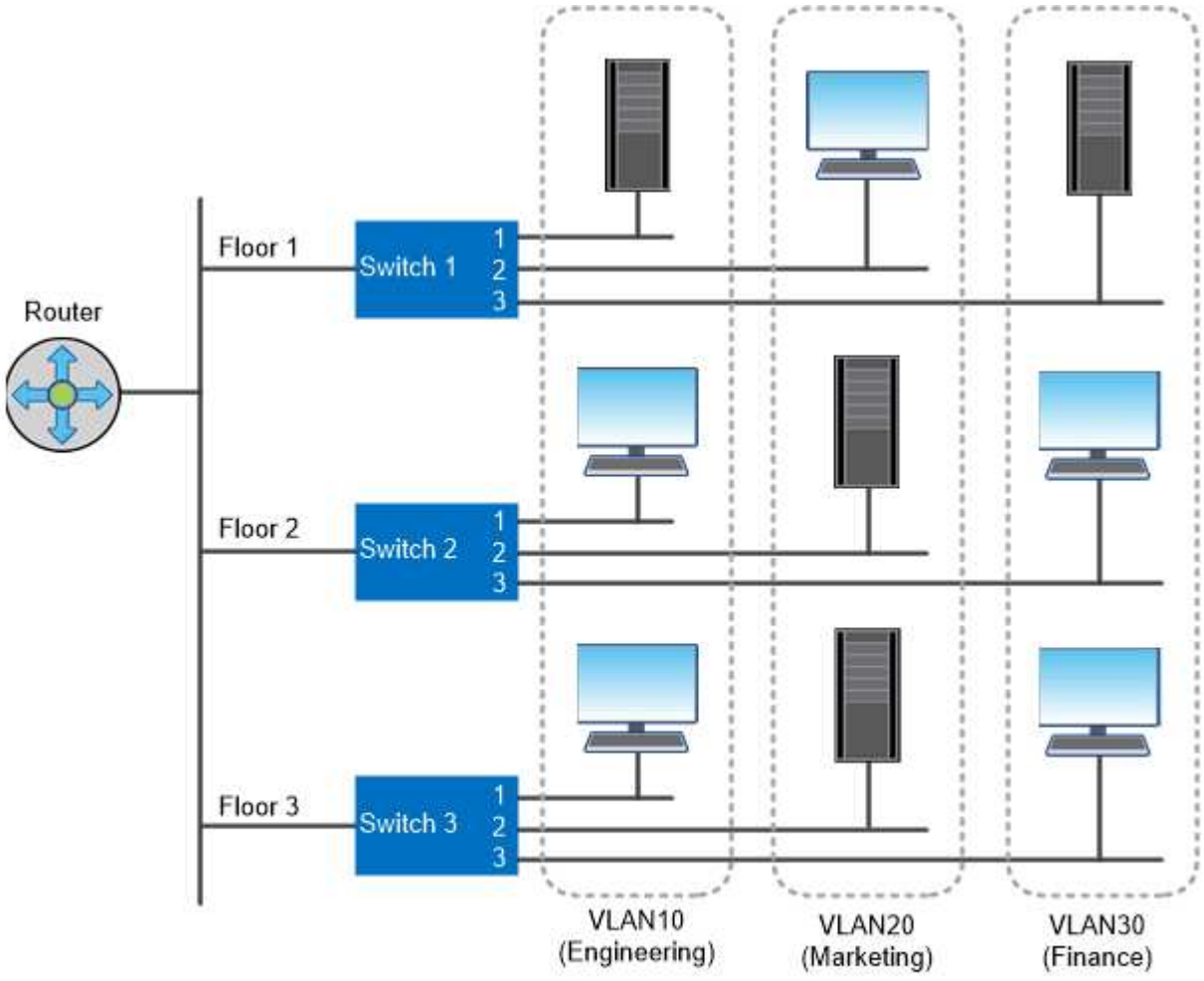
_Interface Groups_將多個實體連接埠合併為單一邏輯「'trunk port'」。您可能想要在不同的PCI插槽中建立一個介面群組、由NIC的連接埠組成、以確保不會發生插槽故障、進而降低業務關鍵流量。

介面群組可以是單一模式、多重模式或動態多重模式。每種模式都提供不同的容錯層級。您可以使用任一類型的多重模式介面群組來平衡網路流量負載。

VLAN

_vlans_可將流量從網路連接埠（可能是介面群組）分隔成以交換器連接埠為基礎而非實體邊界所定義的邏輯區段。屬於VLAN的_end-stations是根據功能或應用程式而定。

您可以依部門（例如工程與行銷部門）或專案（例如releasease1和releasease2）來分組終端站台。由於終端站台的實體鄰近與VLAN無關、因此終端站台可在地理上處於遠端位置。



You can use VLANs to segregate traffic by department.

支援所有主要的產業標準網路技術。ONTAP關鍵技術包括IPspaces、DNS負載平衡及SNMP設陷。

廣播網域、容錯移轉群組及子網路的說明請參閱 NAS路徑容錯移轉。

IPspaces

您可以使用_IPspace_為叢集中的每個虛擬資料伺服器建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

例如、服務供應商可以為使用相同IP位址的租戶設定不同的IPspace、以存取叢集。

DNS負載平衡

您可以使用_DNS負載平衡_、在可用的連接埠之間分散使用者網路流量。DNS伺服器會根據介面上掛載的用戶端數目、動態選取流量的網路介面。

SNMP設陷

您可以使用_SNMP陷阱_定期檢查作業臨界值或故障。SNMP設陷會擷取從SNMP代理程式非同步傳送至SNMP管理程式的系統監控資訊。

FIPS法規遵循

所有SSL連線均符合聯邦資訊處理標準（FIPS）140-2。ONTAP您可以開啟和關閉SSL FIPS模式、全域設定SSL傳輸協定、以及關閉任何弱式加密器、例如RC4。

RDMA 總覽

ONTAP 的遠端直接記憶體存取（ RDMA ）產品支援對延遲敏感的高頻寬工作負載。RDMA可讓資料直接複製到儲存系統記憶體和主機系統記憶體之間、避免CPU中斷和負荷。

NFS over RDMA

從功能組態9.10.1開始ONTAP 、您就可以進行設定 "NFS over RDMA" 在支援NVIDIA GPU的主機上、啟用NVIDIA GPUDirect Storage以GPU加速工作負載。

SMB 協定不支援 RDMA。

叢集互連 RDMA

叢集互連 RDMA 可減少延遲，縮短容錯移轉時間，並加速叢集中節點之間的通訊。

從 ONTAP 9.10.1 開始、當與 X1151A 叢集 NIC 搭配使用時、某些硬體系統支援叢集互連 RDMA 。從 ONTAP 9.13.1 開始、 X91153A NIC 也支援叢集互連 RDMA 。請參閱下表、瞭解不同 ONTAP 版本支援哪些系統。

系統	支援 **ONTAP** 的支援版本
• AFF A50 • AFF A30 • AFF A20 • AFF C80 • AFF C60 • AFF C30 • ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 及更新版本
• AFF A1K • AFF A90 • AFF A70 • ASA A1K • ASA A90 • ASA A70 • FAS90 • FAS70	ONTAP 9.15.1 及更新版本
• 解答900 AFF • ASA A900 • FAS9500	ONTAP 9.13.1 及更新版本
• 解答400 AFF • ASA A400	更新版本ONTAP

根據適當的儲存系統設定，使用叢集互連 RDMA 不需要額外的組態。

用戶端傳輸協定

ONTAP 支援所有主要的業界標準用戶端通訊協定： NFS 、 SMB 、 FC 、 FCoE 、 iSCSI 、 NVMe 和 S3 。

NFS

NFS是UNIX和Linux系統的傳統檔案存取傳輸協定。用戶端可以使用下列通訊協定存取 ONTAP 磁碟區中的檔案。

- NFSv3.
- NFSv4.

- NFSv4.2
- NFSv4.1
- pNFS

您可以使用UNIX型權限、NTFS型權限或兩者的組合來控制檔案存取。

用戶端可以使用NFS和SMB傳輸協定存取相同的檔案。

中小企業

SMB是Windows系統的傳統檔案存取傳輸協定。用戶端可以ONTAP 使用SMB 2.0、SMB 2.1、SMB 3.0和SMB 3.1.1傳輸協定來存取位於支援區內的檔案。就像NFS一樣、支援各種權限樣式。

SMB 1.0可在ONTAP 更新版本中使用、但依預設為停用。

FC

Fibre Channel是原始的網路區塊傳輸協定。區塊傳輸協定會將整個虛擬磁碟呈現給用戶端、而非檔案。傳統FC傳輸協定使用專用FC網路搭配專用FC交換器、因此用戶端電腦必須具備FC網路介面。

LUN代表虛擬磁碟、一個或多個LUN則儲存在ONTAP 一個實體磁碟區中。相同的LUN可透過FC、FCoE和iSCSI傳輸協定存取、但只有當多個用戶端是防止寫入衝突的叢集一部分時、才能存取相同的LUN。

FCoE

FCoE基本上與FC相同、但使用資料中心等級的乙太網路來取代傳統的FC傳輸。用戶端仍需要FCoE專屬的網路介面。

iSCSI

iSCSI是一種區塊傳輸協定、可在標準乙太網路上執行。大多數用戶端作業系統都提供軟體啟動器、可透過標準乙太網路連接埠執行。如果您需要特定應用程式的區塊傳輸協定、但沒有專屬的FC網路功能、iSCSI是很好的選擇。

NVMe / FC 和 **NVMe / TCP**

最新的區塊傳輸協定 NVMe 是專為搭配 Flash 型儲存設備而設計。它提供可擴充的工作階段、大幅縮短延遲、並增加平行處理量、非常適合記憶體內的資料庫和分析等低延遲和高處理量的應用程式。

與FC和iSCSI不同、NVMe不使用LUN。而是使用儲存在ONTAP 功能區中的命名空間。NVMe命名空間只能透過NVMe傳輸協定存取。

S3

從功能支援的S9.8開始ONTAP 、您可以在ONTAP 一個叢集中啟用一個功能不穩定的儲存服務（S3）伺服器ONTAP 、讓您使用S3儲存桶在物件儲存設備中提供資料。

支援兩種內部部署使用案例情境、以提供S3物件儲存服務：ONTAP

- 將資料層移至本機叢集（層級移至本機資源庫）或遠端叢集（雲端層）上的資源桶。FabricPool
- S3用戶端應用程式可存取本機叢集或遠端叢集上的儲存區。

如果您想要在現有叢集上使用S3功能、而不需要額外的硬體和管理、那麼支援該功能就很合適。ONTAP對於超過300TB的部署、NetApp StorageGRID 產品技術仍是NetApp物件儲存的旗艦解決方案。瞭解 "StorageGRID"。

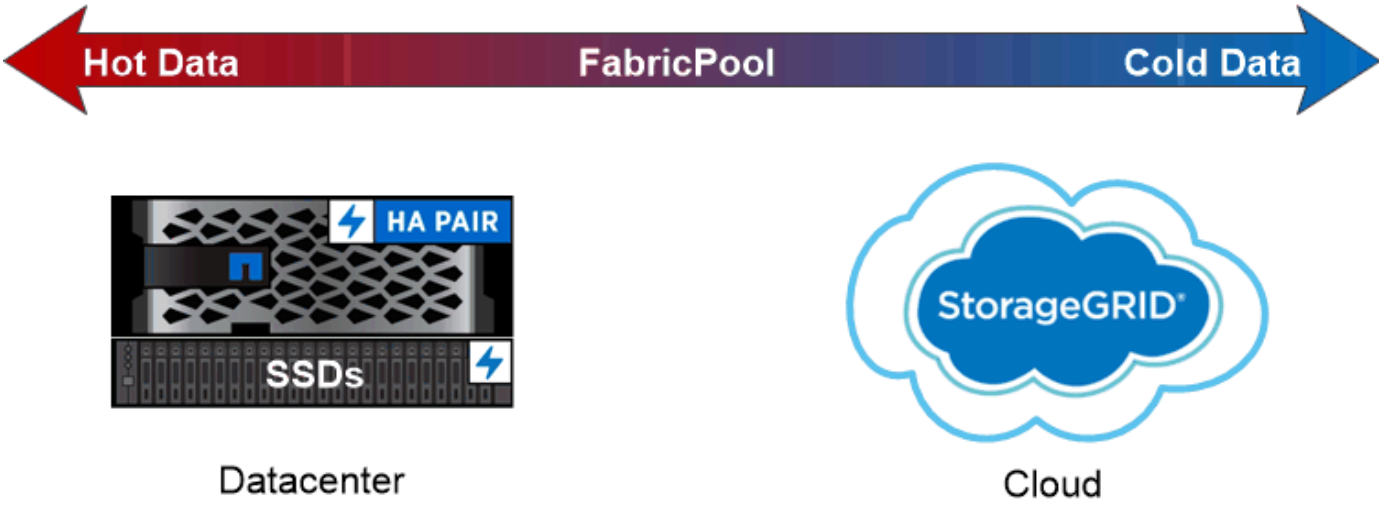
磁碟和本機層

磁碟與 **ONTAP** 本機層

_local st層 _ 也稱為 _aggregate ，是由節點所管理之磁碟的邏輯容器。您可以使用本機層來隔離具有不同效能需求的工作負載、以不同存取模式分層資料、或將資料隔離以符合法規要求。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。

- 對於需要最低延遲和最高效能的業務關鍵應用程式、您可以建立一個完全由SSD組成的本機層。
- 若要以不同的存取模式來分層資料、您可以建立_混合式本機層_、將Flash部署為高效能快取、以供工作資料集使用、同時使用成本較低的HDD或物件儲存設備來儲存較少存取的資料。
  - A "*Flash Pool*"由 SSD 和 HDD 組成。
  - A "FabricPool" 由附有物件存放區的全 SSD 本機層所組成。
- 如果您需要將已歸檔的資料與作用中資料隔離、以供法規遵循之用、您可以使用由容量HDD所組成的本機層級、或是結合效能與容量HDD。



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed “hot” data and object storage for rarely accessed “cold” data.

在 **MetroCluster** 組態中使用本機層級

如果您有 MetroCluster 組態，則應遵循文件中的程序，以取得初始組態，並遵循"MetroCluster"本機層和磁碟管理的準則。

相關資訊

- "管理本機層"
- "管理磁碟"
- "管理RAID組態"
- "管理Flash Pool階層"
- "管理FabricPool 各種雲端階層"

ONTAP RAID 群組和本機層

現代化的RAID技術可在備用磁碟上重建故障磁碟的資料、避免磁碟故障。系統會將「同位元磁碟」上的索引資訊與剩餘健全磁碟上的資料進行比較、以重建遺失的資料、完全不需要停機或大幅降低效能成本。

本機層由一或多個 RAID 群組組成。本機層的_RAID類型_決定RAID群組中的同位元檢查磁碟數目、以及RAID組態保護的同時磁碟故障數目。

預設的RAID類型RAID-DP（RAID雙同位元檢查）每個RAID群組需要兩個同位元檢查磁碟、可在兩個磁碟同時故障時防止資料遺失。對於RAID-DP、建議的RAID群組大小介於12至20個HDD、以及20至28個SSD之間。

您可以在規模調整建議的較高端建立RAID群組、以分散同位元磁碟的成本。尤其是SSD、它比容量磁碟機更可靠。對於使用HDD的本機層級、您應該在最大化磁碟儲存空間的需求與反補貼因素之間取得平衡、例如較大RAID群組所需的重建時間較長。

鏡射和無鏡射的本機階層

您可以使用 ONTAP *RAID* SyncMirror 同步鏡射儲存在不同 RAID 群組中的複本或 *plexs* 中的本機層資料。如果有更多磁碟故障、或是RAID群組磁碟失去連線、則會利用叢碼來確保資料不會遺失。

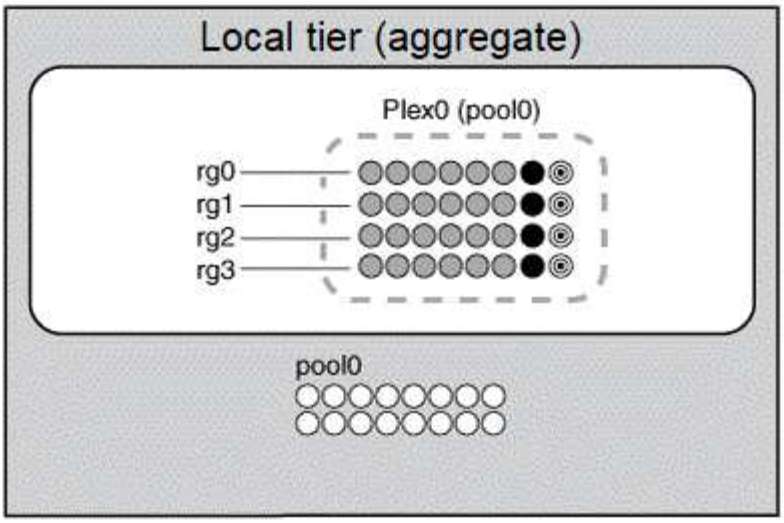
建立本地層時，您可以指定本地層是鏡像的還是非鏡像的。

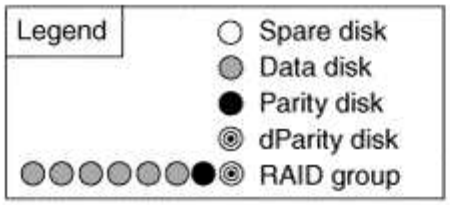
> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

未鏡射的本機階層如何運作

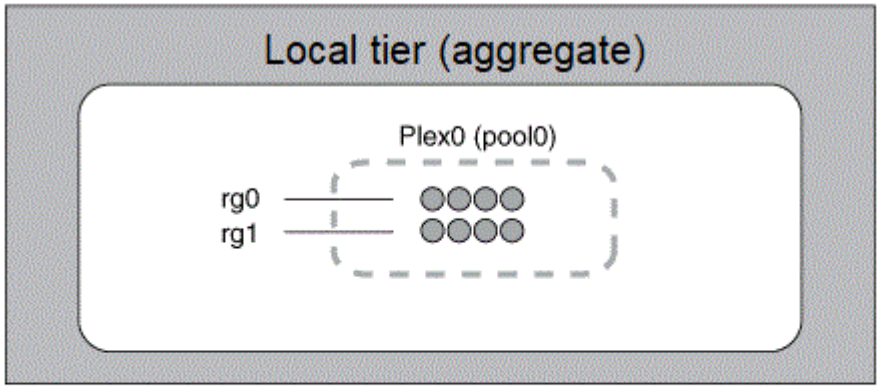
如果您未指定要鏡射本機階層，則會建立為未鏡射的階層。無鏡射的本機層只有一個_plex（資料複本）、其中包含屬於該本機層的所有RAID群組。

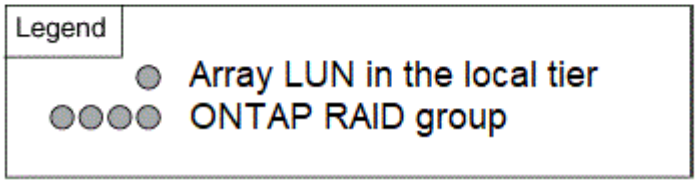
下圖顯示由磁碟組成的無鏡射本機層，分為一個叢集。本機層有四個RAID群組：rg0、rg1、rg2和rg3。每個RAID群組都有六個資料磁碟、一個同位元檢查磁碟和一個同位元檢查（雙同位元檢查）磁碟。本機層所使用的所有磁碟都來自相同的資源池「'Pool0'」。





下圖顯示具有陣列 LUN 的無鏡射本機層，分為一個叢。它有兩個RAID群組：rg0和rg1。本機層所使用的所有陣列LUN均來自同一個集區「'Pool0'」。





鏡射的本機階層運作方式

鏡射本機層有兩個 *plexs* （其資料複本），使用 SyncMirror 功能複製資料以提供備援。

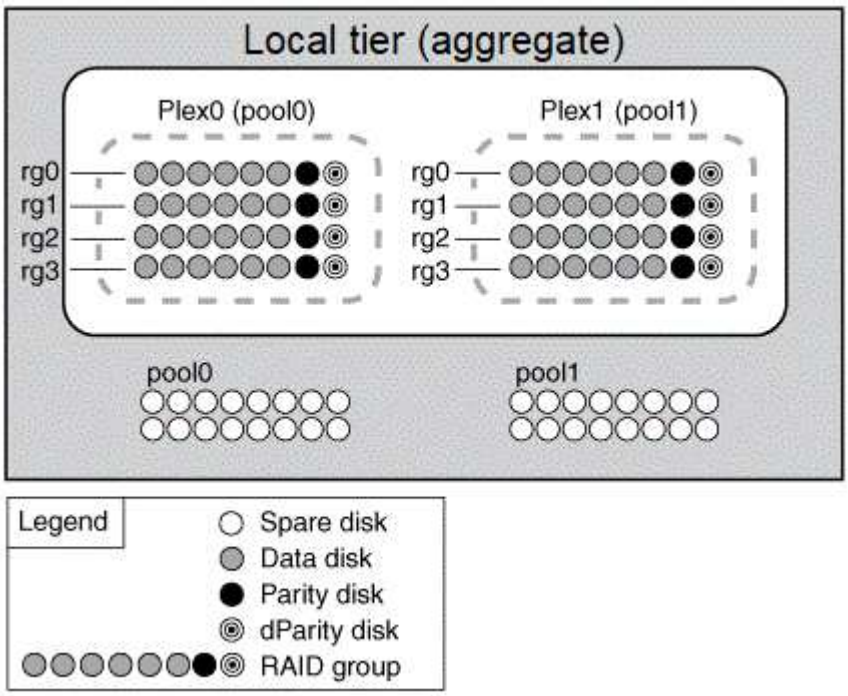
當您建立本機層時，可以指定它是鏡射的。此外、您也可以將第二個叢新增至現有的無鏡射本機層、使其成為鏡射層。ONTAP 使用 SyncMirror 將原始叢（ plex0 ）中的資料複製到新叢（ plex1 ）。實體分離的叢集（每個叢集都有自己的RAID群組及其本身的資源池）、並同時更新叢集。

此組態可在磁碟故障超過本機層級的 RAID 層級時提供額外的保護，避免資料遺失，或是在連線中斷時提供保護

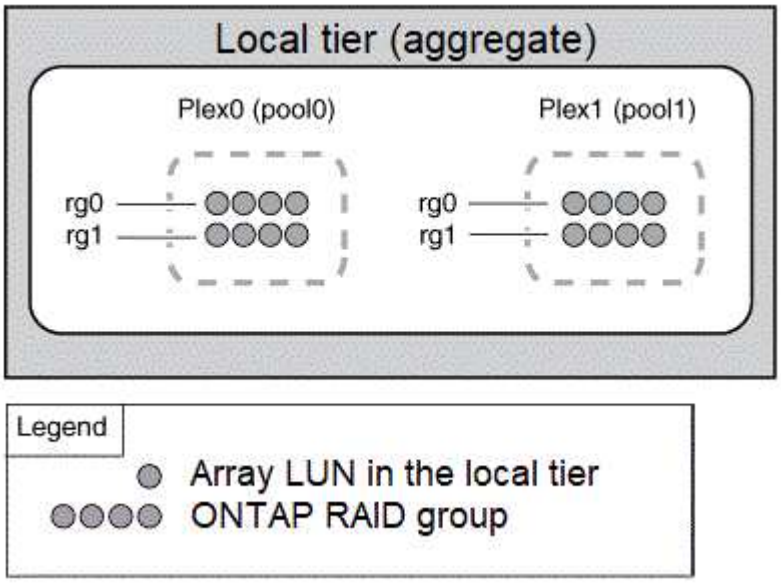
，因為當您修正故障原因時，未受影響的叢會繼續提供資料服務。修復有問題的叢之後、兩個叢會重新同步、並重新建立鏡射關係。

系統上的磁碟和陣列 LUN 分為兩個集區： `pool0`和 `pool1`。Plex0從Pool0取得其儲存設備、而plex1則從Pool1取得其儲存設備。

下圖顯示由啟用並實作 SyncMirror 的磁碟所組成的本機層。已為本機層建立第二個叢 `plex1`。plex1中的資料是plex0中的資料複本、RAID群組也相同。32個備用磁碟會使用16個磁碟來分配給每個集區的Pool0或Pool1。



下圖顯示由啟用SyncMirror 並實作了「支援」功能的陣列LUN所組成的本機層級。已為本機層建立第二個叢 `plex1`。Plex1是plex0的複本、RAID群組也相同。



為了獲得最佳儲存效能和可用性，建議您為鏡像聚合保留至少 20% 的可用空間。雖然建議非鏡像聚合使用 10% 的空間，但額外的 10% 空間可供檔案系統吸收增量變更。由於 ONTAP 的基於寫入時重定向快照的架構，增量變更提高了鏡像聚合的空間利用率。未能遵守這些最佳實踐可能會對績效產生負面影響。

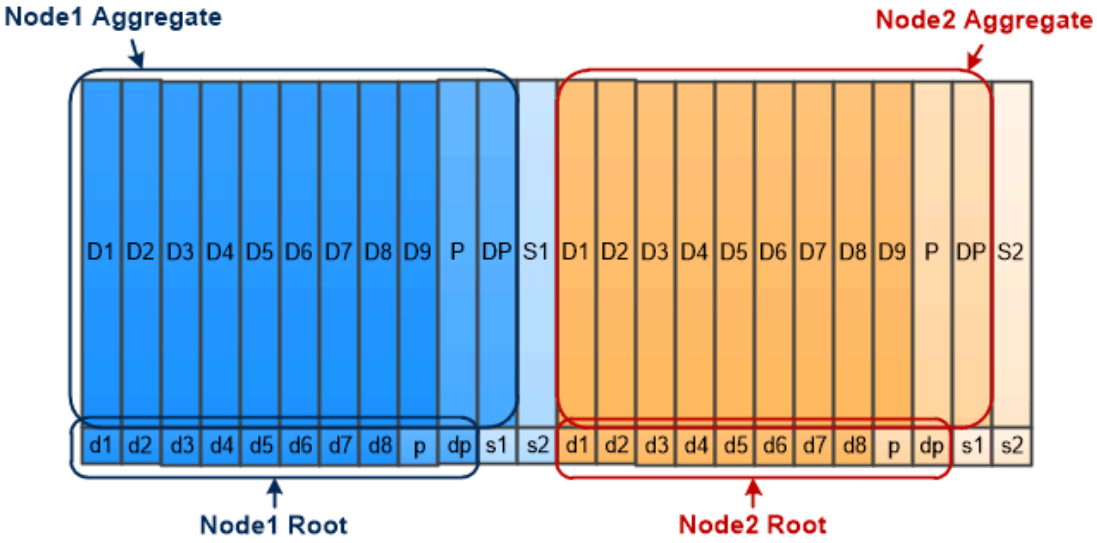
根資料分割

每個節點都必須具有儲存系統組態檔案的根Aggregate。根Aggregate具有資料Aggregate的RAID類型。

System Manager不支援根資料或根資料資料分割。

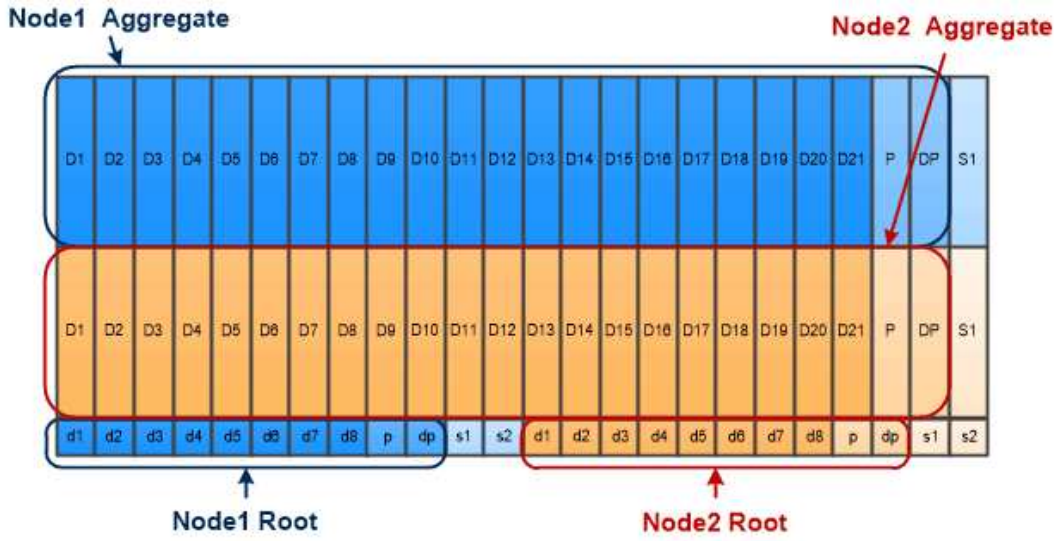
RAID-DP類型的根Aggregate通常由一個資料磁碟和兩個同位元檢查磁碟組成。當系統已為集合體中的每個RAID群組保留兩個磁碟做為同位元磁碟時、這是支付儲存系統檔案的重大「同位元檢查稅金」。

_root-data partition_可在磁碟分割之間分配根Aggregate、將每個磁碟上的一個小分割區保留為根分割區、並將一個大分割區保留給資料、藉此降低同位元檢查的稅金。



Root-data partitioning creates one small partition on each disk as the root partition and one large partition on each disk for data.

如圖所示、用於儲存根Aggregate的磁碟越多、根分割區就越小。這也是一種稱為_root-data-data partition_的根資料分割形式、它會建立一個小分割區做為根分割區、以及兩個較大、大小相同的資料分割區。



Root-data-data partitioning creates one small partition as the root partition and two larger, equally sized partitions for data.

這兩種類型的根資料分割都是ONTAP 《SUR_Advanced Drive Partitioning（ADP）》功能的一部分。這兩種資料都是在原廠設定的：適用於入門級FAS2xxx、FAS9000、FAS8200、FAS80xx和AFF 整套系統的根資料分割、僅適用於AFF 各種系統的根資料分割。

深入瞭解 "進階磁碟分割"。

磁碟機已分割並用於根**Aggregate**

磁碟分割以供根Aggregate使用取決於系統組態。

知道root Aggregate使用多少個磁碟機、有助於判斷根分割區保留多少磁碟機容量、以及資料Aggregate可用的容量。

入門級平台、All Flash FAS 支援平台及FAS 僅連接SSD的支援基礎資料分割功能。

對於入門級平台、只會分割內部磁碟機。

對於FAS 僅連接SSD的All Flash支援平台和FAS 支援功能平台、系統初始化時附加至控制器的所有磁碟機都會進行分割、每個節點最多24個磁碟機。系統組態之後新增的磁碟機不會分割。

磁碟區、**qtree**、檔案和**LUN**

從邏輯容器（稱為_SURO Volumes）將資料提供給用戶端和主機。由於這些磁碟區只與包含Aggregate的磁碟區鬆散結合、因此在管理資料方面比傳統磁碟區更具彈性。ONTAP FlexVol

您可以將多FlexVol 個支援區指派給一個集合體、每個集合區都是專屬於不同的應用程式或服務。您可以擴充及收縮FlexVol 一個邊區、移動FlexVol 一個邊區、並製作FlexVol 一份有效的邊區複本。您可以使用_qtree _將FlexVol 一個流通磁碟區分割成更易於管理的單元、並使用_quotality_來限制磁碟區資源使用量。

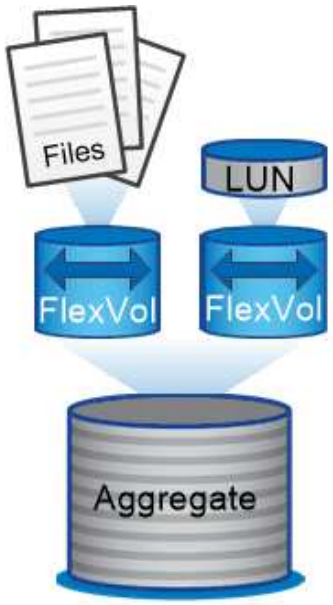
磁碟區包含NAS環境中的檔案系統、以及SAN環境中的LUN。LUN（邏輯單元編號）是SAN傳輸協定所定址的_邏輯單元_裝置識別碼。

LUN是SAN組態中的基本儲存單元。Windows主機將儲存系統上的LUN視為虛擬磁碟。您可以視需要、不中斷營運地將LUN移至不同的磁碟區。

除了資料磁碟區之外、還有幾個您需要知道的特殊磁碟區：

- 節點根磁碟區_（通常為「vol0」）包含節點組態資訊和記錄。
- _SVM根磁碟區_是SVM所提供命名空間的入口點、其中包含命名空間目錄資訊。
- _系統磁碟區_包含特殊的中繼資料、例如服務稽核記錄。

您無法使用這些磁碟區來儲存資料。



Volumes contain files in a NAS environment and LUNs in a SAN environment.

- FlexGroup 《》

在某些企業中、單一命名空間可能需要數PB的儲存容量、甚至遠遠超過FlexVol 了一個不支援的功能。

a _支援多達4000億個檔案、擁有200個組成成員磁碟區、可協同作業、在所有成員之間動態平衡負載與空間分配。FlexGroup

不需要使用FlexGroup 任何功能來維護或管理負荷。您只需建立FlexGroup 一個這個解決方案、然後與NAS用戶端分享。剩下的是、ONTAP

儲存虛擬化

儲存虛擬化總覽

您可以使用_storage虛擬機器（SVM）_為用戶端和主機提供資料。SVM就像虛擬機器在Hypervisor上執行一樣、是將實體資源抽象化的邏輯實體。透過 SVM 存取的資料不會繫結至儲存設備中的位置。對 SVM 的網路存取並未繫結至實體連接埠。

SVM 先前稱為「 vservers 」。 ONTAP 命令列介面仍使用「 vserver 」一詞。

SVM透過一或多個網路邏輯介面（lifs）_、從一或多個磁碟區向用戶端和主機提供資料。磁碟區可指派給叢集中的任何資料集合體。任何實體或邏輯連接埠均可裝載LIF。無論您是執行硬體升級、新增節點、平衡效能、或是跨集合體最佳化容量、都能在不中斷資料服務的情況下移動磁碟區和LIF。

相同的SVM可以有適用於NAS流量的LIF、以及適用於SAN流量的LIF。用戶端和主機只需要LIF的位址（NFS、SMB或iSCSI的IP位址；FC的WWPN）即可存取SVM。LIF會在移動時保留其位址。連接埠可裝載多個LIF。每個SVM都有自己的安全性、管理和命名空間。

除了資料SVM之外、ONTAP 還可部署特殊的SVM來進行管理：

- 建立叢集時會建立_admin SVM_。
- 節點加入新的或現有的叢集時、會建立節點SVM_。
- 系統會自動建立一個_system SVM_、以便在IPspace中進行叢集層級的通訊。

您無法使用這些SVM來提供資料。叢集內與叢集之間的流量、以及叢集與節點管理也有特殊的生命量。

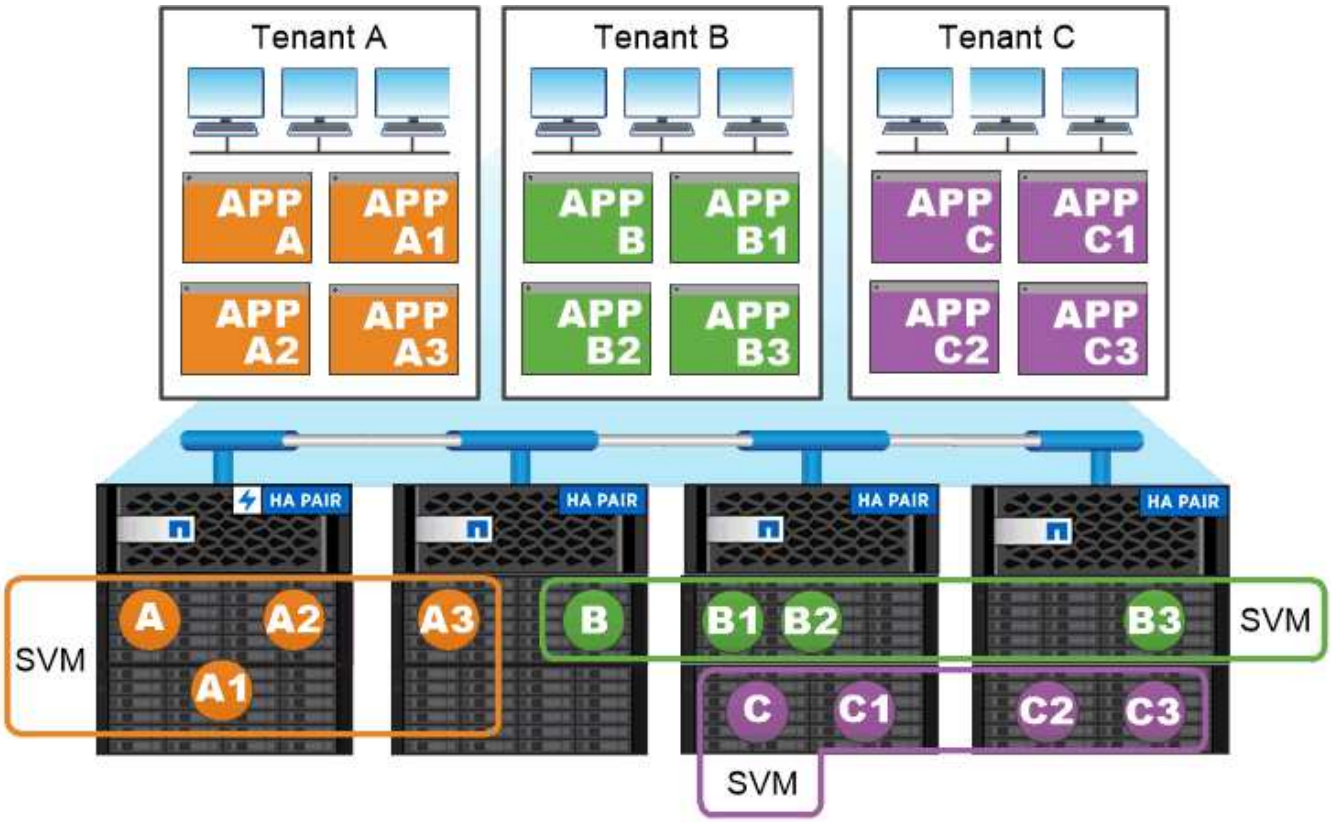
ONTAP 為何像中介軟體

用於儲存管理工作的邏輯物件ONTAP 可滿足設計完善的中介軟體套件所熟悉的目標：保護系統管理員不受低階實作詳細資料的影響、並使組態不受節點和連接埠等實體特性的變更影響。基本的想法是、系統管理員應該能夠輕鬆地移動磁碟區和LIF、重新設定幾個欄位、而非整個儲存基礎架構。

SVM使用案例

服務供應商使用SVM進行安全的多租戶共享安排、隔離每個租戶的資料、為每個租戶提供自己的驗證與管理、並簡化計費。您可以為同一個SVM指派多個LIF、以滿足不同的客戶需求、也可以使用QoS來保護其他租戶的工作負載不會受到「欺負」。

系統管理員將SVM用於企業中的類似用途。您可能想要將資料與不同部門區隔、或是讓某個SVM中的主機存取儲存磁碟區、並讓使用者共用另一個SVM中的磁碟區。有些系統管理員將iSCSI/FC LUN和NFS資料存放區放在一個SVM中、而SMB共用區則放在另一個SVM中。



Service providers use SVMs in multitenant environments to isolate tenant data and simplify chargeback.

叢集與**SVM**管理

_叢集管理員_存取叢集的管理SVM。管理員 SVM 和具有保留名稱的叢集管理員 `admin` 會在叢集設定時自動建立。

具有預設值的叢集管理員 `admin` 角色可以管理整個叢集及其資源。叢集管理員可視需要建立其他具有不同角色的叢集管理員。

_SVM系統管理員_存取資料SVM。叢集管理員會視需要建立資料SVM和SVM管理員。

SVM 系統管理員會被指派 `vsadmin` 依預設、角色。叢集管理員可視需要指派不同的角色給SVM管理員。

角色型存取控制（**RBAC**）_

指派給系統管理員的_role_決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

命名空間和交會點

NAS *namespacity*_是一個邏輯群組、集合在_交會點、以建立單一檔案系統階層架構。具有足夠權限的用戶端可存取命名空間中的檔案、而無需指定檔案在儲存設備中的位置。未

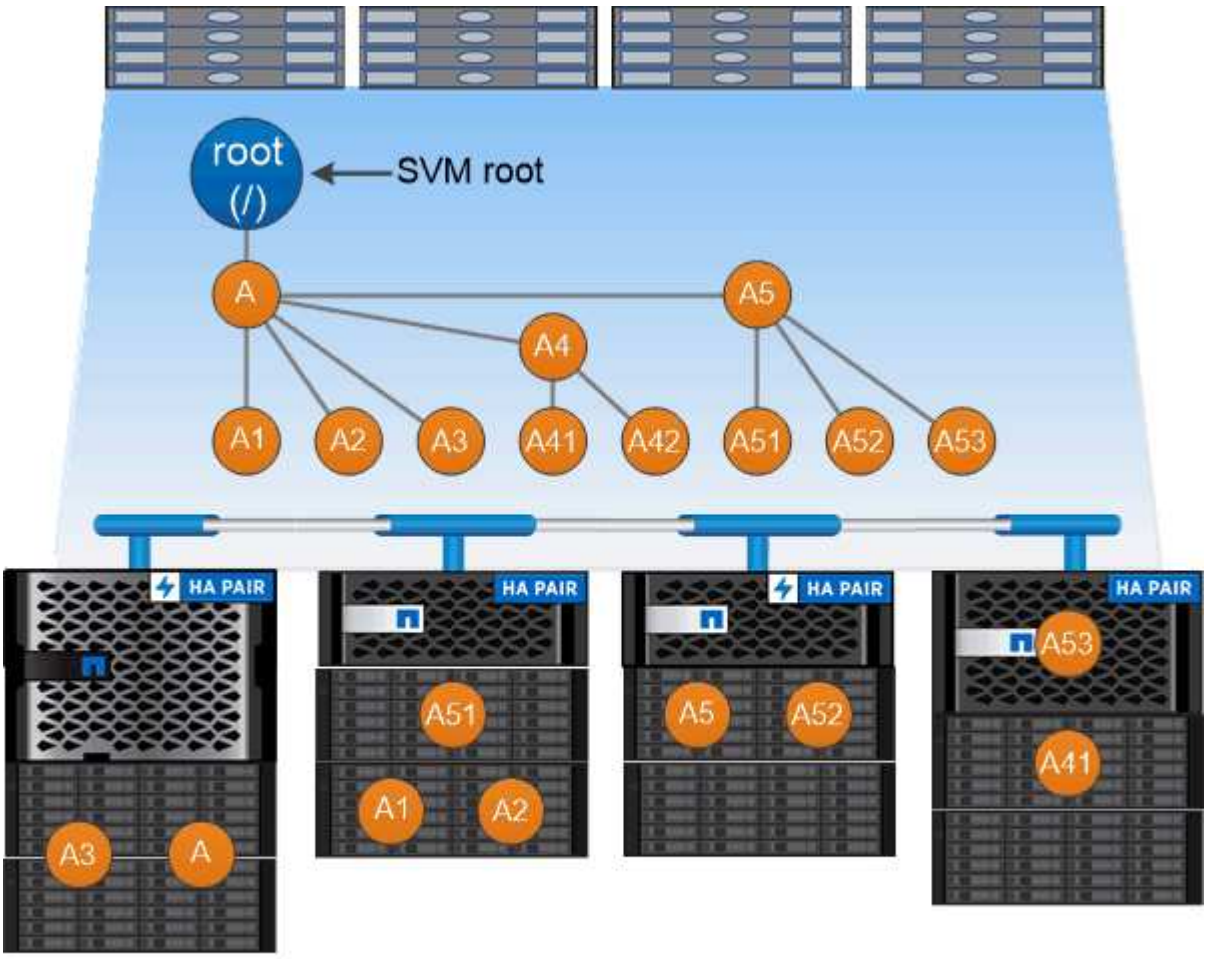
分段的磁碟區可位於叢集中的任何位置。

NAS用戶端不會掛載每個包含感興趣檔案的磁碟區、而是掛載NFS _EX出口_或存取SMB共享區。_匯出或共用區代表整個命名空間或命名空間內的中繼位置。用戶端只會存取裝載於其存取點下方的磁碟區。

您可以視需要將磁碟區新增至命名空間。您可以直接在父磁碟區交會下方或磁碟區內的目錄上建立交會點。名稱為「 'vol3' 」的 Volume 交會路徑可能是 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`或甚至 `/dir1/dir2/vol3`。路徑稱為_junction路徑。_

每個SVM都有一個獨特的命名空間。SVM根磁碟區是命名空間階層架構的起點。

為了確保資料在節點中斷或容錯移轉的情況下仍然可用、您應該為SVM根磁碟區建立_load-sharing mirror _複本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

範例

以下範例建立一個名為「 'home4' 」的 Volume 、該 Volume 位於 SVM VS1 上、且具有交會路徑 `/eng/home` ：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

路徑容錯移轉

路徑容錯移轉總覽

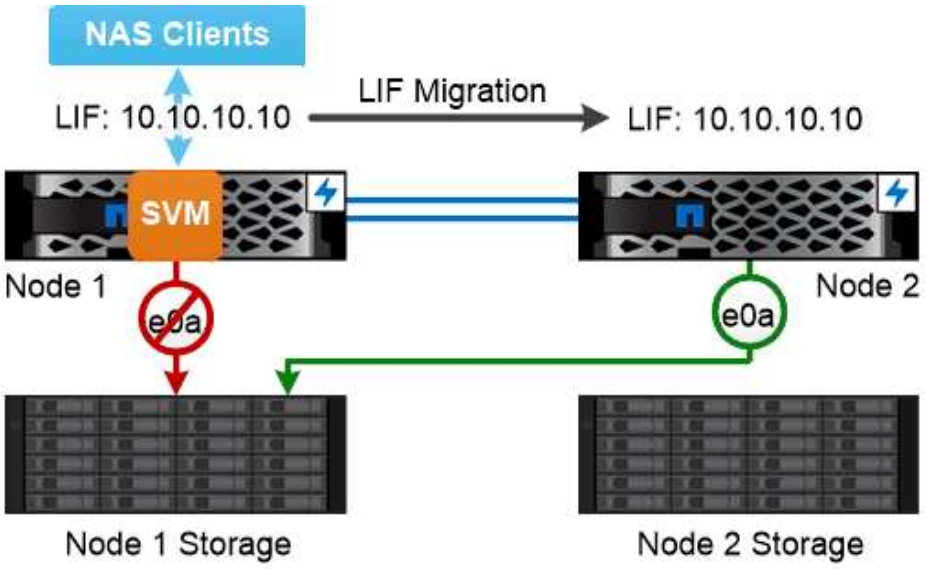
在NAS和SAN拓撲中、由哪種方式進行路徑容錯移轉、有很大的差異ONTAP 。NAS LIF會在連結失敗後自動移轉至不同的網路連接埠。SAN LIF不會移轉（除非您在故障後手動移動）。相反地、主機上的多重路徑技術會將流量轉移到同一個SVM上的不同LIF、但會存取不同的網路連接埠。

NAS路徑容錯移轉

NAS LIF會在目前連接埠的連結失敗後、自動移轉至正常運作的網路連接埠。LIF移轉的連接埠必須是LIF的_Failover群組_成員。容錯移轉群組原則_將資料LIF的容錯移轉目標縮小為擁有資料及其HA合作夥伴的節點上的連接埠。

為了管理上的便利性、ONTAP 在網路架構中為每個_broadcast domain_建立一個容錯移轉群組。廣播網域群組屬於同一個第2層網路的連接埠。例如、如果您使用VLAN來依部門（工程、行銷、財務等）分隔流量、則每個VLAN會定義一個獨立的廣播網域。每次新增或移除廣播網域連接埠時、都會自動更新與廣播網域相關的容錯移轉群組。

使用廣播網域來定義容錯移轉群組、以確保容錯移轉群組保持最新狀態、幾乎永遠都是個好主意。不過，有時候您可能會想要定義與廣播網域無關的容錯移轉群組。例如、您可能希望LIF僅容錯移轉至廣播網域中所定義之連接埠子集內的連接埠。



A NAS LIF automatically migrates to a surviving network port after a link failure on its current port.

子網路_

子網路_保留廣播網域中的IP位址區塊。這些位址屬於同一個第3層網路、當您建立LIF時、會分配給廣播網域中的連接埠。在定義LIF位址時、指定子網路名稱通常比指定IP位址和網路遮罩更容易且更容易出錯。

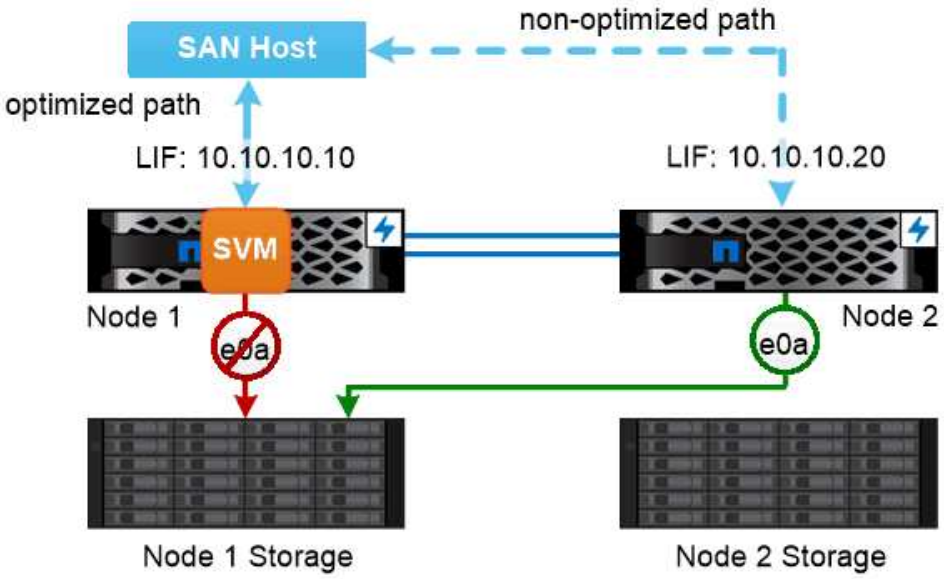
SAN 路徑容錯移轉

SAN主機使用ALUA（非對稱邏輯單元存取）和MPIO（多重路徑I/O）、在連結失敗後將流量重新路由至存續的LIF。預先定義的路徑會決定SVM服務的LUN可能路由。

在SAN環境中、主機會被視為向LUN *Target*提出要求的_啟動器。_ MPIO可啟用從啟動器到目標的多個路徑。ALUA會識別最直接的路徑、稱為_最佳化路徑。_

您通常會在LUN所屬節點上設定多個最佳化的生命路徑、並在HA合作夥伴上設定多個未最佳化的生命路徑。如果擁有節點上的某個連接埠故障、主機會將流量路由傳送至正常運作的連接埠。如果所有連接埠都失敗、主機會透過未最佳化的路徑路由流量。

根據預設、「選擇性LUN對應」（SLM）會限制從主機到LUN的路徑數量。ONTAP新建立的LUN只能透過通往擁有LUN或其HA合作夥伴之節點的路徑存取。您也可以在啟動器的連接埠集_中設定lifs、以限制對LUN的存取。



A SAN host uses multipathing technology to reroute traffic to a surviving LIF after a link failure.

在SAN環境中移動磁碟區_*

根據預設、ONTAP 將從SAN主機到LUN的路徑數量限制為由SURE_Selective LUN Map（SLM__）。新建立的*LUN*只能透過通往擁有*LUN*或其*HA*合作夥伴（*LUN*的_報告節點）節點的路徑存取。

這表示當您將磁碟區移至另一個HA配對上的節點時、您需要將目的地HA配對的報告節點新增至LUN對應。然後您可以在MPIO設定中指定新的路徑。磁碟區移動完成後、您可以從對應中刪除來源HA配對的報告節點。

ONTAP 中的負載平衡

當節點上的工作量超過可用資源時、工作負載的效能會開始受到延遲的影響。您可以增加可用資源（升級磁碟或CPU）、或減少負載（視需要將磁碟區或LUN移至不同節點）、來管理過載的節點。

您也可以使用 ONTAP _ 儲存服務品質（ QoS ） _ 來保證關鍵工作負載的效能不會因為競爭工作負載而降低：

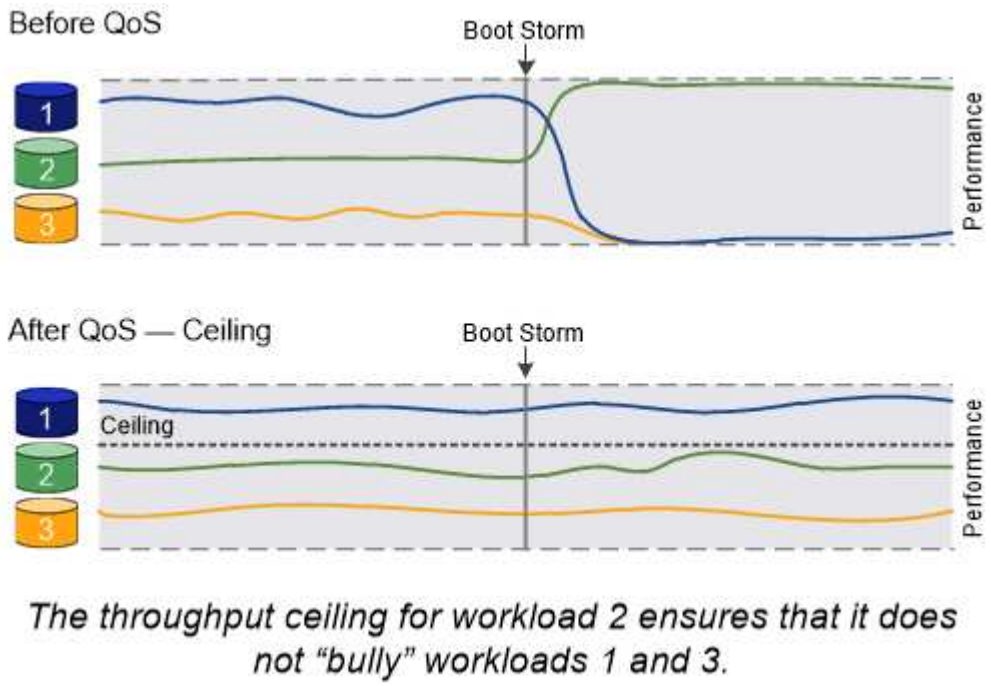
- 您可以在競爭的工作負載上設定QoS處理量上限、以限制其對系統資源的影響（QoS上限）。
- 您可以針對關鍵工作負載設定QoS處理量_flo__、確保無論競爭工作負載的需求為何、它都能達到最低處理量目標（QoS下限）。
- 您可以為相同的工作負載設定QoS上限和樓層。

處理量上限

處理量上限會將工作負載的處理量限制為最大IOPS或MB/s在下圖中、工作負載2的處理量上限可確保其不會「受到欺凌」的工作負載1和3。

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

工作負載的處理量可能超過指定上限10%、尤其是當工作負載處理量發生快速變化時。處理突發的上限可能超過50%。



The throughput ceiling for workload 2 ensures that it does not "bully" workloads 1 and 3.

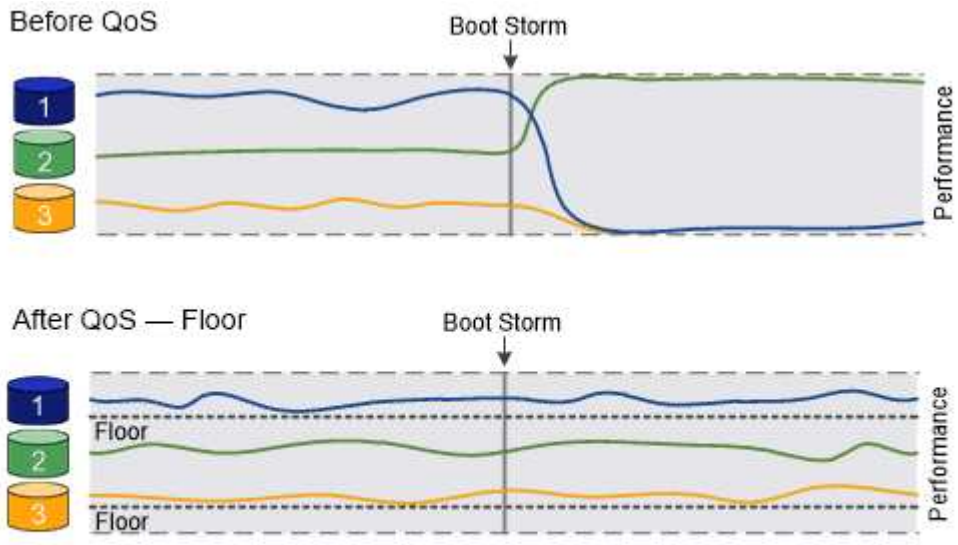
處理量層

處理量層級可確保工作負載的處理量不會低於最低IOPS數。在下圖中、工作負載1和工作負載3的處理量層級可確保它們符合最低處理量目標、無論工作負載2的需求為何。

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

工作負載代表磁碟區、LUN或ONTAP 從檔名不含資訊的9.3開始的I/O作業。定義處理量層的原則群組無法套用至SVM。您可以在建立原則群組時指定樓層、也可以等到監控工作負載之後再指定樓層。

如果節點或集合體上的效能容量（保留空間）不足、或在類似的關鍵作業期間、工作負載的處理量可能會低於指定的樓層 `volume move trigger-cutover`。即使有足夠的可用容量且未執行關鍵作業、工作負載的處理量仍可能低於指定樓層達5%。



The throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

調適性**QoS**

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

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

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

在ONTAP 更新版本的更新版本中、可在處理量層使用已用的空間。ONTAP 9.4 及更早版本的處理量樓層不支援此功能。

+ 從 ONTAP 9.13.1 開始，您可以使用調適性 QoS 來設定 SVM 層級的處理量樓層和天花板。

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

IOPS/GB、則儲存100 GB資料的150 GB磁碟區的處理量上限為10、000 IOPS。隨著使用空間量的變化、調適性QoS會根據比率調整處理量上限。

複寫

快照

傳統上、功能完善的複寫技術可滿足災難恢復（DR）和資料歸檔的需求。ONTAP隨著雲端服務的問世、ONTAP NetApp Data Fabric中的端點之間的資料傳輸功能已經過調整、因此可進行此功能的不中斷複寫。這些用途的基礎是 ONTAP 快照技術。

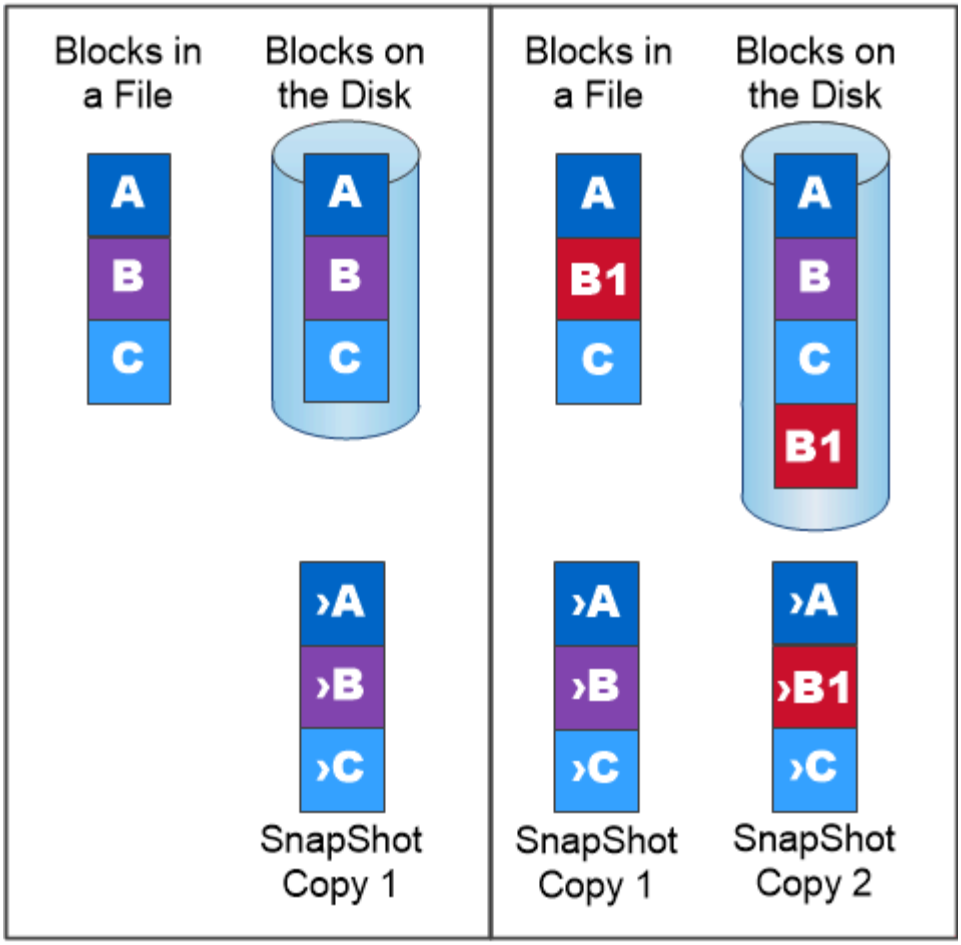
_snapshot （前身為 _Snapshot 複本）是磁碟區的唯讀時間點映像。建立快照之後，作用中檔案系統和快照會指向相同的磁碟區塊，因此快照不會使用額外的磁碟空間。隨著時間的推移，映像會佔用最小的儲存空間，而且效能成本也可忽略不計，因為它只會記錄自上次快照建立以來對檔案所做的變更。

快照的效率是 ONTAP 核心儲存虛擬化技術 _ 隨處寫入檔案配置（ WAFL ） _ 。 WAFL 像資料庫一樣，使用中繼資料來指向磁碟上的實際資料區塊。但是WAFL 、不像資料庫、不像是使用什麼功能來覆寫現有的區塊。它會將更新的資料寫入新的區塊、並變更中繼資料。

快照非常有效率，因為 ONTAP 在建立快照時會參考中繼資料，而非複製資料區塊。如此一來、其他系統就不再需要「尋找時間」來尋找要複製的區塊、也不需要自行製作複本。

您可以使用快照來恢復個別檔案或 LUN ，或還原磁碟區的全部內容。ONTAP 會將快照中的指標資訊與磁碟上的資料進行比較，以重建遺失或損壞的物件，而不會造成停機或重大效能成本。

_snapshot 原則 _ 定義系統如何建立磁碟區快照。原則會指定何時建立快照，要保留多少份複本，如何命名快照，以及如何將其標示為複寫。例如，系統可能每天在上午 12 ： 10 建立一個快照，保留兩個最新的複本，將其命名為「 daily 」（附加時間戳記），並將其標示為「 daily 」以供複寫。



A Snapshot copy records only changes to the active file system since the last Snapshot copy.

SnapMirror災難恢復和資料傳輸

_SnapMirror是災難恢復技術、專為從一線儲存設備容錯移轉到位於地理位置遠端站台的二線儲存設備而設計。顧名思義、SnapMirror會在二線儲存設備中建立工作資料的複本（或鏡射）、以便在主站台發生災難時、繼續提供資料。

資料會在磁碟區層級鏡射。一線儲存設備的來源磁碟區與二線儲存設備的目的地磁碟區之間的關係稱為「資料保護」關係。_磁碟區所在的叢集與從磁碟區提供資料的SVM必須經過_處理。_對等關係可讓叢集與SVM交換資料資料安全無虞。

您也可以在SVM之間建立資料保護關係。在這種關係中、系統會複寫SVM組態的全部或部分內容、從NFS匯出、SMB共用到RBAC、以及SVM所擁有的磁碟區中的資料。

從 ONTAP 9 。 10.1 開始、您可以使用 SnapMirror S3 在 S3 儲存區之間建立資料保護關係。目的地庫位可位於本機ONTAP 或遠端的不支援系統、或StorageGRID 是位於非ONTAP系統上、例如：

第一次叫用SnapMirror時、它會執行從來源磁碟區到目的地磁碟區的_基準傳輸_。基礎傳輸通常涉及下列步驟：

- 製作來源 Volume 的快照。

- 將快照及其參照的所有資料區塊傳輸至目的地 Volume 。
- 將來源磁碟區上的剩餘快照傳輸到目的地磁碟區，以便在「 'active' 」鏡像毀損時使用。

一旦完成基礎傳輸， SnapMirror 只會將新的快照傳輸至鏡像。更新是非同步的、會依照您設定的排程進行。保留會鏡射來源上的快照原則。當主要站台發生災難時、您可以在最少中斷的情況下啟動目的地Volume、並在還原服務時重新啟動來源Volume。

由於 SnapMirror 只會在建立基準線之後傳輸快照，因此複寫作業快速且不中斷營運。如同容錯移轉使用案例所暗示、次要系統上的控制器應與主要系統上的控制器相當或幾乎等同、以有效率地從鏡射儲存設備提供資料。

A SnapMirror data protection relationship mirrors the Snapshot copies available on the source volume.

使用**SnapMirror**進行資料傳輸

您也可以使用SnapMirror在NetApp資料架構的端點之間複寫資料。建立SnapMirror原則時、您可以選擇一次性複寫或重複複複寫。

SnapMirror 雲端備份至物件儲存設備

SnapMirror Cloud 是一項備份與還原技術、專為想要將資料保護工作流程移轉至雲端的 ONTAP 使用者所設計。從舊有備份到磁帶架構移轉的組織、可以使用物件儲存設備做為長期資料保留和歸檔的替代儲存庫。SnapMirror 雲端提供 ONTAP 對物件的儲存複寫、作為永久遞增備份策略的一部分。

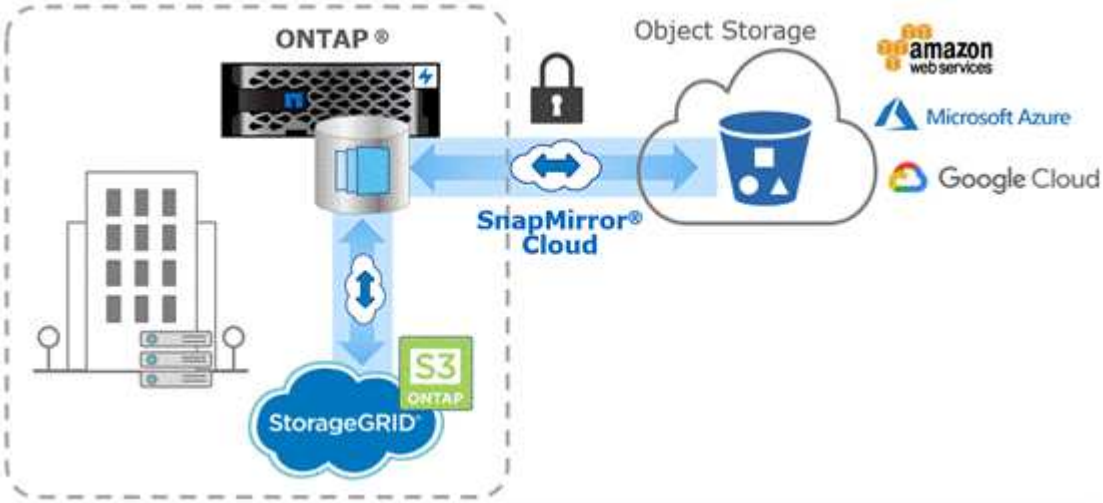
SnapMirror 雲端複寫是一項授權的 ONTAP 功能。SnapMirror Cloud 是在 ONTAP 9 8 中推出、作為 SnapMirror 複寫技術系列的延伸。雖然 SnapMirror 經常用於 ONTAP 對 ONTAP 備份，但 SnapMirror 雲端使用相同的複寫引擎，將 ONTAP 的快照傳輸至符合 S3 標準的物件儲存備份。

SnapMirror 雲端的目標是備份使用案例、同時支援長期保留和歸檔工作流程。與 SnapMirror 一樣、初始 SnapMirror 雲端備份會執行磁碟區的基礎傳輸。對於後續備份， SnapMirror 雲端會產生來源磁碟區的快照，並只將變更的資料區塊傳輸到物件儲存目標。

SnapMirror 雲端關係可在 ONTAP 系統和特定內部部署和公有雲物件儲存目標之間進行設定、包括 Amazon S3 、 Google Cloud Storage 和 Microsoft Azure Blob Storage 。其他內部部署物件儲存目標包括 StorageGRID 和 ONTAP S3 。

除了使用 ONTAP 系統管理員來管理 SnapMirror 雲端組態之外，還有幾個協調選項可用於管理 SnapMirror 雲端備份：

- 支援 SnapMirror 雲端複寫的多個協力廠商備份合作夥伴。您可以在上找"NetApp部落格"到參與廠商。
- NetApp Backup and Recovery 是適用於ONTAP環境的NetApp原生解決方案
- API可用於開發自訂的資料保護工作流程軟體、或是運用自動化工具



歸檔**SnapVault**

SnapMirror授權可用於支援SnapVault 以還原為備份的功能、以及用於災難恢復的SnapMirror關係。從 ONTAP 9.3 開始、 SnapVault 授權已過時、 SnapMirror 授權可用於設定資料保險箱、鏡射和鏡射與資料保險箱的關係。SnapMirror 複寫可用於快照的 ONTAP 對 ONTAP 複寫，同時支援備份和災難恢復使用案例。

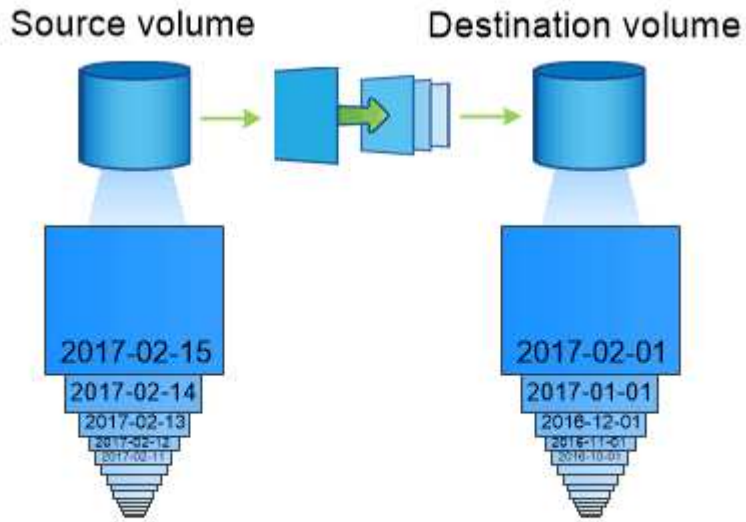
SnapVault 是一項歸檔技術，專為磁碟對磁碟快照複寫所設計，以符合標準及其他治理相關用途。與 SnapMirror 關係不同的是，目的地通常只包含目前位於來源 Volume 中的快照， SnapVault 目的地通常會保留在較長時間內建立的時間點快照。

例如，您可能想要在 20 年內保留每月資料快照，以符合貴企業的政府會計法規。由於不需要從保存庫儲存設備提供資料、因此您可以在目的地系統上使用速度較慢、成本較低的磁碟。

與SnapMirror一樣、SnapVault 當您第一次叫用時、會執行基礎傳輸。它會建立來源磁碟區的快照，然後將複本及其參照的資料區塊傳輸至目的地磁碟區。與 SnapMirror 不同的是， SnapVault 在基準線中不包含較舊的快照。

更新是非同步的、會依照您設定的排程進行。您在關係原則中定義的規則，可識別哪些新快照要包含在更新中，以及保留多少份複本。原則中定義的標籤（例如「每月」）必須符合來源上快照原則中定義的一或多個標籤。否則、複寫會失敗。

SnapMirror和SnapVault SnapMirror共用相同的命令基礎架構。您可以指定建立原則時要使用的方法。這兩種方法都需要經過處理的叢集和經過處理的SVM。



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

雲端備份與支援傳統備份

除了 SnapMirror 和 SnapVault 資料保護關係（僅適用於 ONTAP 9.7 及更早版本的磁碟對磁碟）之外、現在還有多種備份解決方案、可為長期資料保留提供較便宜的替代方案。

許多第三方資料保護應用程式提供ONTAP管理資料的傳統備份。Veeam、Veritas和CommVault等產品均可提供ONTAP 整合式的支援功能、以供支援各種系統的使用。

從 ONTAP 9.8 開始， SnapMirror 雲端可將快照從 ONTAP 執行個體非同步複寫至物件儲存端點。SnapMirror 雲端複寫需要授權應用程式、才能協調及管理資料保護工作流程。ONTAP 系統支援 SnapMirror 雲端關係、可選擇內部部署和公有雲物件儲存目標、包括 AWS S3 、 Google Cloud Storage Platform 或 Microsoft Azure Blob Storage 、這些目標可透過廠商備份軟體提供更高的效率。請聯絡您的NetApp代表、以取得支援的認證應用程式與物件儲存廠商清單。

如果您對雲端原生資料保護感興趣，可以使用NetApp控制台設定本機磁碟區和公有雲中的Cloud Volumes ONTAP個體之間的SnapMirror或SnapVault關係。

此控制台還使用軟體即服務 (SaaS) 模型提供Cloud Volumes ONTAP實例的備份。使用者可以使用NetApp備份和還原將其Cloud Volumes ONTAP實例備份到 S3 和符合 S3 的公有雲物件儲存。

"本文檔Cloud Volumes ONTAP"

"NetApp控制台文檔"

"NetApp控制台"

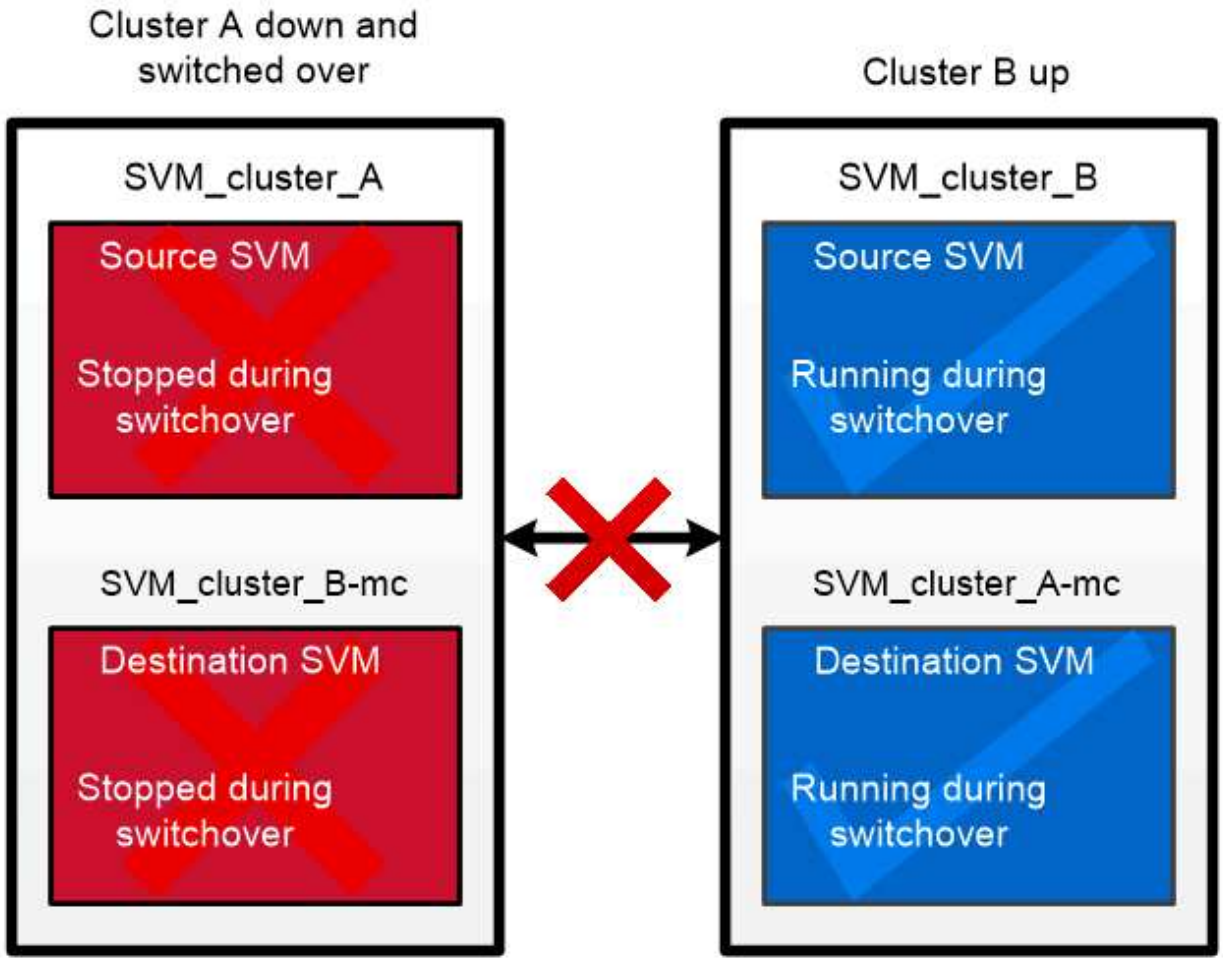
持續可用度**MetroCluster**

透過實作兩個實體獨立的鏡射叢集、可利用各種組態來保護資料。MetroCluster每個叢集都會同步複寫另一個叢集的資料和SVM組態。萬一某站台發生災難、系統管理員可以啟動鏡射SVM、並從存續站台開始提供資料。

- *Fabric* 附加的 *MetroCluster* 和 *MetroCluster IP* 組態支援全城叢集。
- _Stretch MetroCluster S__組態可支援園區內的叢集。

無論是哪種情況、都必須執行叢集處理。

使用稱為「*Estres*」的功能、在另一個叢集的儲存設備中、以複本或_plexes_同步鏡射每個叢集的集合體資料。MetroCluster ONTAP SyncMirror如果發生切換、則存續叢集上的遠端叢集會上線、而次要SVM會開始提供資料。



When a MetroCluster switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

在非 MetroCluster 實作中使用 SyncMirror *
您可以選擇在非 MetroCluster 實作中使用 SyncMirror 來防止資料遺失、如果磁碟故障的數量超過 RAID 類型所保護的數量、或是連線到 RAID 群組磁碟的連線中斷。此功能僅適用於HA配對。

Aggregate資料會鏡射到儲存在不同磁碟櫃上的叢中。如果其中一個磁碟櫃無法使用、則未受影響的叢會在您修復故障原因時繼續提供資料。

請記住、使用SyncMirror 仰賴不鏡射的Aggregate鏡射需要兩倍的儲存容量。每個叢需要的磁碟數量、與鏡射的叢磁碟數量相同。例如、您需要2、880 GB的磁碟空間來鏡射1、440 GB的集合體、每個叢體需要1、440 GB的空間。

有了 SyncMirror 、建議您至少保留 20% 的可用空間來容納鏡射的集合體、以獲得最佳的儲存效能和可用度。雖然建議非鏡射的集合體為 10% 、但檔案系統可能會使用額外 10% 的空間來吸收遞增變更。由於 ONTAP 的寫入時複製快照架構，遞增變更可增加鏡射集合體的空間使用率。不遵守這些最佳實務做法可能會對 SyncMirror 重新同步效能造成負面影響、間接影響非共享雲端部署的作業工作流程、以及 MetroCluster 部署的切換。

儲存效率

ONTAP 儲存效率總覽

儲存效率是透過最佳化儲存資源，將浪費的空間減至最低，以及減少寫入資料的實體佔用空間，來衡量儲存系統使用可用空間的效率。更高的儲存效率可讓您以最低的成本、在最小的空間內儲存最大數量的資料。例如、利用儲存效率技術來偵測及消除重複的資料區塊、以及填滿零的資料區塊、可減少您所需的實體儲存設備總容量、並降低整體成本。

ONTAP 提供各式各樣的儲存效率技術、可減少資料所消耗的實體硬體或雲端儲存容量、並大幅提升系統效能、包括更快讀取資料、更快複本資料集、以及更快的 VM 資源配置。

ONTAP 儲存效率技術包括：

- 精簡配置

  資源隨需配置 可讓您視需要在磁碟區或 LUN 中分配儲存設備、而非事先保留。 如此可讓您根據潛在使用量過度分配磁碟區或 LUN 、而無需保留目前未使用的空間、進而減少所需的實體儲存容量。

- 重複資料刪除

  重複資料刪除 以三種不同方式減少磁碟區所需的實體儲存容量。

  - * 零區塊重複資料刪除 *

    零區塊重複資料刪除功能可偵測並消除填滿全部零的資料區塊、而且只會更新中繼資料。然後會儲存零區塊通常使用的 100% 空間。 在所有已進行重複資料刪除的磁碟區上、預設會啟用零區塊重複資料刪除。

  - * 內嵌重複資料刪除 *

    內嵌重複資料刪除功能會偵測重複資料區塊、並在資料寫入磁碟之前、以唯一的共用區塊參照來取代這些區塊。內嵌重複資料刪除技術可將 VM 資源配置加快 20% 至 30% 。 視您的 ONTAP 版本和平台而定、可在 Volume 或 Aggregate 層級使用即時重複資料刪除技術。 AFF 和 ASA 系統預設會啟用此功

能。您需要在 FAS 系統上手動啟用內嵌重複資料刪除功能。

- * 背景重複資料刪除 *

  背景重複資料刪除功能也會偵測重複資料區塊、並以唯一的共用區塊參照來取代它們、但在資料寫入磁碟後、會進一步提升儲存效率。 您可以設定背景重複資料刪除功能、以便在儲存系統符合特定條件時執行。例如、您可以啟用背景重複資料刪除功能、以便在磁碟區達到 10% 使用率時執行。 您也可以手動觸發背景重複資料刪除、或將其設定為在特定排程上執行。AFF 和 ASA 系統預設會啟用此功能。您需要在 FAS 系統上手動啟用背景重複資料刪除功能。

在磁碟區內及在集合體內的磁碟區之間支援重複資料刪除技術。 讀取已刪除重複資料通常不會收取效能費用。

- 壓縮

  壓縮 將資料區塊合併在壓縮群組中、每個資料區塊都儲存為單一區塊、藉此減少磁碟區所需的實體儲存容量。收到讀取或覆寫要求時、只會讀取一小群區塊、而非整個檔案。此程序可最佳化讀取和覆寫效能、並在壓縮檔案的大小上提供更大的擴充性。

  壓縮可以在線上或後處理中執行。即時壓縮可在資料寫入磁碟之前、先壓縮記憶體中的資料、立即節省空間。後處理壓縮會先將區塊以未壓縮的方式寫入磁碟、然後在排程時間壓縮資料。在 AFF 系統上、預設會啟用此功能。您需要在所有其他系統上手動啟用壓縮。

- * Compaction *

  資料壓縮可將儲存在 4 KB 區塊中但大小小於 4 KB 的資料區塊結合成單一區塊、藉此減少磁碟區所需的實體儲存容量。資料仍在記憶體中時、就會進行壓縮、因此不會在磁碟上消耗不必要的空間。 AFF 和 ASA 系統預設會啟用此功能。您需要手動啟用 FAS 系統上的壓縮功能。

- * FlexClone 磁碟區、檔案和 LUN*

  FlexClone 技術利用快照中繼資料來建立磁碟區，檔案或 LUN 的可寫入時間點複本。複本會與父資料區塊共用資料區塊、除非將變更寫入複本或其父資料、否則不會使用任何儲存區。寫入變更時、只會儲存差異。

  傳統的資料集複本可能需要幾分鐘甚至數小時的時間才能建立、 FlexClone 技術甚至能讓您即時複製最大的資料集。

- * 對溫度敏感的儲存效率 *

  ONTAP 可評估磁碟區資料的存取頻率、並將該頻率對應至套用至該資料的壓縮程度、進而提供 "對溫度敏感的儲存效率" 更多效益。對於不常存取的冷資料、會壓縮較大的資料區塊。對於經常存取且更常被覆寫的熱資料、會壓縮較小的資料區塊、使程序更有效率。

  ONTAP 9.8 中引入的溫度敏感儲存效率 (TSSE) 會自動在新建立的精簡配置AFF區上啟用。它未啟用"AFF A70 、 AFF A90 和 AFF A1K 平台" ONTAP 9.15.1 中引進了使用硬體卸載處理器的功能。

  TSSE 僅在厚置備卷上不支援。

- * CPU 或專用卸載處理器儲存效率 *

  從ONTAP 9.15.1 開始，"CPU 或專用卸載處理器儲存效率"在某些AFF和FAS平台上自動啟用，無需設定。這些平台不使用對溫度敏感的儲存效率。壓縮無需等待資料冷卻即可開始，並使用主 CPU 或專用卸載處理器執行。這些平台還使用連續物理塊的順序打包來進一步提高壓縮資料的儲存效率。

您可以在日常作業中、以最少的心力實現這些技術的效益。 例如、假設您需要為 5,000 位使用者提供主目錄的儲存空間、而且您估計任何使用者所需的最大空間都是 1 GB 。您可以預先預留 5 TB 的總容量、以滿足總的潛在儲存需求。 不過、您也知道主目錄容量需求在整個組織中有很大差異。 您可以建立 2 TB 的 Aggregate 、而不是為組織保留 5 TB 的總空間。 然後、您可以使用精簡配置、將 1 GB 的儲存設備指派給每位使用者、但只能視需要分配儲存設備。 您可以在一段時間內主動監控集合、並視需要增加實際實體大小。

在另一個範例中、假設您使用的是虛擬桌面基礎架構（ VDI ）、而且虛擬桌面之間有大量的重複資料。重複資料刪除技術可自動消除 VDI 中重複的資訊區塊、並以指向原始區塊的指標取代資料區塊、進而減少儲存使用量。其他 ONTAP 儲存效率技術（例如壓縮）也可以在背景執行、無需您介入。

ONTAP 磁碟分割技術也能提供更高的儲存效率。 RAID DP 技術可防止雙磁碟故障、而不會犧牲效能或增加磁碟鏡射成本。採用 ONTAP 9 的進階 SSD 分割功能可將可用容量增加將近 20% 。

NetApp在雲端提供與本機ONTAP相同的儲存效率功能。當您將資料從本機ONTAP遷移到雲端時，現有的儲存效率得以保留。例如，假設您有一個 SQL 資料庫，其中包含您想要從本機系統移至雲端的業務關鍵資料。您可以使用NetApp控制台中的資料複製來遷移數據，並且作為遷移過程的一部分，您可以為雲端中的快照啟用最新的內部部署策略。

資源隨需配置

除了快照之外， ONTAP 還提供各種儲存效率技術。關鍵技術包括精簡配置、重複資料刪除、壓縮、FlexClone磁碟區、檔案、 和LUN。就像快照一樣，這些都是以 ONTAP 的 Write Anywhere File Layout （ WAFL ）為基礎。

精簡配置的磁碟區或 LUN 是儲存設備未預先保留的磁碟區。而是根據需要動態分配儲存設備。刪除磁碟區或LUN中的資料時、可用空間會釋出回儲存系統。

假設貴組織需要為5、000位使用者提供主目錄的儲存設備。您估計最大的主目錄會耗用1 GB的空間。

在此情況下、您可以購買5 TB的實體儲存設備。對於儲存主目錄的每個磁碟區、您都會保留足夠的空間來滿足最大消費者的需求。

但實際上、您也知道、您社群的主目錄容量需求差異極大。對於每個大型儲存設備使用者而言、只有十位使用者會耗用很少或沒有空間。

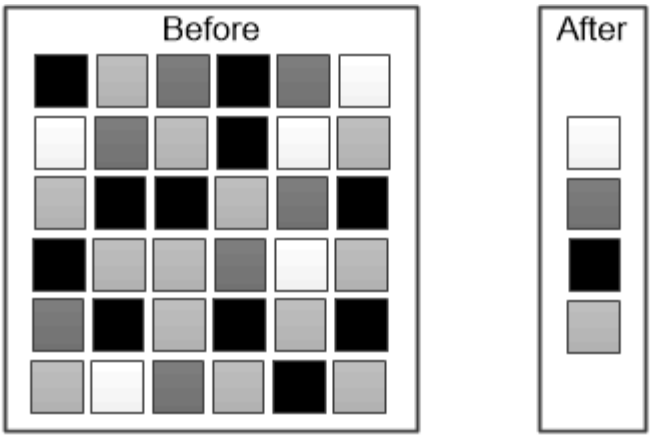
精簡配置可讓您滿足大型儲存設備使用者的需求、而無需購買從未使用過的儲存設備。由於儲存空間在使用之前不會分配，因此您可以將大小為 1 GB 的資料，指派給該集合所包含的 5 ， 000 個磁碟區中的每個，以「過度使用」 2 TB 的集合體。

只要您正確無誤、輕度與重度使用者的比例為10：1、而且只要您主動監控Aggregate上的可用空間、就能確信磁碟區寫入不會因為空間不足而失敗。

重複資料刪除

重複資料刪除 AFF 捨棄重複區塊、並以單一共用區塊的參考資料取代、藉此減少磁碟區（或是整個物件區塊中的所有磁碟區）所需的實體儲存容量。讀取已刪除重複資料通常不會收取效能費用。除了在過載節點上、寫入作業所產生的費用可忽略不計。

當資料是在正常使用期間寫入時、WAFL 使用批次程序來建立_block簽名目錄。_重複資料刪除開始後ONTAP、將會比較目錄中的簽名、以識別重複的區塊。如果存在相符項目、則會逐位元組比較、以驗證候選區塊在建立目錄後是否未變更。只有當所有位元組相符時、才會捨棄重複區塊及回收磁碟空間。



Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.

壓縮

_Compression_將資料區塊合併到_compression__群組中、以減少磁碟區所需的實體儲存容量、每個區塊都儲存為單一區塊。壓縮資料的讀取速度比傳統的壓縮方法快、因為ONTAP 只有包含所要求資料的壓縮群組才能解壓縮、而非整個檔案或LUN。

您可以單獨或組合執行內嵌或後處理壓縮：

- _Inline com壓縮_會在資料寫入磁碟之前先壓縮記憶體中的資料、大幅減少磁碟區的寫入I/O量、但可能會降低寫入效能。效能密集的作業會延後至下一次的後處理壓縮作業（如果有）。
- _postProcess com壓縮_會在資料寫入磁碟後、依照與重複資料刪除相同的排程來壓縮資料。

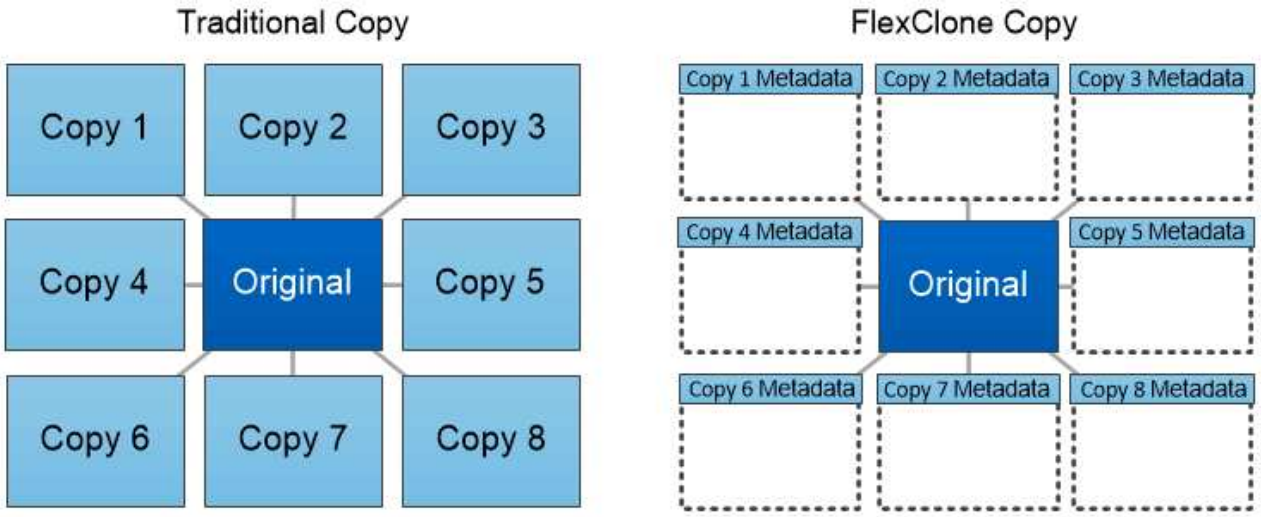
無論小型檔案或I/O是否需要4 KB的實體儲存空間、以零填充的*內嵌資料壓縮*都會儲存在4 KB區塊中。_Inline資料壓縮_將通常會耗用多個4 KB區塊的資料區塊、合併成磁碟上的單一4 KB區塊。資料仍在記憶體中時會進行壓縮、因此最適合用於速度更快的控制器。

FlexClone磁碟區、檔案和**LUN**

FlexClone 技術會參考快照中繼資料，以建立可寫入的磁碟區時間點複本。複本會與其父實體共用資料區塊、除非中繼資料需要的儲存空間、否則在複本中寫入變更之前、這些複本都不會佔用任何儲存空間。FlexClone 檔案和 FlexClone LUN 使用相同的技術，但不需要備份快照。

在傳統複本需要數分鐘甚至數小時才能建立的地方、FlexClone軟體可讓您幾乎即時複製最大的資料集。這使得它非常適合您需要多個相同資料集複本（例如虛擬桌面部署）或資料集暫存複本（針對正式作業資料集測試應用程式）的情況。

您可以複製現有的FlexClone磁碟區、複製包含LUN複製的磁碟區、或是複製鏡射與資料庫資料。您可以從其父磁碟區分割FlexClone磁碟區、在這種情況下、會將複本分配給自己的儲存設備。



FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.

瞭解 **ONTAP** 容量報告和測量

您的 ONTAP 儲存容量可以以實體空間和邏輯空間來衡量。這些測量值的報告方式取決於您的 ONTAP 版本以及您使用的是 System Manager 還是命令列介面（CLI）。了解與容量相關的各種術語、實體容量和邏輯容量之間的差異以及容量類型的報告方式，對於監控儲存使用情況至關重要。

- * 實體容量 * ：實體空間是指磁碟區或本機層所使用的實體儲存區塊。由於儲存效率功能（例如重複資料刪除和壓縮）的資料減少、實體已用容量的值通常會小於邏輯已用容量的值。
- 邏輯容量：邏輯空間是指磁碟區或本機層中的可用空間（邏輯區塊）。邏輯空間是指理論空間的使用方式、不需計算重複資料刪除或壓縮的結果。所用邏輯空間的值來自已使用的實體空間量、以及已設定的儲存效率功能（例如重複資料刪除和壓縮）所節省的成本。這項測量通常會比實體使用容量大，因為它包含快照，複本和其他元件，而且不會反映資料壓縮和實體空間的其他縮減。因此、總邏輯容量可能高於已配置空間。

CLI 中的容量報告

根據您所使用的 ONTAP 版本，ONTAP CLI 中回報的實體已用空間會有所不同。在 ONTAP 9.13.1 及更早版本中， `physical used` 參數顯示於 `volume show` 指令輸出中，包含套用於該 volume 的所有儲存效率節省。自 ONTAP 9.14.1 起， `physical used` 參數不再包含如溫度感知儲存（TSSE）、即時壓縮、壓縮整合及跨 volume 重複資料刪除等集合層級的儲存效率節省，因此無法準確反映該 volume 的實體已用空間。在 ONTAP 9.14.1 及更新版本中，您應該使用 `vol show-footprint` 指令搭配 `effective_total_footprint` 參數，以檢視 volume 的正確實體已用空間。

版本ONTAP	命令	參數	說明
9.14.1 及更高版本	`volume show-footprint`	`effective_total_footprint`	反映實際使用的磁碟空間，包括從 aggregate 節省的空間。
	`volume show-space`	`physical used`	反映磁碟區層級的儲存效率節省，包括來自 aggregate 的節省。
	`volume show`	`physical used`	不包括彙總層級的儲存效率節省，因此無法準確反映 "啟用 TSSE 的平台" 的磁碟區實體使用空間。
9.13.1 及更早版本	`volume show-footprint`	`effective_total_footprint`	反映實際使用的磁碟空間，包括從 aggregate 節省的空間。
	`volume show-space`	`physical used`	僅反映磁碟區層級儲存效率的節省。
	`volume show`	`total physical used`	僅反映磁碟區層級儲存效率的節省。

相關資訊

- 深入瞭解 "9.14.1 及更高版本實體使用空間報告的變更"。
- 深入瞭解 "用於顯示空間使用資訊的命令"。

System Manager 中的容量報告

根據 ONTAP 版本的不同，System Manager 中顯示的已用容量測量值也會有所不同。從 ONTAP 9.7 開始，System Manager 同時提供物理容量和邏輯容量的測量數據。

在System Manager中、容量表示法並不代表root儲存層（Aggregate）容量。

System Manager版本	容量使用詞彙	所指容量類型
9.9.1及更新版本	已用邏輯	使用的邏輯空間 如果已啟用儲存效率設定）
9.7和9.8	已使用	使用的邏輯空間 （如果已啟用儲存效率設定）
9.5 和 9.6 （經典檢視）	已使用	使用的實體空間

容量測量術語

以下術語用於說明容量：

- * 分配容量 * ：已分配給儲存 VM 中磁碟區的空間量。

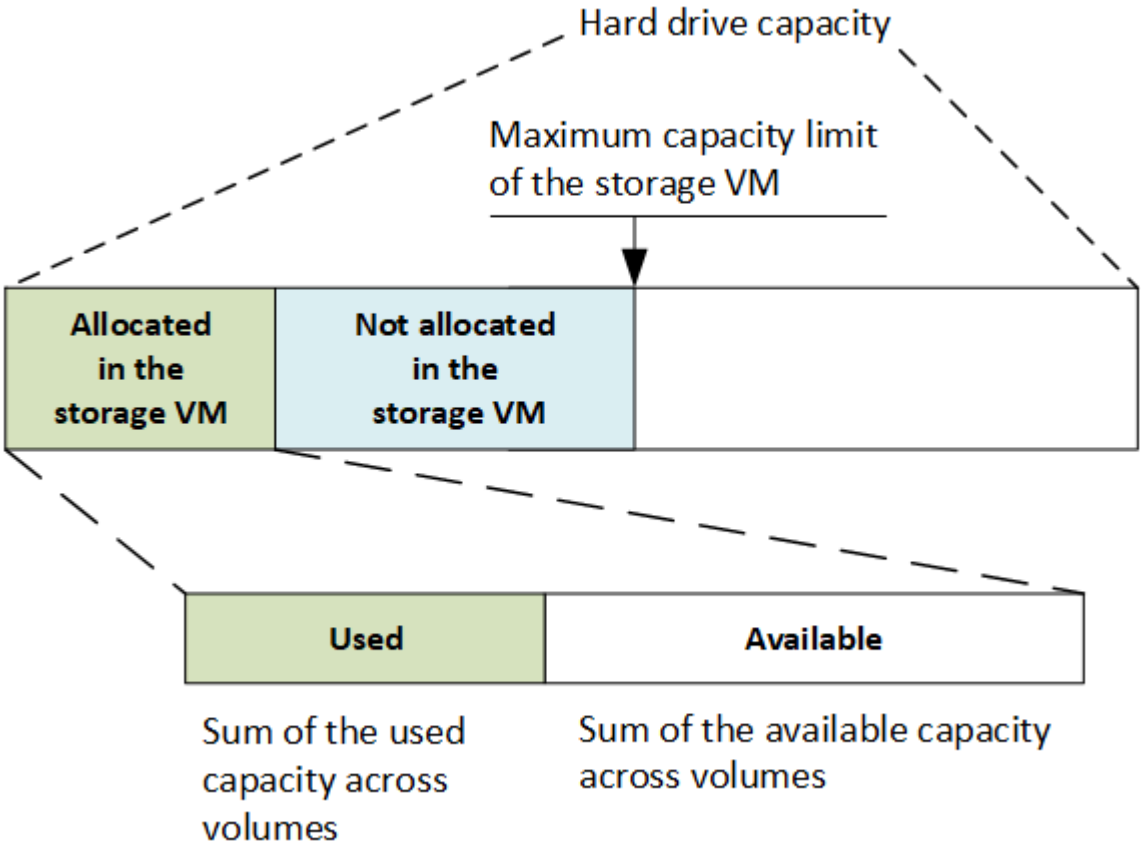
- * 可用 * ：儲存資料或在儲存 VM 或本機層中配置磁碟區的可用實體空間量。
- * 跨磁碟區容量 * ：儲存 VM 上所有磁碟區的已用儲存設備和可用儲存空間總和。
- * 用戶端資料 * ：用戶端資料（實體或邏輯）使用的空間量。
  - 從 ONTAP 9.13.1 開始，用戶端資料所使用的容量稱為 * 已使用邏輯 * ，快照所使用的容量會個別顯示。
  - 在 ONTAP 9.12.1 及更早版本中，新增至快照所使用容量的用戶端資料所使用的容量稱為 * 「已使用的邏輯容量」 * 。
- 已提交：本機層的已提交容量。
- * 資料減量 * ：擷取資料大小與儲存資料大小的比率。
  - 從 ONTAP 9 。 13.1 開始、資料減量會考量大部分儲存效率功能的結果、例如重複資料刪除和壓縮；不過、快照和自動精簡配置並不視為資料減量比率的一部分。
  - 在 ONTAP 9.12.1 及更早版本中、資料減量比率顯示如下：
    - * 容量 * 面板上顯示的資料減量值是所有邏輯使用空間與實體使用空間的整體比率，其中包括使用快照和其他儲存效率功能所帶來的效益。
    - 當您顯示詳細資料面板時，您會同時看到總覽面板上顯示的 * 整體 * 比率，以及僅由用戶端資料使用的邏輯使用空間與僅由用戶端資料使用的實體使用空間（稱為 * 不含快照和複本 * ）的比率。
- * 使用的邏輯 * ：
  - 從 ONTAP 9.13.1 開始，用戶端資料所使用的容量稱為 * 已使用邏輯 * ，快照所使用的容量會個別顯示。
  - 在 ONTAP 9.12.1 及更早版本中，新增至快照所使用容量的用戶端資料所使用的容量稱為 * 邏輯使用 * 。
- * 邏輯已用容量 %* ：目前邏輯已用容量與已配置容量的百分比，不含快照保留。此值可以大於100%、因為其中包含了Volume的效率節約效益。
- * 最大容量 * ：為儲存 VM 上的磁碟區分配的最大空間量。
- 實體已用：磁碟區或本機層實體區塊所使用的容量。
- 實體已用**%**：與已配置的容量相比、磁碟區實體區塊所使用的容量百分比。
- * 已配置容量 * ：已從 Cloud Volumes ONTAP 系統配置且已準備好儲存使用者或應用程式資料的檔案系統（ Volume ）。
- 保留：保留給本機層中已配置磁碟區的空間量。
- * 已使用 * ：包含資料的空間量。
- 已用及保留：實體已用空間與保留空間的總和。

儲存 **VM** 的容量

儲存 VM 的最大容量取決於磁碟區的總分配空間加上剩餘的未分配空間。

- Volume 的分配空間是 FlexVol Volume 、 FlexGroup Volume 和 FlexCache Volume 的已用容量和可用容量的總和。
- 磁碟區的容量會包含在總和中、即使在磁碟區受到限制、離線或刪除之後也會包含在恢復佇列中。
- 如果磁碟區設定為自動擴充、則會以總和來使用磁碟區的最大自動調整大小值。 如果沒有自動擴充、則會以總和來使用 Volume 的實際容量。

下表說明各體積容量的測量與最大容量限制之間的關係。



從 ONTAP 9.13.1 開始、叢集管理員就可以 "為儲存 VM 啟用最大容量限制"。但是、儲存 VM 若包含用於資料保護、 SnapMirror 關係或 MetroCluster 組態的磁碟區、則無法設定儲存限制。此外、配額也無法設定為超過儲存 VM 的最大容量。

設定最大容量限制後、就無法將其變更為小於目前分配容量的大小。

當儲存 VM 達到其最大容量限制時、就無法執行某些作業。System Manager 提供中後續步驟的建議 "* 洞見 * "。

System Manager 中的容量測量單位

System Manager會根據位元組為1024（2^{10}的二進位元組來計算儲存容量。

- 從 ONTAP 9.10.1 開始、儲存容量單位會在系統管理員中顯示為 KiB 、 MIB 、 GiB 、 TiB 和 PIB 。
- 在 ONTAP 9.10.0 及更早版本中、這些單位會在系統管理員中顯示為 KB 、 MB 、 GB 、 TB 及 PB 。

系統管理程式中用於處理量的單位、對於ONTAP 所有版本的不只是kb/s、MB/s、GB/s、TB/s和PB/s。

System Manager中顯示ONTAP 的容量單位、適用於更新版本的版本	System Manager中顯示的容量單位ONTAP 、適用於更新版本的NetApp	計算	以位元組為單位的值

KB	Kib	1024	1024位元組
MB	MIB	1010* 1024.	1、048、576位元組
GB	Gib	1010* 101010* 1024.	1、073、741、824位元組
TB	TIB	101010* 1010* 1024.10* 1024.7	1、099、511、627、776位元組
PB	PIB	1010* 10大於10* 10大於10大於10大於10大於10大於10大於10大於10大於	1 、 125,899,906,842,624 位元組

相關資訊

"在 System Manager 中監控叢集，階層和 SVM 容量"

"磁碟區的邏輯空間報告與強制"

了解**ONTAP**溫度敏感型儲存效率

ONTAP透過評估磁碟區資料的存取頻率並將該頻率對應到應用於該資料的壓縮程度來提供溫度敏感儲存效率 (TSSE) 優勢。對於不經常存取的冷數據，壓縮較大的數據塊；對於經常存取和覆蓋的熱數據，壓縮較小的數據塊，從而使處理更加高效。

TSSE 在ONTAP 9.8 中引入，並在新建立的精簡配置AFF磁碟區上自動啟用。您可以對現有的精簡配置AFF磁碟區和精簡配置的非AFF DP 磁碟區啟用溫度敏感儲存效率。TSSE 不支援在厚置備卷上執行。

以下平台不適用溫度敏感儲存效率：

平台	版本**ONTAP**
• AFF A1K • AFF A90 • AFF A70 • FAS90 • FAS70	9.15.1 或更新版本
• AFF C80 • AFF C60 • AFF C30 • AFF A50 • AFF A30	9.16.1 或更新版本

這些平台使用"CPU 或專用卸載處理器儲存效率"。壓縮是使用主 CPU 或專用卸載處理器執行的，並不是基於熱

數據或冷數據。

> 隨著時間的推移，與 8K 自適應壓縮相比，TSSE 佔用的捲空間量可能會更加明顯。由於 TSSE 和 8K 自適應壓縮之間的架構差異，這種行為是可以預期的。

引進「預設」和「有效率」模式

從 ONTAP 9 。 10.1 開始、 *default* 和 *Effive* 磁碟區層級的儲存效率模式僅適用於 AFF 系統。這兩種模式可選擇檔案壓縮（預設），這是建立新 AFF 磁碟區時的預設模式，或是對溫度敏感的儲存效率（效率），這兩種模式使用自動調適式壓縮技術，可在不常存取的冷資料上，提供更高的壓縮節省。

升級至 ONTAP 9.10.1 及更新版本時、會根據目前在磁碟區上啟用的壓縮類型、為現有磁碟區指派儲存效率模式。在升級期間、已啟用壓縮的磁碟區會被指派預設模式、而已啟用溫度敏感儲存效率的磁碟區則會被指派效率模式。如果未啟用壓縮、儲存效率模式會保持空白。

搭配 ONTAP 9 。 10.1 、"必須明確設定溫度敏感的儲存效率"可啟用自動調適式壓縮。不過、 AFF 平台預設會啟用其他儲存效率功能、例如資料壓縮、自動重複資料刪除排程、內嵌重複資料刪除、跨磁碟區內嵌重複資料刪除、以及跨磁碟區背景重複資料刪除、以提供預設模式和高效率模式。

啟用 FabricPool 的集合體和所有分層原則類型都支援兩種儲存效率模式（預設和有效率）。

在 **C** 系列平台上啟用對溫度敏感的儲存效率

在AFF C 系列平台上，溫度敏感儲存效率 (TSSE) 預設為啟用；當使用磁碟區移動或SnapMirror將精簡配置磁碟區從非 TSSE 平台遷移到啟用 TSSE 的 C 系列平台時，如果目標平台上安裝了以下版本，則也會啟用 TSSE：

- ONTAP 9.12.1P4 及更新版本
- ONTAP 9.13.1 及更新版本

如需更多資訊、請參閱 "Volume Move 和 SnapMirror 作業的儲存效率行為"。

對於現有的精簡配置卷，溫度敏感儲存效率不會自動啟用；但是，您可以... "修改儲存效率模式" 手動切換到高效率模式。

> 將儲存效率模式變更為「有效率」後、您就無法將其變更回來。

連續包裝實體區塊、提升儲存效率

從 ONTAP 9.13.1 開始、對溫度敏感的儲存效率可增加連續實體區塊的連續包裝、進一步改善儲存效率。當您將系統升級至 ONTAP 9.13.1 時、已啟用溫度敏感儲存效率的磁碟區會自動啟用連續封裝。啓用連續打包後"手動重新包裝現有資料"，您必須。

了解**ONTAP**專用卸載處理器的儲存效率

專用卸載處理器儲存效率執行連續實體區塊的順序打包，並使用專用卸載處理器進行 32k 資料壓縮。使用 32k 壓縮可以在聚合層級實現空間節省，這與使用 8k 自適應壓縮的平台不同，後者在磁碟區層級實現空間節省。使用專用卸載處理器儲存效率的平台不使用溫度敏感儲存效率 (TSSE)，這意味著壓縮不是基於熱資料或冷資料。這樣可以立即節省空間，而不會對性能產生任何影響。

以下平台和ONTAP版本預設啟用專用卸載處理器儲存效率。

AFF A20 平台不支援專用卸載處理器的儲存效率。對於AFF A20 平台，使用SnapMirror技術遷移的資料會使用主 CPU 自動轉換為 32k 內聯壓縮。

平台	版本**ONTAP**
• AFF A1K • AFF A90 • AFF A70 • FAS90 • FAS70	9.15.1 或更新版本
• AFF C80 • AFF C60 • AFF C30 • AFF A50 • AFF A30	9.16.1 或更新版本

對於以下平台，儲存效率會自動啟用，無需配置。這適用於所有新建立的精簡配置磁碟區和現有數據，包括從其他平台移動的磁碟區。無論空間保證設定如何，都會啟用重複資料刪除。壓縮和資料壓縮都要求將空間保證設為無。使用磁碟區移動或SnapMirror技術遷移的資料會自動轉換為 32k 內聯壓縮。

- AFF C80
- AFF C60
- AFF C30
- AFF A1K
- AFF A90
- AFF A70
- AFF A50
- AFF A30

對於下列平台，預設僅在升級至ONTAP 9.15.1 或更高版本之前已啟用儲存效率的現有精簡配置磁碟區上啟用儲存效率。您可以使用 CLI 或 REST API 方法在新建立的磁碟區上啟用儲存效率。只有在原始平台上啟用了壓縮時，使用磁碟區移動或SnapMirror技術遷移的資料才會轉換為 32k 內聯壓縮。

- FAS90
- FAS70

有關將控制器升級到受支援平台之一的信息，請參閱 "ONTAP 硬體升級文件"。

安全性

用戶端驗證與授權

使用標準方法來保護用戶端和系統管理員存取儲存設備的安全、並防止病毒入侵。ONTAP

先進的技術可用於加密閒置資料和WORM儲存設備。

利用信任的來源驗證用戶端機器和使用者的身分、藉此驗證其身分。ONTAP利用比較使用者的認證資料與檔案或目錄上設定的權限、即可授權使用者存取檔案或目錄。ONTAP

驗證

您可以建立本機或遠端使用者帳戶：

- 本機帳戶是指帳戶資訊位於儲存系統上的帳戶。
- 遠端帳戶是指帳戶資訊儲存在Active Directory網域控制器、LDAP伺服器或NIS伺服器上的帳戶。

使用本機或外部名稱服務來查詢主機名稱、使用者、群組、netgroup和名稱對應資訊。ONTAP支援下列名稱服務：ONTAP

- 本機使用者
- DNS
- 外部NIS網域
- 外部 LDAP 網域

名稱服務交換器表_指定搜尋網路資訊的來源、以及搜尋這些資訊的順序（提供UNIX系統上/etc/nsswitch.conf檔案的等效功能）。當NAS用戶端連線至SVM時ONTAP 、此功能會檢查指定的名稱服務、以取得所需的資訊。

- Kerberos support_* Kerberos是一種網路驗證傳輸協定、可在用戶端伺服器實作中加密使用者密碼、以提供「長驗證」。支援Kerberos 5驗證、具備完整性檢查（krb5i）和Kerberos 5驗證功能、可進行隱私權檢查（krb5p）ONTAP 。

授權

此功能可評估三種安全層級、以判斷實體是否有權針對位於SVM上的檔案和目錄執行要求的動作。ONTAP存取權取決於評估安全性層級後的有效權限：

- 匯出（NFS）和共用（SMB）安全性

  匯出及共用安全性適用於用戶端存取特定NFS匯出或SMB共用區。具有管理權限的使用者可以從SMB和NFS用戶端管理匯出和共用層級的安全性。

- 儲存層級的存取保護檔案和目錄安全性

  儲存層級的存取保護安全性適用於存取SVM磁碟區的SMB和NFS用戶端。僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

- NTFS、UNIX及NFSv4原生檔案層級安全性

  代表儲存物件的檔案或目錄中存在原生檔案層級安全性。您可以從用戶端設定檔案層級的安全性。無論使用SMB或NFS存取資料、檔案權限都有效。

使用 **SAML** 驗證

ONTAP 支援安全性聲明標記語言（ SAML ）、以驗證遠端使用者。支援數個常見的身分識別供應商（ IDP ）。如需支援的 IDP 及啟用 SAML 驗證指示的詳細資訊、請參閱 "設定SAML驗證"。

OAuth 2.0 搭配 **ONTAP REST API** 用戶端

開放授權（ OAuth 2.0 ）架構的支援從 ONTAP 9.14 開始提供。當用戶端使用 REST API 存取 ONTAP 時、您只能使用 OAuth 2.0 來進行授權和控制存取決策。不過、您可以使用任何 ONTAP 管理介面（包括 CLI 、系統管理員和 REST API ）來設定和啟用此功能。

標準 OAuth 2.0 功能可與數個常用的授權伺服器一起支援。您可以使用以相互 TLS 為基礎的寄件者限制存取權杖、進一步增強 ONTAP 安全性。此外還有多種授權選項可供選擇、包括獨立的範圍、以及與 ONTAP REST 角色和本機使用者定義的整合。請參閱 "ONTAP OAuth 2.0 實作總覽" 以取得更多資訊。

系統管理員驗證與**RBAC**

系統管理員使用本機或遠端登入帳戶、在叢集和SVM上自我驗證。角色型存取控制（RBAC）決定系統管理員可以存取的命令。

驗證

您可以建立本機或遠端叢集和SVM系統管理員帳戶：

- 本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。
- 遠端帳戶是指帳戶資訊儲存在Active Directory網域控制器、LDAP伺服器或NIS伺服器上的帳戶。

除了DNS、ONTAP 在驗證用戶端時、除了使用相同的名稱服務來驗證系統管理員帳戶。

RBAC

指派給系統管理員的_role_決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

掃毒

您可以在儲存系統上使用整合式防毒功能、保護資料免受病毒或其他惡意程式碼的侵害。名為 *VScann* 的還原病毒掃描、結合同級最佳的協力廠商防毒軟體與各種功能、讓您靈活控制掃描檔案的時間與時間。 ONTAP ONTAP

儲存系統會將掃描作業卸載至裝載協力廠商防毒軟體的外部伺服器。由NetApp提供且ONTAP 安裝在外部伺服器上的_《The 停止 防毒連接器（停止 防毒連接器）」、負責處理儲存系統與防毒軟體之間的通訊。

- 當用戶端透過SMB開啟、讀取、重新命名或關閉檔案時、您可以使用「存取時掃描」來檢查是否有病毒。檔案作業會暫停、直到外部伺服器報告檔案的掃描狀態為止。如果檔案已掃描完畢、ONTAP 則支援檔案操作。否則、它會要求伺服器進行掃描。

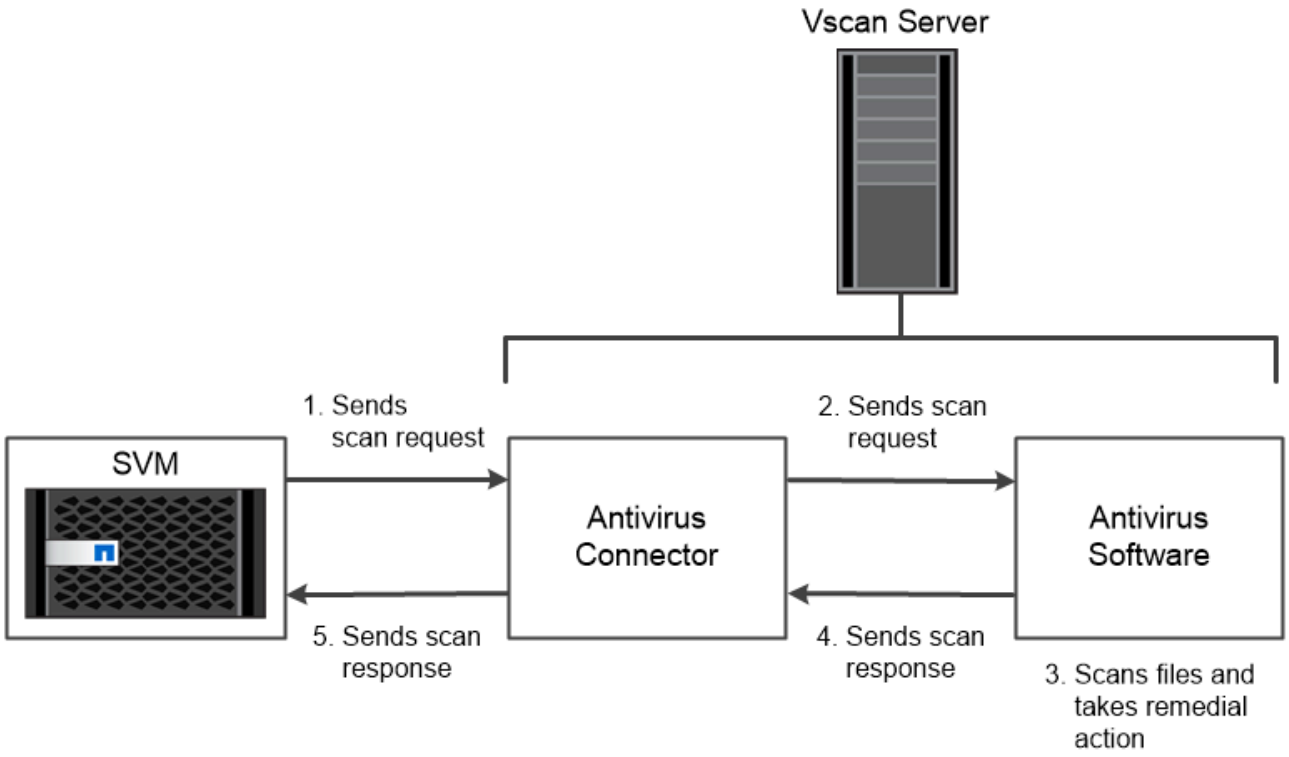
  NFS 不支援存取掃描。

- 您可以使用隨需掃描_來立即或排程檢查檔案是否有病毒。例如、您可能只想在非尖峰時間執行掃描。外部伺服器會更新已檢查檔案的掃描狀態、以便在下次透過SMB存取檔案時、這些檔案的檔案存取延遲（假設尚未修改）通常會縮短。

您可以針對SVM命名空間中的任何路徑使用隨需掃描、即使是僅透過NFS匯出的磁碟區也一樣。

您通常會在SVM上啟用這兩種掃描模式。在這兩種模式中、防毒軟體都會根據您在軟體中的設定、對受感染的檔案採取補救行動。

在災難恢復和MetroCluster 不穩定的組態中執行*病毒掃描 若要進行災難恢復和MetroCluster 還原組態、您必須為本機和合作夥伴叢集分別設定VScan伺服器。



The storage system offloads virus scanning operations to external servers hosting antivirus software from third-party vendors.

加密

支援以軟體和硬體為基礎的加密技術、可確保儲存媒體在重新調整用途、退回、放錯地方或遭竊時、無法讀取閒置的資料。ONTAP

所有SSL連線均符合聯邦資訊處理標準（FIPS）140-2。ONTAP您可以使用下列加密解決方案：

- 硬體解決方案：
  - NetApp儲存加密（NSE）

    NSE是使用自我加密磁碟機（SED）的硬體解決方案。
  - NVMe SED

    針對未獲得FIPS 140-2認證的NVMe SED、提供完整磁碟加密。ONTAP

- 軟體解決方案：
  - NetApp Aggregate Encryption（NAE）

    Nae是一種軟體解決方案、可加密任何磁碟機類型上的任何資料磁碟區、並為每個Aggregate啟用唯一金鑰。

  - NetApp Volume Encryption（NVE）

    NVE是一種軟體解決方案、可加密任何磁碟機類型的任何資料磁碟區、每個磁碟區都有一個唯一的金鑰。

同時使用軟體（NAE或NVE）和硬體（NSE或NVMe SED）加密解決方案、在閒置時實現雙重加密。儲存效率不受 NAE 或 NVE 加密影響。

NetApp儲存加密

NetApp儲存加密（NSE）支援在寫入資料時加密資料的SED。如果沒有儲存在磁碟上的加密金鑰、就無法讀取資料。而加密金鑰則只能由驗證的節點存取。

在I/O要求上、節點會使用從外部金鑰管理伺服器或Onboard Key Manager擷取的驗證金鑰、驗證自己是否為SED：

- 外部金鑰管理伺服器是儲存環境中的第三方系統、使用金鑰管理互通性傳輸協定（KMIP）為節點提供驗證金鑰。
- 內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。

NSE支援自我加密HDD和SSD。您可以將NetApp Volume Encryption與NSE搭配使用、將NSE磁碟機上的資料加倍加密。

> 如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

NVMe自我加密磁碟機

NVMe SED 不具備 FIPS 140-2 認證，但這些磁碟使用 AES 256 位元透明磁碟加密來保護靜止資料。

資料加密作業（例如產生驗證金鑰）會在內部執行。驗證金鑰是在儲存系統第一次存取磁碟時產生。之後、磁碟會在每次要求資料作業時要求儲存系統驗證、以保護閒置的資料。

NetApp Aggregate加密

NetApp Aggregate Encryption（NAE）是一項軟體技術、用於加密Aggregate上的所有資料。NAE的優點是、磁碟區包含在集合層級的重複資料刪除中、而NVE磁碟區則排除在外。

啟用NAE之後、即可使用Aggregate金鑰加密Aggregate內的磁碟區。

從 ONTAP 9 7 開始"NVE 授權"、新建立的集合體和磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。

NetApp Volume Encryption

NetApp Volume Encryption（NVE）是一項軟體技術、可一次加密閒置一個磁碟區的資料。只有儲存系統才能存取的加密金鑰可確保在基礎裝置與系統分離時、無法讀取磁碟區資料。

包括快照和中繼資料在內的資料都會加密。資料的存取權是由唯一的XTS-AES-256金鑰提供、每個磁碟區一個金鑰。內建的Onboard Key Manager可保護同一系統上的金鑰與您的資料。

您可以在任何類型的Aggregate（HDD、SSD、混合式、陣列LUN）上使用NVE、搭配任何RAID類型、也可以在ONTAP 任何支援的支援功能中使用、包括ONTAP Select 用作支援的功能、包括用作支援的功能。您也可以使用NVE搭配NetApp儲存加密（NSE）、對NSE磁碟機上的資料進行雙重加密。

*使用KMIP伺服器的時機*雖然成本較低、而且使用內建金鑰管理程式通常較為方便、但如果符合下列任一項條件、您應該設定KMIP伺服器：

- 您的加密金鑰管理解決方案必須符合聯邦資訊處理標準（FIPS）140-2或OASIS KMIP標準。
- 您需要多叢集解決方案。KMIP伺服器透過集中管理加密金鑰來支援多個叢集。

  KMIP伺服器透過集中管理加密金鑰來支援多個叢集。

- 您的企業需要更高的安全性、將驗證金鑰儲存在系統或與資料不同的位置。

  KMIP伺服器會將驗證金鑰與資料分開儲存。

相關資訊

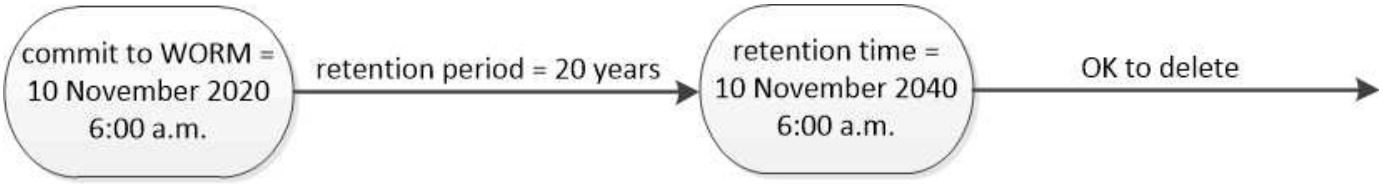
"常見問題集- NetApp Volume Encryption與NetApp Aggregate Encryption"

WORM 儲存設備

_ SnapLock 此為高效能法規遵循解決方案、適用於使用_一次寫入、多次讀取（WORM）_儲存設備、以未經修改的形式保留重要檔案、以利法規遵循與治理。

單一授權可讓您以嚴格的 _ 法規遵循模式使用 SnapLock 、 _ 以滿足如 SEC 法規 17a-4(f) 及較寬鬆 _ 企業模式等外部要求、以符合內部規定的數位資產保護法規。使用防竄改的_ComplianceClock_來判斷WORM檔案的保留期間何時結束。SnapLock

您可以在次要儲存設備上使用 SnapLock for SnapVault ，以 WORM 保護快照。您可以使用SnapMirror將WORM檔案複寫到其他地理位置、以進行災難恢復及其他用途。



SnapLock uses a tamper-proof ComplianceClock to determine when the retention period for a WORM file has elapsed.

ONTAP 和 VMware vSphere

您可以將 ONTAP 及相關 NetApp 產品與 VMware vSphere 整合。視您的技術環境和業務需求而定、有多種選項可供選擇。

選定的概念和術語

當您開始在 VMware 環境中使用 ONTAP 和相關 NetApp 產品時、首先熟悉一些關鍵術語和概念是很有幫助的。

邏輯單元編號

LUN 是用於識別儲存區域網路（ SAN ）中的邏輯單元 _ 的編號。這些可定址的裝置通常是透過小型電腦系統介面（ SCSI ）傳輸協定或其封裝衍生工具之一存取的邏輯磁碟。

VMware vSphere 虛擬 Volume

虛擬磁碟區（ vVol ）可為虛擬機器所使用的儲存設備提供磁碟區層級抽象化。它包含多項優點、可替代傳統 LUN 的使用方式。

持續保留

與以前的 SCSI-2 保留相比、 SCSI-3 支援持續保留。它們允許多個用戶端啟動器與單一目標通訊、同時鎖定其他節點。即使重設匯流排以進行錯誤恢復、保留仍會持續存在。

> 從 ONTAP 9.15.1 開始、您可以使用 SCSI-3 為虛擬磁碟區建立持續保留。此功能僅支援搭配 Windows Server 容錯移轉叢集（ WSFC ）使用適用於 VMware vSphere 9 的 ONTAP 工具。

Windows Server 容錯移轉叢集

Microsoft WSFC 是 Windows Server 作業系統的一項功能、可提供容錯能力和高可用度。一組伺服器節點（實體或虛擬）會以叢集的形式結合在一起、以在發生故障時提供恢復能力。WSFC 通常用於部署基礎架構服務、包括資料庫、檔案和命名空間伺服器。

VMware vSphere 儲存 API - 儲存感知

Vasa 是一組 API 、可將儲存陣列與 vCenter 整合以進行管理。此架構以多個元件為基礎、包括處理 VMware vSphere 與儲存系統之間通訊的 _VASA Provider] 。透過 ONTAP 、提供者將實作為 VMware vSphere ONTAP 工具的一部分。

VMware vSphere 儲存 API - 陣列整合

VAAI 是一組 API 、可在 VMware vSphere ESXi 主機和儲存裝置之間進行通訊。API 包含一組主機用來將儲存作業卸載到陣列的原始作業。VAAI 可大幅改善儲存密集工作的效能。

NetApp SnapCenter

SnapCenter 是一個集中化且可擴充的平台、可為使用 ONTAP 儲存系統的應用程式、資料庫、主機檔案系統和虛擬機器提供資料保護。它採用原生 ONTAP 技術，包括 Snapshot ， SnapRestore ， FlexClone ， SnapMirror 和 SnapVault 。

NetApp 外掛程式和相關技術

NetApp 提供強大的支援、可整合 ONTAP 及相關產品與 VMware vSphere 技術。

VMware vSphere適用的工具ONTAP

適用於 VMware vSphere 的 ONTAP 工具是一套整合 ONTAP 和 vSphere 的工具。它實作 VASA API 架構的供應商功能。ONTAP 工具也包括 vCenter 外掛程式、適用於 VMware Site Recovery Manager 的儲存複寫介面卡（ SRA ）、以及可用於建置自動化應用程式的 REST API 伺服器。

適用於VMware VAAI的NFS外掛程式

NetApp NFS 外掛程式 for VMware VAAI 可讓您存取 VAAI 功能。此外掛程式可安裝在 ESXi 主機上、並可讓主機將 VAAI 與 ONTAP 上的 NFS 資料存放區搭配使用。它提供多種作業、包括複製、空間保留和快照卸載。

VMware Site Recovery Manager

VMware Site Recovery Manager （ SRM ）提供災難恢復功能。SRM 與 ONTAP 工具整合、可讓 VMware vSphere 存取及運用 ONTAP 資料管理功能。

vSphere Metro Storage 叢集

vSphere Metro Storage Cluster （ VMSC ）是一項技術、可在延伸叢集部署中啟用和支援 vSphere 。NetApp MetroCluster 和 SnapMirror 主動同步（以前稱爲 SMBC ）支持 VMSC 解決方案。這些解決方案可在網域發生故障時、提供增強的營運持續性。恢復模式是根據您的特定組態選擇而定。

VMware vSphere的插件SnapCenter

SnapCenter Plug-in for VMware vSphere （ SCV ）是一種 Linux 型虛擬應用程式、可與 SnapCenter 伺服器一起部署、也可做為獨立應用程式部署。在這兩種情況下、選擇控制閥都能為 VM 、資料存放區和 VMDK 提供備份與還原作業。這些作業速度快、節省空間、一致當機、而且 VM 一致。

取得更多資訊

有幾種額外資源可協助您準備在 VMware vSphere 環境中部署 ONTAP 。

- "適用於 VMware vSphere 的 ONTAP 工具文件"
- "企業應用程式： VMware vSphere 搭配 ONTAP"
- "NetApp KB ：什麼是 SCSI 保留和 SCSI 持續保留？"
- "VMware vSphere文件的VMware外掛程式SnapCenter"

FabricPool

許多NetApp客戶的儲存資料量相當可觀、很少有人存取。我們稱之為_Cold資料。客戶也有經常存取的資料、我們稱之為「*hot*」資料。理想情況下、您想要將熱資料保留在最快的儲存設備上、以獲得最佳效能。只要冷資料可在需要時立即使用、就能移至較慢的儲存設備。但您如何知道資料的哪些部分是熱的、哪些是冷的？

FabricPool 是一項 ONTAP 功能，可根據存取模式，自動在高效能本端層和雲端層之間移動資料。分層可釋出昂貴的本機儲存空間來儲存熱資料、同時讓雲端中的低成本物件儲存設備隨時提供冷資料。此功能可持續監控資料存取、並在各層之間移動資料、以獲得最佳效能並實現最大的節約效益。FabricPool

使用功能將冷資料分層至雲端是獲得雲端效率並建立混合雲組態的最簡單方法之一。FabricPool由於可在儲存區塊層級運作、因此可同時處理檔案和LUN資料。FabricPool

但 FabricPool 不只是將內部部署資料分層到雲端。許多客戶使用FabricPool 支援功能的支援功能Cloud Volumes ONTAP 、將冷資料從昂貴的雲端儲存設備分層、到雲端供應商內部成本較低的物件式儲存設備。從 ONTAP 9.8 開始，您可以使用或"對溫度敏感的儲存效率"在啟用 FabricPool 的磁碟區上擷取分析資料"檔案系統分析"。

使用資料的應用程式並不知道資料是分層的、因此不需要變更應用程式。分層完全自動化、因此不需要持續管理。

您可以將冷資料儲存在主要雲端供應商之一的物件儲存設備中。或者選擇NetApp StorageGRID 解決方案、將您的冷資料保存在私有雲端、以獲得最高效能、並完全掌控您的資料。

相關資訊

"系統管理程式文件FabricPool"

"NetApp雲端分層"

"NetApp TechCommTV上的播放清單FabricPool"

ONTAP快速入門

若要開始使用 ONTAP ，您必須設定叢集，設定網路，啟用 BMC 自動網路組態，建立本機層級，設定通訊協定，以及配置儲存設備。

設定叢集

NetApp 建議您使用 System Manager 至"設定新的 ONTAP 叢集"。System Manager 提供簡單易用的叢集設定工作流程，包括指派節點管理 IP 位址和初始化叢集。

設定您的網路

通過創建"廣播網域"，"子網路"和"IP 空間"（可選）來配置您的網絡。

啟用 **BMC** 自動網路組態

"啟用 BMC 自動網路組態"，這樣就不需要手動爲每個節點的 BMC 分配 IP 地址。

建立本機層

"建立本機層"從節點中可用的磁碟或 SSD 。System Manager會根據您的硬體自動計算最佳層級組態。

設定您的通訊協定

"啟用 NAS ， SAN 或 NVMe 通訊協定"在您的叢集上。

配置您的儲存設備

配置或"SAN"組態的儲存設備"NAS"。

接下來呢？

- "獲得深入見解、協助您最佳化系統"。
- "設定 ONTAP 系統管理員驗證和角色型存取控制（ RBAC ）"定義系統管理員的功能。
- "配置ONTAP以發送重要的事件管理系統 (EMS) 通知" 這樣您就可以立即收到需要您注意的系統問題的通知。
- 瞭解如何使用 ONTAP "備份資料以進行災難恢復"與"保護您的資料免受勒索軟體攻擊"。
- "瞭解數位顧問與 AutoSupport"。
- 使用 System Manager 至"監控叢集的健全狀況"。

設定 ONTAP 叢集

ONTAP 叢集設定工作流程摘要

要設定集群，您應該收集完成設定所需的信息，建立集群並加入節點，將管理 LIF 從 IPv4 轉換為 IPv6，使用Active IQ Config Advisor檢查集群，並同步整個集群的系統時間。

此程序適用於FAS、 AFF和ASA系統。

- 如果您有 AFX 系統，請依照 "這些步驟" 設定ONTAP集群。
- 如果您有ASA r2 系統（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30、 ASA A20 或ASA C30），請遵循 "這些步驟" 設定ONTAP集群。ASA r2 系統為僅使用 SAN 的客戶提供簡化的ONTAP體驗。

1. "收集資訊"

開始叢集設定之前，請先收集完成設定程序所需的資訊。

2. "建立 **ONTAP** 叢集並加入節點"

NetApp 建議您使用系統管理員來設定新叢集。System Manager 提供簡單易用的叢集設定工作流程，包括指派節點管理 IP 位址和初始化叢集。

3. "將管理階層的生命從 **IPv4** 轉換為 **IPv6**"

從 ONTAP 9.13.1 開始，您可以使用 ONTAP 命令列介面（ CLI ），在初始叢集設定期間，將 IPv6 位址指派給 AFF A800 和 FAS 8700 平台上的管理階層。對於早於 9.13.1 的 ONTAP 版本、或是在其他平台上的 9.13.1 及更新版本、您必須先將 IPv4 位址指派給管理階層的生命負載、然後在完成叢集設定後轉換成 IPv6 位址。

4. "使用**Active IQ Config Advisor** 功能驗一下叢集"

在您將所有節點加入新叢集之後、您應該執行Active IQ Config Advisor 效益管理功能來驗證組態、並檢查常見的組態錯誤。

5 "在整個叢集之間同步化系統時間"

在叢集中同步處理系統時間，以確保叢集中的每個節點都有相同的時間，並防止 CIFS 和 Kerberos 故障。

收集資訊以設定 ONTAP 叢集

開始叢集設定之前，您應該先收集完成叢集設定所需的資訊，例如叢集管理介面連接埠和 IP 位址。請先從叢集設定工作表中收集所有相關資訊開始著手。叢集設定工作表可讓您記錄叢集設定程序所需的值。如果提供預設值、您可以使用該值、或輸入自己的值。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"設定 ONTAP 叢集。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

系統預設值

系統預設值為私有叢集網路的預設值。最好使用這些預設值。不過、如果它們不符合您的要求、您可以使用表格記錄自己的值。

對於設定為使用網路交換器的叢集、每個叢集交換器都必須使用9000 MTU大小。

資訊類型	您的價值
私有叢集網路連接埠	
叢集網路遮罩	
叢集介面 IP 位址（適用於每個節點上的每個叢集網路連接埠） 每個節點的 IP 位址必須位於相同的子網路上。	

叢集資訊

資訊類型	您的價值
叢集名稱 名稱必須以字母開頭、而且必須少於 44 個字元。名稱可以包含下列特殊字元： . - _	

功能授權金鑰

您可以在 NetApp 支援網站的「**My Support**（我的支援）> **Software Licenses**（軟體授權）」下找到初始或附加軟體訂單的授權金鑰。

資訊類型	您的價值
功能授權金鑰	

管理儲存虛擬機器（**SVM**）

資訊類型	您的價值
叢集管理員密碼 叢集在授予叢集管理員存取主控台或透過安全傳輸協定的權限之前所需的管理員帳戶密碼。 為了安全起見、不建議在此工作表中記錄密碼。 密碼的預設規則如下： • 密碼長度必須至少八個字元。 • 密碼必須包含至少一個字母和一個數字。	
叢集管理介面連接埠 連線至資料網路的實體連接埠、可讓叢集管理員管理叢集。	
叢集管理介面IP位址 叢集管理介面的獨特IPv6位址。叢集管理員使用此位址來存取管理SVM並管理叢集。通常、此位址應位於資料網路上。 您可以向負責指派組織IP位址的管理員取得此IP位址。 範例：192.0.2.66	
叢集管理介面網路遮罩（IPv4） 定義叢集管理網路上有效的IPv4位址範圍的子網路遮罩。 範例：255：255：255	
叢集管理介面網路遮罩長度（IPv6） 如果叢集管理介面使用IPv6位址、則此值代表定義叢集管理網路上有效IPv6位址範圍的字首長度。 範例： 64	

資訊類型	您的價值
叢集管理介面預設閘道 叢集管理網路上路由器的IP位址。	
DNS網域名稱 網路DNS網域的名稱。 網域名稱必須包含英數字元。若要輸入多個DNS網域名稱、請以一個逗號或空格分隔每個名稱。	
名稱伺服器IP位址 DNS名稱伺服器的IP位址。以一個逗號或空格分隔每個位址。	

節點資訊（適用於叢集中的每個節點）

資訊類型	您的價值
控制器的實體位置（選用） 控制器實體位置的說明。請使用說明來識別叢集中的此節點位置（例如「Lab 5、第7列、Rack B」）。	
節點管理介面連接埠 連接至節點管理網路的實體連接埠、並可讓叢集管理員管理節點。	
節點管理介面IP位址 管理網路上節點管理介面的唯一IPV4或IPv6位址。如果您將節點管理介面連接埠定義為資料連接埠、則此IP位址應該是資料網路上的唯一IP位址。 您可以向負責指派組織IP位址的管理員取得此IP位址。 範例：192.0.2.66	

資訊類型	您的價值
節點管理介面網路遮罩（IPv4） 定義節點管理網路上有效IP位址範圍的子網路遮罩。 如果將節點管理介面連接埠定義為資料連接埠、則網路遮罩應該是資料網路的子網路遮罩。 範例：255：255：255	
節點管理介面網路遮罩長度（IPv6） 如果節點管理介面使用IPv6位址、則此值代表定義節點管理網路上有效IPv6位址範圍的前置碼長度。 範例： 64	
節點管理介面預設閘道 節點管理網路上路由器的IP位址。	

NTP伺服器資訊

資訊類型	您的價值
NTP伺服器位址 站台上網路時間傳輸協定（NTP）伺服器的IP位址。這些伺服器可用來同步整個叢集的時間。	

建立 ONTAP 叢集並加入節點

NetApp 建議您使用系統管理員來建立新叢集。System Manager 提供簡單易用的叢集設定工作流程。只有在 MetroCluster 組態中執行 ONTAP 9.7 或更早版本，或是需要在特定平台上設定純 IPv6 叢集時，才需要使用 ONTAP 命令列介面（ CLI ）。

關於這項工作

此程序適用於 "AFF， ASA FAS" 和 "AFX 系統"。如果您擁有ASA r2 系統（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30、 ASA A20 或ASA C30），請依照下列步驟操作。 "這些步驟" 使用系統管理器設定ONTAP集群。ASA r2 系統為僅使用 SAN 的客戶提供簡化的ONTAP體驗。

從 ONTAP 9.13.1 開始，您可以使用 ONTAP CLI 在初始叢集設定期間，將 IPv6 位址指派給 AFF A800 和 FAS8700 平台上的管理階層。對於早於 ONTAP 9.13.1 的 ONTAP 版本，或是其他平台上的 ONTAP 9.13.1 及更新版本，您應該使用系統管理員來使用 IPv4 位址建立叢集，然後在完成叢集設定之後使用"轉換為 IPv6"位址。

System Manager 不支援在 ONTAP 9.6 及更早版本中需要 IPv6 網路的部署。

開始之前

- 您應該已根據平台機型的安裝與設定指示，安裝，連接新的儲存系統並開啟電源。

  請參閱"不再需要使用本技術AFF FAS"。

- "收集您需要的資訊"以完成叢集設定。
- 叢集網路介面應在叢集的每個節點上設定、以進行叢集內通訊。
- 如果您使用 CLI 來設定 IPv6 ，則應在基礎管理控制器（ BMC ）上設定 IPv6 ，以便使用 SSH 存取系統。

範例 **1.** 步驟

系統管理員

1. 指派節點管理IP位址
   - Windows 電腦
     i. 將 Windows 電腦連接至與控制器相同的子網路。

        這會自動將節點管理 IP 位址指派給您的系統。

     ii. 開啟 * 網路 * 磁碟機以探索節點。
     iii. 選取節點以啟動叢集設定精靈。
   - 非 Windows 電腦
     i. 開啟要新增至叢集的所有節點。

        這是啟用叢集設定探索所需的項目。

     ii. 連線至第一個節點的主控台。

        節點會開機、然後從主控台啟動叢集設定精靈。

```
Welcome to the cluster setup wizard....
```

   i. 認可AutoSupport 此聲明。

```
Type yes to confirm and continue {yes}: yes
```

      根據預設會啟用支援。AutoSupport

   ii. 請依照畫面上的指示，將管理 IP 位址指派給節點。
   iii. 在 Web 瀏覽器中，輸入您已設定的節點管理 IP 位址："https://node-management-IP"。

      System Manager會自動探索叢集中的其餘節點。

2. 在 * 初始化儲存系統 * 下、輸入叢集名稱和管理員密碼。
3. 在 * 網路 * 下、輸入叢集管理 IP 位址、子網路遮罩和閘道。
4. 如果您想要使用網域名稱服務來解析主機名稱、請選取 * 使用網域名稱服務（ DNS ） * 、然後輸入 DNS 伺服器資訊。
5. 如果您想要使用網路時間傳輸協定（ NTP ）在整個叢集上保持時間同步、請在 * 其他 * 下選取 * 使用時間服務（ NTP ） * 、然後輸入 NTP 伺服器資訊。
6. 選擇*提交*。

CLI ONTAP

1. 開啟要新增至叢集的所有節點。

   這是啟用叢集設定探索所需的功能。

2. 連線至第一個節點的主控台。

   節點會開機、然後從主控台啟動叢集設定精靈。

   ```
   Welcome to the cluster setup wizard....
   ```

3. 認可AutoSupport 此聲明。

   ```
   Type yes to confirm and continue {yes}: yes
   ```

   根據預設會啟用支援。AutoSupport

4. 請依照畫面上的指示，將管理 IP 位址指派給節點。

   從 ONTAP 9.13.1 開始，您可以為 A800 和 FAS8700 平台上的管理階層指派 IPv6 位址。對於早於 9.13.1 的 ONTAP 版本、或是在其他平台上的 9.13.1 及更新版本、您必須指派管理階層的 IPv4 位址、然後在完成叢集設定後轉換為 IPv6 。

5. 按* Enter鍵*繼續。

   ```
   Do you want to create a new cluster or join an existing cluster?
   {create, join}:
   ```

6. 建立新叢集：

   a. 輸入 `create`

   b. 接受系統預設值或輸入您自己的值。

   c. 完成設定後，請登入叢集，確認叢集為作用中，第一個節點正常： `cluster show`

      以下範例顯示第一個節點（cluster1-01）健全且符合參與資格的叢集：

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   cluster1-01           true    true
   ```

   +
   如有需要，您可以使用 `cluster setup`命令存取叢集設定精靈，並變更您為管理或節點 SVM 輸入的任何值。

7. 將節點加入叢集：

   您可以一次將一個節點加入叢集。您必須完成每個節點的連接作業，而且節點必須是叢集的一部分，才能開始加入下一個節點。

   如果您的 FAS2720 具有 24 個或更少的 NL-SAS 磁碟機，則應確認儲存組態預設值設定為主動 / 被動，以最佳化效能。如需詳細資訊，請參閱的文件 "在使用根資料分割的節點上設定主動被動式組態"。

   a. 登入您打算加入叢集的節點。

      叢集設定精靈會在主控台上啟動。

      ```
      Welcome to the cluster setup wizard....
      ```

   b. 認可AutoSupport 此聲明。

      根據預設會啟用支援。AutoSupport

      ```
      Type yes to confirm and continue {yes}: yes
      ```

   c. 請依照畫面上的指示、將IP位址指派給節點。

      從 ONTAP 9.13.1 開始，您可以為 A800 和 FAS8700 平台上的管理階層指派 IPv6 位址。對於早於 9.13.1 的 ONTAP 版本、或是在其他平台上的 9.13.1 及更新版本、您必須指派管理階層的 IPv4 位址、然後在完成叢集設定後轉換為 IPv6 。

   d. 按* Enter鍵*繼續。

      ```
      Do you want to create a new cluster or join an existing cluster?
      {create, join}:
      ```

   e. 輸入 `join`

   f. 依照畫面上的指示設定節點、並將其加入叢集。

   g. 完成設定後，請確認節點狀況良好且符合參加叢集的資格： `cluster show`

      以下範例顯示第二個節點（cluster1-02）加入叢集之後的叢集：

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
cluster1-01           true    true
cluster1-02           true    true
```

8. 重複步驟 7 以加入其餘的每個節點。

下一步

- 如有需要、 "從 IPv4 轉換為 IPv6"。
- "執行 Active IQ Config Advisor 來驗證您的組態，並檢查常見的組態錯誤"。

或者，也可以將 ONTAP 管理階層的生命從 IPv4 轉換為 IPv6

從 ONTAP 9.13.1 開始，您可以使用 ONTAP 命令列介面（ CLI ），在初始叢集設定期間，將 IPv6 位址指派給 AFF A800 和 FAS 8700 平台上的管理階層。對於早於 9.13.1 的 ONTAP 版本、或是在其他平台上的 9.13.1 及更新版本、您必須先將 IPv4 位址指派給管理階層的生命負載、然後在完成叢集設定後轉換成 IPv6 位址。

如果您在使用 DHCP 完成硬體設定後，以自動指派的 IP 位址啟動 System Manager ，並使用 Windows 探索功能，則 System Manager 可以設定 IPv6 管理位址。

步驟

1. 為叢集啟用 IPv6 ：

```
network options ipv6 modify -enable true
```

2. 將權限設為進階：

```
set priv advanced
```

3. 檢視在各種介面上學習到的 RA 前置詞清單：

```
network ndp prefix show
```

4. 建立 IPv6 管理 LIF ：

使用格式 `prefix::id` 在位址參數中、手動建構 IPv6 位址。

```
network interface create -vserver <svm_name> -lif <LIF> -home-node
<home_node> -home-port <home_port> -address <IPv6prefix::id> -netmask
-length <netmask_length> -failover-policy <policy> -service-policy
<service_policy> -auto-revert true
```

5. 確認LIF已建立：

```
network interface show
```

6. 確認已設定的IP位址可連線：

```
network ping6
```

7. 將 IPv4 LIF 標記為管理性關閉：

```
network interface modify -vserver <svm_name> -lif <lif_name> -status
-admin down
```

8. 刪除 IPv4 管理 LIF ：

```
network interface delete -vserver <svm_name> -lif <lif_name>
```

9. 確認刪除了 IPv4 管理 LIF ：

```
network interface show
```

相關資訊

- "網路介面"
- "顯示網路NDP前置詞"
- "網路選項IPv6修改"

使用數位顧問 **Config Advisor** 檢查您的 **ONTAP** 叢集

在您將所有節點加入新叢集之後、您應該執行Active IQ Config Advisor 效益管理功能來驗證組態、並檢查常見的組態錯誤。

支援以網路為基礎的應用程式、可安裝在筆記型電腦、虛擬機器或伺服器上、並可在Windows、Linux和Mac平台上運作。Config Advisor

執行一系列命令來驗證安裝、並檢查組態的整體健全狀況、包括叢集和儲存交換器。Config Advisor

1. 下載並安裝Active IQ Config Advisor 此功能。

   "Active IQ Config Advisor"

2. 啟動 Digital Advisor 、並在出現提示時設定密碼。
3. 檢閱您的設定、然後按一下*「Save（儲存）」*。

4. 在* Objectives 頁面上、按一下 ONTAP 《更新部署後驗證》。
5. 選擇「引導」或「專家」模式。

   如果您選擇引導模式、會自動探索連接的交換器。

6. 輸入叢集認證資料。
7. （選用）按一下*表單驗證*。
8. 若要開始收集資料、請按一下*儲存並評估*。
9. 資料收集完成後、在*工作監控>動作*下、按一下*資料檢視*圖示來檢視收集的資料、然後按一下*結果*圖示來檢視結果。
10. 解決Config Advisor 由解決所識別的問題。

在 ONTAP 叢集上同步處理系統時間

同步時間可確保叢集中的每個節點都有相同的時間、並防止CIFS和Kerberos故障。

您的站台應設定網路時間傳輸協定（NTP）伺服器。從功能完善的9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。如需詳細資訊，請參閱的文件 "管理叢集時間（僅限叢集管理員）"。

您可以將叢集與一或多個NTP伺服器建立關聯、以同步整個叢集的時間。

1. 確認每個節點的系統時間和時區設定正確：

   ```
   cluster date show
   ```

   叢集中的所有節點都應設定為相同的時區。

   此範例顯示叢集中每個節點的日期和時區。

   ```
   cluster1::> cluster date show
   Node         Date                Time zone
   ------------ ------------------- -----------------
   cluster1-01  01/06/2015 09:35:15 America/New_York
   cluster1-02  01/06/2015 09:35:15 America/New_York
   cluster1-03  01/06/2015 09:35:15 America/New_York
   cluster1-04  01/06/2015 09:35:15 America/New_York
   4 entries were displayed.
   ```

2. 變更所有節點的日期或時區：

   ```
   cluster date modify
   ```

   此範例將叢集的時區變更為GMT:

```
cluster1::> cluster date modify -timezone GMT
```

3. 將叢集與 NTP 伺服器建立關聯：

   若要設定不使用對稱驗證的 NTP 伺服器、請輸入下列命令：

   ```
   cluster time-service ntp server create -server <server_name>
   ```

   若要使用對稱驗證設定 NTP 伺服器、請輸入下列命令：

   ```
   cluster time-service ntp server create -server <server_ip_address> -key
   -id <key_id>
   ```

   對稱驗證從 ONTAP 9.5 開始提供。不適用於ONTAP 更新版本的版本。

   此範例假設已為叢集設定DNS。如果您尚未設定DNS、則必須指定NTP伺服器的IP位址：

   ```
   cluster1::> cluster time-service ntp server create -server
   ntp1.example.com
   ```

4. 確認叢集與 NTP 伺服器相關聯：

   ```
   cluster time-service ntp server show
   ```

   此範例顯示叢集與 NTP 伺服器 ntp1.example.com 相關聯。

   ```
   cluster1::> cluster time-service ntp server show
   Server               Version
   -------------------- -----------
   ntp1.example.com     auto
   ```

用於管理**NTP**伺服器上對稱驗證的命令

從推出支援的版本號為《支援網路時間傳輸協定》（NTP）第3版。ONTAPNTPv3包含使用SHA-1金鑰的對稱驗證、可提高網路安全性。

若要這麼做...	使用此命令...
設定NTP伺服器而不進行對稱驗證	`cluster time-service ntp server create -server server_name`
設定採用對稱驗證的NTP伺服器	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
為現有的NTP伺服器啟用對稱驗證 您可以修改現有的NTP伺服器、藉由新增必要的金鑰ID來啟用驗證。	`cluster time-service ntp server modify -server server_name -key-id key_id`
設定共用的NTP金鑰	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` *附註：*共享金鑰是由ID所指。節點和NTP伺服器上的ID、其類型和值必須相同
使用未知的金鑰ID設定NTP伺服器	`cluster time-service ntp server create -server server_name -key-id key_id`
在NTP伺服器上設定未設定金鑰ID的伺服器。	`cluster time-service ntp server create -server server_name -key-id key_id` *附註：*金鑰ID、類型和值必須與NTP伺服器上設定的金鑰ID、類型和值相同。
停用對稱驗證	`cluster time-service ntp server modify -server server_name -authentication disabled`

相關資訊

- "系統管理"
- "叢集時間服務 NTP"

升級及還原 ONTAP 軟體與韌體

升級ONTAP

瞭解 ONTAP 升級

當您升級 ONTAP 軟體時、您可以利用新的增強 ONTAP 功能、協助您降低成本、加速關鍵工作負載、改善安全性、並擴大組織可用的資料保護範圍。

重大 ONTAP 升級包括從較低的 ONTAP 編號版本移至較高的版本。例如、將叢集從 ONTAP 9.8 升級至 ONTAP 9.12.1 。次要（或修補程式）升級包括從較低的 ONTAP 版本移至相同編號版本中較高的 ONTAP 版本。例如、將叢集從 ONTAP 9.12.1P1 升級至 9.12.1P4 。

若要開始升級，您應該做好升級準備。如果您有 Active IQ 數位顧問（也稱為數位顧問）的有效 SupportEdge 合約、您應該"準備使用 Upgrade Advisor 升級"。升級顧問提供的智慧功能可協助您評估叢集並建立專屬組態的升級計畫、以將不確定性和風險降至最低。如果您沒有適用於 Active IQ 數位顧問的有效 SupportEdge 合約"準備升級而不使用 Upgrade Advisor"，您應該。

準備升級之後，建議您使用執行升級"從 System Manager 自動進行不中斷升級（ andu ）"。ANDU 利用 ONTAP 的高可用度（ HA ）容錯移轉技術，確保叢集在升級期間能持續提供資料，而不會中斷。

> 從ONTAP 9.12.1 開始，系統管理器與NetApp控制台完全整合。如果您的系統上配置了控制台，您可以透過系統頁面進行升級。

如果您需要升級 ONTAP 軟體的協助、 NetApp 專業服務提供 "託管升級服務"。如果您有興趣使用此服務、請聯絡您的 NetApp 銷售代表或 "提交 NetApp 的銷售查詢表"。託管升級服務以及其他類型的升級支援、均提供給客戶 "SupportEdge Expert 服務" 無需額外成本。

相關資訊

- "支援的升級途徑"

我應該何時升級 ONTAP ？

您應該定期升級 ONTAP 軟體。升級 ONTAP 可讓您充分利用新增和增強的功能、並針對已知問題實作目前的修正。

重大 ONTAP 升級

主要的 ONTAP 升級或功能版本通常包括：

- 全新 ONTAP 功能
- 關鍵基礎架構變更、例如 NetApp WAFL 作業或 RAID 作業的基本變更
- 支援 NetApp 設計的新硬體系統
- 支援更換硬體元件、例如較新的網路介面卡或主機匯流排介面卡

全新 ONTAP 版本享有 3 年完整支援。NetApp 建議您在一般供應（ GA ）之後、執行最新版本一年、然後在完整支援期間內使用剩餘時間來規劃如何移轉至較新的 ONTAP 版本。

ONTAP 修補程式升級

修補程式升級可及時修正關鍵錯誤、而這些錯誤無法等待下一次重大的 ONTAP 功能版本發佈。非關鍵修補程式升級應每 3 至 6 個月套用一次。應盡快套用重要的修補程式升級。

深入瞭解 "建議的最低修補程式層級" 適用於 ONTAP 版本。

ONTAP 發行日期

從 ONTAP 9.8 版本開始、 NetApp 每個日曆年度提供 ONTAP 版本兩次。雖然計畫可能會有所變更、但其目的是在每個日曆年度的第二季和第四季推出新的 ONTAP 版本。使用此資訊規劃升級的時間範圍、以充分利用最新的 ONTAP 版本。

版本	發行日期
9.18.1	2025年11月
9.17.1	2025年9月
9.16.1.	2025 年 1 月
9.15.1..	2024 年 7 月
9.14.1.	2024 年 1 月
9.13.1.12.9.12.9.	2023 年 6 月
9.12.1	2023 年 2 月
9.11.1.	2022 年 7 月
9.10.1	2022 年 1 月
9.9.1	2021 年 6 月

ONTAP 支援層級

特定 ONTAP 版本可用的支援層級會因軟體發行時間而異。

支援層級	完全支援			有限支援		自助服務支援		
年	1.	2.	3.	4.	5.	6.	7.	8.
存取線上文件	是的	是的	是的	是的	是的	是的	是的	是的
技術支援	是的	是的	是的	是的	是的			

支援層級	完全支援			有限支援		自助服務支援		
根本原因分析	是的	是的	是的	是的	是的			
軟體下載	是的	是的	是的	是的	是的			
服務更新（修補程式版本 [P-版本] ）	是的	是的	是的					
有關弱點的警示	是的	是的	是的					

相關資訊

- 瞭解 "目前支援的 ONTAP 版本有哪些新功能"。
- 深入瞭解 "建議的最低 ONTAP 版本"。
- 深入瞭解 "ONTAP 軟體版本支援"。
- 深入瞭解 "ONTAP 版本模式"。

在計畫性升級之前執行 **ONTAP** 自動升級前檢查

您不需要升級 ONTAP 軟體、就能執行 ONTAP 自動升級預先檢查。 獨立於 ONTAP 自動升級程序執行升級前檢查、可讓您查看哪些檢查是針對叢集執行、並在您開始實際升級之前、提供任何應更正的錯誤或警告清單。 例如、假設您預期在排定於兩週內進行的維護期間內升級 ONTAP 軟體。 在等待排程日期時、您可以執行自動升級預先檢查、並在維護期間之前採取任何必要的修正行動。 這將在您開始升級後、降低發生非預期組態錯誤的風險。

如果您已準備好開始 ONTAP 軟體升級、則不需要執行此程序。 您應該遵循 "自動化升級程序"，包括執行自動升級預先檢查。

對於 MetroCluster 組態、您應該先在叢集 A 上執行這些步驟、然後在叢集 B 上執行相同的步驟

開始之前

您應該 "下載目標 ONTAP 軟體映像"。

若要執行的自動升級預先檢查"直接多跳升級"、您只需下載目標 ONTAP 版本的軟體套件。在您開始實際升級之前、您不需要載入中繼 ONTAP 版本。例如、如果您要執行自動升級前檢查、以從 9.7 升級至 9.11.1 、則需要下載 ONTAP 9.11.1 的軟體套件。您不需要下載 ONTAP 9.8.1 的軟體套件。

範例 **2.** 步驟

系統管理員

1. 驗證 ONTAP 目標映像：

   如果您要升級 MetroCluster 組態、您應該驗證叢集 A 、然後在叢集 B 上重複驗證程序

   a. 視您執行的版本而定ONTAP 、請執行下列其中一個步驟：

如果您正在執行…	執行此動作…
部分9.8或更新版本ONTAP	按一下*叢集>總覽*。
S69.5、9.6及9.7 ONTAP	按一下*組態*>*叢集*>*更新*。
更新版本ONTAP	按一下「組態>*叢集更新*」。

   b. 在 **Overview** （總覽）窗格的右角，單擊 ⋮。

   c. 按一下* ONTAP 《更新*》。

   d. 在 * 叢集更新 * 索引標籤中、新增映像或選取可用的映像。

如果您想要…	然後…
從本機資料夾新增新的軟體映像。 您應該已經擁有了 "已下載映像" 至本機用戶端。	i. 在 * 可用的軟體映像 * 下、按一下 * 從本機 * 新增。 ii. 瀏覽至儲存軟體映像的位置、選取映像、然後按一下*「Open*（開啟*）」。
從 HTTP 或 FTP 伺服器新增軟體映像	i. 按一下「從伺服器新增」。 ii. 在 * 新增軟體映像 * 對話方塊中、輸入您從 NetApp 支援網站 下載 ONTAP 軟體映像的 HTTP 或 FTP 伺服器 URL 。 對於匿名FTP、您必須在中指定URL ftp://anonymous@ftpserver 格式。 iii. 按一下「 * 新增 * 」。
選取可用的映像	選擇所列的其中一個影像。

   e. 按一下 * 驗證 * 以執行升級前驗證檢查。

   如果在驗證期間發現任何錯誤或警告、則會顯示這些錯誤或警告、並附上修正動作清單。您必須先解決所有錯誤、才能繼續升級。 最佳做法是也解決警告。

CLI

1. 將目標 ONTAP 軟體映像載入叢集套件儲存庫：

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.15.1/image.tgz

Package download completed.
Package processing completed.
```

2. 驗證叢集套件儲存庫中是否有可用的軟體套件：

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.15.1              MM/DD/YYYY 10:32:15
```

3. 執行自動升級前檢查：

```
cluster image validate -version <package_version_number> -show
-validation-details true
```

```
cluster1::> cluster image validate -version 9.15.1 -show-validation
-details true

It can take several minutes to complete validation...
Validation checks started successfully.  Run the "cluster image
show-update-progress" command to check validation status.
```

4. 檢查驗證狀態：

```
cluster image show-update-progress
```

如果 * 狀態 * 為「進行中」、請等待並再次執行命令、直到完成為止。

```
cluster1::*> cluster image show-update-progress

Update Phase         Status                    Duration
Duration
-------------------- ----------------- ---------------
---------------
Pre-update checks    completed                 00:10:00
00:01:03

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
...
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
Overall Status       Warning           Warning
75 entries were displayed.
```

系統會顯示完整的自動升級預先檢查清單、以及在您開始升級程序之前應解決的任何錯誤或警告。

輸出範例

升級預先檢查的完整輸出範例

```
cluster1::*> cluster image validate -version 9.14.1 -show-validation
-details true
It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed successfully.
Refer to the Upgrade Advisor Plan or the "What should I verify before I
upgrade with or without Upgrade Advisor" section in the "Upgrade ONTAP"
documentation for the remaining manual validation checks that need to
be performed before update.
Upgrade ONTAP documentation available at: https://docs.netapp.com/us-
en/ontap/upgrade/index.html
The list of checks are available at: https://docs.netapp.com/us-
en/ontap/upgrade/task_what_to_check_before_upgrade.html
Failing to do so can result in an update failure or an I/O disruption.
Use the Interoperability Matrix Tool (IMT
http://mysupport.netapp.com/matrix) to verify host system
supportability configuration information.

Validation checks started successfully.  Run the "cluster image show-
update-progress" command to check validation status.


fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    in-progress              00:10:00        00:00:42

Details:

Pre-update Check     Status            Error-Action
-------------------- -----------------
--------------------------------------

fas2820-2n-wic-1::*> cluster image show-update-progress

                                          Estimated         Elapsed
Update Phase         Status                Duration        Duration
-------------------- ----------------- --------------- ---------------
Pre-update checks    completed                00:10:00        00:01:03
```

```
Details:

Pre-update Check     Status            Error-Action
-------------------- ----------------
--------------------------------------
AMPQ Router and      OK                N/A
Broker Config
Cleanup
Aggregate online     OK                N/A
status and parity
check
Aggregate plex       OK                N/A
resync status check
Application          OK                N/A
Provisioning Cleanup
Autoboot Bootargs    OK                N/A
Status
Backend              OK                N/A
Configuration Status
Boot Menu Status     Warning           Warning: bootarg.init.bootmenu
is
                                       enabled on nodes: fas2820-wic-
1a,
                                       fas2820-wic-1b. The boot process
of
                                       the nodes will be delayed.
                                       Action: Set the
bootarg.init.bootmenu
                                       bootarg to false before
proceeding
                                       with the upgrade.
Broadcast Domain     OK                N/A
availability and
uniqueness for HA
pair status
CIFS compatibility   OK                N/A
status check
CLAM quorum online   OK                N/A
status check
CPU Utilization      OK                N/A
Status
Capacity licenses    OK                N/A
install status check
Check For SP/BMC     OK                N/A
Connectivity To
Nodes
```

```
Check LDAP fastbind  OK              N/A
users using
unsecure connection.
Check for unsecure   OK              N/A
kex algorithm
configurations.
Check for unsecure   OK              N/A
mac configurations.
Cloud keymanager     OK              N/A
connectivity check
Cluster health and   OK              N/A
eligibility status
Cluster quorum       OK              N/A
status check
Cluster/management   OK              N/A
switch check
Compatible New       OK              N/A
Image Check
Current system       OK              N/A
version check if it
is susceptible to
possible outage
during NDU
Data ONTAP Version   OK              N/A
and Previous
Upgrade Status
Data aggregates HA   OK              N/A
policy check
Disk status check    OK              N/A
for failed, broken
or non-compatibility
Duplicate Initiator  OK              N/A
Check
Encryption key       OK              N/A
migration status
check
External             OK              N/A
key-manager with
legacy KMIP client
check
External keymanager  OK              N/A
key server status
check
Fabricpool Object    OK              N/A
Store Availability
High Availability    OK              N/A
```

```
configuration
status check
Infinite Volume      OK               N/A
availibility check
LIF failover         OK               N/A
capability status
check
LIF health check     OK               N/A
LIF load balancing   OK               N/A
status check
LIFs is on home      OK               N/A
node status
Logically over       OK               N/A
allocated DP
volumes check
MetroCluster         OK               N/A
configuration
status check for
compatibility
Minimum number of    OK               N/A
aggregate disks
check
NAE Aggregate and    OK               N/A
NVE Volume
Encryption Check
NDMP sessions check  OK               N/A
NFS mounts status    Warning          Warning: This cluster is serving
NFS
check                                 clients. If NFS soft mounts are
used,
                                      there is a possibility of
frequent
                                      NFS timeouts and race conditions
that
                                      can lead to data corruption
during
                                      the upgrade.
                                      Action: Use NFS hard mounts, if
                                      possible. To list Vservers
running
                                      NFS, run the following command:
                                      vserver nfs show
Name Service         OK               N/A
Configuration DNS
Check
Name Service         OK               N/A
```

```
Configuration LDAP
Check
Node to SP/BMC       OK                N/A
connectivity check
OKM/KMIP enabled     OK                N/A
systems - Missing
keys check
ONTAP API to REST    Warning           Warning: NetApp ONTAP API has
been
transition warning                     used on this cluster for ONTAP
data
                                       storage management within the
last 30
                                       days. NetApp ONTAP API is
approaching
                                       end of availability.
                                       Action: Transition your
automation
                                       tools from ONTAP API to ONTAP
REST
                                       API. For more details, refer to
                                       CPC-00410 - End of availability:
                                       ONTAPI

https://mysupport.netapp.com/info/
                                       communications/ECMLP2880232.html
ONTAP Image          OK                N/A
Capability Status
OpenSSL 3.0.x        OK                N/A
upgrade validation
check
Openssh 7.2 upgrade  OK                N/A
validation check
Platform Health      OK                N/A
Monitor check
Pre-Update           OK                N/A
Configuration
Verification
RDB Replica Health   OK                N/A
Check
Replicated database  OK                N/A
schema consistency
check
Running Jobs Status  OK                N/A
SAN LIF association  OK                N/A
status check
```

```
SAN compatibility    OK                N/A
for manual
configurability
check
SAN kernel agent     OK                N/A
status check
Secure Purge         OK                N/A
operation Check
Shelves and Sensors  OK                N/A
check
SnapLock Version     OK                N/A
Check
SnapMirror           OK                N/A
Synchronous
relationship status
check
SnapMirror           OK                N/A
compatibility
status check
Supported platform   OK                N/A
check
Target ONTAP         OK                N/A
release support for
FiberBridge 6500N
check
Upgrade Version      OK                N/A
Compatibility Status
Verify all bgp       OK                N/A
peer-groups are in
the up state
Verify if a cluster  OK                N/A
management LIF
exists
Verify that e0M is   OK                N/A
home to no LIFs
with high speed
services.
Volume Conversion    OK                N/A
In Progress Check
Volume move          OK                N/A
progress status
check
Volume online        OK                N/A
status check
iSCSI target portal  OK                N/A
groups status check
```

```
Overall Status       Warning           Warning
75 entries were displayed.
```

準備 ONTAP 升級

判斷 ONTAP 升級所需的時間

您應該規劃至少 30 分鐘來完成 ONTAP 升級的準備步驟、 60 分鐘來升級每個 HA 配對、至少 30 分鐘來完成升級後的步驟。

> 如果您使用NetApp加密搭配外部金鑰管理伺服器和金鑰管理互通性傳輸協定（KMIP）、則每個HA配對的升級時間應超過一小時。

這些升級持續時間準則是根據一般組態和工作負載而定。您可以使用這些準則來預估在環境中執行不中斷升級所需的時間。升級程序的實際持續時間取決於您的個別環境和節點數量。

使用升級建議程式準備 ONTAP 升級

如果您有的有效"部門服務SupportEdge"合約"數位顧問"、建議您使用 Upgrade Advisor 來產生升級計畫。

Digital Advisor 的 Upgrade Advisor 服務提供智慧功能、協助您規劃升級、並將不確定性和風險降至最低。

數位顧問可識別環境中的問題、這些問題可透過升級至較新版本的 ONTAP 來解決。Upgrade Advisor服務可協助您規劃成功升級、並提供升級ONTAP 時可能需要注意的問題報告。

> 升級建議程式需要 AutoSupport 記錄才能建立報告。如果您已啟用 AutoSupport ，升級建議程式就能存取記錄檔，並能成功建立報告。如果您尚未啟用 AutoSupport ，您可以 "手動上傳 AutoSupport 檔案"。

如果您沒有適用於 Digital Advisor 的 Active Support Edge Services 合約"準備升級、無需升級顧問"、您應該。

步驟

1. "啟動 Active IQ 數位顧問"
2. 在 Digital Advisor 中"檢視與叢集相關的任何風險、並手動採取修正行動"。

   執行 ONTAP 升級之前、 * 軟體組態變更 * 、 * 硬體組態變更 * 和 * 硬體更換 * 類別所包含的風險必須先解決。

3. 檢閱建議的升級路徑和 "產生您的升級計畫"。

下一步

- 您應該檢閱 "發行說明ONTAP" 對於 Upgrade Advisor 建議用於叢集的目標 ONTAP 版本、您應該遵循 Upgrade Advisor 所產生的計畫來升級叢集。
- 您應該 "重新啟動 SP 或 BMC" 升級開始之前。

準備升級而不使用 **Upgrade Advisor**

準備進行 **ONTAP** 軟體升級、而不使用升級顧問

正確準備 ONTAP 軟體升級、有助於您在開始升級程序之前、識別並減輕潛在的升級風險或封鎖程式。在升級準備期間、您也可以找出升級前可能需要考量的任何特殊考量事項。例如、如果您的叢集已啟用 SSL FIPS 模式、且系統管理員帳戶使用 SSH 公開金鑰進行驗證、則您必須驗證目標 ONTAP 版本是否支援主機金鑰演算法。

如果您有的 SupportEdge 有效合約"數位顧問"、"使用 Upgrade Advisor 規劃升級"。如果您無法存取 Active IQ 數位顧問（也稱為數位顧問）、則應執行下列步驟以準備 ONTAP 升級。

1. "選擇您的目標 ONTAP 版本"。
2. 請參閱目標版本中的 _ 升級注意事項 _ 和 _ 已知問題和限制 _ 章節"發行說明ONTAP"。

   _ 升級注意事項 _ 說明您在升級前應注意的潛在問題。_ 已知的問題和限制 _ 說明您在升級後可能會遇到的潛在非預期系統行為。

   您必須使用 NetApp 帳戶登入、或建立帳戶才能存取版本資訊。

3. "確認 ONTAP 支援您的硬體組態"。

   您的硬體平台、叢集管理交換器和 MetroCluster IP 交換器必須支援目標版本。 如果您的叢集是針對 SAN 進行設定、則必須完全支援 SAN 組態。

4. "使用 Active IQ Config Advisor 驗證您沒有常見的組態錯誤。"
5. 檢閱支援的 ONTAP "升級途徑" 判斷您是否可以執行直接升級、或是否需要分階段完成升級。
6. "驗證 LIF 容錯移轉組態"。

   在執行升級之前、您需要確認叢集的容錯移轉原則和容錯移轉群組已正確設定。

7. "驗證 SVM 路由組態"。
8. "驗證特殊考量" 適用於您的叢集。

   如果叢集上有特定組態、則在開始 ONTAP 軟體升級之前、您需要採取特定行動。

9. "重新啟動 SP 或 BMC"。

選擇 **NetApp** 建議的目標 **ONTAP** 版本進行升級

當您使用 Upgrade Advisor 為叢集產生升級計畫時、該計畫會包含建議的目標 ONTAP 版本以供升級。 Upgrade Advisor 提供的建議是根據您目前的組態和目前的 ONTAP 版本而定。

如果您不使用升級建議程式來規劃升級、則應根據 NetApp 建議選擇目標 ONTAP 版本進行升級、或是您必須達到最低版本、才能滿足您的效能需求。

- 升級至最新的可用版本（建議）

  NetApp 建議您將 ONTAP 軟體升級至最新版本編號 ONTAP 的最新修補程式版本。 如果由於叢集中的儲存

系統不支援最新的編號版本、因此無法執行此動作、您應該升級至支援的最新編號版本。

- 建議的最低版本

  如果您想要將升級限制在叢集的建議最低版本、請參閱 "建議的最低 ONTAP 版本" 若要判斷您應該升級至的 ONTAP 版本。

確認您的硬體組態是否支援 **ONTAP** 目標版本

在升級 ONTAP 之前、您應該確認硬體組態可以支援目標 ONTAP 版本。

所有組態

用於 "NetApp Hardware Universe"確認目標 ONTAP 版本支援您的硬體平台、叢集和管理交換器。

您可以升級的 ONTAP 版本可能會受到硬體組態的限制。如果您的硬體不支援您要升級的 ONTAP 軟體版本、您必須先將新節點新增至叢集、移轉資料、移除舊節點、然後升級 ONTAP 軟體。請遵循的程序"將新節點新增至 ONTAP 叢集"。

叢集與管理交換器包括叢集網路交換器（ NX-OS ）、管理網路交換器（ IOS ）和參考組態檔（ RCF ）。如果您的叢集和管理交換器受到支援、但未執行目標 ONTAP 版本所需的最低軟體版本、請將交換器升級至支援的軟體版本。

- "NetApp下載：Broadcom叢集交換器"
- "NetApp下載：Cisco乙太網路交換器"
- "NetApp下載：NetApp叢集交換器"

如果您需要升級交換器、 NetApp 建議您先完成 ONTAP 軟體升級、然後為交換器執行軟體升級。

內部組態**MetroCluster**

升級 ONTAP 之前、如果您有 MetroCluster 組態、請使用 "NetApp 互通性對照表工具" 確認目標 ONTAP 版本支援您的 MetroCluster IP 交換器。

SAN組態

升級 ONTAP 之前、如果您的叢集已針對 SAN 進行設定、請使用 "NetApp 互通性對照表工具" 確認 SAN 組態完全受支援。

應支援所有SAN元件、包括目標ONTAP 版的整套軟體、主機作業系統和修補程式、必要的主機公用程式軟體、多重路徑軟體、以及介面卡驅動程式和韌體。

使用 **Active IQ Config Advisor** 在升級 **ONTAP** 之前識別常見的設定錯誤

在升級 ONTAP 之前、您可以使用 Active IQ Config Advisor 工具檢查常見的組態錯誤。

Active IQ Config Advisor 是適用於 NetApp 系統的組態驗證工具。它可以部署在安全站台和非安全站台、以進行資料收集和系統分析。

支援功能有限、僅限線上使用。Active IQ Config Advisor

步驟

1. 登入 "NetApp 支援網站"，然後單擊 **tools**>*Tools* 。
2. 在* Active IQ Config Advisor 《*》下、按一下 "下載應用程式"。
3. 下載、安裝及執行 Active IQ Config Advisor 。
4. 執行 Active IQ Config Advisor 之後、請檢閱工具的輸出、並遵循提供的建議來解決工具發現的任何問題。

支援的 **ONTAP** 升級路徑

您可以升級的 ONTAP 版本取決於您的硬體平台和叢集節點上目前執行的 ONTAP 版本。

若要驗證目標升級版本是否支援您的硬體平台、請參閱 "NetApp Hardware Universe"。 使用 "NetApp 互通性對照表工具" 至 "確認支援您的組態"。

若要判斷您目前**ONTAP** 的版本：

- 在System Manager中、按一下*叢集>總覽*。
- 在命令列介面（ CLI ）中、使用 `cluster image show` 命令。+
  您也可以使用 `system node image show` 進階權限層級的命令、以顯示詳細資料。

升級途徑的類型

建議盡可能自動進行不中斷升級（andu）。視您目前的版本和目標版本而定、您的升級途徑將是 * 直接 * 、 * 直接多跳 * 或 * 多階段 * 。

- * 直接 *

  您可以使用單一軟體映像、直接升級至下一個相鄰的 ONTAP 版本系列。對於許多版本、您也可以安裝軟體映像、以便直接升級至比執行版本更新最多四個版本的版本。

  例如，您可以直接從 9.12.1 升級到 9.13.1，或從 9.13.1 升級到 9.17.1。

  支援所有 *direct* 升級路徑 "混合版本叢集"。

- * 直接多跳 *

  對於一些自動不中斷升級（ ANDU ）至非相鄰版本、您需要安裝中間版本和目標版本的軟體映像。自動化升級程序會使用背景中的中繼映像來完成目標版本的更新。

  例如、如果叢集執行9.3且您想升級至9.7、則會載入ONTAP 9.5和9.7的版次安裝套件、然後啟動andu至9.7。ONTAP 會先自動將叢集升級至 9.5 、然後再升級至 9.7 。您應預期在程序期間會有多個接管/恢復作業及相關的重新開機。

- * 多階段 *

  如果您的非相鄰目標版本無法使用直接或直接的多躍點路徑、則必須先升級至支援的中繼版本、然後再升級至目標版本。

  例如，如果您目前執行的是 9.8 版本，並且想要升級到 9.16.1 版本，則必須完成多階段升級：首先從 9.8 升

級到 9.12.1，然後再從 9.12.1 升級到 9.16.1。從早期版本升級可能需要三個或更多階段，其中包含多次中間升級。

在開始進行多階段升級之前、請確定您的硬體平台支援您的目標版本。

在您開始進行任何重大升級之前、最佳做法是先將叢集上執行的 ONTAP 版本升級至最新的修補程式版本。這可確保ONTAP 您目前版本的任何問題都能在升級前解決。

例如、如果您的系統執行ONTAP 的是32個版本的更新版本、而您打算升級至9個版本的版本、您應該先升級至最新版本的9.3修補程式、然後依照從9.3升級至9個版本的升級途徑。

深入瞭解 "NetApp 支援網站上推薦使用的最低 ONTAP 版本"。

支援的升級途徑

以下升級路徑支援ONTAP軟體的自動和手動升級。這些升級路徑適用於本地ONTAP和ONTAP Select。有不同的 "Cloud Volumes ONTAP 支援的升級路徑"。

* 對於混合版本的 ONTAP 叢集 * ：所有 *direct* 和 *direct* 多躍點 _ 升級路徑都包含與混合版本叢集相容的 *ONTAP* 版本。包含在 *_mult-st*階段 _ 升級中的 *ONTAP* 版本與混合版本叢集不相容。例如、從 *9.8* 升級至 *9.12.1* 是 *_direct* 升級。節點執行 9.8 和 9.12.1 的叢集是支援的混合版本叢集。 從 9.8 升級到 9.13.1 是一項 _ 多階段 _ 升級。 節點執行 9.8 和 9.13.1 的叢集並非支援的混合版本叢集。

ONTAP 9.10.1 及更新版本

如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的自動化或手動升級途徑是**...**
9.17.1	9.18.1	直接
9.16.1.	9.18.1	直接
	9.17.1	直接
9.15.1..	9.18.1	直接
	9.17.1	直接
	9.16.1.	直接
9.14.1.	9.18.1	直接
	9.17.1	直接
	9.16.1.	直接
	9.15.1..	直接

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的自動化或手動升級途徑是…
9.13.1.12.9.12.9.	9.18.1	多階段 • 9.13.1 → 9.17.1 • 9.17.1 → 9.18.1
	9.17.1	直接
	9.16.1.	直接
	9.15.1..	直接
	9.14.1.	直接
9.12.1	9.18.1	多階段 • 9.12.1 → 9.16.1. • 9.16.1 → 9.18.1
	9.17.1	多階段 • 9.12.1 → 9.16.1. • 9.16.1 → 9.17.1
	9.16.1.	直接
	9.15.1..	直接
	9.14.1.	直接
	9.13.1.12.9.12.9.	直接

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的自動化或手動升級途徑是…
9.11.1.	9.18.1	多階段 • 9.11.1 → 9.15.1. • 9.15.1 → 9.18.1
	9.17.1	多階段 • 9.11.1 → 9.15.1. • 9.15.1 → 9.17.1
	9.16.1.	多階段 • 9.11.1 → 9.15.1. • 9.15.1 → 9.16.1.
	9.15.1..	直接
	9.14.1.	直接
	9.13.1.12.9.12.9.	直接
	9.12.1	直接

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的自動化或手動升級途徑是…
9.10.1	9.18.1	多階段 • 9.10.1 → 9.14.1. • 9.14.1 → 9.18.1
	9.17.1	多階段 • 9.10.1 → 9.14.1. • 9.14.1 → 9.17.1
	9.16.1.	多階段 • 9.10.1 → 9.14.1. • 9.14.1 → 9.16.1.
	9.15.1..	多階段 • 9.10.1 → 9.14.1. • 9.14.1 → 9.15.1.
	9.14.1.	直接
	9.13.1.12.9.12.9.	直接
	9.12.1	直接
	9.11.1.	直接

從 **ONTAP 9.9.1** 開始

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的自動化或手動升級途徑是…
9.9.1	9.18.1	多階段 • 9.9.1→9.13.1. • 9.13.1→9.17.1 • 9.17.1→9.18.1
	9.17.1	多階段 • 9.9.1→9.13.1. • 9.13.1→9.17.1
	9.16.1.	多階段 • 9.9.1→9.13.1. • 9.13.1→9.16.1.
	9.15.1..	多階段 • 9.9.1→9.13.1. • 9.13.1→9.15.1.
	9.14.1.	多階段 • 9.9.1→9.13.1. • 9.13.1→9.14.1.
	9.13.1.12.9.12.9.	直接
	9.12.1	直接
	9.11.1.	直接
	9.10.1	直接

從 **ONTAP 9.8** 開始

如果您要在 MetroCluster IP 組態中將下列任何平台機型從 ONTAP 9.8 升級至 9.10.1 或更新版本、則必須先升級至 ONTAP 9.9.1 ：

- FAS2750
- FAS500f
- VA220 AFF
- VA250 AFF

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的自動化或手動升級途徑是…
9.8	9.18.1	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1. • 9.16.1 → 9.18.1
	9.17.1	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1. • 9.16.1 → 9.17.1
	9.16.1.	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.16.1.
	9.15.1..	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.15.1.
	9.14.1.	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.14.1.
	9.13.1.12.9.12.9.	多階段 • 9.8 → 9.12.1 • 9.12.1 → 9.13.1.
	9.12.1	直接
	9.11.1.	直接
	9.10.1	直接
	9.9.1	直接

從 **ONTAP 9.7** 開始

ONTAP 9.7 的升級途徑可能會因執行自動或手動升級而有所不同。

自動化路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.7%		

	9.12.1	多階段 • 9.7 → 9.8 • 9.8 → 9.12.1
如果您目前**ONTAP**的版本是**…**	而您的目標**ONTAP**版本是**…**	您的自動升級途徑是**…**
	9.11.1.	直接多跳（ 9.8 和 9.11.1 需要影像）
	9.10.1	直接多跳（ 9.8 和 9.10.1P1 或更新版本 P 版本需要影像）
	9.9.1	直接
	9.8	直接

手動路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的手動升級途徑是...
9.7%		

	9.12.1	多階段 • 9.7 → 9.8
如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的手動升級途徑是**...**
	9.11.1.	多階段 • 9.7 → 9.8 • 9.8 → 9.11.1
	9.10.1	多階段 • 9.7 → 9.8 • 9.8 → 9.10.1
	9.9.1	直接
	9.8	直接

從 **ONTAP 9.6** 開始

ONTAP 9.6 的升級路徑可能會因執行自動或手動升級而異。

自動化路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.6%		

		• 9.6 → 9.8 • 9.8 → 9.12.1
如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的自動升級途徑是...
	9.12.1	多階段 • 9.6 → 9.8 • 9.8 → 9.12.1
	9.11.1.	多階段 • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	直接多跳（ 9.8 和 9.10.1P1 或更新版本 P 版本需要影像）
	9.9.1	多階段 • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	直接
	9.7%	直接

手動路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的手動升級途徑是...
9.6%		

		• 9.6 → 9.8 • 9.8 → 9.12.1
如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的手動升級途徑是**...**
	9.12.1	多階段 • 9.6 → 9.8 • 9.8 → 9.12.1
	9.11.1.	多階段 • 9.6 → 9.8 • 9.8 → 9.11.1
	9.10.1	多階段 • 9.6 → 9.8 • 9.8 → 9.10.1
	9.9.1	多階段 • 9.6 → 9.8 • 9.8 → 9.9.1
	9.8	直接
	9.7%	直接

從 **ONTAP 9.5** 開始

ONTAP 9.5 的升級途徑可能會因執行自動或手動升級而有所不同。

自動化路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.5.		

		• 9.5 → 9.9.1 （直接多跳，需要 9.7 和 9.9.1 的影像）
如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...
	9.12.1	多階段 • 9.5 → 9.9.1 （直接多跳，需要 9.7 和 9.9.1 的影像） • 9.9.1 → 9.12.1.
	9.11.1.	多階段 • 9.5 → 9.9.1 （直接多跳，需要 9.7 和 9.9.1 的影像） • 9.9.1 → 9.11.1.
	9.10.1	多階段 • 9.5 → 9.9.1 （直接多跳，需要 9.7 和 9.9.1 的影像） • 9.9.1 → 9.10.1.
	9.9.1	直接多跳（需要 9.7 和 9.9.1 的影像）
	9.8	多階段 • 9.5 → 9.7 • 9.7 → 9.8
	9.7%	直接
	9.6%	直接

手動升級路徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的手動升級途徑是...
9.5.		

		• 9.7 → 9.9.1 • 9.9.1 → 9.13.1.
如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的手動升級途徑是**...**
	9.13.1.12.9.12.9.	多階段 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.13.1.
	9.12.1	多階段 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.12.1.
	9.11.1.	多階段 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.11.1.
	9.10.1	多階段 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1.
	9.9.1	多階段 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	多階段 • 9.5 → 9.7 • 9.7 → 9.8
	9.7%	直接
	9.6%	直接

從 **ONTAP 9.4%** 至 **9.0**

ONTAP 9.4 、 9.3 、 9.2 、 9.1 和 9.0 的升級路徑可能會因執行自動升級或手動升級而異。

自動化升級途徑

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.4.		

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

		• 9.4 → 9.5 • 9.5 → 9.8 （直接多跳，需要 9.7 和 9.8 版影像）
如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	您的自動升級途徑是**...**
	9.7%	多階段 • 9.4 → 9.5 • 9.5 → 9.7
	9.6%	多階段 • 9.4 → 9.5 • 9.5 → 9.6
	9.5.	直接

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.3.		

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

		） • 9.7 → 9.8
如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的自動升級途徑是… 直接多跳（ 9.5 和 9.7 需要影像）
	9.6%	多階段 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	直接
	9.4.	無法使用

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.2.		

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的升級途徑是...
		• 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.10.1 （直接多跳，需要 9.8 和 9.10.1 的影像）
	9.9.1	多階段 • 9.2 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.9.1
	9.8	多階段 • 9.2 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.8
	9.7%	多階段 • 9.2 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像）
	9.6%	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	多階段 • 9.3 → 9.5 • 9.5 → 9.6
	9.4.	無法使用
	9.3.	直接

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.1.		

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的升級途徑是...
		• 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.10.1 （直接多跳，需要 9.8 和 9.10.1 的影像）
	9.9.1	多階段 • 9.1 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.9.1
	9.8	多階段 • 9.1 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像） • 9.7 → 9.8
	9.7%	多階段 • 9.1 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像）
	9.6%	多階段 • 9.1 → 9.3 • 9.3 → 9.6 （直接多跳，需要 9.5 和 9.6 的影像）
	9.5.	多階段 • 9.1 → 9.3 • 9.3 → 9.5
	9.4.	無法使用
	9.3.	直接
	9.2.	無法使用

如果您目前**ONTAP**的版本是...	而您的目標**ONTAP**版本是...	您的自動升級途徑是...
9.0		

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的自動升級途徑是...
		• 9.1 → 9.3 • 9.3 → 9.7 （直接多跳，需要 9.5 和 9.7 的影像）
	9.6%	多階段 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	多階段 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9.4.	無法使用
	9.3.	多階段 • 9.0 → 9.1 • 9.1 → 9.3
	9.2.	無法使用
	9.1.	直接

手動升級路徑

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的**andu**升級途徑是…
9.4.		

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

		• 9.5 → 9.7 • 9.7 → 9.9.1
如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的major升級途徑是…
	9.9.1	多階段 • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	多階段 • 9.4 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7%	多階段 • 9.4 → 9.5 • 9.5 → 9.7
	9.6%	多階段 • 9.4 → 9.5 • 9.5 → 9.6
	9.5.	直接

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的**andu**升級途徑是…
9.3.		

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

		• 9.5 → 9.7 • 9.7 → 9.9.1
如果您目前**ONTAP**的版本是**…**	而您的目標**ONTAP**版本是**…**	您的**Tanu**升級途徑是**…**
	9.9.1	多階段 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	多階段 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7%	多階段 • 9.3 → 9.5 • 9.5 → 9.7
	9.6%	多階段 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	直接
	9.4.	無法使用

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的**andu**升級途徑是…
9.2.		

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

		• 9.5 → 9.7 • 9.7 → 9.9.1
如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的aadu升級途徑是…
	9.10.1	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1 • 9.9.1 → 9.10.1.
	9.9.1	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.9.1
	9.8	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7 • 9.7 → 9.8
	9.7%	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6%	多階段 • 9.2 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	多階段 • 9.2 → 9.3 • 9.3 → 9.5
	9.4.	無法使用
	9.3.	直接

如果您目前**ONTAP**的版本是**…**	而您的目標**ONTAP**版本是**…**	您的**andu**升級途徑是**…**
9.1.		

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

		• 9.3 → 9.5
	9.4.	無法使用
如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…
9.3	9.3	直接
	9.2.	無法使用

如果您目前**ONTAP**的版本是…	而您的目標**ONTAP**版本是…	您的**andu**升級途徑是…
9.0		

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

如果您目前ONTAP的版本是…	而您的目標ONTAP版本是…	您的andu升級途徑是…

		• 9.3 → 9.5 • 9.5 → 9.7
如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	您的Tandu升級途徑是...
	9.7%	多階段 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.7
	9.6%	多階段 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5 • 9.5 → 9.6
	9.5.	多階段 • 9.0 → 9.1 • 9.1 → 9.3 • 9.3 → 9.5
	9.4.	無法使用
	9.3.	多階段 • 9.0 → 9.1 • 9.1 → 9.3
	9.2.	無法使用
	9.1.	直接

Data ONTAP 8.

請務必使用驗證您的平台是否能執行目標ONTAP 版本的 "NetApp Hardware Universe"。

附註： Data ONTAP 《Sept.8.3升級指南》錯誤地指出、在四節點叢集中、您應該計畫升級最後保留epsilon的節點。這不再是Data ONTAP 升級的必要條件、從版本號為32的版本開始。如需詳細資訊、請參閱 "NetApp錯誤線上錯誤編號805277"。

來自於**Data ONTAP**

您可以直接升級ONTAP 至版本更新、然後升級至更新版本。

發行早於**8.3.x**的版本、包括**8.2.x Data ONTAP**

您必須先升級Data ONTAP 至版本不含更新版本的版本、然後升級ONTAP 至版本不含更新版本的版本。

相關資訊

- "指令參考資料ONTAP"
- "叢集映像顯示"
- "系統節點映像顯示"

升級之前，請先確認 **ONTAP** 叢集 **LIF** 容錯移轉組態

升級 ONTAP 之前、您必須確認叢集的容錯移轉原則和容錯移轉群組已正確設定。

在升級過程中、會根據升級方法來移轉LIF。視升級方法而定、可能會使用或不使用LIF容錯移轉原則。

如果叢集中有8個以上的節點、則會使用批次方法執行自動升級。批次升級方法包括將叢集分成多個升級批次、在第一個批次中升級節點集、升級其高可用度（HA）合作夥伴、然後針對其餘批次重複此程序。在更新的版本中、如果使用批次方法、則會將LIF移轉至要升級之節點的HA合作夥伴。ONTAP在更新的版本中、如果使用批次方法、則會將lifs移轉至其他批次群組。ONTAP

如果叢集中的節點少於8個、則會使用循環方法執行自動升級。復原升級方法包括在 HA 配對中的每個節點上起始容錯移轉作業、更新容錯移轉的節點、啟動恢復、然後針對叢集中的每個 HA 配對重複執行該程序。如果使用循環方法、則會將l生命 移轉至LIF容錯移轉原則所定義的容錯移轉目標節點。

步驟

1. 顯示每個資料LIF的容錯移轉原則：

如果**ONTAP** 您的版本是...	使用此命令
9.6 或更新版本	`network interface show -service-policy *data* -failover`
9.5 或更早版本	`network interface show -role data -failover`

此範例顯示具有兩個資料生命期的雙節點叢集的預設容錯移轉組態：

```
cluster1::> network interface show -role data -failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------
---------------
vs0
         lif0            node0:e0b             nextavail       system-
defined
                         Failover Targets: node0:e0b, node0:e0c,
                                           node0:e0d, node0:e0e,
                                           node0:e0f, node1:e0b,
                                           node1:e0c, node1:e0d,
                                           node1:e0e, node1:e0f
vs1
         lif1            node1:e0b             nextavail       system-
defined
                         Failover Targets: node1:e0b, node1:e0c,
                                           node1:e0d, node1:e0e,
                                           node1:e0f, node0:e0b,
                                           node0:e0c, node0:e0d,
                                           node0:e0e, node0:e0f
```

「容錯移轉目標」欄位會顯示每個LIF的容錯移轉目標優先順序清單。例如、如果 'liL0' 從其主連接埠（ node0 上的 e0b ）容錯移轉、則會先嘗試容錯移轉至 node0 上的連接埠 e0c 。如果生命 0 無法容錯移轉至 e0c 、則會嘗試容錯移轉至 node0 上的連接埠 e0d 、依此類推。

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

2. 如果將容錯移轉原則設定為 * 停用 * 作為任何生命（ SAN 生命期除外）、請使用 `network interface modify` 啟用容錯移轉的命令。

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

3. 對於每個LIF、請確認「容錯移轉目標」欄位包含來自不同節點的資料連接埠、這些連接埠在LIF主節點升級時仍會保持正常運作。

   您可以使用 `network interface failover-groups modify` 命令將容錯移轉目標新增至容錯移轉群組。

   範例

```
network interface failover-groups modify -vserver vs0 -failover-group
fg1 -targets sti8-vsim-ucs572q:e0d,sti8-vsim-ucs572r:e0d
```

相關資訊

- "網路與LIF管理"

- "網路介面"
- "修改網路介面容錯移轉群組"

在升級之前驗證 **ONTAP** 叢集 **SVM** 路由組態

為了避免中斷、在您升級 ONTAP 軟體之前、您應確保預設 SVM 路由能夠到達任何無法透過更特定路由到達的網路位址。最佳做法是為SVM設定一條預設路由。如需詳細資訊、請參閱 "SU134 ：網路存取可能會因為 ONTAP 中不正確的路由組態而中斷"。

SVM的路由表會決定SVM用來與目的地通訊的網路路徑。請務必瞭解路由表的運作方式、以便在發生網路問題之前先加以預防。

路由規則如下：

- 透過最具體的可用路由傳送流量。ONTAP
- 當無法使用更多特定路由時、透過預設閘道路由（網路遮罩為0位元）路由流量。ONTAP

如果路由具有相同目的地、網路遮罩和度量、則無法保證系統在重新開機或升級後會使用相同的路由。如果您已設定多個預設路由、這尤其是一個問題。

特殊考量

在升級之前，請先檢查特定的 **ONTAP** 組態

某些叢集組態需要您在開始 ONTAP 軟體升級之前採取特定動作。 例如、如果您有 SAN 組態、則應在開始升級之前、先確認每個主機都已設定正確的直接和間接路徑數。

請檢閱下表、判斷您可能需要採取哪些額外步驟。

在您升級 **ONTAP** 之前、請自問 ...	如果您的答案是*是*、請執行此動作...
我的叢集目前是否處於混合版本狀態？	檢查混合版本需求
我是否MetroCluster 有一個不知道的組態？	檢閱MetroCluster 有關各種組態的特定升級需求
我是否有SAN組態？	驗證 SAN 主機組態
我的叢集是否定義了 SnapMirror 關係？	"驗證 ONTAP 版本與 SnapMirror 關係的相容性"
我是否定義了 DP 類型的 SnapMirror 關係、以及是否要升級至 ONTAP 9.12.1 或更新版本？	"將現有的DP類型關係轉換成XDP"
我是否正在使用 SnapMirror S3 、是否正在升級至 ONTAP 9 。 12.1 或更新版本？	"驗證 SnapMirror S3 組態的授權"
我是否在級聯的中間磁碟區上啟用了長期保留快照？	"停用串聯拓撲中間磁碟區的長期保留快照"
我是否將NetApp儲存加密與外部金鑰管理伺服器搭配使用？	刪除任何現有的金鑰管理伺服器連線
我是否已將網路群組載入SVM？	驗證每個節點上是否存在 netgroup 文件
我是否建立了 SVM 、並從 ONTAP 9 。 12.1 或更早版本升級至更高版本？	為 v4.2-xattis 選項指派明確的值

在您升級 **ONTAP** 之前、請自問 ...	如果您的答案是*是*、請執行此動作...
我是否有使用SSLv3的LDAP用戶端？	設定LDAP用戶端使用TLS
我是否使用工作階段導向的傳輸協定？	審查會話導向的協議的不利影響
在系統管理員帳戶使用SSH公開金鑰進行驗證的叢集上、是否已啟用SSL FIPS模式？	驗證 SSH 主機金鑰演算法支援
我的自主勒索軟體保護是否有主動式警告？	回應異常活動的自發勒索軟體保護警告

驗證 **ONTAP** 版本與混合版本叢集的相容性

在混合版本的 ONTAP 叢集中，節點會在短時間內執行兩個不同的主要 ONTAP 版本。例如，節點執行 ONTAP 9.8 和 9.12.1 或 ONTAP 9.9.1 和 9.13.1 的叢集是混合版本的叢集。節點在相同版本中執行不同修補層級的叢集（例如 ONTAP 9.9.1P1 和 9.9.9.1P5 ）並非混合版本叢集。

Cloud Volumes ONTAP 不支援混合版本叢集。

NetApp 在有限的時間內和特定案例中支援混合版本的 ONTAP 叢集。

以下是 ONTAP 叢集處於混合版本狀態的最常見案例：

- 大型叢集中的 ONTAP 軟體升級

  升級大型叢集中的所有節點可能需要數天或數週的時間。叢集會進入並保持在混合版本狀態，直到所有節點都升級為止。

- 當您計畫將新節點新增至叢集時、需要進行 ONTAP 軟體升級

  您可以將新節點新增至叢集以擴充其容量、或是在完全取代控制器的過程中新增節點。無論是哪種情況，您都可能需要輸入混合版本狀態，才能將資料從現有控制器移轉至新系統中的新節點。

為了達到最佳叢集作業、叢集處於混合版本狀態的時間長度應儘可能短。叢集在混合版本狀態下符合支援資格的最長時間長度取決於叢集中最低的 ONTAP 版本。

如果在混合版本叢集中執行的 **ONTAP** 最低版本是 ...	然後，您最多可以保持在混合版本狀態 ...
部分9.8或更新版本ONTAP	90 天
更新版本ONTAP	7 天

當叢集處於混合版本狀態時、除了升級或資料移轉程序所需的命令外、您不應輸入任何會改變叢集作業或組態的命令。例如、在升級和資料移轉完成之前、不應執行（但不限於） LIF 移轉、規劃的儲存容錯移轉作業或大規模物件建立或刪除等活動。

支援 **ONTAP** 軟體升級的混合版本叢集

您可以輸入混合式版本狀態，其中任何 ONTAP 版本都支援直接從最低的目前版本升級。例如，如果您執行的是 ONTAP 9.11.1 ，則可以輸入執行 ONTAP 9.15.1 之節點的混合版本狀態。您無法在執行 ONTAP 9.11.1 和 ONTAP 9.16.1 的節點上輸入混合版本狀態。ONTAP 9.16.1 不支援直接從 ONTAP 9.11.1 升級。

ONTAP補丁程式 (P) 版本對混合版本叢集的相容性沒有影響。例如，如果您執行的是ONTAP 9.11.1P6，則目前用於混合版本叢集相容性的ONTAP版本是ONTAP 9.11.1。或者，如果您執行的是ONTAP 9.12.1，並且想要升級到ONTAP 9.15.1P2，則用於混合版本叢集相容性的目標ONTAP版本是ONTAP 9.15.1。

若要升級至目前版本不支援直接升級的 ONTAP 版本，您必須執行多階段升級。在多階段升級中，您必須先輸入混合版本狀態，並以支援的最高版本直接從目前版本升級。您已完成該升級，然後再對目標版本執行個別升級。例如，如果目前最低版本為 ONTAP 9.10.1 ，而您想要升級至 ONTAP 9.16.1 ，請先輸入混合版本狀態，將所有節點升級至 ONTAP 9.14.1 ，然後再從 ONTAP 9.14.1 獨立升級至 ONTAP 9.16.1 。深入瞭解"多階段升級"和"支援的升級路徑"。

混合版本叢集只能包含兩個主要的 ONTAP 版本。例如，您可以使用執行 ONTAP 9.13.1 和 9.15.1 的節點，或執行 ONTAP 9.13.1 和 9.16.1 的節點，來建立混合版本叢集。您不能將節點執行 ONTAP 9.13.1 ， 9.15.1 和 9.16.1 的混合版本叢集。

如果您目前**ONTAP**的版本是**...**	而您的目標**ONTAP**版本是**...**	用於升級的混合版本狀態是**...**
9.17.1	9.18.1	支援
9.16.1.	9.18.1	支援
	9.17.1	支援
9.15.1..	9.18.1	支援
	9.17.1	支援
	9.16.1.	支援
9.14.1.	9.18.1	支援
	9.17.1	支援
	9.16.1.	支援
	9.15.1..	支援
9.13.1.12.9.12.9.	9.18.1	不支援
	9.17.1	支援
	9.16.1.	支援
	9.15.1..	支援
	9.14.1.	支援
9.12.1	9.17.1 或更高版本	不支援
	9.16.1.	支援
	9.15.1..	支援
	9.14.1.	支援
	9.13.1.12.9.12.9.	支援

如果您目前ONTAP的版本是...	而您的目標ONTAP版本是...	用於升級的混合版本狀態是...
9.11.1.	9.16.1 或更新版本	不支援
	9.15.1..	支援
	9.14.1.	支援
	9.13.1.12.9.12.9.	支援
	9.12.1	支援
9.10.1	9.15.1 或更新版本	不支援
	9.14.1.	支援
	9.13.1.12.9.12.9.	支援
	9.12.1	支援
	9.11.1.	支援
9.9.1	9.14.1 或更高版本	不支援
	9.13.1.12.9.12.9.	支援
	9.12.1	支援
	9.11.1.	支援
	9.10.1	支援
9.8	9.13.1 或更高版本	不支援
	9.12.1	支援
	9.11.1.	支援
	9.10.1	支援
	9.9.1	支援

將新節點新增至 **ONTAP** 叢集

如果您打算將新節點新增至叢集、而這些節點需要比叢集目前執行版本更高的最低 ONTAP 版本、則在新增節點之前、您必須在叢集中現有節點上執行任何支援的軟體升級。理想情況下、您可以將所有現有節點升級至您計畫新增至叢集的節點所需的最低 ONTAP 版本。不過、如果因為部分現有節點不支援較新版的 ONTAP 、所以無法這麼做、則在升級程序中、您必須在有限的時間內輸入混合版本狀態。

步驟

1. "升級" 不支援新控制器所需的最低ONTAP版本的節點，應升級到它們支援的最高ONTAP版本。

   例如，如果您有一台運行ONTAP 9.5 的 FAS8080，並且您正在新增一台運行ONTAP 9.12.1 的新 C 系列平台，則應將 FAS8080 升級到ONTAP 9.8（這是它支援的最高ONTAP版本）。

2. "將新節點新增至叢集"。
3. "移轉資料" 從要從叢集移除的節點、移至新增的節點。
4. "從叢集中移除不支援的節點"。
5. "升級" 將叢集遷移到與新節點上運行的ONTAP版本和補丁級別相同的環境，或遷移到... "最新建議的修補程式版本" 適用於在新節點上執行的ONTAP版本。
6. 請確認所有節點運行的ONTAP版本是否相同。

   a. 顯示叢集上執行的ONTAP版本：

   ```
   version
   ```

   b. 顯示叢集中每個節點上運行的ONTAP版本：

   ```
   version *
   ```

   如果輸出中報告的ONTAP版本存在差異， `version *` （集群）和 `version` （單一節點）命令，透過執行以下命令將所有節點更新到相同的ONTAP和修補程式版本： "叢集鏡像更新"。

如需資料移轉的詳細資訊、請參閱：

- "建立Aggregate並將磁碟區移至新節點"
- "設定新的 iSCSI 連線以進行 SAN 磁碟區移動"
- "使用加密來移動磁碟區"

檢查 **ONTAP** 升級需求以取得 **MetroCluster** 組態

在 MetroCluster 組態上升級 ONTAP 軟體之前，叢集必須符合特定需求。

- 兩個叢集都必須執行相同版本ONTAP 的支援。

  您ONTAP 可以使用version命令來驗證此版本。

- 如果您正在執行重大 ONTAP 升級、 MetroCluster 組態必須處於正常模式。
- 如果您正在執行修補程式 ONTAP 升級、 MetroCluster 組態可以是正常模式或切換模式。
- 除了雙節點叢集之外、您可以在不中斷營運的情況下、同時升級兩個叢集。

  若要在雙節點叢集中進行不中斷升級、叢集必須一次升級一個節點。

- 兩個叢集中的集合體不得處於重新同步RAID狀態。

  在MetroCluster修復期間，鏡像聚合會重新同步。您可以使用以下方式驗證MetroCluster配置是否處於此狀態 `storage aggregate plex show -in-progress true`命令。如果正在同步任何聚合，則不應執行升級，直到重新同步完成。

詳細了解 `storage aggregate plex show`在"指令參考資料ONTAP" 。

- 在升級進行期間、議定的切換作業將會失敗。

  為了避免升級或還原作業發生問題、請勿在升級或還原作業期間嘗試非計畫性的切換、除非兩個叢集上的所有節點都執行相同版本ONTAP 的故障恢復。

MetroCluster 正常作業的組態需求

- 來源SVM LIF必須在其主節點上處於開啟狀態。

  目的地SVM的資料生命期不需要達到或位於其主節點上。

- 本機站台上的所有集合體都必須在線上。
- 本機叢集的SVM所擁有的所有根磁碟區和資料磁碟區都必須處於線上狀態。

MetroCluster 的組態需求

- 所有生命都必須在其主節點上處於正常工作狀態。
- 所有的集合體都必須在線上、但DR站台的根集合體除外。

  DR站台的根集合體在切換的特定階段處於離線狀態。

- 所有磁碟區都必須處於線上狀態。

相關資訊

"驗MetroCluster 證網路和儲存設備的資訊不完整組態狀態"

在 **ONTAP** 升級之前驗證 **SAN** 主機組態

在 SAN 環境中升級 ONTAP 會變更直接路徑。在升級 SAN 叢集之前、您應該確認每個主機都已設定正確的直接和間接路徑數、而且每個主機都已連線至正確的生命體。

步驟

1. 在每個主機上、確認已設定足夠數量的直接和間接路徑、而且每個路徑都處於作用中狀態。

   每個主機都必須有通往叢集中每個節點的路徑。

2. 確認每個主機都已連接至每個節點上的LIF。

   您應該記錄啟動器清單、以便在升級後進行比較。如果您執行的是 ONTAP 9.11.1 或更新版本、請使用系統管理員來檢視連線狀態、因為它的顯示比 CLI 更清晰。

系統管理員

a. 在System Manager中、按一下*主機> SAN啟動器群組*。

   此頁面會顯示啟動器群組（igroup）清單。如果清單很大、您可以按一下頁面右下角的頁碼來檢視清單的其他頁面。

   這些欄會顯示有關階層的各種資訊。從9.11.1開始、也會顯示igroup的連線狀態。將游標暫留在狀態警示上以檢視詳細資料。

CLI

- 列出 iSCSI 啟動器：

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- 列出 FC 啟動器：

```
fcp initiator show -fields igroup,wwpn,lif
```

SnapMirror

SnapMirror ONTAP 關係的相容版本

在建立 SnapMirror 資料保護關係之前、來源和目的地磁碟區必須執行相容的 ONTAP 版本。在升級 ONTAP 之前、您應確認目前的 ONTAP 版本與目標 ONTAP 版本相容、以因應 SnapMirror 關係。

統一化複寫關係

對於類型為「'XDP'」的SnapMirror關係、使用內部部署或Cloud Volumes ONTAP 更新版本：

從0版開始ONTAP ：

- ONTAP 9.x.0 版本為純雲端版本、支援 Cloud Volumes ONTAP 系統。發行版本之後的星號（*）表示為純雲端版本。

  ONTAP 9.16.0 是僅限雲端部署規則的例外，因為它提供了以下支援："ASA r2 系統" 。發布版本後的加號（+）表示該版本同時支援ASA r2 和雲端。 ASA r2 系統僅支援與其他ASA r2 系統SnapMirror關係。

- ONTAP 9.x 版本為一般版本、可同時支援內部部署和 Cloud Volumes ONTAP 系統。

  如果"進階容量平衡"在執行 ONTAP 9.16.1 或更新版本的叢集中的磁碟區上啟用，則不支援 SnapMirror 傳輸至執行 ONTAP 9.16.1 之前版本 ONTAP 的叢集。

互通性是雙向的。

- ONTAP 9.4 及更高版本的互通性*

版本…ONTAP	與這些先前ONTAP 版本的功能互通…																				
	9.18.1	9.17.1	9.16.1.	9.16.0+	9.15.1..	9.15.0*	9.14.1.	9.14.0%*	9.13.1.12.9.12.9.	9.13.0*	9.12.1	9.12.0*	9.11.1.	9.11.0*	9.10.1	9.10.5*	9.9.1	9.9.3.0*	9.8	9.7%	9.6%	9.5.
9.18.1	是	是	是	是	是	否	是	否	是	是	否	否	否	否	否	否	否	否	否	否	否	否
9.17.1	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否	否	否	否	否	否	否
9.16.1.	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否	否	否	否	否
9.16.0+	是	是	是	是	是	否	是	否	是	否	是	否	是	否	是	否	否	否	否	否	否	否
9.15.1..	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否
9.15.0*	否	是	是	否	是	是	是	否	是	否	是	否	是	否	是	否	是	否	否	否	否	否
9.14.1.	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否
9.14.0%*	否	是	是	否	是	否	是	是	是	否	是	否	是	否	是	否	是	否	否	否	否	否
9.13.1.12.9.12.9.	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否
9.13.0*	否	是	是	否	是	否	是	否	是	是	是	否	是	否	是	否	是	否	是	否	否	否

9.12.1	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否
9.12.0*	否	否	是	否	是	否	是	否	是	否	是	是	是	否	是	否	是	否	是	是	否	否
9.11.1.	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否
9.11.0*	否	否	否	否	是	否	是	否	是	否	是	否	是	是	是	否	是	否	是	是	是	否
9.10.1	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.10.5*	否	否	否	否	是	否	是	否	是	否	是	否	是	否	是	是	是	否	是	是	是	是
9.9.1	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.9.3.0*	否	否	否	否	否	否	是	否	是	否	是	否	是	否	是	否	是	是	是	是	是	是
9.8	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.7%	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是
9.6%	否	否	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是
9.5.	否	否	否	否	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是

SnapMirror 同步關係

ONTAP 雲端執行個體不支援 SnapMirror 同步。

版本…ONTAP	與這些先前ONTAP 版本的功能互通…													
	9.18.1	9.17.1	9.16.1.	9.15.1..	9.14.1.	9.13.1.12.9.12.9.	9.12.1	9.11.1.	9.10.1	9.9.1	9.8	9.7%	9.6%	9.5.
9.18.1	是	是	是	是	是	是	是	否	否	否	否	否	否	否
9.17.1	是	是	是	是	是	是	是	否	否	否	否	否	否	否
9.16.1.	是	是	是	是	是	是	是	是	否	否	否	否	否	否

9.15.1..	是	是	是	是	是	是	是	是	是	否	否	否	否	否
9.14.1.	是	是	是	是	是	是	是	是	是	是	是	否	否	否
9.13.1.12.9.12.9.	是	是	是	是	是	是	是	是	是	是	是	是	否	否
9.12.1	是	是	是	是	是	是	是	是	是	是	是	是	否	否
9.11.1.	否	否	是	是	是	是	是	是	是	是	否	否	否	否
9.10.1	否	否	否	是	是	是	是	是	是	是	是	否	否	否
9.9.1	否	否	否	否	是	是	是	是	是	是	是	是	否	否
9.8	否	否	否	否	是	是	是	否	是	是	是	是	是	否
9.7%	否	否	否	否	否	是	是	否	否	是	是	是	是	是
9.6%	否	否	否	否	否	否	否	否	否	否	是	是	是	是
9.5.	否	否	否	否	否	否	否	否	否	否	否	是	是	是

SnapMirror SVM 災難恢復關係

- 此矩陣適用於從ONTAP 9.10.1 開始的 SVM 資料移動遷移功能。
- 您可以使用 SVM DR 來遷移不符合指定限制的 SVM。 "SVM遷移（SVM資料遷移）"。
- 在這兩種情況下，來源叢集和目標叢集之間最多可以有 2 個主要的*較新的* ONTAP版本，但要求目標版本必須與來源ONTAP版本相同或更新。

對於 **SVM** 災難恢復資料和 **SVM** 保護：

SVM 災難恢復僅支援在執行相同版本 ONTAP 的叢集之間進行。* SVM 複寫不支援版本獨立性 * 。

對於 **SVM** 移轉的 **SVM** 災難恢復：

- 從來源上的舊版 ONTAP 到目的地上的相同或更新版本 ONTAP 、都支援單一方向的複寫。
- 目標叢集上的 ONTAP 版本必須不超過兩個更新的主要內部部署版本，或兩個更新的主要雲端版本（從 ONTAP 9.0.0 開始），如下表所示。
  - 長期資料保護使用案例不支援複寫。

發行版本之後的星號（*）表示為純雲端版本。

若要判斷支援、請在左表欄中找到來源版本、然後在頂端列中找到目的地版本（適用於相似版本的 DR/Migration 、適用於較新版本的 Migration ）。

如果您使用的是ONTAP 9.10.1 或更高版本，則可以使用 "SVM資料移動性" 使用特性而不是 SVM DR 將 SVM 從一個叢集遷移到另一個叢集。

來源	目的地

	9.5.	9.6%	9.7%	9.8	9.9.3.0*	9.9.1	9.10.5*	9.10.1	9.11.0*	9.11.1.	9.12.0*	9.12.1	9.13.0*	9.13.1.12.9.12.9.	9.14.0%*	9.14.1.	9.15.0*	9.15.1..	9.16.0	9.16.1.	9.17.1	9.18.1
9.5.	災難恢復/移轉	移轉	移轉																			
9.6%		災難恢復/移轉	移轉	移轉																		
9.7%			災難恢復/移轉	移轉	移轉																	
9.8				災難恢復/移轉	移轉	移轉		移轉														
9.9.3.0*					災難恢復/移轉	移轉	移轉	移轉	移轉	移轉												
9.9.1						災難恢復/移轉	移轉	移轉	移轉	移轉												
9.10.5*							災難恢復/移轉	移轉	移轉	移轉	移轉	移轉										

9.10.1								災難恢復/移轉	移轉	移轉	移轉	移轉								
9.11.0*									災難恢復/移轉	移轉	移轉	移轉	移轉	移轉						
9.11.1.										災難恢復/移轉	移轉	移轉	移轉	移轉						
9.12.0*											災難恢復/移轉	移轉	移轉	移轉	移轉	移轉				
9.12.1												災難恢復/移轉	移轉	移轉	移轉	移轉				
9.13.0*													災難恢復/移轉	移轉	移轉	移轉	移轉	移轉		
9.13.1.12.9.12.9.														災難恢復/移轉	移轉	移轉	移轉	移轉		
9.14.0%*															災難恢復/移轉	移轉	移轉	移轉	移轉	移轉

9.14.1.																災難恢復/移轉	移轉	移轉	移轉		
9.15.0*																	災難恢復/移轉	移轉	移轉	移轉	
9.15.1..																		災難恢復/移轉	移轉	移轉	
9.16.0																			災難恢復/移轉	移轉	移轉	移轉
9.16.1.																				災難恢復/移轉	移轉	移轉
9.17.1																					災難恢復/移轉	移轉
9.18.1																						災難恢復/移轉

SnapMirror 災難恢復關係

對於類型為「DP」和原則類型「as同步 鏡射」的SnapMirror關係：

DP型鏡像無法從ONTAP 版本資訊的版本資訊中進行初始化、ONTAP 且在版本資訊的版本資訊中完全不支援。如需詳細資訊、請參閱 "取代資料保護SnapMirror關係"。

在下表中、左欄顯示ONTAP 來源Volume上的版本資訊、而上方列則顯示ONTAP 您在目的地Volume上可以使用的版本資訊。

來源	目的地								
	9.11.1.	9.10.1	9.9.1	9.8	9.7%	9.6%	9.5.	9.4.	9.3.
9.11.1.	是的	否	否	否	否	否	否	否	否
9.10.1	是的	是的	否	否	否	否	否	否	否
9.9.1	是的	是的	是的	否	否	否	否	否	否
9.8	否	是的	是的	是的	否	否	否	否	否
9.7%	否	否	是的	是的	是的	否	否	否	否
9.6%	否	否	否	是的	是的	是的	否	否	否
9.5.	否	否	否	否	是的	是的	是的	否	否
9.4.	否	否	否	否	否	是的	是的	是的	否
9.3.	否	否	否	否	否	否	是的	是的	是的

互通性並非雙向的。

將現有的 **ONTAP SnapMirror DP** 類型關係轉換為 **XDP**

如果您要升級ONTAP 至更新版本的版本、則必須先將DP類型的關係轉換成XDP、然後再升級。不支援DP類型的關係。ONTAP您可以輕鬆地將現有的DP類型關係轉換成XDP、以善用靈活版本的SnapMirror。

在升級ONTAP 至版本更新至版本更新ONTAP 之前、您必須先將現有的DP類型關係轉換成XDP、才能升級至版本更新。

關於這項工作

- SnapMirror不會自動將現有的DP類型關係轉換為XDP。若要轉換關係、您必須中斷並刪除現有的關係、建立新的XDP關係、然後重新同步關係。
- 規劃轉換時、您應該注意、XDP SnapMirror關係的背景準備和資料倉儲階段可能需要很長時間。SnapMirror關係報告長時間處於「準備」狀態、並不罕見。

將SnapMirror關係類型從DP轉換為XDP之後、與空間相關的設定（例如自動調整大小和空間保證）將不再複寫到目的地。

步驟

1. 從目的地叢集、確定SnapMirror關係為DP類型、鏡射狀態為Snapmirror、關係狀態為閒置、關係健全：

```
snapmirror show -destination-path <SVM:volume>
```

下列範例顯示的輸出 `snapmirror show` 命令：

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

您可能會發現保留命令輸出複本有助於 `snapmirror show`追蹤現有的關聯性設定。如"指令參考資料ONTAP"需詳細 `snapmirror show`資訊，請參閱。

2. 從來源和目的地磁碟區，確保兩個磁碟區都有通用的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

下列範例顯示 `volume snapshot show` 來源和目的地磁碟區的輸出：

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 若要確保在轉換期間不會執行排程的更新、請停止現有的DP類型關係：

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

您必須從目的地SVM或目的地叢集執行此命令。

以下範例會暫停來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

4. 打破現有的DP類型關係：

```
snapmirror break -destination-path <SVM:volume>
```

您必須從目的地SVM或目的地叢集執行此命令。

以下範例打破來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

5. 如果在目的地磁碟區上啟用自動刪除快照功能，請停用它：

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

以下範例停用目的地磁碟區上的快照自動刪除 `volA_dst`：

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 刪除現有的DP類型關係：

```
snapmirror delete -destination-path <SVM:volume>
```

如"指令參考資料ONTAP"需詳細 `snapmirror-delete`資訊，請參閱。

您必須從目的地SVM或目的地叢集執行此命令。

以下範例刪除來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. 在來源上釋放原始伺服器 SVM 災難恢復關係：

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

以下範例發佈 SVM 災難恢復關係：

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

如"指令參考資料ONTAP"需詳細 `snapmirror release`資訊，請參閱。

8. 您可以使用從保留的輸出 `snapmirror show` 建立新 XDP 類型關係的命令：

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

新關係必須使用相同的來源和目的地Volume。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

您必須從目的地SVM或目的地叢集執行此命令。

以下範例在來源磁碟區之間建立 SnapMirror 災難恢復關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup` 使用預設值 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. 重新同步來源與目的地磁碟區：

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

為了縮短重新同步時間，您可以使用 `-quick-resync`選項，但您應該意識到儲存效率節省可能會遺失。

> 您必須從目的地SVM或目的地叢集執行此命令。雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

以下範例重新同步來源 Volume 之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

詳細了解 `snapmirror resync`在"指令參考資料ONTAP" 。

10. 如果您停用自動刪除快照功能，請重新啟用：

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

完成後

1. 使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

2. 一旦 SnapMirror XDP 目的地磁碟區開始依照 SnapMirror 原則定義更新快照，請使用來源叢集的命令輸出 `snapmirror list-destinations`來顯示新的 SnapMirror XDP 關係。

DP 型關係的其他資訊

從 ONTAP 9.3 開始， XDP 模式是預設模式，在命令列或新的或現有指令碼中， DP 模式的任何調用都會自動轉換為 XDP 模式。

現有的關係不受影響。如果某個關係已經是DP類型、則會繼續是DP類型。從 ONTAP 9.5 開始，如果未指定資料保護模式或將 XDP 模式指定為關係類型，則 MirrorAndVault 是預設原則。下表顯示預期行為。

如果您指定…	類型為…	預設原則（如果您未指定原則）是…
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
什麼都沒有	XDP	MirrorAndVault（統一化複寫）
XDP	XDP	MirrorAndVault（統一化複寫）

如表所示，在不同情況下指派給 XDP 的預設原則，可確保轉換維持與先前類型的功能等效。當然、您可以視需要使用不同的原則、包括統一化複寫的原則：

如果您指定…	政策是…	結果是…
DP	MirrorAllSnapshots	SnapMirror災難恢復
XDPDefault	SnapVault	MirrorAndVault
統一化複寫	XDP	MirrorAllSnapshots
SnapMirror災難恢復	XDPDefault	SnapVault

轉換的唯一例外情況如下：

- SVM資料保護關係在ONTAP 更新版本的更新版本中、仍預設為DP模式。

  從ONTAP SVM 9.4開始、SVM資料保護關係預設為XDP模式。

- 根Volume負載共享資料保護關係仍預設為DP模式。
- 在更新版本的版本中、資料保護關係仍預設為DP模式。SnapLock ONTAP

  從ONTAP S廳9.5開始、SnapLock 資料保護關係預設為XDP模式。

- 如果您設定下列全叢集選項、DP的明確調用仍會繼續預設為DP模式：

  ```
  options replication.create_data_protection_rels.enable on
  ```

  如果您未明確叫用DP、則會忽略此選項。

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

在 **ONTAP** 升級之前停用長期保留快照

在級聯磁碟區的關係中， ONTAP 9 的所有版本僅支援在級聯的最終SnapMirror目標磁碟區上保留長期快照。在級聯備份的任何中間磁碟區上啟用長期保留快照會導致備份和快照遺失。

詳細了解"長期保留快照"。

如果您在級聯的任何中間磁碟區上啟用了長期保留快照，且設定不受支持，請聯絡技術支援並參考下列連結：https://kb.netapp.com/on-prem/ontap/DP/SnapMirror/SnapMirror-KBs/Cascading_a_volume_with_Long-Term_Retention_ NetApp知識庫：不支援啟用長期保留 (LTR) 快照的磁碟區級聯^] 以取得協助。

以下ONTAP版本不允許您在級聯中的任何磁碟區上啟用長期保留快照，但最終的SnapMirror目標磁碟區除外。

- 9.15.1 及更高版本
- 9.14.1P2 和 P4 至 P14
- 9.13.1P9至P17
- 9.12.1 P12 至 P19
- 9.11.1P15至P20
- 9.10.1P18至P20
- 9.9.1P20

在從允許您在級聯中間磁碟區上啟用長期保留快照的 ONTAP版本升級到阻止該功能的 ONTAP版本之前，您需要停用長期保留快照，以避免錯過備份和快照。

您必須在下列案例中採取行動：

- 長期保留快照配置在「A > B > C」 SnapMirror級聯中的「B」磁碟區上，或配置在更大的級聯中的另一個中間SnapMirror目標磁碟區上。
- 長期保留快照由應用於SnapMirror策略規則的計畫定義。此規則不會從來源磁碟區複製快照，而是直接在目標磁碟區上建立快照。

> ⓘ 有關計劃和SnapMirror策略的更多信息，請參閱"NetApp知識庫： ONTAP 9 SnapMirror策略規則中的「schedule」參數如何運作？"。

步驟

1. 從級聯中間磁碟區的SnapMirror策略中移除長期保留規則：

```
Secondary::> snapmirror policy remove-rule -vserver <> -policy <>
-snapmirror-label <>
```

詳細了解 `snapmirror policy remove-rule`在"指令參考資料ONTAP" 。

2. 再次為SnapMirror標籤新增規則，但不設定長期保留期限：

```
Secondary::> snapmirror policy add-rule -vserver <> -policy <>
-snapmirror-label <> -keep <>
```

> ⓘ 從SnapMirror策略規則中刪除長期保留快照意味著SnapMirror將從來源磁碟區中提取具有給定標籤的快照。您可能還需要在來源磁碟區的快照策略中新增或修改計劃，以建立正確標記的快照。

如"指令參考資料ONTAP"需詳細 `snapmirror policy add-rule`資訊，請參閱。

3. 如有必要、請修改（或建立）來源磁碟區快照原則的排程、以允許使用 SnapMirror 標籤建立快照：

```
Primary::> volume snapshot policy modify-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <>
```

```
Primary::> volume snapshot policy add-schedule -vserver <> -policy <>
-schedule <> -snapmirror-label <> -count <>
```

在SnapMirror級聯配置中，仍然可以在最終的SnapMirror目標磁碟區上啟用長期保留快照。

驗證 **SnapMirror S3** 組態的 **ONTAP** 授權

在升級 ONTAP 之前、如果您使用的是 SnapMirror S3 、而您要升級至 ONTAP 9 。 12.1 或更新版本、則應確認您擁有適當的 SnapMirror 授權。

升級 ONTAP 之後、在 ONTAP 9 · 11.1 及更早版本與 ONTAP 9 · 12.1 及更高版本之間所發生的授權變更、可能會導致 SnapMirror S3 關係失敗。

更新版本**ONTAP**

- 當複寫至 NetApp 主控的目的地貯體（ ONTAP S3 或 StorageGRID ）時、 SnapMirror S3 會在推出"ONTAP One"軟體套件之前、先檢查資料保護套件中所含的 SnapMirror 同步授權。
- 當複寫至非 NetApp 目的地貯體時、 SnapMirror S3 會檢查混合雲套件中的 SnapMirror 雲端授權、而混合雲套件"ONTAP One"是在軟體套件推出之前提供的。

更新版本**ONTAP**

- 當複寫至 NetApp 主控的目的地貯體（ ONTAP S3 或 StorageGRID ）時、 SnapMirror S3 會檢查 SnapMirror S3 授權、此授權包含在"ONTAP One"軟體套件推出前提供的資料保護套件中。
- 當複寫至非 NetApp 目的地貯體時、 SnapMirror S3 會檢查混合雲套件中的 SnapMirror S3 外部授權、此套件是在"ONTAP One"軟體套件和之前提供的"ONTAP One 相容性套件"。

現有的 **SnapMirror S3** 關係

現有的 SnapMirror S3 關係應在從 ONTAP 9 · 11.1 或更早版本升級至 ONTAP 9 · 12.1 或更高版本之後繼續運作、即使叢集沒有新的授權。

如果叢集未安裝適當的授權、建立新的 SnapMirror S3 關係將會失敗。

在升級 **ONTAP** 之前刪除現有的外部金鑰管理伺服器連線

升級 ONTAP 之前、如果您使用 NetApp 儲存加密（ NSE ）執行 ONTAP 9.2 或更早版本、並升級至 ONTAP 9.3 或更新版本、則必須使用命令列介面（ CLI ）刪除任何現有的外部金鑰管理（ KMIP ）伺服器連線。

步驟

1. 確認NSE磁碟機已解除鎖定、開啟並設定為預設製造商安全ID 0x0：

```
storage encryption disk show -disk *
```

如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

2. 進入進階權限模式：

```
set -privilege advanced
```

如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

3. 使用預設製造安全 ID 0x0 將 FIPS 金鑰指派給自我加密磁碟（ SED ）：

```
storage encryption disk modify -fips-key-id 0x0 -disk *
```

如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

4. 確認指派 FIPS 金鑰給所有磁碟已完成：

```
storage encryption disk show-status
```

如"指令參考資料ONTAP"需詳細 `storage encryption disk show-status`資訊，請參閱。

5. 驗證所有磁碟的 * 模式 * 是否已設定為資料

```
storage encryption disk show
```

如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

6. 檢視已設定的 KMIP 伺服器：

```
security key-manager keystore show
```

詳細了解 `security key-manager keystore show`在"指令參考資料ONTAP"。

7. 刪除已設定的 KMIP 伺服器：

```
security key-manager delete -address <kmip_ip_address>
```

如"指令參考資料ONTAP"需詳細 `security key-manager delete`資訊，請參閱。

8. 刪除外部金鑰管理程式組態：

```
security key-manager external disable
```

詳細了解 `security key-manager external disable`在"指令參考資料ONTAP"。

此步驟不會刪除 NSE 憑證。

下一步

升級完成後、您必須 重新設定 KMIP 伺服器連線。

在 **ONTAP** 升級之前、請確認所有節點上都存在 **netgroup** 檔案

升級 ONTAP 之前、如果您已將 netgroup 載入儲存虛擬機器（ SVM ）、則必須確認每個節點上都有 netgroup 檔案。節點上缺少 netgroup 檔案可能會導致升級失敗。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 顯示每個 SVM 的 netgroup 狀態：

```
vserver services netgroup status
```

3. 確認每個 SVM 的每個節點都顯示相同的 netgroup 檔案雜湊值：

```
vserver services name-service netgroup status
```

如果是這種情況、您可以跳過下一步、繼續升級或回復。否則、請繼續下一步。

4. 在叢集的任何一個節點上、手動載入 netgroup 檔案：

```
vserver services netgroup load -vserver vserver_name -source uri
```

此命令會在所有節點上下載netgroup檔案。如果某個節點上已存在netgroup檔案、則會將其覆寫。

相關資訊

"使用 netgroups"

在 **ONTAP** 升級之前，請為 **v4.2-xattis** 選項指派明確的值

如果您有 NFSv4.2 用戶端、則在從某些版本和 ONTAP 9 的修補程式升級之前、您必須為

NFSv4.2 延伸屬性選項提供明確的值、以避免在升級後發生 NFS 回應錯誤。

如果 `v4.2-xattrs`在 ONTAP 升級至受影響版本之前從未明確指派此選項值、則不會通知 NFSv4.2 用戶端伺服器的延伸屬性選項已變更。這會因為用戶端和伺服器不相符而導致特定通話發生 NFS 回應錯誤 `xattrs。

開始之前

如果符合下列條件、您需要為 NFSv4.2 延伸屬性選項指派明確的值：

- 您正在使用 NFSv4.2 搭配使用 ONTAP 9 · 11.1 或更早版本建立的 SVM
- 您正在從下列任何受影響的版本和修補程式升級 ONTAP ：
  - 9.12.1RC1 至 9.12.1P11
  - 9.13.1RC1 至 9.13.1P8
  - 9.14.1RC1 至 9.14.1P1

關於這項工作

您必須執行 ONTAP 9 。 12.1 或更新版本、才能使用本程序所述的命令來設定值。

如果已設定為 enabled、則 `v4.2-xattrs`仍應明確設定為、 `enabled`以避免未來中斷。如果您設定 `v4.2-xattrs`為停用、 NFSv4.2 用戶端在重新掛載或將選項設定為 `enabled`之前、都可以接收「無效的引數」回應 `v4.2-xattrs。

步驟

- 為選項指派明確的值 `v4.2-xattrs`：

```
nfs modify -v4.2-xattrs <enabled/disabled> -vserver <vserver_name>
```

相關資訊

"NFS v4.2-xtrs 欄位會在升級後翻轉"

將 **LDAP** 用戶端設定為在 **ONTAP** 升級之前使用 **TLS**

在升級 ONTAP 之前、您必須使用 SSLv3 設定 LDAP 用戶端、以便與 LDAP 伺服器進行安全通訊、以使用 TLS 。升級後將無法使用SSL。

根據預設、用戶端與伺服器應用程式之間的LDAP通訊不會加密。您必須禁止使用SSL並強制使用TLS。

步驟

1. 確認環境中的LDAP伺服器支援TLS。

   如果沒有、請勿繼續。您應該將LDAP伺服器升級至支援TLS的版本。

2. 檢查哪些 ONTAP LDAP 用戶端組態已啟用 LDAP over SSL/TLS ：

```
vserver services name-service ldap client show
```

如果沒有、您可以跳過其餘步驟。不過、您應該考慮使用LDAP over TLS來提高安全性。

3. 對於每個 LDAP 用戶端組態、不允許 SSL 強制使用 TLS ：

```
vserver services name-service ldap client modify -vserver <vserver_name>
-client-config <ldap_client_config_name> -allow-ssl false
```

4. 確認不再允許任何 LDAP 用戶端使用 SSL ：

```
vserver services name-service ldap client show
```

相關資訊

"NFS管理"

了解 **ONTAP** 升級期間面向會話的協定的不利影響

叢集和工作階段導向的通訊協定可能會對某些領域的用戶端和應用程式造成不良影響、例如升級期間的 I/O 服務。

如果您使用的是以工作階段為導向的傳輸協定、請考慮下列事項：

- 中小企業

  如果您與 SMBv3 一起提供持續可用（ CA ）共享、則可以使用自動化不中斷升級方法（使用 System Manager 或 CLI ）、而且不會造成中斷客戶經驗豐富。

  如果您使用SMBv1或SMBv2提供共用、或使用SMBv3提供非CA共用、則在升級接管和重新開機作業期間、用戶端工作階段會中斷。您應該指示使用者在升級前結束其工作階段。

  Hyper-V和SQL Server over SMB支援不中斷營運（NDOS）。如果您設定Hyper-V或SQL Server over SMB解決方案、則應用程式伺服器和內含的虛擬機器或資料庫將維持在線上狀態、並在ONTAP 更新版本時提供持續可用度。

- NFSv4.x

  NFSv4.x用戶端會使用正常的NFSv4.x還原程序、自動從升級期間發生的連線中斷中恢復。在此程序期間、應用程式可能會遇到暫時性的I/O延遲。

- NDMP

  狀態遺失、用戶端使用者必須重試此作業。

- 備份與還原

狀態遺失、用戶端使用者必須重試此作業。

請勿在升級期間或升級之前立即啟動備份或還原。否則可能導致資料遺失。

- 應用程式（例如Oracle或Exchange）

  影響取決於應用程式。對於以逾時為基礎的應用程式、您可能可以將逾時設定變更為ONTAP 長於重開機時間、以將不良影響降至最低。

在 **ONTAP** 升級之前、請先確認 **SSH** 主機金鑰演算法支援

在升級 ONTAP 之前、如果已在系統管理員帳戶使用 SSH 公開金鑰驗證的叢集上啟用 SSL FIPS 模式、則必須確保目標 ONTAP 版本支援主機金鑰演算法。

下表指出ONTAP 支援哪些主機金鑰類型演算法來進行支援以利執行支援的SSH連線。 這些金鑰類型不適用於設定SSH公用驗證。

發行版ONTAP	FIPS模式支援的金鑰類型	非FIPS模式支援的金鑰類型
9.11.1 及更新版本	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256 RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	ECDSA-SHA2-nistp256 SSH-ed25519 SSH-DSS SSH-RSA

從 ONTAP 9.11.1 開始、移除對 ssh-ed25519 主機金鑰演算法的支援。

如需更多資訊、請參閱 "使用FIPS設定網路安全性"。

如果現有 SSH 公開金鑰帳戶沒有支援的金鑰演算法、則必須使用支援的金鑰類型重新設定、否則系統管理員驗證將會失敗。

"深入瞭解如何啟用SSH公開金鑰帳戶。"

在 **ONTAP** 升級之前，請先解決自主勒索軟體保護（ **ARP** ）中的活動警告

升級至 ONTAP 9 。 16.1 或更新版本之前，您應該回應任何由自主勒索軟體保護（ ARP ）回報的異常活動警告。在 ONTAP 9 。 16.1 中， ARP 改為以機器學習 / 人工智慧（ AI ）為基礎的模型。由於這項變更，從 ONTAP 9 · 15.1 或更早版本中的現有 ARP 中，任何未解決的作用中警告都會在升級後遺失。

步驟

1. 回應回報的任何異常活動警告"ARP"，並解決任何潛在問題。
2. 選擇 * 更新並清除可疑的檔案類型 * 來記錄您的決定並恢復正常的 ARP 監控，以確認這些問題在升級之前的解決方法。

重新啟動 **SP** 或 **BMC** 、以準備在 **ONTAP** 升級期間進行韌體更新

您不需要在ONTAP 進行升級之前手動更新韌體。 叢集的韌體隨附ONTAP 於更新套件中、並複製到每個節點的開機裝置。 新韌體隨後會在升級程序中安裝。

如果叢集中的韌體版本比ONTAP 隨附於此版更新套件的韌體版本舊、則會自動更新下列元件的韌體：

- BIOS /載入程式
- 服務處理器（SP）或基板管理控制器（BMC）
- 儲存櫃
- 磁碟
- Flash 快取

若要準備順利更新、您應該在升級開始之前重新啟動SP或BMC。

使用ONTAP CLI、 SP或BMC重啟。

CLI

1. 重啟SP或BMC：

```
system service-processor reboot-sp -node <node_name>
```

SP

1. 重啟SP：

```
sp reboot
```

BMC

1. 重啟BMC：

```
bmc reboot
```

一次只能重新啟動一個 SP 或 BMC 。 等待重新開機的 SP 或 BMC 完全回收、然後再重新開機。

您也可以"手動更新韌體"在 ONTAP 升級之間進行。如果您有數位顧問、您可以"檢視ONTAP 目前包含在您的ImageImage中的韌體版本清單"。

更新的韌體版本如下所示：

- "系統韌體（BIOS、BMC、SP）"
- "機櫃韌體"
- "磁碟與 Flash Cache 韌體"

在升級之前下載 **ONTAP** 軟體映像

升級 ONTAP 之前、您必須先從 NetApp 支援網站 下載目標 ONTAP 軟體映像。視 ONTAP 版本而定、您可以將 ONTAP 軟體下載到網路上的 HTTPS 、 HTTP 或 FTP 伺服器、或是本機資料夾。

如果您正在執行...	您可以將映像下載至此位置 ...
更新版本ONTAP	• HTTPS 伺服器 伺服器的 CA 憑證必須安裝在本機系統上。 • 本機資料夾 • HTTP或FTP伺服器
更新版本ONTAP	• 本機資料夾 • HTTP或FTP伺服器
不含更新版本ONTAP	HTTP或FTP伺服器

關於這項工作

- 如果您使用執行自動不中斷升級（ andu ） "直接多跳升級途徑"、您需要 "下載" 適用於您升級所需之中介 ONTAP 版本和目標 ONTAP 版本的軟體套件。 例如、如果您要從 ONTAP 9.8 升級至 ONTAP 9.13.1 、則必須同時下載 ONTAP 9.12.1 和 ONTAP 9.13.1 的軟體套件。 請參閱 "支援的升級路徑" 若要判斷您的升級路徑是否需要下載中介軟體套件。
- 如果您要將採用NetApp Volume Encryption的系統升級ONTAP 為版本9.5或更新版本、則必須下載ONTAP 非受限國家/地區的版本、包括NetApp Volume Encryption。

  如果您使用ONTAP 受限國家/地區的「更新版」軟體映像來升級採用NetApp Volume Encryption的系統、系統就會出現問題、而且您無法存取磁碟區。

- 您不需要為韌體下載個別的軟體套件。您叢集的韌體更新隨附於 ONTAP 軟體升級套件中、並複製到每個節點的開機裝置。新韌體隨後會在升級程序中安裝。

步驟

1. 在中找到目標ONTAP 的Software "軟體下載" NetApp 支援網站的區域。

   如需ONTAP Select 升級版、請選取* ONTAP Select 《節點升級*》 。

2. 將軟體映像（例如97_q_image.tgz）複製到適當的位置。

   視ONTAP 您的版本而定、此位置將是HTTP、HTTPS或FTP伺服器的目錄、映像將從該目錄提供給本機系統、或是儲存系統上的本機資料夾。

ONTAP 升級方法

ONTAP 軟體升級方法

您可以使用 System Manager 執行ONTAP軟體的自動升級。或者，您也可以使用ONTAP命令列介面 (CLI) 執行自動或手動升級。升級ONTAP的方法取決於您的配置、目前ONTAP版本以及叢集中的節點數。NetApp 建議您使用系統管理員來執行自動升級、除非您的組態需要不同的方法。例如，如果您有一個運行ONTAP 9.3 或更高版本的四節點MetroCluster配置，則應使用 System Manager 執行自動升級（有時稱為自動無中斷升級或 ANDU）。

如果您透過NetApp控制台升級到ONTAP 9.15.1 或更高版本，請依照"NetApp控制台文件中的升級流程"。

您可以使用循環升級程序或批次升級程序來執行升級。兩者皆不中斷營運。

對於自動升級、 ONTAP 會自動在每個節點上安裝目標 ONTAP 映像、驗證叢集元件、確保叢集可以不中斷地升級、然後根據節點數量在背景執行批次或滾動升級。對於手動升級、管理員會手動確認叢集中的每個節點都已準備好進行升級、然後執行步驟來執行循環升級。

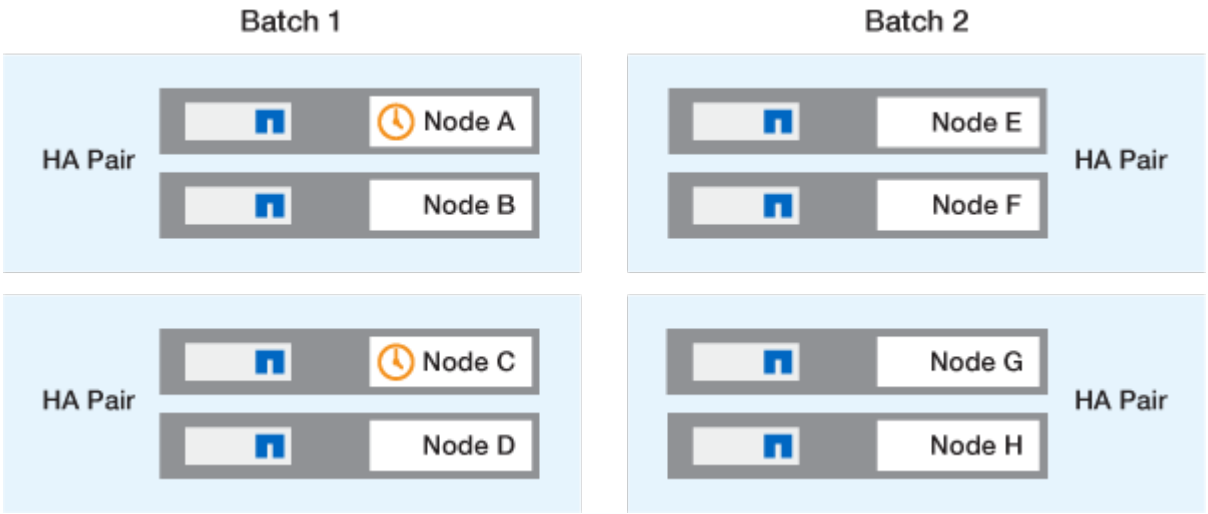
ONTAP 滾動升級

對於節點少於 8 個的叢集而言、循環升級程序是預設程序。 在循環升級程序中、節點會離線並升級、而其合作夥伴則會接管其儲存設備。當節點升級完成時、合作夥伴節點會將控制權交回原始擁有節點、並在合作夥伴節點上重複此程序。每個額外的HA配對都會依序升級、直到所有HA配對都執行目標版本為止。

ONTAP 批次升級

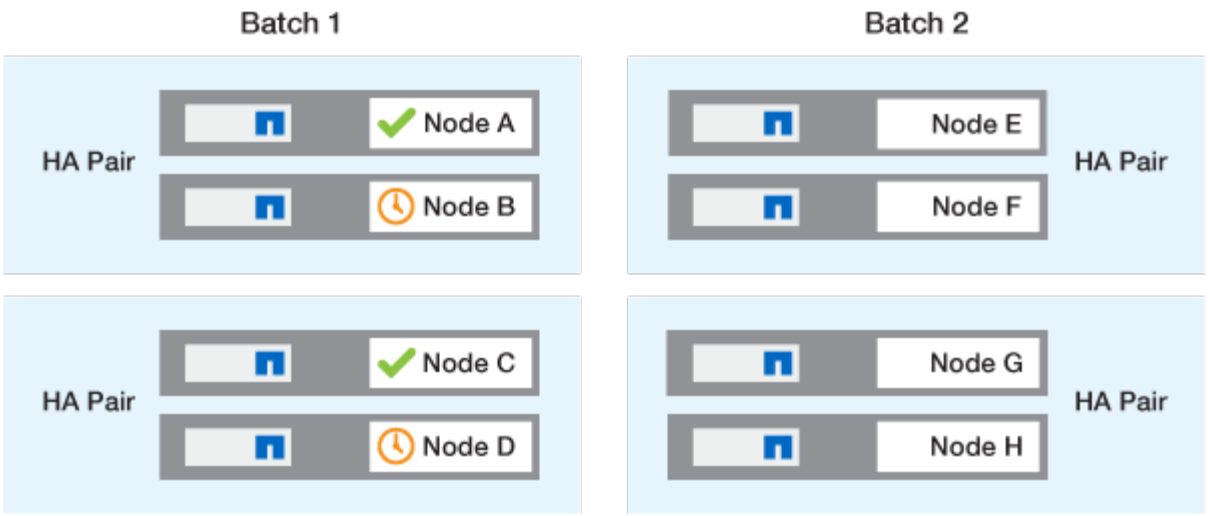
批次升級程序是 8 個以上節點叢集的預設程序。 在批次升級程序中、叢集分為兩批。 每個批次都包含多個 HA 配對。在第一批中、每個 HA 配對的第一個節點會與批次中所有其他 HA 配對的第一個節點同時升級。

在以下範例中、每個批次中有兩個 HA 配對。 批次升級開始時、節點 A 和節點 C 會同時升級。



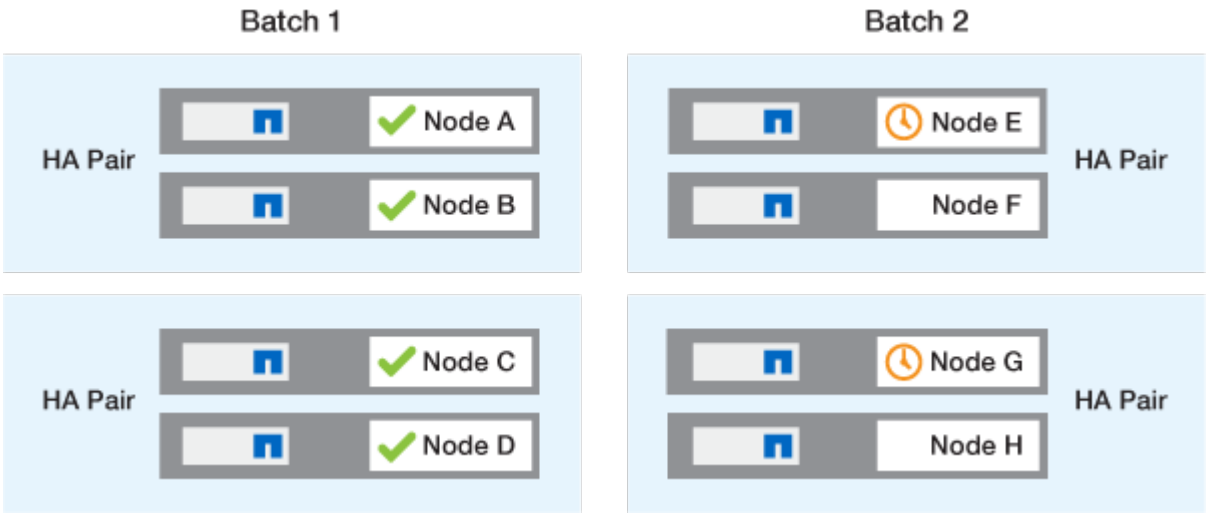
每個 HA 配對的第一個節點升級完成後、批次 1 中的合作夥伴節點會同時升級。

在以下範例中、節點 A 和節點 C 升級之後、節點 B 和節點 D 會同時升級。



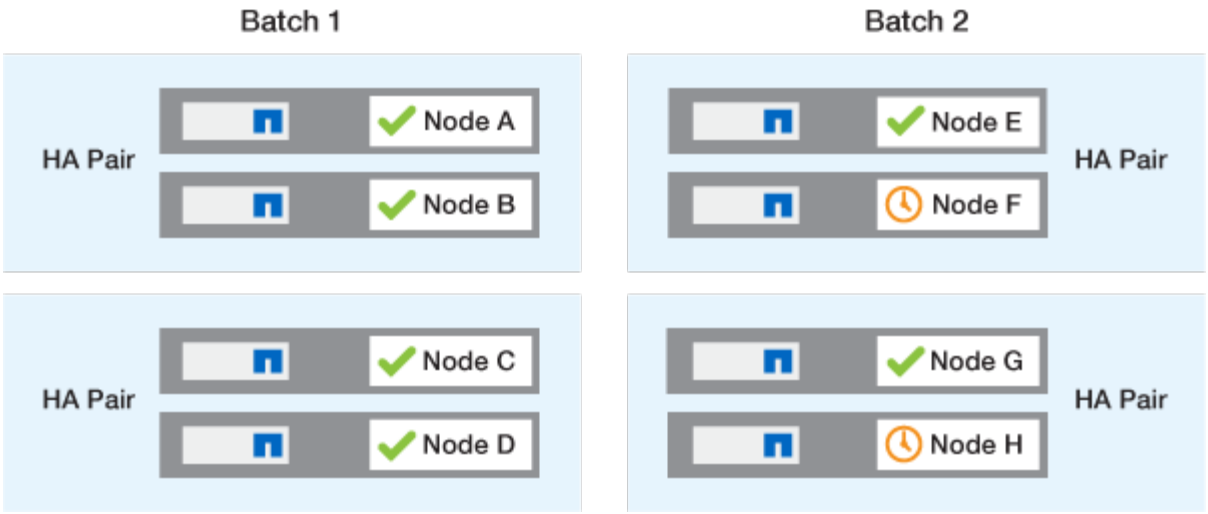
接著會針對批次 2 中的節點重複此程序；每個 HA 配對的第一個節點會與批次中所有其他 HA 配對的第一個節點同時升級。

在以下範例中、節點 E 和節點 G 會同時升級。



每個 HA 配對的第一個節點升級完成後、批次 2 中的合作夥伴節點會同時升級。

在下列範例中、節點 F 和節點 H 會同時升級、以完成批次升級程序。



根據組態建議的 **ONTAP** 升級方法

您的組態所支援的升級方法會依建議的使用順序列出。

組態	版本**ONTAP**	節點數	建議的升級方法
標準	9.0 或更新版本	2 個以上	• 使用System Manager自動不中斷營運 • 使用CLI自動不中斷營運
標準	9.0 或更新版本	單一	"自動化中斷"
MetroCluster	9.3 或更新版本	8.	• 使用CLI自動不中斷營運 • 使用 CLI 手動不中斷 4 或 8 節點 MetroCluster 的運作
MetroCluster	9.3 或更新版本	2、4.	• 使用System Manager自動不中斷營運 • 使用CLI自動不中斷營運
MetroCluster	9.2或更早版本	4、8.	使用 CLI 手動不中斷 4 或 8 節點 MetroCluster 的運作
MetroCluster	9.2或更早版本	2.	使用 CLI 手動不中斷 2 節點 MetroCluster 的運作

無論組態為何、我們都建議您使用系統管理員進行所有修補程式升級。

答 手動中斷升級 可在任何組態上執行。 不過、除非您可以在升級期間讓叢集離線、否則不應執行中斷升級。如果您是在SAN環境中運作、則應準備好在執行中斷升級之前、先關閉或暫停所有SAN用戶端。使用ONTAP 不中斷的CLI執行升級。

執行自動升級時、 ONTAP 會自動在每個節點上安裝目標 ONTAP 映像、驗證叢集是否可以成功升級、然後執行任一項 批次或循環升級 在背景中、根據叢集中的節點數量。

如果您的組態支援此功能、您應該使用 System Manager 來執行自動升級。 如果您的組態不支援使用系統管理員進行自動升級、您可以使用 ONTAP 命令列介面（ CLI ）來執行自動升級。

如果您透過NetApp升級至ONTAP 9.15.1 或更高版本，請依照"NetApp控制台文件中的升級流程"。

在自動不中斷升級（ andu ）開始之前修改命令選項的設定 `storage failover modify-auto-giveback`，不會影響升級程序。在更新所需的接管/恢復期間、andu程序會忽略此選項的任何預設值。例如，在開始之前設定 `-autogiveback`為 false ，則不會在恢復之前中斷自動升級。如"指令參考資料ONTAP"需詳細 `storage failover modify-auto-giveback`資訊，請參閱。

開始之前

- 您應該 "準備升級"。
- 您應該 "下載 ONTAP 軟體映像" 適用於您的目標 ONTAP 版本。

  如果您正在執行"直接多跳升級"，則需要下載您的特定所需的兩個 ONTAP 映像"升級途徑"。

- 對於每個HA配對、每個節點應在同一個廣播網域上有一個或多個連接埠。

  如果您的 ONTAP 叢集有 8 個以上的節點、則批次升級方法會用於自動不中斷升級、以便在 SFO 接管之前預先強制資料 LIF 移轉。 批次升級期間的生命體移轉方式會因您的 ONTAP 版本而異。

如果您執行的是 **ONTAP ...**	已移轉生命 **...**
• 9.15.1 或更新版本 • 9.14.1P5 • 9.13.1P10 • 9.12.1P13 • 9.11.1P16 、 P17 • 9.10.1 第 19 頁	至其他批次群組中的節點。 如果移轉至其他批次群組失敗、則會將生命移轉至同一個批次群組中節點的 HA 合作夥伴。
9.8 至 9.14.1	至其他批次群組中的節點。 如果網路廣播網域不允許 LIF 移轉至其他批次群組、 LIF 移轉會失敗、並暫停。
9.7 或更早版本	升級至節點的 HA 合作夥伴。 如果合作夥伴在同一個廣播網域中沒有任何連接埠、則 LIF 移轉會失敗、並暫停。

- 如果您要在 MetroCluster FC 組態中升級 ONTAP 、則應該啟用叢集、以便自動進行非計畫性切換。
- 如果您不打算監控升級程序的進度、您應該 "要求EMS通知可能需要手動介入的錯誤"。

- 如果您有單節點叢集、請遵循 "自動中斷升級" 流程。

  單節點叢集的升級會造成中斷。

範例 **3.** 步驟

系統管理員

1. 驗證 ONTAP 目標映像：

   如果您要升級 MetroCluster 組態、您應該驗證叢集 A 、然後在叢集 B 上重複驗證程序

   a. 視您執行的版本而定ONTAP 、請執行下列其中一個步驟：

如果您正在執行…	執行此動作…
部分9.8或更新版本ONTAP	按一下*叢集>總覽*。
S69.5、9.6及9.7 ONTAP	按一下*組態*>*叢集*>*更新*。
更新版本ONTAP	按一下「組態>*叢集更新*」。

   b. 在 **Overview** （總覽）窗格的右角，單擊 ⋮ 。

   c. 按一下* ONTAP 《更新*》。

   d. 在 * 叢集更新 * 索引標籤中、新增映像或選取可用的映像。

如果您想要…	然後…
從本機資料夾新增軟體映像 您應該已經擁有了 "已下載映像" 至本機用戶端。	i. 在 * 可用的軟體映像 * 下、按一下 * 從本機 * 新增。 ii. 瀏覽至儲存軟體映像的位置、選取映像、然後按一下*「Open*（開啟*）」。
從 HTTP 或 FTP 伺服器新增軟體映像	i. 按一下「從伺服器新增」。 ii. 在 * 新增軟體映像 * 對話方塊中、輸入您從 NetApp 支援網站 下載 ONTAP 軟體映像的 HTTP 或 FTP 伺服器 URL 。 對於匿名FTP、您必須在中指定URL ftp://anonymous@ftpserver 格式。 iii. 按一下「 * 新增 * 」。
選取可用的映像	選擇所列的其中一個影像。

   e. 按一下 * 驗證 * 以執行升級前驗證檢查。

   如果在驗證期間發現任何錯誤或警告、則會顯示這些錯誤或警告、並附上修正動作清單。您必須先解決所有錯誤、才能繼續升級。 最佳做法是也解決警告。

2. 單擊 * 下一步 * 。

3. 按一下 * 更新 * 。

   再次執行驗證。任何剩餘的錯誤或警告會連同修正行動清單一起顯示。 您必須先修正錯誤、才能繼續升級。 如果驗證過程中出現警告、請修正警告、或選擇 * 更新並顯示警告 * 。

   > 根據預設， ONTAP 會使用"批次升級程序"升級具有八個或更多節點的叢集。從 ONTAP 9.10.1 開始（如果願意），您可以選擇 * 一次更新一個 HA 對 * 來覆蓋默認值，並使用滾動升級過程一次升級一個 HA 對。

   對於節點超過 2 個的 MetroCluster 組態、 ONTAP 升級程序會在兩個站台的 HA 配對上同時開始。 對於雙節點 MetroCluster 組態、升級會先在未初始化升級的站台上啟動。第一次升級完成後、其餘站台的升級便會開始。

4. 如果升級因為錯誤而暫停、請按一下錯誤訊息以檢視詳細資料、然後修正錯誤和 "繼續升級"。

完成後

升級成功完成後、節點會重新開機、並將您重新導向至 System Manager 登入頁面。如果節點需要很長時間重新開機、您應該重新整理瀏覽器。

CLI

1. 驗證 ONTAP 目標軟體映像

   > 如果您要升級 MetroCluster 組態、您應該先在叢集 A 上執行下列步驟、然後在叢集 B 上執行相同的步驟

   a. 刪除先前ONTAP 的版本：

   ```
   cluster image package delete -version <previous_ONTAP_Version>
   ```

   b. 將目標 ONTAP 軟體映像載入叢集套件儲存庫：

   ```
   cluster image package get -url location
   ```

   ```
   cluster1::> cluster image package get -url
   http://www.example.com/software/9.13.1/image.tgz

   Package download completed.
   Package processing completed.
   ```

   如果您執行的"直接多跳升級"是、您也需要載入用於升級所需 ONTAP 中間版本的軟體套件。例如、如果您要從 9.8 升級至 9.13.1 、則需要載入 ONTAP 9.12.1 的軟體套件、然後使用相同的命令載入 9.13.1 的軟體套件。

   c. 驗證叢集套件儲存庫中是否有可用的軟體套件：

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.13.1             MM/DD/YYYY 10:32:15
```

d. 執行自動升級前檢查：

```
cluster image validate -version <package_version_number>
```

如果您執行"直接多跳升級"的是、則只需使用目標 ONTAP 套件進行驗證。您不需要個別驗證中間升級映像。例如、如果您要從 9.8 升級至 9.13.1 、請使用 9.13.1 套件進行驗證。您不需要個別驗證 9.12.1 套件。

```
cluster1::> cluster image validate -version 9.13.1

WARNING: There are additional manual upgrade validation checks that
must be performed after these automated validation checks have
completed...
```

a. 監控驗證進度：

```
cluster image show-update-progress
```

b. 完成驗證所識別的所有必要行動。

c. 如果您要升級 MetroCluster 組態、請在叢集 B 上重複上述步驟

2. 產生軟體升級預估：

```
cluster image update -version <package_version_number> -estimate
-only
```

如果您要升級 MetroCluster 組態、可以在叢集 A 或叢集 B 上執行此命令 您不需要在兩個叢集上執行。

軟體升級預估會顯示每個要更新元件的詳細資料、以及升級的預估期間。

3. 執行軟體升級：

```
cluster image update -version <package_version_number>
```

- 如果您要執行"直接多跳升級"、請將目標 ONTAP 版本用於 package_version_number 。例如、如果您要從 ONTAP 9.8 升級至 9.13.1 、請使用 9.13.1 做為 package_version_number 。
- 根據預設、 ONTAP 會使用 "批次升級程序" 升級具有八個或更多節點的叢集。 如有需要、您可以使用 `-force-rolling` 此參數可覆寫預設程序、並使用循環升級程序、讓叢集一次升級一個節點。
- 完成每次接管與恢復之後、升級會等待8分鐘、讓用戶端應用程式從接管與恢復期間發生的I/O暫停中恢復。如果您的環境需要更多或更少的時間來穩定用戶端、您可以使用 `-stabilize-minutes` 指定不同穩定時間量的參數。
- 如果 MetroCluster 組態的節點數量超過 4 個、則自動升級會在兩個站台的 HA 配對上同時開始。對於雙節點 MetroCluster 組態、升級會從未初始化升級的站台開始。第一次升級完成後、其餘站台的升級便會開始。

```
cluster1::> cluster image update -version 9.13.1

Starting validation for this update. Please wait..

It can take several minutes to complete validation...

WARNING: There are additional manual upgrade validation checks...

Pre-update Check      Status     Error-Action
--------------------- ----------
-------------------------------------------
...
20 entries were displayed

Would you like to proceed with update ? {y|n}: y
Starting update...

cluster-1::>
```

4. 顯示叢集更新進度：

```
cluster image show-update-progress
```

如果您要升級 4 節點或 8 節點 MetroCluster 組態、請使用 `cluster image show-update-progress` 命令只會顯示您執行命令所在節點的進度。您必須在每個節點上執行命令、才能查看個別節點的進度。

5. 驗證是否已在每個節點上成功完成升級。

```
cluster image show-update-progress
```

```
cluster1::> cluster image show-update-progress

                                            Estimated
Elapsed
Update Phase         Status                  Duration
Duration
-------------------- ----------------- --------------
--------------
Pre-update checks    completed               00:10:00
00:02:07
Data ONTAP updates   completed               01:31:00
01:39:00
Post-update checks   completed               00:10:00
00:02:00
3 entries were displayed.

Updated nodes: node0, node1.
```

6. 觸發AutoSupport 功能不支援通知：

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

如果您的叢集未設定為傳送AutoSupport 功能性訊息、則會在本機儲存通知複本。

7. 如果您要升級雙節點 MetroCluster FC 組態、請確認叢集已啟用以進行自動非計畫性切換。

> 如果您要升級的是 2 個以上節點的標準組態、 MetroCluster IP 組態或 MetroCluster FC 組態、則不需要執行此步驟。

a. 檢查是否已啟用自動非計畫性切換：

```
metrocluster show
```

如果啟用自動非計畫性切換、命令輸出中會出現下列陳述：

```
AUSO Failure Domain    auso-on-cluster-disaster
```

a. 如果輸出中未顯示該陳述、請啟用自動非計畫性切換：

```
metrocluster modify -auto-switchover-failure-domain auso-on-
cluster-disaster
```

b. 確認已啟用自動非計畫性切換：

```
metrocluster show
```

在自動升級程序發生錯誤之後繼續 **ONTAP** 軟體升級

如果自動 ONTAP 軟體升級因錯誤而暫停、您應該解決此錯誤、然後繼續升級。 解決錯誤之後、您可以選擇繼續自動升級程序、或手動完成升級程序。如果您選擇繼續自動升級、請勿手動執行任何升級步驟。

範例 **4.** 步驟

系統管理員

1. 視您執行的版本而定ONTAP 、請執行下列其中一個步驟：

如果您正在執行…	然後…
部分9.8或更新版本ONTAP	按一下 * 叢集 * > * 總覽 *
ONTAP 9.7 、 9.6 或 9.5	按一下*組態*>*叢集*>*更新*。
更新版本ONTAP	• 按一下「組態>*叢集更新*」。 • 在 * 總覽 * 窗格的右角、按一下三個藍色垂直點、然後選取 * ONTAP Update* 。

2. 繼續自動升級或取消升級、然後手動繼續。

如果您想要…	然後…
繼續自動升級	按一下*恢復*。
取消自動升級並手動繼續	按一下*取消*。

CLI

1. 檢視升級錯誤：

```
cluster image show-update-progress
```

2. 解決錯誤。
3. 繼續升級：

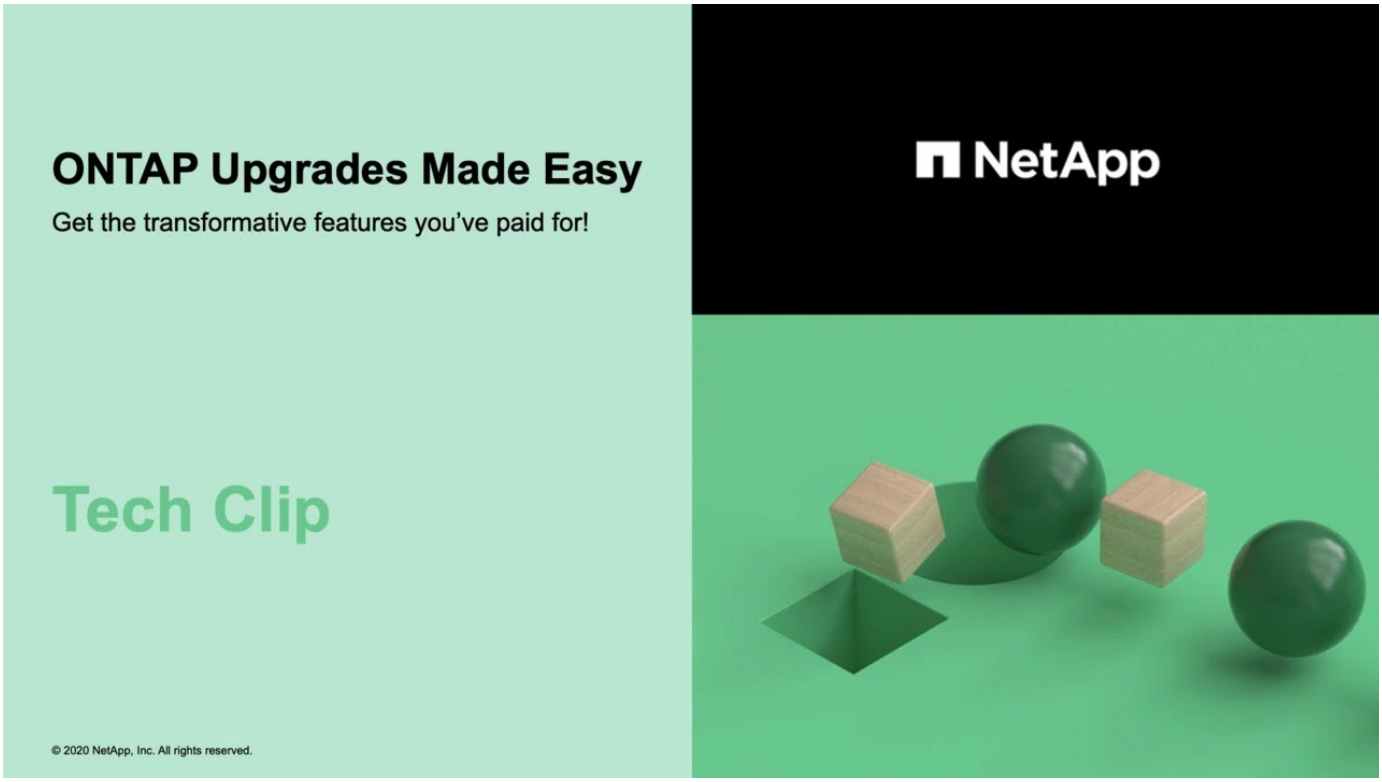
如果您想要…	輸入下列命令…
繼續自動升級	`cluster image resume-update`
取消自動升級並手動繼續	`cluster image cancel-update`

完成後

"執行升級後檢查"。

影片：輕鬆升級

請參閱ONTAP 《System Manager》ONTAP 中的簡化版《系統管理程式》（NetApp）。



相關資訊

- "啟動 Active IQ 數位顧問"
- "Active IQ Digital Advisor 數位顧問文件"
- "叢集映像"
- "AutoSupport 叫用"
- "MetroCluster"

手動升級

安裝 **ONTAP** 軟體套件以進行手動升級

下載 ONTAP 軟體套件以進行手動升級後、您必須先在本機安裝、才能開始升級。

步驟

1. 將權限等級設為「進階」、在提示繼續時輸入 * y* ： `set -privilege advanced`

   進階提示 (`*>`) 。

2. 安裝映像。

如果您有下列組態 ...	使用此命令...
• 非 MetroCluster • 雙節點 MetroCluster	`system node image update -node * -package <location> -replace -package true -setdefault true -background true` <location> 可以是 Web 伺服器或本機資料夾、視 ONTAP 版本而定。如"指令參考資料ONTAP"需詳細 `system node image update`資訊，請參閱。 此命令會同時在所有節點上安裝軟體映像。若要一次在每個節點上安裝映像、請勿指定 -background 參數。
• 4 節點 MetroCluster • 8 節點 MetroCluster 組態	`system node image update -node * -package <location> -replace -package true -background true -setdefault false` 您必須在兩個叢集上發出此命令。 此命令會使用延伸查詢來變更目標軟體映像、此映像會安裝為每個節點的替代映像。

3. 輸入 `y` 以在出現提示時繼續。
4. 確認軟體映像已安裝在每個節點上。

```
system node image show-update-progress -node *
```

此命令會顯示軟體映像安裝的目前狀態。您應該繼續執行此命令、直到所有節點回報*執行狀態退出、*退出狀態*成功*為止。

系統節點映像更新命令可能會失敗、並顯示錯誤或警告訊息。解決任何錯誤或警告之後、您可以再次執行命令。

此範例顯示兩節點叢集、其中軟體映像已成功安裝在兩個節點上：

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

使用 **CLI** 手動進行不中斷的 **ONTAP** 升級（標準組態）

使用 System Manager 自動升級是首選的升級方法。 如果系統管理員不支援您的組態、您可以使用 ONTAP 命令列介面（ CLI ）來執行手動不中斷的升級。 若要使用手動不中斷的方法升級兩個或多個節點的叢集、您必須在HA配對中的每個節點上啟動容錯移轉作業、更新「失敗」節點、啟動還原、然後針對叢集中的每個HA配對重複此程序。

開始之前

您必須已滿意升級 "準備" 要求。

更新**HA**配對中的第一個節點

您可以啟動節點合作夥伴的接管、以更新HA配對中的第一個節點。當第一個節點升級時、合作夥伴會提供節點的資料。

如果您要執行重大升級、第一個要升級的節點必須與您設定外部連線資料生命期的節點相同、並安裝第一個ONTAP 版本的圖片。

升級第一個節點之後、您應該盡快升級合作夥伴節點。請勿讓兩個節點留在中 "混合版本" 狀態時間超過所需時間。

步驟

1. 透過調用 AutoSupport 訊息來更新叢集中的第一個節點：

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

本資訊通知包含更新前的系統狀態記錄。AutoSupport如果更新程序發生問題、它會儲存有用的疑難排解資訊。

如果叢集未設定為傳送AutoSupport 功能性訊息、則會在本機儲存通知複本。

2. 將權限等級設為「進階」、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

3. 將新的 ONTAP 軟體映像設為預設映像：

```
system image modify {-node nodenameA -iscurrent false} -isdefault true
```

系統映像修改命令會使用延伸查詢、將新ONTAP 的更新版軟體映像（安裝為替代映像）變更為節點的預設映像。

4. 監控更新進度：

```
system node upgrade-revert show
```

5. 確認新的 ONTAP 軟體映像已設為預設映像：

```
system image show
```

在下列範例中、image2是新ONTAP 的版本、並設為節點0上的預設映像：

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ---------- -------------------
node0
         image1   false   true    X.X.X      MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y      MM/DD/YYYY TIME
node1
         image1   true    true    X.X.X      MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

6. 如果合作夥伴節點已啟用自動恢復功能、請停用該功能：

```
storage failover modify -node nodenameB -auto-giveback false
```

如果叢集是雙節點叢集、則會顯示一則訊息、警告您停用自動恢復功能、可在發生其他故障情況時、防止管理叢集服務上線。輸入 `y` 以繼續。

7. 確認已停用節點合作夥伴的自動恢復功能：

```
storage failover show -node nodenameB -fields auto-giveback
```

```
cluster1::> storage failover show -node node1 -fields auto-giveback
node     auto-giveback
-------- -------------
node1    false
1 entry was displayed.
```

8. 執行下列命令兩次、以判斷要更新的節點目前是否正在服務任何用戶端

```
system node run -node nodenameA -command uptime
```

正常運作時間命令會顯示節點自上次開機以來、針對NFS、SMB、FC和iSCSI用戶端執行的作業總數。對於每個傳輸協定、您必須執行兩次命令、以判斷作業計數是否增加。如果數量不斷增加、則節點目前正在為該傳輸協定的用戶端提供服務。如果不增加、則節點目前不會為該傳輸協定的用戶端提供服務。

您應該記下每個增加用戶端作業的傳輸協定、以便在節點更新之後、您可以確認用戶端流量已恢復。

以下範例顯示一個節點、其執行NFS、SMB、FC和iSCSI作業。不過、節點目前僅提供NFS和iSCSI用戶端服務。

```
cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node0 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

9. 將所有資料生命從節點移轉至其他位置：

```
network interface migrate-all -node nodenameA
```

10. 驗證您移轉的任何生命：

```
network interface show
```

深入瞭解 `network interface show`和參數"指令參考資料ONTAP"，您可以使用這些參數來驗證中的 LIF 狀態。

以下範例顯示node0的資料lifs已成功移轉。對於每個LIF、本範例中所包含的欄位可讓您驗證LIF的主節點和連接埠、LIF移轉的目前節點和連接埠、以及LIF的作業和管理狀態。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node0 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node0     e0a       node1     e0a       up          up
vs0     data002 node0     e0b       node1     e0b       up          up
vs0     data003 node0     e0b       node1     e0b       up          up
vs0     data004 node0     e0a       node1     e0a       up          up
4 entries were displayed.
```

11. 啟動接管：

```
storage failover takeover -ofnode nodenameA
```

請勿指定-option Immediate參數、因為要將節點接管以開機至新的軟體映像時、需要正常接管。如果您未手動將I生命 從節點移轉至其他節點、則會自動移轉至節點的HA合作夥伴、以確保不會發生服務中斷。

第一個節點會開機、直到等待恢復狀態。

如果啟用 AutoSupport 、則會傳送一則 AutoSupport 訊息、指出節點已超出叢集仲裁。您可以忽略此通知並繼續更新。

12. 確認接管成功：

```
storage failover show
```

您可能會看到錯誤訊息、指出版本不相符和信箱格式問題。這是預期的行為、在重大且不中斷營運的升級中、這是暫時性的狀態、而且不會造成傷害。

以下範例顯示接管作業成功。節點節點0處於等待恢復狀態、其合作夥伴處於接管狀態。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        Waiting for giveback (HA
mailboxes)
node1          node0          false    In takeover
2 entries were displayed.
```

13. 至少等待八分鐘、讓下列情況生效：
    - 用戶端多重路徑（若已部署）會穩定下來。
    - 在接管期間執行I/O作業時、用戶端會從暫停狀態中恢復。

      還原時間是用戶端特有的、可能需要八分鐘以上的時間、視用戶端應用程式的特性而定。

14. 將集合體傳回第一個節點：

```
storage failover giveback -ofnode nodenameA
```

恢復會先將根Aggregate傳回合作夥伴節點、然後在該節點完成開機之後、傳回非根Aggregate及任何設定為自動還原的LIF。新開機的節點會在傳回Aggregate後、立即開始從每個Aggregate向用戶端提供資料。

15. 驗證是否已傳回所有的集合體：

```
storage failover show-giveback
```

如果「歸還狀態」欄位指出沒有要歸還的集合體、則會傳回所有集合體。如果恢復被否決、命令會顯示恢復進度、以及哪個子系統已對恢復執行了指令。

16. 如果尚未傳回任何Aggregate、請執行下列步驟：
    a. 請檢閱「否決因應措施」、以判斷您是否想要處理「『直接』條件、或是要撤銷「否決」。
    b. 如有必要、請解決錯誤訊息中所述的「『驗證』條件、確保所有已識別的作業都能正常終止。
    c. 重新運行 `storage failover giveback`命令。

       如果您決定覆寫「vito'」條件、請將-overre-etoes參數設為true。

17. 至少等待八分鐘、讓下列情況生效：
    - 用戶端多重路徑（若已部署）會穩定下來。
    - 用戶端會從還原期間執行的I/O作業暫停中恢復。

      還原時間是用戶端特有的、可能需要八分鐘以上的時間、視用戶端應用程式的特性而定。

18. 驗證是否已成功完成節點的更新：

    a. 進入進階權限等級：

    ```
    set -privilege advanced
    ```

    b. 確認節點的更新狀態為完成：

    ```
    system node upgrade-revert show -node nodenameA
    ```

    狀態應列示為「完成」。

    如果狀態不完整、請聯絡技術支援部門。

    a. 返回管理權限層級：

    ```
    set -privilege admin
    ```

19. 驗證節點的連接埠是否正常運作：

    ```
    network port show -node nodenameA
    ```

    您必須在升級至ONTAP 更新版本的更新版本的節點上執行此命令。

    下列範例顯示節點的所有連接埠都已啟動：

    ```
    cluster1::> network port show -node node0
                                                                   Speed
    (Mbps)
    Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
    ------ --------- ------------ ---------------- ----- -------
    ------------
    node0
           e0M       Default      -                up       1500  auto/100
           e0a       Default      -                up       1500  auto/1000
           e0b       Default      -                up       1500  auto/1000
           e1a       Cluster      Cluster          up       9000  auto/10000
           e1b       Cluster      Cluster          up       9000  auto/10000
    5 entries were displayed.
    ```

20. 將生命恢復到節點：

```
network interface revert *
```

此命令會傳回從節點移轉的LIF。

```
cluster1::> network interface revert *
8 entries were acted on.
```

21. 驗證節點的資料生命是否已成功還原至節點、以及它們是否正常運作：

```
network interface show
```

下列範例顯示節點所主控的所有資料生命期已成功還原至節點、而且其作業狀態為「up」（開機）：

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0         e0a
true
            data002      up/up    192.0.2.121/24     node0         e0b
true
            data003      up/up    192.0.2.122/24     node0         e0b
true
            data004      up/up    192.0.2.123/24     node0         e0a
true
4 entries were displayed.
```

22. 如果您先前已確定此節點為用戶端提供服務、請確認節點為其先前所服務的每個傳輸協定提供服務：

```
system node run -node nodenameA -command uptime
```

更新期間、作業數會重設為零。

下列範例顯示更新的節點已恢復為其NFS和iSCSI用戶端提供服務：

```
cluster1::> system node run -node node0 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

23. 如果合作夥伴節點先前已停用、請重新啟用自動恢復功能：

```
storage failover modify -node nodenameB -auto-giveback true
```

您應該盡快更新節點的HA合作夥伴。如果您因為任何原因必須暫停更新程序、HA配對中的兩個節點都應該執行相同ONTAP 的版本。

更新**HA**配對中的合作夥伴節點

更新HA配對中的第一個節點之後、您可以在其上啟動接管、藉此更新其合作夥伴。第一個節點會在合作夥伴節點升級時、為合作夥伴的資料提供服務。

1. 將權限等級設為「進階」、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

2. 將新的 ONTAP 軟體映像設為預設映像：

```
system image modify {-node nodenameB -iscurrent false} -isdefault true
```

系統映像修改命令會使用延伸查詢、將新ONTAP 的Imagesoftware映像（安裝為替代映像）變更為節點的預設映像。

3. 監控更新進度：

```
system node upgrade-revert show
```

4. 確認新的 ONTAP 軟體映像已設為預設映像：

```
system image show
```

在下列範例中、 `image2` 是 ONTAP 的新版本、設定為節點上的預設映像：

```
cluster1::*> system image show
                  Is      Is                 Install
Node      Image   Default Current Version    Date
--------- ------- ------- ------- ---------- ------------------
node0
          image1  false   false   X.X.X      MM/DD/YYYY TIME
          image2  true    true    Y.Y.Y      MM/DD/YYYY TIME
node1
          image1  false   true    X.X.X      MM/DD/YYYY TIME
          image2  true    false   Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.
```

5. 如果合作夥伴節點已啟用自動恢復功能、請停用該功能：

```
storage failover modify -node nodenameA -auto-giveback false
```

如果叢集是雙節點叢集、則會顯示一則訊息、警告您停用自動恢復功能、可在發生其他故障情況時、防止管理叢集服務上線。輸入 `y` 以繼續。

6. 確認已停用合作夥伴節點的自動恢復功能：

```
storage failover show -node nodenameA -fields auto-giveback
```

```
cluster1::> storage failover show -node node0 -fields auto-giveback
node      auto-giveback
--------- -------------
node0     false
1 entry was displayed.
```

7. 執行下列命令兩次、判斷要更新的節點目前是否正在服務任何用戶端：

```
system node run -node nodenameB -command uptime
```

正常運作時間命令會顯示節點自上次開機以來、針對NFS、SMB、FC和iSCSI用戶端執行的作業總數。對於每個傳輸協定、您必須執行兩次命令、以判斷作業計數是否增加。如果數量不斷增加、則節點目前正在為該傳輸協定的用戶端提供服務。如果不增加、則節點目前不會為該傳輸協定的用戶端提供服務。

> ⓘ 您應該記下每個增加用戶端作業的傳輸協定、以便在節點更新之後、您可以確認用戶端流量已恢復。

以下範例顯示一個節點、其執行NFS、SMB、FC和iSCSI作業。不過、節點目前僅提供NFS和iSCSI用戶端服務。

```
cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

cluster1::> system node run -node node1 -command uptime
  2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

8. 將所有資料生命從節點移轉至其他位置：

```
network interface migrate-all -node nodenameB
```

9. 確認您移轉的任何生命的狀態：

```
network interface show
```

深入瞭解 `network interface show`和參數"指令參考資料ONTAP"，您可以使用這些參數來驗證中的 LIF 狀態。

以下範例顯示節點1的資料生命量已成功移轉。對於每個LIF、本範例中所包含的欄位可讓您驗證LIF的主節點和連接埠、LIF移轉的目前節點和連接埠、以及LIF的作業和管理狀態。

```
cluster1::> network interface show -data-protocol nfs|cifs -role data
-home-node node1 -fields home-node,curr-node,curr-port,home-port,status-
admin,status-oper
vserver lif     home-node home-port curr-node curr-port status-oper
status-admin
------- ------- --------- --------- --------- --------- -----------
------------
vs0     data001 node1     e0a       node0     e0a       up          up
vs0     data002 node1     e0b       node0     e0b       up          up
vs0     data003 node1     e0b       node0     e0b       up          up
vs0     data004 node1     e0a       node0     e0a       up          up
4 entries were displayed.
```

10. 啟動接管：

```
storage failover takeover -ofnode nodenameB -option allow-version-
mismatch
```

請勿指定-option Immediate參數、因為要將節點接管以開機至新的軟體映像時、需要正常接管。如果您未手動將I生命 從節點移轉至其他節點、則會自動移轉至節點的HA合作夥伴、以避免服務中斷。

畫面會顯示警告。 您必須輸入 `y` 以繼續。

接管的節點會開機至等待恢復狀態。

> 如果啟用 AutoSupport 、則會傳送一則 AutoSupport 訊息、指出節點已超出叢集仲裁。您可以忽略此通知並繼續更新。

11. 確認接管成功：

```
storage failover show
```

以下範例顯示接管作業成功。節點節點1處於等待恢復狀態、其合作夥伴處於接管狀態。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node0          node1          -        In takeover
node1          node0          false    Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

12. 至少等待八分鐘、讓下列情況生效：

+
用戶端多重路徑（若已部署）會穩定下來。
用戶端會從接管期間發生的I/O暫停中恢復。

+
還原時間是用戶端專屬的、可能需要八分鐘以上的時間、視用戶端應用程式的特性而定。

13. 將集合體傳回合作夥伴節點：

```
storage failover giveback -ofnode nodenameB
```

恢復作業會先將根Aggregate傳回合作夥伴節點、然後在該節點完成開機之後、傳回非根Aggregate及任何設定為自動還原的LIF。新開機的節點會在傳回Aggregate後、立即開始從每個Aggregate向用戶端提供資料。

14. 驗證是否已傳回所有的集合體：

```
storage failover show-giveback
```

如果「歸還狀態」欄位指出沒有要歸還的集合體、則會傳回所有集合體。如果恢復被否決、命令會顯示恢復

進度、以及哪些子系統已對恢復作業進行了否決。

15. 如果未傳回任何集合體、請執行下列步驟：
    a. 請檢閱「否決因應措施」、以判斷您是否想要處理「『直接』條件、或是要撤銷「否決」。
    b. 如有必要、請解決錯誤訊息中所述的「『驗證』條件、確保所有已識別的作業都能正常終止。
    c. 重新運行 `storage failover giveback`命令。

       如果您決定覆寫「vito'」條件、請將-overre-etoes參數設為true。

16. 至少等待八分鐘、讓下列情況生效：
    - 用戶端多重路徑（若已部署）會穩定下來。
    - 用戶端會從還原期間執行的I/O作業暫停中恢復。

      還原時間是用戶端特有的、可能需要八分鐘以上的時間、視用戶端應用程式的特性而定。

17. 驗證是否已成功完成節點的更新：
    a. 進入進階權限等級：

       ```
       set -privilege advanced
       ```

    b. 確認節點的更新狀態為完成：

       ```
       system node upgrade-revert show -node nodenameB
       ```

       狀態應列示為「完成」。

    如果狀態未完成、請從節點執行 `system node upgrade-revert upgrade` 命令。如果命令未完成更新、請聯絡技術支援部門。

    a. 返回管理權限層級：

       ```
       set -privilege admin
       ```

18. 驗證節點的連接埠是否正常運作：

    ```
    network port show -node nodenameB
    ```

    您必須在已升級ONTAP 至flex9.4的節點上執行此命令。

    下列範例顯示節點的所有資料連接埠都已啟動：

```
cluster1::> network port show -node node1
                                                                        Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
node1
       e0M       Default      -                up       1500  auto/100
       e0a       Default      -                up       1500  auto/1000
       e0b       Default      -                up       1500  auto/1000
       e1a       Cluster      Cluster          up       9000  auto/10000
       e1b       Cluster      Cluster          up       9000  auto/10000
5 entries were displayed.
```

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

19. 將生命恢復到節點：

```
network interface revert *
```

此命令會傳回從節點移轉的LIF。

```
cluster1::> network interface revert *
8 entries were acted on.
```

20. 驗證節點的資料生命是否已成功還原至節點、以及它們是否正常運作：

```
network interface show
```

以下範例顯示、節點所主控的所有資料生命期都會成功還原回節點、而且其作業狀態為「up」（開機）：

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node1         e0a
true
            data002      up/up    192.0.2.121/24     node1         e0b
true
            data003      up/up    192.0.2.122/24     node1         e0b
true
            data004      up/up    192.0.2.123/24     node1         e0a
true
4 entries were displayed.
```

21. 如果您先前已確定此節點為用戶端提供服務、請確認節點為其先前所服務的每個傳輸協定提供服務：

```
system node run -node nodenameB -command uptime
```

更新期間、作業數會重設為零。

下列範例顯示更新的節點已恢復為其NFS和iSCSI用戶端提供服務：

```
cluster1::> system node run -node node1 -command uptime
  3:15pm up  0 days, 0:16 129 NFS ops, 0 CIFS ops, 0 HTTP ops, 0 FCP
ops, 2 iSCSI ops
```

22. 如果這是要更新叢集中的最後一個節點、請觸發 AutoSupport 通知：

```
autosupport invoke -node * -type all -message "Finishing_NDU"
```

本資訊通知包含更新前的系統狀態記錄。AutoSupport如果更新程序發生問題、它會儲存有用的疑難排解資訊。

如果叢集未設定為傳送AutoSupport 功能性訊息、則會在本機儲存通知複本。

23. 確認新的 ONTAP 軟體正在 HA 配對的兩個節點上執行：

```
set -privilege advanced
```

```
system node image show
```

在下列範例中、image2是ONTAP 更新版的支援功能、是兩個節點上的預設版本：

```
cluster1::*> system node image show
                  Is      Is                    Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   false   X.X.X     MM/DD/YYYY TIME
         image2   true    true    Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

24. 如果合作夥伴節點先前已停用、請重新啟用自動恢復功能：

```
storage failover modify -node nodenameA -auto-giveback true
```

25. 使用驗證叢集是否已達到仲裁、以及是否正在執行服務 `cluster show` 和 `cluster ring show` （進階權限等級）命令。

    在升級任何其他HA配對之前、您必須先執行此步驟。

    深入瞭解 `cluster show`及 `cluster ring show` "指令參考資料ONTAP"。

26. 返回管理權限層級：

```
set -privilege admin
```

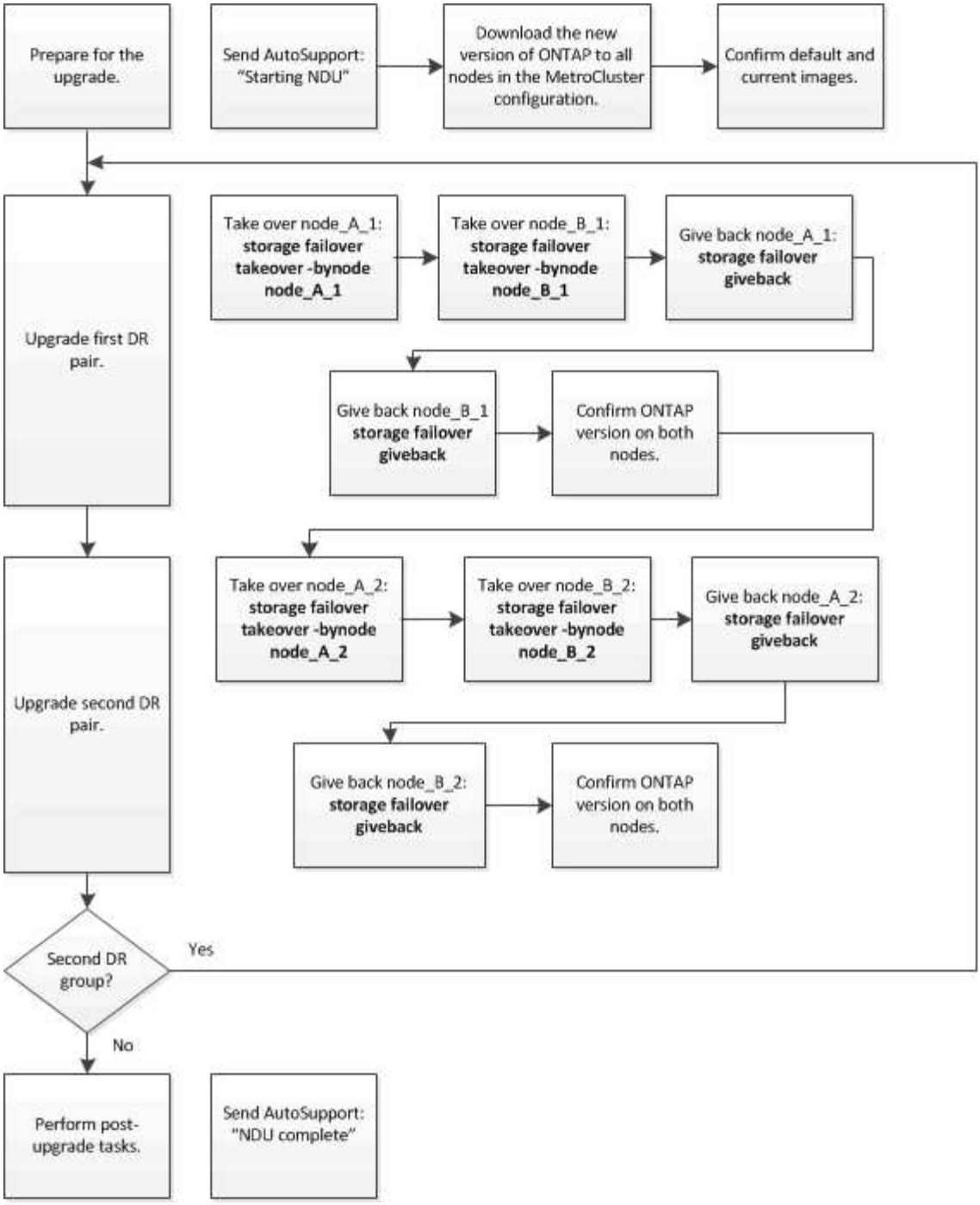
27. 升級任何其他HA配對。

相關資訊

- "AutoSupport 叫用"
- "系統映像"
- "系統節點"
- "儲存設備容錯移轉"
- "網路介面"
- "網路連接埠顯示"
- "設定權限進階"

手動升級四個或八個節點的 MetroCluster 組態、包括準備更新、同時更新一或兩個 DR 群組中的每個 DR 配對、以及執行升級後的工作。

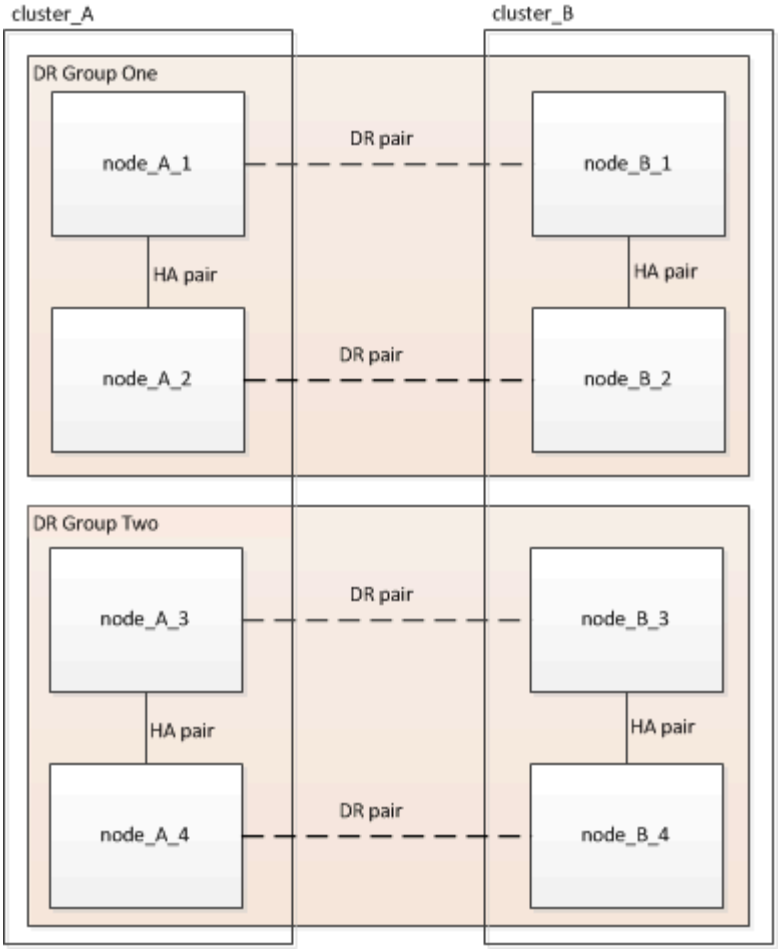
- 此工作適用於下列組態：
  - 執行不含更新版本的4節點MetroCluster 的不含功能的FC或IP組態ONTAP
  - 八節點MetroCluster 的不ONTAP 受限於任何版本的不受影響的不受限的FFC組態
- 如果您有雙節點MetroCluster 的不全功能組態、請勿使用此程序。
- 下列工作是指ONTAP 舊版和新版的《不一樣》。
  - 升級時、舊版ONTAP 是舊版的版次、版本編號比新版ONTAP 的版次低。
  - 降級時、舊版本ONTAP 是更新版本的版次、版本編號比ONTAP 新版的版次更高。
- 此工作使用下列高層級工作流程：



在八節點或四節點 **MetroCluster** 組態上更新 **ONTAP** 軟體時的差異

MetroCluster 軟體升級程序會因 MetroCluster 組態中有八個或四個節點而異。

一個由一或兩個DR群組所組成的支援組態。MetroCluster每個DR群組包含兩個HA配對、每MetroCluster個VMware叢集各一個HA配對。八節點MetroCluster 的功能不全包含兩個DR群組：



您一次升級一個 DR 群組。

對於四節點**MetroCluster** 的不完整組態：

1. 升級 DR Group One ：
   a. 升級 node_a_1 和 node_B_1 。
   b. 升級 node_a_2 和 node_B_2 。

對於八節點 **MetroCluster** 組態、您可以執行 **DR** 群組升級程序兩次：

1. 升級 DR Group One ：
   a. 升級 node_a_1 和 node_B_1 。
   b. 升級 node_a_2 和 node_B_2 。
2. 升級 DR 群組二：
   a. 升級 node_a_3 和 node_B_3 。
   b. 升級 node_a_4 和 node_B_4 。

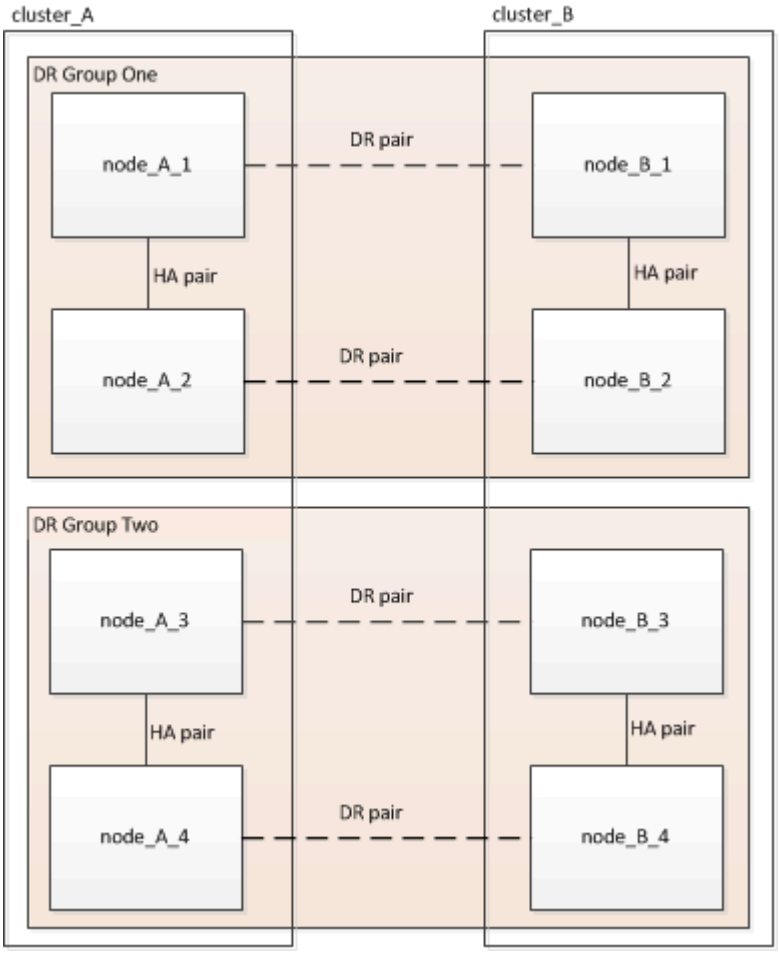
準備升級 **MetroCluster DR** 群組

在節點上升級 ONTAP 軟體之前、您必須先識別節點之間的 DR 關係、傳送一則 AutoSupport 訊息、告知您正在初始化升級、並確認每個節點上執行的 ONTAP 版本。

您必須擁有 "已下載" 和 "已安裝" 軟體映像。

此工作必須在每個DR群組上重複執行。如果這個支援功能組態由八個節點組成、則有兩個DR群組。MetroCluster因此、此工作必須在每個DR群組上重複執行。

本工作所提供的範例使用下圖所示的名稱來識別叢集和節點：



1. 識別組態中的 DR 配對：

```
metrocluster node show -fields dr-partner
```

```
cluster_A::> metrocluster node show -fields dr-partner
  (metrocluster node show)
dr-group-id cluster     node       dr-partner
----------- -------     --------   ----------
1           cluster_A   node_A_1   node_B_1
1           cluster_A   node_A_2   node_B_2
1           cluster_B   node_B_1   node_A_1
1           cluster_B   node_B_2   node_A_2
4 entries were displayed.

cluster_A::>
```

2. 將權限等級從 admin 設定為進階、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

3. 確認叢集 A 上的 ONTAP 版本：

```
system image show
```

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- -------   -------------------
node_A_1
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
node_A_2
         image1   true    true    X.X.X     MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

4. 確認叢集 B 上的版本：

```
system image show
```

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- -------     -------------------
node_B_1
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node_B_2
         image1   true    true    X.X.X       MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.

cluster_B::>
```

5. 觸發AutoSupport 功能不支援通知：

```
autosupport invoke -node * -type all -message "Starting_NDU"
```

此 AutoSupport 通知包含升級前的系統狀態記錄。如果升級程序發生問題、它會儲存實用的疑難排解資訊。

如果您的叢集未設定為傳送AutoSupport 功能性訊息、則通知複本會儲存在本機。

6. 針對第一組中的每個節點、將目標 ONTAP 軟體映像設為預設映像：

```
system image modify {-node nodename -iscurrent false} -isdefault true
```

此命令會使用延伸查詢、將安裝為替代映像的目標軟體映像變更為節點的預設映像。

7. 確認目標 ONTAP 軟體映像已設為叢集 A 上的預設映像：

```
system image show
```

在下列範例中、image2是新ONTAP 的版本、並在第一組的每個節點上設為預設影像：

```
cluster_A::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  -------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true   false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

a. 確認目標 ONTAP 軟體映像已設為叢集 B 上的預設映像：

```
system image show
```

下列範例顯示、目標版本已設定為第一組中每個節點的預設映像：

```
cluster_B::*> system image show
                  Is      Is               Install
Node     Image    Default Current Version  Date
-------- -------  ------- ------- -------  -------------------
node_A_1
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/YY/YYYY TIME
node_A_2
         image1   false   true    X.X.X    MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y    MM/DD/YYYY TIME

2 entries were displayed.
```

8. 確定要升級的節點目前是否為每個節點提供兩次任何用戶端服務：

```
system node run -node target-node -command uptime
```

正常運作時間命令會顯示節點自上次開機以來、針對NFS、CIFS、FC和iSCSI用戶端執行的作業總數。對於每個傳輸協定、您需要執行兩次命令、以判斷作業數是否增加。如果數量不斷增加、則節點目前正在為該傳輸協定的用戶端提供服務。如果不增加、則節點目前不會為該傳輸協定的用戶端提供服務。

ⓘ 您應該記下每個增加用戶端作業的傳輸協定、以便在節點升級之後、您可以確認用戶端流量已恢復。

此範例顯示具有NFS、CIFS、FC和iSCSI作業的節點。不過、節點目前僅提供NFS和iSCSI用戶端服務。

```
 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:16 800000260 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32810 iSCSI ops

 cluster_x::> system node run -node node0 -command uptime
   2:58pm up  7 days, 19:17 800001573 NFS ops, 1017333 CIFS ops, 0 HTTP
ops, 40395 FCP ops, 32815 iSCSI ops
```

更新**MetroCluster** 不只一個**DR**群組的第一個**DR**配對

您必須以正確順序執行節點的接管和恢復、才能使ONTAP 節點的新版本成為節點的目前版本。

所有節點都必須執行舊版ONTAP 的功能。

在此工作中、 node_a_1 和 node_B_1 會升級。

如果您已在第一個 DR 群組上升級 ONTAP 軟體、並正在八節點 MetroCluster 組態中升級第二個 DR 群組、則在此工作中、您將會更新 node_a_3 和 node_B_3 。

1. 如果MetroCluster 啟用了《斷電器軟體》、請將其停用。
2. 針對 HA 配對中的每個節點、停用自動恢復：

   ```
   storage failover modify -node target-node -auto-giveback false
   ```

   此命令必須針對HA配對中的每個節點重複執行。

3. 確認已停用自動恢復：

   ```
   storage failover show -fields auto-giveback
   ```

   此範例顯示兩個節點上的自動恢復功能均已停用：

   ```
   cluster_x::> storage failover show -fields auto-giveback
   node     auto-giveback
   -------- -------------
   node_x_1 false
   node_x_2 false
   2 entries were displayed.
   ```

4. 確保每個控制器的 I/O 不超過約 50% 、而且每個控制器的 CPU 使用率不超過約 50% 。
5. 啟動叢集A上目標節點的接管：

請勿指定-option Immediate參數、因為要重新啟動至新軟體映像的節點需要正常接管。

a. 接管叢集 A （ node_a_1 ）上的 DR 合作夥伴：

```
storage failover takeover -ofnode node_A_1
```

節點會開機至「等待恢復」狀態。

> 如果啟用了「支援」、則會傳送一則消息「不支援」、指出節點已超出叢集仲裁。AutoSupport AutoSupport您可以忽略此通知並繼續升級。

b. 確認接管成功：

```
storage failover show
```

以下範例顯示接管作業成功。node_a_1處於「等待恢復」狀態、node_a_2則處於「接管」狀態。

```
 cluster1::> storage failover show
                                Takeover
 Node           Partner        Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_A_1       node_A_2       -        Waiting for giveback (HA
mailboxes)
 node_A_2       node_A_1       false    In takeover
 2 entries were displayed.
```

6. 接管叢集B（node_B_1）上的DR合作夥伴：

請勿指定-option Immediate參數、因為要重新啟動至新軟體映像的節點需要正常接管。

a. 接管 node_B_1 ：

```
storage failover takeover -ofnode node_B_1
```

節點會開機至「等待恢復」狀態。

> 如果啟用了「支援」、則會傳送一則消息「不支援」、指出節點已超出叢集仲裁。AutoSupport AutoSupport您可以忽略此通知並繼續升級。

b. 確認接管成功：

```
storage failover show
```

以下範例顯示接管作業成功。node_B_1處於「等待恢復」狀態、node_B_2則處於「接管」狀態。

```
 cluster1::> storage failover show
                                 Takeover
 Node           Partner         Possible State Description
 -------------- -------------- --------
-------------------------------------
 node_B_1       node_B_2       -        Waiting for giveback (HA
mailboxes)
 node_B_2       node_B_1       false    In takeover
 2 entries were displayed.
```

7. 至少等待八分鐘、以確保發生下列情況：
   - 用戶端多重路徑（若已部署）會穩定下來。
   - 用戶端會從接管期間發生的I/O暫停中恢復。

   還原時間是用戶端專屬的、視用戶端應用程式的特性而定、可能需要8分鐘以上的時間。

8. 將集合體傳回目標節點：

   將MetroCluster 靜態IP組態升級ONTAP 為EFlash 9.5或更新版本之後、集合體將會在重新同步並返回鏡射狀態之前、處於降級狀態一小段時間。

   a. 將集合物傳回叢集 A 上的 DR 合作夥伴：

   ```
   storage failover giveback -ofnode node_A_1
   ```

   b. 將集合物傳回叢集 B 上的 DR 合作夥伴：

   ```
   storage failover giveback -ofnode node_B_1
   ```

   恢復作業會先將根Aggregate傳回節點、然後在節點完成開機之後、傳回非根Aggregate。

9. 在兩個叢集上發出下列命令、確認已傳回所有的集合體：

```
storage failover show-giveback
```

如果「歸還狀態」欄位指出沒有要歸還的集合體、則會傳回所有集合體。如果恢復被否決、命令會顯示恢復進度、以及哪個子系統已對恢復執行了指令。

10. 如果尚未傳回任何Aggregate、請執行下列動作：
    a. 請檢閱「否決因應措施」、以判斷您是否想要處理「『直接』條件、或是要撤銷「否決」。
    b. 如有必要、請解決錯誤訊息中所述的「『驗證』條件、確保所有已識別的作業都能正常終止。
    c. 重新輸入儲存容錯移轉恢復命令。

       如果您決定覆寫「vito'」條件、請將-overre-etoes參數設為true。

11. 至少等待八分鐘、以確保發生下列情況：
    - 用戶端多重路徑（若已部署）會穩定下來。
    - 用戶端會從還原期間發生的I/O暫停中恢復。

      還原時間是用戶端專屬的、視用戶端應用程式的特性而定、可能需要8分鐘以上的時間。

12. 將權限等級從 admin 設定為進階、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

13. 確認叢集 A 上的版本：

```
system image show
```

下列範例顯示、節點a_1上的系統影像2應為預設版本和目前版本：

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_A_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_A_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

14. 確認叢集 B 上的版本：

```
system image show
```

下列範例顯示、節點ONTAP _a_1上的系統影像2（0版）為預設版本和目前版本：

```
cluster_A::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version   Date
-------- -------  ------- ------- --------- -------------------
node_B_1
         image1   false   false    X.X.X    MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y    MM/DD/YYYY TIME
node_B_2
         image1   false   true     X.X.X    MM/DD/YYYY TIME
         image2   true    false    Y.Y.Y    MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

正在更新**MetroCluster** 不只是個**DR**群組的第二個**DR**配對

您必須以正確順序執行節點接管與恢復、才能使ONTAP 節點的新版本成為節點的目前版本。

您應該已經升級第一個DR配對（node_a_1和node_B_1）。

在此工作中、 node_a_2 和 node_B_2 會升級。

如果您已在第一個 DR 群組上升級 ONTAP 軟體、並正在八節點 MetroCluster 組態中更新第二個 DR 群組、則在此工作中、您將更新 node_a_4 和 node_B_4 。

1. 將所有資料生命從節點移轉至其他位置：

```
network interface migrate-all -node nodenameA
```

2. 啟動叢集A上目標節點的接管：

   請勿指定-option Immediate參數、因為要重新啟動至新軟體映像的節點需要正常接管。

   a. 接管叢集_A上的DR合作夥伴：

```
storage failover takeover -ofnode node_A_2 -option allow-version-
mismatch
```

。 `allow-version-mismatch` 從 ONTAP 9.0 升級至 ONTAP 9.1 或任何修補程式升級時、都不需要選項。

節點會開機至「等待恢復」狀態。

如果啟用了「支援」、則會傳送一則消息「不支援」、指出節點已超出叢集仲裁。AutoSupport AutoSupport您可以忽略此通知並繼續升級。

b. 確認接管成功：

```
storage failover show
```

以下範例顯示接管作業成功。node_a_2處於「等待恢復」狀態、node_a_1處於「接管」狀態。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_A_1       node_A_2       false    In takeover
node_A_2       node_A_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

3. 在叢集B上啟動目標節點的接管：

請勿指定-option Immediate參數、因為要重新啟動至新軟體映像的節點需要正常接管。

a. 接管叢集 B 上的 DR 合作夥伴（ node_B_2 ）：

如果您要從...升級	輸入此命令...
部分版本ONTAP ONTAP	`storage failover takeover -ofnode node_B_2`

如果您要從...升級	輸入此命令...
部分版本的升級版ONTAP Data ONTAP	`storage failover takeover -ofnode node_B_2 -option allow-version-mismatch` 。 `allow-version-mismatch` 從 ONTAP 9.0 升級至 ONTAP 9.1 或任何修補程式升級時、都不需要選項。

節點會開機至「等待恢復」狀態。

如果啟用 AutoSupport 、則會傳送 AutoSupport 訊息、指出節點已超出叢集仲裁。您可以安全地忽略此通知並繼續升級。

b. 確認接管成功：

```
storage failover show
```

以下範例顯示接管作業成功。node_B_2處於「等待恢復」狀態、node_B_1處於「接管中」狀態。

```
cluster1::> storage failover show
                              Takeover
Node           Partner        Possible State Description
-------------- -------------- --------
-------------------------------------
node_B_1       node_B_2       false    In takeover
node_B_2       node_B_1       -        Waiting for giveback (HA
mailboxes)
2 entries were displayed.
```

4. 至少等待八分鐘、以確保發生下列情況：
   - 用戶端多重路徑（若已部署）會穩定下來。
   - 用戶端會從接管期間發生的I/O暫停中恢復。

   還原時間是用戶端專屬的、視用戶端應用程式的特性而定、可能需要8分鐘以上的時間。

5. 將集合體傳回目標節點：

將MetroCluster 靜態IP組態升級ONTAP 為EFlash 9.5之後、集合體將會在重新同步並返回鏡射狀態之前、處於降級狀態一小段時間。

a. 將集合物傳回叢集 A 上的 DR 合作夥伴：

```
storage failover giveback -ofnode node_A_2
```

b. 將集合物傳回叢集 B 上的 DR 合作夥伴：

```
storage failover giveback -ofnode node_B_2
```

恢復作業會先將根Aggregate傳回節點、然後在節點完成開機之後、傳回非根Aggregate。

6. 在兩個叢集上發出下列命令、確認已傳回所有的集合體：

```
storage failover show-giveback
```

如果「歸還狀態」欄位指出沒有要歸還的集合體、則會傳回所有集合體。如果恢復被否決、命令會顯示恢復進度、以及哪個子系統已對恢復執行了指令。

7. 如果尚未傳回任何Aggregate、請執行下列動作：
   a. 請檢閱「否決因應措施」、以判斷您是否想要處理「『直接』條件、或是要撤銷「否決」。
   b. 如有必要、請解決錯誤訊息中所述的「『驗證』條件、確保所有已識別的作業都能正常終止。
   c. 重新輸入儲存容錯移轉恢復命令。

   如果您決定覆寫「vito'」條件、請將-overre-etoes參數設為true。

8. 至少等待八分鐘、以確保發生下列情況：
   - 用戶端多重路徑（若已部署）會穩定下來。
   - 用戶端會從還原期間發生的I/O暫停中恢復。

   還原時間是用戶端專屬的、視用戶端應用程式的特性而定、可能需要8分鐘以上的時間。

9. 將權限等級從 admin 設定為進階、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

10. 確認叢集 A 上的版本：

```
system image show
```

下列範例顯示、節點ONTAP _a_2上的系統影像2（目標版本）為預設版本和目前版本：

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_A_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_A_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

11. 確認叢集 B 上的版本：

```
system image show
```

下列範例顯示、節點ONTAP _B_2上的系統影像2（目標版本）為預設版本和目前版本：

```
cluster_B::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- ----------  -------------------
node_B_1
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
node_B_2
         image1   false   false    X.X.X      MM/DD/YYYY TIME
         image2   true    true     Y.Y.Y      MM/DD/YYYY TIME
4 entries were displayed.

cluster_A::>
```

12. 針對 HA 配對中的每個節點、啟用自動恢復：

```
storage failover modify -node target-node -auto-giveback true
```

此命令必須針對HA配對中的每個節點重複執行。

13. 確認已啟用自動恢復：

```
storage failover show -fields auto-giveback
```

此範例顯示兩個節點均已啟用自動恢復功能：

```
cluster_x::> storage failover show -fields auto-giveback
node     auto-giveback
-------- -------------
node_x_1 true
node_x_2 true
2 entries were displayed.
```

相關資訊

- "儲存故障轉移交還"
- "儲存故障轉移修改"
- "儲存故障轉移顯示-恢復"
- "儲存故障轉移接管"

在 **ONTAP 9.2** 或更早版本中手動不中斷升級雙節點 **MetroCluster** 組態

升級雙節點 MetroCluster 組態的方式會因 ONTAP 版本而異。如果您執行的是 ONTAP 9.2 或更早版本、您應該使用此程序來執行手動不中斷升級、包括啟動交涉式切換、更新「失敗」站台上的叢集、啟動切換、然後在其他站台的叢集上重複該程序。

如果您有執行 ONTAP 9.3 或更新版本的雙節點 MetroCluster 組態、請執行 使用 System Manager 自動升級。

步驟

1. 將權限等級設為「進階」、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

2. 在要升級的叢集上、安裝新的 ONTAP 軟體映像做為預設：

```
system node image update -package package_location -setdefault true
-replace-package true
```

```
cluster_B::*> system node image update -package
http://www.example.com/NewImage.tgz -setdefault true -replace-package
true
```

3. 確認目標軟體映像已設為預設映像：

```
system node image show
```

以下範例顯示了這一點 `NewImage` 設為預設映像：

```
cluster_B::*> system node image show
                     Is      Is                            Install
Node     Image       Default Current Version               Date
-------- -------     ------- ------- --------------------
-------------------
node_B_1
         OldImage  false   true    X.X.X                 MM/DD/YYYY TIME
         NewImage  true    false   Y.Y.Y                 MM/DD/YYYY TIME
2 entries were displayed.
```

4. 如果目標軟體映像未設為預設映像、請加以變更：

```
system image modify {-node * -iscurrent false} -isdefault true
```

5. 確認所有叢集 SVM 都處於健全狀況狀態：

```
metrocluster vserver show
```

6. 在未更新的叢集上、啟動交涉的切入：

```
metrocluster switchover
```

此作業可能需要數分鐘的時間。您可以使用MetroCluster flexoperationshow命令來驗證切換是否已完成。

在下列範例中、會在遠端叢集（「叢集_a`」）上執行協調式切換。這會導致本機叢集（「叢集B」）停止、以便更新。

```
cluster_A::> metrocluster switchover

Warning: negotiated switchover is about to start. It will stop all the
data
         Vservers on cluster "cluster_B" and
         automatically re-start them on cluster
         "cluster_A". It will finally gracefully shutdown
         cluster "cluster_B".
Do you want to continue? {y|n}: y
```

7. 確認所有叢集 SVM 都處於健全狀況狀態：

```
metrocluster vserver show
```

8. 重新同步「儲存」叢集上的資料集合體：

```
metrocluster heal -phase aggregates
```

將MetroCluster 靜態IP組態升級ONTAP 為EFlash 9.5或更新版本之後、集合體將會在重新同步並返回鏡射狀態之前、處於降級狀態一小段時間。

```
cluster_A::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

9. 確認修復作業已成功完成：

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

10. 重新同步「儲存」叢集上的根集合體：

```
metrocluster heal -phase root-aggregates
```

```
cluster_A::> metrocluster heal -phase root-aggregates
[Job 131] Job succeeded: Heal Root Aggregates is successful.
```

11. 確認修復作業已成功完成：

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

12. 在停止的叢集上、從載入器提示字元啟動節點：

```
boot_ontap
```

13. 等待開機程序完成、然後確認所有叢集 SVM 都處於健全狀況狀態：

```
metrocluster vserver show
```

14. 從「影片」叢集執行切換：

```
metrocluster switchback
```

15. 確認切換已成功完成：

```
metrocluster operation show
```

```
cluster_A::> metrocluster operation show
Operation: switchback
State: successful
Start Time: MM/DD/YYYY TIME
End Time: MM/DD/YYYY TIME
Errors: -
```

16. 確認所有叢集 SVM 都處於健全狀況狀態：

```
metrocluster vserver show
```

17. 在其他叢集上重複上述所有步驟。
18. 驗證MetroCluster 此功能是否正常：
    a. 檢查組態：

```
metrocluster check run
```

```
cluster_A::> metrocluster check run
Last Checked On: MM/DD/YYYY TIME
Component           Result
------------------- ---------
nodes               ok
lifs                ok
config-replication  ok
aggregates          ok
4 entries were displayed.

Command completed. Use the "metrocluster check show -instance"
command or sub-commands in "metrocluster check" directory for
detailed results.
To check if the nodes are ready to do a switchover or switchback
operation, run "metrocluster switchover -simulate" or "metrocluster
switchback -simulate", respectively.
```

    b. 如果您想要檢視更詳細的結果、請使用 MetroCluster check run 命令：

```
metrocluster check aggregate show
```

```
metrocluster check config-replication show
```

```
metrocluster check lif show
```

```
metrocluster check node show
```

c. 將權限層級設為進階：

```
set -privilege advanced
```

d. 模擬「變更作業：

```
metrocluster switchover -simulate
```

e. 檢閱「移動模擬：

```
metrocluster operation show
```

```
cluster_A::*> metrocluster operation show
    Operation: switchover
        State: successful
   Start time: MM/DD/YYYY TIME
     End time: MM/DD/YYYY TIME
       Errors: -
```

f. 返回管理權限層級：

```
set -privilege admin
```

g. 在其他叢集上重複這些子步驟。

完成後

執行任何 "升級後的工作"。

相關資訊

"災難恢復MetroCluster"

使用 CLI 手動進行中斷 ONTAP 升級

如果您可以讓叢集離線升級至新ONTAP 版的版本、則可以使用中斷升級方法。此方法有數個步驟：停用每個HA配對的儲存容錯移轉、重新啟動叢集中的每個節點、然後重新啟用儲存容錯移轉。

- 您必須 "下載" 和 "安裝" 軟體映像。
- 如果您是在SAN環境中運作、則必須關閉或暫停所有SAN用戶端、直到升級完成為止。

  如果SAN用戶端在中斷升級之前未關機或暫停、則用戶端檔案系統和應用程式會發生錯誤、可能需要在升級完成後手動恢復。

在中斷升級中、因為停用每個HA配對的儲存容錯移轉、而且每個節點都會更新、所以需要停機。停用儲存容錯移轉時、每個節點都會做為單一節點叢集、也就是與節點相關的系統服務會中斷、只要系統重新開機即可。

步驟

1. 將權限等級從 admin 設定為進階、在提示繼續時輸入 * y* ：

```
set -privilege advanced
```

進階提示 (*>) 。

2. 將新的 ONTAP 軟體映像設為預設映像：

```
system image modify {-node * -iscurrent false} -isdefault true
```

此命令會使用延伸查詢、將目標ONTAP 的支援軟體映像（安裝為替代映像）變更為每個節點的預設映像。

3. 確認新的 ONTAP 軟體映像已設為預設映像：

```
system image show
```

在下列範例中、影像2是新ONTAP 的版本、並在兩個節點上設為預設影像：

```
cluster1::*> system image show
                  Is      Is                Install
Node     Image    Default Current Version    Date
-------- -------  ------- ------- --------- -------------------
node0
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
node1
         image1   false   true    X.X.X     MM/DD/YYYY TIME
         image2   true    false   Y.Y.Y     MM/DD/YYYY TIME
4 entries were displayed.
```

4. 執行下列任一步驟：

如果叢集包含...	執行此動作...
單一節點	繼續下一步。

如果叢集包含...	執行此動作...

兩個節點	a. 停用叢集高可用度：
	`cluster ha modify -configured false`
	輸入 `y` 以在出現提示時繼續。
	b. 停用 HA 配對的儲存容錯移轉：
	`storage failover modify -node * -enabled false`

兩個以上的節點	停用叢集中每個 HA 配對的儲存容錯移轉： `storage failover modify -node * -enabled false`

5. 重新啟動叢集中的節點：

```
system node reboot -node nodename -ignore-quorum-warnings
```

請勿一次重新開機超過一個節點。

節點會開機新ONTAP 的「介紹」影像。出現此畫面的功能登入提示、表示重新開機程序已完成。ONTAP

6. 使用新的 ONTAP 映像重新啟動節點或節點集之後、請將權限等級設為進階：

```
set -privilege advanced
```

當系統提示您繼續時、請輸入 * y*

7. 確認新軟體正在執行：

```
system node image show
```

在下列範例中、image1是新ONTAP 的版本、並設為節點0上的目前版本：

```
cluster1::*> system node image show
                  Is      Is                  Install
Node      Image   Default Current Version     Date
--------- ------- ------- ------- --------    -------------------
node0
          image1  true    true    X.X.X        MM/DD/YYYY TIME
          image2  false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
          image1  true    false   X.X.X       MM/DD/YYYY TIME
          image2  false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

8. 確認升級成功完成：

   a. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

   b. 確認每個節點的升級狀態為完成：

   ```
   system node upgrade-revert show -node nodename
   ```

   狀態應列示為「完成」。

   如果狀態未完成、"請聯絡NetApp支援部門"請立即進行。

   a. 返回管理權限層級：

   ```
   set -privilege admin
   ```

9. 針對每個額外節點重複步驟 5 至 8 。
10. 如果叢集包含兩個以上的節點、請為叢集中的每個 HA 配對啟用儲存容錯移轉：

    ```
    storage failover modify -node * -enabled true
    ```

11. 如果叢集僅包含兩個節點、請啟用叢集高可用度：

    ```
    cluster ha modify -configured true
    ```

相關資訊

- "儲存故障轉移修改"

ONTAP 升級後的處理方式

ONTAP 升級後的處理方式

升級 ONTAP 之後、您應該執行數項工作來驗證叢集就緒性。

1. "驗證您的叢集"。

   升級 ONTAP 之後、您應該驗證叢集版本、叢集健全狀況和儲存健全狀況。如果您使用MetroCluster 的是SFC組態、您也需要確認叢集已啟用自動非計畫性切換功能。

2. "確認所有的生命都在主連接埠上"。

   在重新開機期間、部分LIF可能已移轉至指派的容錯移轉連接埠。升級叢集之後、您必須啟用及還原任何不在主連接埠上的生命。

3. 驗證 "特殊考量" 特定於您的叢集。

   如果叢集上存在某些組態、您可能需要在升級後執行其他步驟。

4. "更新磁碟認證套件（ DQP ）"。

   不會在ONTAP 進行升級時更新DQP。

在 ONTAP 升級後驗證叢集

升級 ONTAP 之後、請確認叢集版本、叢集健全狀況和儲存健全狀況。 對於 MetroCluster FC 組態、也請確認叢集已啟用、可自動進行非計畫性切換。

驗證叢集版本

升級所有 HA 配對後、您必須使用 version 命令來驗證所有節點是否都在執行目標版本。

叢集版本是ONTAP 叢集內任何節點上執行的最低版本的功能。如果叢集版本不是目標ONTAP 版本的版本、您可以升級叢集。

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 驗證叢集版本是否為目標ONTAP 版本的發行版本：

   ```
   system node image show -version
   ```

3. 如果叢集版本不是目標 ONTAP 版本、您應該驗證所有節點的升級狀態：

```
system node upgrade-revert show
```

驗證叢集健全狀況

升級叢集之後、您應該確認節點狀況良好且符合參與叢集的資格、而且叢集已達到仲裁數。

1. 驗證叢集中的節點是否處於線上狀態、並符合參加叢集的資格：

```
cluster show
```

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

如果有任何節點不健全或不符合資格、請檢查EMS記錄是否有錯誤、並採取修正行動。

2. 驗證每個RDB程序的組態詳細資料。
   - 每個節點的關聯式資料庫時期和資料庫時期應相符。
   - 所有節點的每個環仲裁主機都應該相同。

     請注意、每個振鈴都可能有不同的仲裁主機。

若要顯示此RDB程序…	輸入此命令…
管理應用程式	`cluster ring show -unitname mgmt`
Volume位置資料庫	`cluster ring show -unitname vldb`
虛擬介面管理程式	`cluster ring show -unitname vifmgr`
SAN管理精靈	`cluster ring show -unitname bcomd`

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

     此範例顯示Volume位置資料庫程序：

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

3. 如果您是在SAN環境中運作、請確認每個節點都位於SAN仲裁中：

```
cluster kernel-service show
```

```
cluster1::*> cluster kernel-service show
Master            Cluster           Quorum        Availability
Operational
Node              Node              Status        Status        Status
----------------- ----------------- ------------- -------------
-------------
cluster1-01       cluster1-01       in-quorum     true
operational
                  cluster1-02       in-quorum     true
operational
2 entries were displayed.
```

4. 將權限等級傳回管理員：

```
set -privilege admin
```

相關資訊

"系統管理"

確認已啟用自動非計畫性切換（僅限 **MetroCluster FC** 組態）

如果您的叢集是在 MetroCluster FC 組態中、您應該驗證在升級 ONTAP 之後、是否已啟用自動非計畫性切換。

如果您使用MetroCluster 的是一套靜態IP組態、請跳過此程序。

步驟

1. 檢查是否已啟用自動非計畫性切換：

```
metrocluster show
```

如果啟用自動非計畫性切換、命令輸出中會出現下列陳述：

```
AUSO Failure Domain  auso-on-cluster-disaster
```

2. 如果未出現該陳述、請啟用自動非計畫性切換：

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

3. 確認已啟用自動非計畫性切換：

```
metrocluster show
```

相關資訊

"磁碟與Aggregate管理"

在 **ONTAP** 升級之後、確認所有的生命體都位於主連接埠上

在 ONTAP 升級程序中進行的重新開機期間、可能會將部分生命體從其主連接埠移轉至指派的容錯移轉連接埠。升級後、您需要啟用及還原不在其主連接埠上的任何生命。

步驟

1. 顯示所有生命的狀態：

```
network interface show -fields home-port,curr-port
```

如果 * 狀態管理員 * 為「關閉」或 * 為首頁 * 對於任何生命週期為「假」、請繼續下一步。

2. 啟用資料生命：

```
network interface modify {-role data} -status-admin up
```

3. 將LIF還原至其主連接埠：

```
network interface revert *
```

4. 確認所有的生命都在其主連接埠中：

```
network interface show
```

此範例顯示SVM vs0的所有lifs都位於其主連接埠上。

```
cluster1::> network interface show -vserver vs0
         Logical    Status     Network          Current  Current Is
Vserver  Interface  Admin/Oper Address/Mask     Node     Port    Home
-------- ---------- ---------- ---------------- -------- ------- ----
vs0
         data001    up/up      192.0.2.120/24   node0    e0e     true
         data002    up/up      192.0.2.121/24   node0    e0f     true
         data003    up/up      192.0.2.122/24   node0    e2a     true
         data004    up/up      192.0.2.123/24   node0    e2b     true
         data005    up/up      192.0.2.124/24   node1    e0e     true
         data006    up/up      192.0.2.125/24   node1    e0f     true
         data007    up/up      192.0.2.126/24   node1    e2a     true
         data008    up/up      192.0.2.127/24   node1    e2b     true
8 entries were displayed.
```

相關資訊

- "網路介面"

特殊組態

升級後，請檢查特定的 **ONTAP** 組態

如果您的叢集已設定下列任何功能、您可能需要在升級 ONTAP 軟體之後執行其他步驟。

請自問...	如果您的答案是*是*、請執行此動作...
我是從 ONTAP 9.7 或更早版本升級到 ONTAP 9.8 或更高版本嗎？	驗證您的網路組態 從不提供 EMS 目標可及性的網路服務策略中刪除 EMS LIF 服務
我的叢集是否採用 MetroCluster 組態？	驗證您的網路和儲存狀態
我是否有SAN組態？	驗證SAN組態
我是否從 ONTAP 9.3 或更早版本升級、並使用 NetApp 儲存加密？	重新設定KMIP伺服器連線
我是否有負載共用鏡像？	重新部署移動的負載共用鏡射來源磁碟區
我是否擁有 ONTAP 9.9.1 之前建立的服務處理器（ SP ）存取使用者帳戶？	驗證可存取服務處理器的帳戶變更

升級後，請驗證您的 **ONTAP** 網路組態

從 ONTAP 9.7x 或更早版本升級到 ONTAP 9.8 或更高版本後，應驗證網絡配置。升級

後ONTAP 、功能自動化監控第2層的連線能力。

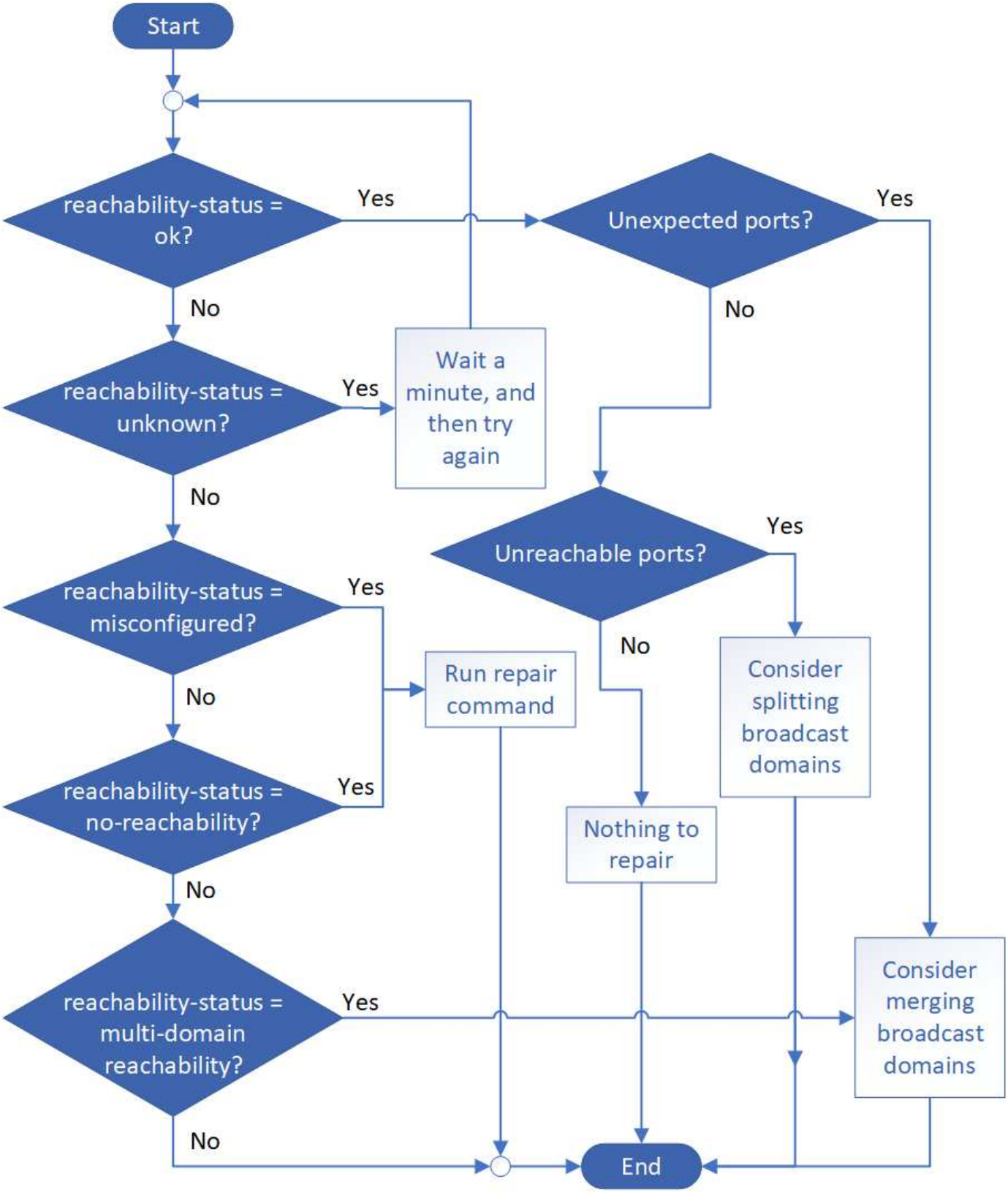
步驟

1. 驗證每個連接埠是否可連線至其預期的廣播網域：

```
network port reachability show -detail
```

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

命令輸出包含可到達性結果。請使用下列決策樹狀結構和表格來瞭解連線結果（連線狀態）、並判斷接下來要做什麼（如果有的話）。


Start
reachability-status = ok?
Yes
No
Unexpected ports?
Yes
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
No
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
reachability-status = no-reachability?
Yes
No
Nothing to repair
reachability-status = multi-domain reachability?
Yes
No
Consider merging broadcast domains
End

連線狀態	說明

好的	連接埠可連線至其指派的廣播網域的第2層。 如果連線狀態為「正常」、但有「非預期的連接埠」、請考慮合併一或多個廣播網域。如需詳細資訊、請參閱 "合併廣播網域"。 如果連線狀態為「正常」、但有「無法連線的連接埠」、請考慮分割一或多個廣播網域。如需詳細資訊、請參閱 "分割廣播網域"。 如果連線狀態為「正常」、而且沒有非預期或無法連線的連接埠、表示您的組態正確。
設定錯誤的連線能力	連接埠無法連線至其指派的廣播網域的第2層；不過連接埠確實可連線至不同的廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給可連線的廣播網域： `network port reachability repair -node -port` 如需詳細資訊、請參閱 "修復連接埠連線能力"。 如"指令參考資料ONTAP"需詳細 `network port reachability repair`資訊，請參閱。
不可到達性	連接埠無法連線至任何現有廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給預設IPspace中自動建立的新廣播網域： `network port reachability repair -node -port` 如需詳細資訊、請參閱 "修復連接埠連線能力"。
多網域連線能力	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷其是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域" 或 "修復連接埠連線能力"。
不明	如果連線狀態為「未知」、請稍候幾分鐘、然後再試一次命令。

修復連接埠之後、您需要檢查並解決已移轉的LIF和VLAN。如果連接埠是介面群組的一部分、您也需要瞭解該介面群組發生了什麼事。 如需詳細資訊、請參閱 "修復連接埠連線能力"。

在 **ONTAP** 升級之後，從網路服務原則中移除 **EMS LIF** 服務

如果您在從 ONTAP 9.7 或更早版本升級至 ONTAP 9.8 或更高版本之前設定了事件管理系統 (EMS) 訊息，升級後您的 EMS 訊息可能無法傳遞。

在升級過程中， `management-ems` ，即 EMS LIF 服務，已新增至管理 SVM 中所有現有的服務策略。這樣，就可以從與服務策略關聯的任何 LIF 發送 EMS 訊息。如果選取的LIF無法連線至事件通知目的地、則不會傳送訊息。

為防止這種情況，升級後您應該從不提供目標可及性的網路服務策略中刪除 EMS LIF 服務。

"了解有關 ONTAP LIF 和服務策略的更多信息"。

步驟

1. 確定可透過其發送 EMS 訊息的 LIF 和相關網路服務策略：

```
network interface show -fields service-policy -services management-ems
```

```
vserver        lif             service-policy
-------------- ------------    ------------------
cluster-1      cluster_mgmt    default-management
cluster-1      node1-mgmt      default-management
cluster-1      node2-mgmt      default-management
cluster-1      inter_cluster   default-intercluster
4 entries were displayed.
```

2. 檢查每個LIF是否可連線至EMS目的地：

```
network ping -lif <lif_name> -vserver <svm_name> -destination
<destination_address>
```

在每個節點上執行此操作。

範例

```
cluster-1::> network ping -lif node1-mgmt -vserver cluster-1
-destination 10.10.10.10
10.10.10.10 is alive

cluster-1::> network ping -lif inter_cluster -vserver cluster-1
-destination 10.10.10.10
no answer from 10.10.10.10
```

3. 輸入進階權限層級：

```
set advanced
```

4. 對於不具可達性的 LIF，刪除 `management-ems`對應服務策略中的 LIF 服務：

```
network interface service-policy remove-service -vserver <svm_name>
-policy <service_policy_name> -service management-ems
```

如"指令參考資料ONTAP"需詳細 `network interface service-policy remove-service`資訊，請參閱。

5. 確認管理- EMS LIF現在僅與提供EMS目的地連線能力的LIF相關聯：

```
network interface show -fields service-policy -services management-ems
```

在 **ONTAP** 升級之後，確認 **MetroCluster** 組態的網路和儲存狀態

在 MetroCluster 組態中升級 ONTAP 叢集之後、您應該驗證每個叢集的生命體、集合體和磁碟區的狀態。

1. 驗證 LIF 狀態：

```
network interface show
```

在正常操作中、來源SVM的l生命 區必須具有UP（啟動）管理狀態、並且位於其主節點上。目的地SVM的LIF不需要在其主節點上啟動或定位。在切換時、所有生命期的管理員狀態都為up、但不需要位於主節點上。

```
cluster1::> network interface show
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
Cluster
            cluster1-a1_clus1
                         up/up    192.0.2.1/24       cluster1-01
                                                                  e2a
true
            cluster1-a1_clus2
                         up/up    192.0.2.2/24       cluster1-01
                                                                  e2b
true


cluster1-01
            clus_mgmt    up/up    198.51.100.1/24    cluster1-01
                                                                  e3a
true
            cluster1-a1_inet4_intercluster1
                         up/up    198.51.100.2/24    cluster1-01
                                                                  e3c
true
            ...

27 entries were displayed.
```

2. 驗證集合體的狀態：

```
storage aggregate show -state !online
```

此命令會顯示任何非連線的Aggregate。正常運作時、位於本機站台的所有集合體都必須在線上。但是MetroCluster 、如果將S還原 組態切換到災難恢復站台、則允許位於災難恢復站台的根集合體離線。

此範例顯示叢集處於正常運作狀態：

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

此範例顯示切換中的叢集、災難恢復站台的根集合體處於離線狀態：

```
cluster1::> storage aggregate show -state !online
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
aggr0_b1
                0B        0B    0% offline      0 cluster2-01
raid_dp,

mirror

degraded
aggr0_b2
                0B        0B    0% offline      0 cluster2-02
raid_dp,

mirror

degraded
2 entries were displayed.
```

3. 驗證磁碟區的狀態：

```
volume show -state !online
```

此命令會顯示任何非連線的磁碟區。

如果MetroCluster 此支援功能組態處於正常運作狀態（非切換狀態）、則輸出應顯示叢集次要SVM擁有的所有磁碟區（其SVM名稱會附加「-MC」）。

這些磁碟區只有在切換時才會上線。

此範例顯示正常運作的叢集、災難恢復站台的磁碟區不在線上。

```
cluster1::> volume show -state !online
  (volume show)
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2-mc    vol1         aggr1_b1     -          RW            -
-     -
vs2-mc    root_vs2     aggr0_b1     -          RW            -
-     -
vs2-mc    vol2         aggr1_b1     -          RW            -
-     -
vs2-mc    vol3         aggr1_b1     -          RW            -
-     -
vs2-mc    vol4         aggr1_b1     -          RW            -
-     -
5 entries were displayed.
```

4. 確認沒有不一致的磁碟區：

```
volume show -is-inconsistent true
```

查看"NetApp知識庫：顯示WAFL不一致的捲"如何解決不一致的問題。

在 **ONTAP** 升級之後驗證 **SAN** 組態

在 ONTAP 升級之後、在 SAN 環境中、您應該在升級成功重新連線至 LIF 之前、確認每個連接至 LIF 的啟動器。

1. 確認每個啟動器都已連接至正確的LIF。

   您應該將啟動器清單與您在升級準備期間所做的清單進行比較。如果您執行的是 ONTAP 9.11.1 或更新版本、請使用系統管理員來檢視連線狀態、因為它的顯示比 CLI 更清晰。

系統管理員

a. 在System Manager中、按一下*主機> SAN啟動器群組*。

   此頁面會顯示啟動器群組（igroup）清單。如果清單很大、您可以按一下頁面右下角的頁碼來檢視清單的其他頁面。

   這些欄會顯示有關階層的各種資訊。從9.11.1開始、也會顯示igroup的連線狀態。將游標暫留在狀態警示上以檢視詳細資料。

CLI

- 列出 iSCSI 啟動器：

```
iscsi initiator show -fields igroup,initiator-name,tpgroup
```

- 列出 FC 啟動器：

```
fcp initiator show -fields igroup,wwpn,lif
```

從 **ONTAP 9.2** 或更早版本升級後、重新設定 **KMIP** 伺服器連線

從 ONTAP 9.2 或更新版本升級至 ONTAP 9.3 或更新版本後、您需要重新設定任何外部金鑰管理（ KMIP ）伺服器連線。

步驟

1. 設定金鑰管理程式連線能力：

```
security key-manager setup
```

2. 新增 KMIP 伺服器：

```
security key-manager add -address <key_management_server_ip_address>
```

3. 確認 KMIP 伺服器已連線：

```
security key-manager show -status
```

4. 查詢關鍵伺服器：

```
security key-manager query
```

5. 建立新的驗證金鑰和密碼：

```
security key-manager create-key -prompt-for-key true
```

設定至少包含 32 個字元的密碼。

6. 查詢新的驗證金鑰：

```
security key-manager query
```

7. 將新的驗證金鑰指派給自我加密磁碟（ SED ）：

```
storage encryption disk modify -disk <disk_ID> -data-key-id <key_ID>
```

使用查詢中的新身份驗證金鑰。

8. 如有需要、請指派 FIPS 金鑰給 SED ：

```
storage encryption disk modify -disk <disk_id> -fips-key-id
<fips_authentication_key_id>
```

如果您的安全設定要求您使用不同的金鑰進行資料認證和 FIPS 140-2 認證，則您應該為每個認證建立單獨的金鑰。否則，對兩者使用相同的身份驗證金鑰。

相關資訊

- "安全金鑰管理程式設定"
- "儲存加密磁碟修改"

在 **ONTAP** 升級之後重新定位移動的負載共用鏡射來源磁碟區

升級 ONTAP 之後、您需要將負載共用鏡射來源磁碟區移回其升級前的位置。

步驟

1. 使用您在移動負載共用鏡射來源磁碟區之前所建立的記錄、找出您要將負載共用鏡射來源磁碟區移至的位置。
2. 將負載共用鏡射來源磁碟區移回其原始位置：

```
volume move start
```

在 **ONTAP** 升級後，可存取服務處理器的使用者帳戶變更

如果您在 ONTAP 9.8 或更早版本中建立了使用者帳戶、以便以非系統管理角色存取服務處理器（ SP ）、而且您升級至 ONTAP 9.9.1 或更新版本、則中的任何非系統管理值 `-role` 參數已修改為 `admin`。

如需詳細資訊、請參閱 "可存取SP的帳戶"。

在 **ONTAP** 升級之後更新磁碟資格審查套件

升級 ONTAP 軟體之後、您應該下載並安裝 ONTAP 磁碟資格審查套件（ DQP ）。 不會在ONTAP 進行升級時更新DQP。

DQP 包含 ONTAP 與所有新合格磁碟機互動的適當參數。如果您的 DQP 版本不包含新合格磁碟機的資訊、ONTAP 將無法取得正確設定磁碟機的資訊。

最佳做法是每季更新 DQP 。 您也應該更新 DQP 、原因如下：

- 每當您新增磁碟機類型或大小至叢集中的節點時

  例如、如果您已經有1 TB磁碟機並新增2 TB磁碟機、則必須檢查是否有最新的DQP更新。

- 每當您更新磁碟韌體時
- 只要有較新的磁碟韌體或DQP檔案可用

相關資訊

- "NetApp下載：磁碟認證套件"
- "NetApp下載：磁碟機韌體"

韌體，系統和安全性更新

ONTAP 中的韌體，系統和安全性更新總覽

視您的 ONTAP 版本而定，您可以啟用自動韌體，系統和安全性更新。

版本**ONTAP**	自動更新中包含的內容
9.16.1 及更新版本	• 人工智慧的自主勒索軟體保護（ ARP/AI ） • ONTAP 時區資料庫 • 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體

版本**ONTAP**	自動更新中包含的內容
9.13.1 及更新版本	• ONTAP 時區資料庫 • 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體
9.10.1 及更新版本	• 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體
9.9.1 及更早版本	不支援

如果您的 ONTAP 版本無法使用自動更新，或您沒有啟用自動更新，您可以手動執行韌體，時區資料庫和安全性更新。

相關連結

- "瞭解如何手動進行韌體更新"
- "知識庫文章：如何更新 ONTAP 9 中的時區資訊"
- "瞭解如何手動進行安全性更新"

影片：自動韌體更新功能

請參考 ONTAP 9.10.1 開始提供的自動韌體更新功能。

如何排程自動更新以進行安裝

同一個叢集中的所有合格節點都會分組、以進行自動更新。 根據更新的優先順序層級和環境中需要更新的系統百分比、排程合格節點進行自動更新的時間範圍會有所不同。

例如、如果您的總系統中有 10% 或更少的系統符合非優先順序更新的資格、則會在 1 週內為所有符合資格的系統排程更新。 不過、如果您的系統總數中有 76% 以上符合非優先順序更新的資格、則此更新會在 8 週內在合格的系統之間交錯進行。 如果需要補救更新的問題、這種交錯式安裝有助於降低整體環境的風險。

您排定每週自動更新的系統總數百分比如下：

- 關鍵更新 *

需要更新的系統百分比	第 **1** 週的更新百分比	第 **2** 週所發生的更新百分比
50% 或更低	100%	
50-100%	30%	70%

- 適用於高優先順序更新 *

需要更新的系統百分比	每週更新的百分比			
	* 第 1 週 *	* 第 2 週 *	* 第 3 週 *	* 第 4 週 *
* 25% 或更低 *	100%			
* 26-50% *	30%	70%		
* 50-100% *	10%	20%	30%	40%

- 適用於一般優先順序更新 *

需要更新的系統百分比	每週更新的百分比							
	* 第 1 週 *	* 第 2 週 *	* 第 3 週 *	* 第 4 週 *	* 第 5 週 *	* 第 6 週 *	* 第 7 週 *	* 第 8 週 *
* 10% 或更低 *	100%							
* 11-20% *	30%	70%						
* 21-50% *	10%	20%	30%	40%				
* 51-75% *	5%	10%	15%	20%	20%	30%		
* 76-100% *	5%	5%	10%	10%	15%	15%	20%	20%

啟用自動更新

啟用自動更新，讓 ONTAP 無需您介入即可下載及安裝韌體，系統和安全性更新。

啟用自動更新需要您接受 EULA 的條款並根據您的環境確認或配置每個系統元件的預設更新行為。

每個系統組件的自動更新的可用性取決於您的ONTAP版本。

版本**ONTAP**	可用的自動更新
9.16.1 及更新版本	• 人工智慧的自主勒索軟體保護（ ARP/AI ） • ONTAP 時區資料庫 • 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體 • 磁碟資格審查套件（ DQP ）
9.13.1 及更新版本	• ONTAP 時區資料庫 • 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體 • 磁碟資格審查套件（ DQP ）
9.10.1 及更新版本	• 儲存裝置、磁碟和磁碟櫃的儲存韌體 • 服務處理器和 BMC 模組的 SP/BMC 韌體 • 磁碟資格審查套件（ DQP ）

開始之前

- 您必須擁有目前的支援權利。您可以在「 * 系統詳細資料 * 」頁面中的檢查"NetApp 支援網站"。
- 若要啟用自動更新，您必須先啟用 AutoSupport with HTTPS 。如果叢集上未啟用 AutoSupport ，或是叢集上已使用其他傳輸傳輸通訊協定啟用 AutoSupport ，您可以在此程序中使用 HTTPS 來啟用。

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

- 從 ONTAP 9.10.1 開始，如果您啟用自動更新，請確保您有 HTTPS 連線功能可連線至下列其他 URL ：
  - https://support-sg-naeast.netapp.com
  - https://support-sg-nawest.netapp.com

關於這項工作

對於在ONTAP 9.16.1 之前建立並升級到 9.16.1 或更高版本的叢集：

- 如果已啟用自動更新功能，升級後系統元件更新預設值不會改變。
- 如果尚未啟用自動更新，則將套用ONTAP 9.16.1 及更高版本中的系統元件更新預設值。

自動系統組件更新預設為自動更新或顯示通知，視您的ONTAP版本而定。在完成流程之前，請確認這些設定適合您的環境。

這 "影片"會顯示使用自動更新程序的快速概觀。

範例 **5.** 步驟

System Manager - ONTAP 9.16.1 及更新版本

1. 在System Manager中、選取*叢集>設定*。
2. 如果您未啟用 AutoSupport 隨需模式與 HTTPS ，請選取以啟用繼續所需的設定。
3. 在 * 軟體更新 * 區段中，選取 * 啟用 * 。
4. 指定每個更新類型要採取的動作。

   您可以選擇自動更新，顯示通知，或自動關閉每種更新類型的更新。

5. 接受條款與條件、然後選取 * 儲存 * 。

System Manager - ONTAP 9.15.1 及更早版本

1. 在 System Manager 中，選取 * 事件 * 。
2. 在 * 總覽 * 區段的 * 啟用自動更新 * 旁，選取 * 動作 > 啟用 * 。
3. 如果您沒有啟用 HTTPS 的 AutoSupport ，請選取以啟用。
4. 接受條款與條件、然後選取 * 儲存 * 。

CLI

1. 啟用自動韌體更新：

```
system service-processor image modify -node <node_name> -autoupdate
true
```

相關資訊

- "準備使用 AutoSupport"
- "疑難排解AutoSupport 透過HTTPS傳送訊息的問題"

修改自動更新

啟用自動更新功能並配置預設系統元件首選項後， ONTAP可以自動偵測、下載和安裝所有建議的更新。如果您希望在安裝之前查看建議的更新，或者希望自動忽略建議，您可以根據自己的喜好修改預設行為。

範例 **6.** 步驟

ONTAP 9.16.1 及更新版本

1. 在 System Manager 中，瀏覽至 * 叢集 > 設定 * 。
2. 在 * 軟體更新 * 區段中，選擇 → 。
3. 選取 * 所有其他更新 * 索引標籤，然後按一下 * 編輯自動更新設定 * 。
4. 指定每個更新類型的預設動作。

   您可以選擇自動更新，顯示通知，或自動關閉每種更新類型的更新。

   ⓘ ONTAP 時區資料庫是由 * 系統檔案 * 更新類型所控制。

5. 接受條款與條件、然後選取 * 儲存 * 。

ONTAP 9.15.1 及更早版本

1. 在System Manager中、按一下*叢集>設定*。
2. 在 * 自動更新 * 區段中、按一下 ⋮ 以檢視動作清單。
3. 按一下*編輯自動更新設定*。
4. 指定每個更新類型的預設動作。

   您可以選擇自動更新，顯示通知，或自動關閉每種類型的更新。

   ⓘ ONTAP 時區資料庫是由系統檔案更新類型所控制。

管理建議的自動更新

自動更新記錄會顯示每個更新建議的清單和詳細資料、包括說明、類別、排程的安裝時間、狀態和任何錯誤。您可以檢視記錄、然後決定您想針對每項建議執行的動作。

步驟

1. 檢視建議清單：

從叢集設定檢視	從更新索引標籤檢視
a. 按一下*叢集>設定*。 b. 視您的 ONTAP 版本而定，請執行下列其中一項： ◦ 對於 ONTAP 9 ・ 15.1 和更早版本，請在 * 自動更新 * 部分中單擊 ⋮，然後單擊選項以查看所有更新。 ◦ 對於 ONTAP 9 ・ 16.1 及更高版本，請在 * 軟件更新 * 部分中選擇 →。在 * 所有其他更新 * 窗格的右角，按一下 * 更多 * ⋮，然後按一下選項以檢視所有更新。	a. 按一下*叢集>總覽*。 b. 在 * 概述 * 部分中，單擊 * 更多 * ⋮，然後單擊 * ONTAP Update* 。 c. 視您的 ONTAP 版本而定、請執行下列步驟： ◦ 對於 ONTAP 9 ・ 15.1 及更早版本，請按一下 * 韌體更新 * 。 ◦ 若為 ONTAP 9 。 16.1 及更新版本，請按一下 * 所有其他更新 * 。 d. 在更新頁面上，單擊 * 更多 * ⋮，然後單擊選項以查看所有更新。

2. 按一下 ⋮ 說明旁的、以檢視您可以對建議執行的動作清單。

   視建議狀態而定、您可以執行下列其中一項動作：

如果更新處於此狀態…	您可以…
尚未排程	更新：開始更新程序。 排程：可讓您設定開始更新程序的日期。 解除：從清單中移除建議。
已排程	更新：開始更新程序。 編輯排程：可讓您修改開始更新程序的排程日期。 取消排程：取消排程日期。
已遭解僱	• 取消關閉 * ：將建議傳回清單。
正在套用或正在下載	取消：取消更新。

手動更新韌體

從 ONTAP 9.9.1 開始、如果您已向註冊 "Active IQ Unified Manager"、您可以在 System Manager 中接收警示、通知您叢集上支援的裝置（例如磁碟、磁碟櫃、服務處理器（ SP ）或基礎板管理控制器（ BMC ）的韌體更新擱置中的時間。

如果您執行的是 ONTAP 9 8 ，或您尚未向 Active IQ Unified Manager 註冊，請瀏覽至 NetApp 支援網站下載韌體更新。

開始之前

若要準備順暢的韌體更新、您應該在更新開始之前重新啟動SP或BMC。使用 `system service-processor reboot-sp -node node_name`命令重新開機。如"指令參考資料ONTAP"需詳細 `system service-processor reboot-sp`資訊，請參閱。

步驟

請根據您的 ONTAP 版本以及您已向 Active IQ Unified Manager 註冊的情況、遵循適當的程序。

ONTAP 9 。 16.1 及更新版本，搭配數位顧問

步驟

1. 在 System Manager 中、前往 * 儀表板 * 。

   在「健全狀況」區段中、如果叢集有任何建議的韌體更新、就會顯示一則訊息。

2. 按一下警示訊息。
3. 在建議更新清單中的安全性更新旁，選取 * 動作 * 。
4. 按一下 * 更新 * 立即安裝更新、或按 * 排程 * 排程稍後更新。

   如果已排程更新、您可以 * 編輯 * 或 * 取消 * 。

ONTAP 9 。 9.1 至 **9.15.1** ，含數位顧問

1. 在 System Manager 中、前往 * 儀表板 * 。

   在「健全狀況」區段中、如果叢集有任何建議的韌體更新、就會顯示一則訊息。

2. 按一下警示訊息。

   「韌體更新」標籤會顯示在「更新」頁面中。

3. 按一下 * 從 NetApp 支援網站 * 下載以取得您要執行的韌體更新。

   隨即顯示 NetApp 支援網站。

4. 登入 NetApp 支援網站 並下載更新所需的韌體映像套件。
5. 將檔案複製到網路上的HTTP或FTP伺服器、或複製到本機資料夾。
6. 在System Manager中、按一下*叢集>總覽*。
7. 在 * 總覽 * 窗格的右角、按一下 * 更多 * ⋮ 、然後選取 * ONTAP Update* 。
8. 按一下*韌體更新*。
9. 視您的 ONTAP 版本而定、請執行下列步驟：

ONTAP 9.9.1 和 **9.10.0**	更新版本**ONTAP**
a. 選擇*從伺服器*或*本機用戶端* b. 提供伺服器URL或檔案位置。	a. 在建議的更新清單中、選取 * 動作 * 。 b. 按一下 * 更新 * 立即安裝更新、或按 * 排程 * 排程稍後更新。 如果已排程更新、您可以 * 編輯 * 或 * 取消 * 。 c. 選擇 * 更新韌體 * 按鈕。

ONTAP 9 8 及更新版本、不含數位顧問

1. 瀏覽至 "NetApp 支援網站" 並登入。
2. 選取您要用來更新叢集韌體的韌體套件。
3. 將檔案複製到網路上的HTTP或FTP伺服器、或複製到本機資料夾。
4. 在System Manager中、按一下*叢集>總覽*。
5. 在 * 總覽 * 窗格的右角，按一下 * 更多 * ⋮，然後選取 * ONTAP Update* 或 * 軟體更新 * （視您的版本而定）。
6. 視您的 ONTAP 版本而定，請執行下列步驟：
   - 對於 ONTAP 9 · 15.1 及更早版本，請按一下 * 韌體更新 * 。
   - 若為 ONTAP 9 。 16.1 及更新版本，請按一下 * 所有其他更新 * 。
7. 視您的 ONTAP 版本而定、請執行下列步驟：

ONTAP 9 。 8 ， 9.9.1 和 9.10.0	更新版本**ONTAP**
1. 選擇*從伺服器*或*本機用戶端* 2. 提供伺服器URL或檔案位置。	1. 在建議的更新清單中、選取 * 動作 * 。 2. 按一下 * 更新 * 立即安裝更新、或按 * 排程 * 排程稍後更新。 如果已排程更新、您可以 * 編輯 * 或 * 取消 * 。 3. 選擇 * 更新韌體 * 按鈕。

完成後

您可以在*韌體更新摘要*下監控或驗證更新。若要檢視已解除安裝或安裝失敗的更新，請根據您的 ONTAP 版本執行下列其中一項：

- 對於 ONTAP 9 · 15.1 及更早版本，請按一下 * 叢集 > 設定 > 自動更新 > 檢視所有自動更新 *
- 若為 ONTAP 9 。 16.1 及更新版本，請按一下 * 叢集 > 設定 > 軟體更新 * 。在 * 所有其他更新 * 窗格的右角，按一下 * 更多 * ⋮，然後選取 * 檢視所有自動更新 * 。

還原ONTAP

我是否需要技術支援才能還原 **ONTAP** 叢集？

在下列情況下，您應該先聯絡技術支援人員，然後再嘗試還原 ONTAP 叢集：

- 正式作業環境

  請勿在沒有技術支援協助的情況下，嘗試還原正式作業叢集。

- 您在ONTAP S還原9.5或更新版本中建立了Volume、因此需要還原至較早版本。

  使用調適性壓縮的磁碟區必須先解壓縮、才能還原。

您可以在不需要協助的情況下還原新叢集或測試叢集。如果您嘗試自行還原叢集，並遇到下列任何問題，請致電技術支援部門：

- 還原失敗或無法完成。
- 還原作業完成，但叢集在正式作業環境中無法使用。
- 還原作業完成，叢集進入正式作業環境，但您對其行為不滿意。

支援的 **ONTAP** 還原路徑

您可以直接將ONTAP軟體回滾到比目前ONTAP版本低一個版本的版本。例如，如果您正在執行 9.15.1 版本，則無法直接回滾到 9.13.1 版本。您必須先恢復到 9.14.1 版本；然後從 9.14.1 版本單獨恢復到 9.13.1 版本。

不支援還原至 ONTAP 9.4 或更早版本。您不應還原為不支援的 ONTAP 版本。

您可以使用 `system image show`命令來判斷每個節點上執行的 ONTAP 版本。

下列支援的還原路徑僅適用於內部部署 ONTAP 版本。如需在雲端中還原 ONTAP 的相關資訊，請參閱 "還原Cloud Volumes ONTAP 或降級功能"。

"AFX 儲存系統"不支援回滾ONTAP軟體。

您可以從...	至...
ONTAP 9.18.1	ONTAP 9.17.1
ONTAP 9.17.1	ONTAP 9.16.1.
ONTAP 9.16.1.	ONTAP 9.15.1.1
ONTAP 9.15.1.1	ONTAP 9.14.1.
ONTAP 9.14.1.	ONTAP 9.13.1.12.9.11.9.11.
ONTAP 9.13.1.12.9.11.9.11.	ONTAP 9.12.1
ONTAP 9.12.1	零點9.11.1. ONTAP
零點9.11.1. ONTAP	零點9.10.1 ONTAP
零點9.10.1 ONTAP	部分9.9.1 ONTAP
部分9.9.1 ONTAP	部分9.8 ONTAP
部分9.8 ONTAP	更新ONTAP

您可以從...	至...
更新ONTAP	ONTAP 9.6
ONTAP 9.6	版本9.5 ONTAP

ONTAP 回復問題和限制

還原 ONTAP 叢集之前，您必須先考慮還原問題和限制。

- 還原會中斷營運。

  還原期間無法進行用戶端存取。如果您要還原正式作業叢集、請務必將此中斷納入規劃。

- 還原會影響叢集中的所有節點。

  還原作業會影響叢集中的所有節點、但是還原作業必須在每個HA配對上執行並完成、才能還原其他HA配對。

  "AFX 儲存系統"不支援回滾。

- 當所有節點都執行新的目標版本時、還原即告完成。

  當叢集處於混合版本狀態時、您不應輸入任何變更叢集作業或組態的命令、除非是為了滿足還原需求；允許監控作業。

  如果您已經還原了部分節點，但並非全部節點，請不要嘗試將叢集升級回來源版本。

- 當您還原節點時、節點會清除Flash Cache模組中的快取資料。

  由於Flash Cache模組中沒有快取資料、因此該節點可處理磁碟的初始讀取要求、因此在此期間會降低讀取效能。節點會在處理讀取要求時重新填入快取。

- 備份到ONTAP 執行於還原作業系統上的磁帶的LUN、只能還原至9.x版及更新版本、而不能還原至較早版本。
- 如果您目前版本ONTAP 的支援頻內ACP（IBACP）功能、而且您回復ONTAP 到不支援IBACP的版本、則磁碟櫃的替代路徑將會停用。
- 如果您的任何儲存虛擬機器（SVM）使用LDAP、則必須在還原之前停用LDAP參照。
- 在使用符合MetroCluster標準但未經MetroCluster驗證的交換器的MetroCluster IP 系統中，從ONTAP 9.7 回滾到 9.6 會造成乾擾，因為不支援使用ONTAP 9.6 及更早版本的系統。
- 在將節點還原為 ONTAP 9.13.1 或更早版本之前、您必須先將加密的 SVM 根 Volume 轉換為未加密的 Volume

  如果您嘗試還原到不支援 SVM 根磁碟區加密的ONTAP版本，系統將發出警告並阻止復原。

準備 ONTAP 還原

還原 ONTAP 叢集之前要檢閱的資源

在還原 ONTAP 叢集之前，您應該先確認硬體支援，並檢閱資源，以瞭解您可能會遇到或需要解決的問題。

1. 檢閱目標版本的"發行說明ONTAP"。

   「重要注意事項」一節說明降級或還原之前應注意的潛在問題。

2. 確認目標版本支援您的硬體平台。

   "NetApp Hardware Universe"

3. 確認目標版本支援您的叢集和管理交換器。

   您必須驗證NX-OS（叢集網路交換器）、IOS（管理網路交換器）和參考組態檔（RCF）軟體版本是否與ONTAP 您要還原的版本不一致。

   "NetApp下載：Cisco乙太網路交換器"

4. 如果您的叢集已設定為SAN、請確認SAN組態已完全受支援。

   應支援所有SAN元件、包括目標ONTAP 版的整套軟體、主機作業系統和修補程式、必要的主機公用程式軟體、以及介面卡驅動程式和韌體。

   "NetApp 互通性對照表工具"

在還原 ONTAP 叢集之前執行的系統驗證

還原 ONTAP 叢集之前，您應該先確認叢集健全狀況，儲存健全狀況和系統時間。您也應該確認叢集上沒有執行任何工作。

驗證叢集健全狀況

在還原 ONTAP 叢集之前，您應該先確認節點狀況良好且符合參與叢集的資格，而且叢集已達到仲裁。

步驟

1. 驗證叢集中的節點是否處於線上狀態、並符合參加叢集的資格：

   ```
   cluster show
   ```

   在此範例中，所有節點都是健全且符合參與叢集的資格。

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node0                 true    true
node1                 true    true
```

如果有任何節點不健全或不符合資格、請檢查EMS記錄是否有錯誤、並採取修正行動。

2. 將權限層級設為進階：

```
set -privilege advanced
```

輸入 `y` 以繼續。

3. 驗證每個RDB程序的組態詳細資料。

   - 每個節點的關聯式資料庫時期和資料庫時期應相符。
   - 所有節點的每個環仲裁主機都應該相同。

     請注意、每個振鈴都可能有不同的仲裁主機。

若要顯示此**RDB**程序...	輸入此命令...
管理應用程式	`cluster ring show -unitname mgmt`
Volume位置資料庫	`cluster ring show -unitname vldb`
虛擬介面管理程式	`cluster ring show -unitname vifmgr`
SAN管理精靈	`cluster ring show -unitname bcomd`

此範例顯示Volume位置資料庫程序：

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. 返回管理權限層級：

```
set -privilege admin
```

5. 如果您是在SAN環境中運作、請確認每個節點都位於SAN仲裁中：

```
event log show  -severity informational -message-name scsiblade.*
```

每個節點的最新scsimblet事件訊息應指出SCSI刀鋒處於仲裁狀態。

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node       Severity       Event
---------------  ---------- -------------- ---------------------------
MM/DD/YYYY TIME  node0      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME  node1      INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

相關資訊

"系統管理"

驗證儲存設備健全狀況

還原 ONTAP 叢集之前，您應該先確認磁碟，集合體和磁碟區的狀態。

步驟

1. 驗證磁碟狀態：

若要檢查...	執行此動作...
中斷的磁碟	a. 顯示任何毀損的磁碟： `storage disk show -state broken` b. 移除或更換任何損壞的磁碟。
正在進行維護或重建的磁碟	a. 顯示任何處於維護、擱置或重建狀態的磁碟： `storage disk show -state maintenance`
pending	reconstructing ---- .. 請等待維護或重建作業完成後再繼續。

2. 顯示實體與邏輯儲存設備的狀態，包括儲存區集合體，以確認所有集合體均為線上狀態： +

```
storage aggregate show -state !online
```

此命令會顯示_非_線上的集合體。執行重大升級或還原之前和之後、所有集合體都必須處於線上狀態。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. 顯示任何非連線的磁碟區、以驗證所有磁碟區是否都在線上：

```
volume show -state !online
```

執行重大升級或還原之前和之後、所有磁碟區都必須處於線上狀態。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 確認沒有不一致的磁碟區：

```
volume show -is-inconsistent true
```

查看"NetApp知識庫：顯示WAFL不一致的捲"如何解決不一致的問題。

相關資訊

"磁碟與Aggregate管理"

驗證系統時間

在還原 ONTAP 叢集之前，您應該確認已設定 NTP ，而且時間已在整個叢集上同步。

步驟

1. 確認叢集與 NTP 伺服器相關聯：

```
cluster time-service ntp server show
```

2. 驗證每個節點的日期和時間是否相同：

```
cluster date show
```

```
cluster1::> cluster date show
Node      Date                Timezone
--------- ------------------- -------------------------
node0     4/6/2013 20:54:38   GMT
node1     4/6/2013 20:54:38   GMT
node2     4/6/2013 20:54:38   GMT
node3     4/6/2013 20:54:38   GMT
4 entries were displayed.
```

確認沒有工作正在執行

還原 ONTAP 叢集之前，您應該先確認叢集工作的狀態。如果有任何 Aggregate ， Volume ， NDMP （傾印或還原）或 Snapshot 工作（例如建立，刪除，移動，修改，複寫及掛載工作）正在執行或佇列中，您應該允許工作順利完成或停止佇列中的項目。

步驟

1. 檢閱任何執行中或佇列中的 Aggregate ， Volume 或 Snapshot 工作清單：

```
job show
```

在此範例中，有兩個工作排入佇列：

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
8629   Vol Reaper           cluster1   -              Queued
       Description: Vol Reaper Job
8630   Certificate Expiry Check
                            cluster1   -              Queued
       Description: Certificate Expiry Check
```

2. 刪除任何執行中或佇列中的 Aggregate ， Volume 或 Snapshot 工作：

```
job delete -id <job_id>
```

3. 確認沒有執行或佇列任何 Aggregate ， Volume 或 Snapshot 工作：

```
job show
```

在此範例中、所有執行中和佇列中的工作都已刪除：

```
cluster1::> job show
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
9944   SnapMirrorDaemon_7_2147484678
                            cluster1   node1          Dormant
       Description: Snapmirror Daemon for 7_2147484678
18377  SnapMirror Service Job
                            cluster1   node0          Dormant
       Description: SnapMirror Service Job
2 entries were displayed
```

相關資訊

- "儲存磁碟顯示"

執行 ONTAP 版本特定的還原前檢查

ONTAP 版本所需的還原前工作

視您的 ONTAP 版本而定，您可能需要在開始還原程序之前執行其他準備工作。

如果您從 ...	開始還原程序之前，請執行下列步驟 ...
任何 ONTAP 9 版本	• "終止非持續可用的 SMB 工作階段"。 • "檢閱SnapMirror和SnapVault 彼此之間的還原要求"。 • "確認已刪除的重複磁碟區有足夠的可用空間"。 • "準備快照"。 • "將 SnapLock 磁碟區的自動認可期間設為小時"。 • 如果您有 MetroCluster 組態"停用自動非計畫性切換"，。 • "回應異常活動的自發勒索軟體保護警告"恢復之前。
ONTAP 9.18.1	• 如果已將 ARP 的自動啟用設定為 ONTAP 9.18.1 升級的一部分，則需要"停用它"。
ONTAP 9.17.1	• 如果您已為 SAN 啟用ONTAP ARP 功能， "停用它" 。
ONTAP 9.16.1.	• 如果您設定了 TLS 來進行 NVMe / TCP 連線"停用 NVMe 主機上的 TLS 組態"，。 • 如果您已啟用延伸 qtree 效能監控，"停用它"。 • 如果您使用 CORS 來存取 ONTAP S3 儲存區"移除 CORS 組態"，。
ONTAP 9.14.1.	如果您已啟用用戶端連線的主幹連線，"停用任何 NFSv4.1 伺服器上的主幹連線"。
ONTAP 9.12.1	• 如果您已設定 S3 用戶端存取 NAS 資料，"移除 S3 NAS 貯體組態。" • 如果您執行的是 NVMe 傳輸協定，並已設定頻內驗證，請參閱"停用頻內驗證"。 • 如果您有 MetroCluster 組態"停用 IPsec"，。
ONTAP 9.11.1.	如果您已設定了自動勒索軟體保護（ARP），"檢查 ARP 授權"。
ONTAP 9.6	如果您有 SnapMirror 同步關係，"準備要還原的關係"。

任何 **ONTAP 9** 版本

在還原 **ONTAP** 之前終止某些 **SMB** 工作階段

從任何版本的 ONTAP 9 還原 ONTAP 叢集之前，您應該先識別並妥善終止任何非持續可用的 SMB 工作階段。

使用SMB 3.0傳輸協定的Hyper-V或Microsoft SQL Server用戶端可存取持續可用的SMB共用區、不需要在升級或降級之前終止。

步驟

1. 找出任何無法持續使用的既有SMB工作階段：

```
vserver cifs session show -continuously-available No -instance
```

此命令會顯示任何無法持續可用的 SMB 工作階段的詳細資訊。您應該先終止這些程式、再繼續ONTAP 執行「停止降級」。

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
            Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. 如有必要、請識別您所識別的每個 SMB 工作階段所開啟的檔案：

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare         No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare         No
Path: \file1.txt
2 entries were displayed.
```

ONTAP 還原 SnapMirror 和 SnapVault 關係的需求

`system node revert-to`命令會通知您任何需要刪除或重新設定的 SnapMirror 和 SnapVault 關係，以便完成還原程序。不過、在您開始還原之前、請務必瞭解這些需求。

- 所有SnapVault 的資料保護鏡射關係必須先靜止、然後再中斷。

  還原完成後，如果存在一般快照，您可以重新同步並恢復這些關係。

- 不應包含下列SnapMirror原則類型：SnapVault
  - 非同步鏡射

    您必須刪除使用此原則類型的任何關聯。

  - MirrorAndVault

    如果存在任何這些關係、您應該將SnapMirror原則變更為鏡射保存庫。

- 必須刪除所有負載共用鏡射關係和目的地磁碟區。
- 必須刪除與FlexClone目的地Volume的SnapMirror關係。
- 必須針對每個SnapMirror原則停用網路壓縮。
- 您必須從任何非同步鏡射類型的SnapMirror原則中移除all_source_snapshot規則。

  根磁碟區上的單一檔案Snapshot還原（SFSR）和部分檔案Snapshot還原（PFSR）作業已過時。

- 任何目前執行的單一檔案和快照還原作業都必須先完成，才能繼續還原。

您可以等待還原作業完成、也可以中止還原作業。

- 任何不完整的單一檔案和快照還原作業都必須使用命令來移除 `snapmirror restore`。

  如"指令參考資料ONTAP"需詳細 `snapmirror restore`資訊，請參閱。

在還原 **ONTAP** 之前，請先確認已刪除重複資料的磁碟區可用空間

在從任何版本的 ONTAP 9 還原 ONTAP 叢集之前，您必須確保這些磁碟區包含足夠的可用空間，以便進行還原作業。

該卷必須具有足夠的空間來容納透過內聯檢測零塊而實現的節省。查看"NetApp知識庫：如何在ONTAP 9 中透過重複資料刪除、壓縮和壓縮節省空間"。

如果您已在要還原的磁碟區上啟用重複資料刪除和資料壓縮、則必須在還原重複資料刪除之前還原資料壓縮。

步驟

1. 檢視在磁碟區上執行的效率作業進度：

```
volume efficiency show -fields vserver,volume,progress
```

2. 停止所有作用中和佇列中的重複資料刪除作業：

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. 將權限層級設為進階：

```
set -privilege advanced
```

4. 將磁碟區的效率中繼資料降級至 ONTAP 的目標版本：

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
-version <version>
```

   以下範例將 Volume Vola 上的效率中繼資料還原為 ONTAP 9.x

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```

   Volume Eff效率Rever-to命令會還原執行此命令之節點上的磁碟區。此命令不會還原節點之間的磁碟區。

5. 監控降級進度：

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. 如果還原失敗，請顯示執行個體，瞭解還原失敗的原因。

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. 還原作業完成後、返回管理權限層級：

```
set -privilege admin
```

深入瞭解 "邏輯儲存管理"。

在還原 **ONTAP** 叢集之前準備快照

在從任何版本的 ONTAP 9 還原 ONTAP 叢集之前，您必須停用所有快照原則，並刪除升級至目前版本後所建立的任何快照。

如果要在SnapMirror環境中還原、您必須先刪除下列鏡射關係：

- 所有負載共用鏡射關係
- 任何資料保護鏡射資料關係、都是ONTAP 以穩健的資料保護方式建立
- 如果叢集是ONTAP 在還原8.3.x中重新建立、則所有資料保護都會鏡射關係

步驟

1. 停用所有資料 SVM 的快照原則：

```
volume snapshot policy modify -vserver * -enabled false
```

2. 針對每個節點的集合體停用快照原則：
   a. 識別節點的集合體：

```
run -node <nodename> -command aggr status
```

   b. 停用每個 Aggregate 的快照原則：

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

   c. 對其餘每個節點重複此步驟。

3. 停用每個節點根磁碟區的快照原則：

   a. 識別節點的根磁碟區：

   ```
   run -node <node_name> -command vol status
   ```

   您可以在命令輸出的「 * 選項 * 」欄中，使用「 root 」字來識別根 Volume `vol status` 。

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

   a. 停用根磁碟區上的快照原則：

   ```
   run -node <node_name> vol options root_volume_name nosnap on
   ```

   b. 對其餘每個節點重複此步驟。

4. 刪除升級至目前版本後建立的所有快照：

   a. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

   b. 停用快照：

   ```
   snapshot policy modify -vserver * -enabled false
   ```

   c. 刪除節點較新版本的快照：

   ```
   volume snapshot prepare-for-revert -node <node_name>
   ```

   此命令會刪除每個資料磁碟區，根 Aggregate 和根磁碟區上較新版本的快照。

   如果無法刪除任何快照，命令會失敗，並通知您必須採取的任何必要動作，才能刪除快照。您必須完成必要的動作，然後重新執行 `volume snapshot prepare-for-revert`命令，才能繼續下一步。

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

a. 確認快照已刪除：

```
volume snapshot show -node nodename
```

b. 如果仍有任何較新版本的快照，請強制將其刪除：

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
-constituent true} -ignore-owners -force
```

c. 對其餘每個節點重複這些步驟。

d. 返回管理權限層級：

```
set -privilege admin
```

您必須在MetroCluster 雙叢集上執行這些步驟、以進行不必要的組態設定。

在還原 **ONTAP** 之前，請先設定 **SnapLock** 磁碟區的自動認可期間

從任何版本的 ONTAP 9 還原 ONTAP 叢集之前， SnapLock 磁碟區的自動認可期間值必須以小時為單位，而非以天為單位。您應該檢查 SnapLock 磁碟區的自動認可值，並視需要從數天修改為數小時。

步驟

1. 驗證叢集中是否有 SnapLock 磁碟區具有不受支援的自動認可期間：

```
volume snaplock show -autocommit-period *days
```

2. 將不支援的自動認可期間修改為小時

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

在恢復**MetroCluster**配置之前停用自動計劃外切換

在恢復運行任何版本ONTAP 9 的MetroCluster配置之前，必須停用自動排程外切換(AUSO)。

步驟

1. 在 MetroCluster 中的兩個叢集上、停用自動非計畫性切換：

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

相關資訊

"支援管理與災難恢復MetroCluster"

在**ONTAP**回溯之前，請先解決自主勒索軟體防護 **(ARP)** 中的活動警告。

在還原至ONTAP 9.17.1 或更早版本之前，您應該對 Autonomous Ransomware Protection (ARP) 報告的任何異常活動警告做出回應，並刪除任何相關的 ARP 螢幕截圖。

開始之前

您需要「進階」權限才能刪除 ARP 快照。

步驟

1. 回應回報的任何異常活動警告"ARP"，並解決任何潛在問題。
2. 確認這些問題已解決後再恢復，選擇「更新並清除可疑檔案類型」以記錄您的決定並恢復正常的 ARP 監控。
3. 執行以下命令，列出與警告相關的所有 ARP 螢幕截圖：

```
volume snapshot snapshot show -fs-version 9.18
```

4. 刪除與警告相關的所有 ARP 螢幕截圖：

> 此指令會刪除所有具有目前ONTAP版本所用格式的快照，可能不只是 ARP 快照。在執行此命令之前，請確保已對所有要刪除的快照採取必要的措施。

```
volume snapshot prepare-for-revert -node <node_name>
```

ONTAP 9.18.1

在從 **ONTAP 9.18.1** 版本回溯之前，請停用自動啟用自主勒索軟體防護功能。

如果您將磁碟區升級到 ONTAP 9.18.1，則在短暫的寬限期（12 小時）後,ONTAP ARP 自動啟用功能可能已為您的磁碟區設定。建議您在降級到 ONTAP 9.17.1 或更早版本之前,先

在已升級至 ONTAP 9.18.1 的磁碟區上停用此自動啟用設定。

步驟

1. 確定已升級至 ONTAP 9.18.1 或更高版本的磁碟區是否已啟動自動啟用選項：

```
security anti-ransomware auto-enable show
```

2. 停用 SVM 上所有磁碟區的勒索軟體防護自動啟用選項：

```
security anti-ransomware volume disable -volume * -auto-enabled-volumes
-only true
```

ONTAP 9.17.1

從**ONTAP 9.17.1** 恢復前，請停用 **SAN** 磁碟區上的自主勒索軟體防護

ONTAP 9.16.1 及更早版本不支援 SAN 磁碟區的ONTAP ARP 功能。建議您在還原到ONTAP 9.16.1 或更早版本之前停用 SAN 磁碟區上的 ARP，以防止此功能保持活動狀態並佔用 CPU 和磁碟資源，而無需對還原的版本執行任何實際偵測。

範例 **7.** 步驟

系統管理員

1. 選擇“儲存 **>** 磁碟區”，然後選擇磁碟區的名稱。
2. 在 **Volumes** 概覽的 **Security** 標籤中，選擇 **Status** 從 Enabled 切換到 Disabled。

CLI

1. 禁用卷上的勒索軟體保護：

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9.16.1.

從 **ONTAP 9.16.1** 還原之前，請先停用 **NVMe** 主機上的 **TLS**

如果您在 NVMe 主機上設定了適用於 NVMe / TCP 連線的 TLS 安全通道，則必須先停用它，才能從 ONTAP 9.16.1 還原叢集。

步驟

1. 從主機移除 TLS 安全通道組態：

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

此命令會從子系統移除主機，然後在沒有 TLS 組態的情況下重新建立子系統中的主機。

2. 確認已從主機移除 TLS 安全通道：

```
vserver nvme subsystem host show
```

從 **ONTAP 9.16.1** 還原之前，請先停用延伸的 **Qtree** 效能監控

從 ONTAP 9 。 16.1 開始，您可以使用 ONTAP REST API 來存取延伸的 qtree 監控功能，包括延遲指標和歷史統計資料。如果在任何 qtree 上啟用延伸 qtree 監控，則在從 9.16.1 還原之前，您必須先將其設 `ext_performance_monitoring.enabled`為假。

深入瞭解 "使用延伸 qtree 效能監控還原叢集"。

從 **ONTAP 9.16.1** 還原之前，請先移除 **CORS** 組態

如果您使用跨來源資源共享（ CORS ）來存取 ONTAP S3 儲存區，則必須先將其移除，才能從 ONTAP 9.16.1 回復。

深入瞭解 "使用 CORS 還原 ONTAP 叢集"。

ONTAP 9.14.1.

從 **ONTAP 9.14.1** 還原之前，請先停用 **NFSv4.1** 工作階段主幹

如果您已啟用用戶端連線的主幹連線，則必須先停用任何 NFSv4.1 伺服器上的主幹連線，然後才能從 ONTAP 9.14.1 還原。

當您輸入時 `revert-to` 命令時、您會看到一則警告訊息、建議您在繼續之前停用主幹連線。

還原至 ONTAP 9.13.1 之後，使用中繼連線的用戶端會恢復為使用單一連線。他們的資料處理量將受到影響、但不會造成中斷。還原行為與將 SVM 的 NFSv4.1 主幹選項從啟用修改為停用相同。

步驟

1. 停用 NFSv4.1 伺服器上的主幹：

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. 確認NFS已設定為所需：

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

從 **ONTAP 9.12.1** 還原之前，請先移除 **S3 NAS** 貯體組態

如果您已設定 S3 用戶端存取 NAS 資料，則應使用 ONTAP 命令列介面（ CLI ）移除 NAS 儲存區組態，並在從 ONTAP 9.12.1 還原之前移除任何名稱對應（ S3 使用者至 Windows 或 Unix 使用者）。

關於這項工作

下列工作會在還原程序的背景中完成。

- 移除所有部分完成的單一物件建立（亦即隱藏目錄中的所有項目）。
- 移除所有隱藏的目錄；每個磁碟區上可能有一個、可從從S3 NAS儲存區對應的匯出根目錄存取。
- 移除上傳表。
- 刪除所有已設定S3伺服器的任何預設UNIX使用者和預設Windows使用者值。

步驟

1. 移除 S3 NAS 貯體組態：

   ```
   vserver object-store-server bucket delete -vserver <svm_name> -bucket
   <s3_nas_bucket_name>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket delete`資訊，請參閱。

2. 移除 UNIX 的名稱對應：

   ```
   vserver name-mapping delete -vserver <svm_name> -direction s3-unix
   ```

   如"指令參考資料ONTAP"需詳細 `vserver name-mapping delete`資訊，請參閱。

3. 移除 Windows 的名稱對應：

   ```
   vserver name-mapping delete -vserver <svm_name> -direction s3-win
   ```

4. 從 SVM 移除 S3 傳輸協定：

   ```
   vserver remove-protocols -vserver <svm_name> -protocols s3
   ```

   如"指令參考資料ONTAP"需詳細 `vserver remove-protocols`資訊，請參閱。

從 **ONTAP 9.12.1** 還原之前，請先停用 **NVMe** 頻內驗證

如果您執行的是 NVMe 傳輸協定，則必須先停用頻內驗證，才能從 ONTAP 9.12.1 還原叢集。如果未停用使用 DH-HMAC-CHAP 的頻內驗證、還原將會失敗。

步驟

1. 從子系統移除主機、以停用DH-HMAP-CHAP驗證：

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. 確認DH-HMAP-CHAP驗證傳輸協定已從主機移除：

```
vserver nvme subsystem host show
```

3. 無需驗證即可將主機重新新增回子系統：

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

從 **ONTAP 9.12.1** 還原之前，請先在 **MetroCluster** 組態中停用 **IPsec**

從 ONTAP 9.12.1 還原 MetroCluster 組態之前，您必須停用 IPsec 。

在還原之前執行檢查、以確保MetroCluster 不存在任何IPsec組態。您必須先移除任何現有的IPsec組態並停用IPsec、才能繼續還原。如果ONTAP 啟用IPsec、即使您尚未設定任何使用者原則、還原功能也會遭到封鎖。

零點**9.11.1. ONTAP**

從 **ONTAP 9.11.1** 還原之前，請先檢查自主勒索軟體保護授權

如果您已設定自動勒索軟體保護（ ARP ），並從 ONTAP 9.11.1 還原至 ONTAP 9.10.1 ，您可能會遇到警告訊息和有限的 ARP 功能。

在VMware 9.11.1中ONTAP 、勒索軟體授權取代了多租戶金鑰管理（MTKM）授權。如果您的系統具有反勒索軟體授權、但沒有MT_EK-Mgmt授權、則在還原期間、您會看到一則警告訊息、指出在還原時、無法在新磁碟區上啟用ARP。

具有現有保護的磁碟區在還原後仍可正常運作、並可使用ONTAP CLI顯示Arp狀態。沒有 MTKM 授權、 System Manager 無法顯示 ARP 狀態。

因此、如果您想要在還原ONTAP 至S還原9.10.1之後繼續使用Arp、請確定已安裝MTKM授權、然後再還原。 "瞭解有關ARP授權的資訊。"

從具有 **SnapMirror** 同步關係的 **ONTAP 9.6** 還原系統的考量事項

在從 ONTAP 9 第 6 節還原至 ONTAP 9 第 5 節之前、您必須注意 SnapMirror 同步關係的考量事項。

還原之前、如果您有 SnapMirror 同步關係、則必須採取下列步驟：

- 您必須刪除來源 Volume 使用 NFSv4 或 SMB 提供資料的任何 SnapMirror 同步關係。

  不支援NFSv4和SMB。ONTAP

- 您必須刪除鏡射鏡射串聯部署中的任何 SnapMirror 同步關係。

  ONTAP 9 中的 SnapMirror 同步關係不支援鏡射鏡射串聯部署。 5

- 如果 ONTAP 9.5 中的一般快照在還原期間不可用，則還原後必須初始化 SnapMirror 同步關係。

  升級至 ONTAP 9.6 兩小時後， ONTAP 9.5 的一般快照會自動取代為 ONTAP 9.6 中的一般快照。因此，如果 ONTAP 9.5 的一般快照無法使用，則還原後就無法重新同步 SnapMirror 同步關係。

下載並安裝**ONTAP** 更新版的軟體映像

在還原目前的 ONTAP 軟體之前，您必須先從 NetApp 支援網站下載目標軟體版本，然後再進行安裝。

下載 **ONTAP** 軟體映像

軟體映像是特定於平台機型。您必須取得適用於叢集的正確映像。NetApp 支援網站上提供適用於您平台機型的軟體映像檔、韌體版本資訊及最新韌體。軟體映像包含ONTAP 系統韌體的最新版本、在發佈特定版本的資訊時、即可取得此版本。

> ⓘ 如果您要從 ONTAP 9.5 或更新版本還原具有 NetApp Volume Encryption 的系統，則必須為非受限國家 / 地區下載 ONTAP 軟體映像，其中包括 NetApp Volume Encryption 。如果您將 ONTAP 軟體映像用於受限國家 / 地區，以還原採用 NetApp Volume Encryption 的系統，系統會出現問題，您將無法存取您的磁碟區。

步驟

1. 在 "軟體下載"NetApp 支援網站的區域中找到目標 ONTAP 軟體。
2. 複製軟體映像（例如， `97_q_image.tgz` ）來自NetApp支援站點

   您可以將映像複製到 HTTP 伺服器或 FTP 伺服器上要提供映像的目錄，或是複製到本機資料夾。

安裝 **ONTAP** 軟體映像

從 NetApp 支援網站下載目標 ONTAP 軟體映像之後，請將其安裝在叢集節點上。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

進階提示 (*>) 。

2. 出現提示時，輸入 `y`以繼續。
3. 安裝軟體映像：
   - 對於標準組態或雙節點 MetroCluster 組態，請輸入下列命令：

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault true
```

此命令可同時下載並安裝所有節點上的軟體映像。若要在每個節點上一次下載並安裝映像，請勿指定 `-background`參數。此命令也會使用延伸查詢，將安裝為替代映像的目標軟體映像變更為節點的預設映像。

   - 對於四節點或八節點 MetroCluster 組態，請在兩個叢集上輸入下列命令：

```
system node image update -node * -package
<http://example.com/downloads/image.tgz> -replace-package true
-replace {image1|image2} -background true -setdefault false
```

此命令可同時下載並安裝所有節點上的軟體映像。若要在每個節點上一次下載並安裝映像，請勿指定 `-background`參數。此命令也會使用延伸查詢來變更目標軟體映像，該映像會安裝為每個節點上的替代映像。

4. 輸入 `y` 以在出現提示時繼續。
5. 確認軟體映像已下載並安裝在每個節點上：

```
system node image show-update-progress -node *
```

此命令會顯示軟體映像下載與安裝的目前狀態。您應該繼續執行此命令，直到所有節點報告“運行狀態”為“退出”，並且“退出狀態”為“成功”。

系統節點映像更新命令可能會失敗、並顯示錯誤或警告訊息。解決任何錯誤或警告之後、您可以再次執行命令。

此範例顯示兩個節點的叢集、其中軟體映像會下載並成功安裝在兩個節點上：

```
cluster1::*> system node image show-update-progress -node *
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node0.
There is no update/install in progress
Status of most recent operation:
        Run Status:     Exited
        Exit Status:    Success
        Phase:          Run Script
        Exit Message:   After a clean shutdown, image2 will be set as
the default boot image on node1.
2 entries were acted on.
```

相關資訊

- "系統節點映像更新"

還原ONTAP 整個叢集

還原 ONTAP 叢集會造成中斷。您必須在還原期間使叢集離線。如果沒有技術支援人員的協助，您不應回復正式作業叢集。

若要還原新叢集或測試叢集，您必須停用儲存容錯移轉，資料生命和位址還原先決條件，然後必須在叢集中的每個節點上還原叢集和檔案系統組態。

開始之前。

- 您應該已經完成了"預先還原驗證"。
- 您應該已完成所需的"預先檢查您的特定 ONTAP 版本"。
- 你應該"下載並安裝目標 ONTAP 軟體映像" 。

步驟 1 ：準備叢集以進行還原

在還原任何叢集節點之前，您應該先確認已安裝目標 ONTAP 映像，而且應該停用叢集中的所有資料生命。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

系統提示您繼續時、請輸入* y*。

2. 確認已安裝目標 ONTAP 軟體：

```
system image show
```

以下範例顯示， 9.13.1 版會安裝為兩個節點上的替代映像：

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

3. 停用叢集中的所有資料生命：

```
network interface modify {-role data} -status-admin down
```

4. 判斷您是否有叢集間FlexCache 的相依關係：

```
flexcache origin show-caches -relationship-type inter-cluster
```

5. 如果存在叢集間的快閃資源包、請停用快取叢集上的資料資源包：

```
network interface modify -vserver <vserver_name> -lif <lif_name> -status
-admin down
```

步驟 **2** ：還原叢集節點

若要還原叢集，您必須還原 HA 配對中的第一個節點，然後還原合作夥伴節點。接著，您可以針對叢集中的每個 HA 配對重複此程序，直到所有節點都還原為止。如果您有 MetroCluster 組態，則需要針對組態中的兩個叢集重複這些步驟。

4 個或更多節點

步驟

1. 登入您要還原的節點。

   若要還原節點、您必須透過節點的節點管理LIF登入叢集。

2. 停用 HA 配對中節點的儲存容錯移轉：

   ```
   storage failover modify -node <nodename> -enabled false
   ```

   HA配對只需停用一次儲存容錯移轉。當您停用節點的儲存容錯移轉時、節點的合作夥伴也會停用儲存容錯移轉。

3. 將節點的目標 ONTAP 軟體映像設定為預設映像：

   ```
   system image modify -node <nodename> -image <target_image>
   -isdefault true
   ```

4. 確認目標 ONTAP 軟體映像已設為您要還原之節點的預設映像：

   ```
   system image show
   ```

   以下範例顯示 9.13.1 版已設為 node0 上的預設映像：

   ```
   cluster1::*> system image show
                    Is      Is                  Install
   Node     Image   Default Current Version     Date
   -------- ------- ------- ------- --------    -------------------
   node0
            image1  false   true    9.14.1       MM/DD/YYYY TIME
            image2  true    false   9.13.1       MM/DD/YYYY TIME
   node1
            image1  true    true    9.14.1       MM/DD/YYYY TIME
            image2  false   false   9.13.1       MM/DD/YYYY TIME
   4 entries were displayed.
   ```

5. 確認節點已準備好進行還原：

   ```
   system node revert-to -node <nodename> -check-only true -version 9.x
   ```

   此 `check-only`參數會識別還原之前必須解決的任何先決條件，例如停用快照原則或刪除升級至較新版

ONTAP 後建立的快照。

此 `-version`選項是指您要還原的 ONTAP 版本。例如，如果您要從 9.14.1 還原至 9.13.1 ，則選項的正確值 `-version`為 9.13.1 。

6. 還原節點的叢集組態：

```
system node revert-to -node <nodename> -version 9.x
```

叢集組態會還原、然後從叢集Shell登出。

7. 等待登入提示；當系統詢問您是否要登入系統殼層時，請輸入 * 否 * 。

登入提示可能需要 30 分鐘或更長時間才會出現。

8. 使用 admin 登入叢集 Shell 。
9. 切換至節點網站：

```
run -node <nodename>
```

再次登入叢集Shell之後、可能需要幾分鐘的時間才能準備好接受nodesdell命令。因此、如果命令失敗、請稍候幾分鐘、然後再試一次。

10. 還原節點的檔案系統組態：

```
revert_to 9.x
```

此命令可驗證節點的檔案系統組態是否已準備好還原、然後還原。如果發現任何先決條件，您必須解決這些先決條件，然後重新執行 `revert_to`命令。

使用系統主控台來監控還原程序、顯示的詳細資料比在節點上看到的更多。

如果自動開機為true、則命令完成後、節點將重新開機ONTAP 至flex.

如果自動開機為假，則命令完成時會顯示 Loader 提示。輸入 `yes`以還原，然後使用 `boot_ontap`手動重新啟動節點。

11. 節點重新開機後、請確認新軟體正在執行：

```
system node image show
```

在下列範例中、image1是新ONTAP 的版本、並設為節點0上的目前版本：

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

12. 確認節點的還原狀態為完成：

```
system node upgrade-revert show -node <nodename>
```

狀態應列為「完成」、「不需要」或「沒有傳回表格項目」。

13. 在 HA 配對的另一個節點上重複這些步驟，然後針對每個額外的 HA 配對重複這些步驟。

如果您有 MetroCluster 組態，則需要在組態中的兩個叢集上重複這些步驟

14. 還原所有節點之後，請重新啟用叢集的高可用度：

```
storage failover modify -node* -enabled true
```

雙節點叢集

1. 登入您要還原的節點。

若要還原節點、您必須透過節點的節點管理LIF登入叢集。

2. 停用叢集高可用度（ HA ）：

```
cluster ha modify -configured false
```

3. 停用儲存容錯移轉：

```
storage failover modify -node <nodename> -enabled false
```

HA配對只需停用一次儲存容錯移轉。當您停用節點的儲存容錯移轉時、節點的合作夥伴也會停用儲存容錯移轉。

4. 將節點的目標 ONTAP 軟體映像設定為預設映像：

```
system image modify -node <nodename> -image <target_image>
-isdefault true
```

5. 確認目標 ONTAP 軟體映像已設為您要還原之節點的預設映像：

```
system image show
```

以下範例顯示 9.13.1 版已設為 node0 上的預設映像：

```
cluster1::*> system image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   false   true    9.14.1       MM/DD/YYYY TIME
         image2   true    false   9.13.1       MM/DD/YYYY TIME
node1
         image1   true    true    9.14.1       MM/DD/YYYY TIME
         image2   false   false   9.13.1       MM/DD/YYYY TIME
4 entries were displayed.
```

6. 檢查節點目前是否保留 epsilon ：

```
cluster show -node <nodename>
```

下列範例顯示節點擁有epsilon：

```
cluster1::*> cluster show -node node1

          Node: node1
          UUID: 026efc12-ac1a-11e0-80ed-0f7eba8fc313
       Epsilon: true
   Eligibility: true
        Health: true
```

a. 如果節點保留 epsilon 、請在節點上將 epsilon 標記為 false 、以便將 epsilon 傳輸至節點的合作夥伴：

```
cluster modify -node <nodename> -epsilon false
```

b. 在合作夥伴節點上標示 epsilon true 、將 epsilon 傳輸至節點的合作夥伴：

```
cluster modify -node <node_partner_name> -epsilon true
```

7. 確認節點已準備好進行還原：

```
system node revert-to -node <nodename> -check-only true -version 9.x
```

此 `check-only`參數可識別還原之前必須解決的任何情況，例如停用快照原則或刪除升級至較新版 ONTAP 後建立的快照。

這 `-version` 選項指的是您要還原到的ONTAP版本。只需要ONTAP版本的前兩個值。例如，如果您要從 9.14.1 版本回溯到 9.13.1 版本，則正確的值為： `-version` 選項為 9.13。

叢集組態會還原、然後從叢集Shell登出。

8. 還原節點的叢集組態：

```
system node revert-to -node <nodename> -version 9.x
```

9. 等待登入提示，然後在系統詢問您是否要登入 systemshell 時輸入 `No`。

登入提示可能需要 30 分鐘或更長時間才會出現。

10. 使用 admin 登入叢集 Shell 。
11. 切換至節點網站：

```
run -node <nodename>
```

再次登入叢集Shell之後、可能需要幾分鐘的時間才能準備好接受nodesdell命令。因此、如果命令失敗、請稍候幾分鐘、然後再試一次。

12. 還原節點的檔案系統組態：

```
revert_to 9.x
```

此命令可驗證節點的檔案系統組態是否已準備好還原、然後還原。如果發現任何先決條件，您必須解決這些先決條件，然後重新執行 `revert_to`命令。

使用系統主控台來監控還原程序、顯示的詳細資料比在節點上看到的更多。

如果自動開機為true、則命令完成後、節點將重新開機ONTAP 至flex.

如果自動開機為假、則命令完成時會顯示載入器提示字元。輸入 `yes` 若要還原、請使用 `boot_ontap` 手動重新啟動節點。

13. 節點重新開機後、請確認新軟體正在執行：

```
system node image show
```

在下列範例中、image1是新ONTAP 的版本、並設為節點0上的目前版本：

```
cluster1::*> system node image show
                  Is      Is                  Install
Node     Image    Default Current Version     Date
-------- -------  ------- ------- --------    -------------------
node0
         image1   true    true    X.X.X        MM/DD/YYYY TIME
         image2   false   false   Y.Y.Y       MM/DD/YYYY TIME
node1
         image1   true    false   X.X.X       MM/DD/YYYY TIME
         image2   false   true    Y.Y.Y       MM/DD/YYYY TIME
4 entries were displayed.
```

14. 確認節點的還原狀態為完成：

```
system node upgrade-revert show -node <nodename>
```

狀態應列為「完成」、「不需要」或「沒有傳回表格項目」。

15. 在 HA 配對的另一個節點上重複這些步驟。
16. 還原兩個節點之後，請重新啟用叢集的高可用度：

```
cluster ha modify -configured true
```

17. 在兩個節點上重新啟用儲存容錯移轉：

```
storage failover modify -node <nodename> -enabled true
```

相關資訊

- "儲存故障轉移修改"

ONTAP 還原後的處理方式

ONTAP 還原後，請驗證叢集和儲存設備健全狀況

還原 ONTAP 叢集之後，您應該確認節點狀況良好且符合參與叢集的資格，而且叢集已達到仲裁。您也應該確認磁碟、集合體和磁碟區的狀態。

驗證叢集健全狀況

步驟

1. 驗證叢集中的節點是否處於線上狀態、並符合參加叢集的資格：

   ```
   cluster show
   ```

   在此範例中，叢集健全，所有節點都有資格參與叢集。

   ```
   cluster1::> cluster show
   Node                  Health  Eligibility
   --------------------- ------- ------------
   node0                 true    true
   node1                 true    true
   ```

   如果有任何節點不健全或不符合資格、請檢查EMS記錄是否有錯誤、並採取修正行動。

2. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

   輸入 `y` 以繼續。

3. 驗證每個RDB程序的組態詳細資料。

   - 每個節點的關聯式資料庫時期和資料庫時期應相符。
   - 所有節點的每個環仲裁主機都應該相同。

     請注意、每個振鈴都可能有不同的仲裁主機。

若要顯示此**RDB**程序...	輸入此命令...
管理應用程式	`cluster ring show -unitname mgmt`
Volume位置資料庫	`cluster ring show -unitname vldb`
虛擬介面管理程式	`cluster ring show -unitname vifmgr`
SAN管理精靈	`cluster ring show -unitname bcomd`

此範例顯示Volume位置資料庫程序：

```
cluster1::*> cluster ring show -unitname vldb
Node      UnitName Epoch    DB Epoch DB Trnxs Master    Online
--------- -------- -------- -------- -------- --------- ---------
node0     vldb     154      154      14847    node0     master
node1     vldb     154      154      14847    node0     secondary
node2     vldb     154      154      14847    node0     secondary
node3     vldb     154      154      14847    node0     secondary
4 entries were displayed.
```

4. 返回管理權限層級：

```
set -privilege admin
```

5. 如果您是在SAN環境中運作、請確認每個節點都位於SAN仲裁中：

```
event log show  -severity informational -message-name scsiblade.*
```

每個節點的最新scsimblet事件訊息應指出SCSI刀鋒處於仲裁狀態。

```
cluster1::*> event log show  -severity informational -message-name
scsiblade.*
Time              Node        Severity       Event
---------------   ----------  -------------- ---------------------------
MM/DD/YYYY TIME   node0       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
MM/DD/YYYY TIME   node1       INFORMATIONAL  scsiblade.in.quorum: The
scsi-blade ...
```

相關資訊

"系統管理"

驗證儲存設備健全狀況

還原或降級叢集之後、您應該確認磁碟、集合體和磁碟區的狀態。

步驟

1. 驗證磁碟狀態：

若要檢查...	執行此動作...
中斷的磁碟	a. 顯示任何毀損的磁碟： `storage disk show -state broken` b. 移除或更換任何損壞的磁碟。
正在進行維護或重建的磁碟	a. 顯示任何處於維護、擱置或重建狀態的磁碟： `storage disk show -state maintenance`
pending	reconstructing ---- .. 請等待維護或重建作業完成後再繼續。

2. 顯示實體與邏輯儲存設備的狀態（包括儲存集合體）、以確認所有集合體均處於線上狀態：

```
storage aggregate show -state !online
```

此命令會顯示_非_線上的集合體。執行重大升級或還原之前和之後、所有集合體都必須處於線上狀態。

```
cluster1::> storage aggregate show -state !online
There are no entries matching your query.
```

3. 顯示任何非連線的磁碟區、以驗證所有磁碟區是否都在線上：

```
volume show -state !online
```

執行重大升級或還原之前和之後、所有磁碟區都必須處於線上狀態。

```
cluster1::> volume show -state !online
There are no entries matching your query.
```

4. 確認沒有不一致的磁碟區：

```
volume show -is-inconsistent true
```

查看"NetApp知識庫：顯示WAFL不一致的捲"如何解決不一致的問題。

驗證用戶端存取（SMB和NFS）

對於已設定的傳輸協定、請測試SMB和NFS用戶端的存取、以驗證叢集是否可存取。

相關資訊

- "磁碟與Aggregate管理"
- "儲存磁碟顯示"

在 ONTAP 還原後，啟用 MetroCluster 組態的自動切換

還原 ONTAP MetroCluster 組態之後，您必須啟用自動非計畫性切換，以確保 MetroCluster 組態完全正常運作。

步驟

1. 啟用自動非計畫性切換：

```
metrocluster modify -auto-switchover-failure-domain auso-on-cluster-
disaster
```

2. 驗證 MetroCluster 組態：

```
metrocluster check run
```

在重新開機期間、部分LIF可能已移轉至指派的容錯移轉連接埠。還原 ONTAP 叢集之後，您必須啟用並還原不在其主連接埠上的任何生命。

如果主連接埠正常運作、網路介面還原命令會將目前不在主連接埠上的LIF還原回主連接埠。LIF的主連接埠是在建立LIF時指定、您可以使用network interface show命令來判斷LIF的主連接埠。

步驟

1. 顯示所有生命的狀態：

```
network interface show
```

此範例顯示儲存虛擬機器（SVM）的所有LIF狀態。

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001    down/down  192.0.2.120/24     node0         e0e
true
            data002    down/down  192.0.2.121/24     node0         e0f
true
            data003    down/down  192.0.2.122/24     node0         e2a
true
            data004    down/down  192.0.2.123/24     node0         e2b
true
            data005    down/down  192.0.2.124/24     node0         e0e
false
            data006    down/down  192.0.2.125/24     node0         e0f
false
            data007    down/down  192.0.2.126/24     node0         e2a
false
            data008    down/down  192.0.2.127/24     node0         e2b
false
8 entries were displayed.
```

如果任何生命週期顯示的狀態為「狀態管理」狀態為「關閉」或「為主目錄」狀態為「假」、請繼續下一步。

2. 啟用資料生命：

```
network interface modify {-role data} -status-admin up
```

3. 將LIF還原至其主連接埠：

```
network interface revert *
```

4. 確認所有的生命都在其主連接埠中：

```
network interface show
```

此範例顯示SVM vs0的所有lifs都位於其主連接埠上。

```
cluster1::> network interface show -vserver vs0
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
vs0
            data001      up/up    192.0.2.120/24     node0          e0e
true
            data002      up/up    192.0.2.121/24     node0          e0f
true
            data003      up/up    192.0.2.122/24     node0          e2a
true
            data004      up/up    192.0.2.123/24     node0          e2b
true
            data005      up/up    192.0.2.124/24     node1          e0e
true
            data006      up/up    192.0.2.125/24     node1          e0f
true
            data007      up/up    192.0.2.126/24     node1          e2a
true
            data008      up/up    192.0.2.127/24     node1          e2b
true
8 entries were displayed.
```

相關資訊

- "網路介面"

在 ONTAP 還原後啟用快照原則

還原至舊版 ONTAP 之後，您必須啟用快照原則，才能再次開始建立快照。

您正在重新啟用已停用的快照排程，然後再還原至舊版 ONTAP 。

步驟

1. 為所有資料 SVM 啟用快照原則：

```
volume snapshot policy modify -vserver * -enabled true
```

```
snapshot policy modify pg-rpo-hourly -enable true
```

2. 針對每個節點，啟用根磁碟區的快照原則：

```
run -node <node_name> vol options <volume_name> nosnap off
```

在 ONTAP 還原後驗證 IPv6 防火牆項目

從ONTAP 任何版本的更新版本還原、可能會導致防火牆原則中的某些服務缺少預設IPv6防火牆項目。您必須確認所需的防火牆項目已還原至您的系統。

步驟

1. 將所有防火牆原則與預設原則進行比較、以確認其正確無誤：

```
system services firewall policy show
```

下列範例顯示預設原則：

```
cluster1::*> system services firewall policy show
Policy           Service    Action IP-List
---------------- ---------- ------ --------------------
cluster
                 dns        allow  0.0.0.0/0
                 http       allow  0.0.0.0/0
                 https      allow  0.0.0.0/0
                 ndmp       allow  0.0.0.0/0
                 ntp        allow  0.0.0.0/0
                 rsh        allow  0.0.0.0/0
                 snmp       allow  0.0.0.0/0
                 ssh        allow  0.0.0.0/0
                 telnet     allow  0.0.0.0/0
data
                 dns        allow  0.0.0.0/0, ::/0
                 http       deny   0.0.0.0/0, ::/0
                 https      deny   0.0.0.0/0, ::/0
                 ndmp       allow  0.0.0.0/0, ::/0
                 ntp        deny   0.0.0.0/0, ::/0
                 rsh        deny   0.0.0.0/0, ::/0
.
.
.
```

2. 建立新的防火牆原則、手動新增任何遺失的預設 IPv6 防火牆項目：

```
system services firewall policy create -policy <policy_name> -service
ssh -action allow -ip-list <ip_list>
```

3. 將新原則套用至 LIF 以允許存取網路服務：

```
network interface modify -vserve <svm_name> -lif <lif_name> -firewall
-policy <policy_name>
```

在還原至 **ONTAP 9.8** 之後，驗證可以存取服務處理器的使用者帳戶

在 ONTAP 9.9.1 及更新版本中， `-role`使用者帳戶的參數會變更為 `admin`。如果您在 ONTAP 9.8 或更早版本上建立使用者帳戶，並升級至 ONTAP 9.9.1 或更新版本，然後還原至 ONTAP 9.8 ，則參數會還原 `-role`為其原始值。您應該確認修改後的值是可接受的。

在還原期間、如果已刪除SP使用者的角色、則會記錄「rbac.spuser.role.notfound" EMS訊息」。

如需詳細資訊、請參閱 "可存取SP的帳戶"。

叢集管理

使用System Manager進行叢集管理

了解如何使用 ONTAP System Manager 進行叢集管理

System Manager 是以 HTML5 為基礎的圖形管理介面、可讓您使用網頁瀏覽器來管理儲存系統和儲存物件（例如磁碟、磁碟區和儲存層）、並執行與儲存系統相關的一般管理工作。

- 系統管理員隨附於 ONTAP 軟體即 Web 服務、預設為啟用、並可使用瀏覽器存取。
- System Manager的名稱已從ONTAP 功能性更新至功能性更新9.6。在更新版本的版本中、它稱為「S25系統管理程式」ONTAP OnCommand 。從版本不含更新版本的版本開始、它稱為System Manager。ONTAP
- 如果您使用的是傳統系統管理員（僅適用於 ONTAP 9.7 及更早版本）、請參閱 "System Manager Classic（ONTAP 版本9.0至9.7）"

使用系統管理員儀表板、您可以一目瞭然地檢視重要警示與通知、儲存層級與磁碟區的效率與容量、叢集中可用的節點、HA配對中節點的狀態、最活躍的應用程式與物件、 以及叢集或節點的效能指標。

有了 ONTAP 9.7 及更新版本中的系統管理員，您可以執行許多常見工作，例如：

- 建立叢集、設定網路、以及設定叢集的支援詳細資料。
- 設定及管理儲存物件、例如磁碟、本機階層、磁碟區、qtree、 和配額。
- 設定SMB和NFS等傳輸協定、並配置檔案共用。
- 設定FC、FCoE、NVMe及iSCSI等傳輸協定以進行區塊存取。
- 建立及設定網路元件、例如子網路、廣播網域、資料與管理介面、以及介面群組。
- 設定及管理鏡射與保存關係。
- 執行叢集管理、儲存節點管理及儲存虛擬機器（儲存VM）管理作業。
- 建立及設定儲存VM、管理與儲存VM相關的儲存物件、以及管理儲存VM服務。
- 監控及管理叢集中的高可用度（HA）組態。
- 將服務處理器設定為遠端登入、管理、監控及管理節點、無論節點的狀態為何。

System Manager術語

System Manager使用不同於CLI的詞彙來執行ONTAP 某些功能。

- * 本機層 * ：儲存資料的一組實體固態硬碟或硬碟機。您可能知道這些是集合體。事實上、如果您使用ONTAP 的是SURFCLI、您仍會看到用來代表本機層的術語_Aggregate。
- * 雲端層 * ：當您想要將部分資料放在內部環境之外時， ONTAP 所使用的雲端儲存空間，其原因有多種。如果您想要瞭解 FabricPool 的雲端部分，您已經知道了。而且StorageGRID 如果您使用的是一套資料不全系統、那麼您的雲端可能根本就不在內部部署。（內部部署的雲端體驗稱為_Private Cloud。）

- * 儲存 VM* ：在 ONTAP 中執行的虛擬機器，可為您的用戶端提供儲存和資料服務。您可能知道這是 *SVM* 或 *vserver* 。
- 網路介面：分配給實體網路連接埠的位址和屬性。您可能將其稱為邏輯介面 (LIF)。
- 暫停：暫停操作的操作。在ONTAP 9.8 之前的版本中，您可能在其他版本的 System Manager 中提到 *quiesce*。

使用 System Manager 存取 ONTAP 叢集

如果您偏好使用圖形介面、而非命令列介面（CLI）來存取及管理叢集、您可以使用ONTAP 預設啟用的、以供使用的System Manager（隨附於以Web服務形式提供的系統管理程式）來執行此作業、並可透過瀏覽器存取。

從ONTAP 9.12.1 開始，系統管理器與NetApp控制台完全整合。

使用控制台，您可以從單一控制平面管理混合多雲基礎設施，同時保留熟悉的系統管理器儀表板。

看"System Manager 與NetApp Console 集成" 。

關於這項工作

您可以使用叢集管理網路介面（LIF）或節點管理網路介面（LIF）來存取System Manager。若要不中斷地存取System Manager、您應該使用叢集管理網路介面（LIF）。

開始之前

- 您必須擁有一個叢集使用者帳戶、且該帳戶必須設定為「admin」角色、以及「http」和「Console」應用程式類型。
- 您必須在瀏覽器中啟用Cookie和網站資料。

步驟

1. 將網頁瀏覽器指向叢集管理網路介面的IP位址：
   - 如果您使用的是 IPv4 ： **`https://cluster-mgmt-LIF`**
   - 如果您使用的是 IPv6 ： **`https://[cluster-mgmt-LIF]`**

     只有HTTPS支援系統管理員的瀏覽器存取。

   如果叢集使用自我簽署的數位憑證、瀏覽器可能會顯示警告、指出該憑證不受信任。您可以確認繼續存取的風險、或是在叢集上安裝憑證授權單位（CA）簽署的數位憑證、以進行伺服器驗證。
2. *選用：*如果您使用CLI設定了存取橫幅、請閱讀*警告*對話方塊中顯示的訊息、然後選擇所需的選項繼續。

   啟用安全性聲明標記語言（SAML）驗證的系統不支援此選項。
   - 如果您不想繼續、請按一下*「取消」*、然後關閉瀏覽器。
   - 如果您要繼續、請按一下「確定」瀏覽至「系統管理員」登入頁面。
3. 使用叢集管理員認證登入System Manager。

從ONTAP 功能區9.11.1開始、當您登入System Manager時、可以指定地區設定。 地區設定會指定特定的本地化設定、例如語言、貨幣、時間和日期格式、以及類似的設定。若為ONTAP 版本號9.10.1或更早版本、則會從瀏覽器偵測到System Manager的區域設定。若要變更System Manager的地區設定、您必須變更瀏覽器的地區設定。

4. 選用：從ONTAP S廳9.12.1開始、您可以指定系統管理員的外觀偏好：
   a. 在 System Manager 右上角、按一下 以管理使用者選項。
   b. 將*系統主題*切換開關置於您偏好的位置：

切換位置	外觀設定
（左）	淡色主題（淡色背景加上暗色文字）
作業系統（中心）	預設為針對作業系統應用程式所設定的佈景主題喜好設定（通常是用於存取System Manager之瀏覽器的佈景主題設定）。
（右）	暗色主題（暗色背景加上亮色文字）

相關資訊

"管理Web服務存取"

"使用網頁瀏覽器存取節點的記錄檔、核心傾印檔和mib檔案"

在 ONTAP 叢集上設定通訊協定

視叢集上啟用的授權而定、您可以在叢集上啟用所需的傳輸協定。然後建立可存取儲存設備的網路介面。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"这些步骤"使用系統管理器設定 ONTAP 叢集。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

步驟

1. 選取 * 儀表板 * ，然後按一下 * 設定通訊協定 * 。
   - 要啓用 NAS 協議，請選擇 **NFS** 或 **SMB** 。
   - 要啓用 SAN 協議，請選擇 **iSCSI** 或 **FC** 。
   - 若要啟用 NVMe 通訊協定，請選取 * NVMe * 。

使用 ONTAP System Manager 新增許可證金鑰來啟用新功能

在早於 ONTAP 9.10.1 的版本中、 ONTAP 功能會啟用授權金鑰、而 ONTAP 9.10.1 及更新版本的功能則會啟用 NetApp 授權檔案。您可以使用系統管理員新增授權金鑰和 NetApp 授權檔案。

從ONTAP 《支援》9.10.1開始、您可以使用System Manager安裝NetApp授權檔案、一次啟用多項授權功能。使用NetApp授權檔案可簡化授權安裝、因為您不再需要新增個別的功能授權金鑰。您可從 NetApp 支援網站下載 NetApp 授權檔案。

如果您已經擁有某些功能的授權金鑰、而且您要升級至ONTAP 版本號的版本號為「版本號9.10.1」、您可以繼續使用這些授權金鑰。

步驟

1. 選擇*叢集>設定*。
2. 在 * Licenses* 下，選擇 →。
3. 選擇*瀏覽*。選擇您下載的 NetApp 授權檔案。
4. 如果您有想要新增的授權金鑰、請選取*使用28個字元的授權金鑰*、然後輸入金鑰。

使用 **ONTAP System Manager** 下載叢集配置

從 ONTAP 9 · 11.1 開始、您可以使用系統管理員下載叢集及其節點的一些組態詳細資料。此資訊可用於庫存管理、硬體更換和生命週期活動。此資訊對於不傳送 AutoSupport （ASUP ）資料的站台特別有用。

叢集組態詳細資料包括叢集名稱、叢集 ONTAP 版本、叢集管理 LIF 、 Volume 和 LIF 計數。

節點組態詳細資料包括節點名稱、系統序號、系統 ID 、系統機型、 ONTAP 版本、 MetroCluster 資訊、 SP / BMC 網路資訊、以及加密組態資訊。

步驟

1. 按一下*叢集>總覽*。
2. 按一下

以顯示下拉式功能表。
3. 選取 * 下載組態 * 。
4. 選取 HA 配對、然後按一下 * 下載 * 。

   組態會下載為 Excel 試算表。

   - 第一頁包含叢集詳細資料。
   - 其他工作表包含節點詳細資料。

使用 **ONTAP** 系統管理員為叢集指派標籤

從 ONTAP 9.14.1 開始、您可以使用系統管理員將標記指派給叢集、以識別屬於類別的物件、例如專案或成本中心。

關於這項工作

您可以將標記指派給叢集。首先、您需要定義並新增標記。 然後、您也可以編輯或刪除標記。

您可以在建立叢集時新增標記、也可以稍後新增標記。

您可以指定金鑰並使用「關鍵字：值」格式將值關聯至標籤、藉此定義標籤。 例如： "Dept:Engineering （部門

：工程） " 或 "`location ： San Jose （地點： San Jose ） " 。

建立標記時、應考慮下列事項：

- 金鑰的長度下限為 1 個字元、不可為 null 。 值可以是 null 。
- 可以使用多個值來配對金鑰、方法是以逗號分隔值、例如「 'location ： San Jose 、 Torontora' 」
- 標記可用於多個資源。
- 金鑰必須以小寫字母開頭。

步驟

若要管理標記、請執行下列步驟：

1. 在 System Manager 中、按一下 * 叢集 * 以檢視總覽頁面。

   標記列在 * 標記 * 區段中。

2. 按一下 * 管理標記 * 以修改現有標記或新增標記。

   您可以新增、編輯或刪除標記。

若要執行此動作...	執行下列步驟...
新增標記	a. 按一下 * 新增標記 * 。 b. 指定金鑰及其值（以逗號分隔多個值）。 c. 按一下「 * 儲存 * 」。
編輯標記	a. 修改 **Key** 和 *Values （可選） * 字段中的內容。 b. 按一下「 * 儲存 * 」。
刪除標記	a. 按一下 您要刪除的標記旁的。

使用 **ONTAP** 系統管理員檢視和提交支援案例

從ONTAP 9.9.1 開始，您可以從與叢集關聯的Active IQ Digital Advisor （也稱為Digital Advisor）查看支援案例。您還可以複製所需的叢集詳細信息，以便在NetApp支援網站上提交新的支援案例。從ONTAP 9.10.1 開始，您可以啟用遙測日誌記錄，這有助於支援人員排除故障。

若要接收韌體更新的相關警示、您必須向Active IQ Unified Manager NetApp註冊。請參閱 "支援的文件資源Active IQ Unified Manager"。

步驟

1. 在System Manager中、選取* Support*。

   隨即顯示與此叢集相關的開放式支援案例清單。

2. 按一下下列連結以執行程序：
   - 案例編號：請參閱案例詳細資料。
   - 前往 **NetApp** 支援網站：瀏覽至 NetApp 支援網站上的「**My AutoSupport**」頁面，即可查看知識庫文章或提交新的支援案例。
   - 查看我的案例：瀏覽至 NetApp 支援網站上的「**My Cases**（我的案例）」頁面。
   - 檢視叢集詳細資料：檢視並複製提交新案例時所需的資訊。

啟用遙測記錄

從ONTAP 《支援資料》9.10.1開始、您可以使用System Manager來啟用遙測記錄功能。 當允許遙測記錄時、系統管理員所記錄的訊息會指定特定的遙測識別碼、指出觸發訊息的確切程序。 與該程序相關的所有訊息都有相同的識別碼、其中包含作業工作流程名稱和編號（例如「add-volume -1941290」）。

如果遇到效能問題、您可以啟用遙測記錄、讓支援人員更容易識別發出訊息的特定程序。 將遙測識別碼新增至訊息時、記錄檔只會稍微放大。

步驟

1. 在System Manager中、選取*叢集>設定*。
2. 在「* UI設定*」區段中、按一下「允許遙測記錄*」核取方塊。

在 **ONTAP** 系統管理員中管理儲存虛擬機器的最大容量限制

從 ONTAP 9.13.1 開始、您可以使用系統管理員來啟用儲存 VM 的最大容量限制、並設定臨界值、在使用的儲存設備達到最大容量的特定百分比時觸發警示。

為儲存 **VM** 啟用最大容量限制

從 ONTAP 9.13.1 開始、您可以指定儲存 VM 中所有磁碟區可配置的最大容量。 您可以在新增儲存 VM 或編輯現有儲存 VM 時啟用最大容量。

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。
2. 執行下列其中一項：
   - 若要新增儲存 VM 、請按一下 + Add 。
   - 若要編輯儲存 VM 、請按一下 ⋮ 儲存 VM 名稱旁的、然後按一下 * 編輯 * 。
3. 輸入或修改儲存 VM 的設定、然後選取標有「啟用最大容量限制」的核取方塊。
4. 指定最大容量大小。
5. 指定您要用來做為觸發警示臨界值的最大容量百分比。
6. 按一下「 * 儲存 * 」 。

編輯儲存 **VM** 的最大容量限制

從 ONTAP 9.13.1 開始、您可以編輯現有儲存 VM 的最大容量限制（如果有） 已啟用最大容量限制 已有。

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。
2. 按一下 ⋮ 儲存 VM 名稱旁邊的，然後按一下 * 編輯 * 。

   已勾選標有「啟用最大容量限制」的核取方塊。

3. 請執行下列其中一個步驟：

行動	步驟
停用最大容量限制	1. 取消勾選核取方塊。 2. 按一下「 * 儲存 * 」 。
修改最大容量限制	1. 指定新的最大容量大小。（您無法指定小於儲存 VM 中已分配空間的大小。） 2. 指定要用作觸發警示臨界值的最大容量百分比。 3. 按一下「 * 儲存 * 」 。

相關資訊

- "檢視儲存 VM 的最大容量限制"
- "System Manager中的容量測量"
- "管理 SVM 容量限制"

在 ONTAP System Manager 中監控叢集，階層和 SVM 容量

使用 System Manager 、您可以監控已使用的儲存容量、以及叢集、本機層或儲存 VM 的可用容量。

每個 ONTAP 版本的系統管理員都能提供更強大的容量監控資訊：

- 從 ONTAP 9.13.1 開始、您可以為儲存 VM 啟用最大容量限制、並設定臨界值、以便在使用的儲存設備達到最大容量的特定百分比時觸發警示。
- 從 ONTAP 9.12.1 開始、系統管理員會顯示本機層的已認可容量。
- 從 ONTAP 9.10.1 開始，系統管理員可讓您檢視叢集容量的歷史資料，以及未來使用或可用容量的預測。您也可以監控本機層級和磁碟區的容量。

根據您的 ONTAP 版本、使用容量的測量顯示方式會有所不同。如需詳細"System Manager中的容量測量"資訊，請參閱。

檢視叢集的容量

您可以在System Manager的儀表板上檢視叢集的容量測量。

開始之前

若要檢視與雲端容量相關的資料、您必須擁有 Digital Advisor 帳戶並連線。

步驟

1. 在System Manager中、按一下*儀表板*。
2. 在「容量」區段中、您可以檢視下列項目：
   - 叢集的已用容量總計
   - 叢集的總可用容量
   - 已用容量和可用容量的百分比。
   - 資料減量比率。
   - 雲端使用的容量。
   - 容量使用記錄。
   - 容量使用量的預測

   在System Manager中、容量表示法並不代表root儲存層（Aggregate）容量。
3. 按一下圖表以檢視叢集容量的詳細資料。

   容量測量顯示在兩個橫條圖中：
   - 上方圖表會顯示實體容量：實體使用空間、保留空間和可用空間的大小。
   - 下圖顯示邏輯容量：用戶端資料，快照和複本的大小，以及總的邏輯使用空間。

   橫條圖下方是資料減量的測量：
   - 僅限用戶端資料的資料減量比率（不含快照和複本）。
   - 整體資料減量比率。

如需詳細資訊、請參閱 "System Manager中的容量測量"。

檢視本機層的容量

您可以查看本地層容量的詳細資訊。從ONTAP 9.12.1 開始，「容量」視圖還包含本地層的已提交容量，以便您確定是否需要向本地層添加容量以容納已提交的容量並避免可用空間耗盡。

步驟

1. 按一下*儲存設備> Tiers*。
2. 選取本機層的名稱。
3. 在「總覽」頁面的「容量」區段中、容量會顯示在橫條圖中、其中包含三個測量值：
   - 已用及保留容量
   - 可用容量
   - 承諾容量（從ONTAP 功能9.12.1開始）
4. 按一下圖表以檢視本機層級容量的詳細資料。

   容量測量顯示在兩個橫條圖中：

- 上方橫條圖顯示實體容量：實體已用空間、保留空間和可用空間的大小。
- 底部橫條圖會顯示邏輯容量：用戶端資料，快照和複本的大小，以及邏輯使用空間的總計。

橫條圖下方是資料減量的測量比率：

- 僅限用戶端資料的資料減量比率（不含快照和複本）。
- 整體資料減量比率。

如需詳細資訊、請參閱 "System Manager中的容量測量"。

選用動作

- 如果已提交的容量大於本機層的容量、您可以考慮在本機層用盡可用空間之前、先將容量新增至該層。 請參閱 "新增容量至本機層（新增磁碟至集合體）"。
- 您也可以選取 *Volumes * 標籤、來檢視特定磁碟區在本機層中使用的儲存設備。

檢視儲存 **VM** 中磁碟區的容量

您可以檢視儲存 VM 中的磁碟區所使用的儲存容量、以及可用的容量。已用與可用儲存設備的總測量值稱為「跨磁碟區的容量」。

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。
2. 按一下儲存 VM 的名稱。
3. 捲動至 * 容量 * 區段、其中顯示含有下列測量值的長條圖：
   - * 實體使用 * ：此儲存 VM 中所有磁碟區的實體使用儲存設備總和。
   - * 可用 * ：此儲存 VM 中所有磁碟區的可用容量總和。
   - * 已用邏輯 * ：此儲存 VM 中所有磁碟區的邏輯已用儲存設備總和。

如需測量的詳細資訊、請參閱 "System Manager中的容量測量"。

檢視儲存 **VM** 的最大容量限制

從 ONTAP 9.13.1 開始、您可以檢視儲存 VM 的最大容量限制。

開始之前

您必須 "啟用儲存 VM 的最大容量限制" 在您檢視之前。

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。

   您可以透過兩種方式檢視最大容量測量：

   - 在儲存 VM 的列中、檢視 * 最大容量 * 欄、其中包含一個長條圖、顯示已用容量、可用容量和最大容量。
   - 按一下儲存 VM 的名稱。在 * 總覽 * 索引標籤上、捲動以檢視左欄中的最大容量、分配容量和容量警示

臨界值。

相關資訊

- "編輯儲存 VM 的最大容量限制"
- "System Manager中的容量測量"

查看硬體配置以確定 ONTAP 系統管理員的問題

從 ONTAP 9.8 開始、您可以使用系統管理員來檢視網路上的硬體組態、並判斷硬體系統和纜線組態的健全狀況。

步驟

若要檢視硬體組態、請執行下列步驟：

1. 在System Manager中、選取*叢集>硬體*。
2. 將滑鼠游標停在元件上、即可檢視狀態和其他詳細資料。

   您可以檢視各種類型的資訊：

   - [有關控制器的資訊]
   - [磁碟櫃的相關資訊]
   - [儲存交換器的相關資訊]
3. 從《2019年9月12日》開始ONTAP 、您可以在System Manager中檢視纜線連接資訊。按一下「顯示纜線」核取方塊以檢視纜線、然後將游標暫留在纜線上以檢視其連線資訊。
   - [纜線相關資訊]

有關控制器的資訊

您可以檢視下列項目：

節點

- 您可以檢視前後視圖。
- 對於具有內部磁碟櫃的機型、您也可以在正面檢視中檢視磁碟配置。
- 您可以檢視下列平台：

平台	在 ONTAP 版本的系統管理員中支援 …										
	9.18.1	9.17.1	9.16.1.	9.15.1. .	9.14.1. .	9.13.1. 12.9.1 2.9.	9.12.1	9.11.1.	9.10.1	9.9.1	9.8 （僅限預覽模式）
AFF A20	是的	是的	是的								
AFF A30	是的	是的	是的								
AFF A50	是的	是的	是的								
AFF A70	是的	是的	是的	是的							
AFF A90	是的	是的	是的	是的							
AFF A1K	是的	是的	是的	是的							
解答150 AFF				是的	是的	是的					
VA220 AFF				是的	是的	是的	是的	是的	是的	是的	是的
VA250 AFF				是的	是的	是的	是的	是的	是的	是的	
部分A300 AFF				是的	是的	是的	是的	是的	是的	是的	是的
解答320 AFF				是的	是的	是的	是的	是的	是的	是的	

解答400 AFF				是的	是的	是的	是的	是的	是的	是的	是的
AFF A700				是的	是的	是的	是的	是的	是的	是的	是的
S4A700s AFF				是的	是的	是的	是的	是的	是的	是的	
解答800 AFF				是的	是的	是的	是的	是的	是的	是的	
解答900 AFF	是的	是的	是的	是的	是的	是的	是的	是的	是的		
AFF C30	是的	是的	是的								
AFF C60	是的	是的	是的								
AFF C80	是的	是的	是的								
C190 AFF				是的	是的	是的	是的	是的	是的	是的	是的
AFF C250				是的	是的	是的	是和#42 ；	是和#42 ；	是和#42 ；		
AFF C400				是的	是的	是的	是和#42 ；	是和#42 ；	是和#42 ；		
AFF C800	是的	是的	是的	是的	是的	是的	是和#42 ；	是和#42 ；	是和#42 ；		
ASA A150				是的	是的	是的					
ASA A250				是的	是的	是的					

ASA A400				是的	是的	是的					
ASA A800				是的	是的	是的					
ASA A900				是的	是的	是的					
ASA C250	是的	是的	是的	是的	是的	是的					
ASA C400	是的	是的	是的	是的	是的	是的					
ASA C800	是的	是的	是的	是的	是的	是的					
AFX 1X	是的	是的									
FAS50	是的	是的	是的								
FAS70	是的	是的	是的	是的							
FAS90	是的	是的	是的	是的							
FAS500f				是的	是的	是的	是的	是的	是的	是的	
FAS2720				是的	是的	是的	是的	是的			
FAS2750	是的	是的	是的	是的	是的	是的	是的	是的	是的	是的	是的
FAS8300				是的	是的	是的	是的	是的			
FAS8700				是的	是的	是的	是的	是的			
FAS9000					是的	是的	是的	是的	是的		

FAS9500					是的	是的	是的	是的	是的		

連接埠

- 如果連接埠關閉、您會看到紅色反白顯示的連接埠。
- 當您將游標移到連接埠上時、可以檢視連接埠的狀態和其他詳細資料。
- 您無法檢視主控台連接埠。

  附註：

  - 從 ONTAP 9.11.1 開始、只有當 SAS 連接埠處於錯誤狀態或使用的有線連接埠離線時、才會以紅色強調顯示。 如果連接埠離線且未停用、則會以白色顯示。
  - 對於 ONTAP 9.10.1 及更早版本、停用 SAS 連接埠時、會以紅色反白顯示。

FRU

只有在FRU狀態不是最佳狀態時、才會顯示FRU相關資訊。

- 節點或機箱中的PSU故障。
- 節點偵測到高溫度。
- 節點或機箱上的風扇故障。

介面卡

- 如果已插入外部卡片、插槽中會顯示已定義零件編號欄位的卡片。
- 連接埠會顯示在插卡上。
- 對於支援的卡片、您可以檢視該卡片的影像。 如果卡片不在支援的零件編號清單中、則會出現一般圖形。

磁碟櫃的相關資訊

您可以檢視下列項目：

磁碟櫃

- 您可以顯示前後視圖。
- 您可以檢視下列磁碟櫃機型：

如果您的系統正在執行…	然後您可以使用System Manager來檢視…
更新版本ONTAP	所有未被指定為「服務終止」或「終止供應」的機櫃
部分9.8 ONTAP	DS4243、DS4486、DS212C、DS2246、DS224C、 和NS224

機櫃連接埠

- 您可以檢視連接埠狀態。
- 如果連接埠已連線、您可以檢視遠端連接埠資訊。

機櫃**FRU**

- 顯示 PSU 故障資訊。

儲存交換器的相關資訊

您可以檢視下列項目：

儲存交換器

- 顯示幕會顯示做為儲存交換器的交換器、用來將磁碟櫃連接至節點。
- 從功能表9.9開始ONTAP 、System Manager會顯示交換器的相關資訊、該交換器可做為儲存交換器和叢集、也可在HA配對的節點之間共用。
- 將顯示下列資訊：
  - 交換器名稱
  - IP 位址
  - 序號
  - SNMP 版本
  - 系統版本
- 您可以檢視下列儲存交換器機型：

如果您的系統正在執行…	然後您可以使用System Manager來檢視…
更新版本ONTAP	Cisco Nexus 3232C Cisco Nexus 9336C-FX2 NVIDIA SN2100
ONTAP 9.10.1 和 9.9.1	Cisco Nexus 3232C Cisco Nexus 9336C-FX2
部分9.8 ONTAP	Cisco Nexus 3232C

儲存交換器連接埠

- 將顯示下列資訊：
  - 身分識別名稱
  - 身分識別索引
  - 州/省
  - 遠端連線
  - 其他詳細資料

纜線相關資訊

從《產品介紹指南（英語）：9.12.12開始ONTAP 、您可以檢視下列纜線資訊：

- * 在沒有使用儲存橋接器的情況下、控制器、交換器和機櫃之間的佈線 *
- **Connectivity** ，顯示纜線兩端連接埠的 ID 和 MAC 位址

使用 **ONTAP** 系統管理員管理節點

使用 System Manager 、您可以將節點新增至叢集並重新命名。 您也可以重新開機、接管及回饋節點。

新增節點至叢集

您可以新增節點來增加叢集的大小和功能。

開始之前

您應該已經將新節點連接至叢集。

關於這項工作

在ONTAP 9.8 及更高版本或ONTAP 9.7 中使用系統管理員有單獨的流程。

ONTAP 9.8 及更新版本程序

- 使用系統管理程式（ ONTAP 9.8 及更新版本） * 將節點新增至叢集 *

步驟

1. 選擇*叢集>總覽*。

   新控制器顯示為連接至叢集網路但不在叢集內的節點。

2. 選取*「Add*」。
   - 節點會新增至叢集。
   - 儲存設備會以隱含方式配置。

ONTAP 9.7 程序

- 使用系統管理程式將節點新增至叢集（ ONTAP 9.7 ） *

步驟

1. 選擇 *（返回經典版本） * 。
2. 選擇 * 組態 > 叢集擴充 * 。

   System Manager會自動探索新節點。

3. 選擇 * 切換至新體驗 * 。
4. 選取 * 叢集 > 總覽 * 以檢視新節點。

關閉、重新開機或編輯服務處理器

當您重新開機或關機節點時、其 HA 合作夥伴會自動執行接管。

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"關閉並重啟節點。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

步驟

1. 選擇*叢集>總覽*。
2. 在 * 節點 * 下，選擇 ⋮ 。

3. 選取節點、然後選取 * 關機 * 、 * 重新開機 * 或 * 編輯服務處理器 * 。

   如果節點已重新開機並正在等待恢復、也可以使用 **GiveBack** 選項。

   如果您選取 * 編輯服務處理器 * 、您可以選擇 * 手動 * 來輸入 IP 位址、子網路遮罩和閘道、或是選擇 * DHCP 來進行動態主機組態。

重新命名節點

從 ONTAP 9.14.1 開始、您可以從叢集概觀頁面重新命名節點。

> 此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"重命名節點。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

步驟

1. 選擇 * 叢集 * 。 隨即顯示叢集概觀頁面。
2. 向下捲動至 * 節點 * 區段。
3. 在您要重新命名的節點旁邊，選取 ⋮ ，然後選取 * 重新命名 * 。
4. 修改節點名稱、然後選取 * 重新命名 * 。

授權管理

ONTAP 授權總覽

授權是一或多個軟體授權的記錄。從 ONTAP 9.10.1 開始、所有授權都會以 NetApp 授權檔案（ NLF ）的形式交付、這是一個可啟用多項功能的單一檔案。 自 2023 年 5 月起、所有 AFF 系統（ A 系列和 C 系列）和 FAS 系統均隨附 ONTAP One 軟體套件或 ONTAP Base 軟體套件、自 2023 年 6 月起、所有 ASA 系統均隨 ONTAP One for SAN 銷售。每個軟體套件均以單一 NLF 形式提供、取代 ONTAP 9.10.1 中首次推出的獨立 NLF 套件。

ONTAP One 隨附授權

ONTAP One 包含所有可用的授權功能。其中包含前一代核心套件、資料保護套裝組合、安全性與法規遵循套件、混合雲套裝組合和加密套件的內容組合、如表所示。加密功能不適用於受限制的國家 / 地區。

以前的套件名稱	隨附 ONTAP 金鑰
核心套裝組合	FlexClone
	SnapRestore
	NFS 、 SMB 、 S3
	FC 、 iSCSI
	NVMe

安全性與法規遵循套裝組合	自主勒索軟體保護
	MKM
	SnapLock
資料保護套裝組合	SnapMirror （非同步，同步，主動同步）
	SnapCenter
	適用於 NetApp 目標的 SnapMirror S3
混合雲套裝組合	SnapMirror 雲端
	適用於非 NetApp 目標的 SnapMirror S3
加密套件	NetApp Volume Encryption
	信任平台模組

ONTAP One 不含授權

ONTAP One 不包含任何 NetApp 的雲端服務、包括：

- NetApp雲端分層
- 資料基礎架構洞見
- NetApp備份與復原
- 資料治理

適用於現有系統的 **ONTAP One**

如果您現有的系統目前支援 NetApp 、但尚未升級至 ONTAP One 、則這些系統上的現有授權仍有效、並繼續如預期運作。例如，如果 SnapMirror 許可證已經安裝在現有系統上，則無需升級到 ONTAP One 即可獲得新的 SnapMirror 許可證。但是，如果現有系統上沒有安裝 SnapMirror 許可證，則獲得該許可證的唯一方法是以額外的費用升級到 ONTAP One 。

自 2023 年 6 月起、使用 28 個字元授權金鑰的 ONTAP 系統也可以使用 "升級至 ONTAP One 或 ONTAP Base 相容性套件"。

ONTAP Base 隨附授權

ONTAP Base 是選用的軟體套件、是 ONTAP One for ONTAP 系統的替代方案。這適用於不需要 SnapMirror 和 SnapCenter 等資料保護技術、以及不需使用自治勒索軟體等安全功能的特定使用案例、例如專用測試或開發環境的非正式作業系統。無法將其他授權新增至 ONTAP Base 。如果您需要額外的授權、例如 SnapMirror 、則必須升級至 ONTAP One 。

以前的套件名稱	隨附 ONTAP 金鑰

核心套裝組合	FlexClone
	SnapRestore
	NFS 、 SMB 、 S3
	FC 、 iSCSI
	NVMe
加密套件	NetApp Volume Encryption
	信任平台模組

ONTAP One for SAN 隨附授權

ONTAP One for SAN 適用於 ASA A 系列和 C 系列系統。這是唯一適用於 SAN 的軟體套件。ONTAP One for SAN 包含下列授權：

隨附 ONTAP 金鑰
FlexClone
SnapRestore
FC 、 iSCSI
NVMe
MKM
SnapLock
SnapMirror （非同步，同步，主動同步）
SnapCenter
SnapMirror 雲端
NetApp Volume Encryption
信任平台模組

其他授權交付方法

在從功能更新到功能更新到版本9.9.1的過程中、授權金鑰會以28個字元的字串形式提供、每個功能有一個金鑰。ONTAP ONTAP ONTAP如果您使用的是 ONTAP 8.2 至 ONTAP 9.9.1 、則可使用 ONTAP CLI 來安裝授權金鑰。

ONTAP 9.10.1 支援使用系統管理員或 CLI 安裝 28 個字元的授權金鑰。不過、如果針對某項功能安裝了 NLF 授權、您就無法在 NetApp 授權檔案上安裝 28 個字元的授權金鑰、以取得相同的功能。有關使用 System Manager 安裝 NLF 或授權金鑰的資訊、請參閱"安裝 ONTAP 授權"。

相關資訊

"當系統已有 NLF 時、如何取得 ONTAP One 授權"

"如何使用支援網站來驗證 ONTAP 軟體授權與相關授權金鑰"

"NetApp ： ONTAP 權利金風險狀態"

從 **NetApp** 支援網站 下載 **NetApp** 授權檔案（ **NLF** ）

如果您的系統執行的是 ONTAP 9.10.1 或更新版本、您可以從 NetApp 支援網站 下載適用於 ONTAP One 或 ONTAP Core 的 NLF 、以升級現有系統上的套件授權檔案。

ONTAP One 不含 SnapMirror 雲端和 SnapMirror S3 授權。它們是 ONTAP One 相容性套件的一部分、如果您有 ONTAP One 和"請另行申請"、可以免費取得。

步驟

您可以為具有現有 NetApp 授權檔案套件的系統、以及在執行 ONTAP 9.10.1 及更新版本的系統上、將具有 28 個字元授權金鑰的系統下載 ONTAP One 授權檔案、以轉換成 NetApp 授權檔案。您也可以付費將系統從 ONTAP Base 升級至 ONTAP One 。

升級現有的 **NLF**

1. 請聯絡您的 NetApp 銷售團隊、並索取您要升級或轉換的授權檔案套件（例如、 ONTAP Base 至 ONTAP One 、或核心套件與資料保護套件至 ONTAP One ）。

   處理您的申請時，您會收到 netappsw@netapp.com 的電子郵件，主旨為「 NetApp 軟體授權通知（適用於 sso 號碼）」，電子郵件中會附上 PDF 附件，其中包含您的授權序號。

2. 登入 "NetApp 支援網站"。
3. 選擇 * 系統 > 軟體授權 * 。
4. 從功能表中選擇 * 序號 * 、輸入您收到的序號、然後按一下 * 新搜尋 * 。
5. 找出您要轉換的授權套件。
6. 單擊 * 獲取每個許可證套件的 NetApp 許可證文件 * ，並在可用時下載 NLF 。
7. "安裝"ONTAP One 檔案。

升級從授權金鑰轉換的 **NLF**

1. 登入 "NetApp 支援網站"。
2. 選擇 * 系統 > 軟體授權 * 。
3. 從功能表中選擇 * 序號 * 、輸入系統序號、然後按一下 * 新搜尋 * 。
4. 找到要轉換的授權、然後在 * 資格 * 欄中按一下 * 檢查 * 。
5. 在 * 檢查資格表單 * 中、按一下 * 產生 9.10. x 及更新版本的授權 * 。
6. 關閉 * 檢查資格表單 * 。

   您需要等待至少 2 小時、才能產生授權。

7. 重複步驟 1 至 3 。
8. 找到 ONTAP One 授權、按一下 * 取得 NetApp 授權檔案 * 、然後選擇交付方法。
9. "安裝"ONTAP One 檔案。

在 **ONTAP** 中安裝 **NetApp** 授權

您可以使用系統管理員（這是安裝 NLF 的首選方法）來安裝 NetApp 授權檔案（ NLF ）和授權金鑰、或使用 ONTAP CLI 來安裝授權金鑰。在 ONTAP 9.10.1 及更新版本中、功能是以 NetApp 授權檔案啟用、而在 ONTAP 9.10.1 之前的版本中、 ONTAP 功能則是以授權金鑰啟用。

步驟

如果您已經擁有"已下載 NetApp 授權檔案"或授權金鑰、可以使用系統管理員或 ONTAP CLI 來安裝 NLF 和 28 個字元的授權金鑰。

System Manager - ONTAP 9.8 及更新版本

1. 選擇*叢集>設定*。
2. 在 * Licenses* 下，選擇 → 。
3. 選擇*瀏覽*。選擇您下載的 NetApp 授權檔案。
4. 如果您有想要新增的授權金鑰、請選取*使用28個字元的授權金鑰*、然後輸入金鑰。

System Manager - ONTAP 9.7 及更早版本

1. 選取 * 組態 > 叢集 > 授權 * 。
2. 在 * Licenses* 下，選擇 → 。
3. 在「套件」視窗中、按一下「新增」。
4. 在「新增授權套件」對話方塊中、按一下「選擇檔案」以選取您下載的NetApp授權檔案、然後按一下「新增」將檔案上傳至叢集。

CLI

1. 新增一或多個授權金鑰：

```
system license add
```

下列範例會從本機節點「 /mroot/etc/lic_file 」安裝授權（如果檔案存在於此位置）：

```
cluster1::> system license add -use-license-file true
```

下列範例將包含 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA 和 BBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBBB 金鑰的授權清單新增至叢集：

```
cluster1::> system license add -license-code
AAAAAAAAAAAAAAAAAAAAAAAAAAAA, BBBBBBBBBBBBBBBBBBBBBBBBBBB
```

深入瞭解 ONTAP 命令參照中的連結： https://docs 。 NetApp 。 ONTAP - CLI/system-license-add.html[`system license add`^] 命令。

管理**ONTAP** 不需購買的授權

您可以使用系統管理員或 ONTAP CLI 來檢視及管理系統上安裝的授權、包括檢視授權序號、檢查授權狀態、以及移除授權。

檢視授權的詳細資料

步驟

如何檢視授權的詳細資料、取決於您使用的 ONTAP 版本、以及您是使用系統管理員還是使用 ONTAP CLI 。

System Manager - ONTAP 9.8 及更新版本

1. 若要檢視特定功能授權的詳細資料、請選取 * 叢集 > 設定 * 。
2. 在 * Licenses* 下，選擇 → 。
3. 選擇 * 功能 * 。
4. 找到您要檢視的授權功能、然後選取 ⌄ 以檢視授權詳細資料。

System Manager - ONTAP 9.7 及更早版本

1. 選取 * 組態 > 叢集 > 授權 * 。
2. 在*授權*視窗中、執行適當的動作：
3. 按一下*詳細資料*索引標籤。

CLI

1. 顯示已安裝授權的詳細資料：

```
system license show
```

刪除授權

System Manager - ONTAP 9.8 及更新版本

1. 若要刪除授權、請選取 * 叢集 > 設定 * 。
2. 在 * Licenses* 下，選擇 → 。
3. 選擇 * 功能 * 。
4. 選取您要刪除的授權功能、然後 * 刪除舊金鑰 * 。

System Manager - ONTAP 9.7 及更早版本

1. 選取 * 組態 > 叢集 > 授權 * 。
2. 在*授權*視窗中、執行適當的動作：

如果您想要...	執行此動作...
刪除節點或主要授權上的特定授權套件	按一下*詳細資料*索引標籤。
刪除叢集中所有節點的特定授權套件	按一下「套件」索引標籤。

3. 選取您要刪除的軟體授權套件、然後按一下*刪除*。

   一次只能刪除一個授權套件。

4. 選取確認核取方塊、然後按一下*刪除*。

CLI

1. 刪除授權：

```
system license delete
```

   下列範例從叢集刪除名為CIFS的授權、序號為1-81-81-00000000000000000000000000000000123456：

```
cluster1::> system license delete -serial-number 1-81-
00000000000000000000123456 -package CIFS
```

   下列範例會從叢集刪除已安裝授權核心產品組合下的所有授權、序號為123456789：

```
cluster1::> system license delete { -serial-number 123456789
-installed-license "Core Bundle" }
```

相關資訊

"用於管理授權的 ONTAP CLI 命令"

"指令參考資料ONTAP"

授權類型與授權方法

瞭解授權類型和授權方法、有助於管理叢集中的授權。

授權類型

一個套件可以在叢集中安裝下列一或多個授權類型。。 `system license show` 命令會顯示套件的已安裝授權類型。

- 標準授權 (`license`)

  標準授權是節點鎖定的授權。它是針對具有特定系統序號（也稱為_Controller序號_）的節點發出的。標準授權僅適用於序號相符的節點。

  安裝標準的節點鎖定授權可讓節點享有授權功能。若要讓叢集使用授權功能、至少必須授權一個節點才能使用此功能。在沒有功能應有權利的節點上使用授權功能可能會違反法規。

- 站台授權 (`site`)

  站台授權不會繫結至特定的系統序號。當您安裝站台授權時、叢集中的所有節點都有權使用授權功能。。 `system license show` 命令會以叢集序號顯示站台授權。

  如果您的叢集擁有站台授權、而您從叢集移除節點、則節點不會隨附站台授權、也不再有權使用授權功能。如果您將節點新增至具有站台授權的叢集、則節點會自動獲得站台授權所授予的功能。

- 評估授權 (`demo`)

  評估版授權是一種在一段時間後過期的暫用授權（如所示） `system license show` 命令）。它可讓您在不購買授權的情況下、嘗試特定的軟體功能。這是全叢集的授權、並未繫結至節點的特定序號。

  如果叢集具有套件的評估授權、而您從叢集移除節點、則節點不會隨附評估授權。

授權方法

您可以同時安裝叢集範圍的授權（ `site` 或 `demo` 類型）和節點鎖定的授權（ `license` 類型）。因此、安裝的套件在叢集中可以有多種授權類型。但是、對於叢集而言、套件只有一個_licensed方法。。 `licensed method` 的欄位 `system license status show` 命令會顯示套件使用的權利。此命令會決定授權方法、如下所示：

- 如果套件在叢集中只安裝一種授權類型、則安裝的授權類型為授權方法。
- 如果套件在叢集中未安裝任何授權、則授權方法為 `none`。
- 如果某個套件在叢集中安裝了多種授權類型、則授權方法會依照授權類型的下列優先順序來決定 `--site`、`license`和 `demo`。

  例如：

  - 如果您擁有站台授權、標準授權和套件評估授權、叢集中套件的授權方法就是 `site`。

- 如果您擁有套件的標準授權和評估授權、叢集中套件的授權方法就是 `license`。
- 如果您只有套件的試用版授權、叢集中套件的授權方法就是 `demo`。

用於管理 ONTAP 中授權的命令

您可以使用 ONTAP CLI `system license` 用於管理叢集功能授權的命令。您可以使用 `system feature-usage` 監控功能使用的命令。

如需本主題中所述命令的詳細"指令參考資料ONTAP"資訊，請參閱。

下表列出了一些用於管理許可證的常用 CLI 命令，以及指向命令手冊頁的鏈接，以瞭解更多信息。

如果您想要...	使用此命令...
顯示所有需要授權的套件及其目前授權狀態、包括： • 套件名稱 • 授權方法 • 到期日（如果適用）	"系統授權顯示狀態"
顯示或移除過期或未使用的授權	"系統授權清除"
以每個節點為基礎、顯示叢集中的功能使用量摘要	"系統功能使用量顯示摘要"
以每節點和每週為單位顯示叢集中的功能使用狀態	"系統功能使用量顯示歷程記錄"
顯示每個授權套件的授權權利風險狀態	"系統授權權利風險顯示"

相關資訊

- "指令參考資料ONTAP"
- "NetApp知識庫： ONTAP 9.10.1 及更高版本的授權概述"
- "使用系統管理員安裝 NetApp 授權檔案"
- "系統功能"

使用CLI進行叢集管理

使用 ONTAP CLI 瞭解叢集管理

您可以ONTAP 使用命令列介面（CLI）來管理不一致的系統。您可以使用ONTAP 原地管理介面、存取叢集、管理節點等等。

您應在下列情況下使用這些程序：

- 您想要瞭解ONTAP 一系列的管理員功能。
- 您想要使用CLI、而非System Manager或自動化指令碼工具。

相關資訊

如需 CLI 語法和使用方式的詳細資訊、請參閱 "指令參考資料ONTAP" 文件。

叢集與SVM管理員

瞭解 ONTAP 叢集和 SVM 管理員角色

叢集管理員負責管理整個叢集及其所包含的儲存虛擬機器（SVM、先前稱為Vserver）。SVM管理員只能管理自己的資料SVM。

叢集管理員可以管理整個叢集及其資源。他們也可以設定資料SVM、並將SVM管理委派給SVM管理員。叢集管理員的特定功能取決於其存取控制角色。根據預設、具有「admin」帳戶名稱或角色名稱的叢集管理員、具有管理叢集和SVM的所有功能。

SVM系統管理員只能管理自己的SVM儲存設備和網路資源、例如磁碟區、傳輸協定、LIF和服務。SVM系統管理員的特定功能取決於叢集管理員指派的存取控制角色。

ONTAP 命令列介面（ CLI ）會繼續在輸出和中使用字詞 *vserver* `vserver` 因為命令或參數名稱並未變更。

啟用或停用 ONTAP 系統管理員的網頁瀏覽器存取

您可以啟用或停用網頁瀏覽器對System Manager的存取。您也可以檢視System Manager記錄。

您可以使用 [`true|false`] 來控制網路瀏覽器對 System Manager 的存取 `vserver services web modify -name sysmgr -vserver <cluster_name> -enabled`。

系統管理員記錄會記錄在中 `/mroot/etc/log/mlog/sysmgr.log` 存取 System Manager 時、主控叢集管理 LIF 的節點檔案。您可以使用瀏覽器來檢視記錄檔。系統管理程式記錄也包含在AutoSupport 資訊內容中。

瞭解 ONTAP 叢集管理伺服器

叢集管理伺服器也稱為_admin_SVM、是一種特殊的儲存虛擬機器（SVM）實作、可將叢集視為單一可管理實體。叢集管理伺服器除了充當最高層級的管理網域之外、還擁有邏輯上不屬於資料SVM的資源。

叢集管理伺服器永遠可在叢集上使用。您可以透過主控台或叢集管理LIF來存取叢集管理伺服器。

當主網路連接埠故障時、叢集管理LIF會自動容錯移轉至叢集中的另一個節點。視您使用的管理傳輸協定的連線特性而定、您可能會注意到或不會注意到容錯移轉。如果您使用的是無連線傳輸協定（例如SNMP）或連線有限（例如HTTP）、則不太可能注意到容錯移轉。不過、如果您使用長期連線（例如SSH）、則在容錯移轉之後、您必須重新連線至叢集管理伺服器。

建立叢集時、會設定叢集管理LIF的所有特性、包括其IP位址、網路遮罩、閘道和連接埠。

與資料SVM或節點SVM不同、叢集管理伺服器沒有根Volume或主機使用者磁碟區（雖然它可以裝載系統磁碟區）。此外、叢集管理伺服器只能擁有叢集管理類型的生命。

如果您執行 `vserver show` 命令時、叢集管理伺服器會出現在該命令的輸出清單中。

ONTAP 叢集中的 **SVM** 類型

叢集由四種類型的SVM組成、有助於管理叢集及其資源、以及對用戶端和應用程式的資料存取。

叢集包含下列類型的SVM：

- 管理SVM

  叢集設定程序會自動建立叢集的管理SVM。管理SVM代表叢集。

- 節點 SVM

  節點加入叢集時會建立節點SVM、節點SVM則代表叢集的個別節點。

- 系統SVM（進階）

  系統SVM會自動建立、以便在IPspace中進行叢集層級的通訊。

- Data SVM

  資料SVM代表為SVM服務的資料。叢集設定完成後、叢集管理員必須建立資料SVM並將磁碟區新增至這些SVM、以利從叢集存取資料。

  叢集必須至少有一個資料SVM、才能將資料提供給其用戶端。

> 除非另有說明、否則SVM一詞是指資料（資料服務）SVM。
>
> 在CLI中、SVM會顯示為Vserver。

使用**CLI**存取叢集（僅限叢集管理員）

使用節點序列連接埠存取 **ONTAP** 叢集

您可以直接從連接至節點序列連接埠的主控台存取叢集。

步驟

1. 在主控台按Enter。

   系統會以登入提示回應。

2. 在登入提示下、執行下列其中一項：

若要存取叢集：	輸入下列帳戶名稱...
預設叢集帳戶	**admin**
另一個管理使用者帳戶	*username*

系統會以密碼提示回應。

3. 輸入admin或管理使用者帳戶的密碼、然後按Enter。

使用 **SSH** 要求存取 **ONTAP** 叢集

您可以向 ONTAP 叢集發出 SSH 要求、以執行管理工作。SSH 預設為啟用。

開始之前

- 您必須擁有設定為使用的使用者帳戶 `ssh` 作為存取方法。

  `-application`命令參數 `security login`
  會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/security-login-create.html#description["指令參考資料ONTAP"^]需詳細`security login`資訊，請參閱。

- 如果您使用 Active Directory （ AD ）網域使用者帳戶來存取叢集、則必須透過啟用 CIFS 的儲存 VM 來設定叢集的驗證通道、而且您的 AD 網域使用者帳戶也必須新增至具有的叢集 `ssh` 作為存取方法和 `domain` 作為驗證方法。

關於這項工作

- 您必須使用OpenSSH 5.7或更新版本的用戶端。
- 僅支援SSH v2傳輸協定；不支援SSH v1。
- 支援每個節點最多64個並行SSH工作階段。ONTAP

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- 支援SSH的AES和3DES加密演算法（也稱為_ciphers_）ONTAP 。

  AES支援128、192和256位元金鑰長度。3DES的金鑰長度為56位元、與原始的DES相同、但會重複三次。

- 當FIPS模式開啟時、SSH用戶端應與省略曲線數位簽章演算法（ECDSA）公開金鑰演算法協商、以使連線成功。
- 如果您想ONTAP 要從Windows主機存取此功能、可以使用第三方公用程式、例如Putty。
- 如果您使用Windows AD使用者名稱登入ONTAP 到功能表、則應該使用在ONTAP 功能表中建立AD使用者名稱和網域名稱時所用的大小寫字母。

  AD使用者名稱和網域名稱不區分大小寫。不過ONTAP 、不區分使用者名稱大小寫。使用者名稱ONTAP 若

不相符、而使用者名稱與在AD中建立的使用者名稱不相符、將導致登入失敗。

SSH 驗證選項

- 從 ONTAP 9.3 開始、您可以 "啟用 SSH 多因素驗證" 適用於本機系統管理員帳戶。

  啟用SSH多因素驗證時、使用者會使用公開金鑰和密碼進行驗證。

- 從 ONTAP 9.4 開始、您可以 "啟用 SSH 多因素驗證" 適用於 LDAP 和 NIS 遠端使用者。
- 從 ONTAP 9.13.1 開始、您可以選擇性地將憑證驗證新增至 SSH 驗證程序、以增強登入安全性。若要這麼做、 "將 X.509 憑證與公開金鑰建立關聯" 帳戶使用的。如果您同時使用 SSH 公開金鑰和 X.509 憑證登入、ONTAP 會先檢查 X.509 憑證的有效性、然後再使用 SSH 公開金鑰進行驗證。如果該憑證已過期或撤銷、SSH 公開金鑰會自動停用、則 SSH 登入會遭到拒絕。
- 從 ONTAP 9.14.1 開始、 ONTAP 系統管理員就可以 "將 Cisco 雙核心雙因素驗證新增至 SSH 驗證程序" 以增強登入安全性。啟用 Cisco 雙核心驗證之後、首次登入時、使用者必須註冊裝置、以作為 SSH 工作階段的驗證者。
- 從 ONTAP 9.15.1 開始、系統管理員就可以 "設定動態授權" 根據使用者的信任分數、為 SSH 使用者提供額外的自適應驗證。

步驟

1. 從可存取 ONTAP 叢集網路的主機、輸入 `ssh` 命令的格式如下：

   - **`ssh username@hostname_or_IP [command]`**
   - **`ssh -l username hostname_or_IP [command]`**

如果您使用的是 AD 網域使用者帳戶、則必須指定 *username* 的格式 *domainname\\AD_accountname* （在網域名稱後面加上雙反斜線）或 "*domainname\AD_accountname*" （以雙引號括住、並在網域名稱之後加上單一反斜線）。

hostname_or_IP 是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

command 不需要 SSH 互動式工作階段。

SSH要求範例

下列範例顯示名為「'joe'」的使用者帳戶如何發出SSH要求、以存取叢集管理LIF為10.72.137.28的叢集：

```
$ ssh joe@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l joe 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

下列範例顯示、名為「DOMAIN1」之網域中的「'John」使用者帳戶如何發出SSH要求、以存取叢集管理LIF為10.72.137.28的叢集：

```
$ ssh DOMAIN1\\john@10.72.137.28
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

```
$ ssh -l "DOMAIN1\john" 10.72.137.28 cluster show
Password:
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

下列範例顯示名為「'joe'」的使用者帳戶如何發出SSH MFA要求、以存取叢集管理LIF為10.72.137.32的叢集：

```
$ ssh joe@10.72.137.32
Authenticated with partial success.
Password:
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.
```

相關資訊

"系統管理員驗證與RBAC"

ONTAP SSH 登入安全性

從功能表9.5開始ONTAP 、您可以檢視上次成功登入後、先前登入、登入失敗、以及權限變更等資訊。

當您以SSH管理員使用者身分成功登入時、會顯示安全性相關資訊。您會收到下列情況的警示：

- 您的帳戶名稱上次登入的時間。
- 自上次成功登入以來、嘗試登入失敗的次數。
- 角色自上次登入後是否有所變更（例如、如果管理員帳戶的角色從「admin」變更為「備份」）。
- 自上次登入後、是否已修改角色的新增、修改或刪除功能。

如果顯示的任何資訊可疑、請立即聯絡您的安全部門。

若要在登入時取得此資訊、必須符合下列先決條件：

- 您的SSH使用者帳戶必須以ONTAP 功能不均的形式配置。
- 您必須建立SSH安全登入。
- 您的登入嘗試必須成功。

SSH登入安全性的限制和其他考量

下列限制與考量事項適用於SSH登入安全資訊：

- 此資訊僅適用於SSH型登入。
- 對於群組型管理帳戶（例如LDAP/NIS和AD帳戶）、如果使用者所屬的群組被配置為ONTAP 位於Sof the SView的管理帳戶、則使用者可以檢視SSH登入資訊。

  不過、這些使用者無法顯示使用者帳戶角色變更的警示。此外、屬於AD群組的使用者ONTAP 若已在無法檢視上次登入後發生的不成功登入嘗試次數、則會被配置為在無法執行的系統管理帳戶。

- 當使用者帳戶從ONTAP 下列項目刪除時、系統會刪除為使用者維護的資訊：
- 除了SSH之外、不會顯示連線至應用程式的資訊。

SSH登入安全資訊範例

下列範例示範登入後顯示的資訊類型。

- 此訊息會在每次成功登入後顯示：

```
Last Login : 7/19/2018 06:11:32
```

- 如果自上次成功登入後嘗試登入失敗、則會顯示下列訊息：

```
Last Login : 4/12/2018 08:21:26
Unsuccessful login attempts since last login - 5
```

- 如果嘗試登入失敗、且自上次成功登入後您的權限已修改、則會顯示下列訊息：

```
Last Login : 8/22/2018 20:08:21
Unsuccessful login attempts since last login - 3
Your privileges have changed since last login
```

啟用 **ONTAP** 叢集的 **Telnet** 或 **RSH** 存取

最佳安全性做法是預設停用 Telnet 和 RSH 。若要讓叢集能夠接受 Telnet 或 RSH 要求、您必須在預設管理服務原則中啟用該服務。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

關於這項工作

- ONTAP 每個節點最多可支援 50 個並行 Telnet 或 RSH 工作階段。

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 RSH 或 Telnet 安全性通訊協定：

   ```
   security protocol show
   ```

   a. 如果啟用了 RSH 或 Telnet 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 RSH 或 Telnet 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application <rsh/telnet> -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify` "指令參考資料ONTAP"。

2. 確認 `management-rsh-server` 或 `management-telnet-server` 服務存在於管理階層中：

   ```
   network interface show -services management-rsh-server
   ```

   或

   ```
   network interface show -services management-telnet-server
   ```

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

   a. 如果 `management-rsh-server` 或 `management-telnet-server` 服務存在、請繼續下一步。

   b. 如果 `management-rsh-server` 或 `management-telnet-server` 服務不存在、請使用下列命令加以新增：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server

      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

關於這項工作

ONTAP 可防止您變更預先定義的防火 `mgmt`牆原則、但您可以複製預先定義的管理防火牆原則、然後在新原則下啟用 Telnet 或 RSH 來建立新原則。

步驟

1. 進入進階權限模式：

   ```
   set advanced
   ```

2. 啟用安全性傳輸協定（ RSH 或 Telnet ）：

```
security protocol modify -application security_protocol -enabled true
```

3. 根據 `mgmt`管理防火牆原則建立新的管理防火牆原則：

   ```
   system services firewall policy clone -policy mgmt -destination-policy
   policy-name
   ```

4. 在新的管理防火牆原則中啟用 Telnet 或 RSH ：

   ```
   system services firewall policy create -policy policy-name -service
   security_protocol -action allow -ip-list ip_address/netmask
   ```

   若要允許所有 IP 位址、您應該指定 `-ip-list 0.0.0.0/0`

5. 將新原則與叢集管理 LIF 建立關聯：

   ```
   network interface modify -vserver cluster_management_LIF -lif cluster_mgmt
   -firewall-policy policy-name
   ```

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

使用 **Telnet** 要求存取 **ONTAP** 叢集

您可以向叢集發出遠端登入要求、以執行管理工作。預設會停用Telnet。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

開始之前

在使用Telnet存取叢集之前、必須符合下列條件：

- 您必須擁有一個叢集本機使用者帳戶、並設定為使用遠端登入作為存取方法。

  `-application`命令參數 `security login`
  會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["指令參考資料ONTAP"^]需詳細 `security login`資訊，請參閱。

關於這項工作

- 支援每個節點最多50個並行的遠端登入工作階段。ONTAP

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- 如果您想ONTAP 要從Windows主機存取此功能、可以使用第三方公用程式、例如Putty。
- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 Telnet 安全性傳輸協定：

   ```
   security protocol show
   ```

   a. 如果已啟用 Telnet 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 Telnet 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application telnet -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify`"指令參考資料ONTAP"。

2. 確認管理階層中存在該 `management-telnet-server` 服務：

   ```
   network interface show -services management-telnet-server
   ```

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

   a. 如果 `management-telnet-server` 服務存在、請繼續下一步。

   b. 如果 `management-telnet-server` 服務不存在、請使用下列命令來新增服務：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-telnet-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

開始之前

在使用Telnet存取叢集之前、必須符合下列條件：

- 叢集或節點管理生命里所使用的管理防火牆原則中、必須已啟用遠端登入、以便透過防火牆來處理遠端登入要求。

  預設會停用Telnet。 `system services firewall policy show`含有 `-service telnet`參數的命令會顯示是否已在防火牆原則中啟用 Telnet 。如"指令參考資料ONTAP"需詳細 `system services firewall policy`資訊，請參閱。

- 如果您使用IPv6連線、則必須在叢集上設定並啟用IPv6、而且防火牆原則必須已設定IPv6位址。

  此 `network options ipv6 show`命令會顯示是否已啟用 IPv6 。如"指令參考資料ONTAP"需詳細 `network options ipv6 show`資訊，請參閱。 `system services firewall policy show`命令會顯示防火牆原則。

步驟

1. 從管理主機輸入下列命令：

```
telnet hostname_or_IP
```

`hostname_or_IP`是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

Telnet要求範例

以下範例顯示了名為「joe」的使用者（已設定 Telnet 存取權限）如何發出 Telnet 請求來存取叢集管理 LIF 為 10.72.137.28 的叢集：

```
admin_host$ telnet 10.72.137.28

Data ONTAP
login: joe
Password:

cluster1::>
```

使用 **RSH** 要求存取 **ONTAP** 叢集

您可以向叢集發出RSHE要求以執行管理工作。rsh並非安全傳輸協定、預設為停用。

Telnet 和 RSH 不是安全的通訊協定；您應該考慮使用 SSH 來存取叢集。SSH提供安全的遠端Shell和互動式網路工作階段。如需詳細資訊、請 "使用 SSH 存取叢集"參閱。

開始之前

您必須符合下列條件、才能使用RSH存取叢集：

- 您必須擁有一個叢集本機使用者帳戶、並將其設定為使用RSH作為存取方法。

  `-application`命令參數 `security login`會指定使用者帳戶的存取方法。如link:https://docs.netapp.com/us-en/ontap-cli/search.html?q=security+login["指令參考資料ONTAP"^]需詳細 `security login`資訊，請參閱。

關於這項工作

- 支援每個節點最多50個並行的RSH工作階段。ONTAP

  如果叢集管理LIF位於節點上、則會與節點管理LIF共用此限制。

  如果傳入連線速度高於每秒10次、服務會暫時停用60秒。

- rsh 命令需要進階權限。

ONTAP 9 。 10.1 或更新版本

步驟

1. 確認已啟用 RSH 安全性通訊協定：

   ```
   security protocol show
   ```

   a. 如果啟用了 RSH 安全性通訊協定、請繼續下一步。

   b. 如果未啟用 RSH 安全性通訊協定、請使用下列命令加以啟用：

      ```
      security protocol modify -application rsh -enabled true
      ```

   深入瞭解 `security protocol show`及 `security protocol modify` "指令參考資料ONTAP"。

2. 確認管理階層中存在該 `management-rsh-server` 服務：

   ```
   network interface show -services management-rsh-server
   ```

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

   a. 如果 `management-rsh-server` 服務存在、請繼續下一步。

   b. 如果 `management-rsh-server` 服務不存在、請使用下列命令來新增服務：

      ```
      network interface service-policy add-service -vserver cluster1 -policy
      default-management -service management-rsh-server
      ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy add-service`資訊，請參閱。

ONTAP 9 9 或更早版本

開始之前

您必須符合下列條件、才能使用RSH存取叢集：

- Rsh必須已在叢集或節點管理生命體所使用的管理防火牆原則中啟用、以便讓RSHH要求能夠通過防火牆。

  依預設、 RSH 會停用。系統服務防火牆原則 show 命令及 `-service rsh`參數會顯示是否已在防火牆原則中啟用 RSH 。如"指令參考資料ONTAP"需詳細 `system services firewall policy`資訊，請參閱。

- 如果您使用IPv6連線、則必須在叢集上設定並啟用IPv6、而且防火牆原則必須已設定IPv6位址。

  此 `network options ipv6 show`命令會顯示是否已啟用 IPv6 。如"指令參考資料ONTAP"需詳細 `network options ipv6 show`資訊，請參閱。 `system services firewall policy show`命令會顯示防火牆原則。

步驟

1. 從管理主機輸入下列命令：

   ```
   rsh hostname_or_IP -l username:passwordcommand
   ```

`hostname_or_IP`是叢集管理 LIF 或節點管理 LIF 的主機名稱或 IP 位址。建議使用叢集管理LIF。您可以使用IPv4或IPv6位址。

`command`是您要透過 RSH 執行的命令。

RSH申請範例

下列範例顯示已設定 RSH 存取權限的使用者「 Joe 」如何發出 RSHE 要求來執行 `cluster show` 命令：

```
admin_host$ rsh 10.72.137.28 -l joe:password cluster show

Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
2 entries were displayed.

admin_host$
```

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

使用ONTAP 指令行介面

瞭解 ONTAP 命令列介面

支援指令行介面（CLI）ONTAP 、提供管理介面的命令型檢視。您可以在儲存系統提示字元輸入命令、命令結果會以文字顯示。

CLI 命令提示字元表示為 `cluster_name::>`。

如果您設定權限層級（也就是 `-privilege` 的參數 `set` 命令） `advanced`，提示包含星號（ `*` ），例如：

```
cluster_name::*>
```

如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

瞭解 CLI 命令的不同 ONTAP Shell

叢集有三種不同的CLI命令Shell：*clusterShell*、*nodesler_*和*_systemShell*。這些Shell的用途各不相同、而且每個Shell都有不同的命令集。

- 叢集Shell是在您登入叢集時自動啟動的原生Shell。

  它提供您設定及管理叢集所需的所有命令。clusterShell CLI 說明（在 clusterShell 提示字元觸發 `?`）會顯示可用的 clusterShell 命令。 `man clustershell` 中的命令顯示指定 `clustershell` 命令的手冊頁（`man <command_name>`）。如"指令參考資料ONTAP"需詳細 `man`資訊，請參閱。

- nodesdell是一種特殊的命令Shell、僅在節點層級生效。

  可透過命令存取 nodesdesh 。 `system node run`如"指令參考資料ONTAP"需詳細 `system node run`資訊，請參閱。

  nodesdeshed CLI 幫助（由 `help` Nodesdesh 提示符觸發 `?`）顯示可用的 nodesdesh 命令。 `man`nodesdesh 中的命令將顯示指定 nodesdesh 命令的手冊頁。

  許多常用的nodeslell命令和選項都經過通道處理或別名處理到clusterShell中、也可以從clusterShell執行。

- 系統Shell是一種低層Shell、僅用於診斷和疑難排解。

  systemshell 和相關 `diag` 帳戶是為了低層級的診斷目的而設計。他們的存取權限需要診斷權限層級、僅保留給技術支援人員執行疑難排解工作。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

存取叢集**Shell**中的**nodesdell**命令和選項

可以透過nodesdro解除 來存取Nodesl解除 命令和選項：

```
system node run -node nodename
```

許多常用的nodeslell命令和選項都經過通道處理或別名處理到clusterShell中、也可以從clusterShell執行。

可以使用以下方式存取叢集 shell 中支援的 Nodeshell 選項： `vserver options clustershell` 命令。若要查看這些選項，您可以使用下列命令查詢 clustershell CLI： `vserver options -vserver nodename_or_clustername -option-name ?`

如果您在clusterShell中輸入nodeslell或legacy命令或選項、且命令或選項具有等效的clusterShell命令、ONTAP則此功能會通知您要使用clusterShell命令。

如果您輸入叢集Shell不支援的nodeslell或legacy命令或選項、ONTAP 則會將命令或選項的「不支援」狀態通知您。

顯示可用的**nodesdro**解除 命令

您可以使用nodesdro解除 程序中的CLI說明、取得可用的nodesdro解除 命令清單。

步驟

1. 若要存取nodesdell、請在clusterShell的系統提示字元中輸入下列命令：

   `system node run -node {nodename|local}`

   `local` 是您用來存取叢集的節點。

   ⓘ ◦ `system node run` 命令具有 alias 命令、 `run`。

2. 在nodesdro解除 命令中輸入以下命令以查看可用的nodesl解除 命令列表：

   `[commandname] help`

`_commandname_` 是您要顯示其可用度的命令名稱。如果您不包括在內 `_commandname_`，CLI 會顯示所有可用的 nodesdesh 命令。

您輸入 exit 或鍵入 Ctrl-d 返回至 clustershell CLI 。

如"指令參考資料ONTAP"需詳細 `exit`資訊，請參閱。

顯示可用的**nodesl**解除 命令的範例

以下示例訪問名爲 node2 的節點的 nodesbate ，並顯示 nodesbate 命令的信息 environment：

```
cluster1::> system node run -node node2
Type 'exit' or 'Ctrl-D' to return to the CLI

node2> environment help
Usage: environment status |
     [status] [shelf [<adapter>[.<shelf-number>]]] |
     [status] [shelf_log] |
     [status] [shelf_stats] |
     [status] [shelf_power_status] |
     [status] [chassis [all | list-sensors | Temperature | PSU 1 |
     PSU 2 | Voltage | SYS FAN | NVRAM6-temperature-3 | NVRAM6-battery-3]]
```

如何瀏覽 **ONTAP CLI** 命令目錄

CLI中的命令會依命令目錄組織成階層。您可以輸入完整的命令路徑或瀏覽目錄結構、在階層中執行命令。

使用CLI時、您可以在提示字元中輸入目錄名稱、然後按Enter鍵來存取命令目錄。然後、目錄名稱會包含在提示字元中、表示您正在與適當的命令目錄互動。若要深入進入命令階層架構、請輸入命令子目錄的名稱、然後按Enter鍵。然後、子目錄名稱會包含在提示字元中、而內容會移至該子目錄。

您可以輸入整個命令、瀏覽多個命令目錄。例如、您可以輸入來顯示磁碟機的相關資訊 storage disk show 命令。您也可以一次瀏覽一個命令目錄來執行命令、如下列範例所示：

```
cluster1::> storage
cluster1::storage> disk
cluster1::storage disk> show
```

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

您可以在命令中只輸入最小字母數來縮短命令的縮寫、使命令對目前目錄具有唯一性。例如、若要在上一個範例中縮寫命令、您可以輸入 st d sh。您也可以使用分頁鍵來展開縮寫命令、並顯示命令的參數、包括預設參數值。

您可以使用 `top` 命令以移至命令階層的最上層、以及 `up` 命令或 `..` 命令可在命令階層中上移一層。

CLI中以星號（*）開頭的命令和命令選項只能在進階權限層級或更高層級執行。

相關資訊

- "頁首"
- "向上"

瞭解在 **ONTAP CLI** 中指定值的規則

大多數命令都包含一個或多個必要或選用的參數。許多參數都需要您為其指定一個值。在CLI中指定值的規則有幾種。

- 值可以是數字、布林指定符號、預先定義值列舉清單中的選取項目、或是文字字串。

  有些參數可以接受以逗號分隔的兩個或多個值清單。以逗號分隔的值清單不需要在引號中（""）。每當您指定文字、空格或查詢字元（若不是以小於或大於符號開頭的查詢或文字）時、必須以引號括住實體。

- CLI 將問號(`?`（問號）解釋爲用於顯示特定命令的幫助信息的命令。
- 您在CLI中輸入的某些文字（例如命令名稱、參數和某些值）不區分大小寫。

  例如、當您輸入的參數值時 `vserver cifs` 命令會忽略大寫。不過、大多數的參數值（例如節點名稱、儲存虛擬機器（SVM）、集合體、磁碟區和邏輯介面）都會區分大小寫。

- 如果您想要清除某個參數的值、而該參數取用字串或清單、請指定一組空白的引號（""）或破折號（""-""）。
- 雜湊符號 (`#`) 也稱為井字號，表示命令列輸入的註解；如果使用，則應該出現在命令列的最後一個參數之後。

  CLI 會忽略該行與結尾之間的文字 `#`。

在下列範例中、會以文字註解建立SVM。然後修改SVM以刪除註解：

```
cluster1::> vserver create -vserver vs0 -subtype default -rootvolume
root_vs0
-aggregate aggr1 -rootvolume-security-style unix -language C.UTF-8 -is
-repository false -ipspace ipspaceA -comment "My SVM"
cluster1::> vserver modify -vserver vs0 -comment ""
```

在下列範例中，使用符號的命令列註解 `#`會指出命令的作用。

```
cluster1::> security login create -vserver vs0 -user-or-group-name new-
admin
-application ssh -authmethod password #This command creates a new user
account
```

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

檢視 **ONTAP** 命令歷程記錄，然後重新執行歷程記錄中的任何命令

每個CLI工作階段都會記錄其中發出的所有命令。您可以檢視目前所在工作階段的命令歷程記錄。您也可以重新發出命令。

若要檢視命令歷程記錄、您可以使用 `history` 命令。

若要重新發出命令、您可以使用 `redo` 具有下列其中一個引數的命令：

- 符合先前命令一部分的字串

  例如、如果是唯一的 `volume` 您執行的命令是 `volume show`、您可以使用 `redo volume` 命令以重新執行命令。

- 上一個命令的數字ID、如所列 `history` 命令

  例如、您可以使用 `redo 4` 命令重新發出記錄清單中的第四個命令。

- 歷史記錄清單結尾的負偏移量

  例如、您可以使用 `redo -2` 命令重新發出您之前執行兩個命令的命令。

例如、若要重做命令歷程記錄結尾第三個命令、請輸入下列命令：

```
cluster1::> redo -3
```

相關資訊

- "歷史記錄"
- "重作"
- "Volume"

用於編輯 **CLI** 命令的 **ONTAP** 鍵盤快速鍵

目前命令提示字元的命令是作用中命令。使用鍵盤快速鍵可讓您快速編輯作用中命令。這些鍵盤快速鍵類似於UNIX tcsh Shell和EmACS編輯器。

下表列出用於編輯 CLI 命令的鍵盤快速鍵。 `Ctrl-`表示您在鍵入之後指定的字元時，按住 Ctrl 鍵。 `Esc-`表示您按下並放開 Esc 鍵，然後輸入之後指定的字元。

如果您想要...	使用下列其中一個鍵盤快速鍵 ...
將游標移回一個字元	• Ctrl-B • 返回箭號

如果您想要...	使用下列其中一個鍵盤快速鍵 ...
將游標往前移一個字元	• Ctrl-F • 下一頁箭頭
將游標移回一個字	ECB-B
將游標往前移一個字	ECF-F
將游標移到行首	Ctrl-A
將游標移到行尾	Ctrl-E
將命令列的內容從行首移至游標、然後儲存到剪下緩衝區。切割緩衝區的作用類似於暫存記憶體、類似於某些程式中稱為_剪 貼簿_的功能。	Ctrl-U
從游標移除命令列的內容至行尾、並將其儲存在剪下緩衝區中	Ctrl-K
從游標移除命令列的內容至下列字詞的結尾、並將其儲存在剪下緩衝區中	不需要
移除游標之前的字詞、並將其儲存在剪下緩衝區中	Ctrl-W
記下剪下緩衝區的內容、然後將其推入游標的命令列	Ctrl-Y
刪除游標前的字元	• Ctrl-H • 退格鍵
刪除游標所在的字元	Ctrl-D
清除此行	Ctrl-C
清除畫面	Ctrl-L
將命令列的目前內容取代為歷程記錄清單上的上一個項目。 每重複一次鍵盤快速鍵、歷程游標就會移到上一個項目。	• Ctrl-P • ECP-P • 向上箭頭

如果您想要...	使用下列其中一個鍵盤快速鍵 ...
將命令列的目前內容取代為歷程記錄清單上的下一個項目。每重複一次鍵盤快速鍵、歷程游標就會移至下一個項目。	• Ctrl-N • 不需要 • 向下鍵
展開部分輸入的命令、或列出目前編輯位置的有效輸入	• 索引標籤 • Ctrl-I
顯示內容相關的說明	？
轉義問題標記的特殊對應 `?`字元。例如，若要在命令的引數中輸入問號，請按 Esc 鍵，然後按下該 `?`字元。	不知道嗎？
啟動tty輸出	Ctrl-Q
停止tty輸出	Ctrl-S

瞭解 **ONTAP CLI** 命令的權限等級

下列三種權限層級定義了各種指令和參數：*admin*、*advanced* _和_*diagnostic*。ONTAP權限層級反映執行工作所需的技能層級。

- 管理

  大部分的命令和參數都可在此層級使用。它們用於一般或例行工作。

- 進階

  此層級的命令和參數不常使用、需要進階知識、如果使用不當、可能會造成問題。

  您只能在支援人員的建議下使用進階命令或參數。

- 診斷

  診斷命令和參數可能會中斷運作。只有支援人員才會使用這些工具來診斷及修正問題。

在 **ONTAP CLI** 中設定權限等級

您可以使用在 CLI 中設定權限等級 `set` 命令。權限層級設定的變更僅適用於您所在的工作階段。它們不會持續存在於各工作階段之間。

步驟

1. 若要在 CLI 中設定權限等級、請使用 `set` 命令 `-privilege` 參數。

設定權限層級的範例

下列範例將權限層級設為進階、然後設為管理：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by NetApp personnel.
Do you wish to continue? (y or n): y
cluster1::*> set -privilege admin
```

如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

設定 **ONTAP CLI** 的顯示偏好設定

您可以使用設定 CLI 工作階段的顯示偏好選項 `set` 命令和 `rows` 命令。您設定的偏好設定僅適用於您所在的工作階段。它們不會持續存在於各工作階段之間。

關於這項工作

您可以設定下列CLI顯示喜好設定：

- 命令工作階段的權限層級
- 是否針對可能造成中斷的命令發出確認
- 是否 `show` 命令會顯示所有欄位
- 用來做為欄位分隔符號的字元
- 報告資料大小的預設單位
- 在介面暫停輸出之前、螢幕在目前CLI工作階段中顯示的列數

  如果未指定偏好的列數、則會根據終端機的實際高度自動調整。如果未定義實際高度、則預設的列數為24。

- 預設的儲存虛擬機器（SVM）或節點
- 如果持續命令遇到錯誤、是否應停止

步驟

1. 若要設定 CLI 顯示偏好設定、請使用 `set` 命令。

   若要設定畫面在目前 CLI 工作階段中顯示的列數、您也可以使用 `rows` 命令。

   深入瞭解 `set`及 `rows` "指令參考資料ONTAP"。

在**CLI**中設定顯示喜好設定的範例

下列範例將逗號設定為欄位分隔符號集 `GB` 做為預設的資料大小單位、並將列數設定為 50 ：

```
cluster1::> set -showseparator "," -units GB
cluster1::> rows 50
```

相關資訊

- "顯示"
- "設定"
- "列"

在 **ONTAP CLI** 中使用查詢運算子

管理介面支援查詢和UNIX樣式的模式和萬用字元、可讓您在命令參數引數中比對多個值。

下表說明支援的查詢運算子：

營運者	說明
*	符合所有項目的萬用字元。 例如、命令 `volume show -volume *tmp*` 顯示名稱包含字串的所有磁碟區清單 `tmp`。
！	非營運者。 指出不相符的值；例如、 **`!vs0`** 表示不符合該值 `vs0`。
或營運者。 分隔要比較的兩個值；例如、 `*vs0	vs2*` 符合 Vs0 或 VS2 。您可以指定多個或敘述、例如 `a
b*	*c*` 符合項目 `a`，任何以開頭的項目 `b`以及任何包含的項目 `c`。
…	範圍運算子。 例如、 **`5..10`** 符合中的任何值 `5` 至 `10`、內含：
<	低於運算子。 例如、 **`<20`** 符合任何小於的值 `20`。
>	優於運算子。 例如、 **`>5`** 符合任何大於的值 `5`。
<=	小於或等於運算子。 例如、 **⇐5** 符合任何小於或等於的值 `5`。

營運者	說明
>=	大於或等於運算子。 例如、 **>=5** 符合任何大於或等於的值 `5`。
{query}	延伸查詢： 延伸查詢必須在命令名稱之後的第一個引數中指定為任何其他參數之前的第一個引數。 例如、命令 `volume modify {-volume *tmp*} -state offline` 將名稱包含字串的所有磁碟區設為離線 `tmp`。

如果您要將查詢字元剖析為文字、則必須將字元括在雙引號中（例如、 `"<10"`、 `"0..100"`、 `"*abc*"`或 `"a|b"`）以取得正確的結果。

您必須以雙引號括住原始檔案名稱、以避免特殊字元的解譯。這也適用於 clusterShell 使用的特殊字元。

您可以在單一命令列中使用多個查詢運算子。例如，此命令 `volume show -size >1GB -percent-used <50 -vserver !vs1`會顯示大小大於 1 GB ，使用率低於 50% 的所有磁碟區，而非名稱為「 'VS1' 」的儲存虛擬機器（ SVM ）中的所有磁碟區。

相關資訊

"用於編輯CLI命令的鍵盤快速鍵"

在 **ONTAP CLI** 中使用修改和刪除命令的延伸查詢

您可以使用延伸查詢來比對具有指定值的物件、並對其執行作業。

您可以在大括弧（ {} ）內將延伸查詢括起來、以指定延伸查詢。延伸查詢必須在命令名稱之後的第一個引數中指定為任何其他參數之前的第一個引數。例如、若要離線設定名稱包含字串的所有磁碟區 `tmp`，您可以在下列範例中執行命令：

```
cluster1::> volume modify {-volume *tmp*} -state offline
```

一般而言、延伸查詢僅適用於 `modify` 和 `delete` 命令。它們在中沒有意義 `create` 或 `show` 命令。

查詢與修改作業的組合是一項實用工具。但是、如果實作不正確、可能會造成混淆和錯誤。例如、使用（進階權限） `system node image modify` 用於設定節點預設軟體映像的命令會自動將其他軟體映像設為非預設。下列範例中的命令實際上是null作業：

```
cluster1::*> system node image modify {-isdefault true} -isdefault false
```

此命令會將目前的預設映像設為非預設映像、然後將新的預設映像（前一個非預設映像）設為非預設映像、進而保留原始的預設設定。若要正確執行作業、您可以使用下列範例所提供的命令：

```
cluster1::*> system node image modify {-iscurrent false} -isdefault true
```

使用 **Fields** 參數限制 **ONTAP show** 命令的輸出

當您使用 `-instance`參數搭配 `show`命令來顯示詳細資料時，輸出可能會很長，而且會包含比您需要的更多資訊。 `-fields`命令參數 `show`可讓您只顯示指定的資訊。

例如，執行 `volume show -instance`可能會導致多個資訊畫面。您可以使用 `volume show -fields *fieldname[,fieldname…]*`自訂輸出，使其僅包含指定的欄位（除了永遠顯示的預設欄位之外）。您可以使用 `-fields ?`來顯示命令的有效欄位 `show`。

下列範例顯示參數與 `-fields`參數之間的輸出差異 `-instance`：

```
cluster1::> volume show -instance

                                    Vserver Name: cluster1-1
                                     Volume Name: vol0
                                  Aggregate Name: aggr0
                                     Volume Size: 348.3GB
                              Volume Data Set ID: -
                       Volume Master Data Set ID: -
                                    Volume State: online
                                     Volume Type: RW
                                    Volume Style: flex
                                              ...
                           Space Guarantee Style: volume
                       Space Guarantee in Effect: true
                                              ...
Press <space> to page down, <return> for next line, or 'q' to quit...
...
cluster1::>

cluster1::> volume show -fields space-guarantee,space-guarantee-enabled

vserver  volume space-guarantee space-guarantee-enabled
-------- ------ --------------- ----------------------
cluster1-1 vol0   volume          true
cluster1-2 vol0   volume          true
vs1      root_vol
                  volume          true
vs2      new_vol
                  volume          true
vs2      root_vol
                  volume          true
...
cluster1::>
```

在命令輸入中使用 **ONTAP CLI** 位置參數

您可以利用ONTAP 資訊中心的位置參數功能來提高命令輸入的效率。您可以查詢命令以識別命令的位置參數。

什麼是位置參數

- 位置參數是一個參數、在指定參數值之前、不需要指定參數名稱。
- 位置參數可以與命令輸入中的非位置參數互連、只要它在同一個命令中觀察其相對順序與其他位置參數、如所示 ***command_name ?*** 輸出。
- 位置參數可以是命令的必要或選用參數。

- 參數可以是一個命令的位置、但不能是另一個命令的位置。

> 不建議在指令碼中使用位置參數功能、尤其是當指令的位置參數為選用、或是在指令碼之前列出選用參數時。

識別位置參數

您可以在中識別位置參數 ***command_name ?*** 命令輸出。位置參數的參數名稱前後有方括弧、格式如下：

- [*-parameter_name*] *parameter_value* 顯示位置所需的參數。
- [[*-parameter_name*] *parameter_value*] 顯示位置的選用參數。

例如、當顯示為中的下列項目時 ***command_name ?*** 輸出時、參數是其所顯示命令的位置：

- `[-lif] <lif-name>`
- `[[-lif] <lif-name>]`

但是、當顯示為下列項目時、參數會與顯示於中的命令非位置：

- `-lif <lif-name>`
- `[-lif <lif-name>]`

使用位置參數的範例

在下列範例中、 ***volume create ?*** 輸出顯示命令的位置為三個參數： `-volume`、 `-aggregate`和 `-size`。

```
cluster1::> volume create ?
   -vserver <vserver name>                Vserver Name
   [-volume] <volume name>                Volume Name
   [-aggregate] <aggregate name>          Aggregate Name
  [[-size] {<integer>[KB|MB|GB|TB|PB]}]   Volume Size
  [ -state {online|restricted|offline|force-online|force-offline|mixed} ]
                                          Volume State (default: online)
  [ -type {RW|DP|DC} ]                    Volume Type (default: RW)
  [ -policy <text> ]                      Export Policy
  [ -user <user name> ]                   User ID
  ...
  [ -space-guarantee|-s {none|volume} ]   Space Guarantee Style (default:
volume)
  [ -percent-snapshot-space <percent> ]   Space Reserved for Snapshot
Copies
  ...
```

在下列範例中、 `volume create` 命令是在不使用位置參數功能的情況下指定的：

```
cluster1::> volume create -vserver svm1 -volume vol1 -aggregate aggr1 -size 1g
-percent-snapshot-space 0
```

下列範例使用位置參數功能來提高命令輸入的效率。位置參數會與中的非位置參數互置 `volume create` 命令和位置參數值是在沒有參數名稱的情況下指定的。位置參數的指定順序與所指示的順序相同 **`volume create ?`** 輸出。也就是的價值 `-volume` 在的之前指定 `-aggregate`，而這又是在的之前指定的 `-size`。

```
cluster1::> volume create vol2 aggr1 1g -vserver svm1 -percent-snapshot-space 0
```

```
cluster1::> volume create -vserver svm1 vol3 -snapshot-policy default aggr1
-nvfail off 1g -space-guarantee none
```

如何訪問 **ONTAP CLI** 手冊頁

手冊（man）頁面說明如何使用CLI指令ONTAP ONTAP 。這些頁面可從命令列取得、也會發佈於特定版本的_command參考資料_。

在 ONTAP 命令列上，使用 `man <command_name>`命令顯示指定命令的手動頁面。如果未指定命令名稱、則會顯示手動頁面索引。您可以使用 `man man`命令來檢視命令本身的相關資訊 `man`。您可以輸入退出手冊頁 **`q`**。

如需更多關於您版本中所提供之管理層級和進階層級 ONTAP 命令"指令參考資料ONTAP"的資訊，請參閱。

錄製 **ONTAP CLI** 工作階段，並管理錄製的工作階段

您可以將CLI工作階段記錄到具有指定名稱和大小限制的檔案中、然後將檔案上傳至FTP或HTTP目的地。您也可以顯示或刪除先前錄製的CLI工作階段所在的檔案。

記錄**CLI**工作階段

當您停止錄製或結束CLI工作階段、或檔案達到指定的大小限制時、CLI工作階段的記錄即告結束。預設檔案大小限制為1 MB。檔案大小上限為2 GB。

記錄CLI工作階段很有用、例如、如果您正在疑難排解某個問題、想要儲存詳細資訊、或是想要在特定時間點建立永久的空間使用記錄。

步驟

1. 開始將目前的 CLI 工作階段錄製到檔案中：

   ```
   system script start
   ```

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

   將CLI工作階段記錄到指定的檔案中。ONTAP

2. 繼續進行CLI工作階段。
3. 完成後、停止錄製工作階段：

```
system script stop
```

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

停止記錄您的CLI工作階段。ONTAP

用於管理**CLI**工作階段記錄的命令

您可以使用 `system script` 用於管理 CLI 工作階段記錄的命令。

如果您想要...	使用此命令...
開始將目前的CLI工作階段錄製到指定的檔案	`system script start`
停止錄製目前的CLI工作階段	`system script stop`
顯示有關CLI工作階段記錄的資訊	`system script show`
將CLI工作階段的記錄上傳至FTP或HTTP目的地	`system script upload`
刪除CLI工作階段的記錄	`system script delete`

相關資訊

"指令參考資料ONTAP"

用於管理**CLI**工作階段自動逾時期間的命令

超時值指定CLI工作階段在自動終止之前保持閒置的時間。CLI逾時值為整個叢集範圍。也就是叢集中的每個節點都使用相同的CLI逾時值。

根據預設、CLI工作階段的自動逾時期間為30分鐘。

您可以使用 `system timeout` 用於管理 CLI 工作階段自動逾時期間的命令。

如果您想要...	使用此命令...
顯示CLI工作階段的自動逾時期間	`system timeout show`
修改CLI工作階段的自動逾時期間	`system timeout modify`

相關資訊

"指令參考資料ONTAP"

叢集管理（僅限叢集管理員）

檢視 ONTAP 叢集中的節點層級詳細資料

您可以檢視節點名稱，節點是否健全，以及是否符合參加叢集的資格。在進階權限層級、您也可以顯示節點是否保留epsilon。

步驟

1. 若要檢視叢集中節點的相關資訊，請使用 `cluster show`命令。

   如果您希望輸出顯示某個節點是否保留epsilon、請在進階權限層級執行命令。

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

叢集中顯示節點的範例

以下範例顯示四節點叢集中所有節點的相關資訊：

```
cluster1::> cluster show
Node                  Health  Eligibility
--------------------- ------- ------------
node1                 true    true
node2                 true    true
node3                 true    true
node4                 true    true
```

以下範例顯示進階權限層級中名稱為「'node1'」之節點的詳細資訊：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> cluster show -node node1

       Node: node1
  Node UUID: a67f9f34-9d8f-11da-b484-000423b6f094
    Epsilon: false
Eligibility: true
     Health: true
```

檢視 ONTAP 叢集層級詳細資料

您可以顯示叢集的唯一識別碼（UUID）、名稱、序號、位置和聯絡資訊。

步驟

1. 若要顯示叢集的屬性、請使用 `cluster identity show` 命令。

顯示叢集屬性的範例

下列範例顯示叢集的名稱、序號、位置和聯絡資訊。

```
cluster1::> cluster identity show

          Cluster UUID: 1cd8a442-86d1-11e0-ae1c-123478563412
          Cluster Name: cluster1
 Cluster Serial Number: 1-80-123456
      Cluster Location: Sunnyvale
       Cluster Contact: jsmith@example.com
```

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

修改 ONTAP 叢集屬性

您可以視需要修改叢集的屬性、例如叢集名稱、位置和聯絡資訊。

關於這項工作

您無法變更建立叢集時所設定的叢集UUID。

步驟

1. 若要修改叢集屬性、請使用 `cluster identity modify` 命令。

   此 `-name`參數指定叢集的名稱。深入瞭解 `cluster identity modify`以及在中指定叢集名稱"指令參考資料ONTAP"的規則。

   - `-location` 參數指定叢集的位置。
   - `-contact` 參數指定聯絡資訊、例如姓名或電子郵件地址。

重新命名叢集的範例

下列命令會將目前的叢集（「cluster1」）重新命名為「cluster2」：

```
cluster1::> cluster identity modify -name cluster2
```

檢視 ONTAP 叢集環狀圖的複寫狀態

您可以檢視叢集複寫環的狀態，以協助您診斷叢集範圍內的問題。如果叢集發生問題、支援人員可能會要求您執行此工作、以協助進行疑難排解。

步驟

1. 若要顯示叢集複寫環的狀態、請使用 `cluster ring show` 進階權限層級的命令。

顯示叢集環複寫狀態的範例

下列範例顯示名稱為node0之節點上VLDB複寫環的狀態：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you wish to continue? (y or n): y

cluster1::*> cluster ring show -node node0 -unitname vldb
          Node: node0
     Unit Name: vldb
        Status: master
         Epoch: 5
   Master Node: node0
    Local Node: node0
      DB Epoch: 5
DB Transaction: 56
 Number Online: 4
      RDB UUID: e492d2c1-fc50-11e1-bae3-123478563412
```

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

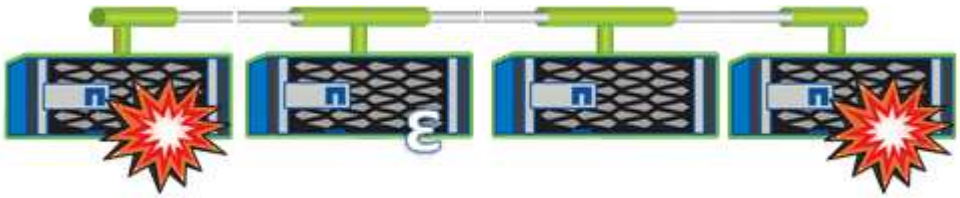
使用仲裁和 **epsilon** 進行 **ONTAP** 叢集健全狀況評估

仲裁和epsilon是叢集健全狀況和功能的重要衡量標準、可一起指出叢集如何因應潛在的通訊和連線挑戰。

_Quorum _是完整運作叢集的先決條件。當叢集達到仲裁數時、大多數的節點都很正常、可以彼此通訊。當仲裁遺失時、叢集便無法完成正常的叢集作業。由於所有節點共同共用資料的單一檢視、因此任何時候只有一個節點集合可以有仲裁。因此、如果允許兩個非通訊節點以不同方式修改資料、就無法再將資料協調成單一資料檢視。

叢集中的每個節點都會參與投票傳輸協定、選擇一個節點_master_；其餘每個節點都是_secondary _。主節點負責跨叢集同步處理資訊。當達到法定人數時、它會透過持續投票來維持。如果主節點離線且叢集仍處於仲裁狀態、則會由保持連線的節點選取新的主節點。

由於叢集內有一個節點數量偶數的關聯、因此一個節點有一個額外的分數投票權重稱為_epsilon_。如果大型叢集的兩個等部分之間的連線失敗、則包含epsilon的節點群組會維持仲裁、假設所有節點都正常運作。例如、下圖顯示其中兩個節點發生故障的四節點叢集。但是、由於其中一個可用節點保留了epsilon、即使沒有簡單多數的正常節點、叢集仍會維持在仲裁中。



在建立叢集時、Epsilon會自動指派給第一個節點。如果擁有epsilon的節點變得不健全、接管其高可用度合作夥

伴、或由其高可用度合作夥伴接管、則epsilon會自動重新指派至不同HA配對中的正常節點。

使節點離線可能會影響叢集保持仲裁狀態的能力。因此ONTAP 、如果您嘗試將叢集從仲裁中移出、或是將叢集從仲裁中移出一次中斷、就會發出警告訊息。您可以在進階權限層級使用命令來停用仲裁警告訊息 `cluster quorum-service options modify`。如"指令參考資料ONTAP"需詳細 `cluster quorum-service options modify`資訊，請參閱。

一般而言、假設叢集節點之間的連線可靠、較大型的叢集比較小的叢集更穩定。在24個節點的叢集中、只需簡單多數節點加上epsilon、就能比在兩個節點的叢集內更容易維護仲裁需求。

雙節點叢集在維護仲裁方面帶來一些獨特的挑戰。雙節點叢集使用_叢集HA _、其中兩個節點都不保留epsilon；而是會持續輪詢兩個節點、以確保當一個節點故障時、另一個節點擁有對資料的完整讀寫存取權、以及對邏輯介面和管理功能的存取權。

檢視 **ONTAP** 叢集中系統磁碟區的儲存容量使用率

系統磁碟區FlexVol 是包含特殊中繼資料的功能區、例如檔案服務稽核記錄的中繼資料。這些磁碟區可在叢集中看到、因此您可以充分考慮叢集中的儲存設備使用量。

系統磁碟區由叢集管理伺服器（也稱為管理SVM）擁有、當檔案服務稽核啟用時、系統就會自動建立這些磁碟區。

您可以使用檢視系統磁碟區 `volume show` 命令、但不允許執行大多數其他 Volume 作業。例如、您無法使用修改系統磁碟區 `volume modify` 命令。

此範例顯示管理SVM上的四個系統磁碟區、當叢集中的資料SVM啟用檔案服務稽核時、系統會自動建立這些磁碟區：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          2GB     1.90GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          2GB     1.90GB
5%
4 entries were displayed.
```

管理節點

將節點新增至 ONTAP 叢集

建立叢集之後、您可以新增節點來擴充叢集。您一次只能新增一個節點。

開始之前

- 如果您要將節點新增至多節點叢集，叢集中所有現有的節點都必須健全（如所示 `cluster show`）。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
- 如果您要將節點新增至雙節點無交換器叢集、則必須使用 NetApp 支援的叢集交換器、將雙節點無交換器叢集轉換為交換器連接的叢集。

  無交換器式叢集功能僅在雙節點叢集上受支援。

- 如果您要將第二個節點新增至單一節點叢集、則必須已安裝第二個節點、而且必須已設定叢集網路。
- 如果叢集已啟用 SP 自動組態、則為 SP 指定的子網路必須有可用資源、以允許連接節點使用指定的子網路自動設定 SP 。
- 您必須已收集下列資訊、以供新節點的節點管理LIF使用：
  - 連接埠
  - IP 位址
  - 網路遮罩
  - 預設閘道

關於這項工作

節點必須為偶數、才能形成HA配對。開始將節點新增至叢集之後、您必須完成此程序。節點必須是叢集的一部分、才能開始新增其他節點。

步驟

1. 開啟您要新增至叢集的節點。

   節點會開機、然後在主控台上啟動「節點設定精靈」。

```
Welcome to node setup.

You can enter the following commands at any time:
  "help" or "?" - if you want to have a question clarified,
  "back" - if you want to change previously answered questions, and
  "exit" or "quit" - if you want to quit the setup wizard.
     Any changes you made before quitting will be saved.

To accept a default or omit a question, do not enter a value.

Enter the node management interface port [e0M]:
```

2. 結束「節點設定精靈」：`exit`

   「節點設定」精靈會結束、並出現登入提示、警告您尚未完成設定工作。

   如"指令參考資料ONTAP"需詳細 `exit`資訊，請參閱。

3. 使用登入管理帳戶 `admin` 使用者名稱。
4. 啟動叢集設定精靈：

```
::> cluster setup

Welcome to the cluster setup wizard.

You can enter the following commands at any time:
 "help" or "?" - if you want to have a question clarified,
 "back" - if you want to change previously answered questions, and
 "exit" or "quit" - if you want to quit the cluster setup wizard.
 Any changes you made before quitting will be saved.

You can return to cluster setup at any time by typing "cluster setup".
To accept a default or omit a question, do not enter a value....

Use your web browser to complete cluster setup by accessing
https://<node_mgmt_or_e0M_IP_address>

Otherwise, press Enter to complete cluster setup using the
command line interface:
```

   有關使用設定 GUI 設定叢集的更多信息，請參閱"節點管理文檔" 。如"指令參考資料ONTAP"需詳細 `cluster setup`資訊，請參閱。

5. 按Enter鍵以使用CLI完成此工作。當系統提示您建立新叢集或加入現有叢集時、請輸入 **`join`**。

```
Do you want to create a new cluster or join an existing cluster?
{create, join}:
join
```

   如果新節點上執行的 ONTAP 版本與現有叢集上執行的版本不同，系統會回報 `System checks Error: Cluster join operation cannot be performed at this time`錯誤。這是預期的行為。若要繼續，請從叢集中的現有節點，以進階權限層級執行 `cluster add-node -allow-mixed-version-join true -cluster-ips <IP address> -node-names <new_node_name>`命令。

6. 依照提示設定節點並將其加入叢集：
   - 若要接受提示的預設值、請按Enter。

- 若要在提示字元中輸入您自己的值、請輸入值、然後按Enter。

7. 針對您要新增的每個額外節點、重複上述步驟。

完成後

將節點新增至叢集後、您應該為每個HA配對啟用儲存容錯移轉。

相關資訊

- "支援 ONTAP 軟體升級的混合版本叢集"
- "叢集附加節點"

從 **ONTAP** 叢集移除節點

您可以從叢集移除不需要的節點、一次移除一個節點。移除節點之後、您也必須移除其容錯移轉合作夥伴。如果您要移除節點、則其資料將無法存取或遭到清除。

開始之前

從叢集中移除節點之前，必須滿足以下條件：

- 叢集中有一半以上的節點必須健全。
- 所有資料、磁碟區和非根聚合都必須從節點中遷移或刪除。
  - 您要移除之節點上的所有資料都必須已清空。這可能包括"從加密磁碟區清除資料"。
  - 所有非根磁碟區都已存在 "已移動" 來自節點擁有的Aggregate。
  - 所有非根集合體都已存在 "已刪除" 從節點。
- 所有的生命和 VLAN 都已重新定位或從節點移除。
  - 資料生命之年 "已刪除" 或 "重新定位" 從節點。
  - 叢集管理生命 "重新定位" 從節點和主連接埠變更。
  - 所有叢集間的生命都是"已移除"。當您移除叢集間的lifs時、會顯示可忽略的警告。
  - 節點上的所有VLAN都是如此 "已刪除"。
- 節點未參與任何容錯移轉關係。
  - 儲存設備容錯移轉 "已停用" 用於節點。
  - 所有LIF容錯移轉規則都已達到 "已修改" 移除節點上的連接埠。
- 如果節點擁有聯邦資訊處理標準（FIPS）磁碟或自我加密磁碟（SED）、 "磁碟加密已移除" 將磁碟恢復為無保護模式。
  - 您可能也想要 "清除FIPS磁碟機或SED"。
- 如果要移除節點上的 LUN ，則應"修改「選擇性LUN對應（SLM)報告節點」清單"在移除節點之前先移除。

  如果您未將節點及其HA合作夥伴從「SLM-報告節點」清單中移除、即使將包含LUN的磁碟區移至另一個節點、先前在節點上的LUN存取仍可能遺失。

建議您發出AutoSupport 一份資訊消息、通知NetApp技術支援部門正在移除節點。

請勿執行如，，等作業 `cluster remove-node`， `cluster unjoin`以及 `node rename`正在進行自動化 ONTAP 升級時。

關於這項工作

- 如果您執行的是混合版本叢集、您可以使用ONTAP 以《更新版本》9.3開頭的進階權限命令之一、移除最後一個低版本節點：
  - ONTAP 9.3 ： `cluster unjoin -skip-last-low-version-node-check`
  - ONTAP 9.4 及更新版本： `cluster remove-node -skip-last-low-version-node-check`
- 如果從四節點叢集中移除兩個節點，則剩餘兩個節點上的叢集 HA 將自動啟用。

在將節點從叢集中移除之前，必須使連接到該節點的所有磁碟上的所有系統和使用者資料對使用者無法存取。

如果節點被錯誤地從叢集中移除，請聯絡 NetApp 支援以取得恢復選項的協助。

步驟

1. 將權限層級變更為進階：

```
set -privilege advanced
```

2. 識別叢集中具有 epsilon 的節點：

```
cluster show
```

在以下範例中、「node0」目前持有 epsilon：

```
cluster::*>
Node                  Health  Eligibility  Epsilon
--------------------- ------- ------------ ------------
node0                 true    true         true
node1                 true    true         false
node2                 true    true         false
node3                 true    true         false
```

3. 如果您要移除的節點包含 epsilon：
   a. 將 epsilon 從要移除的節點中移出：

```
cluster modify -node <name_of_node_to_be_removed> -epsilon false
```

   b. 將 epsilon 移到您不會刪除的節點：

```
cluster modify -node <node_name> -epsilon true
```

4. 識別目前的主節點：

```
cluster ring show
```

主節點是保存諸如，， `vldb`， `vifmgr` `bcomd`和 `crs`等處理程序的節點 `mgmt`。

5. 如果要移除的節點是目前的主節點，請啟用叢集中的另一個節點以選舉為主節點：

a. 使目前的主節點不符合參加叢集的資格：

```
cluster modify -node <node_name> -eligibility false
```

該節點會被標記為不健康，直到其恢復資格。當主節點失去資格時，叢集仲裁會從剩餘節點中選出一個作為新的主節點。

> 如果您在 HA 對中的第一個節點上執行此步驟，則只需將該節點標記為不符合條件。請勿修改 HA 夥伴的狀態。
>
> 如果選擇合作夥伴節點作為新的主節點，您需要在將其設為不符合資格之前驗證它是否持有 epsilon。如果合作夥伴節點持有 epsilon，您需要在將其設為不符合資格之前，將 epsilon 移至叢集中剩餘的其他節點。當您重複這些步驟以移除合作夥伴節點時，您需要執行此操作。

a. 讓先前的主節點符合資格再次參與叢集：

```
cluster modify -node <node_name> -eligibility true
```

6. 登入您不會從叢集中移除之節點上的遠端節點管理 LIF 或叢集管理 LIF。
7. 從叢集中移除節點：

此版本... **ONTAP**	使用此命令...
ONTAP 9.3	`cluster unjoin`

此版本... ONTAP	使用此命令...

更新版本ONTAP	使用節點名稱：
	`cluster remove-node -node <node_name>`
	使用節點 IP ：
	`cluster remove-node -cluster_ip <node_ip>`

如果您有混合版本的叢集、而且要移除最後一個較低版本的節點、請使用 `-skip-last-low-version -node-check` 參數。

系統會通知您下列事項：

- 您也必須從叢集移除節點的容錯移轉合作夥伴。
- 節點被移除後，在它重新加入叢集之前，必須使用啟動選單選項 **(4) Clean configuration and initialize all disks** 或選項 **(9) Configure Advanced Drive Partitioning** 來擦除節點的配置並初始化所有磁碟。

  如果您在移除節點之前必須處理的條件、就會產生故障訊息。例如、此訊息可能表示節點具有必須移除的共用資源、或節點位於叢集HA組態或必須停用的儲存容錯移轉組態中。

如果節點是仲裁主機、叢集將會短暫遺失、然後返回仲裁。此仲裁損失是暫時性的、不會影響任何資料作業。

8. 如果失敗訊息指出錯誤情況、請解決這些情況、然後重新執行 `cluster remove-node` 或 `cluster unjoin` 命令。

   節點從叢集中成功移除後會自動重新開機。

9. 如果您要重新規劃節點的用途、請清除節點組態並初始化所有磁碟：
   a. 在開機程序期間、當系統提示時、按Ctrl-C可顯示開機功能表。
   b. 選擇開機選單選項 **(4) Clean configuration and initialize all disks**。
10. 返回管理員權限等級：

```
set -privilege admin
```

11. 重複步驟 1. 至 9，從叢集中移除容錯移轉合作夥伴。

相關資訊

- "叢集移除節點"

服務處理器基礎架構 (spi）網路服務預設為啟用、可讓網頁瀏覽器存取叢集中節點的記錄檔、核心傾印和 MIB 檔案。即使節點關閉、只要節點由其合作夥伴接管、檔案仍可存取。

開始之前

- 叢集管理LIF必須已啟動。

  您可以使用叢集或節點的管理 LIF 來存取 spi Web 服務。不過、建議使用叢集管理LIF。

  ◦ network interface show 命令會顯示叢集中所有生命的狀態。

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

- 您必須使用本機使用者帳戶來存取 spi Web服務、不支援網域使用者帳戶。
- 如果您的使用者帳戶沒有 admin`角色（有權訪問 `spi web 服務），您的存取控制角色必須被授予訪問 `spi`網路服務。

  ◦ vserver services web access show 命令會顯示哪些角色可存取哪些 Web 服務。

- 如果您不使用 `admin`用戶帳戶（包括 `http`訪問方法），您的用戶帳戶必須設定 `http`訪問方法。

  ◦ security login show 命令會顯示使用者帳戶的存取和登入方法及其存取控制角色。

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

- 如果您想要使用HTTPS進行安全的網路存取、則必須啟用SSL並安裝數位憑證。

  ◦ system services web show 命令會顯示叢集層級的 Web 傳輸協定引擎組態。

關於這項工作

◦ spi Web 服務預設為啟用、且可手動停用該服務 (vserver services web modify -vserver * -name spi -enabled false) 。

這 admin`角色被授予存取權限 `spi`預設的 Web 服務，可以手動停用訪問 (`services web access delete -vserver *cluster_name* -name spi -role admin`) 。

步驟

1. 將 Web 瀏覽器指向 spi 下列其中一種格式的 Web 服務 URL ：

   ◦ http://*cluster-mgmt-LIF*/spi/

   ◦ https://*cluster-mgmt-LIF*/spi/

   cluster-mgmt-LIF 是叢集管理 LIF 的 IP 位址。

2. 當瀏覽器提示時、請輸入您的使用者帳戶和密碼。

   驗證帳戶後、瀏覽器會顯示的連結 /mroot/etc/log/、 /mroot/etc/crash/`和 `/mroot/etc/mib/ 叢集中每個節點的目錄。

存取 **ONTAP** 節點的系統主控台

如果節點掛在開機功能表或開機環境提示字元、您只能透過系統主控台（也稱為_serial主控台_）來存取。您可以從SSH連線存取節點的系統主控台、以連線至節點的SP或叢集。

關於這項工作

SP ONTAP 和供應項目命令均可讓您存取系統主控台。不過、從SP、您只能存取自己節點的系統主控台。您可以從叢集存取叢集中任何其他節點（本機節點除外）的系統主控台。

步驟

1. 存取節點的系統主控台：

如果您在...	輸入此命令...
節點的SP CLI	`system console`
CLI ONTAP	`system node run-console`

2. 當系統提示您登入系統主控台時、請立即登入。
3. 若要結束系統主控台、請按Ctrl-D

存取系統主控台的範例

下列範例顯示輸入的結果 `system console` 命令。系統主控台指出節點2在開機環境提示字元掛起。。`boot_ontap` 在主控台輸入命令、將節點開機至 ONTAP 。然後按Ctrl-D退出主控台並返回SP。

```
SP node2> system console
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

（按Ctrl-D退出系統主控台。）

```
Connection to 123.12.123.12 closed.
SP node2>
```

下列範例顯示輸入的結果 `system node run-console` ONTAP 命令存取 node2 的系統主控台、節點 2 會在

開機環境提示字元下掛起。。 `boot_ontap` 在主控台輸入命令、將 node2 開機至 ONTAP 。然後按Ctrl-D離開主控台並返回ONTAP 到還原。

```
cluster1::> system node run-console -node node2
Pressing Ctrl-D will end this session and any further sessions you might
open on top of this session.
Type Ctrl-D to exit.

LOADER>
LOADER> boot_ontap
...
******************************
*                            *
* Press Ctrl-C for Boot Menu. *
*                            *
******************************
...
```

（按Ctrl-D退出系統主控台。）

```
Connection to 123.12.123.12 closed.
cluster1::>
```

管理 **ONTAP** 節點根磁碟區和根集合體

節點的根Volume FlexVol 是指由原廠安裝或安裝軟體安裝的一個現象。它保留給系統檔案、記錄檔和核心檔案。目錄名稱為 `/mroot`，只有技術支援人員才能透過系統 Shell 存取。節點根磁碟區的最小大小取決於平台模型。

管理節點根磁碟區和根集合體總覽的規則

節點的根磁碟區包含該節點的特殊目錄和檔案。根Aggregate包含根磁碟區。節點的根磁碟區和根Aggregate有幾項規則。

- 下列規則管理節點的根Volume：
  - 除非技術支援人員指示您這麼做、否則請勿修改根磁碟區的組態或內容。
  - 請勿將使用者資料儲存在根Volume中。

    將使用者資料儲存在根磁碟區中、會增加HA配對中節點之間的儲存恢復時間。

  - 您可以將根磁碟區移至其他Aggregate。 請參閱 [relocate-root]。
- 根Aggregate僅專供節點的根Volume使用。

  無法在根Aggregate中建立其他磁碟區。ONTAP

"NetApp Hardware Universe"

釋放節點根磁碟區上的空間

當節點的根磁碟區已滿或幾乎已滿時、會出現警告訊息。當節點的根磁碟區已滿時、節點無法正常運作。您可以刪除核心傾印檔案，封包追蹤檔案和根磁碟區快照，來釋放節點根磁碟區上的空間。

步驟

1. 顯示節點的核心傾印檔案及其名稱：

   `system node coredump show`

2. 從節點刪除不需要的核心傾印檔案：

   `system node coredump delete`

3. 存取節點：

   `system node run -node nodename`

   `nodename` 是要釋放其根磁碟區空間的節點名稱。

4. 從nodesdro解除 高階權限層級：

   `priv set advanced`

5. 透過nodesdro解除 顯示及刪除節點的封包追蹤檔案：
   a. 顯示節點根磁碟區中的所有檔案：

      `ls /etc`

   b. 如果有任何封包追蹤檔案 (`*.trc`）位於節點的根磁碟區中、請分別刪除：

      `rm /etc/log/packet_traces/file_name.trc`

6. 透過節點公用區識別並刪除節點的根磁碟區快照：
   a. 識別根磁碟區名稱：

      `vol status`

      根 Volume 由的「選項」欄中的「 root 」一詞表示 `vol status` 命令輸出。

      在以下範例中、根磁碟區是 `vol0`：

```
node1*> vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
                                64-bit
```

a. 顯示根磁碟區快照：

```
snap list root_vol_name
```

b. 刪除不需要的根磁碟區快照：

```
snap delete root_vol_namesnapshot_name
```

7. 退出nodesdell並返回clusterShell：

```
exit
```

將根磁碟區重新部署到新的**Aggregate**

根置換程序會將目前的根Aggregate移轉到另一組磁碟、而不會造成中斷。

關於這項工作

必須啟用儲存容錯移轉、才能重新部署根磁碟區。您可以使用 `storage failover modify -node` *`nodename`* `-enable true` 啟用容錯移轉的命令。

您可以在下列案例中、將根磁碟區的位置變更為新的Aggregate：

- 當根集合體不在您偏好的磁碟上時
- 當您想要重新排列連接至節點的磁碟時
- 當您執行更換EOS磁碟櫃的磁碟櫃時

步驟

1. 將權限層級設為進階：

```
set privilege advanced
```

2. 重新部署根Aggregate：

```
system node migrate-root -node nodename -disklist disklist -raid-type raid-type
```

◦ 節點

指定擁有您要移轉之根Aggregate的節點。

◦ 磁碟清單

指定要在其中建立新根Aggregate的磁碟清單。所有磁碟都必須是備援磁碟、且必須由同一個節點擁有。所需的磁碟數目下限取決於RAID類型。

- * RAID類型*

  指定根Aggregate的RAID類型。預設值為 `raid-dp`。

3. 監控工作進度：

   `job show -id jobid -instance`

結果

如果所有的預先檢查都成功、命令會啟動根磁碟區置換工作並結束。期望節點重新啟動。

相關資訊

- "儲存故障轉移修改"

啟動或停止 **ONTAP** 節點以進行維護或疑難排解

基於維護或疑難排解的理由、您可能需要啟動或停止節點。您可以從ONTAP 支援的CLI、開機環境提示字元或SP CLI執行此動作。

使用 SP CLI 命令 `system power off` 或 `system power cycle` 若要關閉或重新啟動節點、可能會導致節點關機不正確（也稱為 _ 不正常關機 _ ）、無法取代使用 ONTAP 的正常關機 `system node halt` 命令。

在系統提示下重新啟動節點

您可以在系統提示字元中、以正常模式重新開機節點。節點已設定為從開機裝置（例如PC compactflash卡）開機。

步驟

1. 如果叢集包含四個或更多節點、請確認要重新開機的節點未保留epsilon：

   a. 將權限層級設為進階：

      `set -privilege advanced`

   b. 判斷哪個節點擁有epsilon：

      `cluster show`

      以下範例顯示「'node1'」擁有epsilon：

```
cluster1::*> cluster show
Node                  Health  Eligibility   Epsilon
--------------------- ------- ------------  ------------
node1                 true    true          true
node2                 true    true          false
node3                 true    true          false
node4                 true    true          false
4 entries were displayed.
```

a. 如果要重新開機的節點保留了epsilon、請從節點移除epsilon：

cluster modify -node *node_name* -epsilon false

b. 將epsilon指派給另一個將維持正常運作的節點：

cluster modify -node *node_name* -epsilon true

c. 返回管理權限層級：

set -privilege admin

2. 使用 `system node reboot` 命令重新啟動節點。

如果您未指定 `-skip-lif-migration` 參數時、命令會嘗試在重新開機之前、將資料和叢集管理同步移轉至另一個節點。如果LIF移轉失敗或逾時、重新開機程序便會中止、ONTAP 而導致錯誤顯示LIF移轉失敗。

```
cluster1::> system node reboot -node node1 -reason "software upgrade"
```

節點會開始重新開機程序。出現此畫面的功能登入提示、表示重新開機程序已完成。ONTAP

在**ONTAP** 開機環境提示字元中開機

當您處於節點的開機環境提示時、可以開機目前版本或ONTAP 是發行的支援版本。

步驟

1. 使用從儲存系統提示存取開機環境提示 `system node halt` 命令。

儲存系統主控台會顯示開機環境提示字元。

2. 在開機環境提示字元中、輸入下列其中一個命令：

若要開機...	輸入...
目前發行ONTAP 的	`boot_ontap`
從開機裝置獲得的鏡像ONTAP	`boot_primary`

若要開機...	輸入...
來自開機裝置的支援鏡像ONTAP	`boot_backup`

如果您不確定要使用哪一個映像、您應該使用 `boot_ontap` 在第一個執行個體中。

關閉節點

如果某個節點沒有回應、或是支援人員引導您進行疑難排解、您可以關閉該節點。

步驟

1. 如果叢集包含四個或更多節點、請確認要關閉的節點未保留epsilon：

   a. 將權限層級設為進階：

      `set -privilege advanced`

   b. 判斷哪個節點擁有epsilon：

      `cluster show`

      以下範例顯示「'node1'」擁有epsilon：

```
cluster1::*> cluster show
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node1                true    true          true
node2                true    true          false
node3                true    true          false
node4                true    true          false
4 entries were displayed.
```

   a. 如果要關閉的節點保留了epsilon、請從節點移除epsilon：

      `cluster modify -node node_name -epsilon false`

   b. 將epsilon指派給另一個將維持正常運作的節點：

      `cluster modify -node node_name -epsilon true`

   c. 返回管理權限層級：

      `set -privilege admin`

2. 使用 `system node halt` 關閉節點的命令。

   如果您未指定 `-skip-lif-migration` 參數時、命令會嘗試在關機之前、同步將資料和叢集管理移轉至另一個節點。如果LIF移轉失敗或逾時、關機程序便會中止、ONTAP 而導致錯誤顯示LIF移轉失敗。

您可以使用這兩種方式、在關機時手動觸發核心傾印 `-dump` 參數。

下列範例會關閉名為「'node1'」的節點、以進行硬體維護：

```
cluster1::> system node halt -node node1 -reason 'hardware maintenance'
```

使用開機功能表管理 **ONTAP** 節點

您可以使用開機功能表來修正節點上的組態問題、重設管理密碼、初始化磁碟、重設節點組態、以及將節點組態資訊還原回開機裝置。

如果HA配對正在使用 "加密SAS或NVMe磁碟機（SED、NSE、FIPS）"、您必須遵循主題中的指示 "將FIPS磁碟機或SED恢復為無保護模式" 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

步驟

1. 重新啟動節點、以使用存取開機功能表 `system node reboot` 命令。

   節點會開始重新開機程序。

2. 在重新開機程序期間、當系統提示時、按Ctrl-C可顯示開機功能表。

   節點會顯示開機功能表的下列選項：

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set onboard key management recovery secrets.
(11) Configure node for external key management.
Selection (1-11)?
```

   開機功能表選項（2）不使用/etc/rc開機已過時、對系統不會有任何影響。

3. 輸入對應的號碼、選取下列其中一個選項：

至...	選取...
繼續以正常模式開機節點	1）正常開機

至...	選取...
變更節點的密碼、也就是「admin」帳戶密碼	3）變更密碼
初始化節點的磁碟、並為節點建立根磁碟區	4）清除組態並初始化所有磁碟 此功能表選項會清除節點磁碟上的所有資料、並將節點組態重設為原廠預設值。 僅當節點已從叢集中移除且未加入其他叢集時，才選擇此選單項目。 對於具有內部或外部磁碟櫃的節點、會初始化內部磁碟上的根磁碟區。如果沒有內部磁碟櫃、則會初始化外部磁碟上的根磁碟區。 如果您要初始化的節點有磁碟已分割以進行根資料分割、則磁碟必須先取消分割、才能初始化節點、請參閱* 9）設定進階磁碟分割*和 "磁碟與集合體管理"。
執行Aggregate和磁碟維護作業、並取得詳細的Aggregate和磁碟資訊。	5）維護模式開機 您可以使用結束維護模式 `halt` 命令。
將組態資訊從節點的根磁碟區還原至開機裝置、例如PC compactflash卡	6）從備份組態更新Flash 將部分節點組態資訊儲存在開機裝置上。ONTAP當節點重新開機時、開機裝置上的資訊會自動備份到節點的根磁碟區。如果開機裝置毀損或需要更換、您必須使用此功能表選項、將組態資訊從節點的根磁碟區還原回開機裝置。
在節點上安裝新軟體	7）先安裝新軟體 如果ONTAP 開機裝置上的支援不支援您要用於根磁碟區的儲存陣列、您可以使用此功能表選項來取得支援儲存陣列的軟體版本、並將其安裝在節點上。 此功能表選項僅適用於在ONTAP 未安裝根Volume的節點上安裝更新版本的點菜軟體。請勿使用此功能表選項來升級ONTAP 功能表。
重新啟動節點	8）重新開機節點

至...	選取...

取消分割所有磁碟、移除其擁有權資訊、或清除組態、然後以整個或分割磁碟初始化系統	9）設定進階磁碟分割
	
	進階磁碟機分割選項為配置為根資料或根資料資料分割區的磁碟提供了額外的管理功能。以下選項可從Boot Option 9取得：
	
	`(9a) Unpartition all disks and remove their ownership information.`
	`(9b) Clean configuration and initialize system with partitioned disks.`
	`(9c) Clean configuration and initialize system with whole disks.`
	`(9d) Reboot the node.`
	`(9e) Return to main boot menu.`

檢視 **ONTAP** 叢集中節點的屬性

您可以檢視叢集中一或多個節點的屬性，例如名稱，擁有者，位置，型號，序號，節點執行時間，健全狀況狀態，以及參與叢集的資格。

步驟

1. 若要顯示指定節點或叢集中所有節點的屬性、請使用 `system node show` 命令。

顯示節點資訊的範例

以下範例顯示節點1的詳細資訊：

```
cluster1::> system node show -node node1
                           Node: node1
                          Owner: Eng IT
                       Location: Lab 5
                          Model: model_number
                  Serial Number: 12345678
                      Asset Tag: -
                         Uptime: 23 days 04:42
                NVRAM System ID: 118051205
                      System ID: 0118051205
                         Vendor: NetApp
                         Health: true
                    Eligibility: true
       Differentiated Services: false
           All-Flash Optimized: true
            Capacity Optimized: false
                 QLC Optimized: false
    All-Flash Select Optimized: false
 SAS2/SAS3 Mixed Stack Support: none
```

修改 **ONTAP** 節點的屬性

您可以視需要修改節點的屬性。您可以修改的屬性包括節點的擁有者資訊、位置資訊、資產標籤、以及參與叢集的資格。

關於這項工作

您可以使用、在進階權限層級修改節點參與叢集的資格 `-eligibility` 的參數 `system node modify` 或 `cluster modify` 命令。如果您將節點的資格設定為 `false`，節點在叢集中變成非作用中。

您無法在本機修改節點資格。必須從不同的節點進行修改。也無法使用叢集HA組態來修改節點資格。

您應該避免將節點的資格設定為 `false`，但還原節點組態或延長節點維護等情況除外。當節點不符合資格時、SAN和NAS對節點的資料存取可能會受到影響。

步驟

1. 使用 `system node modify` 修改節點屬性的命令。

修改節點屬性的範例

下列命令會修改「'node1'」節點的屬性。節點的擁有者設定為「'Joe Smith」、其資產標籤設定為「js1234'」：

```
cluster1::> system node modify -node node1 -owner "Joe Smith" -assettag
js1234
```

相關資訊

- "系統節點修改"
- "叢集修改"

重新命名 **ONTAP** 節點

您可以視需要變更節點名稱。

步驟

1. 若要重新命名節點、請使用 `system node rename` 命令。

   此 `-newname`參數會指定節點的新名稱。如"指令參考資料ONTAP"需詳細 `system node rename`資訊，請參閱。

   如果您要重新命名叢集中的多個節點、則必須個別執行每個節點的命令。

   節點名稱不能為「all」、因為「all」是系統保留名稱。

重新命名節點的範例

下列命令會將節點「'node1'」重新命名為「'node1a'」：

```
cluster1::> system node rename -node node1 -newname node1a
```

管理單節點 **ONTAP** 叢集

單節點叢集是在獨立節點上執行的叢集的特殊實作。 不建議使用單節點叢集、因為它們不提供備援。 如果節點故障、資料存取就會遺失。

為了容錯與不中斷營運、強烈建議您使用來設定叢集 "高可用度（ HA 配對）"。

如果您選擇設定或升級單節點叢集、您應該瞭解下列事項：

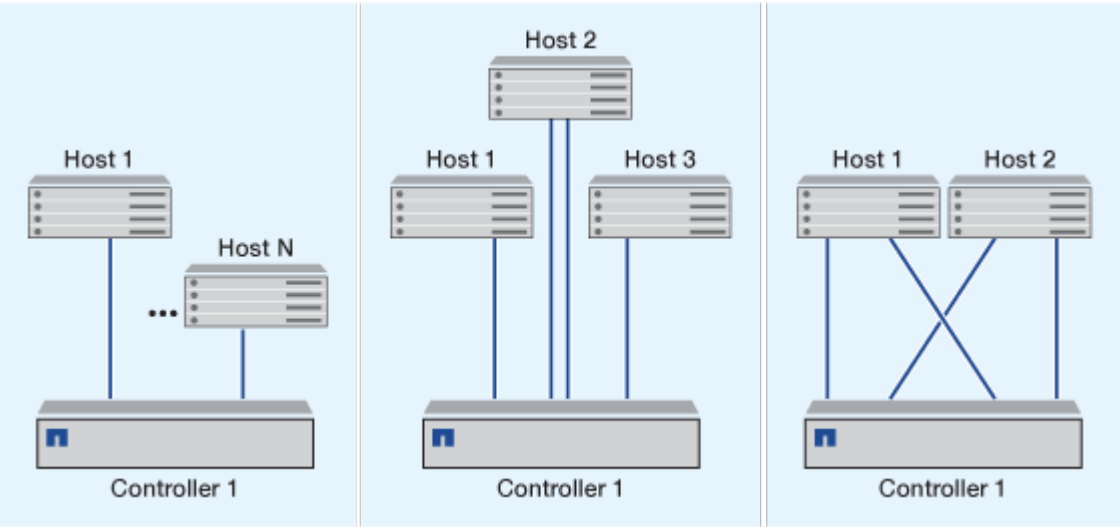
- 單一節點叢集不支援根磁碟區加密。
- 如果您移除節點以擁有單節點叢集、則應修改叢集連接埠、將叢集連接埠修改為資料連接埠、然後在資料連接埠上建立資料生命體、以提供資料流量。
- 對於單節點叢集、您可以在軟體設定期間指定組態備份目的地。設定完成後、您可以使用ONTAP 各種指令來修改這些設定。
- 如果有多個主機連線至節點、則每個主機都可以使用不同的作業系統設定、例如 Windows 或 Linux 。如果從主機到控制器有多個路徑、則必須在主機上啟用ALUA。

使用單一節點設定**iSCSI SAN**主機的方法

您可以將 iSCSI SAN 主機設定為直接連線至單一節點、或透過一或多個 IP 交換器進行連線。節點可與交換器建立多個 iSCSI 連線。

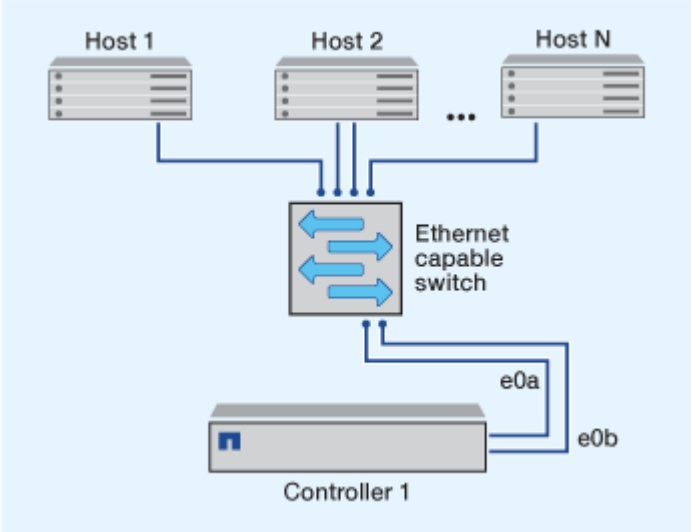
直接附加的單節點組態

在直接附加的單節點組態中、一個或多個主機會直接連線至節點。



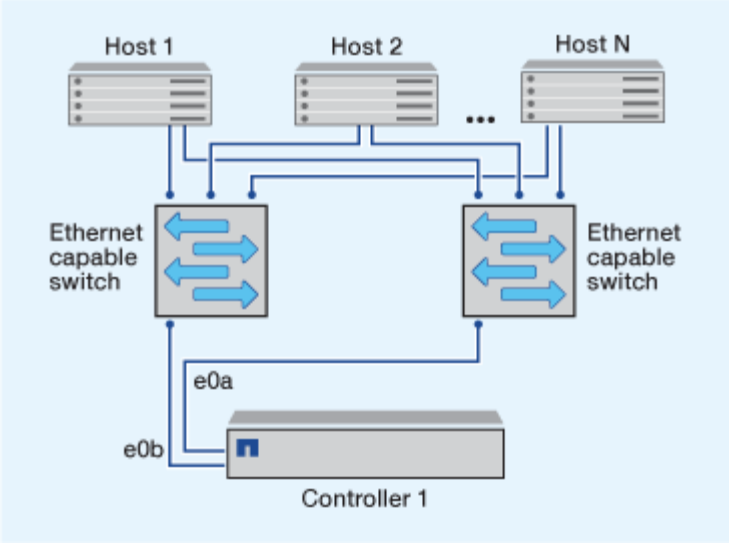
單一網路單節點組態

在單一網路單節點組態中、一台交換器會將單一節點連接至一或多個主機。由於只有一台交換器、因此此組態並未完全備援。



多網路單節點組態

在多網路單節點組態中、兩個或多個交換器會將單一節點連接至一或多個主機。由於有多個交換器、因此此組態完全備援。



使用單一節點設定**FC**和**FC-NVMe SAN**主機的方法

您可以透過一個或多個架構、使用單一節點來設定FC和FC-NVMe SAN主機。需要N連接埠ID虛擬化（NPIV）、而且必須在網路中的所有FC交換器上啟用。如果不使用FC交換器、則無法將FC或FC-NVE SAN主機直接連接至單一節點。

單一架構單節點組態

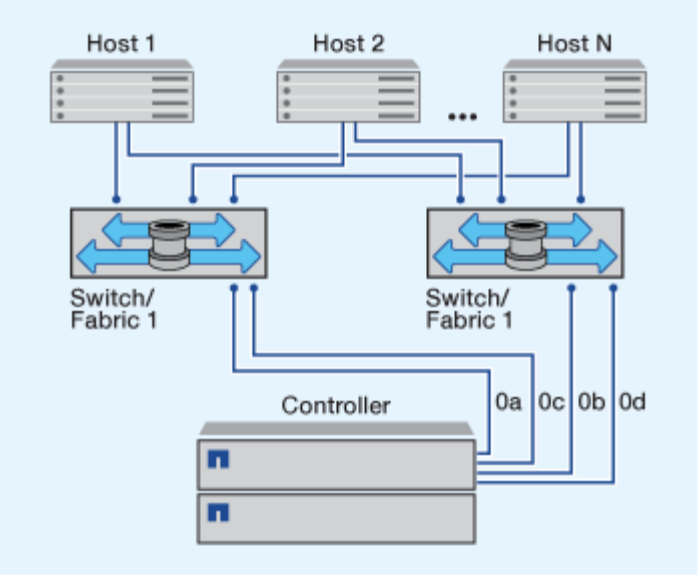
在單一架構單節點組態中、有一部交換器可將單一節點連接至一或多部主機。由於只有一台交換器、因此此組態並未完全備援。

在單一架構單節點組態中、如果您只有從主機到節點的單一路徑、則不需要多重路徑軟體。

多種單節點組態

在Mertifabric單節點組態中、有兩個或多個交換器可將單一節點連接至一或多個主機。為了簡化操作、下圖顯示只有兩個Fabric的Mertifabric單節點組態、但您可以在任何Mertifabric組態中使用兩個或多個Fabric。在本圖中、儲存控制器安裝在上機箱中、底部機箱可以是空的、也可以是IOMX模組、如同本範例所示。

圖示中的FC目標連接埠（0A、0c、0b、0d）為範例。實際的連接埠編號會因儲存節點的機型和是否使用擴充介面卡而有所不同。



相關資訊

"NetApp 技術報告 4684 ：使用 NVMe 實作及設定現代化 SAN"

單節點叢集的 ONTAP 升級

您可以使用ONTAP CLI 執行單節點叢集的自動更新。單節點叢集缺乏冗餘，這意味著更新始終會造成中斷。您無法使用 System Manager 執行中斷性升級。

開始之前

您必須完成升級 "準備" 步驟。

步驟

1. 刪除先前ONTAP 的版本：

```
cluster image package delete -version <previous_package_version>
```

2. 下載目標ONTAP 版的更新軟體套件：

```
cluster image package get -url location
```

```
cluster1::> cluster image package get -url
http://www.example.com/software/9.7/image.tgz

Package download completed.
Package processing completed.
```

3. 驗證叢集套件儲存庫中是否有可用的軟體套件：

```
cluster image package show-repository
```

```
cluster1::> cluster image package show-repository
Package Version  Package Build Time
---------------- ------------------
9.7              M/DD/YYYY 10:32:15
```

4. 確認叢集已準備好升級：

```
cluster image validate -version <package_version_number>
```

```
cluster1::> cluster image validate -version 9.7

WARNING: There are additional manual upgrade validation checks that must
be performed after these automated validation checks have completed...
```

5. 監控驗證進度：

```
cluster image show-update-progress
```

6. 完成驗證所識別的所有必要行動。
7. 您也可以產生軟體升級預估：

```
cluster image update -version <package_version_number> -estimate-only
```

軟體升級預估會顯示每個要更新元件的詳細資料、以及預估的升級期間。

8. 執行軟體升級：

```
cluster image update -version <package_version_number>
```

如果遇到問題、更新會暫停、並提示您採取修正行動。您可以使用叢集映像show-update-progress命令來檢視任何問題和更新進度的詳細資料。修正問題之後、您可以使用叢集映像resume-update命令繼續更新。

9. 顯示叢集更新進度：

```
cluster image show-update-progress
```

節點會在更新過程中重新開機、重新開機時無法存取。

10. 觸發通知：

```
autosupport invoke -node * -type all -message "Finishing_Upgrade"
```

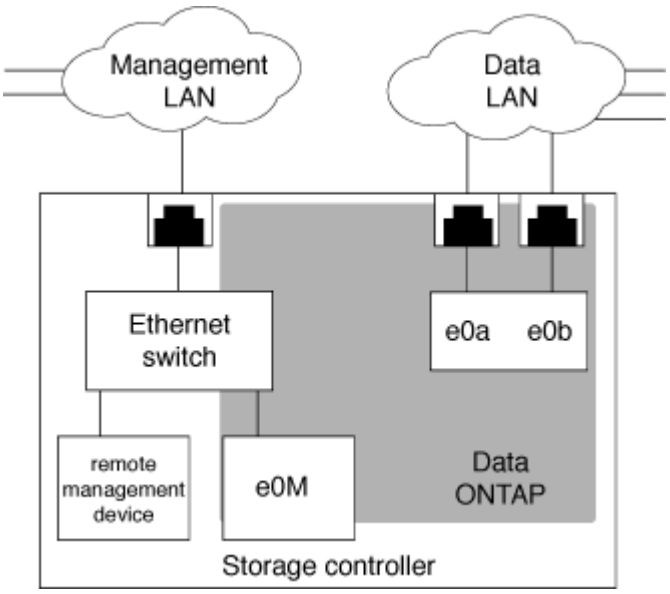
如果叢集未設定為傳送訊息、則通知複本會儲存在本機。

設定SP/BMC網路

隔離網路中的 **ONTAP** 管理流量

最佳實務做法是在專供管理流量使用的子網路上設定SP/BMC和e0M管理介面。透過管理網路執行資料流量可能會導致效能降低和路由問題。

大多數儲存控制器上的管理乙太網路連接埠（以機箱背面的扳手圖示表示）會連接至內部乙太網路交換器。內部交換器可連線至SP/BMC和e0M管理介面、您可以使用這些介面透過TCP/IP通訊協定（例如：Telnet、SSH和SNMP）來存取儲存系統。



如果您打算同時使用遠端管理裝置和e0M、則必須在相同的IP子網路上設定。由於這些是低頻寬介面、因此最佳做法是在專供管理流量使用的子網路上設定SP/BMC和e0M。

如果您無法隔離管理流量、或您的專屬管理網路異常龐大、您應該盡量將網路流量保持在最低。過多的入站廣播或多點傳送流量可能會降低SP/BMC效能。

有些儲存控制器AFF （例如、ESIEA800）有兩個外部連接埠、一個用於BMC、另一個用於e0M。對於這些控制器、不需要在相同的IP子網路上設定BMC和e0M。

瞭解 **ONTAP SP / BMC** 網路組態

您可以為SP啟用叢集層級的自動網路組態（建議）。您也可以停用SP自動網路組態（預設）、並在節點層級手動管理SP網路組態。每個案例都有幾個考量因素。

本主題同時適用於SP和BMC。

SP自動網路組態可讓SP使用指定子網路的位址資源（包括IP位址、子網路遮罩和閘道位址）、自動設定網路。有了SP自動網路組態、您不需要為每個節點的SP手動指派IP位址。依預設、SP自動網路組態會停用；這是因為啟用組態需要先在叢集中定義要用於組態的子網路。

如果啟用SP自動網路組態、則適用下列情境與考量：

- 如果SP從未設定、則會根據SP自動網路組態所指定的子網路、自動設定SP網路。
- 如果SP先前是手動設定的、或現有SP網路組態是以不同的子網路為基礎、則叢集中所有節點的SP網路會根據您在SP自動網路組態中指定的子網路重新設定。

  重新設定可能會導致SP被指派不同的位址、這可能會影響DNS組態及其解析SP主機名稱的能力。因此、您可能需要更新DNS組態。

- 加入叢集的節點會使用指定的子網路自動設定其SP網路。
- 。 `system service-processor network modify` 命令不允許您變更 SP IP 位址。

  啟用SP自動網路組態時、此命令僅允許您啟用或停用SP網路介面。

  - 如果先前已啟用SP自動網路組態、停用SP網路介面會釋放指派的位址資源並返回子網路。
  - 如果停用SP網路介面、然後重新啟用、則SP可能會以不同的位址重新設定。

如果停用SP自動網路組態（預設）、則適用下列情境與考量：

- 如果從未設定SP、則SP IPv4網路組態預設為使用IPV4 DHCP、且IPv6停用。

  加入叢集的節點預設也會使用IPV4 DHCP來進行SP網路組態。

- 。 `system service-processor network modify` 命令可讓您設定節點的 SP IP 位址。

  當您嘗試以分配給子網路的位址手動設定SP網路時、會出現一則警告訊息。忽略警告並繼續手動指派位址、可能會導致案例中出現重複位址。

如果在之前啟用SP自動網路組態之後、停用了該組態、則適用下列情況和考量：

- 如果 SP 自動網路組態已停用 IPv4 位址系列、則 SP IPv4 網路預設為使用 DHCP 、以及 `system service-processor network modify` 命令可讓您修改個別節點的 SP IPv4 組態。
- 如果 SP 自動網路組態已停用 IPv6 位址系列、則 SP IPv6 網路也會停用、且會停用 `system service-processor network modify` 命令可讓您啟用及修改個別節點的 SP IPv6 組態。

啟用 **ONTAP SP / BMC** 自動網路組態

啟用SP以使用自動網路組態優先於手動設定SP網路。由於SP自動網路組態是整個叢集範

圍、因此您不需要手動管理個別節點的SP網路。

此工作同時適用於SP和BMC。

- 您要用於SP自動網路組態的子網路必須已在叢集中定義、且與SP網路介面之間不得發生資源衝突。

  。 `network subnet show` 命令顯示叢集的子網路資訊。

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

  強制子網路關聯的參數（ `-force-update-lif-associations` 的參數 `network subnet` 命令）僅在網路階層上支援、而不在 SP 網路介面上支援。

- 如果您想要使用SP的IPv6連線、則必須已設定並啟用IPv6 ONTAP 才能執行支援。

  命令會 `network options ipv6 show`顯示 ONTAP 的 IPv6 設定目前狀態。如"指令參考資料ONTAP"需詳細 `network options ipv6 show`資訊，請參閱。

步驟

1. 使用指定要 SP 使用的子網路的 IPv4 或 IPv6 位址系列和名稱 `system service-processor network auto-configuration enable` 命令。
2. 使用顯示 SP 自動網路組態 `system service-processor network auto-configuration show` 命令。
3. 如果您之後想要停用或重新啟用所有法定節點的 SP IPv4 或 IPv6 網路介面、請使用 `system service-processor network modify` 命令 `-address-family` [`IPv4`|`IPv6`] 和 `-enable` [`true`|`false`] 參數。

   啟用SP自動網路組態時、您無法修改仲裁節點的SP IP位址。您只能啟用或停用SP IPv4或IPv6網路介面。

   如果某個節點超出仲裁量、您可以執行來修改節點的 SP 網路組態、包括 SP IP 位址 `system service-processor network modify` 從節點確認您要覆寫該節點的 SP 自動網路組態。但是、當節點加入仲裁時、會根據指定的子網路、針對節點進行SP自動重新設定。

手動設定 **ONTAP SP / BMC** 網路

如果您沒有設定SP的自動網路組態、則必須手動設定節點的SP網路、才能使用IP位址存取SP。

開始之前

如果您想要使用SP的IPv6連線、則必須已設定並啟用IPv6 ONTAP 才能執行支援。命令會 `network options ipv6`管理 ONTAP 的 IPv6 設定。如"指令參考資料ONTAP"需詳細 `network options ipv6`資訊，請參閱。

此工作同時適用於SP和BMC。

您可以將SP設定為使用IPV4、IPV6或兩者。SP IPV4組態支援靜態和DHCP定址、而SP IPv6組態僅支援靜態定址。

如果已設定 SP 自動網路組態、您就不需要手動設定個別節點和的 SP 網路 `system service-processor network modify` 命令僅允許您啟用或停用 SP 網路介面。

步驟

1. 使用設定節點的 SP 網路 `system service-processor network modify` 命令。
   - `-address-family` 參數指定是否要修改 SP 的 IPv4 或 IPv6 組態。
   - `-enable` 參數可啟用指定 IP 位址系列的網路介面。
   - `-dhcp` 參數指定是從 DHCP 伺服器使用網路組態、還是使用您提供的網路位址。

     您可以啟用 DHCP （透過設定 `-dhcp` 至 `v4`）僅當您使用的是 IPv4 時。您無法為IPv6組態啟用DHCP。

   - `-ip-address` 參數指定 SP 的公有 IP 位址。

     當您嘗試以分配給子網路的位址手動設定SP網路時、會出現一則警告訊息。忽略警告並繼續手動指派位址、可能會導致重複指派位址。

   - `-netmask` 參數指定 SP 的網路遮罩（如果使用的是 IPv4 ）。
   - `-prefix-length` 參數指定 SP 的子網路遮罩的網路前置字元長度（如果使用 IPv6 ）。
   - `-gateway` 參數指定 SP 的閘道 IP 位址。
2. 重複步驟1、為叢集中其餘節點設定SP網路。
3. 顯示 SP 網路組態、並使用驗證 SP 設定狀態 `system service-processor network show` 命令 `-instance` 或 `-field setup-status` 參數。

   節點的SP設定狀態可以是下列其中一項：

   - `not-setup` — 未設定
   - `succeeded` — 組態成功
   - `in-progress` — 正在進行組態
   - `failed` — 組態失敗

設定**SP**網路的範例

以下範例將節點的SP設定為使用IPV4、啟用SP、並顯示SP網路組態以驗證設定：

```
cluster1::> system service-processor network modify -node local
-address-family IPv4 -enable true -ip-address 192.168.123.98
-netmask 255.255.255.0 -gateway 192.168.123.1

cluster1::> system service-processor network show -instance -node local

                             Node: node1
                     Address Type: IPv4
                Interface Enabled: true
                   Type of Device: SP
                           Status: online
                      Link Status: up
                      DHCP Status: none
                       IP Address: 192.168.123.98
                      MAC Address: ab:cd:ef:fe:ed:02
                          Netmask: 255.255.255.0
       Prefix Length of Subnet Mask: -
         Router Assigned IP Address: -
              Link Local IP Address: -
                 Gateway IP Address: 192.168.123.1
                  Time Last Updated: Thu Apr 10 17:02:13 UTC 2014
                        Subnet Name: -
Enable IPv6 Router Assigned Address: -
            SP Network Setup Status: succeeded
    SP Network Setup Failure Reason: -

1 entries were displayed.

cluster1::>
```

修改 **ONTAP** 服務處理器 **API** 組態

SP API是一種安全的網路API、ONTAP 可讓支援透過網路與SP進行通訊。您可以變更SP API服務所使用的連接埠、續約服務用於內部通訊的憑證、或完全停用服務。只有在極少數情況下才需要修改組態。

關於這項工作

- SP API 服務使用連接埠 `50000` 依預設。

  例如、如果您在連接埠所在的網路設定中、則可以變更連接埠值 `50000` 用於其他網路應用程式的通訊、或是您想要區分流量與其他應用程式、以及 SP API 服務所產生的流量。

- SP API服務所使用的SSL和SSH憑證是叢集內部的憑證、不會在外部散佈。

  萬一憑證遭到入侵、您就可以續約。

- 預設會啟用SP API服務。

  您只需要在極少數情況下停用SP API服務、例如在未設定或使用SP且想要停用服務的私有LAN中。

  如果停用SP API服務、API將不接受任何傳入連線。此外、網路型SP韌體更新和網路型SP「自有系統」記錄收集等功能也無法使用。系統會切換至使用序列介面。

步驟

1. 使用切換至進階權限層級 `set -privilege advanced` 命令。
2. 修改SP API服務組態：

如果您想要...	使用下列命令...
變更SP API服務使用的連接埠	`system service-processor api-service modify` 使用 `-port {49152。.65535}` 參數
續約SP API服務用於內部通訊的SSL和SSH憑證	• 適用於 ONTAP 9.5 或更新版本 `system service-processor api-service renew-internal-certificate` • 適用於更新版本的應用ONTAP • `system service-processor api-service renew-certificates` 如果未指定參數、則只會更新主機憑證（包括用戶端和伺服器憑證）。 如果是 `-renew-all true` 指定參數時、主機憑證和根 CA 憑證都會更新。
通訊	
停用或重新啟用SP API服務	`system service-processor api-service modify` 使用 `-is-enabled {true`

3. 使用顯示 SP API 服務組態 `system service-processor api-service show` 命令。

使用 SP/BMC 遠端管理節點

使用 **SP / BMC** 遠端管理 **ONTAP** 節點

您可以使用內建的控制器（稱為服務處理器（SP）或基礎板管理控制器（BMC）、從遠端管理節點。此遠端管理控制器包含在所有目前的平台機型中。無論節點的作業狀態為何、控制器都能維持正常運作。

如需平台 SP 和 BMC 支援的完整詳細說明，請參閱 "支援對照表"NetApp 支援網站上的。

服務處理器（SP）是遠端管理裝置、可讓您從遠端存取、監控及疑難排解節點。

SP的主要功能包括：

- SP可讓您從遠端存取節點、以診斷、關機、重新開機或重新開機節點、無論節點控制器的狀態為何。

  SP由待命電壓供電、只要節點至少有一個電源供應器有輸入電力、就能使用此電壓。

  您可以從管理主機使用Secure Shell用戶端應用程式登入SP。然後、您可以使用SP CLI遠端監控節點並進行疑難排解。此外、您也可以使用SP存取序列主控台、ONTAP 並從遠端執行各種指令。

  您可以從序列主控台存取SP、或從SP存取序列主控台。SP可讓您同時開啟SP CLI工作階段和獨立的主控台工作階段。

  例如、當溫度感測器嚴重偏高或偏低時ONTAP 、會觸發SP正常關閉主機板。序列主控台沒有回應、但您仍可在主控台按Ctrl-G存取SP CLI。然後您就可以使用 `system power on` 或 `system power cycle` 從 SP 啟動或重新啟動節點的命令。

- SP會監控環境感測器並記錄事件、協助您及時採取有效的服務行動。

  SP會監控環境感測器、例如節點溫度、電壓、電流和風扇速度。當環境感測器達到異常狀況時、SP會記錄異常讀數、通知ONTAP 問題、並透過AutoSupport 消息傳送必要的警示和「自有系統」通知、無論節點是否能傳送AutoSupport 不正常訊息。

  SP也會記錄開機進度、現場可更換單元（FRU）變更、ONTAP 由支援中心產生的事件、以及SP命令記錄等事件。您可以手動叫用AutoSupport 一個消息、以包含從指定節點收集的SP記錄檔。

  除了代表當機節點產生這些訊息、並將額外的診斷資訊附加到AutoSupport 消息中之外、SP也不會影響AutoSupport 到功能性。此功能會從無法恢復的功能中繼承整個功能。AutoSupport ONTAP

  > SP 不依賴 `-transport` 的參數設定 `system node autosupport modify` 傳送通知的命令。SP僅使用簡易郵件傳輸傳輸傳輸傳輸傳輸傳輸協定（Simple Mail Transport Protocol、簡稱SMTP）、並要求主機AutoSupport 的整套組態包含郵件主機資訊。

  如果啟用SNMP、SP會針對所有「自訂系統」事件、產生SNMP設陷主機的SNMP設陷。

- SP具有非揮發性記憶體緩衝區、可在系統事件記錄（SEel）中儲存多達4、000個事件、協助您診斷問題。

  該系統會將每個稽核記錄項目儲存為稽核事件。儲存在SP的內建快閃記憶體中。SP會透過AutoSupport 一則消息、自動將來自該系統的事件清單傳送給指定的收件者。

  該系統事件日誌包含下列資訊：

  - SP偵測到的硬體事件、例如電源供應器、電壓或其他元件的感應器狀態
  - SP偵測到的錯誤-例如通訊錯誤、風扇故障或記憶體或CPU錯誤
  - 節點傳送至 SP 的關鍵軟體事件、例如因發行 SP 而發生緊急狀況、通訊故障、開機故障或使用者觸發的「系統」 `system reset` 或 `system power cycle` 命令

- 無論系統管理員是登入或連線至主控台、SP都會監控序列主控台。

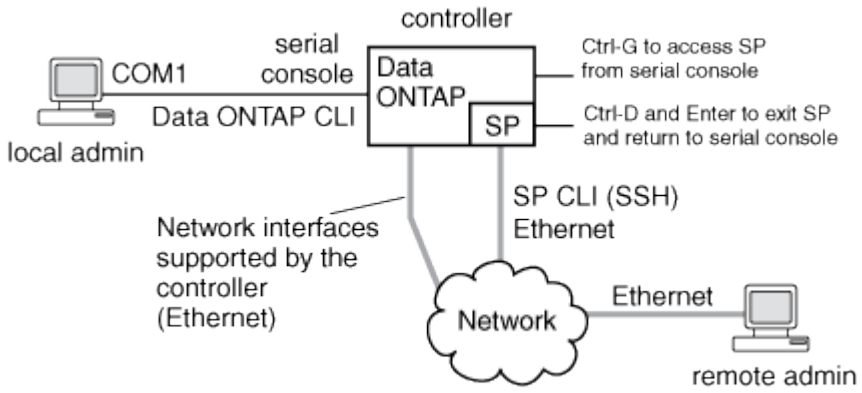
當訊息傳送至主控台時、SP會將訊息儲存在主控台記錄中。只要SP有來自任一節點電源供應器的電力、主控台記錄就會持續存在。由於SP是以待命電源運作、因此即使節點已關機或關機、仍可繼續使用。

- 如果已設定SP、則可使用硬體輔助接管。
- SP API服務可透過ONTAP 網路與SP進行通訊。

  此服務可ONTAP 支援網路型功能、例如使用網路介面進行SP韌體更新、讓節點存取另一個節點的SP功能或系統主控台、以及從另一個節點上傳SP記錄、藉此強化SP的支援功能。

  您可以變更服務使用的連接埠、續訂服務用於內部通訊的SSL和SSH憑證、或完全停用服務、藉此修改SP API服務的組態。

下圖說明ONTAP 如何存取節點的ENetApp和SP。SP介面可透過乙太網路連接埠存取（以機箱背面的扳手圖示表示）：



使用 **ONTAP** 基礎板管理控制器來遠端管理節點

在某些硬體平台上，會自訂軟體以支援基礎板管理控制器（ BMC ）中的新內建控制器。BMC具有命令列介面（CLI）命令、可用於遠端管理裝置。

BMC的運作方式與服務處理器（SP）類似、並使用許多相同的命令。BMC可讓您執行下列動作：

- 設定BMC網路設定。
- 從遠端存取節點、並執行節點管理工作、例如診斷、關機、關機後再開機或重新開機。

SP與BMC之間有一些差異：

- BMC完全控制電源供應器元件、冷卻元件、溫度感測器、電壓感測器和電流感測器的環境監控。BMC會透過ONTAP IPMI將感測器資訊回報給各個方面。
- 有些高可用度（HA）和儲存命令不同。
- BMC不會傳送AutoSupport 一些不知道的訊息。

運行ONTAP時也可以進行自動韌體更新，但需符合以下要求：

- 必須安裝BMC韌體版本1.15或更新版本。

需要手動更新、才能將BMC韌體從1.12升級至1.15或更新版本。

- BMC會在韌體更新完成後自動重新開機。

在BMC重新開機期間、節點作業不會受到影響。

管理 **ONTAP SP / BMC** 韌體更新

包含一個稱為「*baseline image*」的SP韌體映像。ONTAP如果隨後有新版的SP韌體可供使用、您可以選擇下載該韌體、並將SP韌體更新至下載的版本、而不需升級ONTAP 此版本的更新。

本主題同時適用於SP和BMC。

支援下列管理SP韌體更新的方法：ONTAP

- SP自動更新功能預設為啟用、可在下列情況下自動更新SP韌體：
  - 當您升級ONTAP 至新版的更新版本時

    只要與之搭售的SP韌體版本比節點上執行的SP版本更新、即可自動包含SP韌體更新程序。ONTAP ONTAP

    ONTAP偵測到失敗的SP自動更新並觸發糾正措施以重試SP自動更新最多三次。如果三次重試都失敗，請參閱"NetApp知識庫：健康監視器 SPAutoUpgradeFailedMajorAlert SP升級失敗 - AutoSupport訊息"。
  - 當您從 NetApp 支援網站下載 SP 韌體版本，且下載的版本比目前執行的 SP 版本新時
  - 當您降級ONTAP 或回復至舊版的版本時

    SP韌體會自動更新為ONTAP 支援的最新相容版本、由還原或降級至的版本支援。不需要手動更新SP韌體。

  您可以選擇使用停用 SP 自動更新功能 `system service-processor image modify` 命令。不過、建議您保留啟用此功能的狀態。停用此功能可能會導致ONTAP 不佳或不合格的結合、使不佳的影像與SP韌體映像無法搭配使用。

- ONTAP 可讓您手動觸發 SP 更新、並使用指定更新的執行方式 `system service-processor image update` 命令。

  您可以指定下列選項：
  - 要使用的 SP 韌體套件 (`-package`)

    您可以指定套件檔案名稱、將SP韌體更新至下載的套件。進步 `system image package show` 命令會顯示節點上可用的所有套件檔案（包括 SP 韌體套件的檔案）。
  - 是否使用基礎 SP 韌體套件進行 SP 更新 (`-baseline`)

您可以將SP韌體更新至目前執行版本ONTAP 的BIOS所隨附的基礎版本。

如果您使用一些更進階的更新選項或參數、則BMC的組態設定可能會暫時清除。重新開機後ONTAP 、恢復BMC組態最多可能需要10分鐘。

- ONTAP 可讓您使用顯示從 ONTAP 觸發的最新 SP 韌體更新狀態 `system service-processor image update-progress show` 命令。

更新SP韌體時、任何現有的SP連線都會終止。無論是自動或手動觸發SP韌體更新、都會發生這種情況。

相關資訊

"NetApp下載：系統韌體與診斷"

韌體更新使用的 **ONTAP SP / BMC** 和網路介面

在ONTAP 執行1.5、2.5、3.1或更新版本的SP上、從支援使用IP型檔案傳輸機制的支援下、從支援使用支援服務的SP韌體更新。

本主題同時適用於SP和BMC。

透過網路介面進行SP韌體更新的速度比透過序列介面進行更新的速度快。如此可縮短更新SP韌體的維護時間、也不會中斷ONTAP 運作。支援此功能的SP版本隨ONTAP 附於支援此功能的更新版本。它們也可在 NetApp 支援網站上取得，並可安裝於正在執行相容版本 ONTAP 的控制器上。

執行SP 1.5、2.5、3.1或更新版本時、適用下列韌體升級行為：

- 由現象自動觸發的SP韌體更新ONTAP 預設為使用網路介面進行更新；不過、如果發生下列其中一種情況、SP自動更新會切換為使用序列介面進行韌體更新：
  - SP網路介面未設定或無法使用。
  - IP型檔案傳輸失敗。
  - SP API服務已停用。

無論您執行的SP版本為何、從SP CLI觸發的SP韌體更新都會使用SP網路介面進行更新。

相關資訊

"NetApp下載：系統韌體與診斷"

使用叢集使用者帳戶存取 **ONTAP** 服務處理器

當您嘗試存取SP時、系統會提示您提供認證資料。使用建立的叢集使用者帳戶 `service-processor` 應用程式類型可存取叢集任何節點上的 SP CLI 。SP使用者帳戶是從ONTAP無法驗證的地方管理、並由密碼驗證。從 ONTAP 9.9.1 開始、 SP 使用者帳戶必須具有 `admin` 角色：

存取SP的使用者帳戶是透過ONTAP 不使用SP CLI的功能來管理、叢集使用者帳戶如果是使用建立 SP 、則可以存取 SP `-application` 的參數 `security login create` 命令設為 `service-processor` 和 `-authmethod` 參數設為 `password`。SP僅支援密碼驗證。

您必須指定 `-role` 建立 SP 使用者帳戶時的參數。

- 在 ONTAP 9.9.1 及更新版本中、您必須指定 `admin` 適用於 `-role` 參數、以及帳戶的任何修改都需要 `admin` 角色：基於安全考量、不再允許其他角色。
  - 如果您要升級ONTAP 至版本不含更新版本的版本、請參閱 "可存取服務處理器的使用者帳戶變更"。
  - 如果您要回復ONTAP 到版本不含更新版本的版本、請參閱 "驗證可存取服務處理器的使用者帳戶"。
- 在 ONTAP 9.8 和更早版本中、任何角色都可以存取 SP 、但是 `admin` 建議使用。

依預設、名為「 admin 」的叢集使用者帳戶會包含 `service-processor` 應用程式類型、並可存取 SP 。

無法使用保留給系統的名稱（例如「root」和「naroot」）建立使用者帳戶。ONTAP您無法使用系統保留名稱來存取叢集或SP。

您可以使用顯示目前的 SP 使用者帳戶 `-application service-processor` 的參數 `security login show` 命令。

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

從管理主機存取節點的 **ONTAP SP / BMC**

您可以從管理主機登入節點的SP、以從遠端執行節點管理工作。

開始之前

必須符合下列條件：

- 用於存取SP的管理主機必須支援SSHv2。
- 您的使用者帳戶必須已設定、才能存取SP。

  若要存取 SP 、您的使用者帳戶必須已使用建立 `-application` 的參數 `security login create` 命令設為 `service-processor` 和 `-authmethod` 參數設為 `password`。

此工作同時適用於SP和BMC。

如果SP設定為使用IPv4或IPv6位址、而且如果在10分鐘內有五次主機的SSH登入嘗試連續失敗、SP會拒絕SSH登入要求、並暫停與主機IP位址的通訊15分鐘。通訊會在15分鐘後恢復、您可以再次嘗試登入SP。

無法建立或使用系統保留名稱（例如「root」和「naroot」）來存取叢集或SP。ONTAP

步驟

1. 從管理主機登入SP：

   `ssh username@SP_IP_address`

2. 當系統提示您時、請輸入的密碼 `username`。

   出現SP提示字元、表示您可以存取SP CLI。

從管理主機存取**SP**的範例

以下範例說明如何使用使用者帳戶登入 SP `joe`，已設定為存取 SP 。

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

下列範例說明如何使用IPv6全域位址或IPv6路由器通告位址、在已針對IPv6設定SSH、並針對IPv6設定SP的節點上登入SP。

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

從系統主控台存取節點的 **ONTAP SP / BMC**

您可以從系統主控台（也稱為_serial Console）存取SP、以執行監控或疑難排解工作。

關於這項工作

此工作同時適用於SP和BMC。

步驟

1. 在系統主控台存取SP CLI時、請在提示字元中按Ctrl-G。
2. 出現提示時、請登入SP CLI。

   出現SP提示字元、表示您可以存取SP CLI。

3. 結束SP CLI並按Ctrl-D返回系統主控台、然後按Enter。

從系統主控台存取**SP CLI**的範例

以下範例顯示從系統主控台按Ctrl-G存取SP CLI的結果。。 `help system power` 在 SP 提示字元中輸入命令、然後按 Ctrl-D 、再按 Enter 返回系統主控台。

```
cluster1::>
```

（按Ctrl-G存取SP CLI。）

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

（按Ctrl-D、然後按Enter返回系統主控台。）

```
cluster1::>
```

瞭解 **ONTAP SP CLI** ， **SP** 主控台和系統主控台工作階段的關聯性

您可以開啟SP CLI工作階段、從遠端管理節點、並開啟個別的SP主控台工作階段、以存取節點的主控台。SP主控台工作階段會鏡射並行系統主控台工作階段中顯示的輸出。SP和系統主控台具有獨立的Shell環境、並具有獨立的登入驗證。

瞭解SP CLI、SP主控台及系統主控台工作階段的相關資訊、可協助您從遠端管理節點。以下說明工作階段之間的關係：

- 一次只能有一位管理員登入SP CLI工作階段、不過SP可讓您同時開啟SP CLI工作階段和另一個SP主控台工作階段。

  SP CLI 會顯示 SP 提示字元 (`SP>`) 。從 SP CLI 工作階段、您可以使用 SP `system console` 啟動 SP 主控台工作階段的命令。同時、您也可以透過SSH啟動個別的SP CLI工作階段。如果按Ctrl-D退出SP主控台工作階段、則會自動返回SP CLI工作階段。如果SP CLI工作階段已經存在、會出現訊息詢問您是否要終止現有的SP CLI工作階段。如果輸入「y」、現有的SP CLI工作階段將會終止、讓您從SP主控台返回SP CLI。此動作會記錄在SP事件記錄中。

  在透過 SSH 連線的 ONTAP CLI 工作階段中、您可以執行 ONTAP 來切換至節點的系統主控台 `system node run-console` 來自另一個節點的命令。

- 基於安全考量、SP CLI工作階段和系統主控台工作階段具有獨立的登入驗證。

  當您從 SP CLI 啟動 SP 主控台工作階段時（使用 SP `system console` 命令）、系統會提示您輸入系統主控台認證。從系統主控台工作階段（按Ctrl-G）存取SP CLI時、系統會提示您輸入SP CLI認證。

- SP主控台工作階段和系統主控台工作階段具有獨立的Shell環境。

  SP主控台工作階段會鏡射並行系統主控台工作階段中顯示的輸出。但是、並行系統主控台工作階段不會鏡射SP主控台工作階段。

  SP主控台工作階段不會鏡射並行SSH工作階段的輸出。

依預設、SP會接受來自任何IP位址管理主機的SSH連線要求。您可以將SP設定為僅接受來自您指定IP位址之管理主機的SSH連線要求。您所做的變更會套用至叢集中任何節點的SP存取SSH。

步驟

1. 僅將 SP 存取權授予您使用指定的 IP 位址 `system service-processor ssh add-allowed-addresses` 命令 `-allowed-addresses` 參數。

   - 的值 `-allowed-addresses` 參數必須以的格式指定 `address/netmask`和多個 `address/netmask` 配對必須以逗號分隔、例如 `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`。

     設定 `-allowed-addresses` 參數至 `0.0.0.0/0, ::/0` 啟用所有 IP 位址以存取 SP （預設）。

   - 當您只將 SP 存取限制為指定的 IP 位址來變更預設值時、 ONTAP 會提示您確認是否要指定的 IP 位址取代「允許所有」的預設設定 (`0.0.0.0/0, ::/0`）。

   - 。 `system service-processor ssh show` 命令會顯示可存取 SP 的 IP 位址。

2. 如果您要封鎖指定的 IP 位址、使其無法存取 SP 、請使用 `system service-processor ssh remove-allowed-addresses` 命令 `-allowed-addresses` 參數。

   如果您封鎖所有IP位址、使其無法從任何管理主機存取SP。

管理可存取**SP**的**IP**位址範例

下列範例顯示SSH存取SP的預設設定、將SP存取限制為僅指定IP位址、從存取清單中移除指定的IP位址、然後還原所有IP位址的SP存取：

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```

在 **ONTAP SP / BMC CLI** 中檢視說明資訊

線上說明會顯示SP/BMC CLI命令和選項。

關於這項工作

此工作同時適用於SP和BMC。

步驟

1. 若要顯示SP/BMC命令的說明資訊、請輸入下列命令：

若要存取**SP**說明...	若要存取 **BMC** 說明 ...
類型 `help` 在 SP 提示符下。	類型 `system` 在 BMC 提示下。

以下範例顯示SP CLI線上說明。

```
SP> help
date - print date and time
exit - exit from the SP command line interface
events - print system events and event information
help - print command help
priv - show and set user mode
sp - commands to control the SP
system - commands to control the system
version - print SP version
```

以下範例顯示 BMC CLI 線上說明。

```
BMC> system
system acp - acp related commands
system battery - battery related commands
system console - connect to the system console
system core - dump the system core and reset
system cpld - cpld commands
system log - print system console logs
system power - commands controlling system power
system reset - reset the system using the selected firmware
system sensors - print environmental sensors status
system service-event - print service-event status
system fru - fru related commands
system watchdog - system watchdog commands

BMC>
```

2. 若要顯示 SP/BMC 命令選項的說明資訊、請輸入 `help` 在 SP/BMC 命令之前或之後。

   以下範例顯示 SP 的 SP CLI 線上說明 `events` 命令。

```
SP> help events
events all - print all system events
events info - print system event log information
events newest - print newest system events
events oldest - print oldest system events
events search - search for and print system events
```

以下範例顯示 BMC 的 BMC CLI 線上說明 `system power` 命令。

```
BMC> system power help
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status

BMC>
```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "活動"
- "系統電源"

用於遠端節點管理的 **ONTAP** 命令

您可以透過存取其SP並執行SP CLI 命令，或存取BMC並執行BMC CLI 命令來遠端執行節點管理任務。對於幾個常見的遠端節點管理任務，您也可以從叢集中的另一個節點使用ONTAP命令。某些SP和BMC指令是特定於平台的，可能在您的平台上不可用。

某些指令類型可以在SP和BMC指令集中使用。當輸入命令列時就會顯示它們之間的差異。

範例

- 這 `help`SP中的指令： `SP> help`
- 這 `help`BMC中的指令： `BMC> help`

詳細了解 `help`可用於SP和BMC 的指令選項"在 ONTAP SP / BMC CLI 中檢視說明資訊"。

了解有關相應ONTAP BMC CLI 的更多信息"ONTAP 基礎板管理控制器支援的 CLI 命令"。

如果您想要...	使用此**SP**命令...	使用此 **BMC** 命令 ...	使用此**ONTAP**指令...
顯示SP/ BMC/ ONTAP的可用指令或指定指令的子指令	`help [command]`	`help [command]`	不適用

如果您想要...	使用此SP命令...	使用此 BMC 命令 ...	使用此ONTAP指令...
顯示SP/ BMC/ ONTAP CLI 的目前權限級別	priv show	priv show	不適用
設定權限等級以存取SP/ BMC/ ONTAP CLI 的指定模式	priv set {admin	advanced	diag }
priv set {admin	advanced	diag	test }
不適用	顯示系統日期與時間	date	date
date	顯示SP/ BMC/ ONTAP記錄的事件	events {all	info
newest number	oldest number	search keyword }	events {all
info	newest	oldest	search }
不適用	顯示SP/ BMC/ ONTAP狀態和網路設定資訊	sp status [-v	-d] * 這 `-v`選項以詳細形式顯示SP統計資料。 * 這 `-d`選項將SP偵錯日誌新增至顯示。
bmc status [-v	-d] * 這 `-v`選項以詳細形式顯示SP統計資料。 * 這 `-d`選項將SP偵錯日誌新增至顯示。	system service-processor show	顯示SP/ BMC/ ONTAP啟動的時間長度以及過去1、5 和 15 分鐘內運行佇列中的平均作業數
sp uptime	bmc uptime	不適用	顯示系統主控台記錄
system log	system log [-a]	system log （列印系統控制台日誌）	顯示SP/ BMC/ ONTAP日誌檔案或檔案中的文件
sp log history show [-archive {latest	{all	archive-name }][-dump {all	file-name }]

如果您想要...	使用此SP命令...	使用此 BMC 命令 ...	使用此ONTAP指令...

`bmc log history show`
 	
`[-archive {latest`
	`{all`	`archive-name }][-dump {all`	`file-name }]`

不適用	顯示節點控制器的電源狀態	`system power status`	`system power status`
`system node power show`	顯示電池資訊	`system battery show`	`system battery show`

不適用	顯示ACP資訊或擴充器感測器的狀態	`system acp`
		
		`[show`
			`sensors show ]`

不適用	不適用	列出所有系統FRU及其ID	`system fru list`
`system fru list`	不適用	顯示指定FRU的產品資訊	`system fru show fru_id`

`system fru show`
 	
`[ show <id> ]`
	不適用	顯示FRU資料歷程記錄	`system fru log show`
			
			（進階權限層級）

`system fru log show`	不適用	顯示環境感測器的狀態、包括其狀態和目前值	`system sensors`
			
			或
			
			`system sensors show`

`system sensors`
 	
`{show`
	`filter <sensor_string> }`	`system node environment sensors show`	顯示指定感測器的狀態和詳細資料

`system sensors get sensor_name`
 	
您可以取得 `sensor_name` 使用 `system sensors` 或 `system sensors show` 命令。
	`system sensors`
	
	`[ get ]`
		不適用	顯示SP/ BMC/ ONTAP韌體版本信息

如果您想要...	使用此SP命令...	使用此 BMC 命令 ...	使用此ONTAP指令...
`version`	`version`	`system service-processor image show`	顯示SP/ BMC/ ONTAP指令歷史記錄
`sp log audit` （進階權限層級）	`bmc log audit` （進階權限層級）	不適用	顯示SP/ BMC/ ONTAP調試訊息
`sp log debug` （進階權限層級）	`bmc log debug` （進階權限層級）	不適用	顯示SP/ BMC/ ONTAP訊息文件
`sp log messages` （進階權限層級）	`bmc log messages` （進階權限層級）	不適用	顯示在監視器重設事件上收集系統鑑識的設定、顯示在監視器重設事件期間收集的系統鑑識資訊、或清除收集的系統鑑識資訊
`system forensics` [show	`log dump`	`log clear`]	不適用
不適用	登入系統主控台	`system console`	`system console`
`system node run-console`	您應該按Ctrl-D結束系統主控台工作階段。	開啟或關閉節點、或執行電源循環（關閉電源然後重新開啟）	`system power on`
`system power on`	`system node power on` （進階權限層級）	`system power off`	`system power off`
不適用	`system power cycle`	`system power cycle`	不適用

如果您想要...	使用此SP命令...	使用此 BMC 命令 ...	使用此ONTAP指令...
待機電源會持續開啟、讓SP不中斷運作。在關機後再開機之前、會短暫暫停。 使用這些命令來關閉或重新啟動節點、可能會導致節點關機不正確（也稱為 _ 不正常關機 _ ）、無法取代使用 ONTAP 的正常關機 `system node halt` 命令。	建立核心傾印並重設節點	`system core [-f]` 。 `-f` 選項會強制建立核心傾印並重設節點。	`system core`
`system node coredump trigger` （進階權限層級）	這些命令的作用與按下節點上的「不可遮罩的中斷」（NMI）按鈕相同、導致節點不正常關機、並在停止節點時強制傾印核心檔案。當節點上的 ONTAP 掛起或不回應命令時、這些命令很有用、例如 `system node shutdown`。產生的核心傾印檔案會顯示在的輸出中 `system node coredump show` 命令。只要節點的輸入電源不中斷、SP就會維持運作。	使用選擇性指定的BIOS韌體映像（主要、備份或目前）重新開機節點、以從節點開機裝置的毀損映像等問題中恢復	`system reset` {primary
backup	current }	`system reset` { current	primary
backup }	`system node reset` 與 `-firmware {primary`	backup	current } 範圍 （進階權限層級）

如果您想要...	使用此SP命令...	使用此 BMC 命令 ...	使用此ONTAP指令...
此作業會導致節點不正常關機。 如果未指定BIOS韌體映像、則會使用目前映像進行重新開機。只要節點的輸入電源不中斷、SP就會維持運作。	將目前的電池韌體映像與指定的韌體映像進行比較	`system battery verify [image_URL]` （進階權限層級） 如果 `image_URL` 未指定、則會使用預設電池韌體映像進行比較。	`system battery verify [image_URL]` （進階權限層級） 如果 `image_URL` 未指定、則會使用預設電池韌體映像進行比較。
不適用	從指定位置的映像更新電池韌體	`system battery flash [image_URL]` （進階權限層級） 如果自動電池韌體升級程序因故失敗、請使用此命令。	不適用

不適用	使用指定位置的映像更新SP/ BMC/ ONTAP韌體	`sp update`
		
		`image_URL`
		
		`image_URL`不得超過200 個字元。
			`bmc update`
			
			`image_URL`
			
			`image_URL`不得超過200 個字元。

`system service-processor image update`	重新啟動SP/ BMC/ ONTAP	`sp reboot`	`bmc reboot`
`system service-processor reboot-sp`	清除NVRAM Flash內容	`system nvram flash clear` （進階權限層級） 當控制器電源關閉時、無法啟動此命令 (`system power off`) 。	不適用
不適用	退出SP/ BMC/ ONTAP CLI	`exit`	`exit`

相關資訊

- "指令參考資料ONTAP"

臨界值型感應器會定期讀取各種系統元件的讀數。SP會將臨界值型感應器的讀取值與預設臨界值限制進行比較、以定義元件的可接受作業條件。

根據感測器的讀取值、SP會顯示感測器狀態、以協助您監控元件的狀況。

臨界值型感測器的範例包括系統溫度、電壓、電流和風扇速度的感測器。臨界值型感應器的特定清單取決於平台。

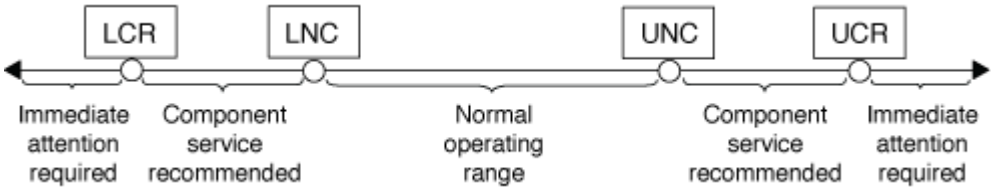
臨界值型感應器的臨界值如下、顯示在 SP 的輸出中 `system sensors` 命令：

- 臨界下限（LCR）
- 非臨界下限（LNC）
- 上非關鍵（UNc）
- 臨界上限（UCR）

LNC和LCR之間或在UNC和UCR之間的感測器讀取表示元件出現問題的徵兆、因此可能會發生系統故障。因此、您應該儘快規劃元件服務。

低於LCR或高於UCR的感測器讀取值表示元件故障、系統即將發生故障。因此、元件需要立即注意。

下圖說明臨界值所指定的嚴重性範圍：



您可以在下找到臨界值型感應器的讀數 `Current` 中的欄 `system sensors` 命令輸出。。 `system sensors get sensor_name` 命令會顯示指定感測器的其他詳細資料。當臨界值型感應器的讀取值超過非臨界臨界臨界臨界臨界臨界臨界臨界臨界臨界臨界臨界值範圍時、感應器會報告嚴重性增加的問題。當讀取超過臨界值限制時、表示感應器在中的狀態 `system sensors` 命令輸出會從變更 `ok` 至 `nc` （非關鍵）或 `cr` （嚴重）視超過的臨界值而定、事件訊息會記錄在 SEL 事件記錄中。

某些臨界值型感應器並未全部達到四個臨界值層級。對於這些感測器、會顯示遺失的臨界值 `na` 成為他們在中的極限 `system sensors` 命令輸出、表示特定感測器對於指定臨界值沒有限制或嚴重性考量、而 SP 則不會監控該臨界值的感測器。

系統感測器命令輸出範例

下列範例顯示所顯示的部分資訊 `system sensors` SP CLI 中的命令：

```
SP node1> system sensors

Sensor Name       | Current    | Unit        | Status| LCR        | LNC
| UNC        | UCR
------------------+------------+-------------+-------+------------+
-----------+-----------+-----------
CPU0_Temp_Margin | -55.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
CPU1_Temp_Margin | -56.000    | degrees C   | ok    | na         | na
| -5.000     | 0.000
In_Flow_Temp      | 32.000     | degrees C   | ok    | 0.000      | 10.000
| 42.000     | 52.000
Out_Flow_Temp     | 38.000     | degrees C   | ok    | 0.000      | 10.000
| 59.000     | 68.000
CPU1_Error        | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Therm_Trip   | 0x0        | discrete    | 0x0180| na         | na
| na         | na
CPU1_Hot          | 0x0        | discrete    | 0x0180| na         | na
| na         | na
IO_Mid1_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
IO_Mid2_Temp      | 30.000     | degrees C   | ok    | 0.000      | 10.000
| 55.000     | 64.000
CPU_VTT           | 1.106      | Volts       | ok    | 1.028      | 1.048
| 1.154      | 1.174
CPU0_VCC          | 1.154      | Volts       | ok    | 0.834      | 0.844
| 1.348      | 1.368
3.3V              | 3.323      | Volts       | ok    | 3.053      | 3.116
| 3.466      | 3.546
5V                | 5.002      | Volts       | ok    | 4.368      | 4.465
| 5.490      | 5.636
STBY_1.8V         | 1.794      | Volts       | ok    | 1.678      | 1.707
| 1.892      | 1.911
…
```

臨界值型感測器的系統感測器 **SENSOR_NAME** 命令輸出範例

以下範例顯示輸入的結果 `system sensors get sensor_name` 在 SP CLI 中、用於臨界值型感應器 5V ：

```
SP node1> system sensors get 5V

Locating sensor record...
Sensor ID               : 5V (0x13)
 Entity ID              : 7.97
 Sensor Type (Analog)   : Voltage
 Sensor Reading         : 5.002 (+/- 0) Volts
 Status                 : ok
 Lower Non-Recoverable  : na
 Lower Critical         : 4.246
 Lower Non-Critical     : 4.490
 Upper Non-Critical     : 5.490
 Upper Critical         : 5.758
 Upper Non-Recoverable  : na
 Assertion Events       :
 Assertions Enabled     : lnc- lcr- ucr+
 Deassertions Enabled   : lnc- lcr- ucr+
```

系統感測器命令輸出中的 **ONTAP SP** 感測器狀態值

獨立感測器沒有臨界值。其讀數會顯示在下 `Current` SP CLI 中的列 `system sensors` 命令輸出，不帶有實際意義，因此 SP 將忽略該命令輸出。。 `Status` 中的欄 `system sensors` 命令輸出會以十六進位格式顯示離散感測器的狀態值。

獨立感測器的範例包括風扇、電源供應器（PSU）故障和系統故障的感測器。獨立感測器的特定清單取決於平台。

您可以使用 SP CLI `system sensors get sensor_name` 命令以協助解讀大多數離散感測器的狀態值。下列範例顯示輸入的結果 `system sensors get sensor_name` 對於離散感測器 CPU0_Error 和 IO_Slot1_Present ：

```
SP node1> system sensors get CPU0_Error
Locating sensor record...
Sensor ID               : CPU0_Error (0x67)
 Entity ID              : 7.97
 Sensor Type (Discrete): Temperature
 States Asserted        : Digital State
                          [State Deasserted]
```

```
SP node1> system sensors get IO_Slot1_Present
Locating sensor record...
Sensor ID              : IO_Slot1_Present (0x74)
 Entity ID             : 11.97
 Sensor Type (Discrete): Add-in Card
 States Asserted       : Availability State
                         [Device Present]
```

儘管如此 `system sensors get sensor_name` 命令會顯示大多數離散感測器的狀態資訊、但不會提供 System_FW_Status 、 System_Watchdog 、 PSU1_Input_Type 和 PSU2_Input_Type 等獨立感測器的狀態資訊。您可以使用下列資訊來解譯這些感測器的狀態值。

System_FW_Status

System_FW_Status 感測器的狀況以形式出現 `0xAABB`。您可以合併的資訊 `AA` 和 `BB` 以判斷感測器的狀況。

`AA` 可以有下列其中一個值：

價值	感測器的狀況
01	系統韌體錯誤
02	系統韌體當機
04	系統韌體進度

`BB` 可以有下列其中一個值：

價值	感測器的狀況
00	系統軟體已正常關機
01	正在初始化記憶體
02	正在進行NVMEM初始化（當有NVMEM時）
04	還原記憶體控制器集線器（MCH）值（若有NVMEM）
05	使用者已進入設定
13.	開機作業系統或載入程式
1F	BIOS正在啟動

價值	感測器的狀況
20.	載入程式正在執行中
21.	載入程式正在設定主要BIOS韌體。您不得關閉系統電源。
22	載入程式正在程式設定替代的BIOS韌體。您不得關閉系統電源。
2F	執行中ONTAP
60	SP已關閉系統電源
61.	SP已開啟系統電源
62.	SP已重設系統
63.	SP Watchdog關機週期
64	SP Watchdog冷重設

例如、System_FW_Status sensor Status 0x042F表示「系統韌體進度（04）、ONTAP 而不執行更新（2F）」。

System_Watchdog

System_Watchdog感應器可能有下列其中一種情況：

- * 0X0080*

  此感測器的狀態尚未變更

價值	感測器的狀況
0X0081	定時器中斷
0180	定時器已過期
0280	硬重設
0480	關機
0X0880	關機再開機

例如、System_Watchdog感應器狀態為0x0880、表示發生監督逾時、並導致系統關機後再開機。

PSU1_INU_Type和PSU2_INUD_Type

若為直流電（DC）電源供應器、則不適用PSU1_INU_Type和PSU2_INPART_Type感測器。對於交流（AC）電源供應器、感測器的狀態可以有下列其中一個值：

價值	感測器的狀況
0X01 xx	220V PSU類型
0x02 xx	110 V PSU類型

例如、PSU1_Input_Type感測器狀態為0x0280、表示感測器回報PSU類型為110V。

用於服務處理器管理的 **ONTAP** 命令

支援支援的指令可用於管理SP、包括SP網路組態、SP韌體映像、SSH存取SP、以及一般SP管理。ONTAP

用於管理**SP**網路組態的命令

如果您想要...	執行**ONTAP** 此指令...
啟用SP的SP自動網路組態、讓SP使用指定子網路的IPv4或IPv6位址系列	`system service-processor network auto-configuration enable`
停用SP所指定之子網路的IPv4或IPv6位址系列的SP自動網路組態	`system service-processor network auto-configuration disable`
顯示 SP 自動網路組態	`system service-processor network auto-configuration show`
手動設定節點的SP網路、包括： • IP位址系列（IPV4或IPV6） • 是否應啟用指定IP位址系列的網路介面 • 如果您使用的是IPV4、則是使用DHCP伺服器的網路組態、還是使用您指定的網路位址 • SP的公有IP位址 • SP的網路遮罩（如果使用的是IPV4） • SP子網路遮罩的網路字首長度（如果使用IPv6） • SP的閘道IP位址	`system service-processor network modify`

如果您想要...	執行ONTAP 此指令...
顯示SP網路組態、包括： • 已設定的位址系列（IPv4或IPv6）、以及是否已啟用 • 遠端管理裝置類型 • 目前的SP狀態和連結狀態 • 網路組態、例如IP位址、MAC位址、網路遮罩、子網路遮罩的字首長度、路由器指派的IP位址、連結本機IP位址和閘道IP位址 • 上次更新SP的時間 • 用於SP自動組態的子網路名稱 • 是否啟用IPv6路由器指派的IP位址 • SP網路設定狀態 • SP網路設定失敗的原因	`system service-processor network show` 若要顯示完整的 SP 網路詳細資料、必須使用 `-instance` 參數。
修改SP API服務組態、包括： • 變更SP API服務使用的連接埠 • 啟用或停用SP API服務	`system service-processor api-service modify` （進階權限層級）
顯示SP API服務組態	`system service-processor api-service show` （進階權限層級）
續約SP API服務用於內部通訊的SSL和SSH憑證	• ONTAP 9.5 或更新版本： `system service-processor api-service renew-internal-certificates` • ONTAP 9.4 或更早版本： `system service-processor api-service renew-certificates` （進階權限層級）

管理**SP**韌體映像的命令

如果您想要...	執行**ONTAP** 此指令...
顯示目前安裝的SP韌體映像詳細資料、包括： • 遠端管理裝置類型 • 從SP開機的映像（主要或備份）、其狀態和韌體版本 • 韌體自動更新是否已啟用、以及上次更新狀態	`system service-processor image show` 。 `-is-current` 參數表示 SP 目前從其開機的映像（主要或備份）、而非安裝的韌體版本最新。
啟用或停用SP自動韌體更新	`system service-processor image modify` 根據預設、當ONTAP 手動下載新版SP韌體時、SP韌體會自動更新以更新版本的功能。不建議停用自動更新、因為這樣做可能會導致ONTAP 不理想或不合格的結合、使整個過程不符合理想的要求。
在節點上手動下載SP韌體映像	`system node image get` 在您執行之前 `system node image` 命令時、您必須將權限等級設為進階（`set -privilege advanced`）、當系統提示您繼續時輸入 * y* 。 SP韌體映像是隨ONTAP 附於Image.您不需要手動下載SP韌體、除非您想要使用不同於ONTAP 隨附的SP韌體版本。
顯示ONTAP 從功能性更新中觸發的最新SP韌體更新狀態、包括下列資訊： • 最新SP韌體更新的開始和結束時間 • 是否正在進行更新、以及完成的百分比	`system service-processor image update-progress show`

管理**SSH**存取**SP**的命令

如果您想要...	執行**ONTAP** 此指令...
僅將SP存取權授予指定的IP位址	`system service-processor ssh add-allowed-addresses`
封鎖指定的IP位址、使其無法存取SP	`system service-processor ssh remove-allowed-addresses`
顯示可存取SP的IP位址	`system service-processor ssh show`

如果您想要...	執行ONTAP 此指令...
顯示一般SP資訊、包括： • 遠端管理裝置類型 • 目前的SP狀態 • 是否已設定SP網路 • 網路資訊、例如公有IP位址和MAC位址 • SP韌體版本和智慧型平台管理介面（IPMI）版本 • 是否已啟用SP韌體自動更新	`system service-processor show` 若要顯示完整的 SP 資訊、必須使用 `-instance` 參數。
在節點上重新啟動SP	`system service-processor reboot-sp`
產生AutoSupport 並傳送包含從指定節點收集的SP記錄檔的資訊	`system node autosupport invoke-splog`
顯示叢集中所收集SP記錄檔的分配對應、包括位於每個收集節點的SP記錄檔順序編號	`system service-processor log show-allocations`

相關資訊

"指令參考資料ONTAP"

BMC管理的支援指令ONTAP

基礎板管理控制器（BMC）支援這些ONTAP 指令。

BMC使用與服務處理器（SP）相同的一些命令。BMC支援下列SP命令。

如果您想要...	使用此命令
顯示BMC資訊	**`system service-processor show`**
顯示/修改BMC網路組態	**`system service-processor network show/modify`**
重設BMC	**`system service-processor reboot-sp`**
顯示/修改目前安裝的BMC韌體映像詳細資料	**`system service-processor image show/modify`**
更新BMC韌體	**`system service-processor image update`**

如果您想要...	使用此命令
顯示最新BMC韌體更新的狀態	**system service-processor image update-progress show**
啟用BMC的自動網路組態、以便在指定的子網路上使用IPv4或IPv6位址	**system service-processor network auto-configuration enable**
停用針對指定給BMC的子網路之IPv6位址的自動網路組態	**system service-processor network auto-configuration disable**
顯示BMC自動網路組態	**system service-processor network auto-configuration show**

對於BMC韌體不支援的命令、會傳回下列錯誤訊息。

```
::> Error: Command not supported on this platform.
```

相關資訊

- "系統服務處理器"

ONTAP 基礎板管理控制器支援的 **CLI** 命令

您可以使用SSH登入BMC。BMC命令列支援下列命令。

命令	功能
系統	顯示所有命令的清單。
系統主控台	連線至系統的主控台。使用 `Ctrl+D` 結束工作階段。
系統核心	傾印系統核心並重設。
系統關機週期	關閉系統電源、然後再開啟。
系統關機	關閉系統電源。
系統開機	開啟系統電源。
系統電源狀態	列印系統電源狀態。
系統重設	重設系統。

命令	功能
系統記錄	列印系統主控台記錄
系統FRU顯示[id]	傾印所有/選定的現場可更換單元（FRU）資訊。

管理 ONTAP 叢集時間（僅限叢集管理員）

當叢集時間不準確時、可能會發生問題。雖然利用此功能、您可以手動設定叢集上的時區、日期和時間、但您應該設定網路時間傳輸協定（NTP）伺服器、以同步叢集時間。ONTAP

從使用S25 9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

NTP一律啟用。不過、叢集仍需要進行組態、才能與外部時間來源同步。利用支援功能、您可以透過下列方式管理叢集的NTP組態：ONTAP

- 您最多可以將 10 個外部 NTP 伺服器與叢集建立關聯 (`cluster time-service ntp server create`) 。
  - 為了提供備援和時間服務品質、您應將至少三部外部NTP伺服器與叢集建立關聯。
  - 您可以使用NTP伺服器的IPv4或IPv6位址或完整主機名稱來指定NTP伺服器。
  - 您可以手動指定要使用的NTP版本（v3或v4）。

    根據預設、ONTAP 支援特定外部NTP伺服器的NTP版本會自動選取。

  如果您指定的NTP版本不支援NTP伺服器、則無法進行時間交換。

  - 在進階權限層級、您可以指定與叢集相關聯的外部NTP伺服器、作為修正及調整叢集時間的主要時間來源。
- 您可以顯示與叢集相關聯的 NTP 伺服器 (`cluster time-service ntp server show`) 。
- 您可以修改叢集的 NTP 組態 (`cluster time-service ntp server modify`) 。
- 您可以取消叢集與外部 NTP 伺服器的關聯 (`cluster time-service ntp server delete`) 。
- 在進階權限層級、您可以清除所有外部 NTP 伺服器與叢集的關聯、以重設組態 (`cluster time-service ntp server reset`) 。

加入叢集的節點會自動採用叢集的NTP組態。

除了使用NTP之外、ONTAP 利用此功能、您還可以手動管理叢集時間。當您需要修正錯誤時間時（例如、重新開機後節點的時間已大不正確）、這項功能很有幫助。在這種情況下、您可以指定叢集的大約時間、直到NTP可以與外部時間伺服器同步為止。您手動設定的時間會在叢集中的所有節點上生效。

您可以使用下列方式手動管理叢集時間：

- 您可以設定或修改叢集上的時區、日期和時間 (`cluster date modify`) 。
- 您可以顯示叢集目前的時區、日期和時間設定 (`cluster date show`) 。

工作排程不會調整為手動叢集日期和時間變更。這些工作會根據目前建立工作的叢集時間或最近執行工作的時間來排程執行。因此、如果您手動變更叢集日期或時間、則必須使用 `job show` 和 `job history show` 用於驗證所有排程工作是否已根據您的需求排入佇列並完成的命令。

管理叢集時間的命令

您可以使用 `cluster time-service ntp server` 用於管理叢集 NTP 伺服器的命令。您可以使用 `cluster date` 手動管理叢集時間的命令。

從使用S25 9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

下列命令可讓您管理叢集的NTP伺服器：

如果您想要...	使用此命令...
將叢集與外部NTP伺服器建立關聯、而不進行對稱驗證	`cluster time-service ntp server create -server server_name`
將叢集與外部NTP伺服器建立關聯、使其具有ONTAP可在版次9.5或更新版本中使用的對稱驗證	`cluster time-service ntp server create -server server_ip_address -key-id key_id` 。 `key_id` 必須參考現有的共用金鑰、該金鑰設定為「叢集時間服務 NTP 金鑰」。
啟用現有NTP伺服器的對稱驗證您可以修改現有NTP伺服器、藉由新增所需的金鑰ID來啟用驗證。 提供版本僅適用於S9.5或更新版本ONTAP	`cluster time-service ntp server modify -server server_name -key-id key_id`
停用對稱驗證	`cluster time-service ntp server modify -server server_name -is-authentication -enabled false`
設定共用的NTP金鑰	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共用金鑰是由ID所指。節點和NTP伺服器上的ID、其類型和值必須相同
顯示與叢集相關聯之NTP伺服器的相關資訊	`cluster time-service ntp server show`
修改與叢集相關聯的外部NTP伺服器組態	`cluster time-service ntp server modify`
將NTP伺服器與叢集取消關聯	`cluster time-service ntp server delete`

如果您想要...	使用此命令...
清除所有外部NTP伺服器與叢集的關聯、以重設組態	`cluster time-service ntp server reset` 此命令需要進階權限層級。

下列命令可讓您手動管理叢集時間：

如果您想要...	使用此命令...
設定或修改時區、日期和時間	`cluster date modify`
顯示叢集的時區、日期和時間設定	`cluster date show`

相關資訊

- "顯示叢集日期"
- "叢集日期修改"
- "叢集時間服務 NTP"
- "工作展示"

管理橫幅和MOTD

瞭解 ONTAP 登入橫幅和當日訊息文字

ONTAP 可讓您設定登入橫幅或當日訊息（ MOTD ），將管理資訊傳達給叢集或儲存虛擬機器（ SVM ）的系統管理員和 CLI 使用者。

主控台工作階段（僅限叢集存取）或SSH工作階段（用於叢集或SVM存取）會顯示橫幅、然後提示使用者進行驗證（例如密碼）。例如、您可以使用橫幅向嘗試登入系統的人員顯示以下警告訊息：

```
$ ssh admin@cluster1-01

This system is for authorized users only. Your IP Address has been logged.

Password:
```

在驗證使用者之後、但叢集Shell提示出現之前、MOTD會顯示在主控台工作階段（僅供叢集存取）或SSH工作階段（供叢集或SVM存取）中。例如、您可以使用MOTD來顯示歡迎訊息或資訊訊息、例如以下只有已驗證的使用者會看到的訊息：

```
$ ssh admin@cluster1-01

Password:

Greetings. This system is running ONTAP 9.0.
Your user name is 'admin'. Your last login was Wed Apr 08 16:46:53 2015
from 10.72.137.28.
```

您可以使用建立或修改橫幅或 MOTD 的內容 `security login banner modify` 或 `security login motd modify` 命令的方式如下：

- 您可以互動或非互動方式使用CLI來指定橫幅或MOTD所使用的文字。

  互動模式、在不使用命令時啟動 `-message` 或 `-uri` 參數、可讓您在訊息中使用新行（也稱為行尾）。

  非互動模式、使用 `-message` 指定訊息字串的參數不支援換行。

- 您可以從FTP或HTTP位置上傳內容、以用於橫幅或MOTD。
- 您可以設定MOTD以顯示動態內容。

  您可以設定MOTD動態顯示的範例包括：

  - 叢集名稱、節點名稱或SVM名稱
  - 叢集日期與時間
  - 登入的使用者名稱
  - 使用者在叢集中任何節點上的上次登入
  - 登入裝置名稱或IP位址
  - 作業系統名稱
  - 軟體版本
  - 有效叢集版本字串

  橫幅不支援動態內容。深入瞭解 `security login motd modify`及可用於讓 MOTD 在中顯示動態產生內容"指令參考資料ONTAP"的逸出序列。

您可以在叢集或SVM層級管理橫幅和MOTD：

- 以下事實適用於橫幅廣告：
  - 為叢集設定的橫幅也會用於未定義橫幅訊息的所有SVM。
  - 您可以為每個SVM設定SVM層級橫幅。

    如果已設定叢集層級橫幅、則會被指定SVM的SVM層級橫幅覆寫。

- 以下事實適用於MOTD：
  - 根據預設、為叢集設定的MOTD也會針對所有SVM啟用。

- 此外、也可針對每個SVM設定SVM層級的MOTD。

  在這種情況下、登入SVM的使用者會看到兩個MOTD、一個在叢集層級定義、另一個在SVM層級定義。

- 叢集管理員可在每個SVM上啟用或停用叢集層級的MOTD。

  如果叢集管理員停用SVM的叢集層級MOTD、則登入SVM的使用者不會看到叢集層級MOTD。

建立 ONTAP 登入橫幅

您可以建立橫幅、向嘗試存取叢集或SVM的人顯示訊息。橫幅會顯示在主控台工作階段（僅限叢集存取）或SSH工作階段（用於叢集或SVM存取）中、然後才會提示使用者進行驗證。

步驟

1. 使用 `security login banner modify` 建立叢集或 SVM 橫幅的命令：

如果您想要...	然後...
指定單一行的訊息	使用 `-message`「」<text>參數來指定文字。
在訊息中加入新行（也稱為行尾）	請使用命令而不使用 `-message` 或 `-uri` 用於啟動互動模式以編輯橫幅的參數。
從橫幅使用的位置上傳內容	使用 `-uri` 指定內容 FTP 或 HTTP 位置的參數。

   橫幅的大小上限為2、048位元組、包括換行字元。

   使用建立的橫幅 `-uri` 參數為靜態。系統不會自動重新整理以反映來源內容的後續變更。

   針對叢集建立的橫幅也會針對所有沒有現有橫幅的SVM顯示。任何後續建立的SVM橫幅都會覆寫該SVM的叢集層級橫幅。指定 `-message` 雙引號內有連字號的參數 (`"-"`）對於 SVM 、 SVM 會將 SVM 重設為使用叢集層級橫幅。

2. 使用顯示橫幅、確認已建立橫幅 `security login banner show` 命令。

   指定 `-message` 含有空白字串的參數 (`""`）顯示沒有內容的橫幅。

   指定 `-message` 參數 `"-"` 顯示未設定橫幅的所有（管理或資料） SVM 。

建立橫幅廣告的範例

以下範例使用非互動模式來建立「叢集1」叢集的橫幅：

```
cluster1::> security login banner modify -message "Authorized users only!"

cluster1::>
```

以下範例使用互動模式來建立 SVM 的橫幅 `svm1`：

```
cluster1::> security login banner modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
The svm1 SVM is reserved for authorized users only!


cluster1::>
```

下列範例顯示已建立的橫幅廣告：

```
cluster1::> security login banner show
Vserver: cluster1
Message
-------------------------------------------------------------------------------
---
Authorized users only!

Vserver: svm1
Message
-------------------------------------------------------------------------------
---
The svm1 SVM is reserved for authorized users only!

2 entries were displayed.

cluster1::>
```

相關資訊

- 管理橫幅
- "修改安全登入橫幅"
- "安全登入橫幅展示"

管理在 **ONTAP** 叢集和 **SVM** 層級顯示的橫幅文字

您可以在叢集或SVM層級管理橫幅。為叢集設定的橫幅也會用於未定義橫幅訊息的所有SVM。隨後建立的SVM橫幅會覆寫該SVM的叢集橫幅。

選擇

- 管理叢集層級的橫幅：

如果您想要...	然後...
建立橫幅以顯示所有登入工作階段	設定叢集層級橫幅： `security login banner modify -vserver <cluster_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	移除所有（叢集和SVM）登入的橫幅
將橫幅設定為空字串（``）： `security login banner modify -vserver * -message`	覆寫SVM管理員所建立的橫幅
修改SVM橫幅訊息： `security login banner modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }`

- 在SVM層級管理橫幅：

  在 SVM 內容中不需要指定 `-vserver <svm_name>`。

如果您想要...	然後...
以不同的SVM橫幅覆寫叢集管理員所提供的橫幅	為SVM建立橫幅： `security login banner modify -vserver <svm_name> { [-message "text"]
[-uri <ftp_or_http_addr>] }`	隱藏叢集管理員提供的橫幅、以便不顯示SVM的橫幅
將SVM橫幅設定為空白字串、以供SVM使用： `security login banner modify -vserver <svm_name> -message`	當SVM目前使用SVM層級橫幅時、請使用叢集層級橫幅

相關資訊

- "修改安全登入橫幅"

為 **ONTAP** 使用者建立當日訊息文字

您可以建立當天訊息（MOTD）、將資訊傳達給已驗證的CLI使用者。MOTD會在驗證使用

者之後顯示於主控台工作階段（僅供叢集存取）或SSH工作階段（用於叢集或SVM存取）、但會在叢集Shell提示出現之前顯示。

步驟

1. 使用 `security login motd modify` 為叢集或 SVM 建立 MOTD 的命令：

如果您想要...	然後...
指定單一行的訊息	使用 `-message "text"` 指定文字的參數。
包括新行（也稱為行尾）	請使用命令而不使用 `-message` 或 `-uri` 用於啟動互動模式以編輯 MOTD 的參數。
從用於MOTD的位置上傳內容	使用 `-uri` 指定內容 FTP 或 HTTP 位置的參數。

MOTD的最大大小為2、048位元組、包括換行字元。

`Security login motd modify`說明可用來讓 MOTD 顯示動態產生內容的逸出順序。

使用建立的 MOTD `-uri` 參數為靜態。系統不會自動重新整理以反映來源內容的後續變更。

根據預設、為叢集建立的MOTD也會針對所有SVM登入顯示、同時也會顯示SVM層級的MOTD、您可以針對特定SVM個別建立。設定 `-is-cluster-message-enabled` 參數至 `false` 對於 SVM 、可防止該 SVM 顯示叢集層級的 MOTD 。

2. 將 MOTD 顯示在中、以確認已建立 `security login motd show` 命令。

指定 `-message`帶有空字串（"`"）的參數顯示未配置或沒有內容的 MOTD。

深入瞭解 `security login motd modify`及參數，讓 MOTD 能夠在中顯示動態產生的內容"指令參考資料ONTAP"。

建立**MOTD**的範例

以下範例使用非互動模式為 `cluster1`簇：

```
cluster1::> security login motd modify -message "Greetings!"
```

以下範例使用互動模式為 `svm1`使用轉義序列顯示動態產生內容的 SVM：

```
cluster1::> security login motd modify -vserver svm1

Enter the message of the day for Vserver "svm1".
Max size: 2048. Enter a blank line to terminate input. Press Ctrl-C to
abort.
0        1         2         3         4         5         6         7
8
12345678901234567890123456789012345678901234567890123456789012345678901234
567890
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.
```

下列範例顯示已建立的教學影片：

```
cluster1::> security login motd show
Vserver: cluster1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Greetings!

Vserver: svm1
Is the Cluster MOTD Displayed?: true
Message
-------------------------------------------------------------------------
---
Welcome to the \n SVM.  Your user ID is '\N'. Your last successful login
was \L.

2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `security login motd show`資訊，請參閱。

管理在 **ONTAP** 叢集和 **SVM** 層級顯示的當日訊息文字

您可以在叢集或SVM層級管理當天訊息（MOTD）。根據預設、為叢集設定的MOTD也會針對所有SVM啟用。此外、也可針對每個SVM設定SVM層級的MOTD。叢集管理員可針對每個SVM啟用或停用叢集層級的MOTD。

在 ONTAP 命令參照中深入瞭解"轉義序列"可用於動態產生 MOTD 內容的。

選擇

- 在叢集層級管理MOTD：

如果您想要...	然後...
如果沒有現有的MOTD、請為所有登入建立MOTD	設定叢集層級的MOTD： `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	如果未設定SVM層級的MOTD、請變更所有登入的MOTD
修改叢集層級的MOTD： `security login motd modify -vserver <cluster_name> { [-message "<text>"] }	[-uri <ftp_or_http_addr>] }`
若未設定SVM層級的MOTD、請移除所有登入的MOTD	將叢集層級的 MOTD 設定為空白字串 (""）： `security login motd modify -vserver <cluster_name> -message ""`
讓每個SVM都顯示叢集層級的MOTD、而非使用SVM層級的MOTD	設定叢集層級的MOTD、然後在啟用叢集層級MOTD的情況下、將所有SVM層級的MOTD設為空白字串： a. `security login motd modify -vserver <cluster_name> { [-message "<text>"]
[-uri <ftp_or_http_addr>] }` .. `security login motd modify { -vserver !"<cluster_name>" } -message "" -is -cluster-message-enabled true`	僅針對選取的SVM顯示MOTD、不使用叢集層級的MOTD
將叢集層級的MOTD設為空白字串、然後為選取的SVM設定SVM層級的MOTD： a. `security login motd modify -vserver <cluster_name> -message ""` b. `security login motd modify -vserver <svm_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] }` + 您可以視需要為每個SVM重複此步驟。
針對所有（資料與管理）SVM、使用相同的SVM層級MOTD	將叢集和所有SVM設定為使用相同的MOTD： `security login motd modify -vserver * { [-message "<text>"]

如果您想要...	然後...
[-uri <ftp_or_http_addr>] }` [NOTE] ==== 如果您使用互動模式、CLI會提示您個別輸入叢集和每個SVM的MOTD。當系統提示您時、您可以將相同的MOTD貼到每個執行個體中。 ====	讓所有SVM都可選用叢集層級的MOTD、但不要在叢集登入時顯示MOTD
設定叢集層級的MOTD、但停用叢集的顯示： `security login motd modify -vserver <cluster_name> { [-message "<text>"]	[-uri <ftp_or_http_addr>] } -is-cluster-message -enabled false`
當只有部分SVM同時具有叢集層級和SVM層級的MOTD時、請移除叢集層級和SVM層級的所有MOTD	將叢集和所有SVM設定為使用MOTD的空白字串： `security login motd modify -vserver * -message ""`
只有當其他SVM使用空字串、以及叢集層級使用不同的MOTD時、才可針對具有非空字串的SVM修改MOTD	使用延伸查詢可選擇性修改MOTD： `security login motd modify { -vserver !"<cluster_name>" -message !"" } { [-message "<text>"]
[-uri <ftp_or_http_addr>] }`	顯示單行或多行訊息中任意位置包含特定文字（例如「January」後面跟著「2015」）的所有 MOTD，即使文字分佈在不同的行上
使用查詢顯示MOTD： `security login motd show -message *"January"*"2015"*`	以互動方式建立包含多個和連續新行（也稱為行尾或EOLS）的MOTD。

- 在SVM層級管理MOTD：

  在 SVM 內容中不需要指定 `-vserver <svm_name>`。

如果您想要...	然後...
當SVM已經有現有的SVM層級MOTD時、請使用不同的SVM層級MOTD	修改SVM層級的MOTD： `security login motd modify -vserver <svm_name> { [-message "<text>"]

如果您想要...	然後...
[-uri <ftp_or_http_addr>] }`	當SVM已經有SVM層級的MOTD時、只能使用SVM的叢集層級MOTD
將SVM層級MOTD設為空白字串、然後讓叢集管理員啟用SVM的叢集層級MOTD： a. `security login motd modify -vserver <svm_name> -message ""` b. （適用於叢集管理員） `security login motd modify -vserver <svm_name> -is -cluster-message-enabled true`	當SVM目前同時顯示叢集層級和SVM層級的MOTD時、SVM不會顯示任何MOTD

相關資訊

- "安全登入motd修改"
- "安全登入motd show"

管理 ONTAP 工作和工作排程

工作會放入工作佇列、並在資源可用時於背景執行。如果工作佔用過多的叢集資源、您可以將其停止或暫停、直到叢集需求減少為止。您也可以監控及重新啟動工作。

工作類別

您可以管理三類工作：伺服器關聯、叢集關聯及私有。

工作可分為下列任一類別：

- 伺服器相關工作

  管理架構會將這些工作排入要執行的特定節點佇列。

- 叢集相關工作

  管理架構會將這些工作排入要執行之叢集中任何節點的佇列。

- 私有工作

  這些工作是專屬於某個節點、不使用複寫資料庫（RDB）或任何其他叢集機制。管理私有工作的命令需要進階權限層級或更高。

管理工作的命令

當您輸入命令以叫用工作時、通常會通知您工作已排入佇列、然後返回CLI命令提示字元。不過、有些命令會回報工作進度、而且在工作完成之前、不會返回CLI命令提示字元。在這些情況下、您可以按Ctrl-C將工作移至背景。

如果您想要...	使用此命令...
顯示所有工作的相關資訊	`job show`
顯示每個節點的工作相關資訊	`job show bynode`
顯示有關叢集關聯工作的資訊	`job show-cluster`
顯示已完成工作的相關資訊	`job show-completed`
顯示有關工作記錄的資訊	`job history show` 叢集中每個節點最多可儲存25、000筆工作記錄。因此、嘗試顯示完整的工作記錄可能需要很長時間。為了避免可能需要長時間等待、您應該依節點、儲存虛擬機器（SVM）或記錄ID來顯示工作。
顯示私有工作清單	`job private show` （進階權限層級）
顯示已完成私有工作的相關資訊	`job private show-completed` （進階權限層級）
顯示工作管理員初始化狀態的相關資訊	`job initstate show` （進階權限層級）
監控工作進度	`job watch-progress`
監控私有工作的進度	`job private watch-progress` （進階權限層級）
暫停工作	`job pause`
暫停私有工作	`job private pause` （進階權限層級）
恢復暫停的工作	`job resume`
恢復暫停的私有工作	`job private resume` （進階權限層級）
停止工作	`job stop`
停止私有工作	`job private stop` （進階權限層級）
刪除工作	`job delete`
刪除私有工作	`job private delete` （進階權限層級）

如果您想要...	使用此命令...
將叢集關聯的工作與擁有該工作的不可用節點解除關聯、以便其他節點可以取得該工作的擁有權	`job unclaim` （進階權限層級）

您可以使用 `event log show`命令來判斷已完成工作的結果。如"指令參考資料ONTAP"需詳細 `event log show`資訊，請參閱。

管理工作排程的命令

許多工作（例如磁碟區快照）可設定為在指定的排程上執行。在特定時間執行的排程稱為 _cron 排程（類似 UNIX `cron` 排程）。每隔一段時間執行的排程稱為「_interval_排程」。您可以使用 `job schedule`命令來管理工作排程。

工作排程不會調整為手動變更叢集日期和時間。這些工作會根據目前建立工作的叢集時間或最近執行工作的時間來排程執行。因此、如果您手動變更叢集日期或時間、則應使用 `job show` 和 `job history show` 用於驗證所有排程工作是否已根據您的需求排入佇列並完成的命令。

如果叢集是MetroCluster 支援功能的一部分、則兩個叢集上的工作排程必須相同。因此、如果您建立、修改或刪除工作排程、則必須在遠端叢集上執行相同的作業。

如果您想要...	使用此命令...
顯示所有排程的相關資訊	`job schedule show`
依排程顯示工作清單	`job schedule show-jobs`
顯示有關cron排程的資訊	`job schedule cron show`
顯示有關時間間隔排程的資訊	`job schedule interval show`
建立cron排程	`job schedule cron create` 從 ONTAP 9.10.1 開始、您可以在工作排程中加入 SVM 。
建立時間間隔排程	`job schedule interval create` 您必須至少指定下列其中一個參數： `-days`、 `-hours`、 `-minutes`或 `-seconds`。
修改cron排程	`job schedule cron modify`
修改時間間隔排程	`job schedule interval modify`
刪除排程	`job schedule delete`

如果您想要...	使用此命令...
刪除cron排程	`job schedule cron delete`
刪除時間間隔排程	`job schedule interval delete`

相關資訊

- "工作"

備份及還原叢集組態（僅限叢集管理員）

瞭解 ONTAP 組態備份檔案

組態備份檔是歸檔檔檔檔檔（.7z）、其中包含叢集及其內節點正常運作所需的所有可設定選項資訊。

這些檔案會儲存每個節點的本機組態、以及整個叢集的複寫組態。您可以使用組態備份檔案來備份及還原叢集的組態。

組態備份檔案有兩種類型：

- 節點組態備份檔案

  叢集中的每個健全節點都包含節點組態備份檔案、其中包含節點在叢集中正常運作所需的所有組態資訊和中繼資料。

- 叢集組態備份檔案

  這些檔案包括叢集中所有節點組態備份檔案的歸檔、以及複寫的叢集組態資訊（複寫的資料庫或RDB檔案）。叢集組態備份檔案可讓您還原整個叢集或叢集中任何節點的組態。叢集組態備份排程會自動建立這些檔案、並將其儲存在叢集中的多個節點上。

組態備份檔案僅包含組態資訊。它們不包含任何使用者資料。如需還原使用者資料的相關資訊、請參閱 "資料保護"。

瞭解如何排程 ONTAP 叢集與節點組態備份檔案的備份

三個獨立的排程會自動建立叢集和節點組態備份檔案、並在叢集中的節點之間複寫這些檔案。

系統會根據下列排程自動建立組態備份檔案：

- 每 8 小時
- 每日
- 每週

每次都會在叢集中的每個健全節點上建立節點組態備份檔案。然後、所有這些節點組態備份檔案都會收集在單一叢集組態備份檔案中、以及複寫的叢集組態、並儲存在叢集中的一或多個節點上。

用於管理組態備份排程的 **ONTAP** 命令

您可以使用 `system configuration backup settings` 管理組態備份排程的命令。

這些命令可在進階權限層級使用。

如果您想要...	使用此命令...
變更組態備份排程的設定： • 除了叢集中的預設位置外，還需指定用於上傳設定備份檔案的遠端 URL（HTTP、HTTPS、FTP 或 FTPS） • 指定用於登入遠端URL的使用者名稱 • 針對每個組態備份排程設定要保留的備份數目	`system configuration backup settings modify` 當您在遠端 URL 中使用 HTTPS 時、請使用 `-validate-certification` 啟用或停用數位憑證驗證的選項。預設會停用憑證驗證。 您要上傳組態備份檔案的Web伺服器必須已啟用HTTP和POST作業的HTTPS作業。如需詳細資訊、請參閱Web伺服器的文件。
設定用來登入遠端URL的密碼	`system configuration backup settings set-password`
檢視組態備份排程的設定	`system configuration backup settings show` 您可以設定 `-instance` 此參數可檢視每個排程的使用者名稱和備份數量。

用於管理節點組態備份檔案的 **ONTAP** 命令

您可以使用 `system configuration backup` 用於管理叢集和節點組態備份檔案的命令。

這些命令可在進階權限層級使用。

如果您想要...	使用此命令...
建立新的節點或叢集組態備份檔案	`system configuration backup create`
將組態備份檔案從節點複製到叢集中的另一個節點	`system configuration backup copy`

如果您想要...	使用此命令...
將設定備份檔案從叢集中的節點上傳到遠端 URL（FTP、HTTP、HTTPS 或 FTPS）	`system configuration backup upload` 當您在遠端 URL 中使用 HTTPS 時、請使用 `-validate-certification` 啟用或停用數位憑證驗證的選項。預設會停用憑證驗證。 您要上傳設定備份檔案的 Web 伺服器必須啟用 HTTP 的 PUT 作業和 HTTPS 的 POST 作業。您可能需要在某些網路伺服器上安裝附加模組。有關更多信息，請參閱 Web 伺服器的文檔。支援的 URL 格式因ONTAP版本而異。了解有關係統配置命令的更多信息 "指令參考資料ONTAP"。
從遠端URL下載組態備份檔案至叢集中的節點、並在指定時驗證數位憑證	`system configuration backup download` 當您在遠端 URL 中使用 HTTPS 時、請使用 `-validate-certification` 啟用或停用數位憑證驗證的選項。預設會停用憑證驗證。
在叢集中的節點上重新命名組態備份檔案	`system configuration backup rename`
檢視叢集中一或多個節點的節點和叢集組態備份檔案	`system configuration backup show`
刪除節點上的組態備份檔案	`system configuration backup delete` 此命令僅會刪除指定節點上的組態備份檔案。如果組態備份檔案也存在於叢集中的其他節點上、則會保留在這些節點上。

相關資訊

- "系統配置備份"

找到 **ONTAP** 節點組態備份檔案以還原節點

您可以使用位於遠端URL或叢集中節點上的組態備份檔案、來還原節點組態。

關於這項工作

您可以使用叢集或節點組態備份檔案來還原節點組態。

步驟

1. 將組態備份檔提供給需要還原組態的節點。

如果組態備份檔案位於...	然後...
位於遠端URL	使用 `system configuration backup download` 進階權限層級的命令、將其下載至還原節點。
在叢集中的節點上	a. 使用 `system configuration backup show` 進階權限層級的命令、可檢視叢集中包含還原節點組態的可用組態備份檔案清單。 b. 如果您識別的組態備份檔案不存在於復原節點上、請使用 `system configuration backup copy` 命令將其複製到恢復節點。

如果您先前重新建立叢集、應該選擇叢集重新建立之後所建立的組態備份檔案。如果您必須使用在叢集重新建立之前所建立的組態備份檔案、則在還原節點之後、您必須重新建立叢集。

相關資訊

- "系統配置備份"

使用 **ONTAP** 節點組態備份檔案還原節點

您可以使用已識別並可供還原節點使用的組態備份檔案來還原節點組態。

關於這項工作

您只能執行此工作、從導致節點本機組態檔遺失的災難中恢復。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 如果節點狀況良好、則在不同節點的進階權限層級、請使用 `cluster modify` 命令 `-node` 和 `-eligibility` 用於標示不符合資格的參數、並將其與叢集隔離。

   如果節點不健全、則應跳過此步驟。

   此範例將節點2修改為不符合參加叢集的資格、以便還原其組態：

   ```
   cluster1::*> cluster modify -node node2 -eligibility false
   ```

   如"指令參考資料ONTAP"需詳細 `cluster modify`資訊，請參閱。

3. 使用 `system configuration recovery node restore` 以進階權限層級執行命令、從組態備份檔案還原節點的組態。

   如果節點遺失其身分識別、包括其名稱、則應使用 `-nodename-in-backup` 參數、以在組態備份檔案中指定節點名稱。

此範例使用儲存在節點上的其中一個組態備份檔案來還原節點的組態：

```
cluster1::*> system configuration recovery node restore -backup
cluster1.8hour.2011-02-22.18_15_00.7z

Warning: This command overwrites local configuration files with
         files contained in the specified backup file. Use this
         command only to recover from a disaster that resulted
         in the loss of the local configuration files.
         The node will reboot after restoring the local configuration.
Do you want to continue? {y|n}: y
```

組態會還原、節點會重新開機。

4. 如果您將節點標示為不合格、請使用 `system configuration recovery cluster sync` 命令將節點標記為合格、並將其與叢集同步。
5. 如果您在 SAN 環境中作業、請使用 `system node reboot` 命令重新啟動節點並重新建立 SAN 仲裁。

完成後

如果您先前重新建立叢集、而且使用重新建立叢集之前所建立的組態備份檔案來還原節點組態、則必須重新建立叢集。

找到 **ONTAP** 叢集組態備份檔案以還原叢集

您可以使用叢集中節點或叢集組態備份檔案的組態來還原叢集。

步驟

1. 選擇要恢復叢集的組態類型。

   - 叢集中的節點

     如果叢集由多個節點組成、而其中一個節點在叢集處於所需組態時具有叢集組態、則您可以使用儲存在該節點上的組態來還原叢集。

     在大多數情況下、包含複寫環的節點、以及最新的交易ID、是還原叢集組態的最佳節點。。 `cluster ring show` 進階權限層級的命令可讓您檢視叢集中每個節點上可用的複寫環清單。

   - 叢集組態備份檔案

     如果您無法識別具有正確叢集組態的節點、或叢集是由單一節點所組成、則可以使用叢集組態備份檔案來還原叢集。

   如果您從配置備份檔案還原集群，則自備份以來所做的任何設定變更都會遺失。還原後，您必須解決配置備份檔案和目前配置之間的任何差異。查看"NetApp知識庫： ONTAP設定備份解決指南"以獲得故障排除指導。

2. 如果您選擇使用叢集組態備份檔案、請將檔案提供給您打算用來還原叢集的節點。

如果組態備份檔案位於...	然後...
位於遠端URL	使用 `system configuration backup download` 進階權限層級的命令、將其下載至還原節點。
在叢集中的節點上	a. 使用 `system configuration backup show` 進階權限層級的命令、可尋找叢集組態備份檔案、該檔案是在叢集處於所需組態時建立的。 b. 如果叢集組態備份檔案未位於您打算用來恢復叢集的節點上、請使用 `system configuration backup copy` 命令將其複製到恢復節點。

相關資訊

- "集群環秀"
- "系統配置備份"

使用 **ONTAP** 叢集組態備份檔案還原叢集

若要在叢集故障後從現有組態還原叢集組態、請使用您選擇的叢集組態重新建立叢集、並將其提供給恢復節點、然後將每個額外節點重新加入新叢集。

關於這項工作

您只能執行此工作、從導致叢集組態遺失的災難中恢復。

> 如果您是從組態備份檔案重新建立叢集、則必須聯絡技術支援部門、以解決組態備份檔案與叢集中現有組態之間的任何差異。
>
> 如果您從配置備份檔案還原集群，則自備份以來所做的任何設定變更都會遺失。還原後，您必須解決配置備份檔案和目前配置之間的任何差異。查看"NetApp知識庫： ONTAP設定備份解決指南"以獲得故障排除指導。

步驟

1. 停用每個HA配對的儲存容錯移轉：

   `storage failover modify -node` *`node_name`* `-enabled false`

   您只需針對每個HA配對停用一次儲存容錯移轉。當您停用節點的儲存容錯移轉時、節點的合作夥伴也會停用儲存容錯移轉。

2. 停止每個節點（恢復節點除外）：

   `system node halt -node` *`node_name`* `-reason "text"`

```
cluster1::*> system node halt -node node0 -reason "recovering cluster"

Warning: Are you sure you want to halt the node? {y|n}: y
```

3. 將權限層級設為進階：

   set -privilege advanced

4. 在恢復節點上、使用 **system configuration recovery cluster recreate** 用於重新建立叢集的命令。

   此範例使用儲存在恢復節點上的組態資訊重新建立叢集：

```
cluster1::*> configuration recovery cluster recreate -from node

Warning: This command will destroy your existing cluster. It will
         rebuild a new single-node cluster consisting of this node
         and its current configuration. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
Do you want to continue? {y|n}: y
```

   在恢復節點上建立新的叢集。

5. 如果您是從組態備份檔案重新建立叢集、請確認叢集還原仍在進行中：

   system configuration recovery cluster show

   如果您是從正常節點重新建立叢集、則不需要驗證叢集還原狀態。

```
cluster1::*> system configuration recovery cluster show
 Recovery Status: in-progress
 Is Recovery Status Persisted: false
```

6. 引導需要重新加入重新建立叢集的每個節點。

   您必須一次重新啟動一個節點。

7. 針對需要加入重新建立叢集的每個節點、執行下列步驟：

   a. 從重新建立的叢集上健全的節點、重新加入目標節點：

      system configuration recovery cluster rejoin -node *node_name*

      此範例將「'node2'」目標節點重新加入重新建立的叢集：

```
cluster1::*> system configuration recovery cluster rejoin -node node2

Warning: This command will rejoin node "node2" into the local
         cluster, potentially overwriting critical cluster
         configuration files. This command should only be used
         to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress.
         This command will cause node "node2" to reboot.
Do you want to continue? {y|n}: y
```

目標節點會重新開機、然後加入叢集。

b. 驗證目標節點是否正常、並已與叢集中的其他節點形成仲裁：

cluster show -eligibility true

目標節點必須重新加入重新建立的叢集、才能重新加入其他節點。

```
cluster1::*> cluster show -eligibility true
Node                 Health  Eligibility   Epsilon
-------------------- ------- ------------  ------------
node0                true    true          false
node1                true    true          false
2 entries were displayed.
```

8. 如果您是從組態備份檔案重新建立叢集、請將恢復狀態設為「完成」：

system configuration recovery cluster modify -recovery-status complete

9. 返回管理權限層級：

set -privilege admin

10. 如果叢集僅包含兩個節點、請使用 **cluster ha modify** 命令以重新啟用叢集 HA 。
11. 使用 **storage failover modify** 為每個 HA 配對重新啟用儲存容錯移轉的命令。

完成後

如果叢集具有SnapMirror對等關係、您也需要重新建立這些關係。如需詳細資訊、請參閱 "資料保護"。

相關資訊

- "指令參考資料ONTAP"
- "儲存故障轉移修改"

如果存在叢集範圍的仲裁、但有一或多個節點與叢集不同步、則您必須同步處理節點、以還原節點上的複寫資料庫（RDB）、並將其加入仲裁。

步驟

1. 從健全的節點、使用 `system configuration recovery cluster sync` 進階權限層級的命令、用於同步與叢集組態不同步的節點。

   此範例可將節點（*node2*）與叢集的其他部分同步：

```
cluster1::*> system configuration recovery cluster sync -node node2

Warning: This command will synchronize node "node2" with the cluster
         configuration, potentially overwriting critical cluster
         configuration files on the node. This feature should only be
         used to recover from a disaster. Do not perform any other
         recovery operations while this operation is in progress. This
         command will cause all the cluster applications on node
         "node2" to restart, interrupting administrative CLI and Web
         interface on that node.
Do you want to continue? {y|n}: y
All cluster applications on node "node2" will be restarted. Verify that
the cluster applications go online.
```

結果

RDB會複寫至節點、節點便有資格參與叢集。

管理 ONTAP 叢集的節點核心傾印（僅限叢集管理員）

當節點出現問題時、會發生核心傾印、系統會建立核心傾印檔案、以便技術支援人員疑難排解問題。您可以設定或顯示核心傾印屬性。您也可以儲存、顯示、區段、上傳或刪除核心傾印檔案。

您可以使用下列方法來管理核心傾印：

- 設定核心傾印並顯示組態設定
- 顯示核心傾印的基本資訊、狀態和屬性

  核心傾印檔案和報告會儲存在中 `/mroot/etc/crash/` 節點目錄。您可以使用來顯示目錄內容 `system node coredump` 命令或 Web 瀏覽器。

- 儲存核心傾印內容、並將儲存的檔案上傳至指定位置或技術支援

  此功能可防止您在接管、集合體重新配置或還原期間、開始儲存核心傾印檔案。ONTAP

- 刪除不再需要的核心傾印檔案

管理核心傾印的命令

您可以使用 `system node coredump config` 管理核心傾印組態的命令 `system node coredump` 管理核心傾印檔案的命令、以及 `system node coredump reports` 管理應用程式核心報告的命令。

如需本主題中所述命令的詳細"指令參考資料ONTAP"資訊，請參閱。

如果您想要...	使用此命令...
設定核心傾印	`system node coredump config modify`
顯示核心傾印的組態設定	`system node coredump config show`
顯示核心傾印的基本資訊	`system node coredump show`
重新開機節點時、手動觸發核心傾印	`system node reboot` 兩者兼具 `-dump` 和 `-skip -lif-migration-before-reboot` 參數 link:https://docs NetApp · ONTAP — CLI/system-node-reboot.html#parameters[`skip-lif-migration-before-reboot`^] 參數指定在重新開機之前略過 LIF 移轉。
當您關閉節點時、手動觸發核心傾印	`system node halt` 兩者兼具 `-dump` 和 `-skip -lif-migration-before-shutdown` 參數 link:https://docs NetApp · ONTAP — CLI/system-node-halt · html#parameters^ 參數[`skip-lif-migration-before-shutdown`指定在關機之前略過 LIF 移轉。
儲存指定的核心傾印	`system node coredump save`
儲存指定節點上所有未儲存的核心傾印	`system node coredump save-all`
使用AutoSupport 您指定的核心傾印檔案來產生及傳送一個不確定的訊息	`system node autosupport invoke-core-upload` 。 `-uri` 選用參數會指定 AutoSupport 訊息的替代目的地。
顯示核心傾印的狀態資訊	`system node coredump status`

如果您想要...	使用此命令...
刪除指定的核心傾印	`system node coredump delete`
刪除節點上所有未儲存的核心傾印或所有已儲存的核心檔案	`system node coredump delete-all`
顯示應用程式核心傾印報告	`system node coredump reports show`
刪除應用程式核心傾印報告	`system node coredump reports delete`

相關資訊

"指令參考資料ONTAP"

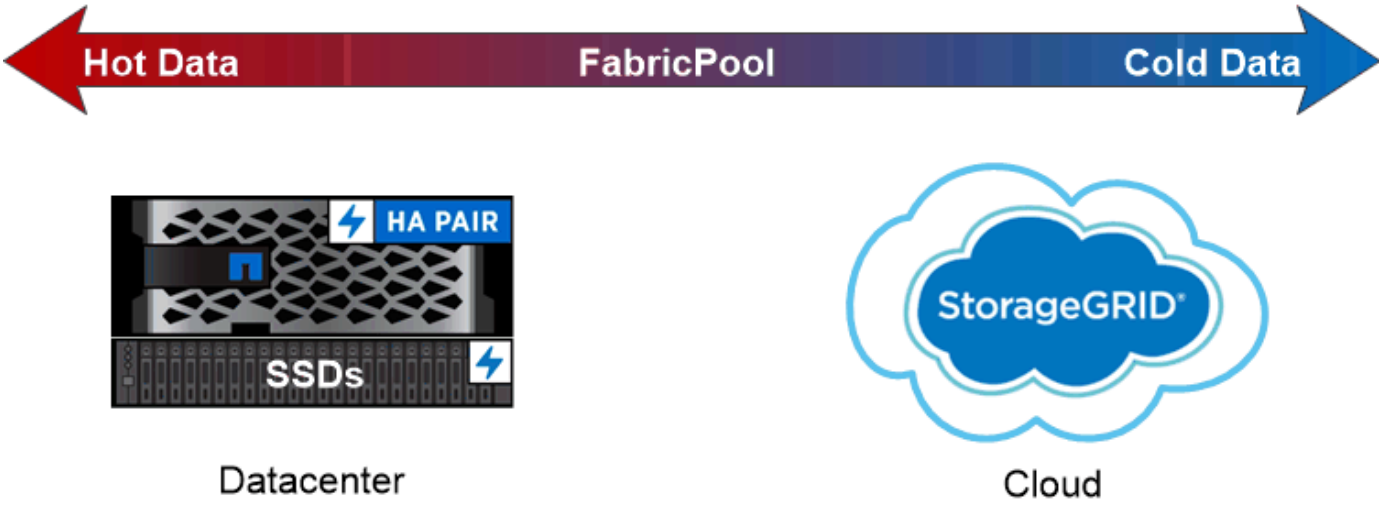
磁碟與階層管理

磁碟與 **ONTAP** 本機層

_local st層 _ 也稱為 _aggregate ，是由節點所管理之磁碟的邏輯容器。您可以使用本機層來隔離具有不同效能需求的工作負載、以不同存取模式分層資料、或將資料隔離以符合法規要求。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。

- 對於需要最低延遲和最高效能的業務關鍵應用程式、您可以建立一個完全由SSD組成的本機層。
- 若要以不同的存取模式來分層資料、您可以建立_混合式本機層_、將Flash部署為高效能快取、以供工作資料集使用、同時使用成本較低的HDD或物件儲存設備來儲存較少存取的資料。
  - A "*Flash Pool*"由 SSD 和 HDD 組成。
  - A "FabricPool" 由附有物件存放區的全 SSD 本機層所組成。
- 如果您需要將已歸檔的資料與作用中資料隔離、以供法規遵循之用、您可以使用由容量HDD所組成的本機層級、或是結合效能與容量HDD。



You can use a FabricPool to tier data with different access patterns, deploying SSDs for frequently accessed "hot" data and object storage for rarely accessed "cold" data.

在 **MetroCluster** 組態中使用本機層級

如果您有 MetroCluster 組態，則應遵循文件中的程序，以取得初始組態，並遵循"MetroCluster"本機層和磁碟管理的準則。

相關資訊

- "管理本機層"
- "管理磁碟"
- "管理RAID組態"
- "管理Flash Pool階層"
- "管理FabricPool 各種雲端階層"

管理本機層

瞭解 **ONTAP** 本機層管理

您可以使用系統管理員或 ONTAP CLI 來新增本機層，管理其使用情形，以及為其新增容量（磁碟）。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

您可以執行下列工作：

- "新增（建立）本機層"

若要新增本機層級、請遵循特定工作流程。您可以決定本機層所需的磁碟或磁碟分割數目、並決定要使用哪種方法來建立本機層。您可以藉由ONTAP 讓「資源不確定」指派組態來自動新增本機層級、也可以手動指定組態。

- "管理本機層的使用"

  對於現有的本機層級、您可以重新命名、設定其媒體成本、或決定其磁碟機和RAID群組資訊。您可以修改本機層的RAID組態、並將本機層級指派給儲存VM（SVM）。
  您可以修改本機層的RAID組態、並將本機層級指派給儲存VM（SVM）。您可以判斷哪些磁碟區位於本機層、以及它們在本機層上使用的空間。您可以控制磁碟區可以使用的空間量。您可以使用HA配對來重新配置本機層所有權。 您也可以刪除本機層。

- "將容量（磁碟）新增至本機層"

  使用不同的方法、您可以依照特定工作流程來新增容量。
  您可以將磁碟新增至本機層、並將磁碟機新增至節點或機櫃。
  如有需要、您可以修正未對齊的備用分割區。

新增（建立）本機層

新增 **ONTAP** 本機層的工作流程

建立本機層可為系統上的磁碟區提供儲存設備。

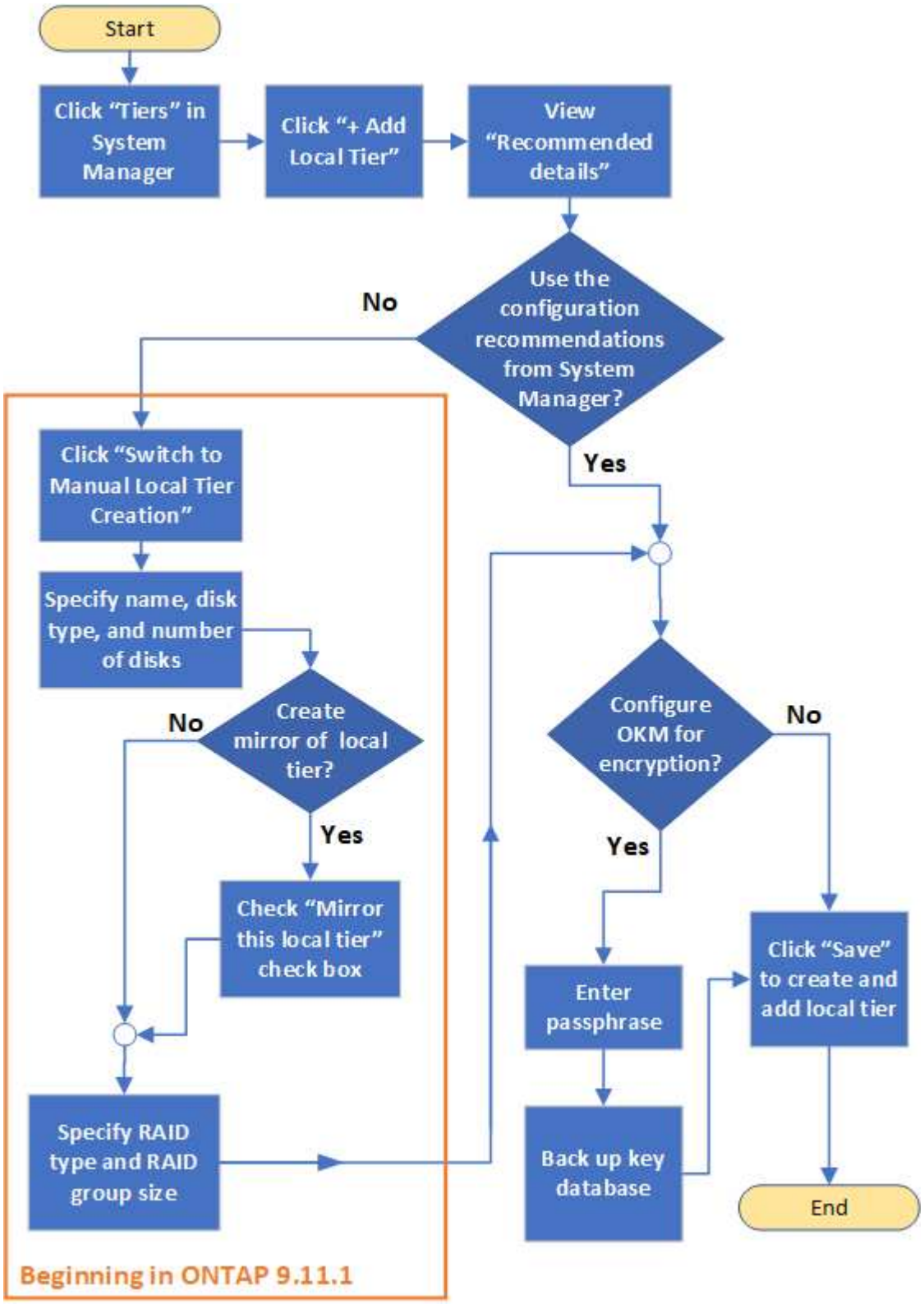
> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

建立本機階層的工作流程是專屬於您使用的介面： System Manager 或 CLI 。

系統管理員

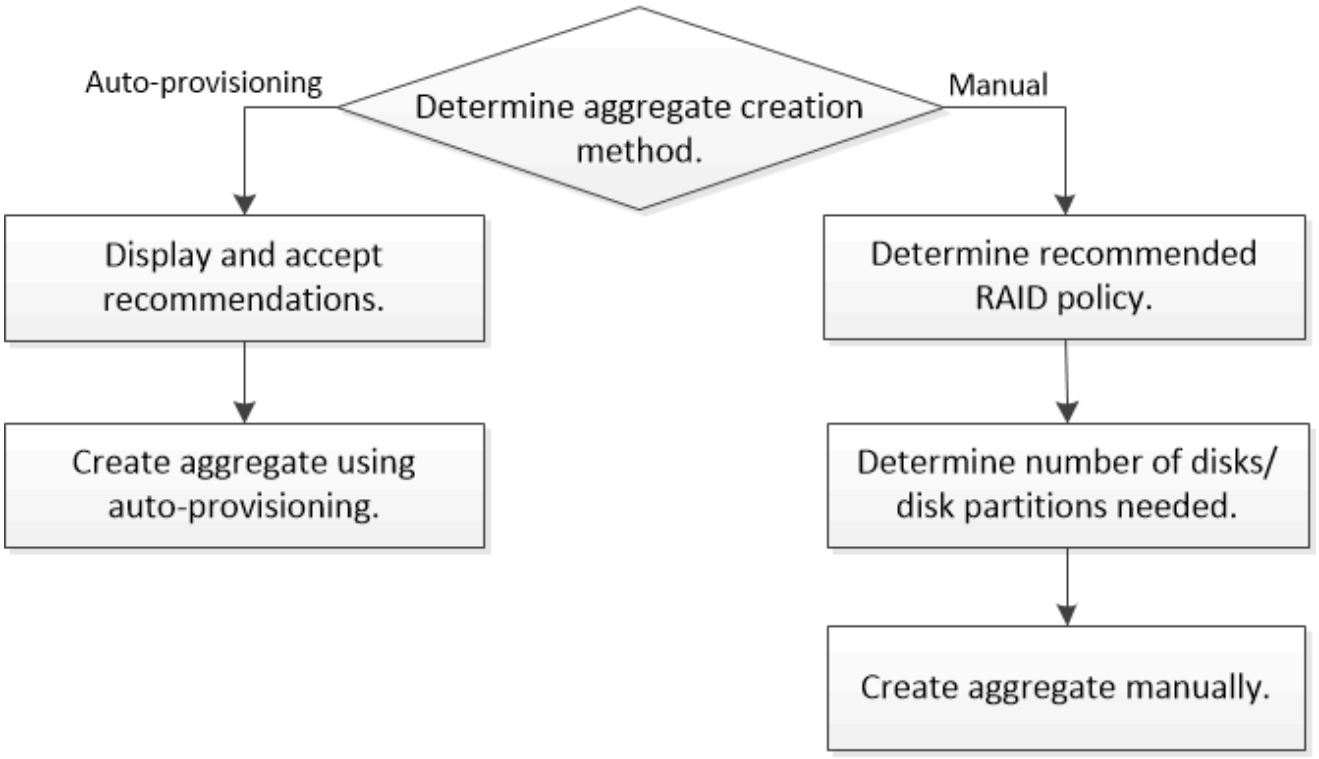
System Manager會根據建議的最佳實務做法來建立本機層級、以供設定本機層級。

從ONTAP 《銷售指南9.11.1：自動程序中建議的組態不同於新增本機層的組態、您可以決定手動設定本機層。



CLI

當您建立本機層（自動設定）時， ONTAP可以提供建議的設定。如果根據最佳實務做法建議的組態適合您的環境，您可以接受這些組態來建立本機層。否則，您可以手動建立本機階層。



判斷 **ONTAP** 本機層所需的磁碟或磁碟分割數目

您的本機層必須有足夠的磁碟或磁碟分割區，才能符合系統和業務需求。您也應該擁有建議的熱備援磁碟或熱備援磁碟分割數目、以將資料遺失的可能性降至最低。

根資料分割預設會在特定組態上啟用。啟用根資料分割的系統會使用磁碟分割來建立本機層級。未啟用根資料分割的系統會使用未分割的磁碟。

您必須擁有足夠的磁碟或磁碟分割區、以符合RAID原則所需的最低數量、並足以滿足最低容量需求。

在物件中ONTAP 、磁碟機的可用空間小於磁碟機的實體容量。您可以在中找到特定磁碟機的可用空間、以及每個RAID原則所需的磁碟或磁碟分割數目下限 "Hardware Universe"。

判斷特定磁碟的可用空間

您遵循的程序取決於您使用的介面-系統管理員或CLI：

系統管理員

使用**System Manager**來判斷磁碟的可用空間

執行下列步驟以檢視磁碟的可用大小：

步驟

1. 移至*儲存設備> Tiers*
2. 按一下 ⋮ 本機層名稱旁的。
3. 選擇*磁碟資訊*索引標籤。

CLI

使用**CLI**來判斷磁碟的可用空間

執行下列步驟以檢視磁碟的可用大小：

步驟

1. 顯示備用磁碟資訊：

```
storage aggregate show-spare-disks
```

除了建立 RAID 群組並符合容量需求所需的磁碟或磁碟分割數目之外，您還應該擁有建議用於本機層的最小熱備援磁碟或熱備援磁碟分割數：

- 對於所有 Flash 本機層，您至少應擁有一個熱備援磁碟或磁碟分割區。

  不使用備援磁碟機的功能預設為不使用。AFF完全支援此例外狀況。

- 對於非 Flash 同質本機層，您至少應該有兩個熱備援磁碟或磁碟分割區。
- 對於SSD儲存資源池、每個HA配對至少應有一個熱備援磁碟。
- 對於 Flash Pool 本機層，每個 HA 配對至少應有兩個備用磁碟。如需 Flash Pool 本機層支援 RAID 原則的詳細資訊，請參閱 "Hardware Universe"。
- 若要支援使用維護中心、並避免多個並行磁碟故障所造成的問題、您在多個磁碟載體中至少應有四個熱備援磁碟。

相關資訊

- "NetApp Hardware Universe"
- "NetApp技術報告3838：儲存子系統組態指南"
- "儲存Aggregate顯示"

決定要使用哪種方法來建立 **ONTAP** 本機階層

雖然 ONTAP 提供自動新增本機層的最佳實務建議，但您必須判斷您的環境是否支援建議的組態。如果不是、您必須決定RAID原則和磁碟組態、然後手動建立本機層級。

自動建立本機層時ONTAP 、即可分析叢集中可用的備用磁碟、並根據最佳實務做法、提出如何使用備用磁碟來新增本機層的建議。顯示建議的組態。ONTAP 您可以接受建議、或手動新增本機層級。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

在您接受**ONTAP** 不推薦的功能之前

如果出現下列任一磁碟情況、則必須先解決這些問題、再接受ONTAP 來自下列的建議：

- 遺失磁碟
- 備用磁碟編號的波動
- 未指派的磁碟
- 非零備援
- 正在進行維護測試的磁碟

當您必須使用手動方法時

在許多情況下、建議的本機層配置最適合您的環境。不過，如果您的環境包含下列組態，則必須使用手動方法建立本機層。

> 從《局部9.11.1》開始ONTAP 、您可以使用System Manager手動新增本機層級。

- 使用第三方陣列 LUN 的本機層
- 虛擬磁碟Cloud Volumes ONTAP 搭配不一樣或ONTAP Select 不一樣的功能
- 系統MetroCluster
- SyncMirror
- MSATA磁碟
- Flash Pool 階層
- 多種磁碟類型或大小會連接至節點

選取建立本機階層的方法

選擇您要使用的方法：

- "自動新增（建立）本機層"
- "手動新增（建立）本機層"

相關資訊

- "指令參考資料ONTAP"
- "儲存聚合自動配置"

如果 ONTAP 提供的自動新增本機層的最佳實務建議適用於您的環境，您可以接受建議，並讓 ONTAP 新增本機層。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

磁碟必須由節點擁有，才能在本機層中使用。如果您的叢集未設定為使用自動磁碟擁有權指派"手動指派擁有權"，您必須。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

系統管理員

步驟

1. 在 System Manager 中、按一下 * Storage > Tiers* 。
2. 在* Tiers*頁面中、按一下 + Add Local Tier 若要建立新的本機層：

   「新增本機層級」頁面顯示可在節點上建立的建議本機層數、以及可用的儲存設備。

3. 按一下*建議詳細資料*以檢視System Manager建議的組態。

   System Manager會顯示ONTAP 下列資訊、從功能表9.8開始：

   - 本機層名稱（您可以編輯以ONTAP 版本S59.10.1開頭的本機層名稱）
   - 節點名稱
   - 可用大小
   - 儲存設備類型

     從版本號《2019年9月10日》開始ONTAP 、將會顯示其他資訊：

   - 磁碟：顯示磁碟的數量、大小和類型
   - 配置：顯示RAID群組配置、包括哪些磁碟為同位元檢查或資料、以及哪些插槽未使用。
   - * 備用磁碟 * ：顯示節點名稱、備用磁碟的數量和大小、以及儲存類型。
4. 請執行下列其中一個步驟：

如果您想…	然後執行此操作…
接受System Manager的建議。	請前往 設定Onboard Key Manager進行加密的步驟。
手動設定本機層級、並*非*使用System Manager的建議。	請前往"手動新增本機層"： • 如需ONTAP 使用版本的版本資訊、請依照下列步驟使用CLI。 • 從ONTAP 《2019年9月11日》開始、請依照步驟使用System Manager。

5. [[step5-okm-bride] （選用）：如果已安裝 Onboard Key Manager 、您可以將其設定為加密。 選中* Configure Onboard Key Manager for加密*複選框。
   a. 輸入通關密碼。
   b. 再次輸入密碼以確認密碼。
   c. 請儲存密碼以供日後使用、以便在系統需要恢復時使用。
   d. 備份金鑰資料庫以供未來使用。
6. 按一下「儲存」以建立本機層級、並將其新增至您的儲存解決方案。

CLI

您可以執行 `storage aggregate auto-provision`命令來產生本機層配置建議。然後，您可以在審查並核准 ONTAP 建議之後，建立本機層級。

關於這項工作

使用命令產生的預設摘要 `storage aggregate auto-provision`會列出建議建立的本機階層，包括名稱和可用大小。您可以檢視清單，並在出現提示時決定是否要建立建議的本機階層。

您也可以使用顯示詳細摘要 `-verbose` 選項、顯示下列報告：

- 在本機層建立之後，每個節點都會摘要列出要建立，探索到的備援磁碟，以及剩餘的備援磁碟和分割區
- 要建立的新資料本機層，包含要使用的磁碟和分割區數
- RAID 群組配置顯示如何在要建立的新資料本機層中使用備用磁碟和分割區
- 本機層建立後剩餘的備用磁碟和分割區詳細資料

如果您熟悉自動資源配置方法，且環境已準備妥當，您可以使用 `-skip-confirmation`選項來建立建議的本機層，而無需顯示和確認。 `storage aggregate auto-provision`命令不受 `CLI` 工作階段設定影響 `-confirmations`。

如"指令參考資料ONTAP"需詳細 `storage aggregate auto-provision`資訊，請參閱。

步驟

1. 執行 `storage aggregate auto-provision` 命令及所需的顯示選項。
   - 無選項：顯示標準摘要
   - `-verbose` 選項：顯示詳細摘要
   - `-skip-confirmation`選項：建立建議的本機階層，不需顯示或確認
2. 請執行下列其中一個步驟：

如果您想…	然後執行此操作…

接受ONTAP 來自本系統的建議。	檢閱建議的本機階層顯示，然後回應建立建議的本機階層的提示。
	
	`myA400-44556677::> storage aggregate auto-provision`
	`Node New Data Aggregate Usable Size`
	`---`
	`myA400-364 myA400_364_SSD_1 3.29TB`
	`myA400-363 myA400_363_SSD_1 1.46TB`
	`---`
	`Total: 2 new data aggregates 4.75TB`
	
	`Do you want to create recommended aggregates? {y`

n}: y Info: Aggregate auto provision has started. Use the "storage aggregate show-auto-provision-progress" command to track the progress. myA400-44556677::> ----	手動設定本機層級、*非*使用ONTAP 來自各地的建議。

相關資訊

- "指令參考資料ONTAP"

手動新增 **ONTAP** 本機層

如果您不想使用 ONTAP 的最佳實務建議來新增本機層級，可以手動執行程序。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

磁碟必須由節點擁有，才能在本機層中使用。如果您的叢集未設定為使用自動磁碟擁有權指派"手動指派擁有權"，您必須。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

系統管理員

從ONTAP 《銷售資訊》9.11.1開始、如果您不想使用System Manager建議的組態來建立本機層、可以指定您想要的組態。

步驟

1. 在 System Manager 中、按一下 * Storage > Tiers* 。
2. 在* Tiers*頁面中、按一下 + Add Local Tier 若要建立新的本機層：

   「新增本機層級」頁面顯示可在節點上建立的建議本機層數、以及可用的儲存設備。

3. 當System Manager顯示本機層的儲存建議時、請按一下「* Spare Disks*（備用磁碟）」區段中的*「Switch to Manual local Tier creation （切換至手動建立本機層）」。

   「新增本機層」頁面會顯示您用來設定本機層的欄位。

4. 在「新增本機層級」頁面的第一節中、完成下列步驟：
   a. 輸入本機層的名稱。
   b. （選用）：如果您要鏡射本機層、請勾選*鏡射此本機層*核取方塊。
   c. 選取磁碟類型。
   d. 選取磁碟數量。
5. 在「* RAID組態*」區段中、完成下列步驟：
   a. 選取RAID類型。
   b. 選取RAID群組大小。
   c. 按一下「RAID分配」以檢視磁碟在群組中的配置方式。
6. （選用）：如果已安裝 Onboard Key Manager 、您可以在頁面的 * 加密 * 區段中設定加密。選中*Configure Onboard Key Manager for加密*複選框。
   a. 輸入通關密碼。
   b. 再次輸入密碼以確認密碼。
   c. 請儲存密碼以供日後使用、以便在系統需要恢復時使用。
   d. 備份金鑰資料庫以供未來使用。
7. 按一下「儲存」以建立本機層級、並將其新增至您的儲存解決方案。

CLI

手動建立本機層之前，您應該先檢閱磁碟組態選項，並模擬建立。

然後、您可以核發 `storage aggregate create` 命令並驗證結果。

開始之前

您必須已確定本地層中所需的磁碟數量和熱備援磁碟數量。

關於這項工作

如果已啟用根資料資料分割、而且組態中有24個或更少的固態磁碟機（SSD）、建議您將資料分割區指派

給不同的節點。

在已啟用根資料分割和根資料資料分割的系統上建立本機階層的程序，與在使用未分割磁碟的系統上建立本機階層的程序相同。如果您的系統上已啟用根資料分割，則應使用磁碟分割區的數量來進行此 `-diskcount`選項。對於 root-data-data 分割區， `-diskcount`選項會指定要使用的磁碟數。

建立多個本機層以搭配 FlexGroup Volume 使用時，本機層的大小應盡可能接近。

如需更多關於 `storage aggregate create`及本機層建立選項與需求"指令參考資料ONTAP"的資訊，請參閱。

步驟

1. 檢視備援磁碟分割清單，確認您有足夠的空間來建立本機層：

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   資料分割區會顯示在下 `Local Data Usable`。根分割區無法作為備援磁碟區使用。

2. 模擬建立本機層：

   ```
   storage aggregate create -aggregate aggregate_name -node node_name
   -raidtype raid_dp -diskcount number_of_disks_or_partitions -simulate true
   ```

3. 如果模擬命令顯示任何警告、請調整命令並重複模擬。
4. 建立本機層：

   ```
   storage aggregate create -aggregate aggr_name -node node_name -raidtype
   raid_dp -diskcount number_of_disks_or_partitions
   ```

5. 顯示本機層以驗證其是否已建立：

   ```
   storage aggregate show-status aggregate_name
   ```

相關資訊

- "儲存Aggregate顯示"

新增啟用SyncMirror的ONTAP本地層

您可以在手動建立本機圖層時啟用SyncMirror ，以同步鏡像本地層資料。

詳細了解"鏡像和非鏡像本地層" 。

開始之前

- 必須僅使用內部儲存來初始化叢集。
- 必須在兩個節點上完成叢集設定。

關於這項工作

此程序在每個叢集節點上建立大小相同的鏡像資料本機層，每個本機層的磁碟數為 44。

步驟

1. 停用儲存自動分配：

   ```
   storage disk option modify -node * -autoassign off
   ```

2. 確認自動分配已停用：

   ```
   storage disk option show
   ```

3. 安裝外部擱板。
4. 將外部磁碟機指派給指定池 1 的每個節點：

   ```
   storage disk assign -disk <disk ID> -owner <node name> -pool 1
   ```

5. 在每個節點上鏡像根本地層：

   ```
   storage aggregate mirror -aggregate <node1 root-aggr>

   storage aggregate mirror -aggregate <node2 root-aggr>
   ```

   池 1 中的磁碟機會自動分割以符合叢 0 中的磁碟機。

6. 在節點 1 上，使用磁碟數量 44 建立鏡像資料本機層。這將從池 0 中選擇 22 個分割區，從池 1 中選擇 22 個分割區。

   ```
   storage aggregate create -node <node1 name> -aggregate <node1 aggr-name>
   -diskcount 44 -mirror true
   ```

7. 在節點 2 上，使用磁碟數量 44 建立鏡像資料本機層。這將從池 0 中選擇 22 個分割區，從池 1 中選擇 22 個分割區。

   ```
   storage aggregate create -node <node2 name> -aggregate <node2 aggr-name>
   -diskcount 44 -mirror true
   ```

8. 驗證是否成功建立了大小相同的本機層：

   ```
   storage aggregate show
   ```

相關資訊

- "儲存磁碟分配"
- "儲存磁碟選項修改"
- "儲存磁碟選項顯示"

管理本機層的使用

重新命名 **ONTAP** 本機層

您可以重新命名本機層。您遵循的方法取決於您使用的介面（ System Manager 或 CLI ）。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

系統管理員

- 使用 System Manager 重新命名本機層 *

從ONTAP 版本號《2019年9月10日》開始、您可以修改本機層的名稱。

步驟

1. 在 System Manager 中、按一下 * Storage > Tiers* 。
2. 按一下 ⋮ 本機層名稱旁的。
3. 選取*重新命名*。
4. 為本機層指定新名稱。

CLI

- 使用 CLI 重新命名本機層 *

步驟

1. 使用 CLI 重新命名本機層：

   ```
   storage aggregate rename -aggregate aggr-name -newname aggr-new-name
   ```

   以下範例將名為「aggr5」的Aggregate重新命名為「shes-aggr」：

   ```
   > storage aggregate rename -aggregate aggr5 -newname sales-aggr
   ```

相關資訊

- "儲存聚合重命名"

設定 **ONTAP** 本機層的媒體成本

從 ONTAP 9.11.1 開始，您可以使用系統管理員來設定本機層的媒體成本。

步驟

1. 在 System Manager 中，按一下 * 儲存 > Tiers* ，然後在所需的本端階層方塊中按一下 * 設定媒體成本 * 。
2. 選取*作用中和非作用中的層級*以進行比較。
3. 輸入貨幣類型和金額。

當您輸入或變更媒體成本時、所有媒體類型都會進行變更。

在剛安裝ONTAP 的系統中、有更新版本的版本為EZ9.4或ONTAP 更新版本、而系統重新初始化為EZ9.4或更新版本時、則使用_fast零位調整_來歸零磁碟機。

有了_fast零位調整_、磁碟機就會在數秒內歸零。這是在資源配置之前自動完成的，可大幅縮短在新增備用磁碟機時初始化系統，建立本機層或擴充本機層所需的時間。

SSD和HDD均支援_Fast零位調整。

> 從ONTAP Ex9.3或更早版本升級的系統不支援_Fast零位調整。必須重新安裝更新版本的組件9.4或更新版本、否則系統必須重新初始化ONTAP 。在 ONTAP 9.3 及更早版本中， ONTAP 也會自動將磁碟機歸零，但程序所需時間較長。

如果您需要手動歸零磁碟機、可以使用下列其中一種方法。 在更新的版本中、手動將磁碟機歸零也只需數秒鐘ONTAP 。

CLI 命令

使用**CLI**命令快速歸零磁碟機

關於這項工作

使用此命令需要管理員權限。

步驟

1. 輸入CLI命令：

```
storage disk zerospares
```

開機功能表選項

從開機功能表中選取選項以快速歸零磁碟機

關於這項工作

- 快速零位調整增強功能不支援ONTAP 從版本更新至版本早於版本9.4的系統。

步驟

1. 從開機功能表中、選取下列其中一個選項：
   - （4）清除組態並初始化所有磁碟
   - （9A）取消分割所有磁碟、並移除其擁有權資訊
   - （9B）全新組態、並以整個磁碟初始化節點

相關資訊

- "儲存磁碟 zerospares"

磁碟必須由節點擁有，才能在本機層中使用。

關於這項工作

- 如果您是在未初始化且不只有 DS460C 機櫃的 HA 配對中手動指派擁有權、請使用選項 1 。
- 如果您正在初始化只有 DS460C 機櫃的 HA 配對、請使用選項 2 手動指派根磁碟機的擁有權。

選項 **1** ：大多數 **HA** 配對

對於未初始化且不只有 DS460C 機櫃的 HA 配對、請使用此程序手動指派擁有權。

關於這項工作

- 您要指派擁有權的磁碟必須位於實體纜線連接至您要指派擁有權之節點的機櫃中。
- 如果您在本機層（ Aggregate ）中使用磁碟：
  - 磁碟必須由節點擁有、才能在本機層（Aggregate）中使用。
  - 您無法重新指派在本機層（ Aggregate ）中使用的磁碟擁有權。

步驟

1. 使用 CLI 顯示所有未擁有的磁碟：

   ```
   storage disk show -container-type unassigned
   ```

2. 指派每個磁碟：

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   您可以使用萬用字元一次指派多個磁碟。如果您要重新指派已由不同節點擁有的備用磁碟、則必須使用「-force」選項。

選項 **2** ：只有 **DS460C** 機櫃的 **HA** 配對

對於正在初始化且只有 DS460C 機櫃的 HA 配對、請使用此程序手動指派根磁碟機的擁有權。

關於這項工作

- 當您初始化只有 DS460C 機櫃的 HA 配對時、必須手動指派根磁碟機、以符合半抽屜原則。

  HA 配對初始化（開機）之後，會自動啟用磁碟擁有權的自動指派，並使用半抽屜原則將擁有權指派給其餘磁碟機（根磁碟機除外），以及未來新增的任何磁碟機，例如更換故障磁碟，回應「低備援磁碟機」訊息或新增容量。

  "瞭解半抽屜式原則"。

- 對於 DS460C 機櫃中任何大於 8TB NL-SAS 磁碟機、每個 HA 配對（每個節點 5 個）至少需要 10 個磁碟機。

步驟

1. 如果您的 DS460C 機櫃未完全填入、請完成下列子步驟；否則、請前往下一步。

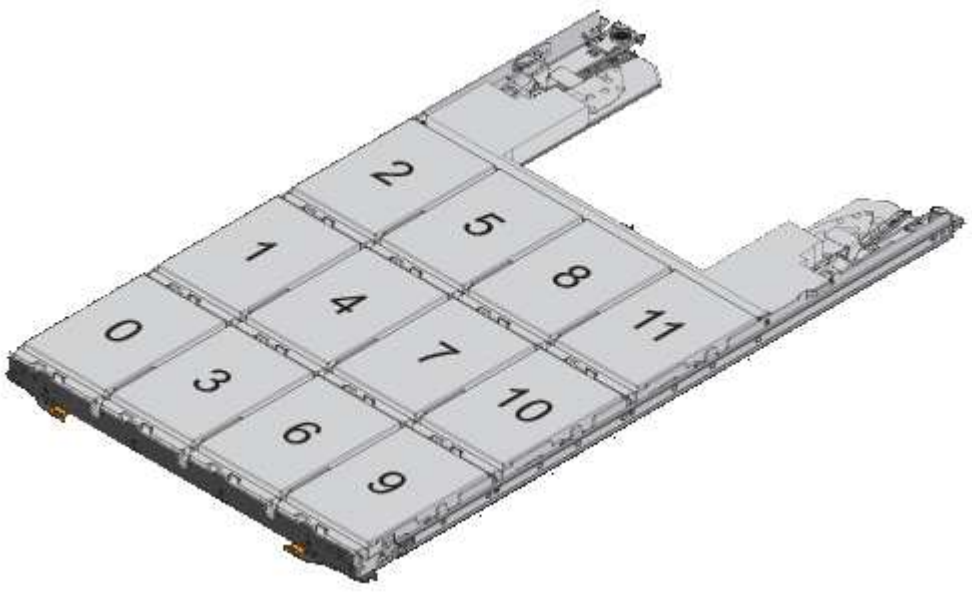
   a. 首先、在每個抽屜的前排（磁碟機支架 0 、 3 、 6 和 9 ）安裝磁碟機。

      在每個抽屜的前排安裝磁碟機、可讓氣流正常、並防止過熱。

   b. 對於其餘的磁碟機、請將其平均分配至每個抽屜。

      從正面到背面填充藥屜列。如果您沒有足夠的磁碟機來填滿列、請成對安裝、讓磁碟機平均地佔據抽屜的左右兩側。

      下圖顯示 DS460C 抽屜中的磁碟機支架編號和位置。



2. 使用節點管理 LIF 或叢集管理 LIF 登入叢集 Shell 。
3. 使用下列子步驟、手動指派每個藥屜中的根磁碟機、以符合半藥屜原則：

半抽屜原則可讓您將抽屜磁碟機（托架 0 至 5 ）的左半部分指派給節點 A 、而抽屜磁碟機（托架 6 至 11 ）的右半部分指派給節點 B

a. 顯示所有未擁有的磁碟：
   `storage disk show -container-type unassigned`

b. 指派根磁碟：
   `storage disk assign -disk disk_name -owner owner_name`

   您可以使用萬用字元一次指派多個磁碟。

如"指令參考資料ONTAP"需詳細 `storage disk`資訊，請參閱。

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"

判斷 **ONTAP** 本機層的磁碟機和 **RAID** 群組資訊

有些本機層管理工作需要您知道哪些類型的磁碟機組成本機層，其大小，總和檢查碼和狀態，是否與其他本機層共用，以及 RAID 群組的大小和組成。

步驟

1. 依 RAID 群組顯示本機層的磁碟機：

   `storage aggregate show-status` *`aggr_name`*

   本機層中的每個 RAID 群組都會顯示磁碟機。

   您可以在中看到磁碟機的 RAID 類型（資料、同位元檢查、同位元檢查） `Position` 欄位。如果是 `Position` 隨即顯示欄 `shared`然後共用磁碟機：如果是 HDD 、則是分割磁碟；如果是 SSD 、則是儲存池的一部分。

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

相關資訊

- "儲存聚合顯示狀態"

將 **ONTAP** 本機層指派給儲存 **VM** （ **SVM** ）

如果您將一或多個本機層指派給儲存虛擬機器（儲存 VM 或 SVM ，先前稱為 vserver ），則只能使用這些本機層來包含該儲存 VM （ SVM ）的磁碟區。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

您要指派給該儲存VM的儲存VM和本機層必須已經存在。

關於這項工作

將本機層級指派給儲存虛擬機器、有助於將儲存虛擬機器彼此隔離、這在多租戶環境中尤其重要。

步驟

1. 檢查已指派給 SVM 的本機層清單：

   ```
   vserver show -fields aggr-list
   ```

   此時會顯示目前指派給 SVM 的本機層。如果沒有指派任何本機層， `-`則會顯示。

2. 視您的需求新增或移除指派的本機階層：

如果您想要...	使用此命令...
指派額外的本機層	`vserver add-aggregates`
取消指派本機層	`vserver remove-aggregates`

   所列的本機階層會指派給 SVM 或從 SVM 中移除。如果SVM已有使用未指派給SVM之集合體的磁碟區、則會顯示警告訊息、但命令會成功完成。任何已指派給 SVM 且未在命令中命名的本機階層，都不會受到影響。

範例

在以下範例中，本機層 aggr1 和 aggr2 會指派給 SVM svm1 ：

```
vserver add-aggregates -vserver svm1 -aggregates aggr1,aggr2
```

判斷哪些磁碟區位於 **ONTAP** 本機層

您可能需要先判斷哪些磁碟區位於本機層，然後才能在本機層上執行作業，例如重新定位磁碟區或將其離線。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

步驟

1. 若要顯示位於本機層的磁碟區，請輸入

   ```
   volume show -aggregate aggregate_name
   ```

   會顯示位於指定本機層的所有磁碟區。

判斷並控制 **ONTAP** 本機層中磁碟區的空間使用量

您可以判斷哪些 FlexVol 磁碟區使用的是本機層中空間最大的磁碟區，特別是磁碟區中的哪些功能。

該 `volume show-footprint`命令提供有關卷佔用空間或其在包含的本地層中的空間使用情況的信息。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

此 `volume show-footprint`命令會顯示本機層中每個磁碟區（包括離線磁碟區）的空間使用量詳細資料。此命令可橋接和 `aggregate show-space`命令輸出之間的間隙 `volume show-space`。所有百分比都是以本機層大小的百分比來計算。

下列範例顯示 `volume show-footprint` 稱為 testvol 的 Volume 命令輸出：

```
cluster1::> volume show-footprint testvol

      Vserver : thevs
      Volume  : testvol

      Feature                                     Used    Used%
      --------------------------------    ----------    -----
      Volume Data Footprint                    120.6MB       4%
      Volume Guarantee                          1.88GB      71%
      Flexible Volume Metadata                 11.38MB       0%
      Delayed Frees                             1.36MB       0%
      Total Footprint                           2.01GB      76%
```

下表說明的輸出部分主要列 `volume show-footprint` 命令以及您可以採取哪些行動來嘗試利用該功能來減少空間使用量：

列/功能名稱	列的說明/內容	減少的方法
`Volume Data Footprint`	使用中檔案系統中的磁碟區資料，以及磁碟區快照所使用的空間總量。此列不包含保留空間。	• 從磁碟區刪除資料。 • 從磁碟區刪除快照。
`Volume Guarantee`	本機層中的磁碟區保留給未來寫入的空間量。保留的空間量取決於磁碟區的保證類型。	將磁碟區的保證類型變更為 `none`。
`Flexible Volume Metadata`	磁碟區中繼資料檔案在本機層中使用的總空間量。	沒有直接的控制方法。
`Delayed Frees`	用於ONTAP 效能的區塊、無法立即釋出。對於 SnapMirror 目的地、此列的值為 `0` 且不會顯示。	沒有直接的控制方法。
`File Operation Metadata`	保留給檔案作業中繼資料的空間總量。	沒有直接的控制方法。

`Total Footprint`	Volume 在本機層中使用的總空間量。這是所有列的總和。	用於減少磁碟區所用空間的任何方法。

相關資訊

"NetApp技術報告3483：NetApp SAN或IP SAN企業環境中的精簡配置"

判斷 **ONTAP** 本機層中的空間使用量

您可以檢視一或多個本機層中所有磁碟區使用的空間量，以便採取行動釋放更多空間。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

WAFL 會保留本機層級中繼資料和效能所需的磁碟空間總量百分比。用於維護本端層中磁碟區的空間來自 WAFL 保留區，無法變更。

在小於 30 TB 的本機層中， WAFL 保留了 10% 的磁碟空間，以供本機層級的中繼資料和效能使用。

從 ONTAP 9.12.1 開始，在 30 TB 或更大的本機階層中，用於本機層級中繼資料和效能的保留磁碟空間量將會減少，導致本機層級的可用空間增加 5% 。此空間節約的可用度會因您的平台和 ONTAP 版本而異。

由 **ONTAP** 在本機層中保留 **30 TB** 以上的磁碟空間	適用於平台	在 **ONTAP** 版本中
5%	所有 AFF 和 FAS 平台	ONTAP 9.14.1 及更新版本
5%	AFF 平台與 FAS500f 平台	更新版本ONTAP
10%	所有平台	更新版本ONTAP

您可以使用命令檢視一個或多個本機層中所有磁碟區的空間使用量 `aggregate show-space`。這有助於您瞭解哪些磁碟區佔用其包含的本機層中最大的空間，以便您採取行動釋放更多空間。

本機層中的已用空間會直接受到其所包含 FlexVol 磁碟區中所用空間的影響。增加磁碟區空間時所採取的措施，也會影響本機層的空間。

從 ONTAP 9.15.1 開始、有兩個新的中繼資料計數器可供使用。加上對多個現有計數器所做的變更、您可以更清楚地瞭解分配的使用者資料量。如需詳細資訊、請參閱 "判斷磁碟區或本機層的空間使用量" 。

下列資料列會包含在中 `aggregate show-space` 命令輸出：

- * Volume Footprints *

  本端層內所有磁碟區佔用空間的總計。它包含所有由包含本端層中所有磁碟區的所有資料和中繼資料所使用或保留的空間。

- * Aggregate中繼資料*

  本機層所需的檔案系統中繼資料總數，例如分配點陣圖和 inode 檔案。

- * Snapshot保留*

  根據磁碟區大小，保留給本機層快照的空間量。它被視為已用空間，無法用於 Volume 或本機層資料或中繼資料。

- * Snapshot保留不可用*

  原本分配給本機層快照保留區的空間量，因為與本機層相關聯的磁碟區正在使用，因此無法用於本機層快照。只有在具有非零本機層快照保留的本機層才會發生。

- 使用總數

  依磁碟區，中繼資料或快照，在本機層中使用或保留的所有空間總和。

- 實際使用總量

  目前用於資料的空間量（而非保留供未來使用）。包括本機層快照所使用的空間。

以下範例顯示 `aggregate show-space`快照保留為 5% 之本機層的命令輸出。如果快照保留為 0 ，則不會顯示該列。

```
cluster1::> storage aggregate show-space

                      Aggregate : wqa_gx106_aggr1

      Feature                                  Used      Used%
      --------------------------------    ----------     ------
      Volume Footprints                      101.0MB         0%
      Aggregate Metadata                       300KB         0%
      Snapshot Reserve                        5.98GB         5%

      Total Used                              6.07GB         5%
      Total Physical Used                    34.82KB         0%
```

相關資訊

- "知識庫文章：空間使用"
- "升級ONTAP 至更新版的更新版、即可釋放5%的儲存容量"
- "儲存聚合展示空間"

在 **HA** 配對中重新配置 **ONTAP** 本機層的擁有權

您可以在 HA 配對中的節點之間變更本機層的擁有權，而不會中斷本機層的服務。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

HA配對中的兩個節點均實體連線至彼此的磁碟或陣列LUN。每個磁碟或陣列LUN均由其中一個節點擁有。

當接管發生時，本機層內所有磁碟或陣列 LUN 的擁有權會暫時從一個節點變更為另一個節點。不過、本地層的重新配置作業也可能永久變更擁有權（例如、如果已完成負載平衡）。所有權會在不進行任何資料複製程序或實體移動磁碟或陣列LUN的情況下變更。

關於這項工作

- 由於磁碟區數限制是在本機層重新配置作業期間以程式設計方式驗證、因此不需要手動檢查。

  如果Volume數超過支援的上限、則本機層重新配置作業會失敗、並顯示相關的錯誤訊息。

- 當來源節點或目的地節點上的系統層級作業正在進行時、您不應該啟動本機層重新配置；同樣地、您也不應該在本機層重新配置期間啟動這些作業。

  這些作業包括：

  - 接管
  - GiveBack
  - 關機
  - 另一個本地層重新配置作業
  - 磁碟擁有權變更
  - 本機層級或磁碟區組態作業
  - 更換儲存控制器
  - 升級ONTAP
  - 還原ONTAP

- 如果您有MetroCluster 一個支援功能組態、則不應在災難恢復作業（_switchover、_rec修復_或_switchback）進行期間、啟動本機層重新配置。
- 如果您有MetroCluster 一個不穩定組態、並在交換式本機層上啟動本機層重新配置、則作業可能會失敗、因為它超過DR合作夥伴的Volume限制數。
- 您不應在毀損或正在進行維護的本機層上啟動本機層重新定位。
- 在初始化本機層重新配置之前、您應該先在來源和目的地節點上儲存任何核心傾印。

步驟

1. 檢視節點上的本機層，以確認要移動的本機層，並確保它們處於線上狀態且狀況良好：

   `storage aggregate show -node` *`source-node`*

   下列命令顯示叢集中四個節點上的六個本機層。所有本地層都在線上。node1和node3形成HA配對、Node2和Node4形成HA配對。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB    0% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB    0% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 發出命令以啟動本機層重新定位：

   `storage aggregate relocation start -aggregate-list` *`aggregate-1`*`, `*`aggregate-2`*`… -node` *`source-node`* `-destination` *`destination-node`*

   以下命令將本地層 agger_1 和 agger_2 從 Node1 移至 node3 。node3是Node1的HA合作夥伴。只能在 HA 配對中移動本機層。

```
cluster::> storage aggregate relocation start -aggregate-list aggr_1,
aggr_2 -node node1 -destination node3
Run the storage aggregate relocation show command to check relocation
status.
node1::storage aggregate>
```

3. 使用命令監控本地層重新定位的進度 `storage aggregate relocation show`：

   `storage aggregate relocation show -node` *`source-node`*

   以下命令顯示要移至 node3 的本地層的進度：

```
cluster::> storage aggregate relocation show -node node1
Source Aggregate   Destination    Relocation Status
------ ----------- -------------  ------------------------
node1
       aggr_1      node3          In progress, module: wafl
       aggr_2      node3          Not attempted yet
2 entries were displayed.
node1::storage aggregate>
```

重新定位完成後，此命令的輸出會顯示每個本機層的重新定位狀態為「 Done 」。

相關資訊

- "儲存聚合搬遷展示"
- "儲存聚合遷移開始"
- "儲存Aggregate顯示"

刪除 **ONTAP** 本機層

如果本機層上沒有磁碟區，您可以刪除本機層。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

命令會 `storage aggregate delete`刪除儲存本機層。如果本機層上有磁碟區，則命令會失敗。如果本機層附加了物件存放區，則除了刪除本機之外，命令也會刪除物件存放區中的物件。此命令不會變更物件存放區組態。

以下範例刪除名為「 aggr1 」的本機層：

```
> storage aggregate delete -aggregate aggr1
```

相關資訊

- "儲存聚合刪除"

用於本地層重新定位的 **ONTAP** 命令

有特定的 ONTAP 命令可在 HA 配對中重新定位本機層擁有權。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

如果您想要…	使用此命令…

啟動本機層重新定位程序	`storage aggregate relocation start`
監控本機層重新定位程序	`storage aggregate relocation show`

相關資訊

- "儲存聚合搬遷展示"
- "儲存聚合遷移開始"

用於管理本機階層的 **ONTAP** 命令

您可以使用 `storage aggregate`命令來管理您的本機階層。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

如果您想要...	使用此命令...
顯示所有 Flash Pool 本機層的快取大小	`storage aggregate show -fields hybrid-cache-size-total -hybrid-cache-size -total >0`
顯示本機層的磁碟資訊和狀態	`storage aggregate show-status`
依節點顯示備用磁碟	`storage aggregate show-spare-disks`
顯示叢集中的根本機階層	`storage aggregate show -has-mroot true`
顯示本機層的基本資訊和狀態	`storage aggregate show`
顯示在本機層中使用的儲存設備類型	`storage aggregate show -fields storage-type`
將本機層上線	`storage aggregate online`
刪除本機層	`storage aggregate delete`
將本機層置於受限狀態	`storage aggregate restrict`
重新命名本機層	`storage aggregate rename`
使本機層離線	`storage aggregate offline`

如果您想要...	使用此命令...
變更本機層的 RAID 類型	`storage aggregate modify -raidtype`

相關資訊

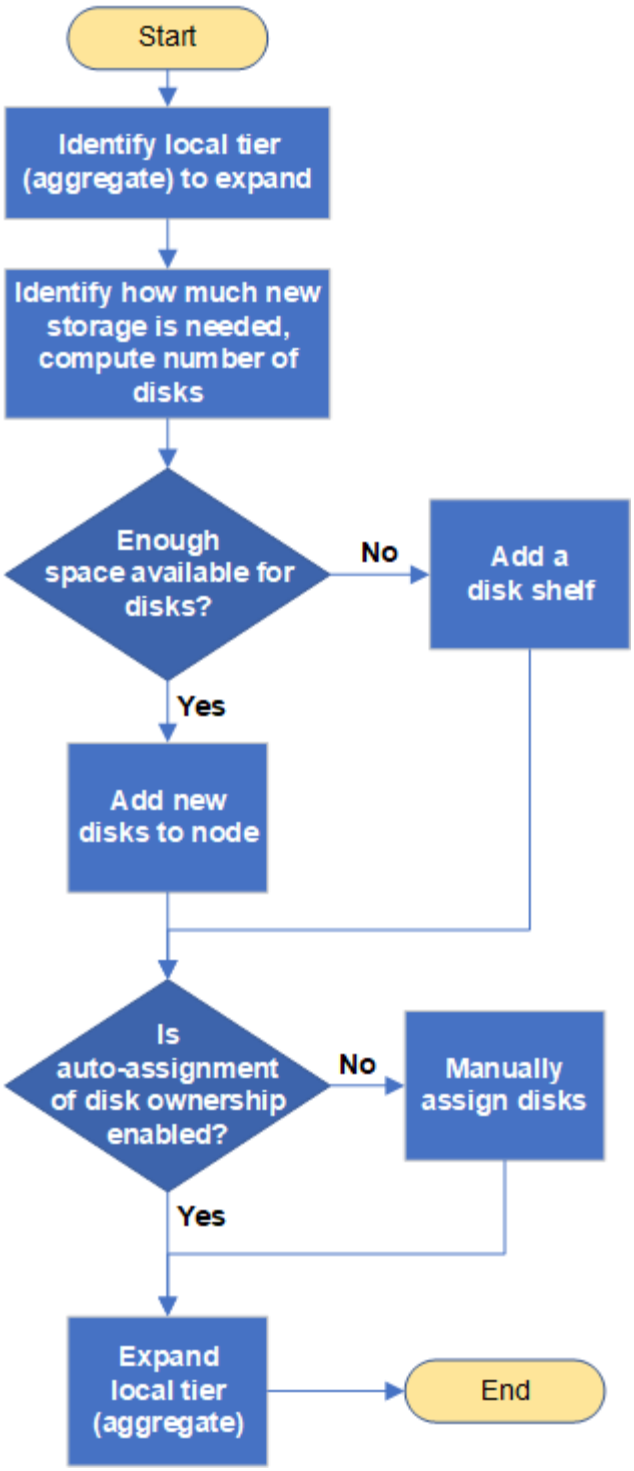
- "儲存聚合刪除"
- "儲存聚合修改"
- "儲存聚合離線"
- "儲存聚合在線"
- "儲存聚合重命名"
- "儲存聚合限制"
- "儲存Aggregate顯示"

將容量（磁碟）新增至本機層

將容量新增至 **ONTAP** 本機層的工作流程

若要將容量新增至本機層，您必須先識別要新增的本機層，判斷需要多少新儲存設備，安裝新磁碟，指派磁碟擁有權，並視需要建立新的 RAID 群組。

您可以使用系統管理員或 ONTAP CLI 來新增容量。



在 **ONTAP** 本機層中建立空間的方法

如果本機層的可用空間不足，可能會導致各種問題，從資料遺失到停用磁碟區保證。有多種方法可以在本機層中增加空間。

所有方法都會產生各種後果。在採取任何行動之前、您應閱讀文件中的相關章節。

以下是在本機層中騰出空間的一些常見方法、至少會造成大部分的後果：

- 將磁碟新增至本機層。

- 將部分磁碟區移至另一個具有可用空間的本機層。
- 縮減本機層中保證Volume大小的容量。
- 如果磁碟區的保證類型為「無」，請刪除不需要的磁碟區快照。
- 刪除不需要的Volume。
- 啟用空間節約功能、例如重複資料刪除或壓縮。
- （暫時）停用使用大量中繼資料的功能。

將容量新增至 **ONTAP** 本機層

您可以將磁碟新增至本機層，以便為其相關的磁碟區提供更多儲存空間。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

System Manager（ONTAP 版本號：NetApp 9.8及更新版本）

從《產品介紹》9.12開始ONTAP 、您可以使用System Manager檢視本機層的已認可容量、以判斷本機層是否需要額外容量。請參閱。 "監控System Manager中的容量"

步驟

1. 選擇 * 儲存 > Tiers* 。
2. 選取您要新增容量的本機層名稱旁的。
3. 選取 * 新增容量 * 。

如果沒有可新增的備用磁碟、則不會顯示「新增容量」選項、而且您無法增加本機層的容量。

4. 請根據ONTAP 安裝的版本執行下列步驟：

如果ONTAP 安裝此版本的lash…	執行下列步驟…
從ONTAP 功能上開始。9.11.1	a. 選取磁碟類型和磁碟數目。 b. 如果您要新增磁碟至新的RAID群組、請勾選核取方塊。 隨即顯示RAID分配。 c. 選擇*保存*。
ONTAP 9.10.1、9.9 或 9.8	a. 如果節點包含多個儲存層、請選取您要新增至本機層的磁碟數量。否則、如果節點只包含單一儲存層、則會自動預估新增的容量。 b. 選取*「Add*」 。

5. （選用）此程序需要一些時間才能完成。如果要在後臺運行該進程，請選擇*在後臺運行*。
6. 程序完成後、您可以在* Storage > Tiers*的本機層資訊中檢視增加的容量量。

系統管理程式**ONTAP** （僅限版本**9.7**及更早版本）

步驟

1. （僅適用於 ONTAP 9.7 ）選擇 * （返回經典版本） * 。
2. 選擇 * 硬體與診斷 > Aggregate * 。
3. 選取您要新增容量磁碟的本機層，然後選取 * 動作 > 新增容量 * 。

您應該新增與本機層中其他磁碟大小相同的磁碟。

4. （僅適用於 ONTAP 9.7 ）選擇 * 切換至新體驗 * 。
5. 選取 * 儲存 > Tiers* 以驗證新本機層的大小。

CLI

開始之前

您必須知道要新增儲存設備的本機層的 RAID 群組大小為何。

關於這項工作

將分割磁碟新增至本機層的程序類似於新增未分割磁碟的程序。

當您展開本機層時，您應該注意是否要將分割區或未分割磁碟新增至本機層。當您將未分割的磁碟機新增至現有的本機層時，新的 RAID 群組會繼承現有 RAID 群組的大小，這可能會影響所需的同位元磁碟數量。如果將未分割磁碟新增至由分割磁碟組成的RAID群組、則新磁碟會分割、留下未使用的備用磁碟分割。

在配置磁碟分割時、您必須確保在沒有磁碟機的情況下、不會將兩個磁碟分割區都保留為備援磁碟機的情況下離開節點。如果您這麼做、而且節點發生控制器中斷、可能無法提供有關問題的寶貴資訊（核心檔案）給技術支援人員。

步驟

1. 在擁有本機層的系統上顯示可用的備援儲存設備：

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

   您可以使用 `-is-disk-shared` 僅顯示分割磁碟機或僅顯示未分割磁碟機的參數。

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type     RPM Checksum         Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.2                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.3                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.4                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.8                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.9                      BSAS    7200 block           753.8GB
0B  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

2. 顯示本機層目前的 RAID 群組：

```
storage aggregate show-status <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                 Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ----------- ---- ----- ------ -------- --------
----------
     shared   1.0.10        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.5         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.6         0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.11        0   BSAS    7200  753.8GB  828.0GB
(normal)
     shared   1.0.0         0   BSAS    7200  753.8GB  828.0GB
(normal)
5 entries were displayed.
```

3. 模擬將儲存設備新增至Aggregate：

```
storage aggregate add-disks -aggregate <aggr_name> -diskcount
<number_of_disks_or_partitions> -simulate true
```

無需實際配置任何儲存設備、即可查看新增儲存設備的結果。如果模擬命令顯示任何警告、您可以調整命令並重複模擬。

```
cl1-s2::> storage aggregate add-disks -aggregate aggr_test
-diskcount 5 -simulate true

Disks would be added to aggregate "aggr_test" on node "cl1-s2" in
the
following manner:

First Plex

  RAID Group rg0, 5 disks (block checksum, raid_dp)
                                                        Usable
Physical
    Position   Disk                      Type           Size
Size
    ---------- ------------------------- ---------- --------
--------
    shared     1.11.4                    SSD         415.8GB
415.8GB
    shared     1.11.18                   SSD         415.8GB
415.8GB
    shared     1.11.19                   SSD         415.8GB
415.8GB
    shared     1.11.20                   SSD         415.8GB
415.8GB
    shared     1.11.21                   SSD         415.8GB
415.8GB

Aggregate capacity available for volume use would be increased by
1.83TB.
```

4. 將儲存設備新增至Aggregate：

```
storage aggregate add-disks -aggregate <aggr_name> -raidgroup new
-diskcount <number_of_disks_or_partitions>
```

建立 Flash Pool 本機層時，如果您要新增的磁碟與本機層的總和檢查碼不同，或者如果您要新增磁碟至混合式 Checksum 本機層，則必須使用此 `-checksumstyle`參數。

如果您要將磁碟新增至 Flash Pool 本機層，則必須使用 `-disktype`參數來指定磁碟類型。

您可以使用此 `-disksize`參數來指定要新增的磁碟大小。只會選取大小約為指定大小的磁碟來新增至本機層。

```
cl1-s2::> storage aggregate add-disks -aggregate data_1 -raidgroup
new -diskcount 5
```

5. 確認儲存設備已成功新增：

```
storage aggregate show-status -aggregate <aggr_name>
```

```
cl1-s2::> storage aggregate show-status -aggregate data_1

Owner Node: cl1-s2
 Aggregate: data_1 (online, raid_dp) (block checksums)
  Plex: /data_1/plex0 (online, normal, active, pool0)
   RAID Group /data_1/plex0/rg0 (normal, block checksums)
                                                                    Usable
Physical
     Position Disk                        Pool Type     RPM     Size
Size Status
     -------- --------------------------- ---- ----- ------ --------
-------- ----------
     shared   1.0.10                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.5                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.6                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.11                       0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.0                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.2                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.3                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.4                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.8                        0   BSAS    7200  753.8GB
828.0GB (normal)
     shared   1.0.9                        0   BSAS    7200  753.8GB
828.0GB (normal)
10 entries were displayed.
```

6. 確認節點仍有至少一個磁碟機、其中根分割區和資料分割區都是備援磁碟機：

```
storage aggregate show-spare-disks -original-owner <node_name>
```

```
cl1-s2::> storage aggregate show-spare-disks -original-owner cl1-s2
-is-disk-shared true

Original Owner: cl1-s2
 Pool0
  Shared HDD Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                       Type      RPM Checksum          Usable
Usable     Size Status
 -------------------------- ----- ------ -------------- --------
-------- -------- --------
 1.0.1                      BSAS    7200 block           753.8GB
73.89GB  828.0GB zeroed
 1.0.10                     BSAS    7200 block                0B
73.89GB  828.0GB zeroed
2 entries were displayed.
```

相關資訊

- "存儲聚合添加磁碟"
- "儲存聚合顯示備用磁碟"
- "儲存聚合顯示狀態"

將磁碟機新增至 **ONTAP** 節點或機櫃

您可以將磁碟機新增至節點或機櫃，以增加熱備援磁碟機的數量，或將空間新增至本機層。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

您的平台必須支援您要新增的磁碟機。您可以使用確認 "NetApp Hardware Universe"。

在單一程序中應新增的磁碟機數量下限為六個。新增單一磁碟機可能會降低效能。

NetApp Hardware Universe 的步驟

1. 在「 產品」 下拉式功能表中、選取您的硬體組態
2. 選擇您的平台。
3. 選擇您正在執行的 ONTAP 版本、然後選擇「顯示結果」 ** 。
4. 在圖形下方、選取 按一下此處以查看替代檢視 。選擇符合您組態的檢視。

安裝磁碟機的步驟

1. 請檢查 "NetApp 支援網站" 適用於較新的磁碟機和機櫃韌體、以及磁碟認證套件檔案。

   如果您的節點或機櫃沒有最新版本、請在安裝新磁碟機之前先進行更新。

   磁碟機韌體會在沒有目前韌體版本的新磁碟機上自動更新（不中斷營運）。

2. 請妥善接地。
3. 從平台正面輕移擋板。
4. 識別新磁碟機的正確插槽。

   新增磁碟機的正確插槽視平台機型和ONTAP 版本而定。在某些情況下、您需要依序將磁碟機新增至特定插槽。例如AFF 、在某個範例中、您可以在特定的時間間隔新增磁碟機、使叢集內的插槽閒置。而AFF 在功能不全的A220中、您可以將新的磁碟機新增至從外側到磁碟櫃中央的下一個空插槽。

   請參閱「開始使用前 ** 」中的步驟、以識別中的組態所需的正確插槽 "NetApp Hardware Universe"。

5. 插入新磁碟機：
   a. 在CAM握把處於開啟位置時、請用手插入新的磁碟機。
   b. 推動直到磁碟機停止。
   c. 合上CAM握把、讓磁碟機完全插入中間平面、並將握把卡入定位。請務必緩慢關閉CAM握把、使其與磁碟機正面正確對齊。
6. 確認磁碟機的活動LED（綠色）亮起。

   當磁碟機的活動LED持續亮起時、表示磁碟機已有電力。當磁碟機的活動LED燈在閃爍時、表示磁碟機已開機且I/O正在進行中。如果磁碟機韌體正在自動更新、LED會開始閃爍。

7. 若要新增其他磁碟機、請重複步驟4至6。

   新磁碟機必須指派給節點、才能被辨識。您可以手動指派新磁碟機、或者、如果ONTAP 您的節點遵循磁碟機自動指派的規則、您也可以等待更新以自動指派新磁碟機。

8. 在所有新磁碟機都被辨識之後、請確認已新增磁碟機、而且已正確指定其擁有權。

確認安裝的步驟

1. 顯示磁碟清單：

   ```
   storage aggregate show-spare-disks
   ```

   您應該會看到新的磁碟機、這些磁碟機屬於正確的節點。

2. （可選）（僅適用於 **ONTAP 9.3** 及更早版本）， 將新增的磁碟機歸零：

   ```
   storage disk zerospares
   ```

   先前在 ONTAP 本機層中使用的磁碟機必須先歸零，才能新增至另一個本機層。在更新版本的版本中、零位調整可能需要數小時才能完成、視節點中的非零位磁碟機大小而定ONTAP 。磁碟機零位調整現在可防止延遲、以便在需要快速增加本機層級的規模時使用。這在ONTAP 僅需數秒鐘的零磁碟機使用_fast零位調整功能進行零位化的情形下、在S得9.4或更新版本中並不是問題。

結果

新磁碟機已準備就緒。您可以將它們新增至本機層，將它們放入熱備援磁碟清單，或在建立新的本機層時新增它們。

相關資訊

- "儲存聚合顯示備用磁碟"
- "儲存磁碟 zerospares"

修正未對齊的 **ONTAP** 備用分割區

當您將分割磁碟新增至本機層時，您必須將具有根分割區和資料分割區的磁碟保留為每個節點的備用磁碟。如果您沒有、而且節點發生中斷、ONTAP 則無法將核心傾印到備用資料分割區。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

您必須在同一節點擁有的相同磁碟類型上、同時擁有備用資料分割區和備用根分割區。

步驟

1. 使用CLI顯示節點的備用磁碟分割：

   ```
   storage aggregate show-spare-disks -original-owner node_name
   ```

   請注意哪一個磁碟有備用資料分割區（備用資料分割區）、哪一個磁碟有備用根分割區（備用根分割區）。備用磁碟分割會在下顯示非零值 `Local Data Usable` 或 `Local Root Usable` 欄位。

2. 使用備用根分割區的磁碟、以備用資料分割區取代磁碟：

   ```
   storage disk replace -disk spare_data -replacement spare_root -action start
   ```

您可以從任一方向複製資料、不過複製根分割區所需的時間較短。

3. 監控磁碟更換進度：

   `storage aggregate show-status -aggregate` *`aggr_name`*

4. 更換作業完成後、再次顯示備用磁碟以確認您擁有完整的備用磁碟：

   `storage aggregate show-spare-disks -original-owner` *`node_name`*

   您應該會在「本機資料可用」和下看到可用空間的備用磁碟 `Local Root Usable`。

範例

您可以顯示節點C1-01的備用磁碟分割、並查看您的備用磁碟分割未對齊：

```
c1::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                               Local    Local
                                Data     Root  Physical
 Disk    Type   RPM Checksum Usable   Usable      Size
 ------- ----- ---- -------- ------- ------- --------
 1.0.1   BSAS  7200 block    753.8GB     0B   828.0GB
 1.0.10  BSAS  7200 block         0B 73.89GB  828.0GB
```

您可以開始磁碟更換工作：

```
c1::> storage disk replace -disk 1.0.1 -replacement 1.0.10 -action start
```

在等待更換作業完成時、您會顯示作業進度：

```
c1::> storage aggregate show-status -aggregate aggr0_1

Owner Node: c1-01
 Aggregate: aggr0_1 (online, raid_dp) (block checksums)
  Plex: /aggr0_1/plex0 (online, normal, active, pool0)
   RAID Group /aggr0_1/plex0/rg0 (normal, block checksums)
                                     Usable Physical
 Position Disk    Pool Type   RPM     Size     Size Status
 -------- ------- ---- ---- ----- -------- -------- ----------
 shared   1.0.1    0   BSAS  7200  73.89GB  828.0GB (replacing,copy in
progress)
 shared   1.0.10   0   BSAS  7200  73.89GB  828.0GB (copy 63% completed)
 shared   1.0.0    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.11   0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.6    0   BSAS  7200  73.89GB  828.0GB (normal)
 shared   1.0.5    0   BSAS  7200  73.89GB  828.0GB (normal)
```

更換作業完成後、請確認您擁有完整的備用磁碟：

```
ie2220::> storage aggregate show-spare-disks -original-owner c1-01

Original Owner: c1-01
 Pool0
  Shared HDD Spares
                              Local    Local
                               Data     Root  Physical
 Disk    Type    RPM Checksum Usable   Usable      Size
 ------ ----- ---- -------- -------- ------- --------
 1.0.1  BSAS  7200 block    753.8GB  73.89GB  828.0GB
```

相關資訊

- "儲存Aggregate顯示"
- "儲存磁碟更換"

管理磁碟

ONTAP 熱備援磁碟的運作方式

熱備援磁碟是指派給儲存系統的磁碟、已準備就緒可供使用、但未供RAID群組使用、且不保留任何資料。

如果RAID群組內發生磁碟故障、熱備援磁碟會自動指派給RAID群組、以取代故障磁碟。故障磁碟的資料會從RAID同位元檢查磁碟在背景的熱備援替換磁碟上重建。重建活動會登入 `/etc/message` 檔案和 AutoSupport 訊息隨即傳送。

如果可用的熱備援磁碟與故障磁碟的大小不同、則會選擇大小較大的磁碟、然後再縮減大小以符合所更換磁碟的大小。

多磁碟載體磁碟的備用需求

在多磁碟機中維持適當數量的磁碟備援、對於最佳化儲存備援、並將ONTAP 複製磁碟所需的時間降至最低、以達到最佳的磁碟配置、至關重要。

您必須隨時為多個磁碟機磁碟保留至少兩個熱備援磁碟。若要支援使用維護中心、並避免多個並行磁碟故障所造成的問題、您應至少保留四個熱備援磁碟、以確保穩定狀態運作、並立即更換故障磁碟。

如果兩個磁碟同時發生故障，且只有兩個可用的熱備用磁碟，則ONTAP可能無法將故障磁碟及其托架配對磁碟的內容交換到備用磁碟。這種情況稱為僵局。如果發生這種情況，您將透過 EMS 訊息和AutoSupport訊息收到通知。當有替代承運人可用時，您必須遵循 EMS 訊息提供的說明。欲了解更多信息，請參閱"NetApp知識庫：RAID 佈局無法自動修正 - AutoSupport訊息"

備援警示不足以協助您管理 **ONTAP** 備援磁碟

根據預設、如果您的熱備援磁碟機少於一個、且符合儲存系統中每個磁碟機的屬性、則會向主控台和記錄發出警告。

您可以變更這些警告訊息的臨界值、以確保系統遵循最佳實務做法。

關於這項工作

您應該將「min_spare _count'」RAID選項設定為「2」、以確保您始終擁有建議的最少備用磁碟數。

步驟

1. 將選項設為「2」：

```
storage raid-options modify -node nodename -name min_spare_count -value 2
```

相關資訊

- "儲存 raid 選項修改"

其他 **ONTAP** 根資料分割管理選項

啟動選單中提供了根資料分割區選項，該選項為配置為根資料分割區的磁碟提供了額外的管理功能。

下列管理功能可在「Boot Menu Option 9（開機功能表選項9）」下使用。

- 取消分割所有磁碟並移除其擁有權資訊

  如果您的系統設定為根資料分割、而且您需要以不同的組態重新初始化、則此選項很有用。

- *使用分割磁碟*來清除組態並初始化節點

  此選項適用於下列項目：

  - 您的系統未設定root資料分割、您想要將其設定為root資料分割

- 您的系統設定不正確、無法進行根資料分割、因此您必須加以修正
- 您有AFF 一個僅FAS 連接SSD的平台或是一個包含先前版本根資料分割的平台、您想要將其升級至較新版本的根資料分割區、以提高儲存效率

- *使用整個磁碟*來清除組態並初始化節點

  如果您需要：

  - 取消分割現有分割區
  - 移除本機磁碟擁有權
  - 使用RAID-DP以整個磁碟重新初始化您的系統

瞭解何時更新 **ONTAP** 磁碟資格認證套件

磁碟認證套件（DQP）新增對新合格磁碟機的完整支援。在更新磁碟機韌體或新增磁碟機類型或大小至叢集之前、您必須先更新「DQP」。最佳實務做法是定期更新DQP、例如每季或每半年更新一次。

您需要在下列情況下下下載並安裝DQP：

- 每當您新增磁碟機類型或大小至節點時

  例如、如果您已經有1 TB磁碟機並新增2 TB磁碟機、則必須檢查是否有最新的DQP更新。

- 每當您更新磁碟韌體時
- 只要有較新的磁碟韌體或DQP檔案可用
- 每當您升級ONTAP 至新版的更新版本時。

  不會在ONTAP 進行升級時更新DQP。

相關資訊

"NetApp下載：磁碟認證套件"

"NetApp下載：磁碟機韌體"

磁碟與分割擁有權

管理 **ONTAP** 磁碟和分割區的擁有權

您可以管理磁碟和分割區的擁有權。

您可以執行下列工作：

- **"顯示磁碟和分割區擁有權"**

  您可以檢視磁碟擁有權、以判斷哪個節點控制儲存設備。 您也可以在使用共用磁碟的系統上檢視磁碟分割擁有權。

- "變更自動指派磁碟擁有權的設定"

  您可以選取非預設原則來自動指派磁碟擁有權、或停用自動指派磁碟擁有權。

- "手動指派未分割磁碟的擁有權"

  如果叢集未設定為使用自動磁碟擁有權指派、則必須手動指派擁有權。

- "手動指派分割磁碟的擁有權"

  您可以手動或使用自動指派來設定容器磁碟或分割區的擁有權、就像對未分割磁碟一樣。

- "移除故障磁碟"

  由於完全故障的磁碟不再被ONTAP 視為可用的磁碟、因此您可以立即將磁碟從磁碟櫃中斷開。

- "移除磁碟的擁有權"

  將磁碟擁有權資訊寫入磁碟。ONTAP 從節點移除備用磁碟或其機櫃之前、您應該先移除其擁有權資訊、以便將其適當整合至其他節點。

瞭解 **ONTAP** 磁碟擁有權的自動指派

預設會啟用自動指派非擁有磁碟。自動磁碟擁有權指派會在 HA 配對初始化 10 分鐘後、在正常系統作業期間每五分鐘執行一次。

當您向 HA 對新增磁碟時（例如，更換故障磁碟、回應「備用磁碟不足」訊息或增加容量時），預設的自動指派原則會將磁碟的所有權指派給節點作為備用磁碟。

預設的自動指派原則是根據平台特定的特性、或是 DS460C 機櫃（如果 HA 配對只有這些機櫃）、並使用下列其中一種方法（原則）來指派磁碟擁有權：

指派方法	對節點指派的影響	預設為指派方法的平台組態
Bay	偶數的磁碟槽會指派給節點A、而零編號的磁碟槽則指派給節點B	HA 配對組態中的入門級系統與單一共用機櫃。
機櫃	磁碟櫃中的所有磁碟都會指派給節點A	HA 配對組態中的入門級系統、其中一個堆疊包含兩個或多個機櫃、而 MetroCluster 組態則包含每個節點一個堆疊、兩個或多個機櫃。
分割機櫃 此原則屬於的「預設」值 `-autoassign-policy` 的參數 `storage disk option` 適用平台與機櫃組態的命令。	機櫃左側的磁碟會指派給節點A、右側的磁碟則指派給節點BHA 配對上的部分機櫃從原廠出貨、磁碟會從機櫃邊緣移往中心。	大多數 AFF 平台和部分 MetroCluster 組態。

堆疊	堆疊中的所有磁碟都會指派給節點A	獨立式入門級系統及所有其他組態。
半抽屜 此原則屬於的「預設」值 `-autoassign-policy` 的參數 `storage disk option` 適用平台與機櫃組態的命令。	DS460C 抽屜（磁碟機支架 0 至 5 ）左半部的所有磁碟機都會指派給節點 A ；抽屜右半部的所有磁碟機（磁碟機支架 6 至 11 ）都會指派給節點 B 初始化僅有 DS460C 機櫃的 HA 配對時、不支援自動指派磁碟擁有權。您必須依照半抽屜原則、為包含根分割區的根 / 容器磁碟機的磁碟機手動指派擁有權。	HA 配對只能與 DS460C 機櫃配對、在 HA 配對初始化（開機）之後。 HA 配對開機後、會自動啟用磁碟擁有權的自動指派、並使用半抽屜原則將擁有權指派給其餘的磁碟機（根磁碟機 / 具有根分割區的容器磁碟機除外）、以及未來新增的任何磁碟機。 如果您的 HA 配對除了其他機櫃機型之外、還配備 DS460C 機櫃、則不會使用半抽屜原則。使用的預設原則是由平台特定特性所決定。

自動指派設定與修改：

- 您可以使用顯示目前的自動指派設定（開啟 / 關閉） `storage disk option show` 命令。
- 您可以使用停用自動指派 `storage disk option modify` 命令。
- 如果您的環境不需要預設的自動指派原則、您可以使用指定（變更）托架、機櫃或堆疊指派方法 `-autoassign-policy` 中的參數 `storage disk option modify` 命令。

  瞭解操作方法 "變更自動指派磁碟擁有權的設定"。

> ⓘ 半抽屜和分割架預設自動指派原則是唯一的、因為它們無法由使用者設定、例如 Bay 、機櫃和堆疊原則。

在進階磁碟分割（ ADP ）系統中、若要在半滿磁碟櫃上自動指派工作、磁碟機必須根據您擁有的磁碟櫃類型安裝在正確的機櫃中：

- 如果您的機櫃不是 DS460C 機櫃、請將磁碟機平均安裝在最左端、最右端則朝向中間移動。例如、 DS224C 機櫃的托架 0-5 中有六個磁碟機、而 DS224C 機櫃的托架 18-23 中則有六個磁碟機。
- 如果您的機櫃是 DS460C 機櫃、請在每個抽屜的前排（磁碟機支架 0 、 3 、 6 和 9 ）安裝磁碟機。對於其餘的磁碟機、請從正面到背面、在每個抽屜中平均分配它們。如果您沒有足夠的磁碟機來填滿列、請成對安裝、讓磁碟機平均地佔據抽屜的左右兩側。

  在每個抽屜的前排安裝磁碟機、可讓氣流正常、並防止過熱。

> ⓘ 如果磁碟機未安裝在半滿磁碟櫃上的正確機櫃托架中、則當容器磁碟機故障並更換時、 ONTAP 不會自動指派擁有權。在這種情況下、需要手動指派新的 Container 磁碟機。指派容器磁碟機的擁有權之後、 ONTAP 會自動處理任何必要的磁碟分割和分割指派。

在某些自動指派無法運作的情況下、您需要使用手動指派磁碟擁有權 `storage disk assign` 命令：

- 如果您停用自動指派、新磁碟必須手動指派給節點、才能作為備用磁碟使用。
- 如果您想要自動指派磁碟、而且您有多個堆疊或磁碟櫃必須擁有不同的擁有權、則必須在每個堆疊或磁碟櫃上手動指派一個磁碟、才能在每個堆疊或磁碟櫃上自動指派擁有權。
- 如果已啟用自動指派、且您手動將單一磁碟機指派給未在作用中原則中指定的節點、則自動指派會停止運作、並顯示EMS訊息。

瞭解操作方法 "手動指派未分割磁碟的磁碟擁有權"。

瞭解操作方法 "手動指派分割磁碟的磁碟擁有權"。

相關資訊

- "儲存磁碟分配"
- "儲存磁碟選項修改"
- "儲存磁碟選項顯示"

顯示 **ONTAP** 磁碟和磁碟分割擁有權

您可以檢視磁碟擁有權、以判斷哪個節點控制儲存設備。您也可以在使用共用磁碟的系統上檢視磁碟分割擁有權。

步驟

1. 顯示實體磁碟的擁有權：

   ```
   storage disk show -ownership
   ```

   ```
   cluster::> storage disk show -ownership
   Disk     Aggregate Home     Owner    DR Home  Home ID     Owner ID   DR
   Home ID  Reserver    Pool
   -------- --------- -------- -------- -------- ---------- -----------
   ----------- ----------- ------
   1.0.0    aggr0_2   node2    node2    -        2014941509 2014941509  -
   2014941509  Pool0
   1.0.1    aggr0_2   node2    node2    -        2014941509 2014941509  -
   2014941509  Pool0
   1.0.2    aggr0_1   node1    node1    -        2014941219 2014941219  -
   2014941219  Pool0
   1.0.3    -         node1    node1    -        2014941219 2014941219  -
   2014941219  Pool0
   ```

2. 如果您的系統使用共享磁碟、您可以顯示分割區擁有權：

   ```
   storage disk show -partition-ownership
   ```

```
cluster::> storage disk show -partition-ownership
                                Root                    Data
Container  Container
Disk     Aggregate Root Owner  Owner ID    Data Owner  Owner ID    Owner
Owner ID
-------- --------- ----------- ----------- ----------- -----------
---------- -----------
1.0.0    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.1    -         node1       1886742616  node1       1886742616  node1
1886742616
1.0.2    -         node2       1886742657  node2       1886742657  node2
1886742657
1.0.3    -         node2       1886742657  node2       1886742657  node2
1886742657
```

相關資訊

- "儲存磁碟顯示"

變更自動指派 **ONTAP** 磁碟擁有權的設定

您可以使用 `storage disk option modify` 命令以選取非預設原則、以自動指派磁碟擁有權或停用自動指派磁碟擁有權。

深入瞭解 "自動指派磁碟擁有權"。

關於這項工作

如果您只有 DS460C 機櫃的 HA 配對、則預設的自動指派原則為半抽屜。您無法變更為非預設原則（ Bay 、 stay 、 stack ）。

步驟

1. 修改自動磁碟指派：
   a. 如果您要選取非預設原則、請輸入：

      `storage disk option modify -autoassign-policy` *`autoassign_policy`* `-node` *`node_name`*

      - 使用 `stack` 做為 *`autoassign_policy`* 在堆疊或迴圈層級設定自動擁有權。
      - 使用 `shelf` 做為 *`autoassign_policy`* 在機櫃層級設定自動擁有權。
      - 使用 `bay` 做為 *`autoassign_policy`* 可在機櫃層級設定自動擁有權。

   b. 如果您要停用自動磁碟擁有權指派、請輸入：

      `storage disk option modify -autoassign off -node` *`node_name`*

2. 驗證磁碟的自動指派設定：

   `storage disk option show`

```
cluster1::> storage disk option show

Node           BKg. FW. Upd.  Auto Copy     Auto Assign    Auto
                                                          Assign Policy
-------------  -------------  ------------  -------------  --------
cluster1-1     on             on            on             default
cluster1-2     on             on            on             default
```

相關資訊

- "儲存磁碟選項修改"
- "儲存磁碟選項顯示"

手動指派未分割磁碟的 **ONTAP** 磁碟擁有權

如果您的 HA 配對未設定為使用自動磁碟擁有權指派、則必須手動指派擁有權。如果您正在初始化只有 DS460C 機櫃的 HA 配對、則必須手動指派根磁碟機的擁有權。

關於這項工作

- 如果您是在未初始化且不只有 DS460C 機櫃的 HA 配對中手動指派擁有權、請使用選項 1 。
- 如果您正在初始化只有 DS460C 機櫃的 HA 配對、請使用選項 2 手動指派根磁碟機的擁有權。

選項 **1** ：大多數 **HA** 配對

對於未初始化且不只有 DS460C 機櫃的 HA 配對、請使用此程序手動指派擁有權。

關於這項工作

- 您要指派擁有權的磁碟必須位於實體纜線連接至您要指派擁有權之節點的機櫃中。
- 如果您在本機層（ Aggregate ）中使用磁碟：
  - 磁碟必須由節點擁有、才能在本機層（Aggregate）中使用。
  - 您無法重新指派在本機層（ Aggregate ）中使用的磁碟擁有權。

步驟

1. 使用 CLI 顯示所有未擁有的磁碟：

   ```
   storage disk show -container-type unassigned
   ```

2. 指派每個磁碟：

   ```
   storage disk assign -disk disk_name -owner owner_name
   ```

   您可以使用萬用字元一次指派多個磁碟。如果您要重新指派已由不同節點擁有的備用磁碟、則必須使用「-force」選項。

選項 **2** ：只有 **DS460C** 機櫃的 **HA** 配對

對於正在初始化且只有 DS460C 機櫃的 HA 配對、請使用此程序手動指派根磁碟機的擁有權。

關於這項工作

- 當您初始化只有 DS460C 機櫃的 HA 配對時、必須手動指派根磁碟機、以符合半抽屜原則。

  HA 配對初始化（開機）之後，會自動啟用磁碟擁有權的自動指派，並使用半抽屜原則將擁有權指派給其餘磁碟機（根磁碟機除外），以及未來新增的任何磁碟機，例如更換故障磁碟，回應「低備援磁碟機」訊息或新增容量。

  "瞭解半抽屜式原則"。

- 對於 DS460C 機櫃中任何大於 8TB NL-SAS 磁碟機、每個 HA 配對（每個節點 5 個）至少需要 10 個磁碟機。

步驟

1. 如果您的 DS460C 機櫃未完全填入、請完成下列子步驟；否則、請前往下一步。

   a. 首先、在每個抽屜的前排（磁碟機支架 0 、 3 、 6 和 9 ）安裝磁碟機。

      在每個抽屜的前排安裝磁碟機、可讓氣流正常、並防止過熱。

   b. 對於其餘的磁碟機、請將其平均分配至每個抽屜。

      從正面到背面填充藥屜列。如果您沒有足夠的磁碟機來填滿列、請成對安裝、讓磁碟機平均地佔據抽屜的左右兩側。

      下圖顯示 DS460C 抽屜中的磁碟機支架編號和位置。

2. 使用節點管理 LIF 或叢集管理 LIF 登入叢集 Shell 。
3. 使用下列子步驟、手動指派每個藥屜中的根磁碟機、以符合半藥屜原則：

半抽屜原則可讓您將抽屜磁碟機（托架 0 至 5 ）的左半部分指派給節點 A 、而抽屜磁碟機（托架 6 至 11 ）的右半部分指派給節點 B

a. 顯示所有未擁有的磁碟：
   `storage disk show -container-type unassigned`

b. 指派根磁碟：
   `storage disk assign -disk disk_name -owner owner_name`

   您可以使用萬用字元一次指派多個磁碟。

如"指令參考資料ONTAP"需詳細 `storage disk`資訊，請參閱。

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"

手動指派 **ONTAP** 分割磁碟的擁有權

您可以手動指派容器磁碟或進階磁碟分割（ ADP ）系統上的分割區擁有權。如果您正在初始化只有 DS460C 機櫃的 HA 配對、則必須手動指派包含根分割區的容器磁碟機擁有權。

關於這項工作

- 您擁有的儲存系統類型決定支援哪種 ADP 方法、根資料（ RD ）或根資料（ RD2 ）。

  FAS 儲存系統使用 RD 和 AFF 儲存系統、使用 RD2 。

- 如果您是在未初始化且不只有 DS460C 機櫃的 HA 配對中手動指派擁有權、請使用選項 1 手動指派具有根資料（ RD ）分割區的磁碟、或使用選項 2 手動指派具有根資料（ RD2 ）分割區的磁碟。
- 如果您正在初始化只有 DS460C 機櫃的 HA 配對、請使用選項 3 手動指派擁有根分割區的容器磁碟機擁有權。

選項 **1** ：手動指派具有根資料（ **RD** ）分割區的磁碟

對於根資料分割、HA配對共有三個擁有實體（容器磁碟和兩個分割區）。

關於這項工作

- 只要所有容器磁碟和兩個分割區都是由HA配對中的其中一個節點所擁有、HA配對中的所有節點就不一定都需要由同一個節點擁有。但是，當您在本機層中使用分割區時，它必須屬於擁有本機層的同一個節點。
- 如果容器磁碟在半填入的機櫃中故障且已更換、您可能需要手動指派磁碟擁有權、因為在這種情況下、ONTAP 並不一定會自動指派擁有權。
- 指派容器磁碟之後， ONTAP 的軟體會自動處理任何必要的分割區和分割區指派。

步驟

1. 使用CLI顯示分割磁碟的目前擁有權：

   ```
   storage disk show -disk disk_name -partition-ownership
   ```

2. 將CLI權限等級設為進階：

   ```
   set -privilege advanced
   ```

3. 根據您要指派所有權的所有權實體、輸入適當的命令：

   如果任何所有權實體已擁有，則您必須納入 `-force`選項。

如果您要指派…的擁有權	使用此命令…
Container磁碟	`storage disk assign -disk disk_name -owner owner_name`
資料分割區	`storage disk assign -disk disk_name -owner owner_name -data true`
根分割區	`storage disk assign -disk disk_name -owner owner_name -root true`

選項 **2** ：手動指派具有根資料資料（ **RD2** ）分割區的磁碟

對於根資料資料分割、HA配對共有四個擁有實體（容器磁碟和三個分割區）。根資料資料分割會建立一個小型分割區做為根分割區、並建立兩個較大、大小相同的資料分割區。

關於這項工作

- 參數必須搭配命令使用 `disk assign`，才能指派根資料分割磁碟的正確分割區。這些參數無法搭配儲存資源池中的磁碟使用。預設值為 `false`。
  - 此參數會 `-data1 true`**指派** `data1` root-data1-data2 分割磁碟的分割區。
  - 此參數會 `-data2 true`**指派** `data2` root-data1-data2 分割磁碟的分割區。
- 如果容器磁碟在半填入的機櫃中故障且已更換、您可能需要手動指派磁碟擁有權、因為在這種情況下、ONTAP 並不一定會自動指派擁有權。
- 指派容器磁碟之後， ONTAP 的軟體會自動處理任何必要的分割區和分割區指派。

步驟

1. 使用CLI顯示分割磁碟的目前擁有權：

   ```
   storage disk show -disk disk_name -partition-ownership
   ```

2. 將CLI權限等級設為進階：

   ```
   set -privilege advanced
   ```

3. 根據您要指派所有權的所有權實體、輸入適當的命令：

   如果任何所有權實體已擁有，則您必須納入 `-force`選項。

如果您要指派…的擁有權	使用此命令…
Container磁碟	`storage disk assign -disk disk_name -owner owner_name`
Data1分割區	`storage disk assign -disk disk_name -owner owner_name -data1 true`
Data2 分割區	`storage disk assign -disk disk_name -owner owner_name -data2 true`
根分割區	`storage disk assign -disk disk_name -owner owner_name -root true`

選項 3 ：手動指派具有根分割區的 DS460C 容器磁碟機

如果您正在初始化只有 DS460C 機櫃的 HA 配對、則必須遵循半抽屜原則、手動指派具有根分割區的容器磁碟機擁有權。

關於這項工作

- 初始化僅有 DS460C 架的 HA 對時，ADP 啟動選單選項 9a 和 9b 不支援自動磁碟機所有權分配。您必須依照半抽屜原則、手動指派具有根分割區的容器磁碟機。

  HA 對初始化（啟動）後，將自動啟用磁碟所有權的自動分配，並使用半抽屜策略將所有權分配給剩餘驅動器（具有根分區的容器驅動器除外）以及將來添加的任何驅動器，例如更換故障驅動器、響應“備件不足”消息或增加容量。

- "瞭解半抽屜式原則"。

步驟

1. 如果您的 DS460C 機櫃未完全填入、請完成下列子步驟；否則、請前往下一步。

   a. 首先、在每個抽屜的前排（磁碟機支架 0 、 3 、 6 和 9 ）安裝磁碟機。

      在每個抽屜的前排安裝磁碟機、可讓氣流正常、並防止過熱。

   b. 對於其餘的磁碟機、請將其平均分配至每個抽屜。

      從正面到背面填充藥屜列。如果您沒有足夠的磁碟機來填滿列，請成對安裝，讓磁碟機平均地佔據抽屜的左右兩側。

      下圖顯示 DS460C 抽屜中的磁碟機支架編號和位置。

2. 使用節點管理 LIF 或叢集管理 LIF 登入叢集 Shell 。
3. 對於每個藥屜、請使用下列子步驟、依照半抽屜原則、手動指派具有根分割區的容器磁碟機：

   半抽屜原則可讓您將抽屜磁碟機（托架 0 至 5 ）的左半部分指派給節點 A ，而抽屜磁碟機（托架 6 至 11 ）的右半部分指派給節點 B

a. 顯示所有未擁有的磁碟：
   `storage disk show -container-type unassigned`

b. 指派具有根分割區的容器磁碟機：
   `storage disk assign -disk disk_name -owner owner_name`

   您可以使用萬用字元一次指派多個磁碟機。

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"

使用根資料分割在 **ONTAP** 節點上設定主動被動式組態

當HA配對設定為由原廠使用根資料分割時、資料分割區的擁有權會在配對中的兩個節點之間分割、以用於雙主動式組態。如果您想在主動被動式組態中使用 HA 配對，則必須先更新分割區擁有權，然後再建立資料本機層。

開始之前

- 您應該已經決定要將哪個節點做為主動節點、以及哪個節點將做為被動節點。
- 必須在HA配對上設定儲存容錯移轉。

關於這項工作

此工作會在兩個節點上執行：節點A和節點B

此程序適用於未從分割磁碟建立資料本機層的節點。

深入瞭解 "進階磁碟分割"。

步驟

所有命令都會在叢集Shell輸入。

1. 檢視資料分割區的目前擁有權：

   `storage aggregate show-spare-disks`

   輸出顯示一半的資料分割區是由一個節點擁有、一半由另一個節點擁有。所有的資料分割區都應該是備用的。

```
cluster1::> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
```

```
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                      BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                          Local
Local
                                                           Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
12 entries were displayed.
```

2. 輸入進階權限層級：

```
set advanced
```

3. 對於將成為被動節點的節點所擁有的每個資料分割區、請將其指派給主動節點：

   `storage disk assign -force -data true -owner active_node_name -disk disk_name`

   您不需要將分割區納入磁碟名稱中。

   您可以針對需要重新指派的每個資料分割區、輸入類似下列範例的命令：

   `storage disk assign -force -data true -owner cluster1-01 -disk 1.0.3`

4. 確認所有分割區都已指派給作用中節點。

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                  Local
Local
                                                                   Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.0                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                       BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                      BSAS    7200 block           753.8GB
0B  828.0GB
```

```
 1.0.11                        BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                              Local
Local
                                                               Data
Root Physical
 Disk                          Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                         BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

請注意、cluster1-02仍擁有備用根分割區。

5. 返回管理權限：

   ```
   set admin
   ```

6. 建立您的資料本機層，至少留下一個資料分割區做為備援：

   ```
   storage aggregate create new_aggr_name -diskcount number_of_partitions -node
   active_node_name
   ```

   資料本機層即會建立，並由作用中節點擁有。

相關資訊

- "儲存聚合創建"
- "儲存Aggregate顯示"
- "儲存磁碟分配"

使用 **root-data-data** 分割在 **ONTAP** 節點上設定主動被動式組態

當HA配對設定為由原廠使用根資料資料分割時、資料分割區的擁有權會在配對中的兩個節點之間分割、以用於雙主動式組態。如果您想在主動被動式組態中使用 HA 配對，則必須先更新分割區擁有權，然後再建立資料本機層。

開始之前

- 您應該已經決定要將哪個節點做為主動節點、以及哪個節點將做為被動節點。
- 必須在HA配對上設定儲存容錯移轉。

關於這項工作

此工作會在兩個節點上執行：節點A和節點B

此程序適用於未從分割磁碟建立資料本機層的節點。

深入瞭解 "進階磁碟分割"。

步驟

所有命令都是在叢集Shell輸入。

1. 檢視資料分割區的目前擁有權：

   `storage aggregate show-spare-disks -original-owner passive_node_name -fields local-usable-data1-size, local-usable-data2-size`

   輸出顯示一半的資料分割區是由一個節點擁有、一半由另一個節點擁有。所有的資料分割區都應該是備用的。

2. 輸入進階權限層級：

   `set advanced`

3. 對於將成為被動節點的節點所擁有的每個資料1分割區、請將其指派給主動節點：

   `storage disk assign -force -data1 -owner active_node_name -disk disk_name`

   您不需要將分割區納入磁碟名稱中

4. 對於將成為被動節點的節點所擁有的每個data2分割區、請將其指派給主動節點：

   `storage disk assign -force -data2 -owner active_node_name -disk disk_name`

   您不需要將分割區納入磁碟名稱中

5. 確認所有分割區都已指派給作用中節點：

   `storage aggregate show-spare-disks`

```
cluster1::*> storage aggregate show-spare-disks

Original Owner: cluster1-01
 Pool0
  Partitioned Spares
                                                                 Local
Local
                                                                  Data
Root Physical
 Disk                        Type      RPM Checksum         Usable
Usable     Size
 -------------------------- ----- ------ -------------- --------
```

```
-------- --------
 1.0.0                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.1                        BSAS    7200 block           753.8GB
73.89GB  828.0GB
 1.0.2                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.3                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.4                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.5                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.6                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.7                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.8                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.9                        BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.10                       BSAS    7200 block           753.8GB
0B  828.0GB
 1.0.11                       BSAS    7200 block           753.8GB
0B  828.0GB

Original Owner: cluster1-02
 Pool0
  Partitioned Spares
                                                             Local
Local
                                                              Data
Root Physical
 Disk                        Type     RPM Checksum         Usable
Usable     Size
 --------------------------- ----- ------ -------------- --------
-------- --------
 1.0.8                        BSAS    7200 block                0B
73.89GB  828.0GB
13 entries were displayed.
```

請注意、cluster1-02仍擁有備用根分割區。

6. 返回管理權限：

```
set admin
```

7. 建立您的資料Aggregate、至少保留一個資料分割區作為備用：

   `storage aggregate create new_aggr_name -diskcount number_of_partitions -node active_node_name`

   資料Aggregate會建立、並由作用中節點擁有。

8. 或者，您也可以使用 ONTAP 建議的本機層配置，其中包括 RAID 群組配置和備用數的最佳實務做法：

   `storage aggregate auto-provision`

相關資訊

- "儲存聚合自動配置"
- "儲存聚合創建"
- "儲存Aggregate顯示"
- "儲存磁碟分配"

從磁碟移除 **ONTAP** 擁有權

將磁碟擁有權資訊寫入磁碟。ONTAP從節點移除備用磁碟或其機櫃之前、您應該先移除其擁有權資訊、以便將其適當整合至其他節點。

如果磁碟已分割成根資料分割區、且您執行的是 ONTAP 9.10.1 或更新版本、請聯絡 NetApp 技術支援部門、以取得移除擁有權的協助。如需詳細資訊、請參閱 "知識庫文章：無法移除磁碟擁有者"。

開始之前

您要移除擁有權的磁碟必須符合下列需求：

- 它必須是備用磁碟。

  您無法移除在本機層中使用的磁碟擁有權。

- 它不能位於維護中心。
- 無法進行消毒。
- 它不能失敗。

  不需要移除故障磁碟的擁有權。

關於這項工作

如果您已啟用自動磁碟指派、ONTAP 則在從節點移除磁碟之前、可能會自動重新指派擁有權。因此、您必須停用自動擁有權指派、直到磁碟移除、然後重新啟用為止。

步驟

1. 如果磁碟擁有權自動指派已開啟、請使用CLI將其關閉：

   `storage disk option modify -node node_name -autoassign off`

2. 如有需要、請針對節點的HA合作夥伴重複上一個步驟。
3. 從磁碟移除軟體擁有權資訊：

   `storage disk removeowner disk_name`

   若要移除多個磁碟的擁有權資訊、請使用以逗號分隔的清單。

   範例：

   ```
   storage disk removeowner sys1:0a.23,sys1:0a.24,sys1:0a.25
   ```

4. 如果磁碟是針對根資料分割進行分割、而且您執行的是 ONTAP 9.9.1 或更早版本、請移除分割區的所有權：

   `storage disk removeowner -disk disk_name -root true`

   `storage disk removeowner -disk disk_name -data true`

   這兩個分割區不再由任何節點擁有。

5. 如果您先前關閉磁碟擁有權的自動指派、請在磁碟移除或重新指派之後將其開啟：

   `storage disk option modify -node node_name -autoassign on`

6. 如有需要、請針對節點的HA合作夥伴重複上一個步驟。

相關資訊

- "儲存磁碟選項修改"
- "儲存磁碟刪除擁有者"

移除故障的 **ONTAP** 磁碟

完全故障的磁碟不再被ONTAP 當成可用的磁碟、您可以立即從磁碟櫃中斷磁碟的連線。不過、您應該讓部分故障的磁碟保持連線足夠長的時間、以便快速RAID恢復程序完成。

關於這項工作

如果您是因為磁碟故障或產生過多錯誤訊息而移除磁碟、則不應在此或任何其他儲存系統中再次使用該磁碟。

步驟

1. 使用CLI尋找故障磁碟的磁碟ID：

   `storage disk show -broken`

   如果磁碟未出現在故障磁碟的清單中、可能是因為正在進行快速RAID恢復而導致部分故障。在這種情況下、您應該等到磁碟出現在故障磁碟清單中（這表示快速RAID恢復程序已完成）、再移除磁碟。

2. 判斷您要移除的磁碟實體位置：

```
storage disk set-led -action on -disk disk_name 2
```

磁碟正面的故障LED會亮起。

3. 依照磁碟櫃機型硬體指南中的指示、從磁碟櫃中取出磁碟。

相關資訊

- "儲存磁碟組主導"
- "儲存磁碟顯示"

磁碟資料抹除

瞭解 **ONTAP** 磁碟清理

磁碟資料抹除是透過覆寫具有指定位元組模式或隨機資料的磁碟或SSD、使原始資料無法恢復的實體資料抹除程序。使用資料抹除程序可確保沒有人能夠還原磁碟上的資料。

所有ONTAP 版本的功能均可透過nodesdro解除、並從ONTAP 維護模式的畫面顯示的畫面顯示為畫面9.6。

磁碟資料抹除程序會連續使用三個預設或使用者指定的位元組覆寫模式、每次作業最多可使用七個週期。每個週期都會重複隨機覆寫模式。

視磁碟容量、模式和週期數而定、此程序可能需要數小時的時間。清理工作會在背景執行。您可以啟動、停止及顯示消毒程序的狀態。消毒程序包含兩個階段：「格式化階段」和「複寫模式覆寫階段」。

格式化階段

針對格式化階段所執行的作業取決於要清理的磁碟類別、如下表所示：

磁碟類別	格式化階段作業
容量HDD	略過
高效能HDD	SCSI格式作業
SSD	SCSI資料抹除作業

模式覆寫階段

指定的覆寫模式會在指定的週期數內重複執行。

當清理程序完成時、指定的磁碟會處於消毒狀態。它們不會自動返回備用狀態。您必須先將已清理的磁碟還原至備援集區，才能將新的已清理磁碟新增至另一個本機層。

瞭解何時無法執行 **ONTAP** 磁碟清理

在這些情況下無法執行磁碟清理。

- HA配對中的系統在接管模式中不受支援。
- 由於易讀性或可寫入性問題而導致磁碟故障、因此無法執行此功能。
- 如果您使用隨機模式、一次無法在超過100個磁碟上執行。
- 陣列LUN不支援此功能。

如果 **ONTAP** 磁碟清理中斷，會發生什麼情況

如果使用者介入或停電等非預期事件中斷磁碟資料抹除、ONTAP 則會採取行動、將正在被消毒的磁碟還原至已知狀態、但您也必須採取行動、才能完成資料抹除程序。

磁碟資料抹除是一項長期執行的作業。如果消毒程序因停電、系統當機或手動介入而中斷、則必須從頭重複消毒程序。磁碟未指定為已消毒。

如果磁碟資料抹除的格式化階段中斷、ONTAP 則必須恢復中斷所毀損的任何磁碟。系統重新開機後、ONTAP 每小時一次、即可針對未完成資料抹除格式化階段的任何正在消毒的目標磁碟進行驗證。如果找到任何這樣的磁碟、ONTAP 則用支援還原磁碟。恢復方法取決於磁碟的類型。磁碟恢復後、您可以重新執行該磁碟上的清理程序；對於 HDD 、您可以使用 `-s` 可指定不再重複格式化階段的選項。

建立及備份 **ONTAP** 本機層的秘訣，其中包含要清理的資料

如果您要建立或備份本機層以包含可能需要清理的資料，請遵循一些簡單的準則，以縮短資料清理所需的時間。

- 請確定含有敏感資料的本機層級不超過所需的大小。

  如果容量大於所需容量、則需要更多時間、磁碟空間和頻寬來進行資料抹除。

- 當您備份含有敏感資料的本機層級時、請避免將其備份到也包含大量非敏感資料的本機層級。

  如此可減少在清除敏感資料之前、移動不敏感資料所需的資源。

清理 **ONTAP** 磁碟

清理磁碟可讓您從已停用或無法運作的系統上的磁碟或磁碟集移除資料、使資料永遠無法恢復。

有兩種方法可以使用CLI對磁碟進行資料抹除：

使用“ 維護模式 ” 命令清理磁碟

從功能支援支援的9.6開始ONTAP 、您可以在維護模式下執行磁碟資料抹除。

開始之前

- 磁碟不能是自我加密磁碟（SED）。

  您必須使用 `storage encryption disk sanitize` 用於清理 SED 的命令。

  "加密閒置的資料"

  如"指令參考資料ONTAP"需詳細 `storage encryption disk sanitize`資訊，請參閱。

步驟

1. 開機進入維護模式。
   a. 輸入結束目前的Shell `halt`。

      隨即顯示載入程式提示。

   b. 進入維護模式 `boot_ontap maint`。

      顯示部分資訊後、會顯示維護模式提示。

2. 如果您要清理的磁碟已分割、請取消分割每個磁碟：

   取消磁碟分割的命令僅在診斷層級可用，且只能在NetApp支援監督下執行。強烈建議您在繼續操作之前聯繫NetApp支援。您也可以參考"NetApp知識庫：如何在ONTAP中取消對備用磁碟機的分割區"

   ```
   disk unpartition <disk_name>
   ```

3. 清除指定的磁碟：

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-r]]] [-c <cycle_count>] <disk_list>
   ```

   切勿關閉節點的電源、中斷儲存連線、或是在清理時移除目標磁碟。如果在格式化階段中斷掃毒、則必須重新啟動格式化階段、並允許在磁碟經過消毒並準備好返回備用集區之前完成。如果您需要中止清理程序、可以使用來中止 `disk sanitize abort` 命令。如果指定的磁碟正在進行資料抹除的格式化階段、則在該階段完成之前不會發生中止。

   `-p` `<pattern1>` `-p` `<pattern2>` `-p` `<pattern3>`指定一個由一到三個使用者定義的十六進位位位元組覆寫模式的週期，可連續套用至正在進行清理的磁碟。預設模式為三次通過、第一次使用的是`0x55`、第二次使用的是`0xAA`、第三次使用的是`0x3c`。

`-r` 以隨機覆寫取代任何或所有 Pass 的模式覆寫。

`-c` `<cycle_count>`指定套用指定覆寫模式的次數。預設值為一個週期。最大值為七個週期。

`<disk_list>`指定要清理的備用磁碟 ID 的空間分隔清單。

4. 如有需要、請檢查磁碟清理程序的狀態：

   ```
   disk sanitize status [<disk_list>]
   ```

5. 在資料抹除程序完成後、將每個磁碟的磁碟恢復為備援狀態：

   ```
   disk sanitize release <disk_name>
   ```

6. 結束維護模式。

使用&#8220清理磁碟；節點和#8221；命令（所有ONTAP 版本均為9）

在節點上使用 nodesdesh 命令啟用磁碟清理功能之後，就無法停用該功能。

開始之前

- 磁碟必須是備用磁碟；它們必須由節點擁有，但不能用於本機層。

  如果磁碟已分割，則兩個磁碟分割都不能在本機層中使用。

- 磁碟不能是自我加密磁碟（SED）。

  您必須使用 `storage encryption disk sanitize` 用於清理 SED 的命令。

  "加密閒置的資料"

- 磁碟不能是儲存資源池的一部分。

步驟

1. 如果您要清理的磁碟已分割、請取消分割每個磁碟：

   取消磁碟分割的命令僅在診斷層級可用，且只能在NetApp支援監督下執行。強烈建議您在繼續操作之前聯繫**NetApp**支援。 您也可以參考"NetApp知識庫：如何在ONTAP中取消對備用磁碟機的分割區"。

   ```
   disk unpartition <disk_name>
   ```

2. 輸入要清理磁碟的節點節點節點的節點節點節點：

   ```
   system node run -node <node_name>
   ```

3. 啟用磁碟資料抹除：

   ```
   options licensed_feature.disk_sanitization.enable on
   ```

   系統會要求您確認命令、因為命令無法還原。

4. 切換至節點的進階權限層級：

   ```
   priv set advanced
   ```

5. 清除指定的磁碟：

   ```
   disk sanitize start [-p <pattern1>|-r [-p <pattern2>|-r [-p <pattern3>|-
   r]]] [-c <cycle_count>] <disk_list>
   ```

   請勿關閉節點電源、中斷儲存連線或移除目標
   磁碟正在進行掃毒。如果在格式化階段中斷清理、則會中斷格式化
   必須重新啟動階段、並允許在磁碟進行清理並準備就緒之前完成
   已返回備援集區。如果您需要中止清理程序、您可以使用磁碟清理來進行
   中止命令。如果指定的磁碟正在進行資料清理的格式化階段、則會執行
   在階段完成之前不會發生中止。

`-p <pattern1> -p <pattern2> -p <pattern3>`指定一個由一到三個使用者定義的十六進位位位元組覆寫模式的週期，可連續套用至正在進行清理的磁碟。預設模式為三次通過、第一次使用的是0x55、第二次使用的是0xAA、第三次使用的是0x3c。

`-r` 以隨機覆寫取代任何或所有 Pass 的模式覆寫。

`-c <cycle_count>`指定套用指定覆寫模式的次數。

預設值為一個週期。最大值為七個週期。

`<disk_list>`指定要清理的備用磁碟 ID 的空間分隔清單。

6. 若要檢查磁碟資料抹除程序的狀態：

   ```
   disk sanitize status [<disk_list>]
   ```

7. 在資料抹除程序完成後、將磁碟恢復為備援狀態：

   ```
   disk sanitize release <disk_name>
   ```

8. 返回nodesdro重 管理權限層級：

   ```
   priv set admin
   ```

9. 返回ONTAP 到CLI：

   ```
   exit
   ```

10. 確定所有磁碟是否都返回到備援狀態：

    ```
    storage aggregate show-spare-disks
    ```

如果…	然後…
所有已消毒的磁碟均列為備援磁碟	您已完成。磁碟已消毒且處於備援狀態。

部分已消毒的磁碟並未列為備援磁碟	完成下列步驟：
	a. 進入進階權限模式：
	`set -privilege advanced`
	b. 將未指派的已消毒磁碟指派給每個磁碟的適當節點：
	`storage disk assign -disk <disk_name> -owner <node_name>`
	c. 將每個磁碟的磁碟恢復為備援狀態：
	`storage disk unfail -disk <disk_name> -s -q`
	d. 返回管理模式：
	`set -privilege admin`

如"指令參考資料ONTAP"需詳細 `storage aggregate show-spare-disks`資訊，請參閱。

結果

指定的磁碟會經過消毒並指定為熱備援磁碟。已清理磁碟的序號會寫入 `/etc/log/sanitized_disks`。

指定磁碟的清理記錄會寫入，顯示每個磁碟上完成的內容 `/mroot/etc/log/sanitization.log`。

相關資訊

- "儲存Aggregate顯示"
- "儲存磁碟分配"
- "儲存磁碟未故障"
- "儲存加密磁碟清理"

用於管理磁碟的 **ONTAP** 命令

您可以使用 `storage disk` 和 `storage aggregate` 管理磁碟的命令。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

如果您想要…	使用此命令…
依擁有者顯示備用磁碟清單、包括分割磁碟	`storage aggregate show-spare-disks`

依本機層顯示磁碟 RAID 類型，目前使用狀況和 RAID 群組	`storage aggregate show-status`
顯示實體磁碟的 RAID 類型，目前使用狀況，本機層和 RAID 群組（包括備援磁碟）	`storage disk show -raid`
顯示故障磁碟的清單	`storage disk show -broken`
顯示磁碟的叢集前（節點）磁碟機名稱	`storage disk show -primary-paths` （進階）
照亮特定磁碟或磁碟櫃的LED	`storage disk set-led`
顯示特定磁碟的Checksum類型	`storage disk show -fields checksum-compatibility`
顯示所有備用磁碟的Checksum類型	`storage disk show -fields checksum-compatibility -container-type spare`
顯示磁碟連線與放置資訊	`storage disk show -fields disk,primary-port,secondary-name,secondary-port,shelf,bay`
顯示特定磁碟的叢集前磁碟名稱	`storage disk show -disk diskname -fields diskpathnames`
顯示維護中心的磁碟清單	`storage disk show -maintenance`
顯示SSD的耗損壽命	`storage disk show -ssd-wear`
取消共用磁碟的分割	`storage disk unpartition` （可在診斷層級取得）
將所有非零磁碟歸零	`storage disk zerospares`
停止在一或多個指定磁碟上進行中的資料抹除程序	`system node run -node nodename -command disk sanitize`
顯示儲存設備加密磁碟資訊	`storage encryption disk show`
從所有連結的金鑰管理伺服器擷取驗證金鑰	`security key-manager restore`

相關資訊

- "儲存Aggregate顯示"

- "儲存磁碟組主導"
- "儲存磁碟顯示"
- "儲存磁碟 zerospares"
- "儲存加密磁碟顯示"

用於顯示空間使用資訊的 **ONTAP** 命令

您可以使用 `storage aggregate`和 `volume`命令來查看本機層和磁碟區中的空間使用情況及其快照。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

若要顯示有關...的資訊	使用此命令...

本機層，包括已用空間和可用空間百分比，快照保留空間大小及其他空間使用資訊的詳細資料	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

磁碟和 RAID 群組在本機層中的使用方式，以及 RAID 狀態	`storage aggregate show-status`
如果刪除特定快照，將會回收的磁碟空間量	`volume snapshot compute-reclaimable`

Volume所使用的空間量	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

包含本機層中的磁碟區所使用的空間量	`volume show-footprint`

相關資訊

- "儲存Aggregate顯示"
- "儲存聚合展示空間"
- "儲存聚合顯示狀態"

用於顯示儲存櫃相關資訊的 **ONTAP** 命令

您可以使用 `storage shelf show` 顯示磁碟櫃組態和錯誤資訊的命令。

如果您要顯示...	使用此命令...
機櫃組態和硬體狀態的一般資訊	`storage shelf show`
特定機櫃的詳細資訊、包括堆疊ID	`storage shelf show -shelf`
未解決、客戶可據以行動、依機櫃錯誤	`storage shelf show -errors`
Bay資訊	`storage shelf show -bay`
連線資訊	`storage shelf show -connectivity`
冷卻資訊、包括溫度感測器和冷卻風扇	`storage shelf show -cooling`
I/O模組的相關資訊	`storage shelf show -module`
連接埠資訊	`storage shelf show -port`
電源資訊、包括PSU（電源供應器單元）、電流感測器和電壓感測器	`storage shelf show -power`

相關資訊

- "倉儲貨架展示"

管理RAID組態

ONTAP 本機層的預設 RAID 原則

RAID-DP 或 RAID-TEC 是所有新本機層的預設 RAID 原則。RAID原則可決定當磁碟故障時所擁有的同位元檢查保護。

RAID-DP可在單一或雙磁碟故障時提供雙同位元檢查保護。RAID-DP 是下列本機層類型的預設 RAID 原則：

- 所有Flash本機層級
- Flash Pool本機層級
- 高效能硬碟（HDD）本機層級

支援所有磁碟類型和所有平台的支援、RAID-TEC AFF 包括包含較大磁碟的本機層級、可能會發生並行磁碟故障。支援三倍同位元檢查保護、讓資料能夠同時發生三次磁碟故障、進而協助降低此風險。RAID-TEC對於容量為6 TB或更大磁碟的HDD本機層、預設的RAID原則為。RAID-TEC

每種RAID原則類型都需要最低數量的磁碟：

- RAID-DP：至少5個磁碟
- 作業系統：至少7個磁碟RAID-TEC

磁碟的 **ONTAP RAID** 保護層級

ONTAP 支援三種層級的本機層級 RAID 保護。RAID保護層級決定了磁碟故障時、可用於資料恢復的同位元檢查磁碟數量。

有了RAID保護、如果RAID群組中有資料磁碟故障、ONTAP 則可將故障磁碟更換為備用磁碟、並使用同位元檢查資料來重建故障磁碟的資料。

- * RAID4*

  利用RAID4保護功能、ONTAP 即可在RAID群組中使用一個備用磁碟來取代和重建故障磁碟的資料。

- * RAID-DP *

  藉由RAID-DP保護、ONTAP 多達兩個備用磁碟可取代及重建RAID群組內最多兩個同時故障磁碟的資料。

- 《》RAID-TEC

  利用支援功能、支援使用多達三個備用磁碟、從RAID群組中最多三個同時故障的磁碟來取代和重建資料。RAID-TEC ONTAP

ONTAP 本機層的磁碟機和 **RAID** 群組資訊

有些本機層管理工作需要您知道哪些類型的磁碟機組成本機層，其大小，總和檢查碼和狀態，是否與其他本機層共用，以及 RAID 群組的大小和組成。

步驟

1. 依 RAID 群組顯示本機層的磁碟機：

   `storage aggregate show-status` *`aggr_name`*

   本機層中的每個 RAID 群組都會顯示磁碟機。

   您可以在中看到磁碟機的 RAID 類型（資料、同位元檢查、同位元檢查） `Position` 欄位。如果是 `Position` 隨即顯示欄 `shared`然後共用磁碟機：如果是 HDD 、則是分割磁碟；如果是 SSD 、則是儲存池的一部分。

```
cluster1::> storage aggregate show-status nodeA_fp_1

Owner Node: cluster1-a
 Aggregate: nodeA_fp_1 (online, mixed_raid_type, hybrid) (block checksums)
  Plex: /nodeA_fp_1/plex0 (online, normal, active, pool0)
   RAID Group /nodeA_fp_1/plex0/rg0 (normal, block checksums, raid_dp)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.1        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.3        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.5        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.7        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.9        0   SAS    10000  472.9GB  547.1GB (normal)
     shared   2.0.11       0   SAS    10000  472.9GB  547.1GB (normal)

   RAID Group /nodeA_flashpool_1/plex0/rg1
   (normal, block checksums, raid4) (Storage Pool: SmallSP)

                                                    Usable Physical
     Position Disk        Pool Type     RPM     Size     Size Status
     -------- ---------- ---- ----- ------ -------- -------- -------
     shared   2.0.13       0   SSD       -  186.2GB  745.2GB (normal)
     shared   2.0.12       0   SSD       -  186.2GB  745.2GB (normal)

8 entries were displayed.
```

相關資訊

- "儲存聚合顯示狀態"

從 **ONTAP RAID-DP** 轉換為 **RAID-TEC**

如果您想要增加三同位元檢查的保護、可以從RAID-DP轉換為RAID-TEC如果本機層中使用的磁碟大小大於 4 TiB ，則建議使用 RAID-TEC 。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

要轉換的本機層必須至少有七個磁碟。

關於這項工作

- 硬碟機（HDD）本機層可從RAID-DP轉換為RAID-TEC這包括Flash Pool本機層中的HDD層級。

對於快閃記憶體池 / 混合聚合，需要使用 **-disktype** 參數來變更每個磁碟類型的流程

[-T, -disktype {ATA | BSAS | FCAL | FSAS | LUN | MSATA | SAS | SSD | VMDISK | SSD-NVM | SSD-CAP | SSD-ZNS | VMLUN | VMLUN-SSD}] - 磁碟類型

此參數指定要修改的 RAID 群組的磁碟類型。對於 Flash Pool，它可以指定 HDD 層或 SSD 層。如果 HDD 層由多種類型的磁碟組成，則指定其中任何一種正在使用的磁碟類型都會導致該層被修改。如果目前 Aggregate RAID 類型為 mixed_raid_type，則此參數為必填項。

步驟

1. 確認本機層已上線，且至少有六個磁碟：

   ```
   storage aggregate show-status -aggregate aggregate_name
   ```

2. 將本機層從 RAID-DP 轉換為 RAID-TEC ：

   ```
   storage aggregate modify -aggregate aggregate_name -raidtype raid_tec
   ```

3. 驗證本機層 RAID 原則是否為 RAID-TEC ：

   ```
   storage aggregate show aggregate_name
   ```

相關資訊

- "儲存聚合修改"
- "儲存聚合顯示狀態"

從 **ONTAP RAID-TEC** 轉換為 **RAID-DP**

如果您減少本機層的大小，而不再需要三同位元檢查，您可以將 RAID 原則從 RAID-TEC 轉換為 RAID-DP ，並減少 RAID 同位檢查所需的磁碟數量。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

支援的最大RAID群組大小RAID-TEC 大於RAID-DP的最大RAID群組大小。如果最大RAID-TEC 的元組大小不在RAID-DP限制之內、您將無法轉換為RAID-DP。

關於這項工作

若要瞭解在 RAID 類型之間轉換的影響、請參閱 "參數" 以取得 `storage aggregate modify` 命令。

步驟

1. 確認本機層已上線，且至少有六個磁碟：

   ```
   storage aggregate show-status -aggregate aggregate_name
   ```

2. 將本機層從 RAID-TEC 轉換為 RAID-DP ：

   ```
   storage aggregate modify -aggregate aggregate_name -raidtype raid_dp
   ```

3. 驗證本機層 RAID 原則是否為 RAID-DP ：

   ```
   storage aggregate show aggregate_name
   ```

相關資訊

- "儲存聚合修改"
- "儲存聚合顯示狀態"

調整 **ONTAP RAID** 群組規模的考量事項

若要設定最佳的RAID群組大小、必須權衡各種因素。您必須決定哪些因素（例如RAID重建速度、保證不會因磁碟機故障而導致資料遺失、最佳化I/O效能、以及最大化資料儲存空間）、對於您正在設定的（本機層）集合體而言最為重要。

當您建立較大的RAID群組時、您可以將資料儲存空間最大化、使用於同位元檢查的相同儲存容量（也稱為「同位元稅金」）。另一方面、當磁碟在較大的RAID群組中故障時、重建時間會增加、影響效能的時間會延長。此外、在RAID群組中擁有更多磁碟、也會增加同一個RAID群組中多個磁碟故障的可能性。

HDD或陣列**LUN RAID**群組

當您調整由HDD或陣列LUN組成的RAID群組時、應遵循下列準則：

- 本機層（Aggregate）中的所有RAID群組應有相同數量的磁碟。

  雖然您在一個本機層上的磁碟數量最多可比不同RAID群組中的磁碟數量少50%或以上、但在某些情況下、這可能會導致效能瓶頸、因此最好避免。

- 建議的RAID群組磁碟編號範圍介於12到20之間。

  如果需要、效能磁碟的可靠性可支援最多28個RAID群組大小。

- 如果您可以使用多個RAID群組磁碟編號來滿足前兩項準則、則應該選擇較多的磁碟。

Flash Pool本機層（**Aggregate**）中的**SSD RAID**群組

SSD RAID群組大小可以不同於Flash Pool本機層（Aggregate）中HDD RAID群組的RAID群組大小。通常、您應該確保Flash Pool本機層只有一個SSD RAID群組、以盡量減少同位元檢查所需的SSD數量。

SSD本機層（**Aggregate**）中的**SSD RAID**群組

在調整由SSD組成的RAID群組規模時、您應該遵循下列準則：

- 本機層（Aggregate）中的所有RAID群組應有類似數量的磁碟機。

  RAID群組的大小不一定完全相同、但您應該避免在相同的本機層中、有任何RAID群組大小小於其他RAID群組大小的一半。

- 對於RAID-DP、建議的RAID群組大小範圍介於20到28之間。

您可以自訂 RAID 群組的大小，以確保 RAID 群組大小適合您計畫在本機層中包含的儲存容量。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

關於這項工作

對於標準本機層，您可以分別變更每個本機層的 RAID 群組大小。對於Flash Pool本機層級、您可以獨立變更SSD RAID群組和HDD RAID群組的RAID群組大小。

下列清單概述變更RAID群組大小的一些事實：

- 根據預設、如果最近建立的RAID群組中的磁碟或陣列LUN數量少於新的RAID群組大小、磁碟或陣列LUN將會新增至最近建立的RAID群組、直到達到新的大小為止。
- 除非您明確新增磁碟到該本機層中的所有其他現有RAID群組、否則它們的大小都會維持不變。
- 您絕不能讓RAID群組大於本機層目前的最大RAID群組大小。
- 您無法減少已建立的RAID群組大小。
- 新的大小適用於該本機層中的所有RAID群組（若為Flash Pool本機層、則適用於受影響RAID群組類型（SSD或HDD）的所有RAID群組）。

步驟

1. 使用適用的命令：

如果您想要…	輸入下列命令…
變更 Flash Pool 本機層的 SSD RAID 群組的最大 RAID 群組大小	`storage aggregate modify -aggregate aggr_name -cache-raid-group-size size`
變更任何其他RAID群組的最大大小	`storage aggregate modify -aggregate aggr_name -maxraidsize size`

範例

下列命令可將本機層 n1_A4 的最大 RAID 群組大小變更為 20 個磁碟或陣列 LUN ：

```
storage aggregate modify -aggregate n1_a4 -maxraidsize 20
```

下列命令可將 Flash Pool 本機層 n1_cache_A2 的 SSD 快取 RAID 群組大小上限變更為 24 ：

```
storage aggregate modify -aggregate n1_cache_a2 -cache-raid-group-size 24
```

相關資訊

- "儲存聚合修改"

管理 **Flash Pool** 本機層

Flash Pool ONTAP 本機層快取原則

Flash Pool 本機層中磁碟區的快取原則可讓您將 Flash 部署為高效能快取，以用於工作資料集，同時使用成本較低的 HDD 來處理較不常存取的資料。如果您要將快取提供給兩個以上的Flash Pool本機層、則應該使用Flash Pool SSD分割區、在Flash Pool的本機層級之間共用SSD。

快取原則會套用至位於Flash Pool本機層的磁碟區。您應該先瞭解快取原則的運作方式、再進行變更。

在大多數情況下，的預設快取原則 `auto`是要使用的最佳快取原則。只有在不同的原則為您的工作負載提供更好的效能時、才應該變更快取原則。設定錯誤的快取原則可能會嚴重降低磁碟區效能、效能降級可能會隨著時間逐漸增加。

快取原則結合了讀取快取原則和寫入快取原則。原則名稱會串連讀取快取原則和寫入快取原則的名稱、並以連字號分隔。如果原則名稱中沒有連字號，則寫入快取原則為 `none`，原則除外 `auto`。

除了HDD上儲存的資料、讀取快取原則也會在快取中放置資料複本、以最佳化未來的讀取效能。對於將資料插入快取以進行寫入作業的讀取快取原則、快取會以寫入快取的形式運作。

使用寫入快取原則插入快取的資料僅存在於快取中、HDD中沒有複本。Flash Pool快取受到RAID保護。啟用寫入快取可讓寫入作業中的資料立即從快取讀取、同時將資料延後寫入HDD、直到資料逾時離開快取為止。

如果您將磁碟區從 Flash Pool 本機層移至單一層本機層，它會遺失其快取原則；如果您稍後將其移回 Flash Pool 本機層，則會將預設的快取原則指派給該磁碟區 `auto`。如果您在兩個Flash Pool本機層之間移動磁碟區、快取原則會保留下來。

變更快取原則

您可以使用 CLI 來變更位於 Flash Pool 本機層的磁碟區快取原則 `-caching-policy` 參數 `volume create` 命令。

當您在 Flash Pool 本機層上建立磁碟區時，預設 `auto`會將快取原則指派給該磁碟區。

管理**Flash Pool**快取原則

判斷是否要修改 **Flash Pool** 本機層的 **ONTAP** 快取原則

您可以將快取保留原則指派給 Flash Pool 本機層中的磁碟區，以決定磁碟區資料在 Flash Pool 快取中保留的時間長度。不過、在某些情況下、變更快取保留原則可能不會影響磁碟區資料保留在快取中的時間量。

關於這項工作

如果您的資料符合下列任一條件、變更快取保留原則可能不會造成影響：

- 您的工作負載是連續的。
- 您的工作負載不會重新讀取固態硬碟（SSD）中快取的隨機區塊。
- 磁碟區的快取大小太小。

步驟

下列步驟會檢查資料必須符合的條件。工作必須在進階權限模式下使用CLI來完成。

1. 使用CLI檢視工作負載Volume：

   ```
   statistics start -object workload_volume
   ```

2. 判斷Volume的工作負載模式：

   ```
   statistics show -object workload_volume -instance volume-workload -counter
   sequential_reads
   ```

3. 判斷Volume的命中率：

   ```
   statistics show -object wafl_hya_vvol -instance volume -counter
   read_ops_replaced_percent|wc_write_blks_overwritten_percent
   ```

4. 確定 `Cacheable Read` 和 `Project Cache Alloc` 磁碟區數量：

   ```
   system node run -node node_name wafl awa start aggr_name
   ```

5. 顯示AWA摘要：

   ```
   system node run -node node_name wafl awa print aggr_name
   ```

6. 將 Volume 的命中率與進行比較 `Cacheable Read`。

   如果 Volume 的命中率大於 `Cacheable Read`然後、您的工作負載不會重新讀取 SSD 中快取的隨機區塊。

7. 比較磁碟區目前的快取大小與 `Project Cache Alloc`。

   如果磁碟區目前的快取大小大於 `Project Cache Alloc`，則您的磁碟區快取大小太小。

相關資訊

- "統計數據顯示"
- "統計開始"

修改 **ONTAP Flash Pool** 本機層的快取原則

只有在預期不同的快取原則能提供更好的效能時、才應該修改磁碟區的快取原則。您可以修改 Flash Pool 本機層上磁碟區的快取原則。

開始之前

您必須判斷是否要修改快取原則。

關於這項工作

在大多數情況下，的預設快取原則 `auto`是您可以使用的最佳快取原則。只有在不同的原則為您的工作負載提供更好的效能時、才應該變更快取原則。設定錯誤的快取原則可能會嚴重降低磁碟區效能、效能降級可能會隨著時間逐漸增加。修改快取原則時、請務必謹慎。如果您在某個已變更快取原則的磁碟區上遇到效能問題，您應該將快取原則傳回 `auto`。

步驟

1. 使用CLI修改磁碟區的快取原則：

   ```
   volume modify -volume volume_name -caching-policy policy_name
   ```

範例

以下範例修改命名為原則 `none`之磁碟區的快取原則 `vol2`：

```
volume modify -volume vol2 -caching-policy none
```

設定 **ONTAP Flash Pool** 本機層的快取保留原則

您可以將快取保留原則指派給 Flash Pool 本機層中的磁碟區。具有高快取保留原則的磁碟區中的資料會保留在快取中的時間更長、而具有低快取保留原則的磁碟區中的資料會更快移除。如此可讓高優先順序的資訊以更快的速度存取更長的時間、進而提升關鍵工作負載的效能。

開始之前

您應該知道您的系統是否有任何可能妨礙快取保留原則影響資料保留在快取中的時間長度的情況。

步驟

以進階權限模式使用CLI執行下列步驟：

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 驗證磁碟區的快取保留原則：

   根據預設、快取保留原則為「正常」。

3. 設定快取保留原則：

   ```
   volume modify -volume volume_name -vserver vserver_name -caching-policy
   policy_name
   ```

4. 確認磁碟區的快取保留原則已變更為您選取的選項。
5. 將權限設定傳回給admin：

   ```
   set -privilege admin
   ```

使用儲存池的 **ONTAP Flash Pool** 本機層的 **Flash Pool SSD** 分割區

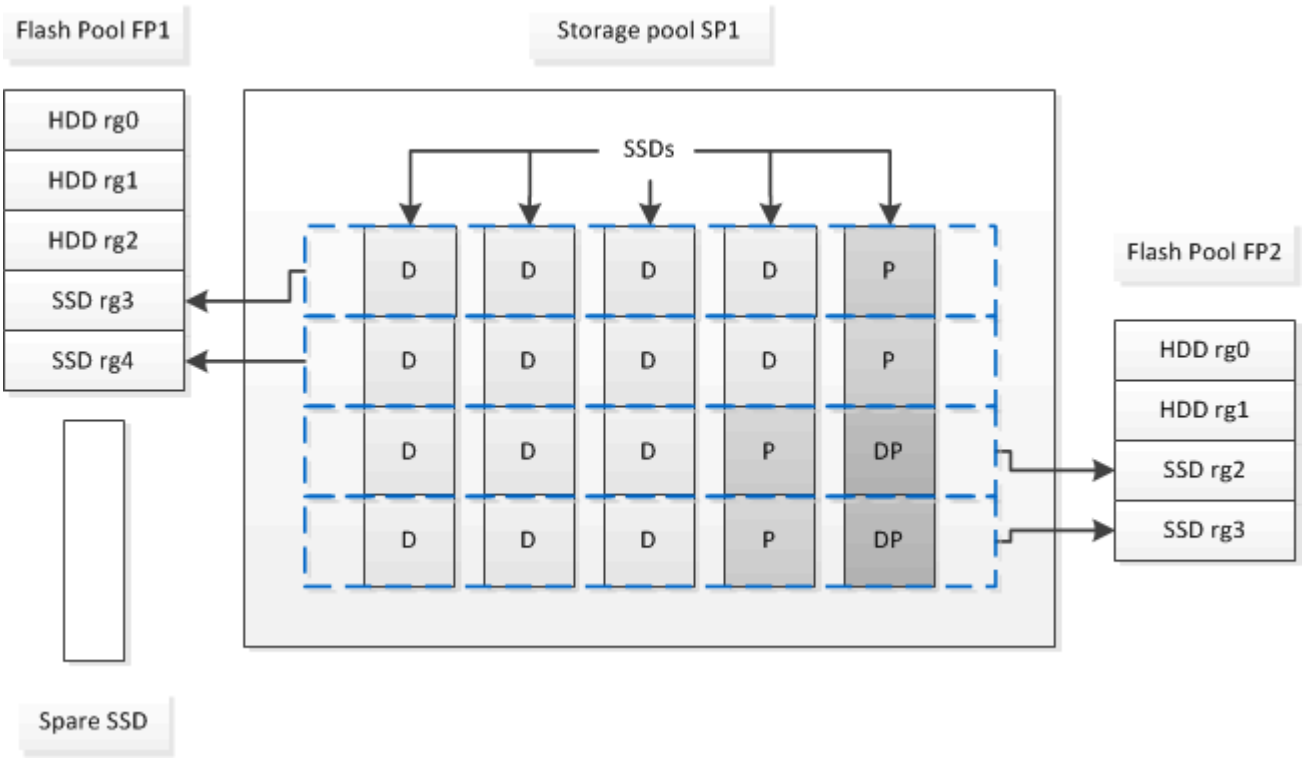
如果您要為兩個以上的 Flash Pool 本機層提供快取，則應該使用 Flash Pool 固態硬碟（ SSD ）分割區。Flash Pool SSD分割區可讓使用Flash Pool的所有本機層共享SSD。如此可將同位元的成本分散於多個本機層、提高SSD快取配置的靈活度、並將SSD效能最大化。

若要在Flash Pool本機層中使用SSD、SSD必須放置在儲存資源池中。您無法在儲存資源池中使用已分割為根資料分割的SSD。將SSD放入儲存資源池之後、SSD就無法再以獨立磁碟的形式進行管理、除非您銷毀與Flash資源池相關的本機層、並銷毀儲存資源池、否則將無法從儲存資源池中移除SSD。

SSD儲存資源池分為四個等量分配單元。新增至儲存資源池的SSD分為四個分割區、四個分配單元各指派一個分割區。儲存資源池中的SSD必須由同一個HA配對擁有。根據預設、HA配對中的每個節點都會指派兩個配置單元。分配單位必須由擁有其所服務之本機層的節點所擁有。如果其中一個節點上的本機層需要更多Flash快取、則可以移轉預設的配置單位數量、以減少一個節點上的數量、並增加合作夥伴節點上的數量。

您可以使用備用SSD來新增至SSD儲存資源池。如果儲存資源池為HA配對中兩個節點所擁有的Flash資源池本機層提供分配單元、則備用SSD可由任一節點擁有。不過、如果儲存資源池僅提供分配單元給HA配對中某個節點所擁有的Flash資源池本機層、則SSD備援磁碟必須由該節點擁有。

下圖為Flash Pool SSD分割區的範例。SSD儲存資源池可將快取提供給兩個Flash Pool本機層：



儲存資源池SP1由五個SSD和一個熱備援SSD組成。其中兩個儲存資源池的分配單元會分配給Flash資源池FP1、兩個則分配給Flash資源池FP2。FP1的快取RAID類型為RAID4。因此、提供給FP1的分配單元僅包含一個指定用於同位元檢查的分割區。FP2的快取RAID類型為RAID-DP。因此、提供給FP2的分配單元包括同位元分割區和雙同位元檢查分割區。

在此範例中、會將兩個配置單元分配給每個Flash Pool本機層。不過、如果某個Flash Pool本機層需要較大的快取、您可以將三個分配單元分配給該Flash Pool本機層、而只將一個分配給另一個層。

判斷 **ONTAP Flash Pool** 候選資格和最佳快取大小

在將現有的本機層轉換為 Flash Pool 本機層之前，您可以判斷本機層是否有 I/O 限制，以及最適合您工作負載和預算的 Flash Pool 快取大小。您也可以檢查現有Flash Pool本機層的快取大小是否正確。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

開始之前

您應該大約知道您分析的本機層何時會經歷其尖峰負載。

步驟

1. 進入進階模式：

   ```
   set advanced
   ```

2. 如果您需要判斷現有的本機層是否適合轉換為 Flash Pool 本機層級，請判斷本機層中的磁碟在尖峰負載期間有多忙碌，以及這會如何影響延遲：

   ```
   statistics show-periodic -object disk:raid_group -instance raid_group_name
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

   您可以決定新增 Flash Pool 快取來減少延遲，是否適合此本機層。

   下列命令顯示本機層 "'aggr1'" 第一個 RAID 群組的統計資料：

   ```
   statistics show-periodic -object disk:raid_group -instance /aggr1/plex0/rg0
   -counter disk_busy|user_read_latency -interval 1 -iterations 60
   ```

3. 啟動自動化工作負載分析程式（AWA）：

   ```
   storage automated-working-set-analyzer start -node node_name -aggregate
   aggr_name
   ```

   Awa 開始收集與指定本端層相關聯之磁碟區的工作負載資料。

4. 結束進階模式：

   ```
   set admin
   ```

   允許AWA執行、直到發生一或多個尖峰負載間隔為止。Awa 會收集與指定本端層相關聯之磁碟區的工作負載統計資料，並分析持續時間長達一週的資料。執行AWA超過一週、只會報告最近一週收集的資料。快取大小預估值是根據資料收集期間所見的最高負載而定；在整個資料收集期間、負載不需要太高。

5. 進入進階模式：

   ```
   set advanced
   ```

6. 顯示工作負載分析：

   ```
   storage automated-working-set-analyzer show -node node_name -instance
   ```

7. 停止AWA：

   ```
   storage automated-working-set-analyzer stop node_name
   ```

所有工作負載資料都會被清除、不再可供分析。

8. 結束進階模式：

```
set admin
```

相關資訊

- "統計資料顯示週期"
- "儲存自動工作集分析器顯示"
- "儲存自動工作集分析器啟動"
- "儲存自動工作集分析器停止"

使用實體 **SSD** 建立 **ONTAP Flash Pool** 本機層

您可以在由 HDD RAID 群組組成的現有本機層上啟用此功能，然後將一或多個 SSD RAID 群組新增至該本機層，藉此建立 Flash Pool 本機層。這會為該本機層建立兩組RAID群組：SSD RAID群組（SSD快取）和HDD RAID群組。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

關於這項工作

將SSD快取新增至本機層以建立Flash Pool本機層之後、您就無法移除SSD快取、將本機層級轉換回原始組態。

根據預設、SSD快取的RAID層級與HDD RAID群組的RAID層級相同。您可以在新增第一個 SSD RAID 群組時指定選項，以覆寫此預設 `raidtype`選項。

開始之前

- 您必須識別由HDD組成的有效本機層、才能轉換成Flash Pool本機層。
- 您必須確定與本機層相關之磁碟區的寫入快取資格、並完成所有必要步驟以解決資格問題。
- 您必須確定要新增的SSD、而且這些SSD必須由您建立Flash Pool本機層的節點擁有。
- 您必須確定要新增的SSD和本機層中已有的HDD的總和檢查碼類型。
- 您必須確定要新增的SSD數量、以及SSD RAID群組的最佳RAID群組大小。

  在SSD快取中使用較少的RAID群組、可減少所需的同位元檢查磁碟數量、但較大的RAID群組則需要RAID-DP。

- 您必須確定要用於SSD快取的RAID層級。
- 您必須確定系統的最大快取大小、並確定將SSD快取新增至本機層不會導致超出上限。
- 您必須熟悉Flash Pool本機層級的組態需求。

步驟

您可以使用系統管理員或 ONTAP CLI 建立 Flash Pool 本機層。

系統管理員

從《物件9.12.1》開始ONTAP 、您可以使用System Manager使用實體SSD來建立Flash Pool本機層。

步驟

1. 選取 * 儲存設備 > Tiers* 、然後選取現有的本機 HDD 儲存層。
2. 選取 ⋮ 「然後 * 新增 Flash Pool Cache* 」。
3. 選擇 使用專用 **SSD** 作為快取 。
4. 選取磁碟類型和磁碟數目。
5. 選擇RAID類型。
6. 選擇*保存*。
7. 找到儲存層，然後選擇⋮
8. 選擇 * 更多詳細資料 * 。驗證 Flash Pool 是否顯示為 * 啟用 * 。

CLI

步驟

1. 將本機層標記為符合資格成為 Flash Pool 本機層：

   ```
   storage aggregate modify -aggregate aggr_name -hybrid-enabled true
   ```

   如果此步驟沒有成功，請判斷目標本機層的寫入快取資格。

2. 使用命令將 SSD 新增至本機層 `storage aggregate add`。
   - 您可以依 ID 或使用來指定 SSD `diskcount` 和 `disktype` 參數。
   - 如果 HDD 和 SSD 沒有相同的 Checksum 類型，或如果本機層是混合式 Checksum 本機層，則必須使用 `checksumstyle`參數來指定要新增至本機層的磁碟的 Checksum 類型。
   - 您可以使用為 SSD 快取指定不同的 RAID 類型 `raidtype` 參數。
   - 如果您想要快取 RAID 群組大小與您所使用 RAID 類型的預設大小不同、您應該現在使用變更快取 RAID 群組大小 `-cache-raid-group-size` 參數。

相關資訊

- "儲存聚合添加"
- "儲存聚合修改"

使用 **SSD** 儲存池建立 **Flash Pool** 本機層

判斷 **ONTAP Flash Pool** 本機層是否使用 **SSD** 儲存池

您可以將一個或多個分配單元從 SSD 儲存池新增至現有 HDD 本機層，以設定 Flash Pool 本機層。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

使用SSD儲存資源池來提供快取時、管理Flash資源池本機層的方式與使用獨立SSD時不同。

步驟

1. 依 RAID 群組顯示本機層的磁碟機：

   ```
   storage aggregate show-status aggr_name
   ```

   如果本機層使用一或多個 SSD 儲存池， SSD RAID 群組欄的值 `Position`會顯示為，儲存池的名稱會顯示在 `Shared` RAID 群組名稱旁邊。

相關資訊

- "儲存聚合顯示狀態"

建立 **SSD** 儲存池，將快取新增至 **ONTAP** 本機層

您可以透過新增固態硬碟（ SSD ），將現有的本機層轉換為 Flash Pool 本機層，來配置快取。

您可以建立固態硬碟（ SSD ）儲存池，為兩至四個 Flash Pool 本機層提供 SSD 快取。Flash Pool 本機層可讓您將 Flash 部署為工作資料集的高效能快取，同時使用成本較低的 HDD 來處理存取頻率較低的資料。

關於這項工作

- 在建立磁碟或將磁碟新增至儲存資源池時、您必須提供磁碟清單。

  儲存資源池不支援 `diskcount` 參數。

- 儲存資源池中使用的SSD大小應相同。

系統管理員

使用**System Manager**新增**SSD**快取（**ONTAP** 更新版本：《》、《》、《》、《》、《》、《》、《

從功能完整的9.12.1開始ONTAP 、您可以使用System Manager來新增SSD快取。

儲存資源池選項不適用於AFF 不適用的系統。

步驟

1. 按一下「叢集>磁碟」、然後按一下「顯示/隱藏」。
2. 選取*類型*並確認叢集上是否有備用SSD。
3. 按一下「to * Storage > Tiers*」、然後按一下「* Add Storage Pool*」。
4. 選取磁碟類型。
5. 輸入磁碟大小。
6. 選取要新增至儲存資源池的磁碟數目。
7. 檢閱預估的快取大小。

使用系統管理程式新增**SSD**快取（**ONTAP** 僅限用率為**9.7**）

如果您使用ONTAP 的是更新於ONTAP 版本更新於版本號的版本、或是ONTAP 更新於版本號不超過版本號的版本號、請使用CLI程序。

步驟

1. 按一下*（返回傳統版本）*。
2. 按一下「 * 儲存設備 > 集合體與磁碟 > Aggregate * 」。
3. 選取本機層，然後按一下 * 動作 > 新增快取 * 。
4. 選取快取來源為「儲存資源池」或「專用SSD」。
5. 按一下*（切換至新體驗）*。
6. 按一下 * 儲存 > Tiers* ，確認新本機層的大小。

CLI

使用**CLI**建立**SSD**儲存資源池

步驟

1. 判斷可用的備用SSD名稱：

   ```
   storage aggregate show-spare-disks -disk-type SSD
   ```

   儲存資源池中使用的SSD可由HA配對的任一節點擁有。

2. 建立儲存資源池：

```
storage pool create -storage-pool sp_name -disk-list disk1,disk2,…
```

3. *選用：*驗證新建立的儲存資源池：

```
storage pool show -storage-pool sp_name
```

結果

將SSD放入儲存資源池之後、即使儲存資源池所提供的儲存設備尚未分配給任何Flash資源池快取、SSD仍不會在叢集上顯示為備援磁碟。您無法將SSD新增至RAID群組做為獨立磁碟機；只能使用SSD所屬儲存資源池的配置單元來配置其儲存設備。

相關資訊

- "儲存Aggregate顯示"
- "儲存池創建"
- "儲水池展示"

使用 **SSD** 儲存池分配單元建立 **ONTAP Flash Pool** 本機層

您可以將一個或多個分配單元從 SSD 儲存池新增至現有 HDD 本機層，以設定 Flash Pool 本機層。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

從功能更新至功能更新版本9.12.1開始ONTAP 、您可以使用重新設計的System Manager、使用儲存資源池配置單元來建立Flash Pool本機層。

開始之前

- 您必須識別由HDD組成的有效本機層、才能轉換成Flash Pool本機層。
- 您必須確定與本機層相關之磁碟區的寫入快取資格、並完成所有必要步驟以解決資格問題。
- 您必須建立SSD儲存池、才能將SSD快取提供給此Flash Pool本機層。

  您要使用的儲存資源池中的任何分配單元、都必須由擁有Flash資源池本機層的同一個節點擁有。

- 您必須確定要新增到本機層的快取容量。

  您可以依配置單位將快取新增至本機層。如果有空間、您可以稍後將SSD新增至儲存資源池、以增加配置單位的大小。

- 您必須確定要用於SSD快取的RAID類型。

  從SSD儲存資源池新增快取至本機層之後、就無法變更快取RAID群組的RAID類型。

- 您必須確定系統的最大快取大小、並確定將SSD快取新增至本機層不會導致超出上限。

  您可以使用查看將新增至快取總大小的快取數量 `storage pool show` 命令。

- 您必須熟悉Flash Pool本機層的組態需求。

關於這項工作

如果您希望快取的RAID類型與HDD RAID群組的RAID類型不同、則必須在新增SSD容量時指定快取RAID類型。將SSD容量新增至本機層之後、您就無法再變更快取的RAID類型。

將SSD快取新增至本機層以建立Flash Pool本機層之後、您就無法移除SSD快取、將本機層級轉換回原始組態。

系統管理員

從《發揮作用》9.12.1開始ONTAP 、您可以使用System Manager將SSD新增至SSD儲存資源池。

步驟

1. 按一下*儲存設備> Tiers*、然後選取現有的本機HDD儲存層。
2. 按一下 ⋮ 並選取 * 新增 Flash Pool Cache* 。
3. 選擇*使用儲存資源池*。
4. 選取儲存資源池。
5. 選取快取大小和RAID組態。
6. 按一下「 * 儲存 * 」 。
7. 再次找到儲存層並點擊⋮
8. 選取*更多詳細資料*、然後確認Flash Pool顯示為*已啟用*。

CLI

步驟

1. 將本機層標記為符合資格成為 Flash Pool 本機層：

   `storage aggregate modify -aggregate` *`aggr_name`* `-hybrid-enabled true`

   如果此步驟沒有成功，請判斷目標本機層的寫入快取資格。

2. 顯示可用的SSD儲存池配置單元：

   `storage pool show-available-capacity`

3. 將 SSD 容量新增至本機層：

   `storage aggregate add` *`aggr_name`* `-storage-pool` *`sp_name`* `-allocation-units` *`number_of_units`*

   如果您想要快取的 RAID 類型與 HDD RAID 群組的 RAID 類型不同、則必須在使用輸入此命令時加以變更 `raidtype` 參數。

   您不需要指定新的RAID群組；ONTAP 而無法自動將SSD快取放入不同於HDD RAID群組的RAID群組。

   您無法設定快取的RAID群組大小；它是由儲存資源池中的SSD數量所決定。

   快取會新增至本機層，而本機層現在則是 Flash Pool 本機層。新增至本機層的每個分配單元都會變成自己的 RAID 群組。

4. 確認SSD快取是否存在及大小：

   `storage aggregate show` *`aggregate_name`*

   快取的大小列於下 `Total Hybrid Cache Size`。

相關資訊

- "NetApp技術報告4070：Flash Pool設計與實作指南"
- "儲存聚合添加"
- "儲存聚合修改"
- "儲水池展示"
- "儲存池顯示可用容量"

判斷 SSD 新增至 SSD 儲存池時，對 ONTAP 快取大小的影響

如果將 SSD 新增至儲存池，導致平台模型的快取限制超出，則 ONTAP 不會將新增的容量分配給任何 Flash Pool 本機層。這可能導致部分或全部新增的容量無法使用。

關於這項工作

當您將 SSD 新增至已分配給 Flash Pool 本機層的 SSD 儲存池時，您會增加每個本機層的快取大小，以及系統上的總快取。如果儲存資源池的分配單元尚未分配、則在將一個或多個分配單元分配給快取之前、將SSD新增至該儲存資源池不會影響SSD快取大小。

步驟

1. 判斷您要新增至儲存資源池的SSD可用大小：

   `storage disk show` *`disk_name`* `-fields usable-size`

2. 判斷儲存資源池中仍有多少配置單元尚未配置：

   `storage pool show-available-capacity` *`sp_name`*

   儲存資源池中所有未分配的分配單元都會顯示出來。

3. 套用下列公式來計算要新增的快取容量：

   （4個未分配的分配單元數）x 25% x可用大小x SSD數量

相關資訊

- "儲存磁碟顯示"
- "儲存池顯示可用容量"

將 SSD 新增至 ONTAP SSD 儲存池

當您將固態硬碟（SSD）新增至SSD儲存池時、就會增加儲存池的實體與可用大小、以及配置單元大小。較大的分配單元大小也會影響已分配給本機層的分配單元。

開始之前

您必須確定此作業不會導致HA配對超過快取限制。將SSD新增至SSD儲存資源池時、不應讓您超過快取限制、否則可能會使新增的儲存容量無法使用。ONTAP

關於這項工作

將SSD新增至現有SSD儲存池時、SSD必須由儲存池中現有SSD的一個節點或同一個HA配對的另一個節點擁

有。您可以新增HA配對任一節點所擁有的SSD。

您新增至儲存資源池的SSD大小必須與儲存資源池中目前使用的磁碟大小相同。

系統管理員

從《發揮作用》9.12.1開始ONTAP 、您可以使用System Manager將SSD新增至SSD儲存資源池。

步驟

1. 按一下「儲存設備>層級」、找到「儲存資源池」區段。
2. 找到儲存池、按一下 ⋮、然後選取 * 新增磁碟 * 。
3. 選擇磁碟類型、然後選取磁碟數量。
4. 檢閱預估的快取大小。

CLI

步驟

1. *選用：*檢視儲存資源池的目前配置單位大小和可用儲存空間：

   ```
   storage pool show -instance sp_name
   ```

2. 尋找可用的SSD：

   ```
   storage disk show -container-type spare -type SSD
   ```

3. 將SSD新增至儲存資源池：

   ```
   storage pool add -storage-pool sp_name -disk-list disk1,disk2…
   ```

   系統會顯示哪些 Flash Pool 本機層的大小會由此作業增加，以及增加多少，並提示您確認作業。

相關資訊

- "儲存磁碟顯示"
- "儲水池展示"
- "儲存池添加"

用於管理 **SSD** 儲存資源池的 **ONTAP** 命令

ONTAP 提供 `storage pool` 管理 SSD 儲存資源池的命令。

如果您想要…	使用此命令…
顯示儲存池提供給哪個本機層的儲存容量	`storage pool show-aggregate`
顯示兩種RAID類型（分配單元資料大小）的整體快取容量會增加多少快取。	`storage pool show -instance`

顯示儲存資源池中的磁碟	`storage pool show-disks`
顯示儲存資源池的未分配配置單元	`storage pool show-available-capacity`
將儲存資源池的一個或多個分配單元的擁有權從一個HA合作夥伴變更為另一個	`storage pool reassign`

相關資訊

- "儲存池重新分配"
- "儲水池展示"
- "儲存池顯示聚合"
- "儲存池顯示可用容量"
- "儲存池顯示磁碟"

資料層管理FabricPool

瞭解 ONTAP FabricPool 的資料分層功能

根據資料存取頻率、您可以使用FabricPool 功能更新來自動分層資料。

FabricPool 是混合式儲存解決方案、在 AFF 系統上使用 All Flash （所有 SSD ）集合體、而在 FAS 系統上則使用 All Flash （所有 SSD ）或 HDD 集合體做為效能層、並使用物件存放區做為雲端層。使用VMware解決方案有助於降低儲存成本、而不會影響效能、效率或保護。FabricPool

雲端層可位於NetApp StorageGRID 的不二或ONTAP 不二之三（從ONTAP 功能上的問題9.8開始）、或是下列服務供應商之一：

- Alibaba雲端
- Amazon S3
- Amazon商業雲端服務
- Google Cloud
- IBM雲端
- Microsoft Azure Blob儲存設備

> 從 ONTAP 9.7 開始、可選擇 S3_compatible 物件存放區提供者、以使用支援一般 S3 API 的其他物件存放區提供者。

相關資訊

- "NetApp 雲端分層文件"

使用 **ONTAP FabricPool** 的需求

為了協助確保您最佳化 FabricPool 組態、您應該熟悉使用 FabricPool 的幾項考量和要求。

一般考量與要求

ONTAP 9.4

- 您必須執行ONTAP 更新版本的版本才能FabricPool 使用下列功能：
  - 。 `auto` "分層原則"
  - 指定分層的最低冷卻週期
  - 非作用中資料報告（印尼盾）
  - 使用Microsoft Azure Blob Storage for the Cloud做為FabricPool 適用於NetApp的雲端層
  - 搭配使用FabricPool ONTAP Select

版本**9.5 ONTAP**

- 您必須執行ONTAP 更新版本的版本才能FabricPool 使用下列功能：
  - 指定分層完整度臨界值
  - 使用IBM Cloud Object Storage做為FabricPool 雲端層以利實現效益
  - 雲端層的NetApp Volume Encryption（NVE）、預設為啟用。

ONTAP 9.6

- 您必須執行ONTAP 更新版本的版本才能FabricPool 使用下列功能：
  - 。 `all` 分層原則
  - 在HDD Aggregate上手動啟用非使用中資料報告
  - 當您升級ONTAP 至32位9.6時、會自動啟用SSD集合體的非作用中資料報告功能、並在建立集合體時、除非是低階系統的CPU少於4、RAM少於6 GB、或是WAFL緩衝快取大小低於3 GB。

    支援支援支援監控系統負載、如果負載持續高達4分鐘、則會停用印尼盾、而且不會自動啟用。ONTAP 您可以手動重新啟用 IDR ，但不會自動停用手動啟用的 IDR 。
  - 使用Alibaba Cloud Object Storage做為FabricPool 雲端層
  - 使用Google Cloud Platform做FabricPool 為雲端層以利實現效能不打造
  - 不需雲端層資料複本即可移動Volume

更新**ONTAP**

- 您必須執行ONTAP 更新版本的版本才能FabricPool 使用下列功能：
  - 不透明的HTTP和HTTPS Proxy、僅提供對白名單存取點的存取、並提供稽核和報告功能。
  - 可同時將冷資料分層至兩個物件存放區的鏡射FabricPool
  - 可鏡射到各種組態FabricPool MetroCluster

- NDMP傾印與還原功能預設為FabricPool 在連接的支援區上啟用。

> 如果備份應用程式使用NDMP以外的傳輸協定（例如NFS或SMB）、則在效能層中備份的所有資料都會變得很熱、而且可能會影響將該資料分層至雲端層。非NDMP讀取可能導致資料從雲端層移轉回效能層。

"NDMP備份與還原支援FabricPool 、適用於支援功能"

部分9.8 ONTAP

- 您必須執行ONTAP 更新版本的版本才能FabricPool 使用下列功能：
  - 雲端擷取
  - FabricPool with SnapLock Enterprise 。FabricPool with SnapLock Enterprise 需要功能產品差異要求（ FPVR ）。若要建立 FPVR ，請聯絡您的銷售團隊。
  - 最短冷卻期最長183天
  - 使用使用者建立的自訂標記進行物件標記
  - HDD FabricPool 集合體

    HDD FabricPools 僅在具有 6 個或更多 CPU 核心的系統上支援 SAS 、 FSA 、 BSA 和 mSATA 磁碟。

檢查 "Hardware Universe" 適用於支援的最新機型。

零點9.10.1 ONTAP

- 您必須執行 ONTAP 9.10.1 或更新版本、才能使用下列 FabricPool 功能：
  - 設定節流
  - 對溫度敏感的儲存效率（ TSSE ）。

ONTAP 9.12.1

- 您必須執行 ONTAP 9.12.1 或更新版本、才能使用下列 FabricPool 功能：
  - SVM 移轉
  - 支援 FabricPool 、 FlexGroup 和 SVM-DR 搭配使用。（在 9.12.1 之前、這兩項功能都能一起運作、但並非全部三項功能都能一起運作。）

ONTAP 9.14.1.

- 您必須執行 ONTAP 9.14.1 或更新版本、才能使用下列 FabricPool 功能：
  - 雲端寫入
  - 積極預先讀取

本機層（集合體）

支援下列Aggregate類型：FabricPool

- 在 AFF 系統上、您只能將 SSD 集合體用於 FabricPool 。
- 在 FAS 系統上、您可以使用 FabricPool 的 SSD 或 HDD 集合體。
- 在本產品的不只是部分、您也可以使用SSD或HDD Aggregate來執行功能。Cloud Volumes ONTAP ONTAP Select FabricPool建議使用 SSD 集合體。

> 不支援同時包含 SSD 和 HDD 的 Flash Pool Aggregate 。

雲端階層

支援使用下列物件存放區做為雲端層：FabricPool

- Alibaba雲端物件儲存服務（標準、非常用存取）
- Amazon S3 （標準、 Standard-IA 、 One Zone-IA 、 Intelligent Tiering 、 Glacier 即時擷取）
- Amazon商業雲端服務（C2S）
- Google Cloud Storage （多區域、區域、近線、 Coldline 、歸檔）
- IBM Cloud物件儲存設備（Standard、Vault、Cold Vault、Flex）
- Microsoft Azure Blob儲存設備（熱與冷）
- NetApp ONTAP SS3（ONTAP 適用於9.8及更新版本）
- NetApp StorageGRID （ StorageGRID 10.3 及更新版本）

> 不支援 Glacier Flexible Retrieval 和 Glacier Deep Archive 。

- 您打算使用的物件存放區「'Bucke'」（容器）必須已設定完成、至少必須有10 GB的儲存空間、且不得重新命名。
- 您無法在附加雲端層之後、將其從本機層分離；不過、您可以使用 "FabricPool 鏡射" 將本機層附加至不同的雲端層。

叢集間**LIF**

使用 FabricPool 的叢集高可用度（ HA ）配對需要兩個叢集間的生命體才能與雲端層通訊。NetApp 建議在額外的 HA 配對上建立叢集間 LIF ，以便將雲端層順暢地附加到這些節點上的本機層。

停用或刪除叢集間LIF會中斷與雲端層的通訊。

> 由於並行 SnapMirror 和 SnapVault 複寫作業會共用通往雲端層的網路連結，因此初始化和 RTO 會視雲端層的可用頻寬和延遲而定。如果連線資源飽和，可能會導致效能降低。主動式組態多重生命負載可大幅降低這類網路飽和。

如果您在具有不同路由的節點上使用多個叢集間 LIF ， NetApp 建議您將它們放在不同的 IPspace 中。在組態期間， FabricPool 可以從多個 IPspace 中選取，但無法在 IPspace 中選取特定的叢集間生命體。

網路時間協定 **(NTP)**

需要網路時間協定 (NTP) 配置來確保叢集之間的時間同步。"了解如何設定 NTP" 。

儲存效率ONTAP

將資料移至雲端層時、會保留壓縮、重複資料刪除和壓縮等儲存效率、進而降低所需的物件儲存容量和傳輸成本。

> 從 ONTAP 9.15.1 開始， FabricPool 支援 Intel QuickAssist 技術（ QAT4 ），可提供更具競爭力，更高效能，更節省儲存效率。

本機層支援 Aggregate 內嵌重複資料刪除、但相關的儲存效率不會轉移到儲存在雲端層的物件。

當使用 All Volume 分層原則時、由於資料可能會在應用額外的儲存效率之前分層、因此與背景重複資料刪除程序相關的儲存效率可能會降低。

NetApp Cloud Tiering 許可證

當將第三方物件儲存提供者（例如 Amazon S3）附加為AFF和FAS系統的雲端時， FabricPool需要基於容量的授權。當使用StorageGRID或ONTAP S3 作為雲端，或使用Cloud Volumes ONTAP、 Amazon FSx for NetApp ONTAP或 Azure NetApp檔案進行分層時，不需要 Cloud Tiering 授權。

NetApp Cloud Tiering 授權（包括現有FabricPool許可證的附加元件或擴充功能）在NetApp控制台中啟用。了解更多"設定 Cloud Tiering 許可證"。

StorageGRID 一致性控制

StorageGRID 的一致性控制會影響 StorageGRID 用來追蹤物件的中繼資料分佈在節點之間、以及用戶端要求的物件可用度。NetApp 建議使用作為 FabricPool 目標之貯體的預設、新寫入後讀取一致性控制。

> 請勿將可用的一致性控制用於做為 FabricPool 目標的貯體。

SAN傳輸協定存取的分層資料的其他考量事項

當 SAN 通訊協定存取的分層資料時、 NetApp 建議使用私有雲、例如 ONTAP S3 或 StorageGRID 、因為連線能力考量。

> 您應該知道，在具有 Windows 主機的 SAN 環境中使用FabricPool時，如果在將資料分層到雲端時物件儲存在較長時間內不可用，則 Windows 主機上的NetApp LUN 上的檔案可能會變得無法存取或消失。查看"NetApp知識庫：在FabricPool S3 物件儲存不可用期間，Windows SAN 主機報告檔案系統損壞"。

服務品質

- 如果您使用處理量層（ QoS 最小）、則必須將磁碟區上的分層原則設定為 `none` 將 Aggregate 附加至 FabricPool 之前。

  其他分層原則則可防止將Aggregate附加FabricPool 到無法使用的物件上。啟用 FabricPool 時、 QoS 原則不會強制執行處理量層。

功能或功能不受**FabricPool** 支援

- 物件存放區已啟用WORM且已啟用物件版本管理。
- 套用至物件存放區的資訊生命週期管理（ILM）原則

  FabricPool 僅支援 StorageGRID 的資訊生命週期管理原則、用於資料複寫和銷毀編碼、以保護雲端層資料免於故障。不過、 FabricPool 不支援進階 ILM 規則、例如根據使用者中繼資料或標記進行篩選。ILM通常包含各種移動和刪除原則。這些原則可能會破壞FabricPool 雲端層的資料。使用物件存放區上設定的ILM原則時、可能會導致資料遺失。FabricPool

- 7-Mode資料轉換、使用ONTAP VMware CLI命令或7-Mode轉換工具
- RAID SyncMirror 功能、MetroCluster 不包括在一個不支援的組態中
- 使用更新版本時的資料來源SnapLock ONTAP
- "防竄改快照"

  防竄改的快照可提供不可刪除的保護。由於 FabricPool 需要刪除資料的能力，因此無法在同一個磁碟區上啟用 FabricPool 和快照鎖定。

- 使用SMTape備份啟用FabricPool的Aggregate
- 自動平衡功能
- 使用除以外的空間保證的磁碟區 `none`

  除了根SVM磁碟區和CIFS稽核暫存磁碟區之外、FabricPool 不支援將雲端層附加至使用空間保證以外的其他磁碟區的集合體 `none`。例如、使用空間保證的Volume `volume` (`-space-guarantee volume`）不受支援。

- 具有的叢集 "DP_ 最佳化授權"
- Flash Pool Aggregate

利用 **ONTAP FabricPool** 原則有效分層資料

利用此類分層原則、您可以在資料變熱或變冷時、在不同階層之間有效率地搬移資料。FabricPool瞭解分層原則有助於選擇符合儲存管理需求的正確原則。

分層原則的類型**FabricPool**

根據熱（作用中）或冷（非作用中）的Volume「'Temperat'」（Volume「溫度」）、將資料區塊移至雲端層的時機或時機取決於該使用者資料區塊。FabricPool FabricPool經常存取時、Volume「'Temperature」會增加、而非存取時則會減少。有些分層原則具有相關的分層最低冷卻時間、可設定FabricPool 使用者資料在某個部分中必須保持非作用中狀態的時間、以便將資料視為「冷」並移至雲端層。

當區塊被識別為冷區後、就會標示為符合分層的資格。 每日背景分層掃描會尋找冷區塊。當從同一個磁碟區收集足夠的 4KB 區塊時、這些區塊會串連成一個 4 MB 物件、並根據磁碟區分層原則移至雲端層。

使用的磁碟區中的資料 `all` 分層原則會立即標記為冷、並儘快開始分層至雲端層。它不需要等待每日分層掃描執行。

您可以使用 `volume object-store tiering show`命令來檢視 FabricPool Volume 的分層狀態。如"指令參考資

料ONTAP"需詳細 `volume object-store tiering show`資訊，請參閱。

在Volume層級指定了分層原則。FabricPool共有四種選項可供選擇：

- `snapshot-only`分層原則（預設）會將與作用中檔案系統無關的 Volume 快照使用者資料區塊移至雲端層。

  分層的最低冷卻時間為2天。您可以使用修改分層最低冷卻期間的預設設定 `-tiering-minimum-cooling-days` 的進階權限層級中的參數 `volume create` 和 `volume modify` 命令。有效值為2至183天、使用ONTAP NetApp 9.8及更新版本。如果您使用ONTAP 的版本早於9.8、有效值為2至63天。

- `auto`分層原則僅在 ONTAP 9.4 及更新版本上支援，可將快照和作用中檔案系統中的冷使用者資料區塊移至雲端層。

  預設的分層最低冷卻期間為 31 天，適用於整個 Volume ，適用於作用中檔案系統和快照。

  您可以使用修改分層最低冷卻期間的預設設定 `-tiering-minimum-cooling-days` 的進階權限層級中的參數 `volume create` 和 `volume modify` 命令。有效值為2至183天。

- `all`分層原則僅支援 ONTAP 9.6 及更新版本，可將作用中檔案系統和快照中的所有使用者資料區塊移至雲端層。它取代 `backup`分層原則。

  。 `all` 磁碟區分層原則不應用於具有正常用戶端流量的讀取 / 寫入磁碟區。

  分層最低冷卻週期不適用、因為資料會在分層掃描執行後立即移至雲端層、而且您無法修改設定。

- 。 `none` 分層原則可將磁碟區的資料保留在效能層、不會冷移至雲端層。

  將分層原則設為 `none` 防止新的分層。先前移至雲端層的 Volume 資料會保留在雲端層、直到變熱為止、並自動移回本機層為止。

  分層最低散熱週期不適用、因為資料永遠不會移至雲端層、而且您無法修改設定。

  當磁碟區中的冷區塊設為分層原則時 `none` 讀取後、會變熱並寫入本機層。

。 `volume show` 命令輸出會顯示磁碟區的分層原則。FabricPool 從未使用過的 Volume 會顯示 `none` 輸出中的分層原則。

> 在 SVM DR 關係中，來源和目的地磁碟區不需要使用 FabricPool 集合體，但它們必須使用相同的分層原則。

當您修改**FabricPool** 完一份**Volume**的分層原則時、會發生什麼情況

您可以執行來修改磁碟區的分層原則 `volume modify` 營運。您必須瞭解變更分層原則、可能會影響資料冷卻及移至雲端層所需的時間。

- 變更分層原則 `snapshot-only` 或 `none` 至 `auto` 讓 ONTAP 將已冷卻的作用中檔案系統中的使用者資料區塊傳送至雲端層、即使這些使用者資料區塊先前不符合雲端層的資格。
- 將分層原則從另一個原則變更為 `all`，會導致 ONTAP 盡快將作用中檔案系統和快照中的所有使用者區塊移至雲端。在 ONTAP 9.8 之前、區塊需要等到下一次分層掃描執行。

  不允許將區塊移回效能層。

- 變更分層原則 `auto` 至 `snapshot-only` 或 `none` 不會將已移至雲端層的作用中檔案系統區塊移回效能層。

  需要磁碟區讀取、才能將資料移回效能層。

- 每當您變更磁碟區的分層原則時、分層的最小冷卻期間會重設為原則的預設值。

當您移動磁碟區時、分層原則會發生什麼事

- 除非您明確指定不同的分層原則、否則當磁碟區移入和移出啟用FabricPool的Aggregate時、就會保留其原始分層原則。

  不過、分層原則只有在磁碟區位於啟用FabricPool的Aggregate中時才會生效。

- 的現有值 `-tiering-minimum-cooling-days` 除非您為目的地指定不同的分層原則、否則 Volume 的參數會隨著 Volume 一起移動。

  如果您指定不同的分層原則、則該磁碟區會使用該原則的預設分層最小冷卻期間。無論目的地FabricPool 是否為不實、都會發生這種情況。

- 您可以跨集合體移動磁碟區、同時修改分層原則。
- 您應該特別注意 `volume move` 操作涉及 `auto` 分層原則。

  假設來源和目的地都是啟用 FabricPool 的集合體、下表摘要說明的結果 `volume move` 涉及相關原則變更的作業 `auto`：

當您移動具有分層原則的磁碟區時...	您也可以透過移至...來變更分層原則。	然後在磁碟區移動之後...
`all`	`auto`	所有資料都會移至效能層級。
`snapshot-only`、 `none`或 `auto`	`auto`	資料區塊會移至目的地的同一層、如同先前位於來源。
`auto` 或 `all`	`snapshot-only`	所有資料都會移至效能層級。
`auto`	`all`	所有使用者資料都會移至雲端層。
`snapshot-only`,`auto` 或 `all`	`none`	所有資料都保留在效能層級。

當您複製磁碟區時、分層原則會發生什麼變化

- 從ONTAP 功能性的問題9.8開始、複製磁碟區一律會從父磁碟區繼承分層原則和雲端擷取原則。

  在早於 ONTAP 9.8 的版本中、除非父實體具有、否則複本會從父實體繼承分層原則 `all` 分層原則。

- 如果父磁碟區有 `never` 雲端擷取原則、其複製磁碟區必須具有 `never` 雲端擷取原則或 `all` 分層原則、以及對應的雲端擷取原則 `default`。
- 無法將父 Volume 雲端擷取原則變更為 `never` 除非所有的複本磁碟區都有雲端擷取原則 `never`。

當您複製磁碟區時、請謹記下列最佳實務做法：

- 。 `-tiering-policy` 選項與 `tiering-minimum-cooling-days` 複製選項只會控制複製特有之區塊的分層行為。因此、我們建議在父FlexVol 級不知道上使用分層設定、以移動相同數量的資料、或移動的資料量少於任何複本
- 父FlexVol 實體上的雲端擷取原則應移動相同數量的資料、或移動的資料應大於任何實體複本的擷取原則

分層原則如何與雲端移轉搭配運作

利用分層原則來控制實體雲端資料擷取、根據讀取模式從雲端層擷取資料至效能層。FabricPool讀取模式可以是連續的或隨機的。

下表列出各原則的分層原則和雲端資料擷取規則。

分層原則	擷取行為
無	連續和隨機讀取
純快照	連續和隨機讀取
自動	隨機讀取
全部	無資料擷取

從 ONTAP 9.8 開始、就是雲端移轉控制 `cloud-retrieval-policy` 選項會覆寫由分層原則控制的預設雲端移轉或擷取行為。

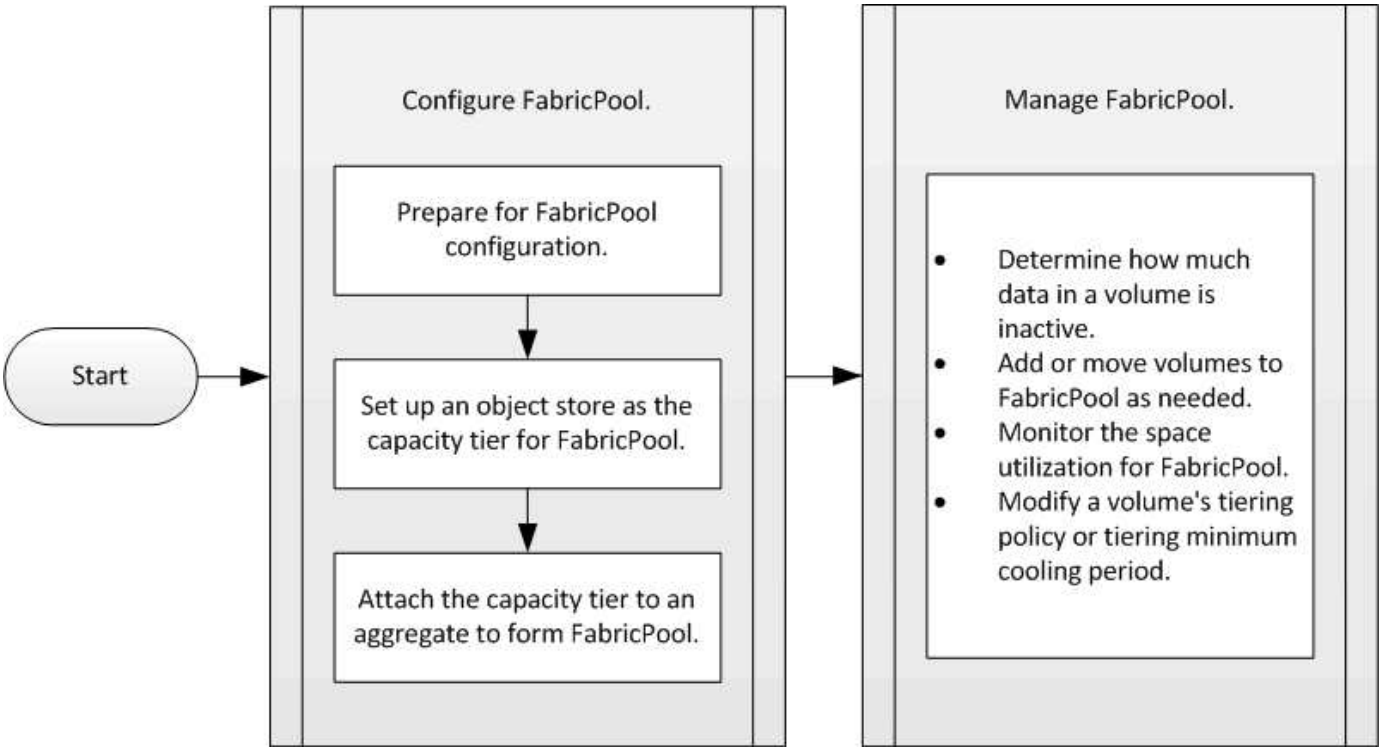
下表列出支援的雲端擷取原則及其擷取行為。

雲端擷取原則	擷取行為
預設	分層原則會決定應將哪些資料取回、因此雲端資料擷取不會有「預設」的變更," `cloud-retrieval-policy`。無論託管的Aggregate類型為何、此原則都是任何Volume的預設值。
讀取時	所有用戶端導向的資料讀取都會從雲端層移至效能層。
永不	不會將用戶端導向的資料從雲端層提取到效能層
促銷	• 對於分層原則「無、」、所有雲端資料都會從雲端層提取到效能層 • 若為分層原則、會擷取「僅限快照」的主動式檔案管理系統資料。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

了解 ONTAP FabricPool 設定和管理任務

您可以使用FabricPool 「支援流程圖」來規劃組態和管理工作。



設定FabricPool 功能

準備FabricPool 好進行不完善的組態設定

開始使用 ONTAP FabricPool

設定FabricPool 功能可協助您根據資料是否經常存取、來管理應儲存的儲存層（本機效能層或雲端層）資料。

進行不必要的物件組態準備FabricPool 、取決於您用做雲端層的物件存放區。

在 ONTAP 叢集上安裝 FabricPool 授權

您過去可能使用過的FabricPool許可證正在發生變化，並且僅針對NetApp控制台中不支援的配置保留。從 2021 年 8 月 21 日開始， NetApp Cloud Tiering BYOL 授權開始適用於使用NetApp Cloud Tiering 在NetApp控制台中支援的分層配置。

"了解有關NetApp Cloud Tiering BYOL 許可的更多信息" 。

NetApp控制台支援的設定必須使用控制台來授權ONTAP叢集的分層。這要求您設定一個NetApp控制台帳戶並為您計劃使用的特定物件儲存提供者設定分層。控制台目前支援分層到以下物件儲存：Amazon S3、Azure Blob 儲存、Google Cloud Storage、S3 相容物件儲存和StorageGRID。

"了解有關NetApp Cloud Tiering 服務的更多信息" 。

如果您擁有控制台不支援的配置之一，則可以使用系統管理員下載並啟動FabricPool許可證：

- 安裝於黑暗環境ONTAP
- 將資料分層儲存至IBM Cloud Object Storage或Alibaba Cloud Object Storage的叢集ONTAP

此功能是叢集範圍的授權。FabricPool其中包含您購買的授權用途限制、用於FabricPool 與叢集中的物件儲存相關聯的物件儲存設備。整個叢集的使用量不得超過授權使用量限制的容量。如果您需要增加授權的使用量上限、請聯絡您的銷售代表。

支援的形式包括永久或定期、1年或3年。FabricPool

對於NetApp控制台不支援的現有叢集配置，首次訂購FabricPool時，可取得基於期限的FabricPool許可證，其中包含 10 TB 的免費容量。永久許可證不提供免費容量。如果您將NetApp StorageGRID或ONTAP S3 用於雲層，則不需要授權。無論您使用哪個供應商， Cloud Volumes ONTAP都不需要FabricPool授權。

只有使用System Manager將授權檔案上傳至叢集、才能支援此工作。

步驟

1. 從下載NetApp授權檔案（NLF）以取得FabricPool 有關的不含故障的授權 "NetApp 支援網站"。
2. 使用System Manager將FabricPool 驗證授權上傳至叢集時、請執行下列動作：
   a. 在 * 叢集 > 設定 * 窗格的 * 授權 * 卡上、按一下 →。
   b. 在 **License** 頁面上，單擊 + Add 。
   c. 在「新增授權」對話方塊中、按一下「瀏覽」以選取您下載的NLF、然後按一下「新增」將檔案上傳至叢集。

相關資訊

"介紹（FP）授權總覽ONTAP FabricPool"

"NetApp軟體授權搜尋"

"NetApp TechCommTV：FabricPool 《支援目標清單"

在適用於 **StorageGRID** 的 **ONTAP** 叢集上安裝 **CA** 憑證

使用 CA 憑證可在用戶端應用程式與 StorageGRID 之間建立信任關係。

除非您計畫停用StorageGRID 驗證以供驗證的功能、否則您必須在StorageGRID 叢集上安裝一份「驗證CA」證書、ONTAP 以便讓「驗證時使用StorageGRID 」作FabricPool 為物件存放區以供使用。

雖然 StorageGRID 可以產生自我簽署的憑證，但建議最佳做法是使用協力廠商憑證授權單位所簽署的憑證。

關於這項工作

雖然建議最好的做法是安裝及使用憑證授權單位（ CA ）憑證，從 ONTAP 9.4 開始， StorageGRID 並不需要安裝 CA 憑證。

步驟

1. 請聯絡您的 StorageGRID 管理員以取得 "StorageGRID 系統的 CA 憑證"。
2. 使用 `security certificate install` 命令 `-type server-ca` 用於在叢集上安裝 StorageGRID CA

憑證的參數。

您輸入的完整網域名稱（FQDN）必須符合StorageGRID 來自訂的通用名稱（在Eqing CA憑證上）。

更新過期的憑證

若要更新過期的憑證、最佳做法是使用信任的CA來產生新的伺服器憑證。此外、您應確保證書在StorageGRID 更新時、ONTAP 同時更新到位在伺服器上和位在整個叢集上、以將任何停機時間降至最低。

相關資訊

- "資源StorageGRID"
- "安全性憑證安裝"

在 **ONTAP S3** 的叢集上安裝 **CA** 憑證

使用 CA 憑證可在用戶端應用程式和 ONTAP S3 物件存放區伺服器之間建立信任的關係。在將 CA 憑證作為遠端用戶端可存取的物件存放區之前，應先在 ONTAP 上安裝 CA 憑證。

除非您計畫停用ONTAP 驗證以檢查S3的憑證、否則您必須在ONTAP 叢集上安裝一個物件S3 CA憑證、ONTAP 以便讓S3驗證ONTAP 為FabricPool 物件存放區。

雖然 ONTAP 可以產生自我簽署的憑證，但建議最佳做法是使用協力廠商憑證授權單位所簽署的憑證。

步驟

1. 取得ONTAP S3系統的CA認證。
2. 使用 `security certificate install` 命令 `-type server-ca` 在叢集上安裝 ONTAP S3 CA 憑證的參數。

   您輸入的完整網域名稱（FQDN）必須與ONTAP 「S3 CA」憑證上的自訂通用名稱相符。

更新過期的憑證

若要更新過期的憑證、最佳做法是使用信任的CA來產生新的伺服器憑證。此外、您應確保在ONTAP 更新驗證證時、ONTAP 同時更新到位址為「S3」的伺服器和「支援」的叢集上、以將任何停機時間降至最低。

您可以使用系統管理員更新 ONTAP 叢集上的過期憑證。

步驟

1. 瀏覽至 * 叢集 > 設定 * 。
2. 滾動至 **Security** 部分，找到 **Certificates** 窗格，然後單擊 → 。
3. 在 * 信任的憑證授權單位 * 索引標籤中，找到您要續約的憑證名稱。
4. 按一下憑證名稱旁的⋮，然後選取 * 更新 * 。
5. 在 * 更新信任的憑證授權單位 * 視窗中，複製並貼上憑證資訊，或將其匯入 * 憑證詳細資料 * 區域。
6. 按一下 * 更新 * 。

相關資訊

- "S3 組態"
- "安全性憑證安裝"

將物件存放區設定為**FabricPool** 雲端層以供使用

將物件存放區設定為雲端層、以**FabricPool** 供瀏覽

設定 FabricPool 包括指定您計畫作為 FabricPool 雲端層的物件存放區（ StorageGRID 、 ONTAP S3 、 Alibaba 雲端物件儲存設備、 Amazon S3 、 Google 雲端儲存設備、 IBM 雲端物件儲存設備或 Microsoft Azure Blob 儲存設備）的組態資訊。

將 **StorageGRID** 設定為 **ONTAP FabricPool** 雲端層

您可以將StorageGRID設定為FabricPool的雲層。在分層SAN傳輸協定存取的資料時、NetApp建議使用私有雲端、例如StorageGRID 由於連線考量、所以使用像是「物件」的私有雲端。

搭配使用時的考**StorageGRID** 量事項**FabricPool**

- 除非您明確停用憑證檢查、否則您必須安裝CA認證StorageGRID 以供使用。
- 請勿在物件存放區貯體上啟用 StorageGRID 物件版本設定。
- 不需要使用此功能。FabricPool
- 如果StorageGRID 將某個節點部署在虛AFF 擬機器上、且該虛擬機器的儲存設備已從NetApp支援系統指派、請確認該磁碟區FabricPool 並未啟用「分層原則」。

  停用FabricPool 與物件節點搭配使用的磁碟區的分層StorageGRID 功能、可簡化疑難排解和儲存作業。

  > 切勿使用FabricPool 無法將StorageGRID 任何與還原StorageGRID 本身相關的資料分層。將StorageGRID 資料分層還原StorageGRID 至物件、可增加疑難排解和作業複雜度。

關於這項工作

負載平衡功能可在StorageGRID VMware 9.8及更新版本中實現。ONTAP當伺服器的主機名稱解析為多個IP位址時ONTAP 、即可建立用戶端連線、並傳回所有IP位址（最多16個IP位址）。建立連線時、會以循環配置資源的方式來取用IP位址。

步驟

您可以StorageGRID 使用NetApp系統管理程式或CLI、將無法使用的功能組建成FabricPool 可用於執行功能的雲端層ONTAP 。ONTAP

系統管理員

1. 按一下「儲存設備>層級>新增雲端層」、然後選取StorageGRID 「以物件儲存區供應商的形式提供」。
2. 填寫要求的資訊。
3. 如果您想要建立雲端鏡射、請按一下*「Add as FabricPool Swirror （*新增為鏡射）」。

利用這個鏡射技術、您可以順暢地更換資料儲存區、並確保在發生災難時能夠取得您的資料。FabricPool

CLI

1. 使用指定 StorageGRID 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type SGWS` 參數。

   - 。 `storage aggregate object-store config create` 如果 ONTAP 無法使用提供的資訊存取 StorageGRID 、則命令會失敗。
   - 您可以使用 `-access-key` 指定存取金鑰以授權 StorageGRID 物件存放區的要求。
   - 您可以使用 `-secret-password` 指定密碼（秘密存取金鑰）以驗證 StorageGRID 物件存放區的要求。
   - 如果變更了該密碼、您應該立即更新儲存在BIOS中的對應密碼。StorageGRID ONTAP

     這樣做可ONTAP 讓支援不StorageGRID 中斷地存取資料的不間斷資料。

   - 將參數設定 `-is-certificate-validation-enabled`為 `false`停用 `StorageGRID` 的憑證檢查。使用 (-is-certificate-validation-enabled true`第三方憑證授權單位的簽署憑證是建議的最佳做法。

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name mySGWS -provider-type SGWS -server mySGWSserver
   -container-name mySGWScontainer -access-key mySGWSkey
   -secret-password mySGWSpass
   ```

2. 使用顯示和驗證 StorageGRID 組態資訊 `storage aggregate object-store config show` 命令。

   。 `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 StorageGRID 組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **ONTAP S3** 設定為 **FabricPool** 雲端層

如果您執行ONTAP 的是版本不支援的版本、您可以將ONTAP S3設定為FabricPool 適用於

該產品的雲端層。

開始之前

- 您必須在ONTAP 遠端叢集上擁有該伺服器的名稱及其相關生命的IP位址。

  用戶端應用程式會將伺服器名稱用作完整網域名稱（ FQDN ）。在 ONTAP 之外，請確認 DNS 記錄指向正在使用的 SVM 資料生命。

- 本機叢集上必須有難以克服的生命。

  設定本機叢集分層時，本機層（也稱為 ONTAP CLI 中的儲存集合體）會附加到本機儲存區。FabricPool 使用叢集生命來處理叢集內的流量。

  如果叢集 LIF 資源飽和，可能會導致效能降低。為了避免這種情況， NetApp 建議您在分層至本機儲存區時，使用四節點或更高的叢集，並針對本機層使用 HA 配對，以及將 HA 配對用於本機儲存區。不建議在單一 HA 配對上分層至本機貯體。

- 若要使用 ONTAP S3 啟用遠端 FabricPool 容量（雲端）分層，您必須"設定叢集間的生命"在 FabricPool 用戶端和物件儲存區伺服器上"設定資料生命"。

關於這項工作

支援以更新版本的功能、在更新版本的更新版本中、啟用Ss3伺服器的負載平衡ONTAP 功能。ONTAP當伺服器的主機名稱解析為多個IP位址時ONTAP 、即可建立用戶端連線、並傳回所有IP位址（最多16個IP位址）。建立連線時、會以循環配置資源的方式來取用IP位址。

步驟

您可以使用ONTAP 支援功能的支援功能、將S3設定為FabricPool 適用於各種功能的雲端層ONTAP 、以供使用。ONTAP

系統管理員

1. 按一下「儲存設備>層級>新增雲端層」、然後選取ONTAP 「物件儲存區供應商」「S3」。
2. 填寫要求的資訊。
3. 如果您想要建立雲端鏡射、請按一下*「Add as FabricPool Swirror （*新增為鏡射）」。

利用這個鏡射技術、您可以順暢地更換資料儲存區、並確保在發生災難時能夠取得您的資料。FabricPool

CLI

1. 將S3伺服器和LIF的項目新增至DNS伺服器。

選項	說明
如果您使用外部**DNS**伺服器	將S3伺服器名稱和IP位址提供給DNS伺服器管理員。
如果您使用本機系統的**DNS**主機表	輸入下列命令： `dns host create -vserver <svm_name> -address ip_address -hostname <s3_server_name>`

2. 使用指定 ONTAP S3 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type ONTAP_S3` 參數。

   - 。 `storage aggregate object-store config create` 如果本機 ONTAP 系統無法使用所提供的資訊存取 ONTAP S3 伺服器、則命令會失敗。
   - 您可以使用 `-access-key` 指定存取金鑰以授權 ONTAP S3 伺服器的要求。
   - 您可以使用 `-secret-password` 指定密碼（秘密存取金鑰）以驗證 ONTAP S3 伺服器的要求。
   - 如果ONTAP 變更了「S3伺服器密碼」、您應該立即更新儲存在本機ONTAP 版的BIOS系統中的對應密碼。

     如此一來、ONTAP 即可在不中斷的情況下、存取位於現象中心S3物件儲存區的資料。

   - 將參數設定 `-is-certificate-validation-enabled`為 `false`停用 `ONTAP S3` 的憑證檢查。使用 (-is-certificate-validation-enabled true`第三方憑證授權單位的簽署憑證是建議的最佳做法。

```
cluster1::> storage aggregate object-store config create
-object-store-name myS3 -provider-type ONTAP_S3 -server myS3server
-container-name myS3container -access-key myS3key
-secret-password myS3pass
```

3. 使用顯示和驗證 ONTAP S3 組態資訊 `storage aggregate object-store config show` 命令。

- `storage aggregate object-store config modify` 命令可讓您修改 `ONTAP_S3` FabricPool 組態資訊。

相關資訊

- "為 SMB 建立 LIF"
- "建立 LIF for NFS"
- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **Alibaba** 雲端物件儲存設備設定為 **ONTAP FabricPool** 雲端層

如果您執行ONTAP 的是32個以上版本的版本、您可以將Alibaba Cloud Object Storage設定為FabricPool 適用於此功能的雲端層。

搭配**FabricPool** 使用**Alibaba Cloud Object Storage**的考量事項

- 一個"NetApp Cloud Tiering 許可證"在分層到阿里雲物件儲存時是必需的。有關更多信息，請參閱"在 ONTAP 叢集上安裝 FabricPool 授權" 。
- 在支援下列Alibaba物件儲存服務課程的支援對象系統和功能區上：AFF FAS ONTAP Select FabricPool
  - Alibaba物件儲存服務標準
  - Alibaba物件儲存服務不常存取

    "Alibaba Cloud：儲存課程簡介"

請聯絡您的NetApp銷售代表、以取得未列出的儲存類別相關資訊。

步驟

1. 使用指定 Alibaba Cloud Object Storage 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type AliCloud` 參數。

   - `storage aggregate object-store config create` 如果 ONTAP 無法使用所提供的資訊存取 Alibaba 雲端物件儲存設備、則命令會失敗。
   - 您可以使用 `-access-key` 此參數可指定存取金鑰、以授權對 Alibaba Cloud Object Storage 物件儲存區的要求。
   - 如果Alibaba Cloud Object Storage密碼已變更、您應該ONTAP 立即更新儲存在效益管理系統中的對應密碼。

     這樣做可ONTAP 讓支援中心在不中斷的情況下存取Alibaba Cloud Object Storage中的資料。

```
storage aggregate object-store config create my_ali_oss_store_1
-provider-type AliCloud -server oss-us-east-1.aliyuncs.com
-container-name my-ali-oss-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. 使用顯示並驗證 Alibaba Cloud Object Storage 組態資訊 `storage aggregate object-store config show` 命令。

   ◦ `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 Alibaba 雲端物件儲存組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **Amazon S3** 設定為 **ONTAP FabricPool** 雲端層級

您可以將 Amazon S3 設定為FabricPool 的雲層。如果您執行的是 ONTAP 9.5 或更新版本、您可以為 FabricPool 設定 Amazon 商業雲端服務（ C2S ）。

搭配 **FabricPool** 使用 **Amazon S3** 的考量事項

- 一個"NetApp Cloud Tiering 許可證"在分層到 Amazon S3 時是必需的。
- 建議 ONTAP 用來連線 Amazon S3 物件伺服器的 LIF 位於 10 Gbps 連接埠上。
- 在支援下列Amazon S3儲存課程的支援對象包括：AFF FAS ONTAP Select FabricPool

  ◦ Amazon S3 Standard

  ◦ Amazon S3 Standard -非常用存取（標準- IA）

  ◦ Amazon S3 One Zone -不常用存取（單一區域- IA）

  ◦ Amazon S3智慧分層

  ◦ Amazon商業雲端服務

  ◦ 從 ONTAP 9.11.1 開始、 Amazon S3 Glacier 即時擷取（ FabricPool 不支援 Glacier Flexible Retrieval 或 Glacier Deep Archive ）

  "Amazon Web Services 文件： Amazon S3 儲存課程"

  如需未列出的儲存類別資訊、請聯絡您的銷售代表。

- 在支援的基礎上、支援從通用SSD（gp2）和Amazon Elastic Block Store（EBS）的Througs Optimized HDD（ST1）Volume進行分層。Cloud Volumes ONTAP FabricPool

步驟

1. 使用指定 Amazon S3 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type AWS_S3` 參數。

   ◦ 您可以使用 `-auth-type CAP` 取得 C2S 存取認證的參數。

   當您使用時 `-auth-type CAP` 參數、您必須使用 `-cap-url` 指定完整 URL 以要求 C2S 存取的暫存認證的參數。

   ◦ ◦ `storage aggregate object-store config create` 如果 ONTAP 無法使用提供的資訊存取

Amazon S3 、則命令會失敗。

- 您可以使用 `-access-key` 此參數可指定存取金鑰、以將要求授權給 Amazon S3 物件存放區。
- 您可以使用 `-secret-password` 此參數可指定密碼（秘密存取金鑰）、以驗證對 Amazon S3 物件存放區的要求。
- 如果 Amazon S3 密碼已變更、您應該立即更新儲存在 ONTAP 中的對應密碼。

  如此一來、 ONTAP 就能在不中斷的情況下存取 Amazon S3 中的資料。

```
cluster1::> storage aggregate object-store config create
-object-store-name my_aws_store -provider-type AWS_S3
-server s3.amazonaws.com -container-name my-aws-bucket
-access-key DXJRXHPXHYXA9X31X3JX
```

+

```
cluster1::> storage aggregate object-store config create -object-store
-name my_c2s_store -provider-type AWS_S3 -auth-type CAP -cap-url
https://123.45.67.89/api/v1/credentials?agency=XYZ&mission=TESTACCT&role
=S3FULLACCESS -server my-c2s-s3server-fqdn -container my-c2s-s3-bucket
```

2. 使用顯示並驗證 Amazon S3 組態資訊 `storage aggregate object-store config show` 命令。

   。 `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 Amazon S3 組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **Google Cloud Storage** 設定為 **ONTAP FabricPool** 雲端層

如果您執行ONTAP 的是32個以上版本的版本、您可以將Google Cloud Storage設定為FabricPool 適用的雲端層。

搭配**FabricPool** 使用**Google Cloud Storage**的其他考量事項

- 一個"NetApp Cloud Tiering 許可證"在分層到 Google Cloud Storage 時是必需的。
- 建議ONTAP 將用於連接Google Cloud Storage物件伺服器的LIF放在10 Gbps連接埠上。
- 在支援下列Google Cloud Object儲存課程的支援對象包括：AFF FAS ONTAP Select FabricPool
  - Google Cloud Multi-Regional
  - Google Cloud區域

- Google Cloud Nearline
- Google Cloud Coldline

  "Google Cloud：儲存類別"

步驟

1. 使用指定 Google Cloud Storage 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type GoogleCloud` 參數。

   - 。 `storage aggregate object-store config create` 如果 ONTAP 無法使用所提供的資訊存取 Google Cloud Storage 、則命令會失敗。
   - 您可以使用 `-access-key` 此參數可指定存取金鑰、以將要求授權給 Google Cloud Storage 物件儲存區。
   - 如果Google Cloud Storage密碼已變更、您應該ONTAP 立即更新儲存在BIOS中的對應密碼。

     如此一來、即可讓支援中心在不中斷的情況下存取Google Cloud Storage中的資料。ONTAP

   ```
   storage aggregate object-store config create my_gcp_store_1 -provider
   -type GoogleCloud  -container-name my-gcp-bucket1 -access-key
   GOOGAUZZUV2USCFGHGQ511I8
   ```

2. 使用顯示和驗證 Google Cloud Storage 組態資訊 `storage aggregate object-store config show` 命令。

   。 `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 Google 雲端儲存組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **IBM Cloud Object Storage** 設定為 **ONTAP FabricPool** 雲端層

如果您執行ONTAP 的是版本不符合要求的9.5或更新版本、可以將IBM Cloud Object Storage設定為FabricPool 適用的雲端層。

搭配**FabricPool** 使用**IBM Cloud Object Storage**的考量事項

- 一個"NetApp Cloud Tiering 許可證"在分層到 IBM Cloud Object Storage 時是必要的。
- 建議ONTAP 將用於連接IBM Cloud物件伺服器的LIF放在10 Gbps連接埠上。

步驟

1. 使用指定 IBM Cloud Object Storage 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type IBM_COS` 參數。

- 。 `storage aggregate object-store config create` 如果 ONTAP 無法使用提供的資訊存取 IBM Cloud Object Storage 、則命令會失敗。
- 您可以使用 `-access-key` 此參數可指定存取金鑰、以將要求授權給 IBM Cloud Object Storage 物件存放區。
- 您可以使用 `-secret-password` 此參數可指定密碼（秘密存取金鑰）、以驗證對 IBM Cloud Object Storage 物件儲存區的要求。
- 如果IBM Cloud Object Storage密碼已變更、您應該ONTAP 立即更新儲存在BIOS中的對應密碼。

  如此一來、即可讓支援中心在不中斷的情況下存取IBM Cloud Object Storage中的資料。ONTAP

```
storage aggregate object-store config create
-object-store-name MyIBM -provider-type IBM_COS
-server s3.us-east.objectstorage.softlayer.net
-container-name my-ibm-cos-bucket -access-key DXJRXHPXHYXA9X31X3JX
```

2. 使用顯示及驗證 IBM Cloud Object Storage 組態資訊 `storage aggregate object-store config show` 命令。

   。 `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 IBM 雲端物件儲存組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

將 **Azure Blob Storage** 設定為 **ONTAP FabricPool** 雲端層

如果您執行的是 ONTAP 9.4 或更新版本，您可以將 Azure Blob 儲存設備設定為 FabricPool 的雲端層。

搭配**FabricPool** 使用**Microsoft Azure Blob**儲存設備的考量事項

- 一個"NetApp Cloud Tiering 許可證"在分層到 Azure Blob 儲存體時是必要的。
- 如果您搭配使用Azure Blob Storage搭配使用、則不需要取得此功能的證書。FabricPool Cloud Volumes ONTAP
- 建議ONTAP 將用於連接Azure Blob Storage物件伺服器的LIF放在10 Gbps連接埠上。
- 目前不支援Azure Stack（內部部署Azure服務）FabricPool 。
- 在Microsoft Azure Blob Storage的帳戶層級、FabricPool 不支援熱儲存層和冷儲存層。

  不支援Blob層級分層。FabricPool也不支援分層至Azure的歸檔儲存層。

關於這項工作

目前不支援Azure Stack（內部部署Azure服務）FabricPool 。

步驟

1. 使用指定 Azure Blob Storage 組態資訊 `storage aggregate object-store config create` 命令 `-provider-type Azure_Cloud` 參數。

   ◦ ◦ `storage aggregate object-store config create` 如果 ONTAP 無法使用所提供的資訊存取 Azure Blob 儲存設備、則命令會失敗。

   ◦ 您可以使用 `-azure-account` 指定 Azure Blob Storage 帳戶的參數。

   ◦ 您可以使用 `-azure-private-key` 此參數可指定驗證 Azure Blob Storage 要求的存取金鑰。

   ◦ 如果Azure Blob儲存設備密碼已變更、您應ONTAP 立即更新儲存在BIOS中的對應密碼。

   如此一來、即可讓支援中心在不中斷的情況下存取Azure Blob Storage中的資料。ONTAP

```
cluster1::> storage aggregate object-store config create
-object-store-name MyAzure -provider-type Azure_Cloud
-server blob.core.windows.net -container-name myAzureContainer
-azure-account myAzureAcct -azure-private-key myAzureKey
```

2. 使用顯示並驗證 Azure Blob Storage 組態資訊 `storage aggregate object-store config show` 命令。

   ◦ `storage aggregate object-store config modify` 命令可讓您修改 FabricPool 的 Azure Blob 儲存設備組態資訊。

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置修改"
- "儲存聚合物件儲存配置顯示"

在 **MetroCluster** 配置中為 **ONTAP FabricPool** 設定物件存儲

如果您執行ONTAP 的是更新版本的版本、您可以在FabricPool 一個靜態組態上設定鏡射版的功能、MetroCluster 將冷資料分層處理至兩個不同故障區的物件儲存區。

關於這項工作

- 在不需要基礎鏡射Aggregate和相關物件存放區組態的情況下、必須由相同的組態擁有。FabricPool MetroCluster MetroCluster
- 您無法將Aggregate附加至遠端MetroCluster 站台所建立的物件存放區。
- 您必須在MetroCluster 擁有Aggregate的物件儲存組態上建立物件儲存組態。

開始之前

- 此功能已設定完成、並已正確設定。MetroCluster
- 在適當MetroCluster 的實體網站上設置兩個物件儲存區。
- 每個物件存放區都會設定容器。

- IP空間是在兩MetroCluster 個「知識區」組態上建立或識別、其名稱相符。

步驟

1. 使用在每個 MetroCluster 站台上指定物件儲存區組態資訊 `storage object-store config create` 命令。

   在此範例中FabricPool 、MetroCluster 只有一個叢集需要使用此功能。為該叢集建立兩個物件存放區組態、每個物件存放區一個組態。

```
storage aggregate
    object-store config create -object-store-name mcc1-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-1> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate object-store config create -object-store-name mcc1-
ostore-config-s2
    -provider-type SGWS -server <SGWS-server-2> -container-name <SGWS-
bucket-2> -access-key <key> -secret-password <password> -encrypt
<true|false> -provider <provider-type>
    -is-ssl-enabled <true|false> ipspace <IPSpace>
```

   此範例可在FabricPool 採用列舉功能的第二個叢集上設定功能。MetroCluster

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s1
-provider-type SGWS -server
    <SGWS-server-1> -container-name <SGWS-bucket-3> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

```
storage aggregate
    object-store config create -object-store-name mcc2-ostore-config-s2
-provider-type SGWS -server
    <SGWS-server-2> -container-name <SGWS-bucket-4> -access-key <key>
-secret-password <password> -encrypt
    <true|false> -provider <provider-type> -is-ssl-enabled <true|false>
ipspace
    <IPSpace>
```

相關資訊

- "儲存物件儲存配置創建"

測試 **ONTAP** 雲端層的延遲和處理量效能

在將物件存放區附加至本機層之前、您可以使用物件存放區 Profiler 來測試物件存放區的延遲和處理量效能。

物件存放區檔案器結果是 ONTAP 與雲端層物件存放區之間的連線量測，使用 4 MB 的放置和隨機讀取位元組範圍的大小介於 4 MB 到 256 KB 之間。（只有 SnapMirror 等內部 ONTAP 功能可以使用大於 32KB 的「取得」。）

由於物件存放區 Profiler 的結果並不代表競爭工作負載或獨特的用戶端應用程式行為，因此無法完美地顯示分層效能。

開始之前

- 您必須先將雲端層新增至 ONTAP 、才能將其與物件存放區檔案器搭配使用。
- 您必須處於 ONTAP CLI 進階權限模式。

步驟

1. 啟動物件存放區 Profiler ：

   ```
   storage aggregate object-store profiler start -object-store-name <name> -node
   <name>
   ```

2. 檢視結果：

   ```
   storage aggregate object-store profiler show
   ```

相關資訊

- "儲存聚合物件儲存分析器顯示"
- "儲存聚合物件儲存分析器啟動"

將 **ONTAP** 雲端層與本機層建立關聯

將物件存放區設定為雲端層之後，您可以將其附加至 FabricPool ，以指定要使用的本機

層。在 ONTAP 9.5 或更新版本中，您也可以附加包含合格 FlexGroup Volume 成分的本機階層。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

關於這項工作

將雲端層附加到本機層是一項永久性動作。附加雲端層之後、無法從本機層解除附加。不過、您可以使用"FabricPool 鏡射"將本機層附加至不同的雲端層。

開始之前

當您使用 ONTAP CLI 設定 FabricPool 的本機層時，本機層必須已經存在。

> 當您使用System Manager設定本地層FabricPool 以供執行效能分析時、您可以建立本機層、並將其設定FabricPool 為同時用於執行效能分析。

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 將本機層附加至 FabricPool 物件存放區。

系統管理員

1. 瀏覽至 * 儲存設備 > Tiers* 、選取雲端層、然後按一下 ⋮。
2. 選取*「附加本機層級」*。
3. 在「新增為主要」下、確認磁碟區符合附加條件。
4. 如有必要、請選取*將磁碟區轉換成精簡配置*。
5. 按一下「 * 儲存 * 」。

CLI

若要使用**CLI**將物件存放區附加至**Aggregate**：

1. 選用：若要查看磁碟區中有多少資料處於非使用中狀態、請依照中的步驟進行 "使用非作用中資料報告來判斷Volume中有多少資料處於非作用中狀態"。

   查看某個Volume中有多少資料處於非作用中狀態、有助於決定哪些Aggregate可用於FabricPool 哪些用途。

2. 使用將物件存放區附加至 Aggregate `storage aggregate object-store attach` 命令。

   如果 FabricPool 從未使用過 Aggregate 、而且其中包含現有的 Volume 、則會將這些 Volume 指派為預設 `snapshot-only` 分層原則。

   ```
   cluster1::> storage aggregate object-store attach -aggregate myaggr
   -object-store-name Amazon01B1
   ```

   您可以使用 `allow-flexgroup true` 可附加包含 FlexGroup Volume 成分的集合體。

3. 顯示物件存放區資訊、並使用來驗證附加的物件存放區是否可用 `storage aggregate object-store show` 命令。

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   myaggr       Amazon01B1           available
   ```

相關資訊

- "存儲聚合物件存儲附加"
- "儲存聚合物件儲存顯示"

將資料分層到本地 **ONTAP S3** 儲存桶

從功能支援的9.8開始ONTAP 、您可以使用ONTAP 功能支援的S3、將資料分層至本機物件儲存設備。

將資料分層至本機儲存庫、是將資料移至不同本機層的簡單替代方案。此程序使用本機叢集上的現有儲存區，或讓 ONTAP 自動建立新的儲存 VM 和新的儲存區。

請記住，一旦您連接了主要的本機貯體，就無法將其取消連接。

開始之前

- 此工作流程需要S3授權、以建立新的S3伺服器和新儲存區、或使用現有的伺服器。本授權包含在"ONTAP One"中。此工作流程不需要使用此功能的不含授權。FabricPool
- "啟用ONTAP 對本地FabricPool 資訊的「支援」功能、以存取「S3」"。

步驟

1. 將資料分層至本機儲存區：按一下 * 儲存區 > Tiers* ，在 * SSD * 窗格中選取本機層，按一下 ，然後選取 * 階層至本機儲存區 * 。
2. 在 * 主要階層 * 區段中，選擇 * 現有 * 或 * 新 * 。
3. 按一下「 * 儲存 * 」。

管理FabricPool

使用非使用中的資料報告來分析非使用中的 **ONTAP** 資料

查看磁碟區中有多少資料處於非使用中狀態、可讓您充分運用儲存層。非作用中資料報告中的資訊可協助您決定FabricPool 哪些Aggregate可用於哪些用途、是將Volume移入FabricPool 或移出、或是修改Volume的分層原則。

開始之前

您必須執行ONTAP 更新版本的版本、才能使用非作用中的資料報告功能。

關於這項工作

- 某些Aggregate不支援非作用中資料報告。

  無法啟用Inactive data報告功能時、您無法啟用FabricPool 此功能、包括下列情況：

  - 根Aggregate
  - 執行9.7之前版本之非功能的MetroCluster ONTAP
  - Flash Pool（混合式Aggregate或SnapLock
- 在任何磁碟區啟用調適性壓縮的集合體上、預設會啟用非作用中資料報告。
- 根據預設ONTAP 、在所有SSD Aggregate上啟用非作用中資料報告功能、只要執行動作即可。
- 根據預設FabricPool 、非作用中的資料報告功能會在ONTAP 支援的情況下、於支援的情況下、於支援的情況下、於支援的情況下、ONTAP
- 您可以使用ONTAP 包含HDD Aggregate在內的NetApp資源中心、從ONTAP 使用支援功能的支援功能到非FabricPool Aggregate、啟用非使用中資料報告功能、從功能性的9.6開始。

程序

您可以使用ONTAP 「無法使用的資料」功能來判斷哪些資料無法使用「功能」或ONTAP 「功能」CLI。

系統管理員

1. 請選擇下列其中一個選項：
   - 當您擁有現有的 HDD 集合體時、請瀏覽至 * 儲存設備 > Tiers* 、然後按一下 ⋮ 以取得您要啟用非作用中資料報告的集合體。
   - 若未設定任何雲端階層、請瀏覽至*儀表板*、然後按一下* Capacity 下的 Enable inactive data report*連結。

CLI

若要使用**CLI**啟用非作用中資料報告：

1. 如果您要查看非作用中資料報告的集合體未用於 FabricPool 、請使用啟用非作用中的彙總資料報告 `storage aggregate modify` 命令 `-is-inactive-data-reporting-enabled true` 參數。

```
cluster1::> storage aggregate modify -aggregate aggr1 -is-inactive
-data-reporting-enabled true
```

   您必須在非FabricPool 用於支援的Aggregate上明確啟用非作用中資料報告功能。

   您無法也不需要在啟用FabricPool的Aggregate上啟用非作用中資料報告、因為Aggregate已隨附非作用中資料報告。。 `-is-inactive-data-reporting-enabled` 參數無法用於啟用 FabricPool 的集合體。

   。 `-fields is-inactive-data-reporting-enabled` 的參數 `storage aggregate show` 命令會顯示是否在 Aggregate 上啟用非作用中的資料報告。

2. 若要顯示磁碟區上有多少資料處於非作用中狀態、請使用 `volume show` 命令 `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` 參數。

```
cluster1::> volume show -fields performance-tier-inactive-user-
data,performance-tier-inactive-user-data-percent

vserver volume performance-tier-inactive-user-data performance-tier-
inactive-user-data-percent
------- ------ ---------------------------------
-----------------------------------------
vsim1   vol0   0B                                 0%
vs1     vs1rv1 0B                                 0%
vs1     vv1    10.34MB                            0%
vs1     vv2    10.38MB                            0%
4 entries were displayed.
```

   - 。 `performance-tier-inactive-user-data` 欄位會顯示儲存在 Aggregate 中的使用者資料處於非作用中狀態的程度。
   - 此 `performance-tier-inactive-user-data-percent`欄位會顯示作用中檔案系統和快照中的非作用中資

料百分比。

- 對於不用於FabricPool 不供使用的Aggregate、非作用中的資料報告會使用分層原則來決定要報告多少資料為冷資料。
  - 適用於 `none` 分層原則使用 31 天。
  - 適用於 `snapshot-only` 和 `auto`、非使用中的資料報告用途 `tiering-minimum-cooling-days`。
  - 適用於 `ALL` 原則、非作用中的資料報告會假設資料會在一天內分級。

    直到達到週期為止、輸出會顯示非作用中資料量的「」、而非數值。
- 在屬於某個部分的磁碟區上FabricPool 、不活動的功能取決於在某個磁碟區上設定的分層原則。ONTAP
  - 適用於 `none` 分層原則、 ONTAP 會報告整個磁碟區中至少 31 天沒有作用的數量。您無法使用 `-tiering-minimum-cooling-days` 參數 `none` 分層原則。
  - 適用於 `ALL`、 `snapshot-only`和 `auto` 不支援分層原則、非作用中資料報告。

相關資訊

- "儲存聚合修改"

管理 FabricPool 的 Volume

在啟用 FabricPool 的 ONTAP 本機層上建立磁碟區

您可以直接在啟用 FabricPool 的本機層中建立新的磁碟區，或將現有的磁碟區從另一個本機層移至啟用 FabricPool 的本機層，將這些磁碟區新增至 FabricPool 。

> 在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

當您建立FabricPool 一個供使用的Volume時、您可以選擇指定分層原則。如果未指定分層原則、則建立的磁碟區會使用預設值 `snapshot-only` 分層原則。適用於具有的 Volume `snapshot-only` 或 `auto` 分層原則、您也可以指定分層的最低冷卻週期。

開始之前

- 設定要使用的 Volume `auto` 分層原則或指定分層最低冷卻週期需要 ONTAP 9.4 或更新版本。
- 使用本解決方法需要使用更新版本的版本。FlexGroup ONTAP
- 設定要使用的 Volume `all` 分層原則需要 ONTAP 9.6 或更新版本。
- 設定要使用的 Volume `-cloud-retrieval-policy` 參數需要 ONTAP 9.8 或更新版本。

步驟

1. 使用為 FabricPool 建立新的 Volume `volume create` 命令。
   - 。 `-tiering-policy` 選用參數可讓您指定磁碟區的分層原則。

您可以指定下列分層原則之一：

- `snapshot-only` （預設）
- `auto`
- `all`
- `backup` （已過時）
- `none`

  "分層原則的類型FabricPool"

。。 `-cloud-retrieval-policy` 選用參數可讓具有進階權限層級的叢集管理員覆寫由分層原則控制的預設雲端移轉或擷取行為。

您可以指定下列其中一個雲端擷取原則：

- `default`

  分層原則會決定哪些資料會被拉回、因此雲端資料擷取不會有任何變更 `default` 雲端擷取原則。這表示這種行為與ONTAP 9.8之前版本相同：

  - 如果分層原則是 `none` 或 `snapshot-only`接著、「預設」表示任何用戶端導向的資料讀取都會從雲端層移至效能層。
  - 如果分層原則是 `auto`，則會拉出任何用戶端驅動的隨機讀取，但不會拉出連續讀取。
  - 如果分層原則是 `all` 然後、不會從雲端層擷取任何用戶端導向的資料。
- `on-read`

  所有用戶端導向的資料讀取都會從雲端層提取到效能層。
- `never`

  不會將用戶端導向的資料從雲端層提取到效能層
- `promote`
  - 用於分層原則 `none`、所有雲端資料都會從雲端層移至效能層
  - 用於分層原則 `snapshot-only`、所有作用中的檔案系統資料都會從雲端層移至效能層。

。。 `-tiering-minimum-cooling-days` 進階權限層級中的選用參數可讓您指定使用的磁碟區的分層最低冷卻期間 `snapshot-only` 或 `auto` 分層原則。

從功能表9.8開始ONTAP 、您可以指定2到183之間的值、以供分層的最低冷卻天數使用。如果您使用ONTAP 的是9.8之前的版本、則可在分層的最低冷卻天數中指定介於2到63之間的值。

建立**FabricPool** 一套供參考的**Volume**範例

以下範例在啟用 FabricPool 的本機層中建立名為「 myFabricPool 」的 Volume 。分層原則設為，分層最低冷卻期間設 `auto`為 45 天：

```
cluster1::*> volume create -vserver myVS -aggregate myFabricPool
-volume myvol1 -tiering-policy auto -tiering-minimum-cooling-days 45
```

相關資訊

"資料區管理FlexGroup"

將磁碟區移至啟用 **FabricPool** 的 **ONTAP** 本機層

A "Volume搬移" 是 ONTAP 在不中斷營運的情況下，將磁碟區從一個本機層（來源）移至另一個（目的地）的方式。雖然最常見的原因是硬體生命週期管理，叢集擴充和負載平衡，但由於各種原因，可以執行磁碟區移動。

請務必瞭解磁碟區移動如何與 FabricPool 搭配運作，因為本機層，附加雲端層和磁碟區（磁碟區分層原則）所發生的變更都會對功能造成重大影響。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

目的地本端層

如果 Volume Move 的目的地本端層沒有附加的雲端層，則儲存在雲端層的來源磁碟區上的資料會寫入目的地本端層的本端層。

從 ONTAP 9.8 開始，當磁碟區已啟用時"非作用中資料報告"， FabricPool 會使用磁碟區的熱圖，立即將冷資料排入佇列，以便在寫入目的地本機層時立即開始分層。

在 ONTAP 9.8 之前，將磁碟區移至另一個本機層會重設本機層區塊的閒置期間。例如，使用自動磁碟區分層原則的磁碟區，若本機層上的資料已停用 20 天，但尚未分層，則在磁碟區移動後，資料的溫度將會重設為 0 天。

最佳化的 **Volume** 搬移

從 ONTAP 9.6 開始，如果 Volume Move 的目的地本端層使用與來源本端層相同的貯體，則儲存在該貯體中的來源 Volume 上的資料不會移回本端層。階層式資料會保持靜止，只有熱資料需要從一個本機層移至另一個層級。這項最佳化的 Volume 搬移可大幅提升網路效率。

例如，300TB 最佳化磁碟區移動意味著即使 300TB 冷資料從一個本地層移動到另一個本地層，也不會觸發對物件儲存的 300TB 讀取和 300TB 寫入。

未最佳化的 Volume 搬移會產生額外的網路和運算流量（讀取 / 取得和寫入 / 放置），增加對 ONTAP 叢集和物件存放區的需求，可能會在分層到公有物件存放區時增加成本。

部分組態與最佳化的 Volume 移動不相容：

- 在磁碟區移動期間變更分層原則
- 使用不同加密金鑰的來源和目的地本機層
- FlexClone Volume
- FlexClone 父磁碟區
- MetroCluster （支援 ONTAP 9.8 及更新版本中最佳化的 Volume 搬移）
- 非同步的 FabricPool 鏡射貯體

如果 Volume Move 的目的地本端層有附加的雲端層，則儲存在雲端層的來源磁碟區上的資料會先寫入目的地本端層的本端層。如果此方法適用於磁碟區的分層原則，則會寫入目的地本機層的雲端層。

先將資料寫入本機層，可改善磁碟區移動的效能，並縮短轉換時間。如果在執行磁碟區移動時未指定磁碟區分層原則，則目的地磁碟區會使用來源磁碟區的分層原則。

如果在執行磁碟區移動時指定不同的分層原則，則會使用指定的分層原則建立目的地磁碟區，而且不會最佳化磁碟區移動。

Volume 中繼資料

無論磁碟區移動是否經過最佳化，ONTAP 都會儲存大量有關所有資料（包括本機資料和分層資料）的位置、儲存效率、權限、使用模式等的元資料。元資料始終保留在本地層，不會進行分層。當磁碟區從一個本機層移至另一個層時，也需要將此資訊移至目的地本機層。

持續時間

磁碟區移動仍然需要時間才能完成，並且預期優化卷移動將花費與移動等量非分層資料大約相同的時間。

重要的是要理解 `volume move show`命令並不代表從雲層移動的資料的吞吐量，而是代表在本地更新的捲資料。

在 SVM DR 關係中，來源和目的地磁碟區必須使用相同的分層原則。

步驟

1. 使用 `volume move start`命令將磁碟區從來源本機層移至目的地本機層。

移動 **Volume** 的範例

以下範例將名為 SVM 的 `vs1`磁碟區移 `myvol2`至 `dest_FabricPool`啟用 FabricPool 的本機層。

```
cluster1::> volume move start -vserver vs1 -volume myvol2
-destination-aggregate dest_FabricPool
```

讓 **FabricPool** 中的 **ONTAP Volume** 直接寫入雲端

從 ONTAP 9.14.1 開始、您可以在 FabricPool 中的新磁碟區或現有磁碟區上、啟用和停用直接寫入雲端的功能、讓 NFS 用戶端無需等待分層掃描即可直接將資料寫入雲端。SMB

用戶端仍會寫入雲端寫入磁碟區中的效能層。預設會停用雲端寫入模式。

如果能夠直接寫入雲端、就有助於移轉等案例、例如將大量資料傳輸到叢集、而叢集無法在本機層上支援。如果沒有雲端寫入模式、在移轉期間會傳輸較少的資料、然後分層、再重新傳輸和分層、直到移轉完成為止。使用雲端寫入模式時、不再需要這類管理、因為資料永遠不會傳輸到本機層。

開始之前

- 您應該是叢集或 SVM 管理員。
- 您必須處於進階權限層級。
- 磁碟區必須是讀寫類型的磁碟區。
- 磁碟區必須具有所有分層原則。

在磁碟區建立期間、可直接寫入雲端

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 建立磁碟區並啟用雲端寫入模式：

```
volume create -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled <true|false> -aggregate <local tier name>
```

以下範例建立在 FabricPool 本機層（ aggr1 ）上啟用雲端寫入功能的名為 vol1 的磁碟區：

```
volume create -vserver vs1 -volume vol1 -is-cloud-write-enabled true
-aggregate aggr1
```

可直接寫入現有磁碟區的雲端

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 修改磁碟區以啟用雲端寫入模式：

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled true
```

以下範例修改名為 vol1 的磁碟區，以啟用雲端寫入：

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled true
```

停用直接寫入磁碟區上的雲端

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 停用磁碟區上的雲端寫入模式：

```
volume modify -vserver <svm name> -volume <volume name> -is-cloud-write
-enabled false
```

以下範例停用名為 vol1 的磁碟區上的雲端寫入模式：

```
volume modify -vserver vs1 -volume vol1 -is-cloud-write-enabled false
```

在 **FabricPool** 中啟用 **ONTAP Volume** 以執行主動式讀取

從 ONTAP 9 · 14.1 開始，您可以在 FabricPools 中的磁碟區上啟用和停用主動式預先讀取模式。在 ONTAP 9.13.1 中，主動預讀模式僅在雲端平台上推出。從 ONTAP 9.14.1 開始，主動預讀模式可在 FabricPool 支援的所有平台（包括本機平台）上使用。此功能預設為停用。

當主動式預先讀取設為 *disabled* 時， FabricPool 只會讀取用戶端應用程式所需的檔案區塊，而不需要讀取整個檔案。這可能會導致網路流量降低，尤其是大型 GB 和 TB 大小的檔案。在磁碟區上啟用主動式預先讀取會關閉此功能，而 FabricPool 會從物件存放區中預先讀取整個檔案，增加取得處理量並減少用戶端讀取檔案的延遲。依預設，當階層式資料依序讀取時，會保持冷態，不會寫入本機層。

積極的預先讀取功能可提高網路效率，以提升階層式資料的效能。

關於這項工作

。 `aggressive-readahead-mode` 命令有兩個選項：

- `none`：預先讀取已停用。
- `file_prefetch`：系統會先將整個檔案讀取到用戶端應用程式的記憶體中。

開始之前

- 您應該是叢集或 SVM 管理員。

- 您必須處於進階權限層級。

在磁碟區建立期間啟用主動式預先讀取模式

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 建立磁碟區並啟用主動式預先讀取模式：

```
volume create -volume <volume name>  -aggressive-readahead-mode
<none|file_prefetch>
```

以下範例建立一個名為 vol1 的 Volume 、其中啟用檔案預先擷取選項的主動式預先讀取功能：

```
volume create -volume vol1 -aggressive-readahead-mode file_prefetch
```

停用主動預先讀取模式

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 停用主動式預先讀取模式：

```
volume modify -volume <volume name>  -aggressive-readahead-mode none
```

以下範例修改名為 vol1 的磁碟區、以停用主動式預先讀取模式：

```
volume modify -volume vol1 -aggressive-readahead-mode none
```

檢視磁碟區上的主動式預先讀取模式

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 檢視積極的預先讀取模式：

```
volume show -fields aggressive-readahead-mode
```

使用使用者建立的自訂標記來管理 **ONTAP FabricPool Volume**

從使用者建立的自訂標記開始ONTAP 、FabricPool 支援物件標記功能、讓您能夠分類及排序物件、以便更輕鬆地管理。如果您是具有管理權限層級的使用者、可以建立新的物件標記、以及修改、刪除和檢視現有標記。

在磁碟區建立期間指派新標記

當您想要將一或多個標記指派給新物件、並從您建立的新磁碟區分層時、可以建立新的物件標記。您可以使用標記來協助分類及排序分層物件、以利資料管理。從ONTAP 功能介紹9.8開始、您可以使用System Manager建立物件標籤。

關於這項工作

您只能在FabricPool 連接StorageGRID 到不只是一個的資料集上設定標籤。這些標記會在Volume移動期間保留。

- 每個卷最多允許四個標籤。
- 在 CLI 中，每個物件標籤都必須是以等號分隔的金鑰值配對。
- 在 CLI 中，多個標籤必須以逗號分隔。
- 每個標記值最多可包含 127 個字元。
- 每個標記鍵都必須以字母字元或底線開頭。

  金鑰只能包含英數字元和底線、最多允許127個字元。

您可以使用ONTAP 物件標籤來指派物件標籤。ONTAP

範例 **8.** 步驟

系統管理員

1. 瀏覽至*儲存設備> Tiers*。
2. 找出含有您要標記之磁碟區的儲存層。
3. 按一下「* Volumes （*磁碟區）
4. 找到您要標記的磁碟區、然後在「物件標籤」欄中選取「按一下以輸入標籤」。
5. 輸入金鑰和值。
6. 按一下「 * 套用 * 」。

CLI

1. 使用 `volume create` 命令 `-tiering-object-tags` 選項可建立具有指定標記的新 Volume 。您可以使用以逗號分隔的配對來指定多個標記：

```
volume create [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1>
[,<key2=value2>,<key3=value3>,<key4=value4> ]
```

下列範例會建立一個名為fp_dvolume1的磁碟區、其中包含三個物件標籤。

```
vol create -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=abc,content=data
```

修改現有標記

您可以變更標記的名稱、取代物件存放區中現有物件上的標記、或是新增不同的標記至您打算稍後新增的新物件。

範例 **9.** 步驟

系統管理員

1. 瀏覽至*儲存設備> Tiers*。
2. 找出含有您要修改之標記的磁碟區儲存層。
3. 按一下「* Volumes （*磁碟區）
4. 找到含有您要修改之標記的磁碟區、然後在*物件標記*欄中按一下標記名稱。
5. 修改標記。
6. 按一下「 * 套用 * 」。

CLI

1. 使用 `volume modify` 命令 `-tiering-object-tags` 修改現有標記的選項。

```
volume modify [ -vserver <vserver name> ] -volume <volume_name>
-tiering-object-tags <key1=value1> [ ,<key2=value2>,
<key3=value3>,<key4=value4> ]
```

以下範例變更現有標籤的名稱 `type=abc`到 `type=xyz` 。

```
vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags
project=fabricpool,type=xyz,content=data
```

刪除標記

您可以刪除不再需要在磁碟區或物件存放區中的物件上設定的物件標記。

範例 **10.** 步驟

系統管理員

1. 瀏覽至*儲存設備> Tiers*。
2. 找出含有您要刪除標記的磁碟區儲存層。
3. 按一下「* Volumes （*磁碟區）
4. 找到含有您要刪除標記的磁碟區、然後在「物件標記」欄中按一下標記名稱。
5. 若要刪除標記、請按一下垃圾桶圖示。
6. 按一下「 * 套用 * 」。

CLI

1. 使用 `volume modify` 命令 `-tiering-object-tags` 選項後面接著空白值 (""）刪除現有標記。

   下列範例會刪除fp_dvolum1上的現有標記。

   ```
   vol modify -volume fp_volume1 -vserver vs0 -tiering-object-tags ""
   ```

檢視**Volume**上的現有標記

您可以檢視磁碟區上現有的標記、查看哪些標記可供使用、然後再將新標記附加至清單。

步驟

1. 使用 `volume show`帶有選項的命令 `tiering-object-tags`可查看捲上的現有標記。

   ```
   volume show [ -vserver <vserver name> ] -volume <volume_name> -fields
   tiering-object-tags
   ```

檢查**FabricPool** 物件標記狀態的資訊

您可以檢查一FabricPool 或多個版本的功能是否已完成標記。

步驟

1. 使用 `vol show`命令搭配 `-fields needs-object-retagging`選項、查看標記是否正在進行、是否已完成、或是否未設定標記。

   ```
   vol show -fields needs-object-retagging  [ -instance | -volume <volume
   name>]
   ```

   將顯示下列其中一個值：

   ◦ `true`：對象標記掃描程序尚未運行或需要再次運行此卷

- `false`：物件標記掃描器已完成此 Volume 的標記
- `<->`：對象標記掃描儀不適用於此卷。這種情況發生在未駐留在FabricPools上的磁碟區。

監控啟用 **FabricPool** 的 **ONTAP** 本機層的空間使用率

您需要知道資料儲存在效能和雲端層FabricPool 中的資料量、才能供VMware使用。這些資訊可協助您判斷是否需要變更磁碟區的分層原則、增加FabricPool 未獲授權的使用量限制、或是增加雲端層的儲存空間。

在 ONTAP 9.7 之前，系統管理員使用術語 _Aggregate _ 來描述 _ 本機層 _ 。無論您的 ONTAP 版本為何， ONTAP CLI 都會使用術語 _Aggregate 。若要深入瞭解本機階層，請參閱"磁碟和本機層"。

關於這項工作

從 ONTAP 9.18.1 開始， `storage aggregate show-space` 指令變更了邏輯引用容量和邏輯非引用容量的報告方式。邏輯引用容量報告所有物件中的引用區塊以及碎片化物件中的非引用區塊。邏輯非引用容量僅報告已超過滿容量閾值且符合物件刪除和碎片整理條件的物件中的非引用區塊。

例如，當您使用 ONTAP S3 和 StorageGRID 的預設 Aggregate 完整度臨界值 40% 時，物件中 60% 的區塊必須未被引用，然後這些區塊才會被報告為未被引用的容量。

在 ONTAP 9.18.1 之前的版本中，「邏輯引用容量」會報告所有物件（包括已滿物件和碎片物件）中已引用的區塊。「邏輯未引用容量」會報告所有物件中未引用的區塊。

步驟

1. 使用下列其中一個命令來顯示資訊，以監控啟用 FabricPool 的本機階層的空間使用率：

如果您要顯示…	然後使用下列命令：
本機層中雲端層的使用大小	`storage aggregate show` 使用 `-instance` 參數
本機層內空間使用率的詳細資料，包括物件存放區的參考容量	`storage aggregate show-space` 使用 `-instance` 參數
附加至本機層的物件存放區空間使用率，包括使用的授權空間量	`storage aggregate object-store show-space`
本機層中的磁碟區清單，以及其資料和中繼資料的佔用空間	`volume show-footprint`

除了使用CLI命令之外、您也可以使用Active IQ Unified Manager 支援OnCommand 於更新版本叢集的支援功能的支援功能、以及使用支援的功能區（前身為「支援區塊整合管理程式FabricPool 」）、ONTAP 或是System Manager來監控空間使用率。

以下範例顯示FabricPool 如何顯示空間使用率及相關資訊以供參考：

```
cluster1::> storage aggregate show-space -instance

                          Aggregate: MyFabricPool
                                                                      ...
                                                 Aggregate Display Name:
MyFabricPool
                                                                      ...
                          Total Object Store Logical Referenced
Capacity: -
                          Object Store Logical Referenced Capacity
Percentage: -
                                                                      ...
                                                          Object Store
Size: -
                          Object Store Space Saved by Storage
Efficiency: -
                          Object Store Space Saved by Storage Efficiency
Percentage: -
                                                    Total Logical Used
Size: -
                                                    Logical Used
Percentage: -
                                              Logical Unreferenced
Capacity: -
                                            Logical Unreferenced
Percentage: -
```

```
cluster1::> storage aggregate show -instance

                           Aggregate: MyFabricPool
                           ...
                           Composite: true
                           Capacity Tier Used Size:
                           ...
```

```
cluster1::> volume show-footprint

Vserver : vs1
Volume : rootvol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Volume Guarantee                  MB          %
Flexible Volume Metadata          KB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %

Vserver : vs1
Volume : vol

Feature                             Used       Used%
--------------------------------- ---------- -----
Volume Footprint                  KB          %
Footprint in Performance Tier     KB          %
Footprint in Amazon01             KB          %
Flexible Volume Metadata          MB          %
Delayed Frees                     KB          %
Total Footprint                   MB          %
...
```

2. 視需要採取下列其中一項行動：

如果您想要...	然後...
變更磁碟區的分層原則	請遵循中的程序 "透過修改磁碟區的分層原則或分層最短冷卻時間來管理儲存分層"。
增加FabricPool 《不經認證的使用限制	請聯絡您的NetApp或合作夥伴銷售代表。 "NetApp支援"
增加雲端層的儲存空間	請聯絡您用於雲端層的物件存放區供應商。

相關資訊

- "儲存聚合對象"
- "儲存Aggregate顯示"
- "儲存聚合展示空間"

修改 ONTAP Volume 的分層原則和最低冷卻期

您可以變更磁碟區的分層原則、以控制當資料變成非作用中時、是否將其移至雲端層（_Cold）。適用於具有的 Volume `snapshot-only` 或 `auto` 分層原則、您也可以指定在將使用者資料移至雲端層之前、使用者資料必須保持非作用中狀態的分層最低冷卻期間。

開始之前

將 Volume 變更為 `auto` 分層原則或修改分層最低冷卻期需要 ONTAP 9.4 或更新版本。

關於這項工作

變更磁碟區的分層原則只會變更磁碟區的後續分層行為。它不會將資料追溯到雲端層。

變更分層原則可能會影響資料變冷並移至雲端層所需的時間。

"當您修改FabricPool 完一份Volume的分層原則時、會發生什麼情況"

> ⓘ 在 SVM DR 關係中，來源和目的地磁碟區不需要使用 FabricPool 集合體，但它們必須使用相同的分層原則。

步驟

1. 使用修改現有磁碟區的分層原則 `volume modify` 命令 `-tiering-policy` 參數：

   您可以指定下列分層原則之一：

   - `snapshot-only` （預設）
   - `auto`
   - `all`
   - `none`

     "分層原則的類型FabricPool"

2. 如果磁碟區使用 `snapshot-only` 或 `auto` 分層原則、而且您想要修改分層的最低冷卻期、請使用 `volume modify` 命令 `-tiering-minimum-cooling-days` 進階權限層級中的選用參數。

   您可以在分層的最小冷卻天數中指定介於2到183之間的值。如果您使用ONTAP 的是9.8之前的版本、則可在分層的最低冷卻天數中指定介於2到63之間的值。

修改分層原則的範例、以及磁碟區的分層最低冷卻週期

以下範例將 SVM 「 VS1 」中的 Volume 「 myvol 」分層原則變更為 `auto` 並將最低冷卻時間分層至 45 天：

```
cluster1::> volume modify -vserver vs1 -volume myvol
-tiering-policy auto -tiering-minimum-cooling-days 45
```

利用功能歸檔Volume FabricPool （影片）

本影片快速概述如何使用System Manager將Volume歸檔至FabricPool 採用效益分析技術

的雲端層。

"NetApp影片：利用FabricPool 功能來歸檔Volume（備份+ Volume Move）"

相關資訊

"NetApp TechCommTV：FabricPool 《支援目標清單"

修改 ONTAP Volume 的預設 FabricPool 分層原則

您可以使用變更 Volume 的預設分層原則、以控制從雲端層擷取的使用者資料、並將其變更為效能層 `-cloud-retrieval-policy` ONTAP 9.8 提供的選項。

開始之前

- 使用修改磁碟區 `-cloud-retrieval-policy` 選項需要 ONTAP 9.8 或更新版本。
- 您必須具備進階權限層級才能執行此作業。
- 您應該瞭解分層原則的行為 `-cloud-retrieval-policy`。

  "分層原則如何與雲端移轉搭配運作"

步驟

1. 使用修改現有磁碟區的分層原則行為 `volume modify` 命令 `-cloud-retrieval-policy` 選項：

```
 volume create -volume <volume_name> -vserver <vserver_name> - tiering-
policy <policy_name> -cloud-retrieval-policy
```

```
vol modify -volume fp_volume4 -vserver vs0 -cloud-retrieval-policy
promote
```

設定 ONTAP FabricPool 每個節點的放置速率閾值

身為儲存管理員，您可以使用 Put th化 設定每個節點最大置放率的上限。

當網路資源或物件存放區端點受到資源限制時，「放置節流」功能很有用。雖然資源限制很少，但在低功率物件儲存區或 FabricPool 使用量的第一天， TB 或 PB 的冷資料開始分層時，可能會發生資源限制。

Put 節流是根據節點而定。最小的放量節流設定速率限制為每秒 8 MB將輸入速率限制設為低於 8 MB / 秒的值，將會在該節點上產生 8 MB / 秒的處理量。同時分層的多個節點可能會佔用更多頻寬，並可能佔用容量極有限的網路連結。

FabricPool 讓營運不再與其他應用程式競爭資源。FabricPool Put 作業會由用戶端應用程式和其他 ONTAP 工作負載（例如 SnapMirror ）自動置於較低的優先順序（「霸凌」）。使用節流 `put-rate-limit`可能有助於減少與 FabricPool 分層相關聯的網路流量，但它與並行 ONTAP 流量無關。

開始之前

需要進階權限等級。

步驟

1. FabricPool 使用 ONTAP CLI 執行的節流操作：

```
storage aggregate object-store put-rate-limit modify -node <name>
-default <true|false> -put-rate-bytes-limit <integer>[KB|MB|GB|TB|PB]
```

相關資訊

- "修改儲存Aggregate物件存放區的傳輸率限制"

自訂 **ONTAP FabricPool** 物件刪除和碎片整理

FabricPool 不會刪除附加物件存放區的區塊。相反地， FabricPool 會在 ONTAP 不再參照某個百分比的物件區塊之後，刪除物件。

例如，在分層到 Amazon S3 的 4 MB 物件中，有 1 ， 024 個 4KB 區塊。在 ONTAP 參考不到 2054KB 區塊（ 1024 個區塊的 20% ）之前，不會發生磁碟重組和刪除。當足夠（ 1 ， 024 ）的區塊沒有參照時，會刪除其原始的 4 MB 物件，並建立新物件。

您可以自訂未回收空間臨界值百分比，並將其設為不同物件存放區的不同預設層級。預設設定為：

物件存放區	更新版本ONTAP	ONTAP 9.7 至 9.4	ONTAP 9.3 及更早版本	Cloud Volumes ONTAP
Amazon S3	20%	20%	0%	30%
Google Cloud Storage	20%	12%	不適用	35%
Microsoft Azure Blob 儲存設備	25%	15%	不適用	35%
NetApp ONTAP 產品系列S3	40%	不適用	不適用	不適用
NetApp StorageGRID	40%	40%	0%	不適用

未回收空間臨界值

變更預設的未回收空間臨界值設定，將會增加或減少已接受的物件重組量。減少分散會減少雲端層使用的實體容量，而犧牲額外的物件儲存資源（讀寫）。

臨界值減量

為了避免額外支出，請考慮在使用物件存放區定價方案時，降低未回收空間的臨界值，以降低儲存成本，但增加

讀取成本。範例包括 Amazon 的 Standard-IA 和 Azure Blob Storage 的 Cool 。

舉例來說，如果使用標準 IA 等定價方案，或是使用標準定價方案時，由於法律原因而節省的 10 年前專案數量，可能會比使用標準定價方案時更便宜。雖然此類磁碟區的讀取成本較高，包括物件重組所需的讀取，但不太可能經常發生。

臨界值增加

或者，如果物件分散會導致使用的物件儲存區容量大幅超過 ONTAP 所參照資料所需的容量，請考慮增加未回收空間臨界值。例如，在最糟的情況下，使用 20% 的未回收空間臨界值，所有物件都會平均分割至允許的最大範圍，這表示可能會有 80% 的雲端層總容量被 ONTAP 取消參照。例如：

2TB 由 ONTAP 引用 + 8TB （未被 ONTAP 引用） = 10TB 總容量（由雲端層使用）。

在這種情況下，增加未回收空間臨界值或增加磁碟區最小冷卻天數，以減少未參照區塊所使用的容量，可能會有好處。

> 當系統重組物件並提高其儲存效率時，它可能會將參考區塊寫入新的，更有效率的物件，藉此分割基礎檔案。如果您大幅增加未回收空間臨界值，您可以建立儲存效率更高，但連續讀取效能較低的物件。
>
> 這項額外活動會增加第三方 S3 供應商的成本，例如 AWS ， Azure 和 Google 。
>
> NetApp 建議避免將未回收空間臨界值提高到 60% 以上。

變更未回收空間臨界值

您可以自訂不同物件存放區的未回收空間臨界值百分比。

開始之前

需要進階權限等級。

步驟

1. 若要變更預設的未回收空間臨界值，請自訂並執行下列命令：

```
storage aggregate object-store modify -aggregate <name> -object-store
-name <name> -unreclaimed-space-threshold <%> (0%-99%)
```

相關資訊

- "儲存聚合物件儲存修改"

將 **ONTAP** 資料提升至效能層級

從 ONTAP 9.8 開始、如果您是進階權限層級的叢集管理員、您可以使用組合、主動將資料從雲端層級提升至效能層級 `tiering-policy` 和 `cloud-retrieval-policy` 設定：

關於這項工作

如果您想要停止在磁碟區上使用 FabricPool ，或者您有分層原則，而且想要將還原的快照資料帶回效能層，可

以執行此 `snapshot-only`動作。

將**FabricPool** 所有資料從一個數據區提升至效能層

您可以主動擷取雲端層中 FabricPool 磁碟區上的所有資料，並將其提升至效能層級。

步驟

1. 使用 `volume modify` 要設定的命令 `tiering-policy` 至 `none` 和 `cloud-retrieval-policy` 至 `promote`。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy none -cloud-retrieval-policy promote
```

將檔案系統資料提升至效能層級

您可以主動從雲端層的還原快照中擷取作用中檔案系統資料，並將其提升至效能層級。

步驟

1. 使用 `volume modify` 要設定的命令 `tiering-policy` 至 `snapshot-only` 和 `cloud-retrieval-policy` 至 `promote`。

```
volume modify -vserver <vserver-name> -volume <volume-name> -tiering
-policy snapshot-only cloud-retrieval-policy promote
```

檢查效能層促銷的狀態

您可以檢查效能層級促銷的狀態、以判斷作業何時完成。

步驟

1. 使用Volume `object-store` 命令 `tiering` 檢查效能層級促銷狀態的選項。

```
volume object-store tiering show [ -instance | -fields <fieldname>, ...
] [ -vserver <vserver name> ] *Vserver
[[-volume] <volume name>] *Volume [ -node <nodename> ] *Node Name [ -vol
-dsid <integer> ] *Volume DSID
[ -aggregate <aggregate name> ] *Aggregate Name
```

```
volume object-store tiering show v1 -instance

                                  Vserver: vs1
                                   Volume: v1
                                Node Name: node1
                              Volume DSID: 1023
                            Aggregate Name: a1
                                    State: ready
                       Previous Run Status: completed
                  Aborted Exception Status: -
                Time Scanner Last Finished: Mon Jan 13 20:27:30 2020
                  Scanner Percent Complete: -
                       Scanner Current VBN: -
                          Scanner Max VBNs: -
      Time Waiting Scan will be scheduled: -
                            Tiering Policy: snapshot-only
     Estimated Space Needed for Promotion: -
                          Time Scan Started: -
  Estimated Time Remaining for scan to complete: -
                     Cloud Retrieve Policy: promote
```

觸發排定的移轉和分層

從功能性的9.8開始ONTAP 、您可以隨時觸發分層掃描要求、而不必等待預設分層掃描。

步驟

1. 使用 `volume object-store` 命令 `trigger` 申請移轉和分層的選項。

```
volume object-store tiering trigger [ -vserver <vserver name> ] *VServer
Name [-volume] <volume name> *Volume Name
```

管理FabricPool 鏡射

瞭解 ONTAP FabricPool 鏡射

為了確保在災難發生時可以存取數據存儲中的數據，並使您能夠替換數據存儲，您可以透過添加第二個數據存儲來配置 FabricPool 鏡像，以將數據同步分層到兩個數據存儲中。您可以新增第二個資料儲存區至新的FabricPool 或現有的版塊組態、監控鏡射狀態、顯示FabricPool 鏡射詳細資料、升級鏡射、以及移除鏡射。您必須執行ONTAP 的是更新版本的版本。

建立 ONTAP FabricPool 鏡射

若要建立FabricPool 一個鏡射鏡、您可以將兩個物件存放區附加到單FabricPool 一的物件庫。您可以FabricPool 將第二個物件存放區附加到現有的單一物件存放區FabricPool 的物件保存區、或是建立新的單一物件存放FabricPool 區的更新組態、然後將第二個物件存放區附加到其中、藉此建立一個鏡射鏡射。您也可以在FabricPool 不完整的組態上建立鏡像MetroCluster 。

開始之前

- 您必須已使用建立兩個物件存放區 `storage aggregate object-store config` 命令。
- 如果您要在FabricPool 不完整的組態上建立鏡像MetroCluster ：
  - 您必須已經設定MetroCluster 並設定了這個功能
  - 您必須已在所選叢集上建立物件存放區組態。

    如果您是FabricPool 在雙叢集上建立MetroCluster 以供使用的物件鏡射、則必須在兩個叢集上建立物件儲存組態。

  - 如果您不使用內部部署物件存放區進行MetroCluster 不完整的組態設定、則應確保存在下列其中一種情況：
    - 物件存放區位於不同的可用性區域
    - 物件存放區已設定為將物件複本保留在多個可用度區域中

      "設定物件存放區以FabricPool 供在MetroCluster 一個不確定的組態中使用"

關於這項工作

您用於FabricPool 鏡射的物件存放區必須與主要物件存放區不同。

建立FabricPool 一個鏡像的程序與MetroCluster 建立一個不同時適用於整個過程的不同時適用於整個過程的非MetroCluster組態相同。

步驟

1. 如果您不使用現有的 FabricPool 組態，請使用命令將物件存放區附加至本機層，以建立新的物件存放區 `storage aggregate object-store attach`。

   此範例會將物件存放區附加至本機層，以建立新的 FabricPool 。

   ```
   cluster1::> storage aggregate object-store attach -aggregate aggr1 -name
   my-store-1
   ```

2. 使用命令將第二個物件存放區附加至本機層 `storage aggregate object-store mirror`。

   此範例將第二個物件存放區附加至本機層，以建立 FabricPool 鏡像。

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1 -name
my-store-2
```

相關資訊

- "存儲聚合物件存儲附加"
- "儲存聚合物件儲存配置"
- "儲存聚合物件儲存鏡像"

顯示 **ONTAP FabricPool** 鏡射詳細資料

您可以顯示FabricPool 有關一個物件鏡射的詳細資料、查看組態中有哪些物件存放區、以及物件存放區鏡射是否與主要物件存放區同步。

步驟

1. 使用顯示 FabricPool 鏡像的相關資訊 `storage aggregate object-store show` 命令。

   此範例顯示FabricPool 有關主物件和鏡射物件儲存在鏡射中的詳細資料。

```
cluster1::> storage aggregate object-store show
```

```
Aggregate      Object Store Name Availability    Mirror Type
-------------- ----------------- -------------   ----------
aggr1          my-store-1        available       primary
               my-store-2        available       mirror
```

   此範例顯示FabricPool 有關鏡射的詳細資料、包括鏡射是否因重新同步作業而降級。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-store-1        primary           -
               my-store-2        mirror          false
```

相關資訊

- "儲存聚合物件儲存顯示"

升級 ONTAP FabricPool 鏡像

您可以將物件存放區鏡像重新指派為主要物件存放區、方法是加以提升。當物件存放區鏡射成為主要鏡射時、原始主要鏡射會自動變成鏡射。

開始之前

- 此鏡射必須同步FabricPool
- 物件存放區必須正常運作

關於這項工作

您可以使用不同雲端供應商的物件存放區來取代原始物件存放區。例如、您的原始鏡像可能是AWS物件存放區、但您可以用Azure物件存放區來取代它。

步驟

1. 使用命令確認 FabricPool 鏡像已同步 `storage aggregate object-store show-resync-status`。如果將此鏡射同步、則不會顯示任何項目。FabricPool如果鏡像未同步，請等待重新同步完成。

```
aggregate1::> storage aggregate object-store show-resync-status
-aggregate aggr1
```

```
                                          Complete
Aggregate    Primary       Mirror         Percentage
---------    -----------   ----------     ----------
aggr1        my-store-1     my-store-2      40%
```

2. 使用來提升物件存放區鏡射 `storage aggregate object-store modify -aggregate` 命令。

```
cluster1::> storage aggregate object-store modify -aggregate aggr1 -name
my-store-2 -mirror-type primary
```

相關資訊

- "儲存聚合物件儲存修改"
- "儲存聚合物件儲存顯示重新同步狀態"

移除 ONTAP FabricPool 鏡射

如果不再需要複寫物件存放區、您可以移除FabricPool 此鏡射。

開始之前

主要物件存放區必須可運作、否則命令會失敗。

步驟

1. 使用移除 FabricPool 中的物件存放區鏡像 `storage aggregate object-store unmirror`

`-aggregate` 命令。

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

相關資訊

- "儲存聚合物件儲存取消鏡像"

以 **ONTAP FabricPool** 鏡像取代現有的物件存放區

您可以使用FabricPool 鏡射技術、將一個物件存放區換成另一個物件存放區。新的物件存放區不需要使用與原始物件存放區相同的雲端供應商。

關於這項工作

您可以使用使用不同雲端供應商的物件存放區來取代原始物件存放區。例如、您的原始物件存放區可能會使用AWS做為雲端供應商、但您可以將它取代為使用Azure做為雲端供應商的物件存放區、反之亦然。不過、新的物件存放區必須保留與原始物件相同的物件大小。

步驟

1. 使用將新的物件存放區新增至現有的 FabricPool 、以建立 FabricPool 鏡射 `storage aggregate object-store mirror` 命令。

```
cluster1::> storage aggregate object-store mirror -aggregate aggr1
-object-store-name my-AZURE-store
```

2. 使用監控鏡像重新同步狀態 `storage aggregate object-store show-resync-status` 命令。

```
cluster1::> storage aggregate object-store show-resync-status -aggregate
aggr1
```

```
                                                Complete
     Aggregate    Primary          Mirror        Percentage
     ---------    -----------      ----------    ----------
     aggr1        my-AWS-store     my-AZURE-store     40%
```

3. 使用驗證鏡像是否同步 `storage aggregate object-store> show -fields mirror-type,is-mirror-degraded` 命令。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AWS-store        primary           -
               my-AZURE-store      mirror          false
```

4. 使用將主要物件存放區與鏡射物件存放區交換 `storage aggregate object-store modify` 命令。

```
cluster1::> storage aggregate object-store modify -aggregate aggr1
-object-store-name my-AZURE-store -mirror-type primary
```

5. 使用顯示 FabricPool 鏡像的詳細資料 `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` 命令。

   此範例顯示FabricPool 有關鏡射的資訊、包括鏡射是否降級（非同步）。

```
cluster1::> storage aggregate object-store show -fields mirror-type, is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
               my-AWS-store        mirror          false
```

6. 使用移除 FabricPool 鏡像 `storage aggregate object-store unmirror` 命令。

```
cluster1::> storage aggregate object-store unmirror -aggregate aggr1
```

7. 使用驗證 FabricPool 是否回到單一物件存放區組態中 `storage aggregate object-store show -fields mirror-type,is-mirror-degraded` 命令。

```
cluster1::> storage aggregate object-store show -fields mirror-type,is-
mirror-degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          my-AZURE-store      primary           -
```

相關資訊

- "儲存聚合物件儲存鏡像"
- "儲存聚合物件儲存修改"
- "儲存聚合物件儲存顯示重新同步狀態"
- "儲存聚合物件儲存顯示"
- "儲存聚合物件儲存取消鏡像"

更換 **ONTAP MetroCluster** 組態中的 **FabricPool** 鏡像

如果FabricPool 某個物件儲存在一個鏡射中、在MetroCluster 一個物件組態中毀損或永久無法使用、您可以讓物件儲存鏡射（如果鏡射尚未儲存）、從FabricPool 鏡射中移除受損的物件儲存區。 然後將新的物件儲存鏡射新增FabricPool 到這個物件庫。

步驟

1. 如果損壞的物件存放區尚未成為鏡射、請將物件存放在鏡射中 `storage aggregate object-store modify` 命令。

```
storage aggregate object-store modify -aggregate -aggregate fp_aggr1_A01
-name mcc1_ostore1 -mirror-type mirror
```

2. 使用從 FabricPool 移除物件存放區鏡射 `storage aggregate object-store unmirror` 命令。

```
storage aggregate object-store unmirror -aggregate <aggregate name>
-name mcc1_ostore1
```

3. 使用移除鏡射資料存放區之後、您可以強制在主要資料存放區上恢復分層 `storage aggregate object-store modify` 使用 `-force-tiering-on-metrocluster true` 選項。

   沒有鏡射會干擾MetroCluster 到整個流程組態的複寫需求。

```
storage aggregate object-store modify -aggregate <aggregate name> -name
mcc1_ostore1 -force-tiering-on-metrocluster true
```

4. 使用建立替換物件存放區 `storage aggregate object-store config create` 命令。

```
storage aggregate object-store config create -object-store-name
mcc1_ostore3 -cluster clusterA -provider-type SGWS -server <SGWS-server-
1> -container-name <SGWS-bucket-1> -access-key <key> -secret-password
<password> -encrypt <true|false> -provider <provider-type> -is-ssl
-enabled <true|false> ipspace <IPSpace>
```

5. 使用將物件存放區鏡射新增至 FabricPool 鏡射 `storage aggregate object-store mirror` 命令。

```
storage aggregate object-store mirror -aggregate aggr1 -name
mcc1_ostore3-mc
```

6. 使用顯示物件儲存區資訊 `storage aggregate object-store show` 命令。

```
storage aggregate object-store show -fields mirror-type,is-mirror-
degraded
```

```
aggregate      object-store-name mirror-type     is-mirror-degraded
-------------- ----------------- ------------- ------------------
aggr1          mcc1_ostore1-mc    primary            -
               mcc1_ostore3-mc    mirror           true
```

7. 使用監控鏡像重新同步狀態 `storage aggregate object-store show-resync-status` 命令。

```
storage aggregate object-store show-resync-status -aggregate aggr1
```

```
                                                Complete
     Aggregate    Primary        Mirror          Percentage
     ---------    -----------    ----------      ----------
     aggr1        mcc1_ostore1-mc mcc1_ostore3-mc   40%
```

相關資訊

- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存鏡像"
- "儲存聚合物件儲存修改"
- "儲存聚合物件儲存顯示"
- "儲存聚合物件儲存顯示重新同步狀態"
- "儲存聚合物件儲存取消鏡像"

用於管理 **FabricPool** 資源的 **ONTAP** 指令

您可以使用 `storage aggregate object-store` 管理 FabricPool 物件存放區的命令。您可以使用 `storage aggregate` 用於管理 FabricPool 集合體的命令。您可以使用 `volume` 用於管理 FabricPool 磁碟區的命令。

如果您想要...	使用此命令：

定義物件存放區的組態、ONTAP 以便供物件庫存取	`storage aggregate object-store config create`
修改物件存放區組態屬性	`storage aggregate object-store config modify`
重新命名現有的物件存放區組態	`storage aggregate object-store config rename`
刪除物件存放區的組態	`storage aggregate object-store config delete`
顯示物件存放區組態清單	`storage aggregate object-store config show`
將第二個物件存放區附加到新FabricPool 的或現有的用作鏡像的物件存放區	`storage aggregate object-store mirror` 使用 `-aggregate` 和 `-name` 管理權限層級中的參數
從現有FabricPool 的鏡射中移除物件儲存鏡射	`storage aggregate object-store unmirror` 使用 `-aggregate` 和 `-name` 管理權限層級中的參數
監控FabricPool 鏡射重新同步狀態	`storage aggregate object-store show-resync-status`
顯示FabricPool 鏡射詳細資料	`storage aggregate object-store show`
升級物件存放區鏡射、以FabricPool 取代鏡射組態中的主要物件存放區	`storage aggregate object-store modify` 使用 `-aggregate` 管理權限層級中的參數
測試物件存放區的延遲和效能、而不將物件存放區附加至集合體	`storage aggregate object-store profiler start` 使用 `-object-store-name` 和 `-node` 進階權限層級中的參數
監控物件存放區檔案探查器狀態	`storage aggregate object-store profiler show` 使用 `-object-store-name` 和 `-node` 進階權限層級中的參數
物件存放區檔案程式執行時、請將其中止	`storage aggregate object-store profiler abort` 使用 `-object-store-name` 和 `-node` 進階權限層級中的參數
將物件存放區附加至Aggregate以使用FabricPool 物件	`storage aggregate object-store attach`
將物件存放區附加至包含FlexGroup 使用FabricPool 功能的功能區的集合體	`storage aggregate object-store attach` 使用 `allow-flexgroup true`

顯示附加至啟用FabricPool之Aggregate的物件存放區詳細資料	`storage aggregate object-store show`
顯示分層掃描所使用的Aggregate完整臨界值	`storage aggregate object-store show` 使用 `-fields tiering-fullness-threshold` 進階權限層級中的參數
顯示附加至啟用FabricPool之Aggregate的物件存放區空間使用率	`storage aggregate object-store show-space`
啟用非作用中的資料報告功能、以報告未用於FabricPool 支援的Aggregate	`storage aggregate modify` 使用 `-is-inactive-data-reporting-enabled true` 參數
顯示是否在Aggregate上啟用非作用中資料報告	`storage aggregate show` 使用 `-fields is-inactive-data-reporting-enabled` 參數
顯示有關集合體內使用者資料的冷量資訊	`storage aggregate show-space` 使用 `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` 參數
建立FabricPool 一個供使用的Volume、包括指定下列項目： • 分層原則 • 分層最低冷卻期（適用於 `snapshot-only` 或 `auto` 分層原則）	`volume create` • 您可以使用 `-tiering-policy` 指定分層原則的參數。 • 您可以使用 `-tiering-minimum-cooling-days` 進階權限層級中的參數、可指定分層的最低冷卻週期。
修改Volume以FabricPool 供使用、包括修改下列項目： • 分層原則 • 分層最低冷卻期（適用於 `snapshot-only` 或 `auto` 分層原則）	`volume modify` • 您可以使用 `-tiering-policy` 指定分層原則的參數。 • 您可以使用 `-tiering-minimum-cooling-days` 進階權限層級中的參數、可指定分層的最低冷卻週期。

顯示FabricPool 與Volume相關的資訊、包括： • 分層最低冷卻週期 • 多少使用者資料是冷的	`volume show` • 您可以使用 `-fields tiering-minimum-cooling-days` 進階權限層級中的參數、可顯示分層的最低冷卻週期。 • 您可以使用 `-fields performance-tier-inactive-user-data,performance-tier-inactive-user-data-percent` 顯示冷的使用者資料量的參數。
將Volume移入FabricPool 或移出	`volume move start` 您可以使用 `-tiering-policy` 可選參數，用於指定卷的分層策略。
修改恢復未參考空間的臨界值FabricPool （重組臨界值）以供參考	`storage aggregate object-store modify` 使用 `-unreclaimed-space-threshold` 進階權限層級中的參數
修改集合體在分層掃描開始分層資料以供FabricPool 使用之前的百分比已滿量臨界值 在本機層達到98%容量之前、將冷資料持續分層至雲端層。FabricPool	`storage aggregate object-store modify` 使用 `-tiering-fullness-threshold` 進階權限層級中的參數
顯示回收未參考空間以供FabricPool 參考的臨界值	`storage aggregate object-store show` 或 `storage aggregate object-store show-space` 命令 `-unreclaimed-space-threshold` 進階權限層級中的參數

相關資訊

- "儲存聚合修改"
- "儲存聚合對象"
- "儲存聚合展示空間"

SVM資料移動性

了解ONTAP SVM 資料遷移

從ONTAP 9.10.1 開始，叢集管理員可以無中斷地將 SVM 從來源叢集遷移到目標集群，以管理容量和負載平衡，或啟用設備升級或資料中心整合。

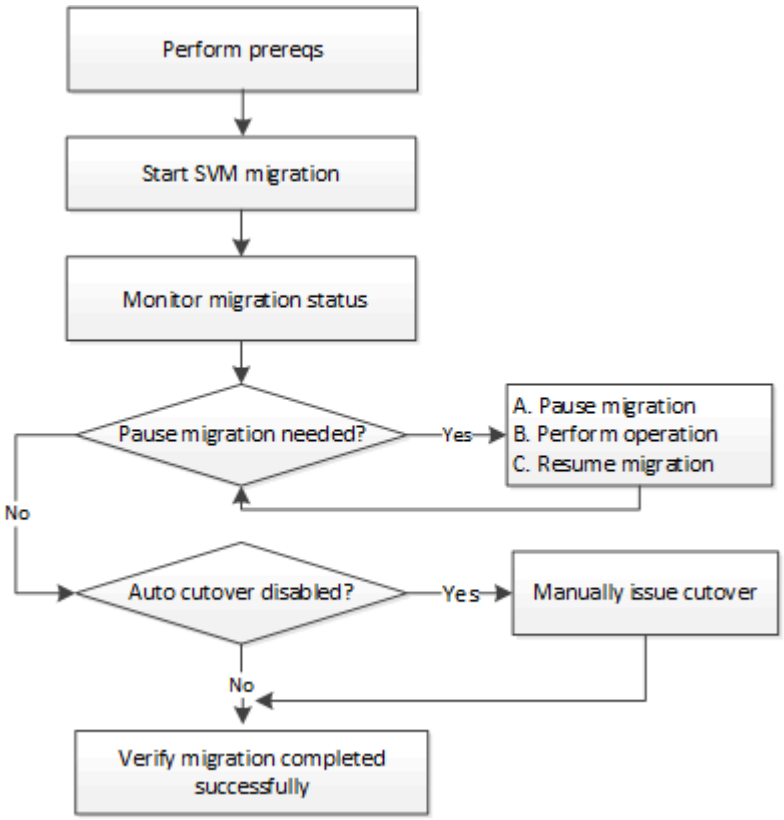
ONTAP 9.10.1 和 9.11.1 版本支援在AFF系統上進行非中斷式 SVM 遷移。從ONTAP 9.12.1 開始， FAS和AFF系統以及混合聚合體均支援此功能。

SVM的名稱和UUID在移轉之後會維持不變、以及資料LIF名稱、IP位址和物件名稱（例如Volume名稱）。SVM中物件的UUID會有所不同。

從ONTAP 9.18.1 開始，支援從ASA儲存系統到ASA r2 儲存系統的 SVM 遷移。如果您擁有ASA r2 儲存系統（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30、 ASA A20 或ASA C30），並且想要將 SVM 從ASA系統移轉到您的ASA r2 系統，請依照下列步驟操作。"這些步驟" 。

SVM移轉工作流程

此圖說明SVM移轉的典型工作流程。您可以從目的地叢集開始SVM移轉。您可以監控從來源或目的地的移轉作業。您可以執行手動轉換或自動轉換。預設會執行自動轉換。



SVM遷移系統支持

控制器系列	支援的 ONTAP 版本
ASA	ONTAP 9.18.1 及更高版本 關注"這些步驟"用於將 SVM 從ASA遷移到ASA r2 系統。
AFF C 系列	ONTAP 9.12.1 修補程式 4 及更新版本
FAS	更新版本ONTAP
AFF A 系列	更新版本ONTAP

從AFF叢集遷移到具有混合聚合的FAS叢集時，自動磁碟區放置會嘗試執行類似的聚合匹配。例如，如果來源叢集有 60 個磁碟區，則磁碟區放置操作會嘗試在目標叢集上找到一個AFF聚合來放置這些磁碟區。當AFF聚合空間不足時，磁碟區將被放置在具有非快閃磁碟的聚合上。

ONTAP 版本支援擴充性

版本ONTAP	HA 在來源和目的地中配對

ONTAP 9.14.1 及更新版本	12.
ONTAP 9.13.1.12.9.11.9.11.	6.
零點9.11.1. ONTAP	3.
零點9.10.1 ONTAP	1.

來源叢集與目的地叢集之間 **TCP** 往返時間（ **RTT** ）的網路基礎架構效能需求

視叢集上安裝的 ONTAP 版本而定、連接來源叢集和目的地叢集的網路必須具有下列所示的最長往返時間：

版本ONTAP	最大 RTT
更新版本ONTAP	10毫秒
更新版本ONTAP	2毫秒

每個 **SVM** 支援的最大磁碟區數

在混合叢集中，每個 SVM 可遷移的最大磁碟區數取決於支援磁碟區數較少的叢集成員。

來源	目的地	ONTAP 9.14.1 及更新版本	ONTAP 9.13.1.12.9.11.9.11.	ONTAP 9.12.1	更新版本ONTAP
AFF	AFF	400	200	100	100
FAS	FAS	80	80	80	不適用
FAS	AFF	80	80	80	不適用
AFF	FAS	80	80	80	不適用

先決條件

在開始 SVM 移轉之前、您必須符合下列先決條件：

- 您是叢集管理員。
- "源集群和目標集群彼此互聯"。
- 來源叢集和目標叢集具有同步的SnapMirror 。 "已安裝授權"。此許可證包含在內 "ONTAP One"。
- 來源叢集中的所有節點均運行ONTAP 9.10.1 或更高版本。有關ONTAP陣列控制器的具體支持，請參閱 "Hardware Universe"。
- 來源叢集中的所有節點都運行相同的ONTAP版本。
- 目標叢集中的所有節點都運行相同的ONTAP版本。
- 目標叢集的ONTAP版本與來源叢集的 ONTAP 版本相同，或最多比來源叢集的新兩個主要版本。
- 來源叢集和目標叢集支援相同的 IP 子網路以進行資料 LIF 存取。
- 來源叢集和目標叢集都必須至少有一個介面可以存取所有遷移的 SVM 網絡，否則遷移預檢查將會失敗。
- 源SVM包含的數量少於 版本支援的資料磁碟區數量上限。

- 目的地有足夠的空間放置書籍。
- 如果來源 SVM 具有加密磁碟區，則需要在目標叢集層級設定板載金鑰管理器或外部金鑰管理。
  - 在這種情況下，在來源端 SVM 層級配置的金鑰管理器不會遷移到目標端。目標位置使用叢集級密鑰管理器。
- 如果來源具有加密磁碟區且配置了NetApp聚合加密 (NAE)，則目標也必須配置為 NAE。
- 如果您要在非 MetroCluster 組態和 MetroCluster 組態之間移轉 SVM ，或在兩個 MetroCluster 組態之間移轉 SVM ，請確認您的組態符合下列需求：

  在MetroCluster配置中，不支援在本地叢集和夥伴叢集之間遷移 SVM。

  - 來源和目的地 MetroCluster 叢集處於「正常」狀態。這表示它們無法處於切換模式或「等待切換回復」狀態。
  - 來源和目的地 MetroCluster 叢集並未在 FC 對 IP 轉換或硬體更新的過程中。
  - 來源叢集和目標叢集必須都執行ONTAP 9.16.1 或更高版本。
  - 如果來源為 MetroCluster 叢集， SVM 子類型為「 SYNC 來源」（非「 SYNC 目的地」）。

    如果目的地是 MetroCluster 叢集，則在目的地上建立的 SVM 一律為「 SYNC 來源」。
    如果目的地是非 MetroCluster 叢集，則 SVM 子類型一律為「預設」。

最佳實務做法

執行 SVM 移轉時、最佳做法是在來源叢集和目的地叢集上保留 30% 的 CPU 保留空間、以便執行 CPU 工作負載。

SVM 作業

檢查是否有可能與 SVM 遷移衝突的操作：

- 目前並未進行容錯移轉作業
- WAFLIRON無法執行
- 指紋未在進行中
- 流量移動、重新託管、複製、建立、轉換或分析功能未運行
- 目標叢集上沒有執行SVM遷移程序。任何時候都只允許進行一次SVM遷移。

支援和不支援的功能

下表顯示 SVM 資料移動性支援的 ONTAP 功能、以及提供支援的 ONTAP 版本。

如需 SVM 移轉中來源與目的地之間 ONTAP 版本互通性的相關資訊、請參閱 "SnapMirror ONTAP 關係的相容版本"。

功能	第一版支援	註解

審計日誌（NFS 和 SMB）	ONTAP 9.13.1.12.9.11.9.11.	若為內部部署 SVM 移轉並啟用稽核、您應停用來源 SVM 的稽核、然後執行移轉。 在 SVM 移轉之前： • "必須在目標叢集上啟用稽核日誌。"。 • "必須在目的地叢集上建立來源 SVM 的稽核記錄目的地路徑"。
自主勒索軟體保護	ONTAP 9.12.1	
雲端實例	不支援	不支援將 SVM 從本機執行個體遷移到雲端或從本機執行個體遷移到雲端。
Cloud Volumes ONTAP	不支援	
外部金鑰管理程式	零點9.11.1. ONTAP	
FabricPool	不支援	
扇出關係（移轉來源具有 SnapMirror 來源 Volume 、其中有多個目的地）	零點9.11.1. ONTAP	
FC SAN	不支援	
Flash Pool	ONTAP 9.12.1	
資料量FlexCache	不支援	
資料量FlexGroup	不支援	
IPsec 原則	不支援	
IPv6生命里數	不支援	
iSCSI SAN	不支援	
工作排程複寫	零點9.11.1. ONTAP	在《銷售指南》9.10.1中ONTAP 、工作排程不會在移轉期間複寫、而且必須在目的地手動建立。從ONTAP 版本號《銷售資料9.11.1（更新版本）：移轉期間、來源使用的工作排程會自動複寫。
負載共享鏡像	不支援	

SVM MetroCluster	ONTAP 9.16.1.	從 ONTAP 9.16.1 開始，支援下列 MetroCluster SVM 移轉： • 在非 MetroCluster 組態和 MetroCluster IP 組態之間移轉 SVM • 在兩個 MetroCluster IP 組態之間移轉 SVM • 在 MetroCluster FC 組態和 MetroCluster IP 組態之間移轉 SVM 注意：來源叢集和目標叢集必須都執行ONTAP 9.16.1或更高版本才能支援 SVM 遷移。 並非所有 ONTAP 版本都支援下列 MetroCluster SVM 移轉： • 在兩個 MetroCluster FC 組態之間移轉 SVM • 在非 MetroCluster 組態和 MetroCluster FC 組態之間移轉 SVM • 在相同的MetroCluster配置中，將 SVM 從本地叢集遷移到夥伴叢集。 查看先決條件在MetroCluster配置中遷移 SVM。
NetApp Aggregate Encryption（NAE）	零點9.11.1. ONTAP	NAE 磁碟區必須放置在 NAE 支援的目標位置。如果沒有可用的 NAE 目標，則遷移操作失敗。
NDMP 組態	不支援	
NetApp Volume Encryption（NVE）	零點9.10.1 ONTAP	NVE 磁碟區將作為 NVE 磁碟區遷移到目標位置。
NFS v3 、 NFS v4.1 和 NFS v4.2	零點9.10.1 ONTAP	
NFS v4.0	ONTAP 9.12.1	
具有 pNFS 的 NFSv4.1	ONTAP 9.14.1.	
NVMe over Fabric	不支援	
在來源叢集上啟用 Common Criteria 模式的 Onboard Key Manager （ OKM ）	不支援	
ONTAP Select	不支援	不支援將 SVM 遷移到 ONTAP Select 實例或從ONTAP Select實例遷移 SVM。
qtree	ONTAP 9.14.1.	
配額	ONTAP 9.14.1.	
S3	不支援	

SMB 傳輸協定	ONTAP 9.12.1 但是不支援 SMB1 協定。	中小企業遷移會造成混亂，遷移後需要更新客戶端。
SnapMirror 雲端關係	ONTAP 9.12.1	從 ONTAP 9 。 12.1 開始，當您移轉內部部署具有 SnapMirror 雲端關係的 SVM 時，目的地叢集必須已安裝，而且必須有"SnapMirror 雲端授權"足夠的容量來支援將鏡射磁碟區中的容量移轉至雲端。
SnapMirror 非同步目的地	ONTAP 9.12.1	
SnapMirror 非同步來源	零點9.11.1. ONTAP	• 在FlexVol 大多數移轉期間、傳輸作業仍可正常繼續進行有關SnapMirror關係的作業。 • 切換期間，所有正在進行的轉帳都會被取消，新的轉帳也會失敗。在遷移完成之前，它們無法重新啟動。 • 移轉完成後、移轉期間取消或錯過的排程傳輸不會自動啟動。 當 SnapMirror 來源移轉時、ONTAP 不會在移轉後阻止刪除磁碟區、直到 SnapMirror 更新生效為止。發生這種情況的原因是、移轉後的 SnapMirror 來源磁碟區的 SnapMirror 相關資訊、只有在移轉完成後、以及第一次更新之後才能使用。
SMTape 設定	不支援	
SnapLock	不支援	
SnapMirror 主動同步	不支援	
SnapMirror SVM 對等關係	ONTAP 9.12.1	
SnapMirror SVM 災難恢復	不支援	
SnapMirror 同步	不支援	
快照	零點9.10.1 ONTAP	
防竄改快照鎖定	ONTAP 9.14.1.	防竄改的快照鎖定與 SnapLock 並不相同。SnapLock Enterprise 和 SnapLock Compliance 仍不受支援。
虛擬 IP 生命 / BGP	不支援	
Virtual Storage Console 7.0 及更新版本	不支援	
Volume複製	不支援	
垂直掃描	不支援	不支援遷移啟用 Vscan 的 SVM。

vStorage	不支援	啟用 vStorage 時不允許移轉。若要執行移轉、請停用 vStorage 選項、然後在移轉完成後重新啟用。

移轉期間支援的作業

下表指出移轉 SVM 內支援的 Volume 作業、以移轉狀態為基礎：

Volume作業	SVM 移轉狀態		
	正在進行中	* 暫停 *	轉換
建立	不允許	允許	不支援
刪除	不允許	允許	不支援
檔案系統分析停用	允許	允許	不支援
檔案系統分析功能可實現	不允許	允許	不支援
修改	允許	允許	不支援
離線 / 線上	不允許	允許	不支援
移動 / 重新裝載	不允許	允許	不支援
qtree 建立 / 修改	不允許	允許	不支援
配額建立 / 修改	不允許	允許	不支援
重新命名	不允許	允許	不支援
調整大小	允許	允許	不支援
限制	不允許	允許	不支援
快照屬性會修改	允許	允許	不支援
Snapshot 自動刪除修改	允許	允許	不支援
Snapshot 建立	允許	允許	不支援
快照刪除	允許	允許	不支援
從快照還原檔案	允許	允許	不支援

移民後訊息

- 遷移後，本機快照策略會帶有 -MIG 副檔名，這可能會破壞某些自動化功能。您應該搜尋此擴充功能並重新命名所需的策略。
- 遷移到 Vault 目標SnapMirror磁碟區必須執行重新同步才能重新啟動保護。需要重新同步儲存庫，因為遷移會在遷移 SVM 之間建立一個新的基線，該基線比儲存庫之前的基線更新。執行重新同步操作會重新啟動儲存庫，同時也會刪除比目前儲存庫基準更新的任何數據，特別是遷移期間產生的快照。

遷移**ONTAP SVM**

SVM移轉完成後、用戶端會自動切換至目的地叢集、並從來源叢集移除不必要的SVM。預設會啟用自動轉換和自動來源清除功能。如有必要、您可以停用用戶端自動切換功能、以便在轉換之前暫停移轉、也可以停用自動來源SVM清除功能。

關於這項工作

此程序適用於FAS、 AFF和ASA系統。如果您擁有ASA r2 系統（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30、 ASA A20 或ASA C30），請依照下列步驟操作。"這些步驟"遷移 SVM。ASA r2 系統為僅使用 SAN 的客戶提供簡化的ONTAP體驗。

- 您可以使用 `-auto-cutover false` 當自動用戶端轉換通常發生時暫停移轉的選項、然後稍後手動執行轉換。

  在SVM移轉之後手動切換用戶端

- 您可以使用進階權限 `-auto-source-cleanup false` 此選項可在轉換後停用來源 SVM 的移除、然後在轉換之後手動觸發來源清理。

  轉換後手動移除來源SVM

遷移啟用自動切換的**ONTAP SVM**

根據預設、當移轉完成時、用戶端會自動切換至目的地叢集、而不必要的SVM則會從來源叢集移除。

步驟

1. 從目的地叢集執行移轉預先檢查：

   ```
   vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
   -check-only true`
   ```

2. 從目的地叢集開始SVM移轉：

   ```
   vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
   ```

3. 檢查移轉狀態：

   ```
   vserver migrate show
   ```

   SVM移轉完成時、狀態會顯示「移轉完成」。

遷移已停用自動客戶端切換的**ONTAP SVM**

您可以使用-autom-cover假選項、在自動用戶端切換正常執行時暫停移轉、然後稍後手動執行切換。請參閱在SVM移轉之後手動切換用戶端。

步驟

1. 從目的地叢集執行移轉預先檢查：

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true`
```

2. 從目的地叢集開始SVM移轉：

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-cutover false`
```

3. 檢查移轉狀態：

```
vserver migrate show
```

當 SVM 遷移完成非同步資料傳輸後，狀態顯示為“準備切換”，此時即可進行切換操作。

遷移已停用來源清理的**ONTAP SVM**

您可以使用進階權限-autose-source-cleanup假選項、在轉換後停用移除來源SVM、然後在轉換之後手動觸發來源清除。請參閱 手動移除來源SVM。

步驟

1. 從目的地叢集執行移轉預先檢查：

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-check-only true`
```

2. 從目的地叢集開始SVM移轉：

```
vserver migrate start -vserver <SVM_name> -source-cluster <cluster_name>
-auto-source-cleanup false`
```

3. 檢查移轉狀態：

```
vserver migrate show
```

當SVM移轉轉換完成、且準備好移除來源叢集上的SVM時、狀態會顯示為「準備好進行來源清理」。

監控**ONTAP**卷遷移

除了使用監控 SVM 整體移轉之外 `vserver migrate show` 命令、您可以監控 SVM 所包含磁碟區的移轉狀態。

步驟

1. 在目標群集上，檢查卷宗遷移狀態：

```
vserver migrate show-volume
```

暫停和恢復ONTAP SVM 遷移

您可能想要在移轉開始之前暫停SVM移轉。您可以使用暫停 SVM 移轉 `vserver migrate pause` 命令。

暫停移轉

您可以在用戶端轉換開始之前、使用暫停 SVM 移轉 `vserver migrate pause` 命令。

移轉作業進行時、某些組態變更會受到限制；不過、從 ONTAP 9.12.1 開始、您可以暫停移轉以修正某些限制的組態、以及某些失敗狀態、以便修正可能導致故障的組態問題。您可以在暫停 SVM 移轉時修正的部分失敗狀態包括：

- `setup-configuration-failed`
- `migrate-failed`

步驟

1. 從目的地叢集暫停移轉：

```
vserver migrate pause -vserver <vserver name>
```

恢復移轉

當您準備好恢復暫停的 SVM 移轉，或 SVM 移轉失敗時，您可以使用 `vserver migrate resume`命令。

步驟

1. 從目標叢集恢復 SVM 遷移：

```
vserver migrate resume
```

2. 確認SVM移轉已恢復、並監控進度：

```
vserver migrate show
```

取消ONTAP SVM 遷移

如果您需要在 SVM 遷移完成之前取消它，您可以使用 `vserver migrate abort`命令。只有當操作處於暫停或失敗狀態時，您才可以取消 SVM 遷移。當狀態為「切換已開始」或切換完成後，您無法取消 SVM 遷移。您不能使用 `abort`SVM 遷移正在進行時的選項。

步驟

1. 在目標叢集上，檢查遷移狀態：

```
vserver migrate show -vserver <SVM_name>
```

2. 取消移轉：

```
vserver migrate abort -vserver <SVM_name>
```

3. 檢查取消作業的進度：

```
vserver migrate show
```

移轉狀態會在取消作業進行中顯示移轉中止。當取消作業完成時、移轉狀態不會顯示任何內容。

ONTAP SVM 遷移後手動切換客戶端

根據預設、在SVM移轉達到「準備轉換」狀態之後、會自動執行用戶端轉換至目的地叢集。如果您選擇停用自動用戶端轉換、則需要手動執行用戶端轉換。

步驟

1. 手動執行用戶端轉換：

```
vserver migrate cutover -vserver <SVM_name>
```

2. 檢查轉換作業的狀態：

```
vserver migrate show
```

客戶端切換後手動移除來源ONTAP SVM

如果您在停用來源清理的情況下執行SVM移轉、則可在用戶端轉換完成後手動移除來源SVM。

步驟

1. 確認狀態為已準備好進行來源清理：

```
vserver migrate show
```

2. 清除來源：

```
vserver migrate source-cleanup -vserver <SVM_name>
```

HA配對管理

了解 ONTAP 叢集中的 HA 對管理

叢集節點以高可用性 (HA) 對進行配置，以實現容錯和不間斷運行。如果某個節點發生故障，或者您需要將某個節點關閉進行例行維護，其夥伴節點可以接管其儲存空間並繼續從中提供資料。當節點恢復上線時，合作夥伴會歸還儲存空間。

HA 對控制器配置由一對相符的儲存控制器（本機節點和夥伴節點）組成。這些節點彼此之間都透過磁碟架連接。當 HA 對中的一個節點遇到錯誤並停止處理資料時，其夥伴節點會偵測到夥伴節點的故障狀態，並從該控制器接手所有資料處理。

_Takeove_是節點控制其合作夥伴儲存設備的程序。

_Giveback _是將儲存設備歸還給合作夥伴的程序。

根據預設、在下列任一情況下、移轉都會自動發生：

- 軟體或系統故障發生在導致恐慌的節點上。HA配對控制器會自動容錯移轉至其合作夥伴節點。當合作夥伴從恐慌中恢復並開機後、節點會自動執行恢復、讓合作夥伴恢復正常運作。
- 節點發生系統故障、節點無法重新開機。例如、當某個節點因停電而故障時、HA配對控制器會自動容錯移轉至其合作夥伴節點、並從存續的儲存控制器提供資料。

> 如果節點的儲存設備同時斷電、則無法進行標準接管。

- 不會從節點的合作夥伴收到活動訊息。如果合作夥伴遇到硬體或軟體故障（例如互連故障）、但並未造成恐慌、但仍無法正常運作、就可能發生這種情況。
- 您可以停止其中一個節點、而不使用 `-f` 或 `-inhibit-takeover true` 參數。

> 在啟用叢集 HA 的雙節點叢集中、使用停止或重新啟動節點 `-inhibit-takeover true` 參數會導致兩個節點停止提供資料、除非您先停用叢集 HA 、然後將 epsilon 指派給您要保持連線的節點。

- 您無需使用、即可重新啟動其中一個節點 `-inhibit-takeover true` 參數。（ `-onboot` 的參數 `storage failover` 命令預設為啟用。）

- 遠端管理裝置（服務處理器）會偵測合作夥伴節點的故障。如果您停用硬體輔助接管、則不適用此選項。

您也可以使用手動啟動接管 `storage failover takeover` 命令。

從ONTAP 9.18.1 開始，您可以設定 HA 對節點之間的加密通訊。更多信息，請參閱"配置ONTAP HA 流量的加密"。

叢集恢復能力與診斷功能的改善

從 ONTAP 9.9.1 開始，下列恢復能力和診斷新增功能可改善叢集作業：

- * 連接埠監控與避免 * ：在雙節點無交換器叢集組態中、系統會避免發生總封包遺失（連線中斷）的連接埠。在 ONTAP 9.8.1 及更早版本中、此功能僅適用於交換式組態。
- * 自動節點容錯移轉 * ：如果節點無法透過叢集網路提供資料、則該節點不應擁有任何磁碟。反之、如果合作夥伴的健康狀況良好、則HA合作夥伴應該接管。
- * 命令來分析連線問題 * ：使用下列命令來顯示哪些叢集路徑發生封包遺失： `network interface check cluster-connectivity show`

  如"指令參考資料ONTAP"需詳細 `network interface check cluster-connectivity show`資訊，請參閱。

了解 ONTAP 叢集中的硬體輔助接管

依預設、硬體輔助接管功能可使用節點的遠端管理裝置（服務處理器）來加速接管程序。

當遠端管理裝置偵測到故障時、它會快速啟動接管、而非等待ONTAP 看到合作夥伴的活動訊號已經停止。如果在未啟用此功能的情況下發生故障、合作夥伴會等待直到發現節點不再發出活動訊號、確認活動訊號遺失、然後啟動接管。

硬體輔助接管功能使用下列程序來避免此類等待：

1. 遠端管理裝置會監控本機系統是否發生特定類型的故障。
2. 如果偵測到故障、遠端管理裝置會立即傳送警示給合作夥伴節點。
3. 收到警示後、合作夥伴便會啟動接管。

觸發硬體輔助接管的系統事件

視合作夥伴節點從遠端管理裝置（服務處理器）接收到的警示類型而定、合作夥伴節點可能會產生接管。

警示	接收時開始接管？	說明
異常_重新開機	否	節點發生異常重新開機。
L2_Watchder_RESET	是的	系統監督硬體偵測到L2重設。 遠端管理裝置偵測到系統CPU沒有回應、並重新設定系統。
Loss of活動訊號	否	遠端管理裝置不再從節點接收到活動訊號訊息。 此警示並非指HA配對中節點之間的活動訊號訊息、而是指節點與其本機遠端管理裝置之間的活動訊號。
週期性訊息	否	在正常的硬體輔助接管作業期間、會傳送定期訊息。

關機後再開機	是的	遠端管理裝置已關閉並開啟系統電源。
電力損失	是的	節點發生電力中斷。 遠端管理裝置的電源供應器可在電力中斷後的一段短時間內維持電力、讓它向合作夥伴報告電力中斷。
關機透過sp	是的	遠端管理裝置已關閉系統電源。
重設_via sp	是的	遠端管理裝置會重設系統。
測試	否	系統會傳送測試訊息、以驗證硬體輔助接管作業。

相關資訊

"硬體輔助（ HWAssist ）接管 - 解析指南"

了解 ONTAP 叢集中的自動接管和交還

自動接管和恢復作業可搭配運作、以減少並避免用戶端中斷運作。

根據預設、如果HA配對中的某個節點出現問題、重新開機或暫停、則當受影響的節點重新開機時、合作夥伴節點會自動接管、然後返回儲存設備。然後HA配對會恢復正常運作狀態。

如果其中一個節點沒有回應、也可能會自動移轉。

預設會自動還原。如果您想要控制對用戶端的恢復影響，可以停用自動恢復並使用 `storage failover modify -auto-giveback false -node <node>`命令。在執行自動恢復之前（無論觸發的是什麼），合作夥伴節點會等待由命令參數 `storage failover modify`控制的固定時間量 `-delay- seconds`。預設延遲為600秒。

此程序可避免單一、長時間的停機、包括下列需求所需的時間：

- 接管作業
- 接管節點、以開機至準備好恢復的點
- 恢復作業

如果任何非根集合體的自動恢復失敗、系統會自動再嘗試兩次完成恢復。

> 在接管過程中、自動恢復程序會在合作夥伴節點準備好進行恢復之前開始。當自動恢復程序的時間限制到期、且合作夥伴節點仍未就緒時、定時器會重新啟動。因此、合作夥伴節點準備就緒與實際執行的恢復之間的時間、可能會比自動恢復時間短。

接管期間會發生什麼事

當節點接管其合作夥伴時、它會繼續提供及更新合作夥伴的集合體和磁碟區中的資料。

在接管過程中會執行下列步驟：

1. 如果交涉接管是由使用者啟動、則彙總資料會從合作夥伴節點移至執行接管的節點。當每個集合體的目前擁有者（根集合體除外）變更為接管節點時、會發生短暫的停機。這種停機時間比在接管期間發生的停機時間更為短暫、而且不會進行集合體重新配置。

在發生緊急狀況時，無法在發生緊急情況時進行交涉接管。接管可能是因為故障與恐慌無關。當節點與其合作夥伴之間的通訊中斷、也稱為心跳中斷時、就會發生故障。如果因故障而發生接管、中斷時間可能會較長、因為合作夥伴節點需要時間來偵測心跳中斷。

- 您可以使用命令來監控進度 `storage failover show-takeover`。
- 在此接管執行個體期間，您可以使用命令的參數 `storage failover takeover`來避免重新定位 Aggregate 。 `-bypass-optimization`

  在計畫性的接管作業期間、集合體會依序重新定位、以減少用戶端中斷。如果跳過集合體重新配置、則在計畫性接管事件期間、會發生較長的用戶端停機時間。

2. 如果使用者啟動的接管是交涉式接管、則目標節點會正常關機、接著接管目標節點的根 Aggregate 、以及第一步中未重新部署的任何集合體。
3. 資料生命（邏輯介面）會根據 LIF 容錯移轉規則、從目標節點移轉至接管節點、或移轉至叢集中的任何其他節點。您可以在命令中使用參數 `storage failover takeover`來避免 `LIF 移轉 `-skip-lif-migration`。如果是由使用者啟動的接管、則會在開始接管儲存設備之前移轉資料生命。發生緊急情況或故障時，視您的組態而定，資料生命負載可隨儲存設備一起移轉，或在接管完成後移轉。
4. 當發生接管時、現有的SMB工作階段會中斷連線。

   由於SMB傳輸協定的本質、所有SMB工作階段都會中斷（連線至「持續可用度」內容集之共用的SMB 3.0工作階段除外）。SMB 1.0 和 SMB 2.x 工作階段無法在接管事件後重新連線開啟的檔案處理常式、因此接管會中斷運作、而且可能會發生資料遺失。

5. SMB 3.0工作階段是為了與啟用的Continuous Availability屬性共用而建立、可在接管事件發生後重新連線至中斷連線的共用區。如果您的站台使用SMB 3.0連線至Microsoft Hyper-V、且相關共用上已啟用Continuous Availability屬性、則這些工作階段的接管作業將不會中斷營運。

執行接管的節點會發生什麼情況

如果在啟動接管後60秒內執行接管的節點出現問題、則會發生下列事件：

- 系統重新開機的節點。
- 重新開機後、節點會執行自我恢復作業、不再處於接管模式。
- 容錯移轉已停用。
- 如果節點仍擁有部分合作夥伴的集合體、則在啟用儲存容錯移轉之後、請使用將這些集合體傳回合作夥伴 `storage failover giveback` 命令。

恢復期間會發生什麼事

當問題解決、合作夥伴節點開機或啟動恢復時、本機節點會將擁有權傳回給合作夥伴節點。

下列程序會在一般的恢復作業中執行。在本討論中、節點A已接管節點B節點B上的任何問題均已解決、可繼續處理資料。

1. 節點 B 上的任何問題均已解決、並顯示下列訊息： `Waiting for giveback`
2. 贈品由啟動 `storage failover giveback` 命令或自動恢復（如果系統已設定）。這會啟動將節點B的集合體和磁碟區所有權從節點A傳回節點B的程序

3. 節點A會先傳回根Aggregate的控制權。
4. 節點B完成開機至正常作業狀態的程序。
5. 當節點B到達開機程序中可接受非根集合體的點時、節點A會一次傳回其他集合體的擁有權、直到恢復完成為止。您可以使用監控恢復的進度 `storage failover show-giveback` 命令。

> ◦ `storage failover show-giveback` 命令不會（也不會用於）顯示儲存容錯移轉恢復作業期間所有作業的相關資訊。您可以使用 `storage failover show` 命令顯示有關節點目前容錯移轉狀態的其他詳細資料、例如節點是否完全正常運作、是否可以接管、以及恢復是否完成。

每個集合體的I/O會在該集合體的還原完成後恢復、進而縮短其整體中斷時間。

HA原則及其對接管與恢復的影響

自動將CFO（控制器容錯移轉）和SFO（儲存容錯移轉）的HA原則指派給Aggregate。ONTAP此原則可決定集合體及其磁碟區的儲存容錯移轉作業執行方式。

CFO和SFO這兩種選項可決定ONTAP 儲存容錯移轉和還原作業期間的集合體控制順序。

雖然CFO和SFO這兩個術語有時會非正式地用於指儲存容錯移轉（接管和恢復）作業、但它們實際上代表指派給集合體的HA原則。例如、詞彙SFO Aggregate或CFO Aggregate只是指Aggregate的HA原則指派。

HA原則會影響接管和恢復作業、如下所示：

- 在不含根磁碟區的根Aggregate以外的ONTAP 任何其他系統上建立的Aggregate、均具有SFO的HA原則。手動啟動的接管功能已針對效能最佳化、因為在接管之前、會將SFO（非root）集合體以序列方式重新定位至合作夥伴。在恢復程序期間、集合體會在接管系統開機且管理應用程式上線後、以序列方式傳回、讓節點能夠接收其集合體。
- 由於Aggregate重新配置作業需要重新指派Aggregate磁碟擁有權、並將控制權從節點移轉至合作夥伴、因此只有符合SFO HA原則的Aggregate才有資格進行Aggregate重新配置。
- 根Aggregate一律具有CFO的HA原則、並在恢復作業開始時提供。這是允許接管系統開機的必要步驟。在接管系統完成開機程序且管理應用程式上線之後、所有其他集合體都會連續傳回、讓節點能夠接收其集合體。

> 將Aggregate的HA原則從SFO變更為CFO是一項維護模式作業。除非客戶支援代表指示、否則請勿修改此設定。

背景更新如何影響接管和恢復

磁碟韌體的背景更新會以不同的方式影響HA配對接管、恢復和集合重新配置作業、具體取決於這些作業的啟動方式。

下列清單說明背景磁碟韌體更新如何影響接管、恢復及集合重新定位：

- 如果在任一節點的磁碟上進行背景磁碟韌體更新、則手動啟動的接管作業會延遲、直到該磁碟上的磁碟韌體更新完成為止。如果背景磁碟韌體更新所需時間超過120秒、則接管作業將會中止、而且必須在磁碟韌體更新完成後手動重新啟動。如果使用命令的參數 `storage failover takeover` set 設為 `true`**來啟動接管** `-bypass-optimization`，則目的地節點上發生的背景磁碟韌體更新不會影響接管。
- 如果在來源（或接管）節點的磁碟上發生背景磁碟韌體更新，且已手動啟動接管，並將命令參數 `storage`

failover takeover`設為 `immediate，則接管`-options`作業會立即開始。

- 如果背景磁碟韌體更新發生在節點上的磁碟上、而且發生問題、則會立即開始接管發生問題的節點。
- 如果背景磁碟韌體更新發生在任一節點的磁碟上、資料集合體的恢復會延遲、直到磁碟韌體更新完成為止。
- 如果背景磁碟韌體更新所需時間超過120秒、則會中止還原作業、而且必須在磁碟韌體更新完成後手動重新啟動。
- 如果在任一節點的磁碟上進行背景磁碟韌體更新、則會延遲Aggregate重新配置作業、直到該磁碟上的磁碟韌體更新完成為止。如果背景磁碟韌體更新所需時間超過120秒、則會中止集合體重新配置作業、而且必須在磁碟韌體更新完成後手動重新啟動。如果已使用啟動 Aggregate 重新定位 `-override-destination-checks` 的 `storage aggregate relocation` 命令設為 `true`、目的地節點上發生的背景磁碟韌體更新不會影響 Aggregate 重新定位。

相關資訊

- "倉儲聚合搬遷"
- "儲存故障轉移交還"
- "儲存故障轉移修改"
- "儲存故障轉移顯示-恢復"
- "儲存故障轉移接管"

ONTAP 自動接管指令

所有支援的NetApp FAS 解決方案、AFF 功能及ASA 功能均預設啟用自動接管功能。您可能需要變更預設行為、並控制當合作夥伴節點重新開機、出現問題或停止時、自動移轉的發生時間。

如果您想要在合作夥伴節點...	使用此命令...
重新開機或停止	`storage failover modify -node nodename -onreboot true`
泛用者	`storage failover modify -node nodename -onpanic true`

如果停用接管功能、請啟用電子郵件通知

若要在接管功能停用時收到提示通知、您應該設定系統、針對「無法接管」的EMS訊息啟用自動電子郵件通知：

- `ha.takeoverImpVersion`
- `ha.takeoverImpLowMem`
- `ha.takeoverImpDegraded`
- `ha.takeoverImpUnsync`
- `ha.takeoverImpIC`
- `ha.takeoverImpHotShelf`
- `ha.takeoverImpNotDef`

相關資訊

- "儲存故障轉移修改"

ONTAP 自動交還指令

依預設、當離線節點恢復連線時、接管合作夥伴節點會自動提供儲存設備、進而還原高可用度配對關係。在大多數情況下、這是理想的行為。如果您需要停用自動恢復功能（例如、如果您想要在歸還之前調查接管原因）、您需要注意非預設設定的互動。

如果您想要...	使用此命令...
啟用自動恢復功能、以便在接管節點開機、到達「等待歸還」狀態、以及「自動歸還之前的延遲」過期之後、立即進行恢復。 預設設定為true。	`storage failover modify -node` *`nodename`* `-auto-giveback true`
停用自動還原。預設設定為true。 • 附註： * 將此參數設為 false 、並不會在發生緊急情況時自動恢復、而在發生緊急情況時自動恢復必須透過設定來停用 `-auto-giveback-after -panic` 參數為 FALSE 。	`storage failover modify -node` *`nodename`* `-auto-giveback false`
在發生緊急情況時停用接管後自動恢復（此設定預設為啟用）。	`storage failover modify -node` *`nodename`* `-auto-giveback-after-panic false`
延遲自動恢復指定秒數（預設值為600）。此選項可決定在執行自動恢復之前、節點仍處於接管狀態的最短時間。	`storage failover modify -node` *`nodename`* `-delay-seconds` *`seconds`*

儲存容錯移轉修改命令的變化如何影響自動恢復

自動恢復的操作取決於您如何設定儲存容錯移轉修改命令的參數。

下表列出的預設設定 `storage failover modify` 套用至接管事件的命令參數、不是因恐慌所造成。

參數	預設設定
`-auto-giveback` *`true`*	*`false`*
`true`	`-delay-seconds` *`integer`* (seconds)
600	`-onreboot` *`true`*
`false`	*`true`*

下表說明的組合方式 `-onreboot` 和 `-auto-giveback` 參數會影響自動恢復接管事件的恢復、而非因恐慌而造成的。

`storage failover modify` 使用的參數	接管原因	是否會自動還原？

`-onreboot true`
 	
`-auto-giveback true`
	重新開機命令	是的

停止命令、或從服務處理器發出的關機後再開機	是的	`-onreboot true`
		
		`-auto-giveback false`

重新開機命令	是的	停止命令、或從服務處理器發出的關機後再開機

否	`-onreboot false`
	
	`-auto-giveback true`
		重新開機命令

不適用 在這種情況下、不會發生接管	停止命令、或從服務處理器發出的關機後再開機	是的

`-onreboot false`
 	
`-auto-giveback false`
	重新開機命令	否

。 `-auto-giveback` 參數可控制緊急狀況後的恢復和所有其他自動接管。如果是 `-onreboot` 參數設定為 `true` 而且由於重新開機而發生接管、無論是否執行自動恢復、都會執行自動恢復 `-auto-giveback` 參數設定為 `true`。

。 `-onreboot` 此參數適用於從 ONTAP 發出的重新開機和停止命令。當 `-onreboot` 參數設為 false 、節點重新開機時不會發生接管。因此、無論是否執行、都無法自動恢復 `-auto-giveback` 參數設為 true 。發生用戶端中斷。

自動還原參數組合的效果、適用於緊急情況。

下表列出 `storage failover modify` 適用於緊急情況的命令參數：

參數	預設設定
`-onpanic _true	false_`
true	`-auto-giveback-after-panic _true
false_` （權限：進階）	*true*

`-auto-giveback _true	false_`

下表說明的參數組合方式 `storage failover modify` 命令會在緊急情況下影響自動恢復。

`storage failover` 使用的參數	發生緊急狀況後、是否會自動還原？

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic true`
	是的

`-onpanic true`
`-auto-giveback true`
`-auto-giveback-after-panic false`
	是的

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic true`
	是的

`-onpanic true`
`-auto-giveback false`
`-auto-giveback-after-panic false`
	否

`-onpanic false` 如果 `-onpanic` 設為 `false`、無論設定的值為何、都不會執行接管 / 恢復作業 `-auto-giveback` 或 `-auto-giveback-after-panic`	否

接管可能是因為故障與恐慌無關。 當節點與其合作夥伴之間的通訊中斷時、也稱為「活動訊號遺失」、就會發生_故障_。如果因故障而發生接管、則會由控制恢復 `-onfailure` 參數而非 `-auto-giveback-after-panic parameter`。

當節點出現緊急情況時、它會將緊急情況封包傳送至其合作夥伴節點。 如果合作夥伴節點因為任何原因而未收到緊急封包、則該緊急情況可能會被誤解為故障。 如果沒有收到緊急封包、合作夥伴節點就只知道通訊已中斷、而且不知道發生了恐慌。 在這種情況下、合作夥伴節點會將失去通訊視為失敗而非恐慌處理、而傳回則由控制 `-onfailure` 參數（而非 `-auto-giveback -after-panic parameter`）。

如"指令參考資料ONTAP"需詳細 `storage failover modify`資訊，請參閱。

ONTAP 手動接管指令

您可以在合作夥伴需要維護時、以及在其他類似情況下、手動執行接管作業。視合作夥伴的狀態而定、您用來執行接管的命令會有所不同。

如果您想要...	使用此命令...
接管合作夥伴節點	`storage failover takeover`
當合作夥伴的集合體移至執行接管的節點時、請監控接管的進度	`storage failover show-takeover`
顯示叢集中所有節點的儲存容錯移轉狀態	`storage failover show`

接管合作夥伴節點、而不移轉lifs	`storage failover takeover -skip-lif -migration-before-takeover true`
即使磁碟不相符、也要接管合作夥伴節點	`storage failover takeover -allow-disk -inventory-mismatch true`
即使 ONTAP 版本不符、也能接管合作夥伴節點 * 注意： * 此選項僅在不中斷營運的 ONTAP 升級程序期間使用。	`storage failover takeover -option allow -version-mismatch`
接管合作夥伴節點、而不執行Aggregate重新配置	`storage failover takeover -bypass -optimization true`
在合作夥伴有時間正常關閉其儲存資源之前、請接管合作夥伴節點	`storage failover takeover -option immediate`

> 在使用 immediate 選項發出儲存容錯移轉命令之前、您必須使用下列命令、將資料生命負載移轉至另一個節點： `network interface migrate-all -node` *node*
>
> 如"指令參考資料ONTAP"需詳細 `network interface migrate-all`資訊，請參閱。
>
> 如果您指定 `storage failover takeover -option immediate` 命令在不先移轉資料生命期的情況下、從節點移轉資料 LIF 會大幅延遲、即使是 `skip-lif-migration-before -takeover` 未指定選項。
>
> 同樣地、如果您指定「立即」選項、即使「略過最佳化」選項設定為_fals__、也會略過協調的接管最佳化。

移動**epsilon**以進行某些手動啟動的接管

如果您預期任何手動啟動的移轉作業都可能導致儲存系統發生一個非預期的節點故障、而不會造成整個叢集的仲裁損失、則應移除epsilon。

關於這項工作

若要執行計畫性維護、您必須接管HA配對中的其中一個節點。必須維持整個叢集的仲裁、以防止其餘節點發生非計畫性的用戶端資料中斷。在某些情況下、
執行接管可能會導致叢集發生非預期的節點故障、而無法避免整個叢集的仲裁遺失。

如果正在接管的節點保留了epsilon、或使用epsilon的節點不健全、就可能發生這種情況。若要維護更具恢復能力的叢集、您可以將epsilon傳輸至未接管的正常節點。
通常這是HA合作夥伴。

只有健全且符合資格的節點才會參與仲裁投票。若要維持整個叢集的仲裁人數、則需要超過N/2的票數（其中_N_代表健全、符合資格的線上節點總和）。在叢集中
使用偶數個線上節點時、 epsilon 會增加額外的投票權重、以維持分配給它的節點的仲裁。

> 雖然叢集組成投票可以使用修改 `cluster modify -eligibility false` 命令時、除了還原節點組態或延長節點維護等情況外、您應該避免這種情況。如果您將節點設為「不合格」、它會停止提供SAN資料、直到節點重設為符合資格且重新開機為止。當節點不符合資格時、對節點的NAS資料存取也可能受到影響。

步驟

1. 驗證叢集狀態、並確認epsilon是由未接管的健全節點所保留：

   a. 變更為進階權限層級、確認您想要在進階模式提示出現時繼續（*>）：

      ```
      set -privilege advanced
      ```

   b. 判斷哪個節點擁有epsilon：

      ```
      cluster show
      ```

      在下列範例中、Node1包含epsilon：

節點	健全狀況	資格	Epsilon
node1 節點2	是的 是的	是的 是的	是的 錯

      如果您要接管的節點不保留epsilon、請繼續執行步驟4。

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

2. 從您要接管的節點移除epsilon：

   ```
   cluster modify -node Node1 -epsilon false
   ```

3. 將epsilon指派給合作夥伴節點（在此範例中為Node2）：

   ```
   cluster modify -node Node2 -epsilon true
   ```

4. 執行接管作業：

   ```
   storage failover takeover -ofnode node_name
   ```

5. 返回管理權限層級：

   ```
   set -privilege admin
   ```

相關資訊

- "儲存故障轉移顯示"
- "儲存故障轉移接管"

ONTAP 手動交還命令

您可以執行一般的恢復、在合作夥伴節點上終止程序的恢復、或是強制恢復。

在執行恢復之前、您必須先移除接管系統中故障的磁碟機、如所述 "磁碟與集合體管理"。

如果恢復中斷

如果接管節點在恢復程序期間發生故障或停電、則該程序會停止、接管節點會返回接管模式、直到故障修復或電力恢復為止。

不過、這取決於故障發生的還原階段。如果節點在部分恢復狀態期間（在將根Aggregate提供給它之後）遇到故障或停電、就不會返回接管模式。相反地、節點會返回部分恢復模式。 如果發生這種情況、請重複恢復作業來完成程序。

如果已遭否決

如果已遭否決、您必須檢查EMS訊息、以判斷原因。視原因而定、您可以決定是否可以安全地置換否決。

。 `storage failover show-giveback` 命令會顯示恢復進度、並顯示哪個子系統曾否決恢復（如果有）。軟性的否決可以被取代、而硬的否決也無法取代、即使強制使用也一樣。下表摘要說明不應覆寫的軟式使用方式、以及建議的因應措施。

您可以使用下列命令、檢閱任何恢復使用的EMS詳細資料：

```
event log show -node * -event gb*
```

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

根Aggregate的GiveBack

這些否決不適用於集合體重新配置作業：

否決子系統模組	因應措施
vFiler_Low_Level	終止導致否決的SMB工作階段、或關閉建立開放工作階段的SMB應用程式。 如果使用SMB來取代此類使用權、可能會導致應用程式突然中斷連線並遺失資料。
磁碟檢查	在嘗試恢復之前、應先移除所有故障或跳過的磁碟。如果磁碟正在消毒、您應該等到作業完成。 覆寫此否決可能會因為保留衝突或無法存取的磁碟而導致集合體或磁碟區離線而導致中斷運作。

SFO Aggregate的GiveBack

這些否決不適用於集合體重新配置作業：

否決子系統模組	因應措施

鎖定管理程式	正常關閉具有開啟檔案的SMB應用程式、或將這些磁碟區移至不同的Aggregate。 如果忽略此項否決、將會導致SMB鎖定狀態遺失、進而造成中斷和資料遺失。
鎖定管理程式不需要	等待鎖定鏡射。 如果忽略此項限制、將會導致Microsoft Hyper-V虛擬機器中斷運作。
RAID	檢查EMS訊息、以判斷使用者是否因為下列原因而遭到使用： 如果因nvfile而導致使用者遭到使用、請將離線磁碟區和集合體上線。 如果正在進行磁碟新增或磁碟所有權重新指派作業、請等到作業完成後再進行。 如果因Aggregate名稱或UUID衝突而導致使用者遭到使用、請進行疑難排解並解決問題。 如果因為鏡射重新同步、鏡射驗證或離線磁碟而導致使用者使用此功能、則可覆寫使用者使用的功能、並在還原後重新啟動作業。
磁碟資源清冊	疑難排解以找出並解決問題的原因。 目的地節點可能無法看到屬於正在移轉之集合體的磁碟。 無法存取的磁碟可能導致無法存取的集合體或磁碟區。
Volume Move操作	疑難排解以找出並解決問題的原因。 這種否決可防止磁碟區移動作業在重要的轉換階段中止。如果工作在轉換期間中止、則磁碟區可能無法存取。

執行手動恢復的命令

您可以手動在 HA 配對中的節點上啟動恢復、以便在完成維護或解決之後、將儲存設備歸還給原始擁有者導致接管的任何問題。

如果您想要…	使用此命令…
將儲存設備交回合作夥伴節點	`storage failover giveback -ofnode` *`nodename`*

即使合作夥伴未處於等待恢復模式、仍可歸還儲存設備	`storage failover giveback -ofnode` *`nodename`* `-require-partner-waiting false` 除非可以接受較長的用戶端停機時間、否則請勿使用此選項。
即使程序正在否決恢復作業、也要歸還儲存設備（強制歸還）	`storage failover giveback -ofnode` *`nodename`* `-override-vetoes true` 使用此選項可能會導致用戶端停機時間延長、或是在恢復後無法上線的集合體和磁碟區。
僅回饋CFO集合體（根集合體）	`storage failover giveback -ofnode` *`nodename`* `-only-cfo-aggregates true`
發出「恢復」命令後、請監控還原進度	`storage failover show-giveback`

相關資訊

- "儲存故障轉移交還"
- "儲存故障轉移顯示-恢復"

在 ONTAP 叢集中測試接管和交還

在設定HA配對的所有層面之後、您必須確認其運作正常、以便在接管和恢復作業期間、維持對兩個節點儲存設備的不中斷存取。在整個接管過程中、本機（或接管）節點應繼續提供合作夥伴節點通常提供的資料。在還原期間、控制及交付合作夥伴的儲存設備應返回合作夥伴節點。

步驟

1. 檢查HA互連纜線的纜線、確保纜線穩固。
2. 確認您可以在兩個節點上為每個授權傳輸協定建立及擷取檔案。
3. 輸入下列命令：

   ```
   storage failover takeover -ofnode partnernode
   ```

   如"指令參考資料ONTAP"需詳細 `storage failover takeover`資訊，請參閱。

4. 輸入下列任一命令以確認是否發生接管：

   ```
   storage failover show-takeover
   ```

   ```
   storage failover show
   ```

如果您有 `storage failover` 命令 `-auto-giveback` 選項已啟用：

節點	合作夥伴	可以接管	狀態說明
節點1	節點 2	-	正在等待恢復
節點 2	節點1	錯	在接管過程中、自動恢復會在數秒內啟動

如果您有 `storage failover` 命令 `-auto-giveback` 選項已停用：

節點	合作夥伴	可以接管	狀態說明
節點1	節點 2	-	正在等待恢復
節點 2	節點1	錯	在接管過程中

5. 顯示接管節點（節點1）可偵測到的所有屬於合作夥伴節點（節點2）的磁碟：

   `storage disk show -home node2 -ownership`

   以下命令顯示屬於 Node2 的所有磁碟、 Node1 可以偵測到這些磁碟：
   `cluster::> storage disk show -home node2 -ownership`

磁碟	Aggregate	主頁	擁有者	DR主頁	主ID	擁有者ID	DR主ID	保留者	資源池
1.0.2	-	節點2	節點2	-	4078312453	4078312453	-	4078312452	Pool0
1.0.3	-	節點2	節點2	-	4078312453	4078312453	-	4078312452	Pool0

6. 確認接管節點（Node1）控制合作夥伴節點（Node2）集合體：

   `aggr show -fields home-id,home-name,is-home`

Aggregate	主識別碼	主頁名稱	原點
Aggr0_1	2014942045	節點1	是的
Aggr0_2	4078312453	節點2	錯
Aggr1_1	2014942045	節點1	是的
Aggr1_2	4078312453	節點2	錯

   在接管期間、合作夥伴節點的Aggregate的「is主目錄」值為假。

7. 顯示「waiting for恢復」訊息後、請歸還合作夥伴節點的資料服務：

   `storage failover giveback -ofnode partnernode`

8. 輸入下列任一命令、以觀察恢復作業的進度：

   ```
   storage failover show-giveback
   ```

   ```
   storage failover show
   ```

9. 視您是否看到成功完成恢復的訊息而定、繼續進行：

如果接管和恢復...	然後...
已成功完成	在合作夥伴節點上重複步驟2到步驟8。
失敗	修正接管或恢復失敗、然後重複此程序。

相關資訊

- "儲存磁碟顯示"
- "儲存故障轉移交還"
- "儲存故障轉移顯示"
- "儲存故障轉移顯示-恢復"

用於監控 **HA** 對的 **ONTAP** 指令

您可以使用ONTAP 指令來監控HA配對的狀態。如果發生接管、您也可以判斷造成接管的原因。

如果您想要檢查	使用此命令
無論容錯移轉已啟用或已發生、或目前無法進行容錯移轉的原因	`storage failover show`
檢視已啟用儲存容錯移轉 HA 模式設定的節點 您必須將值設為 HA 、節點才能參與儲存容錯移轉（ HA 配對）組態。	`storage failover show -fields mode`
是否啟用硬體輔助接管	`storage failover hwassist show`
發生硬體輔助接管事件的歷史記錄	`storage failover hwassist stats show`
當合作夥伴的集合體移至執行接管的節點時、接管作業的進度會移至該節點	`storage failover show-takeover`
將Aggregate傳回合作夥伴節點的還原作業進度	`storage failover show-giveback`
在接管或恢復作業期間、Aggregate是否位於主目錄	`aggregate show -fields home-id,owner-id,home-name,owner-name,is-home`
是否啟用叢集HA（僅適用於兩個節點叢集）	`cluster ha show`
HA配對元件的HA狀態（在使用HA狀態的系統上）	`ha-config show` 這是維護模式命令。

儲存容錯移轉**show type**命令所顯示的節點狀態

下表說明節點的狀態 `storage failover show` 命令隨即顯示。

節點狀態	說明
已連線至PARTNER_NAME、自動接管已停用。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。停用自動接管合作夥伴。
正在等待合作夥伴備用磁碟的PARTNER_NAME、Giveback等待處理。	本機節點無法透過HA互連與合作夥伴節點交換資訊。合作夥伴的GiveBack of SFO集合體已完成、但合作夥伴備用磁碟仍由本機節點擁有。 • 執行 `storage failover show-giveback` 命令以取得更多資訊。
正在等待PARTNER_NAME。正在等待合作夥伴鎖定同步。	本機節點無法透過HA互連與合作夥伴節點交換資訊、正在等待合作夥伴鎖定同步處理。
正在等待PARTNER_NAME。正在等待叢集應用程式在本機節點上上線。	本機節點無法透過HA互連與合作夥伴節點交換資訊、而且正在等待叢集應用程式上線。
已排程接管。目標節點重新部署其SFO集合體、以準備接管。	接管處理已開始。目標節點正在重新配置其SFO集合體的擁有權、以準備接管。
已排程接管。目標節點已重新部署其SFO集合體、以準備接管。	接管處理已開始。目標節點已重新配置其SFO集合體的擁有權、以準備接管。
已排程接管。正在等待停用本機節點上的背景磁碟韌體更新。節點上正在進行韌體更新。	接管處理已開始。系統正在等待本機節點上的背景磁碟韌體更新作業完成。
將SFO集合體重新部署至接管節點、以準備接管。	本機節點正在將其SFO集合體的擁有權重新配置到接管節點、以準備接管。
將SFO集合體重新部署至接管節點。正在等待接管節點以接管。	已完成將SFO集合體的擁有權從本機節點移轉至接管節點。系統正在等待接管節點接管。
將SFO Aggregate重新定位至PARTNER_NAME。正在等待停用本機節點上的背景磁碟韌體更新。節點上正在進行韌體更新。	SFO集合體所有權從本機節點移轉至接管節點的作業正在進行中。系統正在等待本機節點上的背景磁碟韌體更新作業完成。
將SFO Aggregate重新定位至PARTNER_NAME。正在等待停用PARTNER_NAME的背景磁碟韌體更新。節點上正在進行韌體更新。	SFO集合體所有權從本機節點移轉至接管節點的作業正在進行中。系統正在等待合作夥伴節點上的背景磁碟韌體更新作業完成。

已連線至PARTNER_NAME。先前的接管嘗試已中止、因為原因。本機節點擁有部分合作夥伴的SFO Aggregate。 重新核發與的合作夥伴接管 `-bypass-optimization` 參數設為 true 可接管其餘的集合體、或是核發合作夥伴的贈品以傳回重新部署的集合體。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。先前的接管嘗試已中止、原因如下所示。本機節點擁有部分合作夥伴的SFO集合體。 • 重新核發合作夥伴節點的接管、將「-Bypass」最佳化參數設為「true」以接管其餘的SFO集合體、或執行合作夥伴的還原以返回重新部署的集合體。
已連線至PARTNER_NAME。先前的接管嘗試已中止。本機節點擁有部分合作夥伴的SFO Aggregate。 重新核發與的合作夥伴接管 `-bypass-optimization` 參數設為 true 可接管其餘的集合體、或是核發合作夥伴的贈品以傳回重新部署的集合體。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。先前的接管嘗試已中止。本機節點擁有部分合作夥伴的SFO集合體。 • 重新核發合作夥伴節點的接管、將「-Bypass」最佳化參數設為「true」以接管其餘的SFO集合體、或執行合作夥伴的還原以返回重新部署的集合體。
正在等待PARTNER_NAME。先前的接管嘗試已中止、因為原因。本機節點擁有部分合作夥伴的SFO Aggregate。 將「-bypass optimization」參數設為true、以接管其餘的集合體、或發出合作夥伴的恢復、以歸還重新放置的集合體。	本機節點無法透過HA互連與合作夥伴節點交換資訊。先前的接管嘗試已中止、原因如下所示。本機節點擁有部分合作夥伴的SFO集合體。 • 重新核發合作夥伴節點的接管、將「-Bypass」最佳化參數設為「true」以接管其餘的SFO集合體、或執行合作夥伴的還原以返回重新部署的集合體。
正在等待PARTNER_NAME。先前的接管嘗試已中止。本機節點擁有部分合作夥伴的SFO Aggregate。 將「-bypass optimization」參數設為true、以接管其餘的集合體、或發出合作夥伴的恢復、以歸還重新放置的集合體。	本機節點無法透過HA互連與合作夥伴節點交換資訊。先前的接管嘗試已中止。本機節點擁有部分合作夥伴的SFO集合體。 • 重新核發合作夥伴節點的接管、將「-Bypass」最佳化參數設為「true」以接管其餘的SFO集合體、或執行合作夥伴的還原以返回重新部署的集合體。
已連線至PARTNER_NAME。先前的接管嘗試已中止、因為無法停用本機節點上的背景磁碟韌體更新（BDFU）。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。先前的接管嘗試已中止、因為本機節點上的背景磁碟韌體更新未停用。
已連線至PARTNER_NAME。先前的接管嘗試已中止、因為原因。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。先前的接管嘗試已中止、原因如下所示。
正在等待PARTNER_NAME。先前的接管嘗試已中止、因為原因。	本機節點無法透過HA互連與合作夥伴節點交換資訊。先前的接管嘗試已中止、原因如下所示。
已連線至PARTNER_NAME。由於原因、PARTNER_NAME先前的接管嘗試已中止。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。合作夥伴節點先前的接管嘗試已中止、原因如下所示。
已連線至PARTNER_NAME。PARTNER_NAME先前的接管嘗試已中止。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。合作夥伴節點先前的接管嘗試已中止。

正在等待PARTNER_NAME。由於原因、PARTNER_NAME先前的接管嘗試已中止。	本機節點無法透過HA互連與合作夥伴節點交換資訊。合作夥伴節點先前的接管嘗試已中止、原因如下所示。
先前的恢復在模組：模組名稱中失敗。自動恢復將在秒數內啟動。	先前在模組模組模組名稱中的恢復嘗試失敗。自動恢復將在秒數內啟動。 • 執行 `storage failover show-giveback` 命令以取得更多資訊。
節點在不中斷營運的控制器升級程序中、擁有合作夥伴的集合體。	由於目前正在進行不中斷營運的控制器升級程序、因此節點擁有其合作夥伴的集合體。
已連線至PARTNER_NAME。節點擁有屬於叢集中其他節點的集合體。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。節點擁有屬於叢集中其他節點的集合體。
已連線至PARTNER_NAME。正在等待合作夥伴鎖定同步。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。系統正在等待合作夥伴鎖定同步完成。
已連線至PARTNER_NAME。正在等待叢集應用程式在本機節點上上線。	HA互連處於作用中狀態、可將資料傳輸至合作夥伴節點。系統正在等待叢集應用程式在本機節點上上線。
非HA模式、請重新開機以使用完整NVRAM。	無法進行儲存容錯移轉。HA模式選項設定為非_HA。 • 您必須重新開機節點、才能使用其所有NVRAM。
非HA模式。重新開機節點以啟動HA。	無法進行儲存容錯移轉。 • 節點必須重新開機、才能啟用HA功能。
非HA模式。	無法進行儲存容錯移轉。HA模式選項設定為非_HA。 • 您必須執行 `storage failover modify -mode ha -node nodename` 在 HA 配對中的兩個節點上執行命令、然後重新啟動節點以啟用 HA 功能。

相關資訊

- "指令參考資料ONTAP"
- "叢集ha show"
- "儲存故障轉移 hwassist"
- "儲存故障轉移修改"
- "儲存故障轉移顯示"
- "儲存故障轉移顯示-恢復"

用於啟用和停用儲存故障轉移的 ONTAP 命令

使用下列命令來啟用和停用儲存容錯移轉功能。

如果您想要...	使用此命令...
啟用接管	`storage failover modify -enabled true -node` *nodename*
停用接管	`storage failover modify -enabled false -node` *nodename*

您只能在維護程序中視需要停用儲存容錯移轉。

相關資訊

- "儲存故障轉移修改"

在雙節點叢集中，無需啟動接管即可暫停或重新啟動 ONTAP 節點

當您在節點或機櫃上執行特定的硬體維護、並想要保持合作夥伴節點正常運作、以限制停機時間時、您無需啟動接管、即可停止或重新啟動雙節點叢集中的節點、 或是當發生無法手動接管的問題、而您想要讓合作夥伴節點的集合體維持正常運作並提供資料時。此外、如果技術支援正在協助您疑難排解問題、他們可能會請您執行此程序、做為這些工作的一部分。

關於這項工作

- 禁止接管之前（使用 `-inhibit-takeover true` 參數）、您可以停用叢集 HA 。

- 在雙節點叢集中、叢集HA可確保一個節點的故障不會停用叢集。不過、如果您在使用之前未停用叢集 HA `-inhibit-takeover true` 參數、兩個節點都會停止提供資料。
- 如果您在停用叢集HA之前嘗試停止或重新開機節點、ONTAP 則會發出警告並指示您停用叢集HA。

- 您可以將LIF（邏輯介面）移轉至想要保持連線的合作夥伴節點。
- 如果您要停止或重新開機的節點上有您要保留的集合體、請將其移至您要保持連線的節點。

步驟

1. 確認兩個節點都正常：
   `cluster show`

   對於兩個節點、 `true` 會出現在中 `Health` 欄位。

```
cluster::> cluster show
Node          Health  Eligibility
------------ ------- ------------
node1         true     true
node2         true     true
```

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

2. 將所有生命從您要停止或重新開機的節點移轉至合作夥伴節點：
`network interface migrate-all -node node_name`

   如"指令參考資料ONTAP"需詳細 `network interface migrate-all`資訊，請參閱。

3. 如果您要在節點上停止或重新開機、當節點當機時、有您想要保持線上狀態的集合體、請將它們重新放置到合作夥伴節點；否則、請執行下一步。

   a. 在您要停止或重新開機的節點上顯示集合體：
   `storage aggregates show -node node_name`

   例如、node1是要暫停或重新開機的節點：

```
cluster::> storage aggregates show -node node1
Aggregate  Size  Available  Used%  State  #Vols   Nodes   RAID
Status
---------  ----  ---------  -----  -----  -----   -----   ----
------
aggr0_node_1_0
           744.9GB   32.68GB   96% online       2 node1    raid_dp,

normal
aggr1       2.91TB    2.62TB   10% online       8 node1    raid_dp,

normal
aggr2
            4.36TB    3.74TB   14% online      12 node1    raid_dp,

normal
test2_aggr  2.18TB    2.18TB    0% online       7 node1    raid_dp,

normal
4 entries were displayed.
```

   b. 將集合體移至合作夥伴節點：
   `storage aggregate relocation start -node node_name -destination node_name -aggregate-list aggregate_name`

例如、Agggr1、aggr2和test2_aggr正在從節點1移至節點2：

```
storage aggregate relocation start -node node1 -destination node2 -aggregate
-list aggr1,aggr2,test2_aggr
```

4. 停用叢集 HA ：
   `cluster ha modify -configured false`

   傳回輸出會確認 HA 已停用： `Notice: HA is disabled`

   此作業不會停用儲存容錯移轉。

5. 使用適當的命令來停止或重新開機、並禁止接管目標節點：
   - `system node halt -node node_name -inhibit-takeover true`
   - `system node reboot -node node_name -inhibit-takeover true`

   在命令輸出中、您會看到一則警告、詢問您是否要繼續、請輸入 `y`。

6. 確認仍在線上的節點處於正常狀態（當合作夥伴關機時）：
   `cluster show`

   對於線上節點、 `true` 會出現在中 `Health` 欄位。

   在命令輸出中、您會看到叢集HA未設定的警告。此時您可以忽略此警告。

7. 執行必要的動作、以停止或重新啟動節點。
8. 從載入程式提示字元啟動離線節點：
   `boot_ontap`
9. 確認兩個節點都正常：
   `cluster show`

   對於兩個節點、 `true` 會出現在中 `Health` 欄位。

   在命令輸出中、您會看到叢集HA未設定的警告。此時您可以忽略此警告。

10. 重新啟用叢集 HA ：
    `cluster ha modify -configured true`
11. 如果您在本程序稍早將集合體重新定位至合作夥伴節點、請將它們移回其主節點；否則、請移至下一步：
    `storage aggregate relocation start -node node_name -destination node_name
    -aggregate-list aggregate_name`

    例如、 Aggr1 、 aggr2 和 test2_aggr 正從節點 node2 移至節點 node1 ：
    `storage aggregate relocation start -node node2 -destination node1 -aggregate
    -list aggr1,aggr2,test2_aggr`

12. 將LIF還原至其主連接埠：

a. 檢視不在家裡的生命：
`network interface show -is-home false`

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

b. 如果沒有從下一節點移轉的非主系LIF、請在還原之前確認是否可以安全地移動它們。

c. 如果安全的話、請將所有LIF回復到主目錄。 `network interface revert *` + 深入瞭解 `network interface revert` "指令參考資料ONTAP"。

相關資訊

- "叢集ha修改"
- "儲存聚合遷移開始"

配置ONTAP HA 流量的加密

從ONTAP 9.18.1 開始，您可以設定高可用性 (HA) 對節點之間網路流量的加密。此加密技術可保護高可用性 (HA) 對中節點之間傳輸的客戶資料和元資料。

關於這項工作

- 預設情況下，HA流量加密功能處於停用狀態。
- 啟用或停用 HA 流量加密會影響叢集中的所有 HA 對。您無法為單一節點啟用或停用加密。
- 啟用 HA 流量加密後，HA 會對節點之間傳輸的所有客戶資料和元資料都將進行加密。部分高可用性流量（例如檔案系統元資料和心跳訊息）未加密。
- 啟用 HA 流量加密後，如果向叢集新增了新的 HA 對，則需要透過重新執行以下命令手動為新節點啟用 HA 流量加密： `security ha-network modify -enabled true`命令。

開始之前

- 您必須是ONTAP管理員。 `admin`執行下列步驟所需的權限等級。
- 啟用高可用性流量加密之前，您必須："設定外部金鑰管理" 。
- 叢集中的所有節點必須執行ONTAP 9.18.1 或更高版本才能啟用 HA 流量加密。

步驟

1. 查看HA流量的目前加密狀態：

```
security ha-network show
```

此命令顯示每個節點的 HA 流量加密的目前狀態：

```
security ha-network show
Node                  Enabled
--------------------- --------------------
node1                 true
node2                 true
node3                 true
node4                 true
4 entries were displayed.
```

2. 啟用或停用高可用性流量加密：

```
security ha-network modify -enabled <true|false>
```

此命令啟用或停用叢集中所有節點的加密高可用性流量。當向叢集新增新的 HA 對時，您需要重新執行此命令以啟用新節點的 HA 流量加密。

使用 System Manager 進行 REST API 管理

使用 System Manager 進行 REST API 管理

REST API記錄會擷取System Manager發出的API呼叫ONTAP 以供呈現。您可以使用記錄來瞭解執行ONTAP 各種故障管理工作所需的通話性質和順序。

System Manager如何使用REST API和API記錄

有幾種方法可以讓System Manager發出REST API呼叫ONTAP 來進行介紹。

System Manager何時發出API呼叫

以下是System Manager發出ONTAP 有關呼叫靜止API的最重要範例。

自動重新整理頁面

System Manager會在背景自動發出API呼叫、以重新整理顯示的資訊、例如儀表板頁面。

使用者顯示動作

當您顯示特定的儲存資源或System Manager UI的資源集合時、會發出一或多個API呼叫。

使用者更新動作

當您從ONTAP System Manager UI新增、修改或刪除某個資源時、就會發出API呼叫。

重新發出API呼叫

您也可以按一下記錄項目、手動重新發出API呼叫。這會顯示通話的原始Json輸出。

更多資訊

- "自動化文件ONTAP"

存取REST API記錄

您可以存取記錄檔、其中包含ONTAP 系統管理員所撥打的靜態API呼叫記錄。當顯示記錄時、您也可以重新發出API呼叫並檢閱輸出。

步驟

1. 在頁面頂端、按一下 以顯示 REST API 記錄。

   最近的項目會顯示在頁面底部。

2. 在左側、按一下*儀表板*、然後觀察正在建立的API呼叫項目、以重新整理頁面。
3. 按一下「儲存設備」、然後按一下「* qtree *」。

   這會導致System Manager發出特定的API呼叫、以擷取qtree清單。

4. 找到描述API呼叫的記錄項目、其格式如下：

   ```
   GET /api/storage/qtrees
   ```

   您將會看到該項目隨附的其他 HTTP 查詢參數、例如 `max_records`。

5. 按一下記錄項目以重新發出Get API呼叫、並顯示原始Json輸出。

   範例


```
{
  "records": [
    {
      "svm": {
        "uuid": "19507946-e801-11e9-b984-00a0986ab770",
        "name": "SMQA",
        "_links": {
          "self": {
            "href": "/api/svm/svms/19507946-e801-11e9-b984-00a0986ab770"
          }
        }
      },
      "volume": {
        "uuid": "1e173258-f98b-11e9-8f05-00a0986abd71",
        "name": "vol_vol_test2_dest_dest",
        "_links": {
          "self": {
            "href": "/api/storage/volumes/1e173258-f98b-11e9-8f05-
```

```
00a0986abd71"
          }
        }
      },
      "id": 1,
      "name": "test2",
      "security_style": "mixed",
      "unix_permissions": 777,
      "export_policy": {
        "name": "default",
        "id": 12884901889,
        "_links": {
          "self": {
            "href": "/api/protocols/nfs/export-policies/12884901889"
          }
        }
      },
      "path": "/vol_vol_test2_dest_dest/test2",
      "_links": {
        "self": {
          "href": "/api/storage/qtrees/1e173258-f98b-11e9-8f05-
00a0986abd71/1"
        }
      }
    },
    ],
    "num_records": 1,
    "_links": {
      "self": {
        "href":
"/api/storage/qtrees?max_records=20&fields=*&name=!%22%22"
      }
    }
  }
```

Volume管理

使用System Manager進行Volume與LUN管理

管理磁碟區

使用系統管理器管理 **ONTAP** 卷

在System Manager中顯示磁碟區清單之後、您可以執行各種動作來管理磁碟區。

某些磁碟區類型無法使用 System Manager ，包括下列磁碟區：

- Vol0
- Del 和 TMP 類型的 Volume
- FlexGroup 組成要素
- MetroCluster 組態中的複寫磁碟區

步驟

1. 在System Manager中、按一下* Storage > Volumes *。

   隨即顯示Volume清單。

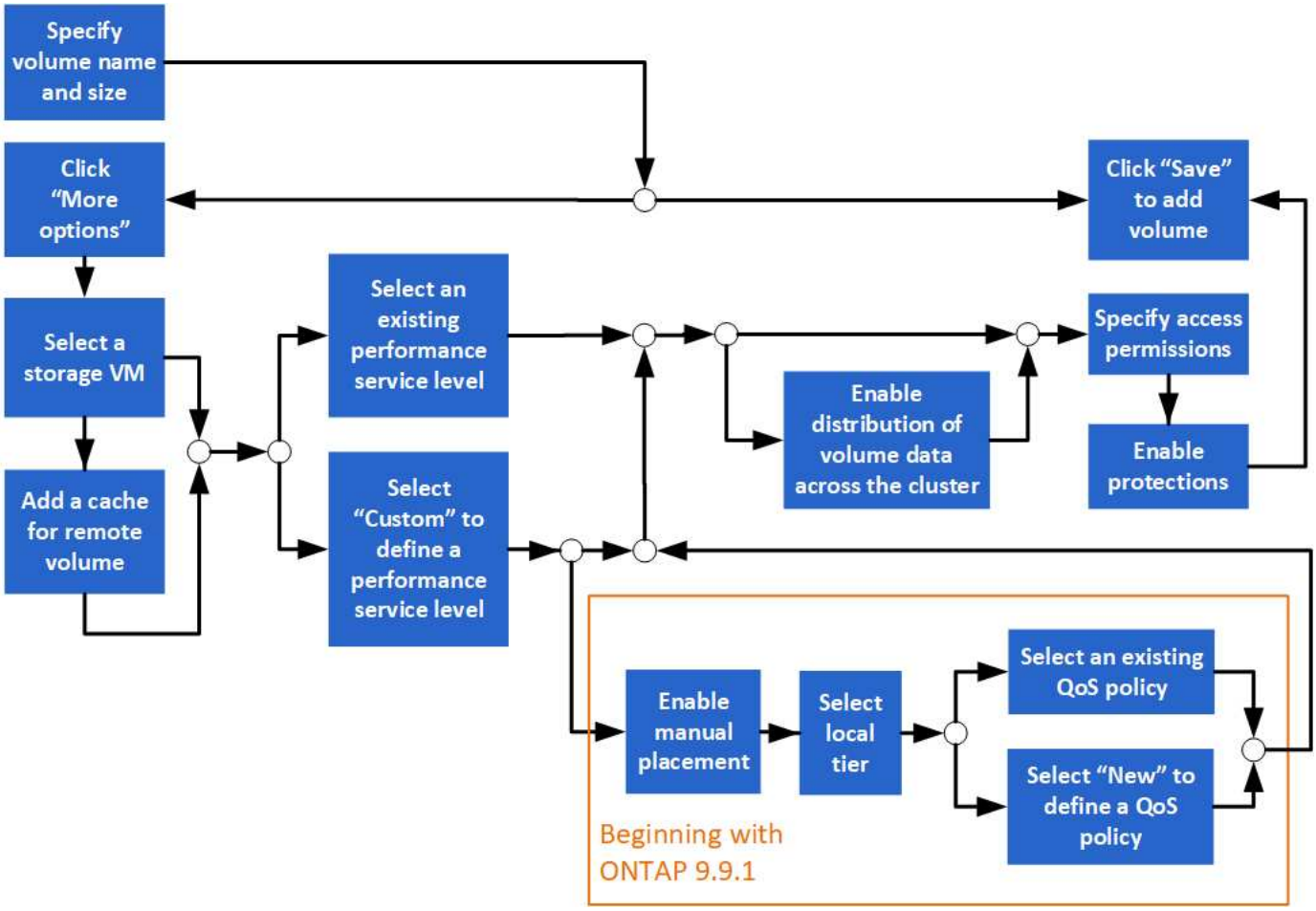
2. 您可以執行下列動作：

若要執行此工作...	請採取下列行動...
新增Volume	單擊。 + Add 請參閱。 "新增Volume"
管理多個Volume	核取磁碟區旁的方塊。 • 按一下 Delete 以刪除選取的磁碟區。 • 按一下 Protect 以將保護原則指派給選取的磁碟區。 • 按一下 More 若要為所有選取的磁碟區選取下列其中一項動作： ◦ 啟用配額 ◦ 離線 ◦ 移動 ◦ 顯示刪除的Volume

管理單一Volume	在磁碟區旁、按一下 ⋮、然後選取下列其中一個動作以執行： • 編輯 • 重新調整大小（從ONTAP 版本號1.10.1開始、僅適用於線上磁碟區和DP FlexVol 等量） • 刪除 • 複製 • 離線（或上線） • 啟用配額（或停用配額） • 編輯匯出原則 • 編輯掛載路徑 • 移動 • 編輯雲端層設定 • 保護
重新命名Volume	您可以從概觀頁面重新命名 Volume 。 按一下 磁碟區名稱旁的、然後修改磁碟區名稱。

新增**Volume**

您可以建立磁碟區、並將其新增至已設定為NFS或SMB服務的現有儲存VM。



開始之前

- 為NFS或SMB服務設定的儲存VM應存在於叢集中。
- 從 ONTAP 9.13.1 開始，您可以在新磁碟區上預設啟用容量分析和活動追蹤。在 System Manager 中、您可以管理叢集或儲存 VM 層級的預設設定。如需更多資訊、請參閱 "啟用檔案系統分析"。

步驟

1. 請前往*儲存> Volumes *。
2. 選取 + Add 。
3. 指定磁碟區的名稱和大小。
4. 請執行下列其中一個步驟：

選取此按鈕 …	若要執行此動作…
儲存	磁碟區是使用系統預設值建立和新增的。 不需要執行其他步驟。
更多選項	請前往 [step5] 定義Volume的規格。

5. [[step5、Step 5]如果您先前已指定磁碟區名稱和大小、則會顯示這些名稱和大小。 否則、請輸入名稱和大小。
6. 從下拉式清單中選取儲存VM。

   只會列出使用NFS傳輸協定設定的儲存VM。如果只有一個使用NFS傳輸協定設定的儲存VM可供使用、則不

會顯示「儲存**VM**」欄位。

7. 若要新增遠端磁碟區的快取、請選取*新增遠端磁碟區的快取*、然後指定下列值：
   - 選取叢集。
   - 選取儲存VM。
   - 選取您要做為快取磁碟區的磁碟區。
8. 在*儲存與最佳化*區段中、指定下列值：
   a. Volume的容量已顯示、但您可以加以修改。
   b. 在*效能服務層級*欄位中、選取服務層級：

當您選取此服務層級…	發生這種情況…
現有的服務層級、例如「極致」、「效能」或「價值」。 只會顯示適用於系統平台AFF （例如、NetApp FAS 或其他平台）的服務層級。	系統會自動選擇本機層級或階層。 請前往 [step9]。
自訂	請前往 [step8c] 定義新的服務層級。

   c. [[step8c、Step 8c]從ONTAP 更新至更新版9.9.1開始、您可以使用System Manager手動選取要放置所建立Volume的本機層（如果您已選取「Custom」（自訂）服務層級）。

> 如果您選取*新增為遠端Volume的快取*或*跨叢集散佈Volume資料*（請參閱下文）、則無法使用此選項。

當您做出此選擇時…	您執行這些步驟…
手動放置	手動放置已啟用。 停用「跨叢集*分散磁碟區資料」選項（請參閱下文）。請前往 [step8d] 以完成程序。
無選擇	未啟用手動放置。 系統會自動選取本機層。 請前往 [step9]。

   a. [[step8d、Step 8d]從下拉式功能表中選取本機層級。
   b. 選取QoS原則。

      選取「現有」以從現有原則清單中選擇、或選取「新增」以輸入新原則的規格。
9. [[step9、Step 9]在*最佳化選項*區段中、判斷您是否要在叢集之間分散磁碟區資料：

當您做出此選擇時…	發生這種情況…
跨叢集散佈**Volume**資料	您要新增的Volume會變成FlexGroup 一個不全的Volume。 如果您先前選擇*手動放置*、則無法使用此選項。
無選擇	根據FlexVol 預設、您要新增的Volume會變成一個不全的Volume。

10. 在「存取權限」區段中、指定已設定磁碟區之傳輸協定的存取權限。

從功能更新9.11.1開始ONTAP 、新的Volume預設將無法共用。您可以確認下列核取方塊已勾選、以指定預設存取權限：

- 透過 **NGS** 導出：建立帶有 `default`授予使用者完全存取資料的匯出策略。
- 透過**SMB/CIFS/CIFS**共享：以自動產生的名稱建立共享區、您可以加以編輯。存取權限 `Everyone` 。此外、您也可以指定權限層級。

11. 在* Protection（保護）*區段中、指定磁碟區的保護。
    - 從ONTAP 9.12.1 開始，您可以選擇*啟用快照（本機）*並選擇快照策略，而不是使用預設策略。
    - 如果您選取*啟用SnapMirror（本機或遠端）*、請從下拉式清單中指定目的地叢集的保護原則和設定。
12. 選擇*保存*。

磁碟區即會建立並新增至叢集和儲存VM。

> 您也可以將本冊的規格儲存至可執行的教戰手冊。 如需詳細資料、請前往 "使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"。

將標記指派給磁碟區

從 ONTAP 9.14.1 開始、您可以使用系統管理員將標記指派給磁碟區、以識別屬於類別的物件、例如專案或成本中心。

關於這項工作

您可以將標記指派給磁碟區。首先、您需要定義並新增標記。 然後、您也可以編輯或刪除標記。

您可以在建立 Volume 時新增標記、也可以稍後新增標記。

您可以指定金鑰並使用「關鍵字：值」格式將值關聯至標籤、藉此定義標籤。 例如： "Dept:Engineering （部門：工程） " 或 "`location ： San Jose （地點： San Jose ） " 。

建立標記時、應考慮下列事項：

- 金鑰的長度下限為 1 個字元、不可為 null 。 值可以是 null 。
- 可以使用多個值來配對金鑰、方法是以逗號分隔值、例如「 'location ： San Jose 、 Torontora' 」
- 標記可用於多個資源。
- 金鑰必須以小寫字母開頭。
- 刪除磁碟區時、將會刪除指派給磁碟區的標籤。
- 如果從恢復佇列復原磁碟區、則無法恢復標記。
- 如果移動或複製磁碟區、則會保留標籤。
- 在災難恢復關係中指派給儲存 VM 的標籤會複寫到合作夥伴站台的磁碟區上。

步驟

若要管理標記、請執行下列步驟：

1. 在 System Manager 中、按一下 * Volumes （磁碟區） * 、然後選取您要新增標記的磁碟區。

標記列在 * 標記 * 區段中。

2. 按一下 * 管理標記 * 以修改現有標記或新增標記。

   您可以新增、編輯或刪除標記。

若要執行此動作…	執行下列步驟…
新增標記	a. 按一下 * 新增標記 * 。 b. 指定金鑰及其值（以逗號分隔多個值）。 c. 按一下「 * 儲存 * 」。
編輯標記	a. 修改 **Key** 和 *Values （可選） * 字段中的內容。 b. 按一下「 * 儲存 * 」。
刪除標記	a. 按一下 您要刪除的標記旁的。

恢復刪除的磁碟區

如果您不小心刪除一FlexVol 或多個不小心刪除的功能、可以使用System Manager來恢復這些磁碟區。從功能性的問題9.8開始ONTAP 、您也可以使用System Manager來恢復FlexGroup 功能性的功能。您也可以透過清除磁碟區來永久刪除磁碟區。

磁碟區保留時間可在儲存VM層級上設定。根據預設、Volume保留時間設為12小時。

選取已刪除的磁碟區

步驟

1. 按一下「儲存設備>磁碟區」。
2. 按一下*更多>顯示刪除的磁碟區*。
3. 選取磁碟區、然後按一下所需的動作以恢復或永久刪除磁碟區。

重設**Volume**組態

刪除磁碟區會刪除該磁碟區的相關組態。恢復磁碟區並不會重設所有組態。恢復磁碟區後、請手動執行下列工作、將磁碟區恢復至原始狀態：

步驟

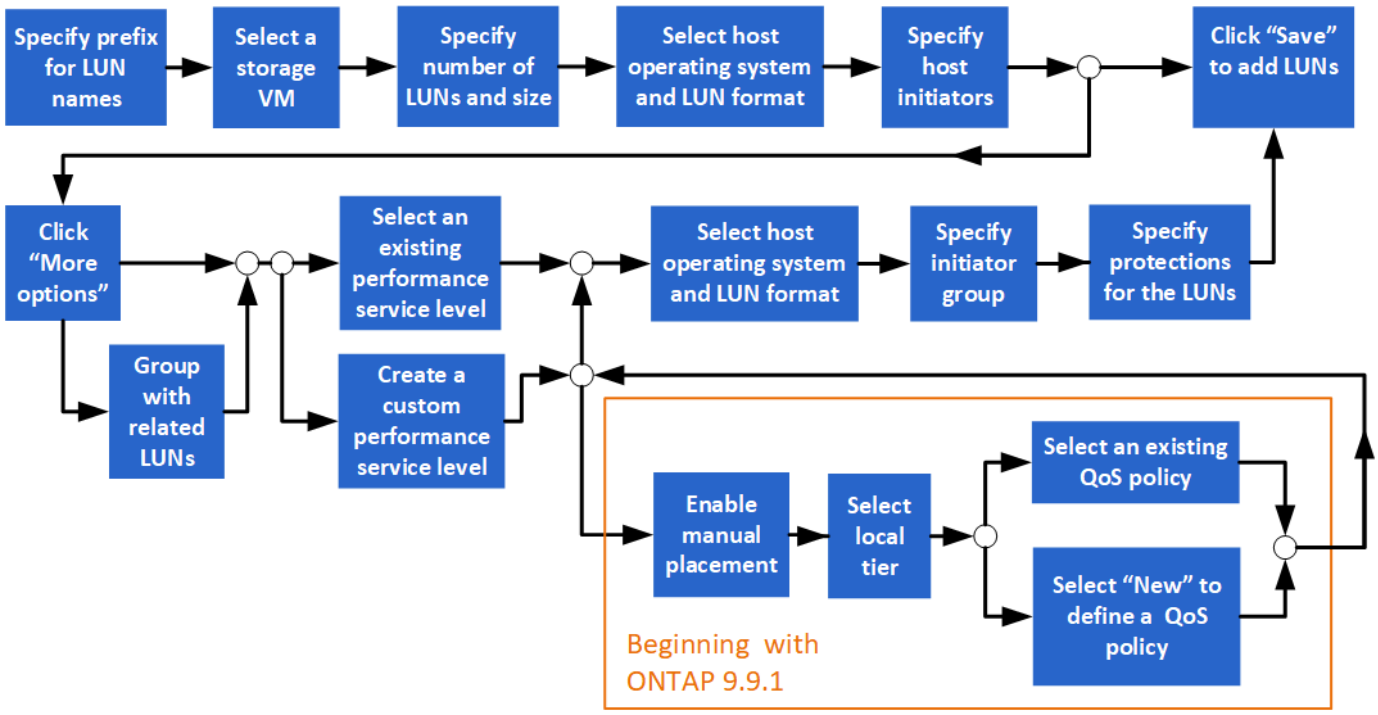
1. 重新命名Volume。
2. 設定交會路徑（NAS）。
3. 建立磁碟區（SAN）中LUN的對應。
4. 建立快照原則與匯出原則與磁碟區的關聯。
5. 新增磁碟區的配額原則規則。

6. 為磁碟區新增QoS原則。

使用 ONTAP 系統管理員管理 LUN

您可以建立LUN、並將其新增至已設定SAN傳輸協定的現有儲存VM。您也可以將 LUN 分組或重新命名。

新增LUN



開始之前

叢集中應該存在設定為SAN服務的儲存VM。

步驟

1. 轉至* Storage > LUN*。
2. 按一下 ＋ Add 。
3. 指定在每個LUN名稱開頭使用的前置詞。（如果您只要建立一個LUN、請輸入LUN名稱。）
4. 從下拉式清單中選取儲存VM。

   僅列出針對SAN傳輸協定所設定的儲存VM。 如果只有一個設定為SAN傳輸協定的儲存VM可供使用、則不會顯示「儲存**VM**」欄位。

5. 指出您要建立多少LUN、以及每個LUN的大小。
6. 從下拉式清單中選取主機作業系統和LUN格式。
7. 輸入主機啟動器、並以逗號分隔。
8. 執行下列其中一項動作：

按一下此按鈕…	若要執行此動作…
儲存	LUN是以您輸入的規格建立。 系統預設值用於其他規格。不需要執行其他步驟。
更多選項	請前往 [step9-define-add-specs] 定義LUN的其他規格。

9. [[step9-defend-add-specs、Step 9]如果您先前輸入LUN首碼、則會顯示該首碼、但您可以加以修改。否則、請輸入前置詞。
10. 從下拉式清單中選取儲存VM。

    僅列出針對SAN傳輸協定所設定的儲存VM。 如果只有一個設定為SAN傳輸協定的儲存VM可供使用、則不會顯示「儲存**VM**」欄位。

11. 確定LUN的分組方式：

當您做出此選擇時…	發生這種情況…
*使用相關LUN*進行分組	LUN將與儲存VM上現有磁碟區上的相關LUN一起分組。
無選擇	LUN將會在稱為「Container」的磁碟區上分組。

12. 在*儲存與最佳化*區段中、指定下列值：
    a. 如果您先前輸入LUN、則LUN的數量和容量已經顯示、但您可以加以修改。否則、請輸入值。
    b. 在*效能服務層級*欄位中、選取服務層級：

當您選取此服務層級…	發生這種情況…
現有的服務層級、例如「極致」、「效能」或「價值」。 只會顯示適用於系統平台AFF （例如、NetApp FAS 或其他平台）的服務層級。	系統會自動選擇本機層級。 請前往 [step13]。
自訂	請前往 [step12c] 定義新的服務層級。

    c. [[step12c、Step 12c]從ONTAP 更新到更新版9.9.1開始、您可以使用System Manager手動選取您要放置所建立LUN的本機層（如果您已選取「Custom」（自訂）服務層級）。

當您做出此選擇時…	您執行這些步驟…
手動放置	手動放置已啟用。 請前往 [step12d] 以完成程序。
無選擇	未啟用手動選擇。 系統會自動選取本機層。請前往 [step13]。

    d. [[step12d、Step 12D]從下拉式功能表中選取本機層級。
    e. 選取QoS原則。

       選取「現有」以從現有原則清單中選擇、或選取「新增」以輸入新原則的規格。

13. [[step13、Step 13]在「主機資訊」區段中、主機作業系統和LUN格式已顯示、但您可以加以修改。
14. 在*主機對應*下、選取LUN的啟動器類型：
    - * 現有啟動器群組 * ：選取顯示清單的啟動器群組。
    - * 使用現有啟動器群組新增啟動器群組 * ：指定新群組的名稱，然後選取您要用來建立新群組的群組。
    - 主機啟動器：指定新啟動器群組的名稱、然後按一下「+新增啟動器」將啟動器新增至群組。
15. 在* Protection（保護）*區段中、指定LUN的保護。

    如果您選取*啟用SnapMirror（本機或遠端）*、請從下拉式清單中指定目的地叢集的保護原則和設定。
16. 按一下「 * 儲存 * 」。

    LUN會建立並新增至叢集和儲存VM。

> 您也可以將這些LUN的規格儲存至可執行的教戰手冊。如需更多詳細資料"使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"、請前往。

重新命名 **LUN**

您可以從概觀頁面重新命名 LUN 。

步驟

1. 在 System Manager 中、按一下 * LUN* 。
2. 按一下 您要重新命名的 LUN 名稱旁的、然後修改 LUN 名稱。
3. 按一下「 * 儲存 * 」。

使用 **ONTAP** 系統管理員擴充存儲

使用System Manager、您可以增加磁碟區或LUN的大小、以便讓主機有更多可用空間。LUN的大小不得超過所含磁碟區的大小。

從 ONTAP 9.12.1 開始，當您輸入磁碟區的新容量時， **Resize Volume** （調整磁碟區大小）視窗會顯示調整磁碟區大小對資料空間和快照保留的影響。

- [增加磁碟區的大小]
- 增加LUN的大小

您也可以將 LUN 新增至現有磁碟區。使用 System Manager 和ONTAP 9.8 及更高版本時，流程會有所不同。

- 新增LUN至現有磁碟區（ONTAP 《》）
- 新增LUN至現有磁碟區（ONTAP NetApp 9.7）

增加磁碟區的大小

步驟

1. 按一下「儲存設備>磁碟區」。

2. 將游標移到您要增加大小的磁碟區名稱上。
3. 單擊。
4. 選擇*編輯*。
5. 提高容量價值。
6. 檢閱 * 現有 * 和 * 新 * 資料空間和快照保留詳細資料。

增加**LUN**的大小

步驟

1. 單擊* Storage（儲存設備）> LUN*。
2. 將游標移到您要增加大小的LUN名稱上。
3. 單擊。
4. 選擇*編輯*。
5. 提高容量價值。

新增**LUN**至現有磁碟區（**ONTAP** 《》）

從功能介紹9.8開始ONTAP 、您可以使用System Manager將LUN新增至現有的磁碟區、該磁碟區至少有一個LUN。

步驟

1. 單擊* Storage（儲存設備）> LUN*。
2. 按一下*「Add+*」。
3. 填寫* Add LUN*（添加LUN*）窗口中的字段。
4. 選擇*更多選項*。
5. 選中標有* Group with related LUN*的複選框。
6. 在下拉式欄位中、選取要新增其他LUN的磁碟區上存在的LUN。
7. 填寫其餘欄位。 對於*主機對應*、請按一下其中一個選項按鈕：
    - *現有的啟動器群組*可讓您從清單中選取現有的群組。
    - *新的啟動器群組*可讓您在欄位中輸入新的群組。

新增**LUN**至現有磁碟區（**ONTAP NetApp 9.7**）

若要將System Manager搭配ONTAP 使用以更新版本的版本9.7、將LUN新增至現有的磁碟區、您應該先切換至「經典檢視」。

步驟

1. 登入ONTAP System Manager（更新）。
2. 按一下*經典檢視*。
3. 選擇* Storage（儲存設備）> LUN > Create*（建立*）
4. 指定要建立LUN的詳細資料。

5. 指定LUN應新增至哪個現有磁碟區或qtree。

使用 ONTAP System Manager 進行壓縮、壓縮和重複資料刪除，節省儲存空間

對於非AFF叢集上的磁碟區、您可以一起執行重複資料刪除、資料壓縮及資料壓縮、或是獨立執行、以達到最佳的空間節約效益。

- 重複資料刪除技術可消除重複的資料區塊
- 資料壓縮會壓縮資料區塊、以減少所需的實體儲存容量。
- 資料壓縮可在較少空間中儲存更多資料、以提升儲存效率。

非AFF叢集上的磁碟區支援這些工作。所有內聯儲存效率功能（例如內聯重複資料刪除和內聯壓縮）在AFF磁碟區上預設為啟用。

步驟

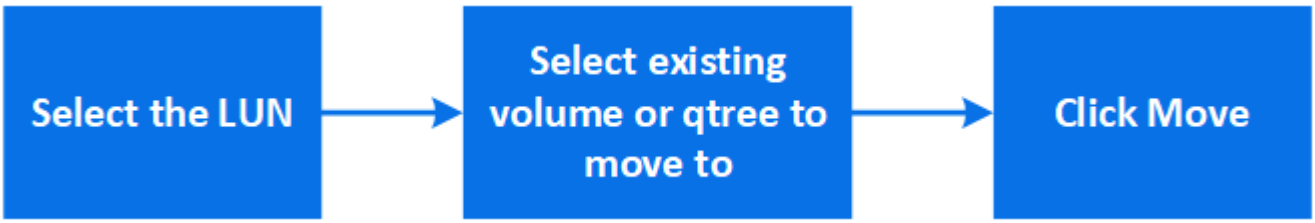
1. 按一下「儲存設備>磁碟區」。
2. 在您要儲存儲存的磁碟區名稱旁、按一下 ⋮。
3. 按一下*編輯*並捲動至*儲存效率*。
4. _Optional _：如果您要啟用背景重複資料刪除、請確認核取方塊已勾選。
5. _Optional _：如果您要啟用背景壓縮、請指定儲存效率原則、並確定核取此核取方塊。
6. _Optional _：如果您要啟用即時壓縮、請確認核取方塊已勾選。

使用 ONTAP 系統管理員移動 LUN 來平衡負載

您可以將LUN移至儲存VM內的其他磁碟區、以平衡負載、或將其移至效能較高的服務層級磁碟區、以提升效能。

移動限制

- 無法將LUN移至同一個磁碟區內的qtree。
- 使用CLI從檔案建立的LUN無法透過System Manager移動。
- 無法移動處於線上且提供資料的LUN。
- 如果目的地磁碟區中的已配置空間無法包含LUN、則無法移動LUN（即使已在磁碟區上啟用自動擴充功能）。
- 無法使用System Manager來移動位於整個資料區上的LUN SnapLock 。



步驟

1. 單擊* Storage（儲存設備）> LUN*。
2. 選取您要移動的LUN、然後按一下*移動*。
3. 選取您要將LUN移至的現有磁碟區。 如果磁碟區包含qtree、請選取qtree。

在移動作業進行期間、LUN會同時顯示在來源和目的地Volume上。

使用 **ONTAP** 系統管理員將磁碟區移至另一層，從而平衡負載

從ONTAP 9.9.1 開始，您可以根據活動和非活動資料儲存的分析來移動磁碟區。在ONTAP 9.8 中，您也可以使用系統管理員將磁碟區移至另一個層以平衡負載。

有關更多信息，請參閱"檔案系統分析總覽" 。

步驟

1. 按一下「儲存設備>磁碟區」。
2. 選取您要移動的磁碟區、然後按一下*移動*。
3. 選取您要將磁碟區或磁碟區移至的現有層（Aggregate）。

使用 **Ansible Playbooks** 透過 **ONTAP System Manager** 新增或編輯磁碟區或 **LUN**

從《支援》9.9.1開始ONTAP 、您可以在想要新增或編輯Volume或LUN時、搭配System Manager使用「可執行教戰手冊」。

此功能可讓您多次使用相同的組態、或是在新增或編輯磁碟區或LUN時、以稍微變更的方式使用相同組態。

啟用或停用可執行的教戰手冊

您可以啟用或停用使用System Manager的Ansible教戰手冊。

步驟

1. 在System Manager中、前往叢集設定頁面中的UI設定：

   叢集>設定

2. 在「* UI設定*」下、將滑桿開關變更為「已啟用」或「已停用」。

將**Volume**組態儲存至可執行的教戰手冊

建立或修改Volume組態時、您可以將組態儲存為可執行教戰手冊檔案。

步驟

1. 新增或編輯磁碟區：
   - Volume > Add* （或 * Volume > Edit* ）
2. 指定或編輯Volume的組態值。
3. 選擇*儲存至可執行教戰手冊*、將組態儲存至可執行教戰手冊檔案。

下載的壓縮檔包含下列檔案：

- **`variable.yaml`**：您輸入或修改以新增或編輯 Volume 的值。
- **`volumeAdd.yaml`** （或 **`volumeEdit.yaml`**）：從讀取輸入時、建立或修改值所需的測試案例 `variable.yaml` 檔案：

將**LUN**組態儲存至可執行教戰手冊

當您建立或修改LUN的組態時、可以將組態儲存為「可執行教戰文檔」。

步驟

1. 新增或編輯LUN：
   - LUN > Add*（或* LUN > Edit *）
2. 指定或編輯LUN的組態值。
3. 選擇*儲存至可執行教戰手冊*、將組態儲存至可執行教戰手冊檔案：

   下載的壓縮檔包含下列檔案：

   - **`variable.yaml`**：您輸入或修改以新增或編輯 LUN 的值。
   - **`lunAdd.yaml`** （或 **`lunEdit.yaml`**）：從讀取輸入時、建立或修改值所需的測試案例 `variable.yaml` 檔案：

從全球搜尋結果下載**Ansible Playbook**檔案

進行全域搜尋時、您可以下載Ansible Playbook檔案。

步驟

1. 在搜尋欄位中，輸入「volume」或「LUN」或「Playbook」。
2. 找到搜尋結果「Volume Management (Ansible Playbook)」或「LUN Management (Ansible Playbook)」。
3. 按一下 以下載 Ansible Playbook 檔案。

使用**Ansible**教戰手冊檔案

可修改及執行Ansible教戰手冊檔案、以指定磁碟區和LUN的組態。

關於這項工作

您使用兩個檔案來執行操作（「新增」或「編輯」）：

如果您想要...	使用此變數檔案...	並使用此執行檔案...
新增Volume	`volumeAdd-varible.yaml`	`valueAdd.yaml`
編輯Volume	`volumeEdit-variable.yaml`	`volumeEdit.yaml`
新增 LUN	`lunAdd-variable.yaml`	`lunAdd.yaml`
編輯LUN	`lunEdit-variable.yaml`	`lunEdit.yaml`

步驟

1. 修改變數檔案。

   該檔案包含您用來設定磁碟區或LUN的各種值。

   - 如果您未變更值、請留下註解。
   - 如果您修改這些值、請移除註解。

2. 執行相關的執行檔案。

   執行檔包含從變數檔案讀取輸入時、建立或修改值所需的測試案例。

3. 輸入您的使用者登入認證資料。

使用 **ONTAP System Manager** 管理儲存效率策略

從功能介紹9.8開始ONTAP 、您可以使用System Manager來啟用、停用、新增、編輯FAS或刪除儲存VM於支援系統上的效率原則。

此功能不適用於AFF 非對稱系統。

步驟

1. 選擇*儲存>儲存VM*
2. 選取您要管理其效率原則的儲存VM。
3. 在 * 設定 * 索引標籤上、選取 → * 效率原則 * 區段。隨即顯示該儲存VM的效率原則。

您可以執行下列工作：

- *按一下「狀態」欄中的切換按鈕、啟用或停用效率原則。
- 按一下「Add+*」來新增效率原則。
- * 編輯 * 按一下原則名稱右側的、然後選取 * 編輯 * 、即可執行效率原則 ⋮ 。
- * 按一下原則名稱右側的、然後選取 * 刪除 * 、即可刪除 * 效率原則 ⋮ 。

效率原則清單

- 自動

  指定在背景中持續執行重複資料刪除。此原則適用於所有新建立的磁碟區、以及尚未手動設定為背景重複資料刪除的所有升級磁碟區。如果您將原則變更為「預設」或任何其他原則、「自動」原則就會停用。

  如果磁碟區從非AFF系統移至AFF 某個支援系統、預設會在目的地節點上啟用「自動」原則。如果磁碟區從AFF 一個支援節點移至非AFF節點、則目的地節點上的「自動」原則預設會被「僅限內嵌」原則取代。

- 政策

  指定效率原則的名稱。

- 狀態

指定效率原則的狀態。狀態可以是下列其中一項：

- 已啟用

  指定可將效率原則指派給重複資料刪除作業。

- 已停用

  指定效率原則已停用。您可以使用狀態下拉式功能表來啟用原則、稍後再指派給重複資料刪除作業。

- 執行者

  指定是根據排程執行儲存效率原則、還是根據臨界值（變更記錄臨界值）執行。

- * QoS原則*

  指定儲存效率原則的QoS類型。QoS類型可以是下列其中一種：

  - 背景

    指定QoS原則在背景執行、如此可降低對用戶端作業的潛在效能影響。

  - 盡最大努力

    指定QoS原則是以最佳方式執行、可讓您將系統資源的使用率最大化。

- 最大執行時間

  指定效率原則的最長執行時間長度。如果未指定此值、則會執行效率原則、直到作業完成為止。

詳細資料區域

效率原則清單下方的區域會顯示所選效率原則的其他資訊、包括排程原則的排程名稱和排程詳細資料、以及臨界值型原則的臨界值。

使用 **ONTAP System Manager** 使用配額管理資源

從使用者介面9.7開始ONTAP 、您可以使用System Manager來設定及管理使用量配額。

如果您使用ONTAP 的是使用無法使用的CLI來設定及管理使用量配額、請參閱 "邏輯儲存管理"。

如果您使用舊OnCommand 版的《支援ONTAP 更新版本的支援功能》來設定及管理使用量配額、請參閱下列版本的資訊：

- "ONTAP 9.7 和 9.6 文檔"
- "S29.5文件ONTAP"
- "供應資料ONTAP"
- "部分9.3文件ONTAP"

配額總覽

配額提供一種方法來限制或追蹤使用者、群組或qtree所使用的磁碟空間和檔案數目。配額會套用至特定的Volume或qtree。

您可以使用配額來追蹤及限制磁碟區中的資源使用量、並在資源使用量達到特定層級時提供通知。

配額可以是軟的或硬的。軟配額會導致ONTAP 當超過指定的限制時、不再傳送通知、硬配額則會在超過指定的限制時、防止寫入作業成功。

使用 **ONTAP System Manager** 設定配額以限制資源使用

新增配額以限制配額目標可以使用的磁碟空間量。

您可以為配額設定硬限制和軟限制。

硬額度會對系統資源造成硬限制、導致超出限制的任何作業都會失敗。軟配額會在資源使用量達到特定層級時傳送警告訊息、但不會影響資料存取作業、因此您可以在超出配額之前採取適當的行動。

步驟

1. 按一下「儲存設備>配額」。
2. 按一下「 * 新增 * 」。

使用 **ONTAP** 系統管理器複製捲和 **LUN** 以進行測試

您可以複製磁碟區和LUN、以建立可寫入的暫存複本進行測試。 複本反映資料目前的時間點狀態。 您也可以使用複本、讓更多使用者存取資料、而不需讓他們存取正式作業資料。

開始之前

FlexClone 授權應該是 "已安裝" 儲存系統上的。

複製磁碟區

建立磁碟區的複本、如下所示：

步驟

1. 按一下「儲存設備>磁碟區」。
2. 按一下 ⋮ 您要複製的磁碟區名稱旁的。
3. 從列表中選擇* Clone（克隆）*。
4. 指定複本的名稱、然後完成其他選擇。
5. 按一下* Clone（複製）*、然後確認Volume Clone（磁碟區複製）出現在Volume（磁碟區）清單中。

或者、您也可以從*總覽*複製磁碟區、此功能會在您檢視磁碟區詳細資料時顯示。

複製**LUN**

您可以透過複製作用中磁碟區中的LUN來建立LUN複本。這些FlexClone LUN是作用中磁碟區中原始LUN的可讀寫複本。

空間保留的FlexClone LUN所需空間與空間保留的父LUN相同。如果FlexClone LUN未保留空間、您必須確保該磁碟區有足夠空間來容納FlexClone LUN的變更。

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"克隆數據。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

範例 **11.** 步驟

系統管理員

1. 單擊* Storage（儲存設備）> LUN*。
2. 按一下 ⋮ 您要複製的 LUN 名稱旁的。
3. 從列表中選擇* Clone（克隆）*。
4. 指定複本的名稱、然後完成其他選擇。
5. 按一下* Clone（複製）*、然後確認LUN複製出現在LUN清單中。

或者、您也可以從*總覽*複製LUN、以在檢視LUN詳細資料時顯示。

建立LUN複製時、System Manager會在需要空間時自動刪除複本。

CLI

1. 在進行複製之前，請確認 LUN 未對應至 igroup 或寫入至。
2. 使用 `lun show` 用於驗證 LUN 是否存在的命令。

   ```
   lun show -vserver vs1
   ```

   ```
   Vserver  Path                State     Mapped    Type      Size
   -------- ------------------- --------- --------- -------- -------
   vs1      /vol/vol1/lun1      online    unmapped  windows  47.07MB
   ```

3. 使用 `volume file clone create` 建立 FlexClone LUN 的命令。

   ```
   volume file clone create -vserver vs1 -volume vol1 -source-path lun1
   -destination-path/lun1_clone
   ```

   如果您需要 FlexClone LUN 才能自動刪除、請加入 `-autodelete true`。如果您使用半厚資源配置在磁碟區中建立此FlexClone LUN、則必須啟用所有FlexClone LUN的自動刪除功能。

4. 使用 `lun show` 用於驗證是否已建立 LUN 的命令。

   ```
   lun show -vserver vs1
   ```

   ```
   Vserver  Path                       State    Mapped   Type      Size
   -------- ------------------------- -------- -------- --------- ------
   vs1      /vol/volX/lun1            online   unmapped windows  47.07MB
   vs1      /vol/volX/lun1_clone      online   unmapped windows  47.07MB
   ```

在 **ONTAP** 系統管理員中搜尋、篩選和排序資訊

您可以在System Manager中搜尋各種動作、物件和資訊主題。 您也可以在表格資料中搜

尋特定項目。

System Manager提供兩種搜尋類型：

- [全域搜尋]

  當您在每個頁面頂端的欄位中輸入搜尋引數時、System Manager會搜尋整個介面以尋找相符項目。 然後您可以排序及篩選結果。

  從《支援》9.12.1開始ONTAP 、System Manager也會提供NetApp 支援網站 來自《支援》的搜尋結果、提供相關支援資訊的連結。

- [表格網格搜尋]

  從ONTAP 功能表9.8開始、當您在表格網格頂端的欄位中輸入搜尋引數時、System Manager只會搜尋該表格的欄和列、以尋找相符項目。

全域搜尋

在System Manager的每個頁面頂端、您可以使用全域搜尋欄位來搜尋介面中的各種物件和動作。例如、您可以依名稱搜尋不同的物件、瀏覽器欄位（左側）中可用的頁面、各種行動項目（例如「Add Volume」（新增Volume）或「Add License」（新增授權）、以及外部說明主題的連結。您也可以篩選及排序結果。

若要獲得更好的結果、請在登入一分鐘後執行搜尋、篩選及排序、並在建立、修改或刪除物件五分鐘後執行。

取得搜尋結果

搜尋不區分大小寫。 您可以輸入各種文字字串、以尋找所需的頁面、動作或資訊主題。 最多列出20個結果。 如果找到更多結果、您可以按一下*顯示更多*來檢視所有結果。 下列範例說明典型搜尋：

搜尋類型	範例搜尋字串	搜尋結果範例
依物件名稱	Vol_	儲存 VM 上的 VOL_LUN_DEST ： svm0 （ Volume ） /vol/vol… 儲存 VM 上的 est1/LUN ： svm0 （ LUN ） svm0 ： vol_lun_dest1 角色：目的地（關係）
依介面中的位置	Volume	新增 Volume （行動） 保護–總覽（頁面） 恢復刪除的磁碟區（說明）
行動	新增	新增 Volume （行動） 網路–總覽（頁面） 擴充磁碟區和 LUN （說明）
透過說明內容	SAN	儲存設備–總覽（頁面） SAN 概觀（說明） 為資料庫配置 SAN 儲存設備（說明）

來自世界各地的搜尋結果NetApp 支援網站

從 ONTAP 9 。 12.1 開始、對於已向 Active IQ 數位顧問（也稱為數位顧問）註冊的使用者、系統管理員會顯示另一欄結果、提供 NetApp 支援網站資訊的連結、包括系統管理員產品資訊。

搜尋結果包含下列資訊：

- 資訊標題、這是HTML、PDF、EPUB或其他格式文件的連結。
- 內容類型、可識別它是產品文件主題、知識庫文章或其他類型的資訊。
- 內容摘要說明。
- *建立日期*第一次發佈日期。
- *更新*上次更新的日期。

您可以執行下列動作：

行動	結果
按一下* ONTAP 《系統管理程式》*、然後在搜尋欄位中輸入文字。	搜尋結果包含NetApp 支援網站 系統管理程式的相關資訊。
按一下*所有產品*、然後在搜尋欄位中輸入文字。	搜尋結果包括NetApp 支援網站 所有NetApp產品的完整資訊、不只適用於System Manager。
按一下搜尋結果。	來自此功能的資訊NetApp 支援網站 會顯示在個別的瀏覽器視窗或索引標籤中。
按一下*查看更多結果*。	如果結果超過十項、您可以在第十項結果之後按一下*查看更多結果*、以檢視更多結果。 每次按一下*查看更多結果*、就會顯示另外十個結果（若有）。
複製連結。	連結會複製到剪貼簿。 您可以將連結貼到檔案或瀏覽器視窗中。
單擊。	顯示結果的面板會固定、因此當您在另一個面板中工作時、結果仍會保持顯示。
單擊。	結果面板不再固定且已關閉。

篩選搜尋結果

您可以使用篩選器來縮小結果範圍、如下列範例所示：

篩選器	語法	範例搜尋字串
依物件類型	類型：	Volume：vol_2
依物件大小	鍵入<<size-symbol ><數字><單位>	LUN<500mb.
以中斷的磁碟為依據	“壞盤”或“不健康磁碟”	不正常的磁碟

透過網路介面	<IP位址>	172.22.108.21

排序搜尋結果

當您檢視所有搜尋結果時、這些結果會依字母順序排序。您可以按一下並選取要排序結果的方式來 Filter 排序結果。

表格網格搜尋

從ONTAP 功能表9.8開始、每當系統管理員以表格網格格式顯示資訊時、表格頂端會出現搜尋按鈕。

當您按一下*搜尋*時、會出現一個文字欄位、您可以在其中輸入搜尋引數。 System Manager會搜尋整個表格、並只顯示含有符合搜尋引數的文字的列。

您可以使用星號（）做為「萬用字元」字元來取代字元。 例如、搜尋 **`vol`** 可能會提供包含下列項目的列：

- Vol_122_D9
- VOL_LUN_dest1
- 第2866卷
- volspec1.
- volim_dest_765
- Volume
- Volume新4
- Volume 9987

使用CLI進行邏輯儲存管理

使用CLI進行邏輯儲存管理總覽

使用支援的CLI、您可以建立及管理支援的資料、使用FlexClone技術來建立磁碟區、檔案和LUN的有效複本、建立配額樹狀結構和配額、以及管理重複資料刪除和壓縮等效率功能。ONTAP FlexVol

您應在下列情況下使用這些程序：

- 您想要瞭解ONTAP FlexVol 各種不同的功能、包括豐富的功能、以及儲存效率功能。
- 您想要使用命令列介面（CLI）、而非System Manager或自動化指令碼工具。

建立及管理磁碟區

建立Volume

您可以使用建立 Volume 並指定其連接點和其他屬性 `volume create` 命令。

關於這項工作

磁碟區必須包含_交會路徑_、才能讓用戶端使用其資料。您可以在建立新磁碟區時指定交會路徑。如果您在建立磁碟區時未指定連接路徑、則必須使用 _ 掛載 _ SVM 命名空間中的磁碟區 `volume mount` 命令。

開始之前

- 新磁碟區的SVM和將儲存設備供應給磁碟區的Aggregate必須已經存在。
- 如果SVM有相關聯的集合體清單、則該集合體必須包含在清單中。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

  若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

步驟

1. 建立Volume：

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -user
   user_name_or_number -group group_name_or_number -junction-path junction_path
   [-policy export_policy_name]
   ```

   。 `-security style`、 `-user`、 `-group`、 `-junction-path`和 `-policy` 選項僅適用於 NAS 命名空間。

   的選擇 `-junction-path` 以下是：

   - 直接位於根目錄下、例如 `/new_vol`

     您可以建立新磁碟區、並指定將其直接掛載到SVM根磁碟區。

   - 在現有目錄下、例如 `/existing_dir/new_vol`

     您可以建立新磁碟區、並指定將其掛載至現有磁碟區（在現有階層架構中）、以目錄形式表示。

   如果您想在新目錄中建立磁碟區（在新磁碟區下的新階層中）、例如：`/new_dir/new_vol`接著、您必須先建立與 SVM 根 Volume 相關的新父 Volume 。接著、您會在新父Volume（新目錄）的交會路徑中建立新的子Volume。

2. 確認已使用所需的交會點建立磁碟區：

   ```
   volume show -vserver svm_name -volume volume_name -junction
   ```

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

範例

下列命令會在 SVM 上建立名為 users1 的新磁碟區 `vs1.example.com` 和 Aggregate `aggr1`。新的 Volume 可在取得 `/users`。磁碟區大小為750 GB、磁碟區保證為磁碟區類型（預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume users1
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users1 -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1    true     /users          RW_volume
```

下列命令會在SVM上建立一個名為「'home4'」的新磁碟區：vs1.example.com`"和Aggr1'集合體。目錄 `/eng/` VS1 SVM 的命名空間已存在、新的 Volume 可從取得 `/eng/home`、成為的主目錄 `/eng/` 命名空間。磁碟區大小為 750 GB 、其磁碟區保證屬於類型 `volume` （預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                          Junction                 Junction
Vserver          Volume   Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4    true     /eng/home       RW_volume
```

在 **ONTAP** 中啟用大容量和大檔案支援

從 ONTAP 9.12.1 P2 開始，您可以建立新的磁碟區或修改現有的磁碟區，以支援最大容量 300TB ，最大大小 60PB ，最大"流通量FlexGroup"檔案（ LUN ）大小 128TB 。

開始之前

- ONTAP 9.12.1 P2 或更新版本已安裝在叢集上。
- 如果您在 SnapMirror 關係中啟用來源叢集上的大容量支援、則必須在主控來源 Volume 的叢集以及主控目的地 Volume 的叢集上安裝 ONTAP 9.12.1 P2 或更新版本。
- 您是叢集或 SVM 管理員。
- 如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立新的 **Volume**

步驟

1. 建立已啟用大容量和檔案支援的 Volume ：

```
volume create -vserver <svm_name> -volume <volume_name> -aggregate
<aggregate_name> -is-large-size-enabled true
```

範例

以下範例建立新的 Volume 、並啟用大容量和檔案大小支援。

```
volume create -vserver vs1 -volume big_vol1 -aggregate aggr1 -is-large
-size-enabled true
```

修改現有的 **Volume**

步驟

1. 修改磁碟區以啟用大容量和檔案支援：

   ```
   volume modify -vserver <svm_name> -volume <volume_name> -is-large-size
   -enabled true
   ```

   範例

   以下範例修改現有的 Volume 、以支援大容量和檔案大小。

   ```
   volume modify -vserver vs2 -volume data_vol -is-large-size-enabled true
   ```

2. 重新安裝 Volume 以啟動新的組態設定：

   ```
   volume unmount -vserver <svm_name> -volume <volume_name>
   ```

   ```
   volume mount -vserver <svm_name> -volume <volume_name>
   ```

相關資訊

- "建立 ONTAP NFS 卷"
- "指令參考資料ONTAP"

SAN 磁碟區

SAN Volume 資源配置總覽

ONTAP 提供數種基本選項來進行 SAN Volume 資源配置。每個選項都使用不同的方法來管理 ONTAP 區塊共用技術的磁碟區空間和空間需求。您應該瞭解每個資源配置選項的運

作方式、以便為您的環境選擇最佳選項。

不建議將 SAN LUN 和 NAS 共用放在同一個 FlexVol volume 上。您應該為 SAN LUN 和 NAS 共用區個別配置 FlexVol 磁碟區。如此可簡化管理與複寫部署。它也與 Active IQ Unified Manager （前身為 OnCommand Unified Manager ）支援 FlexVol 磁碟區的方式相似。

資源隨需配置

建立精簡配置的磁碟區時ONTAP 、建立磁碟區時、不需要保留任何額外空間。當資料寫入磁碟區時、磁碟區會從Aggregate要求所需的儲存設備、以配合寫入作業。使用精簡配置的磁碟區可讓您過度使用Aggregate、這可能會導致磁碟區無法在Aggregate用盡可用空間時、保護所需的空間。

您可以透過設定精簡配置的 FlexVol Volume 來建立它 `-space-guarantee` 選項 `none`。

為磁碟區進行完整資源配置

建立完整資源配置的Volume時ONTAP 、功能組會從集合區中保留足夠的儲存空間、以確保磁碟區中的任何區塊都能隨時寫入。當您將磁碟區設定為使用完整資源配置時、您可以運用ONTAP 任何一套功能（例如壓縮和重複資料刪除）來抵銷較大的前置儲存需求。

您可以透過設定完整佈建的 FlexVol Volume 來建立它 `-space-slo` （服務層級目標）選項 `thick`。

磁碟區的半厚資源配置

建立使用半厚資源配置的磁碟區時ONTAP 、由集合區中的儲存空間來考慮磁碟區大小。如果磁碟區因為區塊共用技術使用區塊而耗盡可用空間， ONTAP 會盡力刪除保護資料物件（快照， FlexClone 檔案和 LUN ），以釋放它們所擁有的空間。只要ONTAP 用足夠快的速度刪除保護資料物件、以跟上覆寫所需的空間、寫入作業就會繼續成功。這稱為「盡力」寫入保證。

您無法在使用半厚資源配置的磁碟區上採用重複資料刪除、壓縮及壓縮等儲存效率技術。

您可以透過設定半完整佈建的 FlexVol Volume 來建立它 `-space-slo` （服務層級目標）選項 `semi-thick`。

與空間保留檔案和**LUN**搭配使用

空間保留檔案或LUN是在建立儲存設備時配置的檔案或LUN。過去、NetApp使用「精簡配置LUN」一詞來表示停用空間保留的LUN（非空間保留LUN）。

非空間保留的檔案一般不會稱為「精簡配置的檔案」。

下表摘要說明三種Volume資源配置選項如何搭配空間保留檔案和LUN使用的主要差異：

Volume資源配置	**LUN /**檔案空間保留	覆寫	保護資料	儲存效率[3]
厚	支援	保證為1^	保證	支援
精簡	無效果	無	保證	支援
半厚	支援	盡力量：1^	盡最大努力	不支援

附註

1. 若要保證覆寫或提供盡力覆寫保證、必須在LUN或檔案上啟用空間保留。
2. 保護資料包括快照，標記為自動刪除的 FlexClone 檔案和 LUN （備份複本）。
3. 儲存效率包括重複資料刪除、壓縮、任何未標示為自動刪除（作用中複本）的FlexClone檔案和LUN、以及FlexClone子檔案（用於複本卸載）。

支援**SCSI**精簡配置**LUN**

支援T10 SCSI精簡配置LUN、以及NetApp精簡配置LUN。ONTAPT10 SCSI精簡配置可讓主機應用程式支援SCSI功能、包括用於區塊環境的LUN空間回收和LUN空間監控功能。您的SCSI主機軟體必須支援T10 SCSI精簡配置。

您使用的是 ONTAP `space-allocation` 設定以啟用 / 停用 LUN 上 T10 精簡配置的支援。您使用的是 ONTAP `space-allocation enable` 在 LUN 上啟用 T10 SCSI 精簡配置的設定。

這 `[-space-allocation {enabled|disabled}]`命令"指令參考資料ONTAP"有更多資訊來啟用/停用對 T10 精簡配置的支援以及如何在 LUN 上啟用 T10 SCSI 精簡配置。

設定**Volume**資源配置選項

您可以根據空間需求、設定磁碟區以進行精簡配置、完整資源配置或半複雜資源配置。

關於這項工作

設定 `-space-slo` 選項 `thick` 確保下列事項：

- 整個磁碟區會預先配置在Aggregate中。您無法使用 `volume create` 或 `volume modify` 用於設定 Volume 的命令 `-space-guarantee` 選項。
- 保留覆寫所需的空間100%。您無法使用 `volume modify` 用於設定 Volume 的命令 `-fractional -reserve` 選項

設定 `-space-slo` 選項 `semi-thick` 確保下列事項：

- 整個磁碟區會預先配置在Aggregate中。您無法使用 `volume create` 或 `volume modify` 用於設定 Volume 的命令 `-space-guarantee` 選項。
- 不會保留空間進行覆寫。您可以使用 `volume modify` 用於設定 Volume 的命令 `-fractional-reserve` 選項。
- 自動刪除快照已啟用。

步驟

1. 設定Volume資源配置選項：

   `volume create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-space-slo none|thick|semi-thick -space-guarantee none|volume`

   。 `-space-guarantee` 選項預設為 `none` 適用於 AFF 系統和非 AFF DP 磁碟區。否則、預設為 `volume`。對於現有的 FlexVol 磁碟區、請使用 `volume modify` 用於設定資源配置選項的命令。

   下列命令可在SVM VS1上設定vol1以進行精簡配置：

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-guarantee
none
```

下列命令可在SVM VS1上設定vol1以進行完整資源配置：

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo thick
```

下列命令可在SVM VS1上設定vol1以進行半厚資源配置：

```
cluster1::> volume create -vserver vs1 -volume vol1 -space-slo semi-
thick
```

相關資訊

- "Volume建立"
- "Volume修改"

判斷 **ONTAP** 中磁碟區或集合體的空間使用量

在某些情況下、在 ONTAP 中啟用功能可能會佔用比您預期的更多空間。提供三種檢視空間的觀點、協助您判斷空間的使用方式：磁碟區、磁碟區在集合體內的佔用空間、以及集合體。ONTAP

檢視空間分配

由於磁碟區空間使用量或磁碟區、Aggregate或兩者的組合空間不足、因此磁碟區可能會耗盡空間。透過從不同角度查看以功能為導向的空間使用量明細、您可以評估您可能想要調整或關閉哪些功能、或是應該採取其他行動（例如增加 Aggregate 或 Volume 的大小）。

您可以從下列任一角度檢視空間使用詳細資料：

- 磁碟區的空間使用量

  此觀點提供磁碟區內空間使用量的詳細資料，包括快照使用量。

  使用 `volume show-space` 命令以查看磁碟區的空間使用量。

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

  從 ONTAP 9.14.1 開始、在使用的磁碟區上 對溫度敏感的儲存效率（ TSSE ） 已啟用、所報告之磁碟區上使用的空間量 `volume show-space -physical used` 命令包含 TSSE 所節省的空間。

- 集合體內的磁碟區佔用空間

  此觀點提供每個磁碟區在包含Aggregate中使用的空間量詳細資料、包括磁碟區的中繼資料。

使用 `volume show-footprint` 命令以查看具有 Aggregate 的 Volume 佔用空間。

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

- Aggregate的空間使用量

  此觀點包括集合體中所有磁碟區的磁碟區佔用空間總計，保留給集合快照的空間，以及其他集合中繼資料。

  支援整合層級中繼資料和效能的資料空間佔總磁碟空間的10% WAFL 。 用於維護集合體中磁碟區的空間來自WAFL 於此保護區、因此無法變更。

  從 ONTAP 9.12.1 開始、 AFF 平台和 FAS500f 平台的 WAFL 保留容量大於 30TB 、從 10% 降至 5% 。從 ONTAP 9.14.1 開始，所有 FAS 平台上的集合體都會有相同的減少，因此可在集合體中增加 5% 的可用空間。

  使用 `storage aggregate show-space` 命令查看 Aggregate 的空間使用量。

  如"指令參考資料ONTAP"需詳細 `storage aggregate show-space`資訊，請參閱。

某些功能（例如磁帶備份和重複資料刪除）會使用磁碟區的中繼資料空間、以及直接從集合體取得的中繼資料空間。這些功能顯示了不同的磁碟區與磁碟區佔用空間使用情況。

Volume 中繼資料和資料度量報告

過去、有幾個磁碟區空間度量報告了使用的總資料量、這些資料是由兩個度量（中繼資料和使用者資料）所組成。從 ONTAP 9.15.1 開始、中繼資料和使用者資料度量會分別報告。我們推出兩個新的中繼資料計數器來支援此功能：

- 總中繼資料

  此計數器提供磁碟區內的中繼資料總大小。它不包含 Aggregate 駐留 Volume 中繼資料。另外報告有助於判斷使用者分配的邏輯資料。

- 總中繼資料佔用空間

  此計數器是 Volume 駐留中繼資料和 Aggregate 駐留 Volume 中繼資料的總和。它可提供集合體內磁碟區的中繼資料總佔用空間。另外報告有助於判斷使用者分配的實體資料。

此外、已更新數個現有計數器、以移除中繼資料元件、並僅顯示使用者資料：

- 使用者資料
- Volume 資料佔用空間

這些變更可更準確地檢視使用者所使用的資料。這有幾項優點、包括能夠更精確地做出計費決策。

相關資訊

- "NetApp知識庫：空間使用狀況"
- "升級ONTAP 至更新版的更新版、即可釋放5%的儲存容量"

您可以定義並啟用原則，以自動刪除快照和 FlexClone LUN 。自動刪除快照和 FlexClone LUN 可協助您管理空間使用率。

關於這項工作

您可以從讀寫父磁碟區自動刪除讀寫磁碟區和 FlexClone LUN 中的快照。您無法設定從唯讀磁碟區自動刪除快照，例如 SnapMirror 目的地磁碟區。

步驟

1. 使用命令定義並啟用自動刪除快照的原則 `volume snapshot autodelete modify`。

   如需瞭解 `volume snapshot autodelete modify`及定義符合您需求"指令參考資料ONTAP"的原則，請參閱。

   下列命令可自動刪除快照，並將 vol3 磁碟區的觸發設為 `snap_reserve`，這是 vs0.example.com 儲存虛擬機器（ SVM ）的一部分：

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger snap_reserve
   ```

   下列命令可自動刪除標示為自動刪除 vol3 磁碟區的快照和 FlexClone LUN ，而 vol3 磁碟區是 vs0.example.com 儲存虛擬機器（ SVM ）的一部分：

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0.example.com
   -volume vol3 -enabled true -trigger volume -commitment try -delete-order
   oldest_first -destroy-list lun_clone,file_clone
   ```

   Aggregate 層級快照的運作方式與 Volume 層級快照不同，並由 ONTAP 自動管理。刪除 Aggregate 快照的選項一律會啟用，有助於管理空間使用率。

   如果將 Aggregate 的觸發參數設為 `snap_reserve`，則會保留快照，直到保留空間超過臨界值容量為止。因此，即使觸發器參數未設定為，命令中快照所使用的空間也 `snap_reserve` 會列為， `0`因為這些快照會自動刪除。此外，快照在集合體中使用的空間也會視為可用空間，並包含在命令的可用空間參數中。

設定磁碟區、以便在磁碟區已滿時自動提供更多空間

當整個過程完成時、利用各種方法來嘗試自動為Volume提供更多可用空間。FlexVol ONTAP您可以根據ONTAP 應用程式和儲存架構的要求、選擇哪些方法可以使用、以及順序。

關於這項工作

使用下列一種或兩種方法、即可自動為整個Volume提供更多可用空間：ONTAP

- 增加磁碟區的大小（稱為_autodg_）。

如果包含Aggregate的磁碟區有足夠的空間來支援較大的磁碟區、則此方法非常實用。您可以設定ONTAP使用者介面來設定Volume的最大大小。根據寫入磁碟區的資料量、相對於目前已用空間量和任何臨界值集、會自動觸發增加。

不會觸發自動擴充以支援建立快照。如果您嘗試建立快照，但空間不足，即使啟用自動擴充功能，快照建立也會失敗。

- 刪除快照， FlexClone 檔案或 FlexClone LUN 。

  例如，您可以將 ONTAP 設定為自動刪除未連結至複製磁碟區或 LUN 中快照的快照，或者您也可以先定義要 ONTAP 刪除哪些快照，亦即最舊或最新的快照。您也可以決定 ONTAP 何時開始刪除快照，例如當磁碟區即將滿或磁碟區的快照保留空間即將滿時。

如果啟用這兩種方法、您可以指定ONTAP 當磁碟區幾乎已滿時、首先使用哪種方法來嘗試。如果第一種方法無法為Volume提供足夠的額外空間、ONTAP 接下來將嘗試其他方法。

根據預設ONTAP 、功能區會先嘗試增加磁碟區的大小。在大多數情況下，最好使用預設組態，因為刪除快照時，就無法還原快照。不過，如果您需要避免盡可能增加磁碟區的大小，您可以設定 ONTAP 在增加磁碟區大小之前刪除快照。

步驟

1. 如果您希望 ONTAP 在磁碟區滿時嘗試增加磁碟區的大小，請使用命令搭配 `grow`模式來啟用磁碟區的自動擴充功能 `volume autosize`。如"指令參考資料ONTAP"需詳細 `volume autosize`資訊，請參閱。

   請記住、當磁碟區成長時、會從其關聯的Aggregate消耗更多可用空間。如果您是根據磁碟區在需要時擴充的能力而定、則必須監控相關聯集合體中的可用空間、並視需要新增更多空間。

2. 如果您希望 ONTAP 在磁碟區滿時刪除快照， FlexClone 檔案或 FlexClone LUN ，請針對這些物件類型啟用自動刪除。

3. 如果您同時啟用 Volume 自動擴充功能和一或多個自動刪除功能，請選擇第一種 ONTAP 應使用的方法，以選項搭配使用命令 `-space-mgmt-try-first`來提供磁碟區的可用空間 `volume modify`。如"指令參考資料ONTAP"需詳細 `volume modify`資訊，請參閱。

   要先指定增加卷的大小（默認值），請使用 `volume_grow`。若要指定先刪除快照，請使用 `snap_delete`。

設定磁碟區以自動擴充及縮小其大小

您可以根據FlexVol 目前所需的空間、設定自動擴充和縮減的功能。如果Aggregate能夠提供更多空間、自動擴充有助於防止磁碟區空間不足。自動壓縮可防止磁碟區大於所需的容量、釋放集合體中的空間供其他磁碟區使用。

關於這項工作

自動壓縮只能搭配自動擴充一起使用、以滿足不斷變化的空間需求、而且無法單獨使用。啟用自動壓縮功能時ONTAP 、支援使用者可自動管理磁碟區的縮減行為、以避免自動擴充和自動縮小動作的循環。

隨著磁碟區的成長、可以包含的檔案數量上限可能會自動增加。當磁碟區縮小時、其可包含的檔案數量上限將維持不變、而且磁碟區無法自動縮減至與其目前最大檔案數相對應的大小。因此、可能無法自動將磁碟區縮小至原始大小。

根據預設、磁碟區可成長為啟用自動擴充的大小的120%。如果您需要確保磁碟區的大小可以大於該磁碟區、則必須據此設定磁碟區的最大大小。

開始之前

此版本必須在線上。FlexVol

步驟

1. 設定磁碟區以自動擴充及縮小其大小：

   ```
   volume autosize -vserver SVM_name -volume volume_name -mode grow_shrink
   ```

   下列命令可針對名為test2的磁碟區自動變更大小。磁碟區已設定為在滿60%時開始縮減。預設值用於開始增加的時間及其最大大小。

   ```
   cluster1::> volume autosize -vserver vs2 test2 -shrink-threshold-percent
   60
   vol autosize: Flexible volume "vs2:test2" autosize settings UPDATED.

   Volume modify successful on volume: test2
   ```

啟用自動壓縮和自動快照刪除的需求

只要符合特定組態需求，自動壓縮功能就能與自動快照刪除搭配使用。

如果您想同時啟用自動壓縮功能和自動快照刪除功能，您的組態必須符合下列需求：

- ONTAP 必須設定為嘗試增加磁碟區大小，才能嘗試刪除快照（ `-space-mgmt-try-first`選項必須設定為 `volume_grow`）。
- 自動刪除快照的觸發程序必須是 Volume fullness （ `trigger`參數必須設為 `volume`）。

自動壓縮功能和快照刪除

由於自動壓縮功能會縮小 FlexVol volume 的大小，因此自動刪除磁碟區快照也會受到影響。

自動壓縮功能會以下列方式與自動磁碟區快照刪除互動：

- 如果同時 `grow_shrink`啟用自動調整模式和自動快照刪除功能，當磁碟區大小縮小時，可能會觸發自動刪除快照。

  這是因為快照保留是以磁碟區大小的百分比（預設為 5% ）為基礎，而該百分比現在是以較小的磁碟區大小為基礎。這可能會導致快照從保留區溢出，並自動刪除。

- 如果 `grow_shrink`啟用自動調整大小模式，而您手動刪除快照，則可能會觸發自動縮小 Volume 。

解決**FlexVol** 全量及過度配置警示

當不存在空間時、系統會發出EMS訊息、以便您為整個Volume提供更多空間來採取修正行

動。ONTAP FlexVol瞭解警示類型及其處理方式、有助於確保資料可用度。

當磁碟區被描述為_Full_時、表示作用中檔案系統（使用者資料）可用磁碟區空間的百分比已降至（可設定）臨界值以下。當某個Volume變成_overallocated時、ONTAP 將會耗盡由支援中繼資料和基本資料存取的空間。有時候、通常保留給其他用途的空間可用於維持磁碟區正常運作、但空間保留或資料可用度可能會受到威脅。

過度配置可以是邏輯或實體配置。_Logical overall撥款_表示保留用於履行未來空間承諾的空間、例如空間保留、已用於其他用途。_Physical overall撥款_表示磁碟區已用完要使用的實體區塊。處於此狀態的磁碟區可能會拒絕寫入、離線或導致控制器中斷。

由於中繼資料已使用或保留空間、因此磁碟區可能已滿100%。不過、容量超過100%的磁碟區可能會過度配置、也可能不會過度配置。如果qtree層級和Volume層級的共享存在於相同FlexVol 的SCVMM或SCVMM資源池中、qtree就會顯示為FlexVol 該共享區上的目錄。因此、您必須小心不要意外刪除。

下表說明磁碟區完整度和過度配置警示、您可採取哪些行動來解決此問題、以及不採取行動的風險：

警示類型	**EMS**層級	可設定的？	定義	解決方法	若未採取任何行動、則有風險
幾乎已滿	偵錯	是	檔案系統已超過此警示設定的臨界值（預設值為95% ）。百分比是 `Used`總和減去快照保留區的大小。	• 增加Volume大小 • 減少使用者資料	還沒有寫入作業或資料可用度的風險。
完整	偵錯	是	檔案系統已超過此警示設定的臨界值（預設值為98% ）。百分比是 `Used`總和減去快照保留區的大小。	• 增加Volume大小 • 減少使用者資料	寫入作業或資料可用度尚無風險、但磁碟區即將進入寫入作業可能面臨風險的階段。
邏輯過度配置	服務錯誤	n	除了檔案系統已滿之外、用於中繼資料的磁碟區空間也已用盡。	• 增加Volume大小 • 刪除快照 • 減少使用者資料 • 停用檔案或LUN的空間保留	寫入未保留檔案的作業可能會失敗。
實體過度分派	節點錯誤	n	磁碟區的實體區塊已用完、無法寫入。	• 增加Volume大小 • 刪除快照 • 減少使用者資料	寫入作業及資料可用度均面臨風險、磁碟區可能離線。

每次跨越某個Volume的臨界值時、無論完整度百分比是上升或下降、都會產生一則EMS訊息。當磁碟區的完整層級低於臨界值時、 A `volume ok` 系統會產生 EMS 訊息。

處理**Aggregate**完整度和過度配置警示

當Aggregate空間不足時、系統會發出EMS訊息、以便您為整個Aggregate提供更多空間來採取修正行動。ONTAP瞭解警示類型及其處理方式、有助於確保資料可用度。

如果將Aggregate描述為_f完整_、表示可供磁碟區使用的Aggregate空間百分比已降至預先定義的臨界值以下。當Aggregate變成_overallocated時、ONTAP 由支援中繼資料和基本資料存取的空間已耗盡。有時候通常保留給其他用途的空間可用於維持集合體的運作、但與集合體或資料可用度相關的磁碟區保證可能會有風險。

過度配置可以是邏輯或實體配置。_Logical overall撥款_表示保留以履行未來空間承諾（例如Volume保證）的空間已用於其他用途。_Physical overall撥款_表示該集合體已用完要使用的實體區塊。此狀態的集合體可能會拒絕寫入、離線或導致控制器中斷。

下表說明Aggregate完整度和過度配置警示、您可以採取哪些行動來解決此問題、以及不採取行動的風險。

警示類型	**EMS**層級	可設定的？	定義	解決方法	若未採取任何行動、則有風險
幾乎已滿	偵錯	n	已配置給磁碟區的空間量（包括它們的保證）已超過此警示設定的臨界值（95%）。百分比是 `Used`總和減去快照保留區的大小。	• 將儲存設備新增至Aggregate • 正在壓縮或刪除磁碟區 • 將磁碟區移至另一個具有更多空間的Aggregate • 移除 Volume 保證（將其設定為 `none`）	還沒有寫入作業或資料可用度的風險。
完整	偵錯	n	檔案系統已超過此警示設定的臨界值（98%）。百分比是 `Used`總和減去快照保留區的大小。	• 將儲存設備新增至Aggregate • 正在壓縮或刪除磁碟區 • 將磁碟區移至另一個具有更多空間的Aggregate • 移除 Volume 保證（將其設定為 `none`）	對集合體中磁碟區的磁碟區保證可能有風險、也可能會對這些磁碟區進行寫入作業。

警示類型	EMS層級	可設定的？	定義	解決方法	若未採取任何行動、則有風險
邏輯過度配置	服務錯誤	n	除了保留給磁碟區的空間已滿之外、用於中繼資料的集合體空間也已用盡。	• 將儲存設備新增至Aggregate • 正在壓縮或刪除磁碟區 • 將磁碟區移至另一個具有更多空間的Aggregate • 移除 Volume 保證（將其設定為 `none`）	對集合體中磁碟區的磁碟區保證會有風險、也會對這些磁碟區進行寫入作業。
實體過度分派	節點錯誤	n	Aggregate已用盡可寫入的實體區塊。	• 將儲存設備新增至Aggregate • 正在壓縮或刪除磁碟區 • 將磁碟區移至另一個具有更多空間的Aggregate	將作業寫入集合體中的磁碟區會受到風險、同時也會影響資料可用度、因為集合體可能會離線。在極致情況下、節點可能會發生中斷。

每當跨越某個集合體的臨界值時、無論全度百分比是上升或下降、都會產生EMS訊息。當集合體的完整層級低於臨界值時 `aggregate ok` 系統會產生 EMS 訊息。

設定部分保留時的考量事項

部分保留（也稱為_LUN覆寫保留區_）可讓您關閉FlexVol 針對空間保留LUN和位於一個實體磁碟區中檔案的覆寫保留。這有助於最大化儲存使用率。

如果您的環境因空間不足而導致寫入作業失敗而受到負面影響、您必須瞭解此組態可能會造成的需求。

百分比保留設定是以百分比表示 `0`、唯一有效的值是和 `100`**`百分比。「部分保留」設定是`**`Volume`**的屬性。設定部分保留以 `0``提高儲存使用率。然而、如果磁碟區的可用空間不足、存取位於磁碟區中資料的應用程式可能會發生資料中斷、即使將磁碟區保證設定為 `volume`。不過、只要有適當的Volume組態和使用、就能將寫入失敗的機率降至最低。ONTAP 為部分保留設定為達到下列要求時 *all* 的磁碟區提供「盡力」寫入保證 `0`：

- 重複資料刪除功能未在使用中
- 壓縮未在使用中
- FlexClone子檔案未在使用中
- 所有FlexClone檔案和FlexClone LUN均已啟用自動刪除功能

  這不是預設設定。您必須明確啟用自動刪除功能、無論是在建立時或是在建立FlexClone檔案或FlexClone LUN之後加以修改。

- 不使用ODX和FlexClone複本卸載
- Volume 擔保設為 `volume`
- 檔案或 LUN 空間保留為 `enabled`
- Volume Snapshot 保留區設為 `0`
- Volume Snapshot 自動刪除的 `enabled`**承諾層級為** `destroy`，的銷毀清單，`lun_clone,vol_clone,cifs_share,file_clone,sfsr`**以及觸發程序** `volume`

  此設定也可確保在必要時刪除FlexClone檔案和FlexClone LUN。

- 如果滿足上述所有要求，但變更率很高，在極少數情況下，快照自動刪除可能會落後，導致磁碟區空間不足。
- 如果滿足上述所有要求，且未使用快照，則磁碟區寫入保證不會用盡空間。

此外，您也可以選擇使用 Volume 自動擴充功能來降低自動刪除磁碟區快照的可能性。如果啟用自動擴充功能、則必須監控相關聯Aggregate中的可用空間。如果 Aggregate 已滿，而磁碟區無法成長，則可能會在磁碟區的可用空間耗盡時刪除更多快照。

如果您無法滿足上述所有組態需求、而且需要確保磁碟區不會用盡空間、則必須將磁碟區的「部分保留」設定設為 `100`。這需要更多的可用空間、但保證資料修改作業即使在使用上述技術時仍能順利完成。

「部分保留」設定的預設值和允許值取決於Volume的保證：

Volume保證	預設的部分保留	允許的值
Volume	100	0 、 100
無	0%	0 、 100

確定卷的文件和 **inode** 使用情況

包含最多檔案數量的資料。FlexVol您可以使用 CLI 命令來判斷是否需要增加 FlexVol 磁碟區的（公有） inode 數量、以防止它們達到其檔案限制。

關於這項工作

公共inode可以是自由的（與檔案無關）、也可以是使用的（指向檔案）。Volume的可用inode數量為Volume的inode總數減去使用的inode數（檔案數）。

如果qtree層級和Volume層級的共享存在於相同FlexVol 的SCVMM或SCVMM資源池中、qtree就會顯示為FlexVol 該共享區上的目錄。因此、您必須小心不要意外刪除。

步驟

1. 若要顯示磁碟區的inode使用量、請輸入下列命令：

```
volume show -vserver <SVM_name> -volume <volume_name> -fields files-used
```

範例

```
cluster1::*> volume show -vserver vs1 -volume vol1 -fields files-used
Vserver Name: vs1
Files Used (for user-visible data): 98
```

利用儲存 **QoS** 來控制和監控 **FlexVol volume I/O** 效能

您可以FlexVol 將磁碟區指派給Storage QoS原則群組、藉此控制輸入/輸出（I/O）至VMware Volume的效能。您可以控制I/O效能、確保工作負載達到特定的效能目標、或是調節對其他工作負載造成負面影響的工作負載。

關於這項工作

策略群組會強制執行最大處理量限制（例如 100 MB/s）。您可以建立策略群組而不指定最大處理量，這樣可以在控制工作負載之前監控效能。您也可以指定選用的最小處理量限制。

您也可以將SVM、LUN和檔案指派給原則群組。

請注意下列有關指派磁碟區給原則群組的需求：

- 磁碟區必須由原則群組所屬的SVM所包含。

  您可以在建立原則群組時指定SVM。

- 從 ONTAP 9.18.1 開始，您可以將 QoS 原則指派給包含在具有 QoS 原則的 SVM 中的磁碟區。使用巢狀 QoS 原則時，會套用限制最嚴格的原則。
- 從 ONTAP 9.14.0 開始、您可以將原則指派給包含在具有 QoS 原則之磁碟區中的 qtree。

如需如何使用Storage QoS的詳細資訊、請參閱 "系統管理參考資料"。

步驟

1. 使用 `qos policy-group create` 建立原則群組的命令。
2. 使用 `volume create` 命令或 `volume modify` 命令 `-qos-policy-group` 將磁碟區指派給原則群組的參數。
3. 使用 `qos statistics` 檢視效能資料的命令。
4. 如有必要、請使用 `qos policy-group modify` 命令來調整原則群組的最大處理量限制。

相關資訊

- "QoS策略組"
- 連結： https://docs.netapp.com/us-en/ontap-cli/qos-policy-group-create.html ://docs.netapp.com/us-en/ontap-cli/qos-policy-group-create.html [qos policy-group create]
- "Volume建立"
- "Volume修改"
- "QoS 統計資料"

刪除FlexVol 一個流通量

您可以刪除不再需要的 FlexVol Volume 。

開始之前

任何應用程式都不得存取您要刪除之磁碟區中的資料。

> 如果您意外刪除了卷，請參閱"NetApp知識庫：如何使用磁碟區復原佇列"。

步驟

1. 如果磁碟區已掛載、請將其卸載：

   ```
   volume unmount -vserver vserver_name -volume volume_name
   ```

2. 如果 Volume 是 SnapMirror 關係的一部分、請使用刪除關係 `snapmirror delete` 命令。
3. 如果磁碟區已上線、請將磁碟區離線：

   ```
   volume offline -vserver vserver_name volume_name
   ```

4. 刪除Volume：

   ```
   volume delete -vserver vserver_name volume_name
   ```

結果

磁碟區會連同任何相關的配額原則和qtree一起刪除。

相關資訊

- "SnapMirror刪除"
- "Volume卸載"
- "Volume離線"
- "Volume刪除"

防止意外刪除磁碟區

預設Volume刪除行為有助於恢復意外刪除FlexVol 的不小心刪除的功能區。

答 `volume delete` 對類型為的 Volume 提出要求 `RW` 或 `DP` （如所示 `volume show` 命令輸出）會將該磁碟區移至「部分刪除」狀態。根據預設、它會保留在恢復佇列中至少12小時、然後才被完全刪除。

> 刪除包含已刪除磁碟區的 SVM 會清除磁碟區復原佇列（VRQ）。只有當您確定無需還原 SVM 擁有的磁碟區時，才應刪除 SVM。刪除擁有磁碟區的 SVM 時，磁碟區復原佇列中的磁碟區將無法存在。

相關資訊

- "如何使用Volume Recovery Queue"

- "Volume刪除"
- "Volume Show"

用於在 **ONTAP** 中管理 **FlexVol Volume** 的命令

ONTAP CLI 提供用於管理 FlexVol Volume 的特定命令。您可以使用下列命令來管理 FlexVol 磁碟區、視您需要執行的作業而定：

如果您想要...	使用此命令...
將Volume上線	`volume online`
變更Volume的大小	`volume size`
判斷磁碟區的相關Aggregate	`volume show`
判斷儲存虛擬機器（SVM）上所有磁碟區的相關Aggregate	`volume show -vserver -fields aggregate`
判斷磁碟區的格式	`volume show -fields block-type`
使用交會將磁碟區掛載到另一個磁碟區	`volume mount`
將磁碟區置於受限狀態	`volume restrict`
重新命名Volume	`volume rename`
使Volume離線	`volume offline`

如"指令參考資料ONTAP"需詳細 `volume`資訊，請參閱。

用於顯示空間使用資訊的命令

您可以使用 `storage aggregate`和 `volume`命令來查看如何在集合體和磁碟區中使用空間及其快照。

從 ONTAP 9.18.1 開始， `storage aggregate show-space` 指令變更了邏輯引用容量和邏輯非引用容量的報告方式。邏輯引用容量報告所有物件中的引用區塊以及碎片化物件中的非引用區塊。邏輯非引用容量僅報告已超過滿容量閾值且符合物件刪除和碎片整理條件的物件中的非引用區塊。

例如，當您使用 ONTAP S3 和 StorageGRID 的預設 Aggregate 完整度臨界值 40% 時，物件中 60% 的區塊必須未被引用，然後這些區塊才會被報告為未被引用的容量。

在 ONTAP 9.18.1 之前的版本中，「邏輯引用容量」會報告所有物件（包括已滿物件和碎片物件）中已引用的區塊。「邏輯未引用容量」會報告所有物件中未引用的區塊。

若要顯示有關...的資訊	使用此命令...

集合體，包括已用空間和可用空間百分比的詳細資料，快照保留空間大小，以及其他空間使用資訊	`storage aggregate show`
	
	`storage aggregate show-space -fields snap-size-total,used-including-snapshot-reserve`

如何在Aggregate和RAID狀態中使用磁碟和RAID群組	`storage aggregate show-status`
如果刪除特定快照，將會回收的磁碟空間量	`volume snapshot compute-reclaimable` （進階）

Volume所使用的空間量	`volume show -fields size,used,available,percent-used`
	
	`volume show-space`

包含Aggregate中某個磁碟區所使用的空間量	`volume show-footprint`

相關資訊

- "儲存Aggregate顯示"
- "儲存聚合展示空間"
- "儲存聚合顯示狀態"
- "Volume Snapshot可運算回收"
- "Volume Show"

移動及複製磁碟區

移動**FlexVol** 一份本產品介紹

您可以移動或複製磁碟區、以提高容量使用率、提升效能、並達成服務層級協議。瞭解如何搬移FlexVol 功能可協助您判斷Volume搬移是否符合服務層級協議、並瞭解Volume搬移程序的位置。

在同一個儲存虛擬機器（SVM）中、將各個集合體或節點之間的各個sf2 Volume移至另一個集合體或節點。FlexVol在移動期間、磁碟區移動不會中斷用戶端存取。

> ⓘ 在Volume Move作業的轉換階段、您無法建立FlexVol FlexClone檔案或FlexClone LUN的整個功能。

在多個階段中移動磁碟區：

- 在目的地Aggregate上建立新磁碟區。
- 原始磁碟區的資料會複製到新磁碟區。

在此期間、原始磁碟區會保持不變、可供用戶端存取。

- 在移動程序結束時、用戶端存取會暫時遭到封鎖。

  在此期間、系統會執行從來源磁碟區到目的地磁碟區的最終複寫、交換來源與目的地磁碟區的識別、並將目的地磁碟區變更為來源磁碟區。

- 完成移動後、系統會將用戶端流量路由傳送至新的來源Volume、並恢復用戶端存取。

這項移轉不會中斷用戶端存取、因為封鎖用戶端存取的時間會在用戶端發現中斷和逾時之前結束。預設會封鎖用戶端存取30秒。如果磁碟區移動作業無法在存取遭拒的時間內完成、系統會中止磁碟區移動作業的最後階段、並允許用戶端存取。系統預設會嘗試最後階段三次。第三次嘗試之後、系統會先等待一小時、然後再嘗試最後的階段順序。系統會執行Volume Move作業的最後階段、直到Volume Move完成為止。

移動磁碟區時的考量與建議

移動磁碟區時、需要注意幾個考量事項和建議。這些資料是根據您要移動的磁碟區、以及系統組態（例如 MetroCluster ）而定。在移動 Volume 之前、您應該先瞭解所有相關問題。

一般考量與建議

- 如果您要升級叢集的版本系列，請在升級叢集中的所有節點之前，不要移動磁碟區。

  此建議可防止您不慎嘗試將磁碟區從較新的發行系列移至較舊的發行系列。

- 來源Volume必須一致。
- 如果您已將一個或多個集合體指派給相關的儲存虛擬機器（SVM）、則目的地集合體必須是其中一個指派的集合體。
- 您只能將磁碟區移至較新的 ONTAP 版本。
- 您無法將磁碟區移至接管的CFO集合體、或從該集合體移出該磁碟區。
- 如果在您移動包含 LUN 的磁碟區之前未啟用 NVFAIL ，則在您移動磁碟區之後，該磁碟區將會啟用 NVFAIL 。
- 您可以將磁碟區從Flash Pool Aggregate移至其他Flash Pool Aggregate。
  - 也會移動該磁碟區的快取原則。
  - 移動可能會影響磁碟區效能。
- 您可以在Flash Pool Aggregate與非Flash Pool Aggregate之間移動磁碟區。
  - 如果您將磁碟區從Flash Pool Aggregate移至非Flash Pool Aggregate、ONTAP 則會顯示訊息警告您移動可能會影響磁碟區效能、並詢問您是否要繼續。
  - 如果您將磁碟區從非 Flash Pool Aggregate 移至 Flash Pool Aggregate 、 ONTAP 會指派 `auto` 快取原則：
- 磁碟區擁有其所在之集合體的閒置資料保護。如果您將磁碟區從包含NSE磁碟機的集合體移至不包含的磁碟區、則該磁碟區將不再具有NSE資料閒置保護。
- 如果您要將FabricPool最佳化磁碟區從ONTAP 9.13.1 或更早版本移至ONTAP 9.15.1 或更高版本，請參閱"NetApp知識庫：CONTAP-307878 - 如果來源ONTAP小於 9.14.1 且目標大於 9.14.1，則在FabricPool優化磁碟區移動期間發生意外重啟"。

- 從ONTAP 9.15.1 開始，將磁碟區從 A400 系統移至 A70、A90 或 A1K 系統可能會導致讀取延遲問題增加。有關詳細資訊和建議措施，請參閱 "NetApp知識庫：CONTAP-556247 - 磁碟區從 A400 遷移到 A70、A90 和 A1K 後壓縮/解壓縮速度緩慢"。

FlexClone Volume考量與建議

- FlexClone Volume在移動時無法離線。
- 您可以將 FlexClone Volume 從一個 Aggregate 移至同一個節點或同一個 SVM 中的另一個節點上的另一個 Aggregate 、而無需啟動 `vol clone split start` 命令。

  藉由在FlexClone Volume上啟動Volume Move作業、複製磁碟區會在移轉過程中分割至不同的Aggregate。在複製磁碟區上移動磁碟區完成之後、移動的磁碟區不再顯示為複製、而是顯示為獨立磁碟區、而不會與先前的父磁碟區建立任何複製關係。

- FlexClone Volume 快照不會在移動複本後遺失。
- 您可以將FlexClone父磁碟區從一個Aggregate移至另一個Aggregate。

  當您移動FlexClone父Volume時、暫存磁碟區會被留在後方、做為所有FlexClone Volume的父Volume。暫用磁碟區上不允許執行任何作業、除非是將其離線或刪除。在所有FlexClone磁碟區分割或銷毀之後、暫存磁碟區會自動清理。

- 在您移動FlexClone子Volume之後、該Volume不再是FlexClone Volume。
- FlexClone Move作業與FlexClone複製或分割作業互不互用。
- 如果正在進行複製分割作業、則移動磁碟區可能會失敗。

  在完成複製分割作業之前、不應移動磁碟區。

MetroCluster 考量與建議

- 在MetroCluster 以等位組態移動磁碟區期間、當在來源叢集的目的地集合體上建立暫存磁碟區時、也會在存續叢集上建立與鏡射磁碟區相對應但未同化的暫存磁碟區記錄。
- 如果MetroCluster 在轉換之前發生了一個故障切換、則目的地Volume會有一筆記錄、而且是一個暫用Volume（TMP類型的Volume）。

  移動工作會在存續（災難恢復）叢集上重新啟動、報告故障、並清除所有與移動相關的項目、包括暫存磁碟區。如果無法正確執行清除作業、系統會產生EMS、提醒系統管理員執行必要的清除作業。

- 如果MetroCluster 在轉換階段開始之後、但在移動工作完成之前（也就是移動到可將叢集更新為指向目的地Aggregate的階段）發生了還原切換、則移動工作會在存續期間重新啟動（災難恢復） 完成叢集和執行。

  所有與移動相關的項目都會清除、包括暫用Volume（原始來源）。如果無法正確執行清除作業、系統會產生EMS、提醒系統管理員執行必要的清除作業。

- 如果屬於切換站台的磁碟區正在執行任何Volume搬移作業、則不MetroCluster 允許強制或非強制性的停止功能。

  當本機磁碟區移轉作業正在進行中，而容後移轉作業仍在運作中的站台，則不會封鎖切換。

- 未強制的 MetroCluster 切換會遭到封鎖，但如果正在進行任何磁碟區移動作業，則不會封鎖強制的 MetroCluster 切換。

在 **SAN** 環境中移動磁碟區的需求

在 SAN 環境中移動磁碟區之前、您必須做好準備。

在移動包含 LUN 或命名空間的磁碟區之前、您必須符合下列需求：

- 對於包含一個或多個LUN的磁碟區、每個LUN（I生命 體）至少應有兩個路徑連線至叢集中的每個節點。

  如此可消除單點故障、並讓系統在元件故障時仍能繼續運作。

- 對於包含命名空間的磁碟區、叢集必須執行ONTAP 的是32個以上版本的版本。

  執行ONTAP Sfor Sfor 9.5的NVMe組態不支援Volume Move。

移動**ONTAP**卷

您可以將FlexVol 某個SVM磁碟區移至同一個儲存虛擬機器（SVM）內的不同集合體、節點或兩者、以在判斷儲存容量不平衡之後、平衡儲存容量。

關於這項工作

根據預設、如果切換作業在30秒內無法完成、將會重試。您可以使用和 `-cutover-action`參數來調整預設行為 `-cutover-window`，這兩者都需要進階權限層級存取。

您必須是叢集管理員才能執行此工作。

開始之前

- 如果您要將使用 8K 自適應壓縮的捲移動到以下平台之一，您應該"增加卷的活動文件系統的大小"在移動音量之前。這些平台上的資料壓縮方式不同，因此節省的空間是在聚合層級而不是磁碟區層級。由於這種差異，磁碟區的活動檔案系統的大小應該會增加 8k 壓縮節省量，以防止磁碟區在磁碟區移動期間耗盡空間。
  - 支援專用卸載處理器儲存效率的AFF和FAS平台

    詳細了解支援以下功能的AFF和FAS平台"專用卸載處理器儲存效率"。

  - AFF C 系列平台

    查看"Hardware Universe"了解 C 系列平台的完整清單。

- 如果您正在移動資料保護鏡像且尚未初始化鏡像關係，請使用 `snapmirror initialize`命令初始化鏡像關係。詳細了解 `snapmirror initialize`在"指令參考資料ONTAP" 。

  必須先初始化資料保護鏡射關係、才能移動其中一個磁碟區。

步驟

1. 確定可以將磁碟區移動到的聚合：

   ```
   volume move target-aggr show
   ```

   您選取的Aggregate必須有足夠的磁碟區空間、也就是可用的大小大於您要移動的磁碟區。

下列範例顯示VS2磁碟區可移至任何列出的集合體：

```
cluster1::> volume move target-aggr show -vserver vs2 -volume user_max
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9GB          hdd
node12a_aggr3    10.34GB          hdd
node12a_aggr2    10.36GB          hdd
node12a_aggr1    10.36GB          hdd
node12a_aggr4    10.36GB          hdd
5 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `volume move target-aggr show`資訊，請參閱。

2. 執行驗證檢查以確認磁碟區可以移動到目標聚合：

```
volume move start -perform-validation-only
```

如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

3. 移動音量：

```
volume move start
```

下列命令可將VS2 SVM上的user_max Volume移至node12a_aggr3 Aggregate。此移動會以背景程序執行。

```
cluster1::> volume move start -vserver vs2 -volume user_max
-destination-aggregate node12a_aggr3
```

4. 確定磁碟區移動操作的狀態：

```
volume move show
```

以下範例顯示完成複寫階段且處於轉換階段的Volume Move狀態：

```
cluster1::> volume move show
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       user_max   healthy  cutover     -                -
```

當 Volume 移動不再出現在中時、即完成移動 `volume move show` 命令輸出。

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

5. 或者，查看壓縮節省：

```
volume show-footprint -vserver <SVM> -volume <volume_name>
```

透過在磁碟區移動完成後不久自動執行的後處理轉換掃描，可以實現額外的聚合級節省。

相關資訊

- "移動磁碟區時的考量與建議"

從 **8k** 自適應壓縮遷移之前增加**ONTAP**磁碟區的活動檔案系統

支援8k自適應壓縮的平台在磁碟區層級節省空間。 AFF C 系列平台和支援 32k 壓縮的平台可在聚合層級節省空間。將磁碟區從 8k 自適應壓縮遷移到AFF C 系列平台或具有 32k 壓縮的平台時，您需要透過 8k 壓縮節省來增加磁碟區的活動檔案系統的大小。這可以防止磁碟區移動期間耗盡可用空間。

以下系統支援 32k 壓縮：

平台	版本**ONTAP**
• AFF A1K • AFF A90 • AFF A70 • FAS90 • FAS70	9.15.1 或更新版本
• AFF C80 • AFF C60 • AFF C30 • AFF A50 • AFF A30	9.16.1 或更新版本

詳細了解"支援 32k 壓縮的AFF和FAS平台" 。

查看"Hardware Universe"以取得AFF C 系列平台的完整清單。

關於這項工作

如果您使用磁碟區移動操作遷移數據，請執行下列步驟。如果您使用SnapMirror操作遷移數據，則無需手動增加活動檔案系統的大小。 SnapMirror目標磁碟區預設使用磁碟區自動調整大小，因此由於在聚合層而不是磁碟區層實現壓縮節省，預計不會耗盡空間。

開始之前

如果您的磁碟區上未啟用邏輯空間報告和強制執行，您可以選擇透過設定 `-is-space-reporting-logical`和 `-is-space-enforcement-logical`參數為*true*。在磁碟區移動之前啟用這些設定可以幫助您評估磁碟區是否足夠大，以適應從 8k 壓縮轉換時磁碟區層的壓縮節省損失。您應該在磁碟區上啟用這些設定。如果在 SVM 層級啟用這些設置，則它們僅適用於新建立的磁碟區。

步驟

1. 驗證磁碟區的目前大小和快照保留：

```
volume show-space
```

2. 檢查卷的壓縮空間節省：

```
volume show -vserver -volume -fields compression-space-saved
```

3. 將磁碟區的活動檔案系統大小增加所示的量 `compression-space-saved`加上快照保留。

```
volume size -vserver <vserver_name> -volume <volume_name> -new-size
+<size>
```

範例

如果磁碟區為 100GB，且具有 20% 的快照保留；則活動檔案系統為 80GB，快照保留為 20GB。要將活動檔案系統增加 20GB，必須將總磁碟區大小增加 25GB；也就是說，20GB 用於活動檔案系統，5GB（20%）用於快照保留。

```
volume size -vserver svm1 -volume volx -size +20GB
```

4. 驗證卷的大小是否增加：

```
volume show -vserver <vserver_name> -volume <volume_name> -fields size
```

結果

您的磁碟區的活動檔案系統大小已增加，您已準備好移動該磁碟區。

接下來呢？

執行"Volume搬移"遷移您的資料。

用於在 **ONTAP** 中移動 **Volume** 的命令

ONTAP CLI 提供管理 Volume 移動的特定命令。視您需要執行的動作而定、請使用下列命令來管理配額規則和配額原則：

如果您想要...	使用此命令...
中止作用中Volume移動作業。	`volume move abort`
顯示從一個Aggregate移至另一個Aggregate的磁碟區狀態。	`volume move show`
開始將磁碟區從一個Aggregate移至另一個Aggregate。	`volume move start`
管理目標Aggregate以進行Volume搬移。	`volume move target-aggr`
觸發轉換移動工作。	`volume move trigger-cutover`
如果預設值不足、請變更用戶端存取被封鎖的時間量。	`volume move start` 或 `volume move modify` 使用 `-cutover-window` 參數。。 `volume move modify` 命令是進階命令和 `-cutover-window` 為進階參數。
判斷當用戶端存取遭封鎖時、如果無法完成Volume Move作業、系統會執行什麼動作。	`volume move start` 或 `volume move modify` 使用 `-cutover-action` 參數。。 `volume move modify` 命令是進階命令和 `-cutover-action` 為進階參數。

相關資訊

- "Volume搬移"

複製**Volume**的方法

複製磁碟區的方法取決於您是將磁碟區複製到相同的 Aggregate 還是不同的 Aggregate ，以及您是否要保留原始磁碟區的快照。複製磁碟區會建立一個獨立的磁碟區複本、供您用於測試及其他用途。

下表列出複本的特性及建立複本的方法。

如果您要複製**Volume ...**	您使用的方法是...
在同一個 Aggregate 中，您不想從原始 Volume 複製快照。	建立原始Volume的FlexClone Volume。
而您不想從原始磁碟區複製快照到另一個 Aggregate 。	建立原始 Volume 的 FlexClone Volume 、然後使用將該 Volume 移至其他 Aggregate `volume move` 命令。
將原始磁碟區的所有快照保留到另一個集合體。	使用SnapMirror複寫原始磁碟區、然後打破SnapMirror關係以建立讀寫磁碟區複本。

使用**FlexClone Volume**來建立**FlexVol** 有效複本的功能

FlexClone Volume 使用概觀

FlexClone磁碟區是父FlexVol 級NetApp磁碟區的可寫入時間點複本。FlexClone磁碟區具有空間效率、因為它們與通用FlexVol 資料的父實體資料磁碟區共用相同的資料區塊。用於建立 FlexClone Volume 的快照也會與父磁碟區共用。

您可以複製現有的FlexClone磁碟區、以建立另一個FlexClone磁碟區。您也可以建立FlexVol 包含LUN和LUN複製的實體磁碟區複本。

您也可以從FlexClone Volume的父Volume分割。從ONTAP 功能不保證的9.4開始AFF 、對於不保證在功能不保證的作業系統、FlexClone Volume的分割作業會共用實體區塊、而不會複製資料。因此AFF 、將FlexClone磁碟區分割到整個系統上的速度、比FAS 在其他版本ONTAP 的更新版本中執行FlexClone分割作業的速度更快。

您可以建立兩種類型的FlexClone磁碟區：讀寫FlexClone磁碟區和資料保護FlexClone磁碟區。雖然您可以為一般FlexVol 的流通量建立一個讀寫FlexClone Volume、但您只能使用SnapVault 一個流通的次要Volume來建立資料保護FlexClone Volume。

建立**FlexClone Volume**

您可以從SnapMirror目的地Volume或FlexVol 從父實體的父實體磁碟區（SnapVault 即次磁碟區）建立資料保護FlexClone磁碟區。從 ONTAP 9.7 開始、您可以從 FlexGroup Volume 建立 FlexClone Volume 。建立FlexClone Volume之後、您無法在FlexClone Volume存在時刪除父Volume。

開始之前

- FlexClone授權必須安裝在叢集上。本授權隨附於"ONTAP One"。
- 您要複製的磁碟區必須在線上。

MetroCluster 組態不支援將 Volume 複製為不同 SVM 上的 FlexClone Volume 。

建立 **FlexVol** 或 **FlexGroup** 的 **FlexClone Volume**

步驟

1. 建立FlexClone Volume：

`volume clone create`

> 從讀寫父磁碟區建立讀寫 FlexClone 磁碟區時，不需要指定基礎快照。如果您未命名任何要作為複本基礎快照的特定快照，則 ONTAP 會建立快照。當父磁碟區是資料保護磁碟區時，您必須指定用於建立 FlexClone 磁碟區的基礎快照。

範例

- 下列命令會從父Volume vol1建立讀寫FlexClone Volume vol1_clone：

```
volume clone create -vserver vs0 -flexclone vol1_clone -type RW -parent-volume
vol1
```

- 下列命令會使用基礎 Snapshot snap1 ，從父 Volume DP_vol 建立資料保護 FlexClone Volume vol_dm_clone ：

```
volume clone create -vserver vs1 -flexclone vol_dp_clone -type DP -parent
-volume dp_vol -parent-snapshot snap1
```

建立任何 **SnapLock** 類型的 **FlexClone**

從 ONTAP 9.13.1 開始、您可以指定三種 SnapLock 類型之一、 `compliance`、 `enterprise`、 `non-snaplock`（創建 RW 卷的 FlexClone 時）。根據預設、 FlexClone Volume 是以與父磁碟區相同的 SnapLock 類型建立。不過、您可以使用來覆寫預設值 `snaplock-type` FlexClone Volume 建立期間的選項。

使用 `non-snaplock` 參數 `snaplock-type` 選項：您可以從 SnapLock 父磁碟區建立非 SnapLock 類型的 FlexClone Volume 、以便在必要時提供更快速的資料恢復線上的方法。

深入瞭解 "SnapLock"。

開始之前

當 FlexClone Volume 的 SnapLock 類型與父 Volume 不同時、您應該瞭解下列 FlexClone Volume 限制。

- 僅支援 RW 類型的複本。不支援 SnapLock 類型與父磁碟區不同的 DP 型複本。
- 由於 SnapLock 磁碟區不支援 LUN 、因此無法使用 SnapLock 類型選項將具有 LUN 的磁碟區複製到「 non-SnapLock 」以外的值。
- MetroCluster 鏡射 Aggregate 上的 Volume 無法以 Compliance SnapLock 類型複製、因為 MetroCluster 鏡射 Aggregate 不支援 SnapLock Compliance Volume 。
- 無法以不同的 SnapLock 類型複製具有保留法的 SnapLock 規範磁碟區。僅 SnapLock Compliance Volume 支援合法保留。
- SVM DR 不支援 SnapLock Volume 。嘗試從 SVM 中屬於 SVM DR 關係一部分的磁碟區建立 SnapLock 複本將會失敗。
- FabricPool 最佳實務做法建議複本保留與父實體相同的分層原則。不過、啟用 FabricPool 的磁碟區的 SnapLock Compliance 複本、不能與父磁碟區具有相同的分層原則。分層原則必須設為 `none`。嘗試從父實體建立 SnapLock 規範複本、但其分層原則並非如此 `none` 將會失敗。

步驟

1. 使用 SnapLock 類型建立 FlexClone Volume ： `volume clone create -vserver` *`svm_name`*

```
-flexclone flexclone_name -type RW [ -snaplock-type {non-
snaplock|compliance|enterprise} ]
```

範例：

```
> volume clone create -vserver vs0 -flexclone vol1_clone -type RW
-snaplock-type enterprise -parent-volume vol1
```

從其父**Volume**分割**FlexClone Volume**

您可以從父磁碟區分割 FlexClone Volume 、使複製成為正常的 FlexVol 磁碟區。

複製分割作業會在背景執行。分割期間、可在複本和父實體上存取資料。從 ONTAP 9.4 開始、空間效率就會保留下來。分割程序只會更新中繼資料、而且需要最少的 IO 。不會複製任何資料區塊。

關於這項工作

- 分割作業期間無法建立 FlexClone Volume 的新快照。
- 如果 FlexClone Volume 屬於資料保護關係、或是負載共用鏡像的一部分、則無法從父 Volume 分割該 Volume 。
- 如果您在分割進行中使 FlexClone Volume 離線、分割作業會暫停；當您將 FlexClone Volume 恢復上線時、分割作業會恢復。
- 分割後、父 FlexVol Volume 和複本都需要由其磁碟區保證所決定的完整空間分配。
- 從父磁碟區分割 FlexClone 磁碟區之後、就無法重新加入這兩個磁碟區。
- 從ONTAP 功能不保證的9.4開始AFF 、對於不保證在功能不保證的作業系統、FlexClone Volume的分割作業會共用實體區塊、而不會複製資料。因此、在 AFF 系統上分割 FlexClone 磁碟區的速度比 ONTAP 9.4 及更新版本中其他 FAS 系統的 FlexClone 分割作業更快。改良後AFF 的FlexClone分割作業在整個過程中有下列優點：
  - 將實體複本從父實體複本分割後、儲存效率仍會維持不變。
  - 不會刪除現有的快照。
  - 作業速度更快。
  - FlexClone磁碟區可從複製階層中的任何點分割。

開始之前

- 您必須是叢集管理員。
- 當分割作業開始時、 FlexClone Volume 必須處於線上狀態。
- 父磁碟區必須處於線上狀態、才能成功分割。

步驟

1. 判斷完成分割作業所需的可用空間量：

   ```
   volume clone show -estimate -vserver vserver_name -flexclone clone_volume_name
   -parent-volume parent_vol_name
   ```

以下範例提供從父磁碟區「 'vol1' 」分割 FlexClone Volume 「 'clone1' 」所需的可用空間資訊：

```
cluster1::> volume clone show -estimate -vserver vs1 -flexclone clone1
-parent-volume volume1
                             Split
Vserver   FlexClone       Estimate
--------- ------------- ----------
vs1       clone1           40.73MB
```

2. 驗證包含FlexClone Volume及其父磁碟區的集合體是否有足夠的空間：
   a. 確定包含FlexClone磁碟區及其父磁碟區的集合體可用空間量：

      `storage aggregate show`

   b. 如果包含的Aggregate沒有足夠的可用空間、請將儲存空間新增至Aggregate：

      `storage aggregate add-disks`

3. 開始分割作業：

   `volume clone split start -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`*

   以下範例說明如何啟動從父磁碟區「 'vol1' 」分割 FlexClone Volume 「 'clone1' 」的程序：

```
cluster1::> volume clone split start -vserver vs1 -flexclone clone1

Warning: Are you sure you want to split clone volume clone1 in Vserver
vs1 ?
{y|n}: y
[Job 1617] Job is queued: Split clone1.
```

4. 監控FlexClone分割作業的狀態：

   `volume clone split show -vserver` *`vserver_name`* `-flexclone` *`clone_volume_name`*

   以下範例顯示AFF 了FlexClone分割作業在整個系統上的狀態：

```
cluster1::> volume clone split show -vserver vs1 -flexclone clone1
                                                  Inodes
Blocks
                                        ---------------------
---------------------
Vserver   FlexClone    Processed Total    Scanned  Updated      % Inode
% Block

Complete  Complete
vs1       clone1         0         0       411247   153600         0
37
```

5. 確認分割磁碟區不再是FlexClone磁碟區：

   `volume show -volume volume_name -fields clone-volume`

   的值 `clone-volume` 對於非 FlexClone Volume 的 Volume 、選項為「 'FALSE' 」。

   以下範例說明如何驗證從父磁碟分割的磁碟區「 clone1 」是否不是 FlexClone 磁碟區。

```
cluster1::> volume show -volume clone1 -fields clone-volume
vserver volume **clone-volume**
------- ------ **-------------**
vs1     clone1 **false**
```

相關資訊

- "存儲聚合添加磁碟"

確定**FlexClone Volume**所使用的空間

您可以根據FlexClone磁碟區的名義大小及其與父FlexVol 實體化的共享空間量、來判斷其所使用的空間。建立FlexClone Volume時、它會將所有資料與其父Volume共用。儘管 FlexVol volume 的標稱大小與父實體大小相同、但它只會從集合體中使用極少的可用空間。

關於這項工作

新建立的FlexClone Volume所使用的可用空間約為其名義大小的0.5%。此空間用於儲存FlexClone Volume的中繼資料。

寫入父磁碟區或FlexClone磁碟區的新資料不會在磁碟區之間共用。寫入FlexClone磁碟區的新資料量增加、會導致FlexClone磁碟區從包含的Aggregate所需的空間增加。

步驟

1. 使用確定 FlexClone Volume 實際使用的實體空間 `volume show` 命令。

以下範例顯示FlexClone磁碟區使用的實體空間總計：

```
cluster1::> volume show -vserver vs01 -volume clone_vol1 -fields
size,used,available,
percent-used,physical-used,physical-used-percent
vserver    volume     size  available  used   percent-used   physical-
used     physical-used-percent
-------   ----------  ----  ---------  -----  ------------
-------------   ---------------------
vs01     clone_vol1   20MB   18.45MB   564KB       7%             196KB
1%
```

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

從**SnapMirror**來源或目的地**Volume**建立**FlexClone Volume**時的考量事項

您可以在現有的Volume SnapMirror關係中、從來源或目的地Volume建立FlexClone Volume。不過、這樣做可能會使SnapMirror複寫作業無法成功完成。

複寫可能無法運作，因為當您建立 FlexClone Volume 時，可能會鎖定 SnapMirror 使用的快照。如果發生這種情況、SnapMirror會停止複寫到目的地Volume、直到FlexClone Volume被銷毀或從其父磁碟區分割為止。您有兩種方法可以解決此問題：

- 如果您暫時需要FlexClone磁碟區、而且可以暫時停止SnapMirror複寫、您可以建立FlexClone磁碟區、並在可能的情況下將其刪除或從其父磁碟區分割。

  當FlexClone磁碟區被刪除或從其父磁碟區分割時、SnapMirror複寫會正常繼續。

- 如果無法接受 SnapMirror 複寫暫時停止，您可以在 SnapMirror 來源 Volume 中建立快照，然後使用該快照建立 FlexClone Volume 。（如果您是從目的地磁碟區建立 FlexClone Volume ，則必須等到該快照複寫到 SnapMirror 目的地磁碟區為止。）

  這種在 SnapMirror 來源磁碟區中建立快照的方法，可讓您建立複本，而無需鎖定 SnapMirror 正在使用的快照。

使用**FlexClone**檔案和**FlexClone LUN**來建立有效率的檔案和**LUN**複本

FlexClone 檔案和 **FlexClone LUN** 使用概觀

FlexClone檔案和FlexClone LUN是父檔案和父LUN的可寫入、節省空間的複本、有助於有效利用實體Aggregate空間。FlexClone檔案和FlexClone LUN僅支援FlexVol 用於支援的不只是功能不完整的磁碟區。

FlexClone 檔案和 FlexClone LUN 使用其大小的 0.4% 來儲存中繼資料。複本會共用其父檔案和父LUN的資料區塊、並佔用可忽略的儲存空間、直到用戶端將新資料寫入父檔案或LUN或複本為止。

用戶端可在父實體和實體實體上執行所有檔案和LUN作業。

您可以使用多種方法來刪除FlexClone檔案和FlexClone LUN。

在 **ONTAP** 中建立 **FlexClone** 檔案或 **FlexClone LUN**

您可以使用來建立 FlexVol Volume 或 FlexClone Volume 中檔案和 LUN 的空間效率與時間效率複本 `volume file clone create` 命令。

開始之前

- FlexClone授權必須安裝在叢集上。本授權隨附於"ONTAP One"。
- 如果將多個區塊範圍用於子LUN複製或子檔案複製、則區塊編號不得重疊。
- 如果您要在啟用調適性壓縮的磁碟區上建立子LUN或子檔案、則區塊範圍不得對齊。

  這表示來源開始區塊編號和目的地開始區塊編號必須是偶數對齊或是ODD對齊。

關於這項工作

根據叢集管理員指派的權限、SVM管理員可以建立FlexClone檔案和FlexClone LUN。

您可以在建立及修改複本時、指定FlexClone檔案和FlexClone LUN的自動刪除設定。依預設、自動刪除設定為停用。

使用建立複本時、您可以覆寫現有的 FlexClone 檔案或 FlexClone LUN `volume file clone create` 命令 `-overwrite-destination` 參數。

當節點達到最大分割負載時、節點會暫時停止接受建立 FlexClone 檔案和 FlexClone LUN 的要求、並發出 `EBUSY` 錯誤訊息。當節點的分割負載低於最大值時、節點會再次接受建立FlexClone檔案和FlexClone LUN的要求。再次嘗試建立要求之前、您應該等到節點有建立複本的容量時再進行。

FlexClone LUN繼承父LUN的空間保留屬性。空間保留的FlexClone LUN所需空間與空間保留的父LUN相同。如果FlexClone LUN未保留空間、則磁碟區必須有足夠的空間來容納對實體複本所做的變更。

步驟

1. 如果您要複製 LUN ，請確認 LUN 未對應或寫入。
2. 建立 FlexClone LUN 或檔案：

   ```
   volume file clone create -vserver vserver_name -volume volume_name -source
   -path source_path -destination-path destination_path
   ```

   以下範例說明如何在Volume vol1中建立父檔案file1_source的FlexClone檔案file1_clone：

   ```
   cluster1::> volume file clone create -vserver vs0 -volume vol1 -source
   -path /file1_source -destination-path /file1_clone
   ```

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

從磁碟區中的快照建立 **FlexClone LUN**

您可以在磁碟區中使用快照來建立 LUN 的 FlexClone 複本。LUN的FlexClone複本可讀取且可寫入。

開始之前

必須安裝FlexClone授權。本授權隨附於"ONTAP One"。

關於這項工作

FlexClone LUN繼承父LUN的空間保留屬性。空間保留的FlexClone LUN所需空間與空間保留的父LUN相同。如果FlexClone LUN未保留空間、則磁碟區必須有足夠的空間來容納對實體複本所做的變更。

步驟

1. 確認LUN未對應或寫入。
2. 建立包含 LUN 的磁碟區快照：

   ```
   volume snapshot create -vserver vserver_name -volume volume_name -snapshot
   snapshot_name
   ```

   您必須為要複製的 LUN 建立快照（備份快照）。

3. 從快照建立 FlexClone LUN ：

   ```
   volume file clone create -vserver vserver_name -volume volume_name -source
   -path source_path -snapshot-name snapshot_name -destination-path
   destination_path
   ```

   如果您需要 FlexClone LUN 才能自動刪除、請加入 `-autodelete true`。如果您使用半厚資源配置在磁碟區中建立此FlexClone LUN、則必須啟用所有FlexClone LUN的自動刪除功能。

4. 驗證FlexClone LUN是否正確：

   ```
   lun show -vserver vserver_name
   ```

   ```
   Vserver Path                      State    Mapped    Type      Size
   ------- ----------------------    -------- --------- -------- -------
   vs1     /vol/vol1/lun1_clone      online   unmapped windows   47.07MB
   vs1     /vol/vol1/lun1_snap_clone online   unmapped windows   47.07MB
   ```

在建立和刪除 **FlexClone** 檔案和 **FlexClone LUN** 之前、請先檢視節點容量

您應該判斷節點是否有容量可接收建立及刪除 FlexClone 檔案和 FlexClone LUN 的要求。這可以透過檢視節點的分割負載來完成。如果達到最大的分割負載、則在分割負載低於最大值之前、不會接受任何新的要求。

關於這項工作

當節點達到其最大分割負載時 `EBUSY` 系統會發出錯誤訊息、以回應建立和刪除要求。當節點的分割負載低於最大值時、節點會再次接受建立及刪除FlexClone檔案和FlexClone LUN的要求。

當 `Allowable Split Load`欄位顯示容量、且建立要求符合可用容量時、節點可以接受新的要求。

步驟

1. 檢視節點使用建立和刪除 FlexClone 檔案和 FlexClone LUN 所需的容量 `volume file clone split load show` 命令。

   在下列範例中、會針對叢集1中的所有節點顯示分割負載。叢集中的所有節點都有能力建立及刪除FlexClone檔案和FlexClone LUN、如「允許的分割負載」欄位所示：

```
cluster1::> volume file clone split load show
Node        Max         Current    Token          Allowable
            Split Load  Split Load Reserved Load  Split Load
----------- ----------- ---------- -------------  ----------
node1          15.97TB          0B          100MB    15.97TB
node2          15.97TB          0B          100MB    15.97TB
2 entries were displayed.
```

相關資訊

- "Volume檔案複製分割載入顯示"

檢視 **FlexClone** 檔案和 **FlexClone LUN** 的空間節約效益

您可以在包含 FlexClone 檔案和 FlexClone LUN 的磁碟區上、檢視區塊共用所儲存的磁碟空間百分比。您可以在容量規劃中執行此動作。

步驟

1. 若要檢視FlexClone檔案與FlexClone LUN所達成的空間節約效益、請輸入下列命令：

   `df -s volname`

   `volname` 為 FlexVol Volume 的名稱。

   如果您執行 `df -s` 命令在啟用重複資料刪除的 FlexVol 磁碟區上、您可以同時檢視重複資料刪除和 FlexClone 檔案及 LUN 所儲存的空間。

範例

以下範例顯示FlexClone Volume test1的空間節約效益：

```
systemA> df -s test1

Filesystem          used   saved   %saved Vserver
/vol/test1/         4828    5744      54%  vs1
```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

刪除FlexClone檔案和FlexClone LUN的方法

您可以使用多種方法來刪除FlexClone檔案和FlexClone LUN。瞭解可用的方法有助於您規劃如何管理複本。

您可以使用下列方法刪除FlexClone檔案和FlexClone LUN：

- 您可以設定FlexVol 使用啟用自動刪除功能的功能自動刪除實體磁碟區、以便在FlexVol 將實體磁碟區的可用空間降至特定臨界值以下時自動刪除。
- 您可以使用NetApp Manageability SDK設定用戶端刪除複本。
- 您可以使用用戶端使用NAS和SAN傳輸協定來刪除複本。

  由於此方法不使用NetApp Manageability SDK、因此預設會啟用較慢的刪除方法。不過、您可以設定系統在使用刪除 FlexClone 檔案時、使用較快的刪除方法 `volume file clone deletion` 命令。

如何使用自動刪除設定來回收可用空間FlexVol

FlexVol 磁碟區和回收可用空間、並提供自動刪除總覽

您可以啟用FlexVol 「自動刪除」功能設定、自動刪除FlexClone檔案和FlexClone LUN。啟用自動刪除功能、即可在磁碟區即將滿時回收磁碟區中的目標可用空間量。

您可以將磁碟區設定為在磁碟區的可用空間減少到特定臨界值以下時、自動開始刪除FlexClone檔案和FlexClone LUN、並在回收磁碟區中的目標可用空間量時、自動停止刪除複本。雖然您無法指定開始自動刪除複本的臨界值、但您可以指定複本是否符合刪除資格、也可以指定磁碟區的目標可用空間量。

當磁碟區中的可用空間降至低於特定臨界值、且符合_兩者_的下列需求時、磁碟區會自動刪除FlexClone檔案和FlexClone LUN：

- 自動刪除功能會針對包含FlexClone檔案和FlexClone LUN的磁碟區啟用。

  您可以使用命令來啟用 FlexVol volume 的自動刪除功能 `volume snapshot autodelete modify`。您必須將參數設 `-trigger`為 `volume`或 `snap_reserve`，讓磁碟區自動刪除 FlexClone 檔案和 FlexClone LUN 。如"指令參考資料ONTAP"需詳細 `volume snapshot autodelete modify`資訊，請參閱。

- FlexClone檔案和FlexClone LUN的自動刪除功能已啟用。

  您可以使用命令搭配 `-autodelete`參數來啟用 FlexClone 檔案或 FlexClone LUN 的自動刪除 `file clone create`功能。因此、您可以停用複本的自動刪除功能、並確保其他Volume設定不會覆寫複本設定、以保留特定的FlexClone檔案和FlexClone LUN。如"指令參考資料ONTAP"需詳細 `file clone create`資訊，請參閱。

設定FlexVol 一個動態磁碟區、以自動刪除FlexClone檔案和FlexClone LUN

您可以將磁碟區設定為在磁碟區的可用空間減少到特定臨界值以下時、自動開始刪除FlexClone檔案和FlexClone LUN、並在回收磁碟區中的目標可用空間量時、自動停止刪除複本。雖然您無法指定開始自動刪除複本的臨界值、但您可以指定複本是否符合刪除資格、也可以指定磁碟區的目標可用空間量。

當磁碟區中的可用空間降至低於特定臨界值、且符合_兩者_的下列需求時、磁碟區會自動刪除FlexClone檔案

和FlexClone LUN：

- 自動刪除功能會針對包含FlexClone檔案和FlexClone LUN的磁碟區啟用。

  您可以使用啟用 FlexVol Volume 的自動刪除功能 `volume snapshot autodelete modify` 命令。您必須設定 `-trigger` 參數至 `volume` 或 `snap_reserve` 讓磁碟區自動刪除 FlexClone 檔案和 FlexClone LUN 。

- FlexClone檔案和FlexClone LUN的自動刪除功能已啟用。

  您可以使用啟用 FlexClone 檔案或 FlexClone LUN 的自動刪除 `file clone create` 命令 `-autodelete` 參數。因此、您可以停用複本的自動刪除功能、並確保其他Volume設定不會覆寫複本設定、以保留特定的FlexClone檔案和FlexClone LUN。

開始之前

- 這個流通量必須包含FlexClone檔案和FlexClone LUN、而且必須處於線上狀態。FlexVol
- 不能將此資訊區做為唯讀磁碟區。FlexVol

步驟

1. 使用命令自動刪除 FlexVol volume 中的 FlexClone 檔案和 FlexClone LUN `volume snapshot autodelete modify` 。如"指令參考資料ONTAP"需詳細 `volume snapshot autodelete modify`資訊，請參閱。

   - 適用於 `-trigger` 參數、您可以指定 `volume` 或 `snap_reserve`。
   - 適用於 `-destroy-list` 參數、您必須一律指定 `lun_clone,file_clone` 無論您是否只想刪除一種類型的複本。
     以下範例說明如何啟用Volume vol1以觸發自動刪除FlexClone檔案和FlexClone LUN以進行空間回收、直到25%的磁碟區包含可用空間為止：

     ```
     cluster1::> volume snapshot autodelete modify -vserver vs1 -volume
     vol1 -enabled true -commitment disrupt -trigger volume -target-free
     -space 25 -destroy-list lun_clone,file_clone

     Volume modify successful on volume:vol1
     ```

     如果您設定的值、則在啟用 FlexVol Volume 進行自動刪除的同時 `-commitment` 參數至 `destroy`的所有 `FlexClone` 檔案和 `FlexClone LUN` `-autodelete` 參數設為 `true` 當磁碟區的可用空間低於指定臨界值時、可能會刪除。不過、 FlexClone 檔案和 FlexClone LUN 都有 `-autodelete` 參數設為 `false` 不會刪除。

2. 使用命令驗證 FlexVol volume 中是否已啟用自動刪除 FlexClone 檔案和 FlexClone LUN `volume snapshot autodelete show` 。如"指令參考資料ONTAP"需詳細 `volume snapshot autodelete show`資訊，請參閱。

   以下範例顯示已啟用Volume vol1來自動刪除FlexClone檔案和FlexClone LUN：

```
cluster1::> volume snapshot autodelete show -vserver vs1 -volume vol1

         Vserver Name: vs1
          Volume Name: vol1
          Enabled: true
            Commitment: disrupt
         Defer Delete: user_created
         Delete Order: oldest_first
  Defer Delete Prefix: (not specified)
    Target Free Space: 25%
              Trigger: volume
     *Destroy List: lun_clone,file_clone*
Is Constituent Volume: false
```

3. 執行下列步驟、確保您要刪除的磁碟區中的FlexClone檔案和FlexClone LUN已啟用自動刪除：

   a. 使用命令自動刪除特定的 FlexClone 檔案或 FlexClone LUN `volume file clone autodelete` 。如"指令參考資料ONTAP"需詳細 `volume file clone autodelete`資訊，請參閱。

      您可以使用強制自動刪除特定的 FlexClone 檔案或 FlexClone LUN `volume file clone autodelete` 命令 `-force` 參數。

      下列範例顯示已啟用磁碟區vol1中所含的FlexClone LUN lun1_clone自動刪除：

      ```
      cluster1::> volume file clone autodelete -vserver vs1 -clone-path
      /vol/vol1/lun1_clone -enabled true
      ```

      您可以在建立FlexClone檔案和FlexClone LUN時啟用自動刪除功能。

   b. 使用命令確認已啟用 FlexClone 檔案或 FlexClone LUN 以自動刪除 `volume file clone show-autodelete`。如"指令參考資料ONTAP"需詳細 `volume file clone show-autodelete`資訊，請參閱。

      下列範例顯示已啟用FlexClone LUN lun1_clone以自動刪除：

      ```
      cluster1::> volume file clone show-autodelete -vserver vs1 -clone
      -path vol/vol1/lun1_clone
      Vserver Name: vs1
      Clone Path: vol/vol1/lun1_clone
      **Autodelete Enabled: true**
      ```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

如果您將FlexVol 某個實體磁碟區設定為自動刪除FlexClone檔案和FlexClone LUN、則任何符合您指定條件的實體複本都可能會被刪除。如果您有想保留的特定FlexClone檔案或FlexClone LUN、您可以將其排除在自動FlexClone刪除程序之外。

開始之前

必須安裝FlexClone授權。本授權隨附於"ONTAP One"。

關於這項工作

當您建立FlexClone檔案或FlexClone LUN時、預設會停用該實體複本的自動刪除設定。當您設定FlexVol 一個自動刪除磁碟區來自動刪除複本、以回收磁碟區上的空間時、會保留已停用自動刪除的FlexClone檔案和FlexClone LUN。

> 如果您設定 `commitment` 將磁碟區的層級調整為 `try` 或 `disrupt`，您可以停用這些複本的自動刪除功能，以個別保留特定的 FlexClone 檔案或 FlexClone LUN 。不過、如果您設定 `commitment` 將磁碟區的層級調整為 `destroy` 而銷毀清單則包含在內 `lun_clone,file_clone`、磁碟區設定會覆寫複本設定、而且無論複本的自動刪除設定為何、都可以刪除所有 FlexClone 檔案和 FlexClone LUN 。

步驟

1. 防止使用自動刪除特定的 FlexClone 檔案或 FlexClone LUN `volume file clone autodelete` 命令。

   以下範例說明如何停用vol1中所含的FlexClone LUN lun1_clone自動刪除：

   ```
   cluster1::> volume file clone autodelete -vserver vs1 -volume vol1
   -clone-path lun1_clone -enable false
   ```

   無法自動刪除已停用自動刪除的FlexClone檔案或FlexClone LUN、以回收磁碟區上的空間。

2. 使用確認已停用 FlexClone 檔案或 FlexClone LUN 的自動刪除功能 `volume file clone show-autodelete` 命令。

   以下範例顯示FlexClone LUN lun1_clone的自動刪除為假：

   ```
   cluster1::> volume file clone show-autodelete -vserver vs1 -clone-path
   vol/vol1/lun1_clone
                                                                  Vserver
   Name: vs1
                                                                  Clone Path:
   vol/vol1/lun1_clone
                                                                  Autodelete
   Enabled: false
   ```

當用戶端不使用 NetApp Manageability SDK 來刪除 FlexClone 檔案時、您可以使用 `volume file clone deletion` 命令可更快地從 FlexVol 磁碟區刪除 FlexClone 檔案。FlexClone檔案的副檔名和最小大小可用來加快刪除速度。

您可以使用 `volume file clone deletion` 用於指定卷中 FlexClone 文件所支持的擴展名列表和最小大小要求的命令。較快的刪除方法僅用於符合需求的FlexClone檔案。對於不符合需求的FlexClone檔案、會使用較慢的刪除方法。

當用戶端使用NetApp Manageability SDK從磁碟區刪除FlexClone檔案和FlexClone LUN時、由於一律使用較快的刪除方法、因此不會套用擴充和大小需求。

至...	使用此命令...
將副檔名新增至支援的Volume副檔名清單	`volume file clone deletion add-extension`
使用更快的刪除方法、變更可從磁碟區刪除的FlexClone檔案最小大小	`volume file clone deletion modify`
從支援的Volume擴充清單中移除副檔名	`volume file clone deletion remove-extension`
檢視支援的副檔名清單、以及用戶端可以使用更快的刪除方法從磁碟區刪除的FlexClone檔案大小下限	`volume file clone deletion show`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "刪除 Volume 檔案複製"

使用**qtree**來分割**FlexVol** 您的等量磁碟區

qtree 與 **ONTAP FlexVol volume** 分割

qtree 可讓您將 FlexVol 磁碟區分割成可個別管理的較小區段。qtree 啟用的磁碟區分割功能可在依專案，使用者或群組管理儲存時，提供更精細的控制等級。您可以使用 qtree 來更有效地管理配額，安全樣式和 CIFS oplocks 。

ONTAP 會為每個名為 **qtree0** 的磁碟區建立預設 qtree 。如果您沒有將資料放在特定 qtree 中，則資料會放在 qtree0 中。

一般限制

在正式作業環境中使用 qtree 之前，您應該瞭解 qtree 的限制。此外，使用延伸 qtree 效能監控功能時，請檢閱[營運與限制]。

- qtree 名稱不得超過 64 個字元。
- qtree 名稱中使用的某些特殊字元，例如逗號和空格，可能會導致其他 ONTAP 功能發生問題，因此應避免使用。
- 您無法在不同的 qtree 之間移動目錄。只能在qtree之間移動檔案。
- 如果您在相同FlexVol 的SCVMM或SCVMM集區上建立qtree層級和Volume層級的共用、qtree就會在FlexVol該共享區上顯示為目錄。您應小心避免意外刪除這些檔案。

用於管理和設定**qtree**的命令

您可以使用 ONTAP CLI 管理和設定 qtree 。根據您要執行的操作，您應該使用下列命令來管理 qtree 。

此命令 `volume rehost`可能會導致針對同一個磁碟區的其他並行管理作業失敗。

如果您想要…	使用此命令…
建立qtree	`volume qtree create`
顯示已篩選的qtree清單	`volume qtree show`
刪除qtree	`volume qtree delete` 除非 qtree 為空或使用旗標，否則此命令將會失敗 `-force true`。
修改qtree的UNIX權限	`volume qtree modify -unix-permissions`
修改qtree的CIFS oplocks設定	`volume qtree oplocks`
修改qtree的安全性設定	`volume qtree security`
重新命名qtree	`volume qtree rename`
顯示qtree的統計資料	`volume qtree statistics`
重設qtree的統計資料	`volume qtree statistics -reset`

延伸 **qtree** 效能監控

從 ONTAP 9 。 16.1 開始，您可以使用 ONTAP REST API 來存取延伸的 qtree 監控功能，包括延遲指標和歷史統計資料。

ONTAP REST API 包含與 qtree 相關的數個端點。在 ONTAP 9 0.16.1 之前，客戶可以存取 qtree 的即時統計資料，包括每秒 IO 作業（ IOP ），以及讀取，寫入和其他作業的處理量。

從 ONTAP 9 開始提供的延伸 qtree 效能監控功能可讓您監控 NFSv3 ， NFSv4.0 ， NFSv4.1 ， NFSv4.2 ，

pNFS （技術上是 NFSv4.1 和 NFSv4.2 的一部分）和 CIFS 的即時延遲統計資料，以及 IOPs 和處理量。它也會收集和歸檔統計資料，以便檢視歷史效能資料。

這項延伸監控功能可讓儲存管理員更深入瞭解系統效能。您可以使用此資料來識別高使用率的 qtree ，潛在瓶頸和其他領域，以改善服務品質。能夠分析這些指標，包括較長時間的趨勢，讓您做出更明智的資料導向決策。

營運與限制

在正式作業環境中使用延伸 qtree 效能監控功能之前，您應該考量幾個營運特性，包括限制。

需要重新掛載

啟用 qtree 延伸監控之後，您需要重新掛載受影響的磁碟區才能啟動此功能。

統計資料的可用性

啟用延伸效能監控之後，統計資料就無法立即使用。這包括 IOPS ，處理量和延遲統計資料。最多可能需要五分鐘的時間，才能顯示 qtree 的資料。

每個叢集的 **qtree**

您可以在 ONTAP 叢集中啟用最多 50,000 個 qtree 的延伸效能監控。

使用 **ONTAP REST API** 存取延伸計量

從 ONTAP 9 。 16.1 開始，您可以透過 ONTAP REST API 存取延伸 qtree 效能監控功能。基本功能分為幾類，如下所述。

啟用和停用延伸效能監控

您可以存取端點 `/api/storage/qtrees`的內容 `ext_performance_monitoring.enabled`，以啟用或停用延伸監控功能。根據您是要建立新的 qtree ，還是要設定現有的 qtree ，可以使用 POST 和修補方法。

擷取全域監控指標和設定

端點已新增數個新的全域內容 `/api/storage/qtrees`。您可以使用「取得」方法擷取這些欄位。

擷取特定 **qtree** 的度量

您可以使用端點的 Get 方法 `/api/storage/qtrees/{volume.uuid}/{id}/metrics`，擷取特定 qtree 的新統計資料和度量內容，如特定 Volume 所定義。

升級與還原

如果您在 ONTAP 9 。 16.1 中啟用此功能，則可在不受限制的情況下升級至後續的 ONTAP 版本。不過，有兩種情況需要考量。

升級至 **9.16.1** ，並處理混合版本叢集

除非叢集的有效叢集版本（ ECV ）為 9.16.1 ，否則無法使用擴充效能監控功能（也就是 `ext_performance_monitoring.enabled`無法設定為 `true`）。

從 **9.16.1** 恢復

如果任何 qtree 的屬性設為 `true`，則 `ext_performance_monitoring.enabled`不允許從 `9.16.1` 回復為 `9.15.1` 。還原作業遭到封鎖。最佳實務做法是在還原至較早的 `ONTAP` 版本之前，先將所有 `qtree` 設 `ext_performance_monitoring.enabled`為 `false`。

深入瞭解

從 ONTAP 自動化文件中深入瞭解 ONTAP REST API ，包括 "ONTAP REST API 的新功能"。您還應該查看 ONTAP 自動化文檔，瞭解有關 ONTAP REST API的詳細信息 "qtree 端點"。

取得**qtree**交會路徑

您可以取得qtree的交會路徑或命名空間路徑來掛載個別qtree。CLI 命令顯示的 qtree 路徑 `qtree show -instance` 為格式 `/vol/<volume_name>/<qtree_name>`。不過、此路徑並未參照qtree的交會路徑或命名空間路徑。

如"指令參考資料ONTAP"需詳細 `qtree show`資訊，請參閱。

關於這項工作

您需要知道磁碟區的交會路徑、才能取得qtree的交會路徑或命名空間路徑。

步驟

1. 使用 `vserver volume junction-path` 取得 Volume 交會路徑的命令。

   下列範例顯示位於名為vs0的儲存虛擬機器（SVM）上、名為vol1的磁碟區交會路徑：

   ```
   cluster1::> volume show -volume vol1 -vserver vs0 -fields junction-path

   ------- ------ -------------

   vs0 vol1 /vol1
   ```

   從上述輸出中、磁碟區的交會路徑為 `/vol1`。由於 qtree 永遠根植於磁碟區、因此 qtree 的交會路徑或命名空間路徑將會是 `/vol1/qtree1`。

如"指令參考資料ONTAP"需詳細 `vserver volume junction-path`資訊，請參閱。

目錄到 **qtree** 的轉換

將目錄轉換成**qtree**

如果您想要轉換成 qtree 的 FlexVol volume 根目錄、則需要使用用戶端應用程式、將目錄中包含的資料移轉至名稱相同的新 qtree 。

關於這項工作

您將目錄轉換成qtree的步驟取決於您使用的用戶端。下列程序概述您需要完成的一般工作。

開始之前

如果目錄與現有的CIFS共用相關聯、則無法刪除該目錄。

步驟

1. 將要建立的目錄重新命名為qtree。

2. 使用原始目錄名稱建立新的qtree。
3. 使用用戶端應用程式將目錄內容移至新的qtree。
4. 刪除NOW清空目錄。

使用**Windows**用戶端將目錄轉換成**qtree**

若要使用 Windows 用戶端將目錄轉換為 qtree 、請重新命名目錄、在儲存系統上建立 qtree 、然後將目錄內容移至 qtree 。

關於這項工作

您必須使用Windows檔案總管來執行此程序。您無法使用Windows命令列介面或DOS提示字元環境。

步驟

1. 開啟Windows檔案總管。
2. 按一下您要變更之目錄的資料夾表示法。

   目錄必須位於其包含Volume的根目錄。

3. 從*檔案*功能表中、選取*重新命名*、為此目錄指定不同的名稱。
4. 在儲存系統上，使用 `volume qtree create`命令建立具有目錄原始名稱的新 qtree 。如"指令參考資料ONTAP"需詳細 `volume qtree create`資訊，請參閱。
5. 在Windows檔案總管中、開啟重新命名的目錄資料夾、然後選取其中的檔案。
6. 將這些檔案拖曳到新qtree的資料夾表示法中。

   您要移動的資料夾中包含的子資料夾越多、移動作業所需時間就越長。

7. 從*檔案*功能表中、選取*刪除*以刪除重新命名的現在為空的目錄資料夾。

使用**UNIX**用戶端將目錄轉換成**qtree**

若要在UNIX中將目錄轉換成qtree、您可以重新命名目錄、在儲存系統上建立qtree、然後將目錄內容移至qtree。

步驟

1. 開啟UNIX用戶端視窗。
2. 使用 `mv` 命令以重新命名目錄。

```
client: mv /n/user1/vol1/dir1 /n/user1/vol1/olddir
```

3. 在儲存系統中、使用 `volume qtree create` 建立具有原始名稱的 qtree 的命令。

```
system1: volume qtree create /n/user1/vol1/dir1
```

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

4. 從用戶端使用 `mv` 命令將舊目錄的內容移至 qtree 。

   目錄中包含的子目錄越多、移動作業所需時間就越長。

```
client: mv /n/user1/vol1/olddir/* /n/user1/vol1/dir1
```

5. 使用 `rmdir` 刪除舊的、現在為空的目錄的命令。

```
client: rmdir /n/user1/vol1/olddir
```

完成後

視 UNIX 用戶端實作的方式而定 `mv` 命令、檔案擁有權和權限可能無法保留。如果發生這種情況、請將檔案擁有者和權限更新至先前的值。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

磁碟區的邏輯空間報告與強制

磁碟區的邏輯空間報告與強制執行總覽

從ONTAP 功能9.4開始、您可以允許使用者顯示磁碟區中使用的邏輯空間、以及剩餘的儲存空間量。從 ONTAP 9.5 開始、您可以限制使用者使用的邏輯空間量。

邏輯空間報告和強制功能預設為停用。

下列磁碟區類型支援邏輯空間報告和強制實施。

Volume類型	是否支援空間報告？	是否支援空間強制？
資料量FlexVol	是、從ONTAP NetApp 9.4開始	是的、從ONTAP SES9.5開始
SnapMirror目的地磁碟區	是的、從ONTAP 功能性的問題9.8開始	是、從 ONTAP 9.13.1 開始
資料量FlexGroup	是的、從ONTAP 版本的問題9.9.1開始	是的、從ONTAP 版本的問題9.9.1開始
資料量FlexCache	原始伺服器設定是在快取中使用	不適用

邏輯空間強制

強制執行邏輯空間可確保在磁碟區已滿或即將滿時通知使用者。當您在ONTAP 更新版本的

支援中啟用邏輯空間時、ONTAP 流通量區會計算磁碟區中邏輯使用的區塊、以判斷該磁碟區中仍有多少空間可用。如果磁碟區中沒有可用空間、系統會傳回ENOSPC（空間不足）錯誤訊息。

邏輯空間強制會傳回三種警示類型、通知您磁碟區中的可用空間：

- `Monitor.vol.full.inc.sav`：使用卷中 98% 的邏輯空間時會觸發此警報。
- `Monitor.vol.nearFull.inc.sav`：使用捲中 95% 的邏輯空間時會觸發此警示。
- `Vol.log.overalloc.inc.sav`：當磁碟區中使用的邏輯空間大於磁碟區的總大小時、就會觸發此警示。

  此警示會告訴您、新增至磁碟區大小可能無法建立可用空間、因為過度配置的邏輯區塊已佔用該空間。

總計（邏輯空間）應等於已配置空間，但不包括執行邏輯空間的磁碟區快照保留空間。

如需更多資訊、請參閱 "設定磁碟區、以便在磁碟區已滿時自動提供更多空間"。

邏輯空間報告

當您在磁碟區上啟用邏輯空間報告時、除了磁碟區的總空間之外、系統還能顯示已使用的邏輯空間量和可用空間量。此外、Linux和Windows用戶端系統上的使用者可以看到已用邏輯和可用空間、而非實體已用空間和實體可用空間。

定義：

- 實體空間是指磁碟區中可用或使用的實體儲存區塊。
- 邏輯空間是指磁碟區中的可用空間。
- 使用的邏輯空間是已使用的實體空間、加上已設定的儲存效率功能（例如重複資料刪除和壓縮）所節省的成本。

從推出支援功能的支援功能支援從功能9.5開始ONTAP 、您就能運用空間報告功能來執行邏輯空間。

啟用時、邏輯空間報告會在中顯示下列參數 `volume show` 命令：

參數	意義
`-logical-used`	僅顯示具有指定邏輯已用大小的磁碟區或磁碟區的相關資訊。此值包括儲存效率功能所節省的所有空間、以及實際使用的空間。這不包括快照保留，但會考慮快照溢漏。
`-logical-used-by-afs`	僅顯示使用中檔案系統所使用之具有指定邏輯大小的磁碟區或磁碟區的相關資訊。此值與超出快照保留量的快照溢漏量值不同`-logical-used`。
`-logical-available`	如果只啟用邏輯空間報告、則只會顯示實體可用空間。啟用空間報告和強制時、會顯示目前可用空間量、並將儲存效率功能所節省的空間視為使用中空間。這不包括快照保留。

參數	意義
`-logical-used -percent`	顯示目前值的百分比 `-logical-used`，以及不含磁碟區快照保留的資源配置大小。 此值可能大於 100% ，因為此 `-logical-used-by-afs`值包括在 Volume 中節省的效率。 `-logical-used-by-afs`磁碟區的值不包括快照溢出作為使用空間。 `-physical-used`Volume 的價值包括使用空間的 Snapshot 溢漏。
`-used`	顯示使用者資料和檔案系統中繼資料佔用的空間量。它與空間的差異 `physical-used`在於保留給未來寫入的空間總和，以及根據集合式儲存效率所節省的空間。其中包括快照溢出（快照超過快照保留空間的空間量）。它不包括快照保留。

在CLI中啟用邏輯空間報告功能、也可在System Manager中顯示「邏輯已用空間」（%）和「邏輯空間」值

用戶端系統會在下列系統顯示器上看到顯示為「已使用」空間的邏輯空間：

- Linux系統上的* df*輸出
- Windows系統上使用Windows檔案總管的內容下的空間詳細資料。

如果啟用邏輯空間報告而不強制使用邏輯空間、則顯示在用戶端系統上的總計可能會高於已配置空間。

啟用邏輯空間報告與強制

從功能區9.4開始ONTAP 、您可以啟用邏輯空間報告功能。從9.5開始、您可以啟用邏輯空間強制、或同時執行報告和強制。

關於這項工作

除了在個別磁碟區層級啟用邏輯空間報告和強制、您也可以在SVM層級為每個支援該功能的磁碟區啟用這些功能。如果您為整個SVM啟用邏輯空間功能、也可以針對個別Volume停用這些功能。

從 ONTAP 9.8 開始、如果您在 SnapMirror 來源磁碟區上啟用邏輯空間報告功能、則傳輸後會自動在目的地磁碟區上啟用。

從 ONTAP 9.13.1 開始、如果在 SnapMirror 來源磁碟區上啟用強制選項、目的地將會報告邏輯空間使用量、並遵守其實施規定、進而實現更好的容量規劃。

如果您執行的 ONTAP 版本早於 ONTAP 9.13.1 、您應該瞭解、雖然強制設定會傳輸至 SnapMirror 目的地 Volume 、但目的地 Volume 不支援強制。因此、目的地會報告邏輯空間使用量、但不會遵守其執行規定。

深入瞭解 "ONTAP 版本支援邏輯空間報告"。

步驟

啟用下列一或多項：

- 啟用磁碟區的邏輯空間報告：

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true
```

- 啟用磁碟區的邏輯空間強制：

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-enforcement-logical true
```

- 為磁碟區同時提供邏輯空間報告與強制：

```
volume modify -vserver svm_name -volume volume_name -size volume_size -is
-space-reporting-logical true -is-space-enforcement-logical true
```

- 啟用新SVM的邏輯空間報告或強制：

```
vserver create -vserver _svm_name_ -rootvolume root-_volume_name_ -rootvolume
-security-style unix -data-services {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

- 啟用現有SVM的邏輯空間報告或強制：

```
vserver modify -vserver _svm_name_ {desired-data-services} [-is-space-
reporting-logical true] [-is-space-enforcement-logical true]
```

管理 **SVM** 容量限制

從 ONTAP 9.13.1 開始、您可以設定儲存 VM （ SVM ）的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。

關於這項工作

SVM 上的容量是以 FlexVols 、 FlexGroup Volume 、 FlexClones 、 FlexCache Volume 的總和來計算。即使磁碟區在刪除後受到限制、離線或位於恢復佇列中、這些磁碟區也會影響容量計算。如果您已將 Volume 設定為自動擴充、則會根據 SVM 大小計算 Volume 的最大自動調整大小值；如果沒有自動增加、則會計算出 Volume 的實際大小。

下表說明如何進行 `autosize-mode` 參數會影響容量計算。

`autosize-mode off`	Size 參數將用於計算
`autosize-mode grow`	◦ `max-autosize` 參數將用於計算
`autosize-mode grow-shrink`	◦ `max-autosize` 參數將用於計算

開始之前

- 您必須是叢集管理員才能設定 SVM 限制。
- 從 ONTAP 9.16.1 開始，可針對包含資料保護磁碟區的 SVM 設定儲存限制，包括下列資料保護類型：
  - 非同步災難恢復中的 FlexVol 磁碟區，無需串聯
  - 同步災難恢復中的 FlexVol Volume （同步和嚴格同步原則）
  - "還原"

- 下列組態不支援 SVM 的儲存限制：
  - SnapMirror 資料保險箱關聯性
  - SnapMirror 主動同步
  - 資料量FlexGroup
  - 一致性群組
  - SVM DR
  - 串聯
  - MetroCluster
- 從ONTAP 9.16.1 開始，當您建立負載共享鏡像關係時，目標 SVM 無法啟用儲存限制。
- 當您移轉 SVM 時、來源 SVM 無法啟用儲存限制。若要完成移轉作業、請停用來源的儲存限制、然後完成移轉。
- SVM 容量與不同 配額。配額不得超過最大大小。
- 當 SVM 上的其他作業正在進行中時、您無法設定儲存限制。使用 `job show vserver <svm_name>`命令查看現有工作。當任何工作完成時、請再次嘗試執行命令。如"指令參考資料ONTAP"需詳細 `job show`資訊，請參閱。

容量影響

當您達到容量上限時、下列作業將會失敗：

- 建立 LUN 、命名空間或磁碟區
- 複製 LUN 、命名空間或磁碟區
- 修改 LUN 、命名空間或磁碟區
- 增加 LUN 、命名空間或磁碟區的大小
- 擴充 LUN 、命名空間或磁碟區
- 重新裝載 LUN 、命名空間或磁碟區

設定新 **SVM** 的容量限制

系統管理員

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。
2. 選取 以建立 SVM 。
3. 命名 SVM 並選取 * 存取通訊協定 * 。
4. 在 * 儲存 VM 設定 * 下、選取 * 啟用最大容量限制 * 。

   為 SVM 提供最大容量。

5. 選擇*保存*。

CLI

步驟

1. 建立 SVM 。若要設定儲存限制、請提供 `storage-limit` 價值。若要設定儲存限制的臨界值警示、請提供的百分比值 `-storage-limit-threshold-alert`。

   ```
   vserver create -vserver <vserver_name> -aggregate <aggregate_name>
   -rootvolume <root_volume_name> -rootvolume-security-style
   {unix|ntfs|mixed} -storage-limit <value> [GiB|TIB] -storage-limit
   -threshold-alert <percentage> [-ipspace <IPspace_name>] [-language
   <language>] [-snapshot-policy <snapshot_policy_name>] [-quota-policy
   <quota_policy_name>] [-comment <comment>]
   ```

   如果您未提供臨界值、預設會在 SVM 容量為 90% 時觸發警示。若要停用臨界值警示、請提供零值。

2. 確認 SVM 已成功建立：

   ```
   vserver show -vserver <vserver_name>
   ```

3. 如果您想要停用儲存限制，請將 SVM 的參數設 `-storage-limit`為零：

   ```
   vserver modify -vserver <vserver_name> -storage-limit 0
   ```

設定或修改現有 **SVM** 的容量限制

您可以在現有的 SVM 上設定容量限制和臨界值警示、或停用容量限制。

設定容量上限後、您就無法將限制修改為小於目前分配容量的值。

系統管理員

步驟

1. 選取 * 儲存 * > * 儲存 VMS* 。
2. 選取您要修改的 SVM 。在 SVM 名稱旁邊、選取 ⋮ * 編輯 * 。
3. 若要啟用容量限制、請選取 * 啟用容量限制 * 旁的方塊。輸入 * 最大容量 * 的值、以及 * 警示臨界值 * 的百分比值。

   如果您想要停用容量限制、請取消勾選 * 啟用容量限制 * 旁的方塊。

4. 選擇*保存*。

CLI

步驟

1. 在裝載 SVM 的叢集上、發出 `vserver modify` 命令。提供的數值 `-storage-limit` 以及百分比值 `-storage-limit-threshold-alert`。

```
vserver modify -vserver <vserver_name> -storage-limit <value>
[GiB|TIB] -storage-limit-threshold-alert <percentage>
```

   如果您未提供臨界值，則會有 90% 容量的預設警示。若要停用臨界值警示、請提供零值。

2. 如果您要停用儲存限制，請將 SVM 的設 `-storage-limit`為零：

```
vserver modify -vserver <vserver_name> -storage-limit 0
```

達到容量限制

當您達到最大容量或警示臨界值時、可以參閱 `vserver.storage.threshold` EMS 訊息或使用 System Manager 中的 * Insights * 頁面來瞭解可能的行動。可能的解決方案包括：

- 編輯 SVM 最大容量限制
- 清除磁碟區恢復佇列以釋放空間
- 刪除快照以提供磁碟區空間

相關資訊

- System Manager中的容量測量
- 在 System Manager 中監控叢集，階層和 SVM 容量
- "Vserver建立"
- "Vserver展示"
- "Vserver修改"

使用配額來限制或追蹤資源使用量

配額程序總覽

瞭解配額、配額規則和配額原則

配額是在FlexVol 特定於功能區的配額規則中定義。這些配額規則會以儲存虛擬機器（SVM）的配額原則一起收集、並在 SVM 上的每個磁碟區上啟動。

配額規則一律專屬於某個磁碟區。在配額規則中定義的磁碟區上啟動配額之前、配額規則才會生效。

配額原則是SVM所有磁碟區的配額規則集合。配額原則不會在SVM之間共用。SVM最多可有五個配額原則、讓您擁有配額原則的備份複本。系統會在任何指定時間將一個配額原則指派給SVM。當您初始化或調整磁碟區上的配額大小時、即會啟動目前指派給SVM的配額原則中的配額規則。

配額是ONTAP 指實際執行的限制、或ONTAP 是執行的實際追蹤。配額規則一律會產生至少一個配額、並可能導致許多額外的衍生配額。強制執行配額的完整清單只能在配額報告中看到。

啟動是從ONTAP 指派配額原則中目前配額規則集觸發以建立強制配額的程序。每個磁碟區都會啟動。第一次啟動磁碟區上的配額稱為初始化。後續啟動稱為重新初始化或調整大小、視變更範圍而定。

使用配額的好處

您可以使用配額來管理和監控 FlexVol Volume 的資源使用量。

定義配額有幾個好處。您可以使用預設、明確、衍生及追蹤配額、以最有效率的方式管理磁碟使用量。

限制資源使用量

您可以限制使用者或群組所使用或包含在 qtree 中的磁碟空間量或檔案數量。

追蹤資源使用率

可以追蹤使用者、群組或 qtree 所使用的磁碟空間量或檔案數量、而不需設定限制。

通知使用者

當資源使用量達到特定層級時、就會產生通知。當使用者的磁碟或檔案使用量過高時、這會發出警示。

配額程序

配額提供一種方法來限制或追蹤使用者、群組或qtree所使用的磁碟空間和檔案數目。配額會套用至特定FlexVol 的流通量或qtree。

配額可以是軟的或硬的。軟配額會導致ONTAP 當超過指定的限制時、不再傳送通知、硬配額則會在超過指定的限制時、防止寫入作業成功。

當收到使用者或使用者群組的寫入要求時、它會檢查該磁碟區上的配額是否已針對使用者或使用者群組啟用、並決定下列事項：ONTAP FlexVol

- 是否會達到硬限制

  如果是、當達到硬限制並傳送硬配額通知時、寫入作業將會失敗。

- 是否會違反軟限制

  如果是、則當軟體限制超出且軟體配額通知已傳送時、寫入作業會成功。

- 寫入作業是否不會超過軟限制

  如果是、寫入作業會成功、而且不會傳送通知。

硬、軟和臨界值配額之間的差異

硬額度會在軟額度觸發通知時、防止作業。

硬額度會對系統資源造成硬限制、導致超出限制的任何作業都會失敗。下列設定會建立硬額度：

- 磁碟限制參數
- 檔案限制參數

軟性配額會在資源使用量達到特定層級時傳送警告訊息、但不會影響資料存取作業、因此您可以在超出配額之前採取適當的行動。下列設定會建立軟性配額：

- 磁碟限制參數臨界值
- Soft Disk限制參數
- Soft Files限制參數

臨界值和軟式磁碟配額可讓系統管理員收到一個以上的配額通知。一般而言、系統管理員會將「磁碟限制臨界值」設定為僅稍微小於「磁碟限制」的值、以便在寫入開始失敗之前、臨界值會提供「最終警告」。

關於配額通知

配額通知是傳送至事件管理系統（EMS）、也設定為SNMP設陷的訊息。

系統會針對下列事件傳送通知：

- 達到硬配額、也就是說、試圖超過配額
- 已超過軟配額
- 不再超過軟配額

臨界值與其他軟性配額稍有不同。臨界值只會在超出時觸發通知、而不會在不再超過通知時觸發通知。

硬配額通知可透過Volume配額修改命令加以設定。您可以完全關閉它們、也可以變更它們的頻率、例如、以防止傳送多餘的訊息。

軟配額通知無法設定、因為它們不太可能產生重複的訊息、而且唯一的目的是通知。

下表列出配額傳送至EMS系統的事件：

發生這種情況時...	此事件會傳送至**EMS** ...
樹狀結構配額已達到硬限制	`wafl.quota.qtree.exceeded`
磁碟區上的使用者配額已達到硬限制	`wafl.quota.user.exceeded` （適用於 UNIX 使用者） `wafl.quota.user.exceeded.win` （適用於 Windows 使用者）
qtree上的使用者配額已達到硬限制	`wafl.quota.userQtree.exceeded` （適用於 UNIX 使用者） `wafl.quota.userQtree.exceeded.win` （適用於 Windows 使用者）
磁碟區上的群組配額已達到硬限制	`wafl.quota.group.exceeded`
qtree上的群組配額已達到硬限制	`wafl.quota.groupQtree.exceeded`
超過軟限制、包括臨界值	`quota.softlimit.exceeded`
不再超過軟限制	`quota.softlimit.normal`

下表列出配額產生的SNMP設陷：

發生這種情況時...	此**SNMP**設陷已傳送...
已達到硬限制	quotaExceed
超過軟限制、包括臨界值	QuotaoExceededed.和softQuotaExceed
不再超過軟限制	QuotaNormal和softQuotaNormal

通知包含qtree ID編號、而非qtree名稱。您可以使用將 qtree 名稱與 ID 編號建立關聯 `volume qtree show -id` 命令。

配額目標和類型

每個配額都有特定類型。配額目標衍生自類型、並指定套用配額限制的使用者、群組或 qtree 。

下表列出配額目標、每個配額目標關聯的配額類型、以及每個配額目標的呈現方式。

配額目標	配額類型	目標的呈現方式	附註

使用者	使用者配額	UNIX使用者名稱UNIX UID 其UID與使用者相符的檔案或目錄 Windows 2000之前版本的Windows使用者名稱 Windows SID 具有使用者SID所擁有之ACL的檔案或目錄	使用者配額可套用至特定磁碟區或qtree。
群組	群組配額	UNIX群組名稱UNIX Gid 一個檔案或目錄、其中的gid與群組相符	群組配額可套用至特定磁碟區或qtree。 不適用以Windows ID為基礎的群組配額。ONTAP
qtree	樹狀結構配額	qtree名稱	樹狀結構配額會套用至特定的磁碟區、不會影響其他磁碟區中的qtree。
""	使用者配額 樹狀結構配額	雙引號（""）	配額目標為「」表示預設配額_。對於預設配額、配額類型取決於類型欄位的值。

特殊配額

預設配額的運作方式

您可以使用預設配額、將配額套用至指定配額類型的所有執行個體。例如、預設的使用者配額會影響系統上指定FlexVol 的某個目標區或qtree的所有使用者。此外、預設配額可讓您輕鬆修改配額。

您可以使用預設配額、自動將限制套用至一組大型配額目標、而不需要為每個目標建立個別配額。例如、如果您想要將大多數使用者的磁碟空間限制為10 GB、您可以指定預設的10 GB磁碟空間使用者配額、而非為每個使用者建立配額。如果您有特定使用者想要套用不同的限制、您可以為這些使用者建立明確的配額。（顯式配額-具有特定目標或目標列表的配額-覆蓋缺省配額。）

此外、預設配額可讓您在想要使配額變更生效時、使用調整大小、而非重新初始化。例如、如果您將明確的使用者配額新增至已有預設使用者配額的磁碟區、您可以調整大小來啟動新的配額。

預設配額可套用至所有三種配額目標類型（使用者、群組和qtree）。

預設配額不一定具有指定的限制、預設配額可以是追蹤配額。

根據內容而定、配額會以空白字串（""）或星號（*）表示：

- 當您使用建立配額時 `volume quota policy rule create` 命令、設定 `-target` 空字串的參數（""

）會建立預設配額。

如"指令參考資料ONTAP"需詳細 `volume quota policy rule create`資訊，請參閱。

- 在中 `volume quota policy rule create` 命令 `-qtree` 參數指定配額規則套用到的 qtree 名稱。此參數不適用於樹狀結構類型規則。對於磁碟區層級的使用者或群組類型規則、此參數應包含「」。
- 在的輸出中 `volume quota policy rule show` 命令時、會出現預設配額、並以空白字串（""）作為目標。

  如"指令參考資料ONTAP"需詳細 `volume quota policy rule show`資訊，請參閱。

- 在的輸出中 `volume quota report` 命令時、預設配額會以星號（*）顯示為 ID 和 Quota 說明符。

  如"指令參考資料ONTAP"需詳細 `volume quota report`資訊，請參閱。

預設使用者配額範例

以下配額規則使用預設的使用者配額、針對 vol1 對每位使用者套用 50 MB 的限制：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                          User          Disk     Disk    Files    Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""      off           50MB        -       -        -
-
```

如果系統上的任何使用者輸入命令、導致該使用者的資料在vol1中佔用超過50 MB的資料（例如、從編輯器寫入檔案）、則命令會失敗。

如何使用明確配額

您可以使用明確配額來指定特定配額目標的配額、或覆寫特定目標的預設配額。

明確的配額會指定特定使用者、群組或qtree的限制。明確的配額會取代相同目標的任何預設配額。

針對具有衍生使用者配額的使用者新增明確的使用者配額時、您必須使用與預設使用者配額相同的使用者對應設定。否則、當您調整配額大小時、明確的使用者配額會被拒絕、因為它被視為新的配額。

明確配額只會影響相同層級（Volume或qtree）的預設配額。例如、qtree的明確使用者配額不會影響包含qtree之磁碟區的預設使用者配額。不過、qtree的明確使用者配額會覆寫（取代定義的限制）該qtree的預設使用者配

額。

明確配額範例

下列配額規則定義預設的使用者配額、將 vol1 中的所有使用者限制在 50MB 空間。不過、由於明確的配額（以粗體顯示）、因此允許一個使用者 jsmith 擁有 80MB 的空間：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "" -qtree "" -disk-limit 50m

cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith" -qtree "" -disk-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           50MB        -       -        -
-
user   jsmith    ""      off           80MB        -       -        -
-
```

以下配額規則將指定的使用者（以四個 ID 表示）限制為 550MB 磁碟空間、以及 vol1 磁碟區中的 10,000 個檔案：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "
jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544" -qtree "" -disk
-limit 550m -file-limit 10000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "jsmith,corp\jsmith,engineering\john smith,S-1-5-32-544"
                 ""      off         550MB        -   10000        -
-
```

下列配額規則將 eng1 群組限制為 150MB 磁碟空間、且 proj1 qtree 中的檔案數量不限：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type group -target "eng1" -qtree "proj1" -disk-limit
150m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                  Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
group  eng1      proj1   off         150MB        -       -        -
-
```

以下配額規則將 vol2 磁碟區中的 proj1 qtree 限制為 750MB 磁碟空間和 75,000 個檔案：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol2
-policy-name default -type tree -target "proj1" -disk-limit 750m -file
-limit 75000

cluster1::> volume quota policy rule show -vserver vs0 -volume vol2

Vserver: vs0               Policy: default           Volume: vol2
                                                  Soft              Soft
                          User          Disk      Disk    Files     Files
Type    Target    Qtree   Mapping      Limit     Limit    Limit     Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree    proj1     ""      -           750MB        -    75000         -
-
```

導出配額的運作方式

由於預設配額而強制執行的配額、而非明確配額（具有特定目標的配額）、稱為_衍生配額_。

衍生配額的數量和位置取決於配額類型：

- 磁碟區上的預設樹狀目錄配額會為磁碟區上的每個 qtree 建立衍生的預設樹狀目錄配額。
- 預設的使用者或群組配額會針對擁有相同層級（Volume或qtree）檔案的每個使用者或群組、建立衍生的使用者或群組配額。
- 磁碟區上的預設使用者或群組配額會在每個也有樹狀目錄配額的 qtree 上建立衍生的預設使用者或群組配額。

衍生配額的設定（包括限制和使用者對應）與對應預設配額的設定相同。例如、磁碟區上具有20-GB磁碟限制的預設樹狀結構配額、會在磁碟區中的qtree上建立具有20-GB磁碟限制的衍生樹狀結構配額。如果預設配額是追蹤配額（無限制）、則衍生配額也會追蹤配額。

若要查看衍生配額、您可以產生配額報告。在報告中、導出的使用者或群組配額會以空白或星號（*）的配額說明符號表示。不過，衍生的樹狀目錄配額卻有 Quota 說明符。若要識別衍生的樹狀目錄配額，您必須在具有相同限制的磁碟區上尋找預設的樹狀目錄配額。

明確配額會以下列方式與衍生配額互動：

- 如果相同目標已存在明確配額、則不會建立衍生配額。
- 如果在建立目標的明確配額時存在衍生配額、您可以調整大小來啟動明確配額、而不必執行完整配額初始化。

使用追蹤配額

追蹤配額會產生磁碟與檔案使用量報告、不會限制資源使用量。使用追蹤配額時、修改配額值的中斷程度較低、因為您可以調整配額的大小、而非關閉再重新開啟配額。

若要建立追蹤配額、請略過「磁碟限制」和「檔案限制」參數。這表示ONTAP 、不需設定任何限制、即可監控該目標（Volume或qtree）的磁碟和檔案使用量。的輸出會指出追蹤配額 `show` 命令和配額報告、並在所有限制中加上破折號（ "-" ）。當您使用系統管理員 UI 建立明確的配額（特定目標的配額）時、 ONTAP 會自動建立追蹤配額。使用 CLI 時、儲存管理員會在明確配額的基礎上建立追蹤配額。

您也可以指定_預設追蹤配額_、以套用至目標的所有執行個體。預設追蹤配額可讓您追蹤配額類型的所有執行個體（例如、所有qtree或所有使用者）的使用量。此外、當您想要使配額變更生效時、這些功能可讓您使用調整大小、而非重新初始化。

範例

追蹤規則的輸出會顯示 qtree 、使用者和群組的追蹤配額、如以下 Volume 層級追蹤規則範例所示：

```
Vserver: vs0              Policy: default             Volume: fv1

                                        Soft           Soft
                       User    Disk     Disk   Files   Files
Type   Target   Qtree  Mapping Limit   Limit  Limit   Limit   Threshold
------ -------- ------- ------- ------ ------ ------ ------ ---------
tree   ""       ""      -       -      -      -      -      -
user   ""       ""      off     -      -      -      -      -
group  ""       ""      -       -      -      -      -      -
```

配額的套用方式

瞭解如何套用配額、可讓您正確設定配額、並設定預期限制。

每當試圖在FlexVol 啟用配額的情況下建立檔案或將資料寫入到位於支援配額的文件中時、就會在作業開始之前檢查配額限制。如果作業超過磁碟限制或檔案限制、則會禁止此作業。

配額限制會依下列順序核取：

1. 該qtree的樹狀結構配額（如果檔案正在建立或寫入qtree0、則此檢查不相關）。
2. 擁有磁碟區上檔案之使用者的使用者配額
3. 擁有磁碟區上檔案之群組的群組配額
4. 在qtree上擁有檔案的使用者配額（如果檔案正在建立或寫入qtree0、則此檢查不相關）。
5. 在qtree上擁有檔案的群組配額（如果檔案正在建立或寫入qtree0、則此檢查不相關）。

上限最小的配額可能不是先超過的配額。例如、如果Volume vol1的使用者配額為100 GB、 Volume vol1中qtree Q2的使用者配額為20 GB、如果該使用者已在Volume vol1中寫入超過80 GB的資料（但在qtree Q2之外）、則磁碟區上限會先達到。

相關資訊

- "如何將配額套用至root使用者"
- "如何將配額套用至具有多個ID的使用者"

配額原則是FlexVol SVM所有的SVM等磁碟區的配額規則群組。指派配額原則時、您必須注意某些考量事項。

- SVM在任何指定時間都有一個指派的配額原則。建立SVM時、會建立空白配額原則並指派給SVM。除非在建立SVM時指定不同的名稱、否則此預設配額原則的名稱為「預設」。
- SVM最多可有五個配額原則。如果SVM有五個配額原則、則在刪除現有的配額原則之前、您無法為SVM建立新的配額原則。
- 當您需要建立配額規則或變更配額原則的配額規則時、可以選擇下列任一種方法：
  - 如果您使用指派給SVM的配額原則、則不需要將配額原則指派給SVM。
  - 如果您使用未指派的配額原則、然後將配額原則指派給SVM、則必須備份配額原則、以便在必要時還原為。

    例如、您可以複製指派的配額原則、變更複本、將複本指派給SVM、以及重新命名原始配額原則。
- 您可以重新命名配額原則、即使配額原則已指派給SVM。

配額如何搭配使用者和群組使用

配額如何與使用者和群組搭配運作的總覽

您可以將使用者或群組指定為配額的目標。定義配額時、需要考量幾個實作差異。

您需要注意的一些差異包括：

- 使用者或群組
- UNIX 或 Windows
- 特殊使用者和群組
- 包含多個 ID

根據您的環境、也有不同的方法可以指定使用者 ID 。

指定 **UNIX** 使用者的配額

您可以使用多種不同格式之一、指定 UNIX 使用者的配額。

指定 UNIX 使用者進行配額時可用的三種格式包括：

- 使用者名稱（例如 jsmith ）。

  如果UNIX使用者名稱包含反斜槓（\）或@符號、則無法使用該名稱來指定配額。這是因為ONTAP 包含這些字元的名稱會被視為Windows名稱。
- 使用者 ID 或 UID （例如 20 ）。
- 該使用者擁有的檔案或目錄路徑、以便檔案的唯一識別碼符合使用者。

如果您指定檔案或目錄名稱、則必須選取一個檔案或目錄、只要使用者帳戶仍保留在系統上、該檔案或目錄就會持續存在。

為UID指定檔案或目錄名稱、並不會導致ONTAP 將配額套用至該檔案或目錄。

指定 **Windows** 使用者的配額

您可以使用多種不同格式之一指定 Windows 使用者的配額。

指定 Windows 使用者進行配額時可用的三種格式包括：

- Windows 2000之前版本的Windows名稱。
- Windows 以文字形式顯示的安全 ID （ SID ） `S-1-5-32-544`、例如。
- 具有該使用者所擁有之ACL的檔案或目錄名稱。

如果您指定檔案或目錄名稱、則必須選取一個檔案或目錄、只要使用者帳戶仍保留在系統上、該檔案或目錄就會持續存在。

若要從ACL取得SID、ACL必須有效。ONTAP

如果檔案或目錄存在於UNIX風格的qtree中、或是儲存系統使用UNIX模式進行使用者驗證、ONTAP 則使用者配額將套用至* UID*（而非SID）符合檔案或目錄的使用者。

指定檔案或目錄名稱來識別配額的使用者、並不會導致ONTAP 系統不向該檔案或目錄套用配額。

預設使用者和群組配額如何建立衍生配額

當您建立預設使用者或群組配額時、系統會針對擁有相同層級檔案的每個使用者或群組、自動建立對應的衍生使用者或群組配額。

衍生的使用者和群組配額會以下列方式建立：

- 在一個使用者配額FlexVol 的情況下、使用者配額會為在磁碟區任何位置擁有檔案的每個使用者建立衍生的使用者配額。
- qtree上的預設使用者配額會針對擁有qtree中檔案的每個使用者、建立衍生的使用者配額。
- 在一個預設的群組配額FlexVol 中、會針對在磁碟區任何位置擁有檔案的每個群組、建立衍生的群組配額。
- qtree上的預設群組配額會為qtree中擁有檔案的每個群組建立衍生的群組配額。

如果使用者或群組未擁有預設使用者或群組配額層級的檔案、則不會為使用者或群組建立衍生配額。例如、如果為qtree proj1建立預設使用者配額、而使用者jsmith擁有不同qtree上的檔案、則不會為jsmith建立任何衍生的使用者配額。

衍生配額的設定與預設配額相同、包括限制和使用者對應。例如、如果預設的使用者配額具有50 MB磁碟限制、且已開啟使用者對應、則任何產生的衍生配額也會有50 MB磁碟限制、且使用者對應已開啟。

不過、三個特殊使用者和群組的衍生配額並不存在任何限制。如果下列使用者和群組擁有預設使用者或群組配額

層級的檔案、則會以與預設使用者或群組配額相同的使用者對應設定來建立衍生配額、但只是追蹤配額（無限制）：

- UNIX root使用者（UID 0）
- UNIX根群組（Gid 0）
- Windows BUILTIN\Administrator群組

  由於Windows群組的配額會追蹤為使用者配額、因此此群組的衍生配額是從預設使用者配額衍生而來的使用者配額、而非預設群組配額。

衍生使用者配額範例

如果您有三個使用者（root、jsmith和bob）擁有的檔案所在的磁碟區、而且您在磁碟區上建立預設的使用者配額、ONTAP 則會自動建立三個衍生的使用者配額。因此、重新初始化磁碟區上的配額之後、配額報告中會出現四個新配額：

```
cluster1::> volume quota report
  Vserver: vs1
                                      ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *          0B   50MB       0       -   *
vol1               user    root       5B      -       1       -
vol1               user    jsmith    30B   50MB      10       -   *
vol1               user    bob       40B   50MB      15       -   *
4 entries were displayed.
```

第一個新行是您建立的預設使用者配額、以星號（*）識別為ID。其他新行是衍生的使用者配額。jsmith和bob的衍生配額與預設配額具有相同的50 MB磁碟限制。根使用者的衍生配額是不受限制的追蹤配額。

如何將配額套用至**root**使用者

UNIX 用戶端上的根使用者（ UID=0 ）受樹狀目錄配額限制、但不受使用者或群組配額限制。這可讓root使用者代表其他使用者採取行動、否則配額就會阻止這些使用者。

當 root 使用者 `chown`代表 Privileges 較少的使用者執行檔案或目錄擁有權變更或其他作業（例如 UNIX 命令）時、 ONTAP 會根據新擁有者檢查配額、但不會報告錯誤或停止作業、即使新擁有者的強制配額限制已超過。當系統管理動作（例如恢復遺失的資料）導致暫時超過配額時、此功能就很有用。

不過、在進行所有權傳輸之後、如果使用者在配額仍超過時嘗試分配更多磁碟空間、用戶端系統將會報告磁碟空間錯誤。

相關資訊

- "配額的套用方式"
- "如何將配額套用至具有多個ID的使用者"

配額如何搭配特殊的**Windows**群組使用

有幾個特殊的 Windows 群組處理配額的方式不同於其他 Windows 群組。您應該瞭解如何為這些特殊群組套用配額。

> 不支援以Windows群組ID為基礎的群組配額。ONTAP如果您將Windows群組ID指定為配額目標、則配額會被視為使用者配額。

每個人

當配額目標是 Everyone 群組時、會將具有 ACL 且顯示擁有者的檔案計入 Everyone 的 SID 下。

內建\系統管理員

當配額目標是 BUILTIN\Administrators 群組時、該項目會被視為使用者配額、僅用於追蹤。您無法對BUILTIN\Administrator施加限制。如果 BUILTIN\Administrators 的成員建立檔案、則檔案歸 BUILTIN\Administrators 所有、並計入 BUILTIN\Administrators 的 SID （而非使用者的個人 SID ）。

如何將配額套用至具有多個**ID**的使用者

使用者可以使用多個ID來表示。您可以指定識別碼清單做為配額目標、為這類使用者定義單一使用者配額。任何這些ID所擁有的檔案都必須受到使用者配額的限制。

假設使用者具有 UNIX UID `20` 、 Windows ID `corp\john_smith` 和 `engineering\jsmith`。對於此使用者、您可以指定配額目標為唯一識別碼和Windows識別碼清單的配額。當此使用者寫入儲存系統時、無論寫入是來自 UID `20`、 `corp\john_smith`或 `engineering\jsmith`、都會套用指定的配額。

請注意、即使 ID 屬於同一位使用者、個別的配額規則也會視為個別的目標。例如、對於同一位使用者、您可以指定一個配額 `20`、將 UID 限制為 1GB 磁碟空間、而另一個配額則將 corp\john_smith 限制為 2GB 磁碟空間、即使兩個 ID 代表相同的使用者。ONTAP 會將配額套用至 UID `20` `corp\john_smith` 、並個別套用。在這種情況下 `engineering\jsmith`、即使將限制套用至相同使用者使用的其他 ID 、也不會套用任何限制。

相關資訊

- "配額的套用方式"
- "如何將配額套用至root使用者"

如何在混合式環境中判斷使用者**ID ONTAP**

如果您的使用者同時從 Windows 和 UNIX 用戶端存取 ONTAP 儲存設備、則 Windows 和 UNIX 安全性都會用來判斷檔案擁有權。套用使用者配額時、有幾個因素決定ONTAP 了哪些因素是使用UNIX或Windows ID。

如果FlexVol 包含檔案的qtree或fidscale Volume的安全樣式只是NTFS或UNIX、則安全樣式會決定套用使用者配額時所使用的ID類型。對於具有混合安全性樣式的qtree、所使用的ID類型取決於檔案是否具有ACL。

下表摘要說明使用的 ID 類型。

安全風格	**ACL**	無**ACL**
UNIX	UNIX ID	UNIX ID

安全風格	**ACL**	無**ACL**
混合	Windows ID	UNIX ID
NTFS	Windows ID	Windows ID

配額如何與多位使用者搭配運作

當您將多個使用者置於相同的配額目標時、配額定義的限制不會套用至每個個別使用者。而是配額目標中的所有使用者都會共用配額限制。

與管理物件（例如磁碟區和qtree）的命令不同、您無法重新命名配額目標、包括多使用者配額。這表示在定義多使用者配額之後、您無法修改配額目標中的使用者、也無法將使用者新增至目標、或從目標中移除使用者。如果您想要從多使用者配額中新增或移除使用者、則必須刪除包含該使用者的配額、以及定義目標中一組使用者的新配額規則。

如果您將個別的使用者配額合併成一個多使用者配額、您可以調整配額大小來啟動變更。不過、如果您想要從具有多個使用者的配額目標中移除使用者、或是將使用者新增至已有多個使用者的目標、則必須在變更生效之前重新初始化配額。

配額規則中有多位使用者的範例

在下列範例中、配額項目中會列出兩位使用者。這兩位使用者最多可同時使用 80MB 的空間。如果使用 75MB 、則另一個只能使用 5MB 。

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "jsmith,chen" -qtree "" -disk
-limit 80m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0                Policy: default           Volume: vol1
                                                     Soft             Soft
                              User          Disk     Disk    Files    Files
Type    Target         Qtree  Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------       ------- -------  --------  -------  ------  -------
---------
user    "jsmith,chen"  ""      off          80MB        -       -        -
-
```

UNIX 與 **Windows** 名稱連結以取得配額

在混合式環境中、使用者可以以Windows使用者或UNIX使用者的身分登入。您可以設定配額、以辨識使用者的UNIX ID和Windows ID代表相同的使用者。

Windows使用者名稱的配額會對應至UNIX使用者名稱、反之亦然、當符合下列兩項條件時：

- 。 `user-mapping` 在使用者的配額規則中、參數設為「開啟」。
- 使用者名稱已與對應 `vserver name-mapping` 命令。

當UNIX和Windows名稱對應在一起時、系統會將它們視為決定配額使用量的同一人員。

樹狀結構配額的運作方式

樹狀目錄配額的運作方式總覽

您可以使用qtree作為目標來建立配額、以限制目標qtree的大小。這些配額也稱為_tree配額_。

您也可以為特定qtree建立使用者和群組配額。此外FlexVol 、有時該磁碟區所包含的qtree會繼承一個適用於該磁碟區的配額。

當您將配額套用至qtree時、結果與磁碟分割區類似、只不過您可以隨時變更配額、以變更qtree的最大大小。套用樹狀結構配額時ONTAP 、無論擁有者為何、均會限制qtree中的磁碟空間和檔案數量。如果寫入作業導致超過樹狀結構配額、則任何使用者（包括root和BUILTIN\Administrator群組的成員）都無法寫入qtree。

配額大小並不保證有任何特定的可用空間量。配額的大小可以大於qtree可用的可用空間量。您可以使用 `volume quota report` 命令來確定 qtree 中的實際可用空間量。

如"指令參考資料ONTAP"需詳細 `volume quota report`資訊，請參閱。

使用者與群組配額如何搭配**qtree**使用

樹狀結構配額會限制qtree的整體大小。若要防止個別使用者或群組佔用整個qtree、請為該qtree指定使用者或群組配額。

qtree中的使用者配額範例

假設您有下列配額規則：

```
cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                  Soft             Soft
                         User          Disk      Disk    Files     Files
Type    Target    Qtree  Mapping      Limit     Limit    Limit     Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""     off           50MB        -       -         -
45MB
user    jsmith    ""     off           80MB        -       -         -
75MB
```

您注意到某位使用者 kjones 佔用大量空間、位於 vol1 中的關鍵 qtree （ project1 ）。您可以新增下列配額規則來限制此使用者的空間：

```
cluster1::> volume quota policy rule create -vserver vs0 -volume vol1
-policy-name default -type user -target "kjones" -qtree "proj1" -disk
-limit 20m -threshold 15m

cluster1::> volume quota policy rule show -vserver vs0 -volume vol1

Vserver: vs0               Policy: default           Volume: vol1
                                                Soft             Soft
                          User          Disk     Disk    Files    Files
Type    Target    Qtree   Mapping      Limit    Limit    Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    ""        ""      off           50MB        -       -        -
45MB
user    jsmith    ""      off           80MB        -       -        -
75MB
user    kjones    proj1   off           20MB        -       -        -
15MB
```

如何在**FlexVol** 一個流通量上建立預設的樹狀結構配額、才能建立衍生的樹狀結構配額

當您在FlexVol 某個流通量上建立預設的樹狀結構配額時、系統會自動為該磁碟區中的每個qtree建立對應的衍生樹狀結構配額。

這些衍生樹狀結構配額的限制與預設樹狀結構配額相同。如果不存在其他配額、則限制會產生下列影響：

- 使用者可以在qtree中使用與分配給整個磁碟區相同的空間（前提是使用根目錄或其他qtree中的空間不會超過磁碟區的限制）。
- 每個qtree都可以擴充以使用整個Volume。

在磁碟區上存在預設的樹狀結構配額、仍會影響所有新增至磁碟區的qtree。每次建立新的qtree時、也會建立衍生的樹狀結構配額。

如同所有衍生配額、衍生樹狀結構配額會顯示下列行為：

- 只有在目標尚未有明確配額時才會建立。
- 會顯示在配額報告中，但當您使用命令顯示配額規則時不會顯示 `volume quota policy rule show`。如"指令參考資料ONTAP"需詳細 `volume quota policy rule show`資訊，請參閱。

衍生樹狀結構配額範例

您的磁碟區有三個qtree（proj1、proj2和proj3）、唯一的樹狀結構配額是proj1 qtree上的明確配額、限制其磁碟大小為10 GB。如果您在磁碟區上建立預設樹狀結構配額、並重新初始化磁碟區上的配額、配額報告現在會包含四個樹狀結構配額：

```
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     tree    1           0B   10GB       1       -   proj1
vol1               tree    *           0B   20GB       0       -   *
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj3     tree    3           0B   20GB       1       -   proj3
...
```

第一行顯示proj1 qtree上的原始明確配額。此配額維持不變。

第二行顯示磁碟區上的新預設樹狀結構配額。星號（*）Quota說明符表示它是預設配額。此配額是您所建立配額規則的結果。

最後兩行顯示專案2和專案3 qtree的新衍生樹狀結構配額。由於磁碟區上的預設樹狀結構配額、所以系統會自動建立這些配額。ONTAP這些衍生的樹狀結構配額具有與磁碟區上預設樹狀結構配額相同的20-GB磁碟限制。由於proj1 qtree已經有明確的配額、所以無法為proj1 qtree建立衍生的樹狀結構配額。ONTAP

在一個流通量上的預設使用者配額**FlexVol** 如何影響該磁碟區中**qtree**的配額

如果針對FlexVol 某個現象磁碟區定義了預設的使用者配額、則會針對該磁碟區所包含的每個qtree、自動建立一個預設的使用者配額、其中存在明確或衍生的樹狀結構配額。

如果qtree上的預設使用者配額已存在、則在建立磁碟區上的預設使用者配額時、該配額不會受到影響。

在qtree上自動建立的預設使用者配額、其限制與您為磁碟區建立的預設使用者配額相同。

qtree的明確使用者配額會覆寫（取代自動建立的限制）自動建立的預設使用者配額、其方式與覆寫系統管理員在該qtree上建立的預設使用者配額相同。

qtree變更如何影響配額

刪除、重新命名或變更qtree的安全樣式時、ONTAP 根據目前套用的配額而定、由效能提升套用的配額可能會有所變更。

qtree 刪除和樹狀配額

刪除qtree時、ONTAP 所有適用於該qtree的配額（無論是明確的或衍生的配額）都不再由停止套用。

配額規則是否持續、取決於您刪除qtree的位置：

- 如果您使用ONTAP 還原刪除qtree、則會自動刪除該qtree的配額規則、包括樹狀結構配額規則、以及為該qtree設定的任何使用者和群組配額規則。
- 如果您使用CIFS或NFS用戶端刪除qtree、則必須刪除該qtree的任何配額規則、以免在重新初始化配額時發生錯誤。如果您建立的新qtree名稱與刪除的qtree名稱相同、則在重新初始化配額之前、現有的配額規則不會套用至新的qtree。

重新命名**qtree**如何影響配額

當您使用ONTAP 還原重新命名qtree時、該qtree的配額規則會自動更新。如果使用CIFS或NFS用戶端重新命名qtree、則必須更新該qtree的任何配額規則。

如果您使用 CIFS 或 NFS 用戶端重新命名 qtree 、且在重新初始化配額之前、並未使用新名稱更新該 qtree 的配額規則、配額將不會套用至 qtree 。qtree 的明確配額、包括樹狀配額和 qtree 的使用者或群組配額、可能會轉換成衍生配額。

qtree 安全樣式和使用者配額

您可以使用NTFS或混合式安全性樣式、在qtree上套用存取控制清單（ACL）、但不能使用UNIX安全性樣式。變更 qtree 的安全樣式可能會影響配額的計算方式。變更qtree的安全性樣式之後、您應該一律重新初始化配額。

如果將qtree的安全樣式從NTFS或混合變更為UNIX、則會忽略該qtree中檔案的任何ACL、並根據UNIX使用者ID來收取檔案使用量。

如果您將qtree的安全樣式從UNIX變更為混合式或NTFS、則先前隱藏的ACL會變成可見的。此外、任何被忽略的ACL都會再次生效、NFS使用者資訊也會被忽略。如果以前沒有ACL、則NFS資訊會繼續用於配額計算。

若要確保在變更qtree的安全性樣式之後、適當計算UNIX和Windows使用者的配額使用量、您必須重新初始化包含qtree的磁碟區配額。

範例

下列範例顯示qtree安全性樣式的變更如何導致不同的使用者因使用特定qtree中的檔案而被收費。

假設 NTFS 安全性在 qtree A 上有效、而 ACL 則賦予 Windows 使用者 `corp\joe` 5MB 檔案的擁有權。使用者`corp\joe`需為 qtree A 收取 5MB 的磁碟空間使用費

現在您可以將qtree A的安全樣式從NTFS變更為UNIX。重新初始化配額之後、 Windows 使用者 `corp\joe`就不會再為此檔案收費、而是會向對應於檔案 UID 的 UNIX 使用者收取檔案費用。UID 可以是對應至的 UNIX 使用者 `corp\joe`或 root 使用者。

配額的啟動方式

配額的啟動方式總覽

必須啟用新配額和現有配額變更、才能生效。啟動會在 Volume 層級執行。瞭解配額啟動的運作方式、可協助您以更少的中斷時間來管理配額。

配額可透過_初始化_（開啟）或_重新調整大小_來啟動。關閉配額並重新開啟配額稱為重新初始化。

啟動程序的長度及其對配額強制的影響取決於啟動類型：

- 初始化程序包括兩個部分： A `quota on` 工作和磁碟區整個檔案系統的配額掃描。掃描會在之後開始 `quota on` 工作已成功完成。配額掃描可能需要一段時間、磁碟區擁有的檔案越多、所需時間就越長。在掃描完成之前、配額啟動不會完成、而且不會強制執行配額。
- 調整大小程序只涉及 `quota resize` 工作。調整大小所需的時間比配額初始化少、因為它不涉及配額掃描。在調整大小的過程中、配額會繼續強制執行。

依預設 `quota on` 和 `quota resize` 工作會在背景中執行、讓您可以同時使用其他命令。

啟動程序的錯誤和警告會傳送至事件管理系統。如果您使用 `-foreground` 參數 `volume quota on` 或 `volume quota resize` 命令時、該命令會在工作完成之前傳回、如果您是從指令碼重新初始化、則此功能非常實用。若要稍後顯示錯誤和警告、您可以使用 `volume quota show` 命令 `-instance` 參數。

停機和重新開機後、配額啟動仍會持續。配額啟動程序不會影響儲存系統資料的可用度。

相關資訊

- "Volume配額開啟"
- "Volume配額大小調整"
- "Volume配額顯示"

瞭解何時使用調整大小功能

配額調整大小是一項實用的 ONTAP 功能。由於調整大小的速度比配額初始化快、因此您應該盡可能使用調整大小。不過、您需要注意一些限制。

調整大小僅適用於特定類型的配額變更。您可以在對配額規則進行下列類型的變更時調整配額大小：

- 變更現有配額。

  例如、變更現有配額的限制。

- 為預設配額或預設追蹤配額所在的配額目標新增配額。
- 刪除已指定預設配額或預設追蹤配額項目的配額。
- 將個別的使用者配額合併成一個多使用者配額。

變更大量配額後、您應該執行完整的重新初始化、以確保所有變更都生效。

如果您嘗試調整大小、但並非所有的配額變更都能透過調整大小作業來整合、ONTAP 則會發出警告。您可以從配額報告中判斷儲存系統是否正在追蹤特定使用者、群組或qtree的磁碟使用量。如果您在配額報告中看到配額、表示儲存系統正在追蹤磁碟空間、以及配額目標擁有的檔案數量。

範例配額變更可藉由調整大小而生效

調整大小可讓部分配額規則變更生效。請考慮下列配額：

```
#Quota Target type             disk  files thold sdisk sfile
#------------ ----             ----  ----- ----- ----- -----
*            user@/vol/vol2    50M   15K
*            group@/vol/vol2  750M   85K
*            tree@/vol/vol2      -     -
jdoe         user@/vol/vol2/  100M   75K
kbuck        user@/vol/vol2/  100M   75K
```

假設您進行下列變更：

- 增加預設使用者目標的檔案數量。
- 為新使用者（鮑里斯）新增使用者配額、此新使用者配額比預設使用者配額需要更多磁碟限制。
- 刪除kbuck使用者的明確配額項目；新使用者現在只需要預設配額限制。

這些變更會產生下列配額：

```
#Quota Target type              disk  files thold sdisk sfile
#------------ ----              ----  ----- ----- ----- -----
*              user@/vol/vol2    50M   25K
*              group@/vol/vol2  750M   85K
*              tree@/vol/vol2      -     -
jdoe           user@/vol/vol2/  100M   75K
boris          user@/vol/vol2/  100M   75K
```

調整大小會啟動所有這些變更、不需要重新初始化完整配額。

需要完整的配額重新初始化時

雖然調整配額大小的速度較快、但如果您對配額做出一些小或大幅的變更、則必須執行完整的配額重新初始化。

在下列情況下、必須重新初始化完整配額：

- 您可以為先前沒有配額的目標建立配額（既不是明確配額、也不是從預設配額衍生出來的配額）。
- 您可以將qtree的安全樣式從UNIX變更為混合式或NTFS。
- 您可以將qtree的安全樣式從混合式或NTFS變更為UNIX。
- 您可以從具有多個使用者的配額目標中移除使用者、或將使用者新增至已有多個使用者的目標。
- 您可以對配額進行廣泛變更。

需要初始化的配額變更範例

假設您的磁碟區包含三個 qtree 、而且該磁碟區中唯一的配額是三個明確的樹狀配額。您決定進行下列變更：

- 新增qtree並為其建立新的樹狀結構配額。
- 新增磁碟區的預設使用者配額。

這兩項變更都需要完整的配額初始化。調整大小並不會使配額生效。

如何檢視配額資訊

檢視配額資訊的總覽

您可以使用配額報告來檢視詳細資料、例如配額規則和原則的組態、強制和設定的配額、以及配額調整和重新初始化期間發生的錯誤。

檢視配額資訊在下列情況下非常實用：

- 設定配額、例如設定配額和驗證組態
- 回應即將達到磁碟空間或檔案限制或已達到限制的通知
- 回應更多空間的要求

使用配額報告查看有效的配額

由於配額互動的方式各不相同、因此與您明確建立的配額相比、配額效果更高。若要查看哪些配額有效、您可以檢視配額報告。

下列範例顯示FlexVol 套用在某個範圍Vol1上的不同配額類型、以及該磁碟區中所含qtree Q1的配額報告：

範例：未針對**qtree**指定使用者配額

在此範例中、磁碟區vol1包含一個qtree、即Q1。系統管理員已建立三個配額：

- vol1 的預設樹狀目錄配額上限為 400MB
- vol1 的預設使用者配額上限為 100MB
- 使用者 jsmith 的 vol1 為 200MB 的明確使用者配額限制

這些配額的配額規則類似於下列範例：

```
cluster1::*> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                Soft             Soft
                         User          Disk     Disk   Files    Files
Type   Target    Qtree   Mapping      Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -           400MB        -       -        -
-
user   ""        ""      off         100MB        -       -        -
-
user   jsmith    ""      off         200MB        -       -        -
-
```

這些配額的配額報告類似於下列範例：

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith    150B  200MB       7       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     q1         user   *           0B  100MB       0       -
vol1     q1         user   jsmith      0B  100MB       5       -
vol1     -          user   root        0B    0MB       1       -
vol1     q1         user   root        0B    0MB       8       -
```

配額報告的前三行顯示系統管理員指定的三個配額。由於其中兩個配額是預設配額、ONTAP 所以不只是由NetApp自動建立衍生配額。

第四行顯示從vol1中每個qtree的預設樹狀結構配額衍生的樹狀結構配額（在此範例中、僅Q1）。

第五行顯示為qtree建立的預設使用者配額、這是因為磁碟區上存在預設使用者配額和qtree配額。

第六行顯示在qtree上為jsmith建立的衍生使用者配額、因為qtree（第5行）有預設的使用者配額、而使用者jsmith擁有該qtree上的檔案。請注意、 qtree Q1 中套用至使用者 jsmith 的限制、並不是由明確的使用者配額限制（ 200MB ）所決定。這是因為磁碟區上有明確的使用者配額限制、所以不會影響qtree的限制。而是由 qtree 的預設使用者配額（ 100MB ）來決定 qtree 的衍生使用者配額限制。

最後兩行會顯示更多使用者配額、這些配額是從磁碟區和qtree上的預設使用者配額衍生而來。在Volume和qtree上為root使用者建立了衍生的使用者配額、因為root使用者在Volume和qtree上擁有檔案。由於root使用者在配額方面獲得特殊處理、因此其衍生配額僅會追蹤配額。

範例：為**qtree**指定使用者配額

此範例與上一個範例類似、只是系統管理員在qtree上新增了兩個配額。

還有一個Volume、vol1和qtree、Q1。系統管理員已建立下列配額：

- vol1 的預設樹狀目錄配額上限為 400MB
- vol1 的預設使用者配額上限為 100MB
- 對於 200MB 的用戶 jsmith 而言、 vol1 的明確使用者配額限制
- qtree Q1 的預設使用者配額上限為 50MB
- 對於 75MB 的使用者 jsmith 、 qtree Q1 的明確使用者配額限制

這些配額的配額規則如下所示：

```
cluster1::> volume quota policy rule show -vserver vs1 -volume vol1

Vserver: vs1               Policy: default           Volume: vol1
                                                Soft             Soft
                          User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   ""        ""      -           400MB        -       -        -
-
user   ""        ""      off         100MB        -       -        -
-
user   ""        q1      off          50MB        -       -        -
-
user   jsmith    ""      off         200MB        -       -        -
-
user   jsmith    q1      off          75MB        -       -        -
-
```

這些配額的配額報告如下所示：

```
cluster1::> volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     -          tree   *           0B  400MB       0       -   *
vol1     -          user   *           0B  100MB       0       -   *
vol1     -          user   jsmith   2000B  200MB       7       -   jsmith
vol1     q1         user   *           0B   50MB       0       -   *
vol1     q1         user   jsmith      0B   75MB       5       -   jsmith
vol1     q1         tree   1           0B  400MB       6       -   q1
vol1     -          user   root        0B    0MB       2       -
vol1     q1         user   root        0B    0MB       1       -
```

配額報告的前五行會顯示系統管理員所建立的五個配額。由於其中有些配額是預設配額、ONTAP 所以不只是使用者配額、所以會自動建立衍生配額。

第六行顯示從vol1中每個qtree的預設樹狀結構配額衍生的樹狀結構配額（在此範例中、僅Q1）。

最後兩行顯示從磁碟區和qtree上的預設使用者配額衍生的使用者配額。在Volume和qtree上為root使用者建立了衍生的使用者配額、因為root使用者在Volume和qtree上擁有檔案。由於root使用者在配額方面獲得特殊處理、因

此其衍生配額僅會追蹤配額。

由於下列原因、未建立其他預設配額或衍生配額：

- 雖然使用者同時擁有磁碟區和qtree上的檔案、但並未為jsmith使用者建立衍生的使用者配額、因為使用者在這兩個層級都有明確的配額。
- 沒有為其他使用者建立衍生的使用者配額、因為其他使用者在磁碟區或qtree上都沒有擁有檔案。
- 磁碟區上的預設使用者配額並未在qtree上建立預設使用者配額、因為qtree已有預設的使用者配額。

強制配額為何與設定的配額不同

強制配額與設定的配額不同、因為導出配額是在未設定的情況下強制執行、但只有在成功初始化之後才會強制執行設定的配額。瞭解這些差異有助於比較配額報告中顯示的強制配額與您設定的配額。

配額報告中顯示的強制配額可能會因下列原因而與設定的配額規則不同：

- 導出的配額不會設定為配額規則而強制執行。ONTAP 會自動建立衍生配額、以回應預設配額。
- 配額規則設定完成後、磁碟區上的配額可能尚未重新初始化。
- 在磁碟區上初始化配額時可能發生錯誤。

使用配額報告來判斷哪些配額限制寫入特定檔案

您可以使用磁碟區配額報告命令搭配特定檔案路徑、來判斷哪些配額限制會影響檔案的寫入作業。這有助於您瞭解哪些配額會妨礙寫入作業。

步驟

1. 使用volume quota report命令搭配-path參數。

顯示影響特定檔案的配額範例

下列範例顯示命令和輸出、以判斷哪些配額對FlexVol 位於「示例」Volume vol2中qtree Q1的檔案檔案檔案1有效：

```
cluster1:> volume quota report -vserver vs0 -volume vol2 -path
/vol/vol2/q1/file1
Virtual Server: vs0
                                       ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     q1        tree    jsmith     1MB  100MB       2   10000   q1
vol2     q1        group   eng        1MB  700MB       2   70000
vol2               group   eng        1MB  700MB       6   70000   *
vol2               user    corp\jsmith
                                      1MB   50MB       1       -   *
vol2     q1        user    corp\jsmith
                                      1MB   50MB       1       -
5 entries were displayed.
```

用於在 **ONTAP** 中顯示配額資訊的命令

您可以使用命令來顯示配額報告、其中包含強制配額和資源使用量、顯示配額狀態和錯誤的相關資訊、或是配額原則和配額規則的相關資訊。

您只能在FlexVol 下列指令上執行：

如果您想要...	使用此命令...
檢視強制配額的相關資訊	`volume quota report`
檢視配額目標的資源使用量（磁碟空間和檔案數）	`volume quota report`
決定允許寫入檔案時、哪些配額限制會受到影響	`volume quota report` 使用 `-path` 參數
顯示配額狀態、例如 `on`、 `off`和 `initializing`	`volume quota show`
檢視配額訊息記錄的相關資訊	`volume quota show` 使用 `-logmsg` 參數
檢視配額初始化和調整大小期間發生的錯誤	`volume quota show` 使用 `-instance` 參數
檢視配額原則的相關資訊	`volume quota policy show`
檢視配額規則的相關資訊	`volume quota policy rule show`

如果您想要...	使用此命令...
檢視指派給儲存虛擬機器（SVM、先前稱為Vserver）的配額原則名稱	`vserver show` 使用 `-instance` 參數

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

何時使用**Volume**配額原則規則**show**和**Volume**配額報告命令

雖然這兩個命令都會顯示配額的相關資訊、但是 `volume quota policy rule show` 在期間快速顯示已設定的配額規則 `volume quota report` 命令會消耗更多時間和資源、顯示強制配額和資源使用量。

- `volume quota policy rule show` 命令可用於下列用途：
  - 在啟動配額規則之前、請先檢查配額規則的組態

    無論配額已初始化或調整大小、此命令都會顯示所有已設定的配額規則。
  - 快速檢視配額規則、而不影響系統資源

    由於此命令不會顯示磁碟和檔案使用量、因此不會像配額報告那樣耗用大量資源。
  - 在未指派給SVM的配額原則中顯示配額規則。

如"指令參考資料ONTAP"需詳細 `volume quota policy rule show`資訊，請參閱。

- `volume quota report` 命令可用於下列用途：
  - 檢視強制配額、包括衍生配額
  - 檢視每個有效配額所使用的磁碟空間和檔案數量、包括受衍生配額影響的目標

    （對於預設配額、使用量會顯示為「0」、因為系統會根據產生的衍生配額來追蹤使用量。）
  - 決定哪些配額限制會影響何時允許寫入檔案

    新增 `-path` 的參數 `volume quota report` 命令。

> 配額報告是資源密集的作業。如果您在FlexVol 叢集中的許多個資料區上執行、可能需要很長時間才能完成。更有效率的方法是檢視SVM中特定磁碟區的配額報告。

如"指令參考資料ONTAP"需詳細 `volume quota report`資訊，請參閱。

配額報告和**UNIX**用戶端顯示的空間使用量差異

配額報告和 **UNIX** 用戶端所顯示的空間使用量差異總覽

FlexVol volume 或 qtree 配額報告中顯示的已用磁碟空間值、可能與 UNIX 用戶端針對相同磁碟區或 qtree 顯示的值不同。這些值的差異在於配額報告後面的方法不同、以及用於

計算 Volume 或 qtree 中資料區塊的 UNIX 命令。

例如、如果磁碟區包含含有空白資料區塊（未寫入資料）的檔案、則磁碟區的配額報告不會在報告空間使用量時計算空白資料區塊。不過、當磁碟區掛載到 UNIX 用戶端時、檔案會顯示為的輸出 `ls` 命令時、空間使用中也會包含空的資料區塊。因此 `ls` 與配額報告所顯示的空間使用量相比、命令會顯示較大的檔案大小。

同樣地、配額報告中顯示的空間使用值也可能與 UNIX 命令（例如）所顯示的值不同 `df` 和 `du`。

配額報告如何計算磁碟空間和檔案使用量

使用的檔案數量、以及配額報告中針對FlexVol 某個相依磁碟區或qtree所指定的磁碟空間量、取決於該磁碟區或qtree中每個inode對應的已使用資料區塊數。

區塊數包括用於一般和串流檔案的直接和間接區塊。用於目錄、存取控制清單（ACL）、串流目錄和中繼檔案的區塊、在配額報告中並未列入考量。如果是UNIX的稀疏檔案、配額報告中不會包含空白資料區塊。

配額子系統是專為考量及僅包含檔案系統的使用者可控制面向而設計。目錄、ACL和快照空間都是配額計算中排除的空間範例。配額用於強制執行限制、而非保證、而且僅在作用中檔案系統上運作。配額會計不會計算某些檔案系統架構、也不會考慮儲存效率（例如壓縮或重複資料刪除）。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

ls 命令與配額報告之間的空間使用差異

當您使用 `ls`命令來檢視安裝在 UNIX 用戶端上的 FlexVol volume 內容時、輸出中顯示的檔案大小可能會與磁碟區配額報告中顯示的空間使用量不同、視檔案的資料區塊類型而定。

的輸出 `ls` 命令僅顯示檔案大小、不包含檔案使用的間接區塊。檔案的任何空白區塊也會包含在命令的輸出中。

因此、如果檔案沒有空白區塊、則會顯示的大小 `ls` 命令可能小於配額報告所指定的磁碟使用量、因為配額報告中包含間接區塊。相反地、如果檔案有空白區塊、則會顯示的大小 `ls` 命令可能超過配額報告所指定的磁碟使用量。

的輸出 `ls` 命令僅顯示檔案大小、不包含檔案使用的間接區塊。檔案的任何空白區塊也會包含在命令的輸出中。

ls命令和配額報告所說明的空間使用量差異範例

下列配額報告顯示qtree Q1的上限為10 MB：

```
                                      ----Disk----  ----Files-----   Quota
  Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
  -------  ---------  ------  --------  -----  -----  ------  ------
---------
  vol1     q1           tree    user1    10MB  10MB         1       -   q1

...
```

從 UNIX 用戶端使用檢視時、同一 qtree 中的檔案大小可能超過配額限制 `ls` 命令、如下列範例所示：

```
[user1@lin-sys1 q1]$ ls -lh
-rwxr-xr-x  1 user1 nfsuser  **27M** Apr 09  2013 file1
```

如"指令參考資料ONTAP"需詳細 `ls`資訊，請參閱。

df命令如何計算檔案大小

在中的方式 `df` 命令會根據兩種情況報告空間使用量：是否為包含 qtree 的磁碟區啟用或停用配額、以及是否追蹤 qtree 內的配額使用量。

當針對 qtree 內包含 qtree 和配額使用量的磁碟區啟用配額時、會追蹤的空間使用量 `df` 命令等於配額報告指定的值。在這種情況下、配額使用量會排除目錄、ACL、串流目錄和中繼檔所使用的區塊。

當磁碟區上未啟用配額、或qtree未設定配額規則時、報告的空間使用量會包含整個磁碟區（包括磁碟區內的其他qtree）的目錄、ACL、串流目錄和中繼檔所使用的區塊。在這種情況下、會回報的空間使用量 `df` 命令大於追蹤配額時所報告的預期值。

當您執行時 `df` 命令從 qtree 的掛載點追蹤配額使用量、命令輸出會顯示與配額報告指定的值相同的空間使用量。在大多數情況下、當樹狀結構配額規則具有硬碟限制時、會報告總大小 `df` 命令等於磁碟限制、可用空間等於配額磁碟限制與配額使用量之間的差異。

不過、在某些情況下、會報告可用空間 `df` 命令可能等於整個磁碟區的可用空間。如果沒有為qtree設定硬碟限制、就可能發生此問題。從供應到供應的更新版本9.9.1開始ONTAP 、當整個磁碟區的可用空間少於剩餘的樹狀結構配額空間時、也會發生此問題。發生上述任一情況時、會報告總大小 `df` 命令是一個合成數字、等於 qtree 內使用的配額、加上 FlexVol Volume 中的可用空間。

> 此總大小既不是qtree磁碟限制、也不是Volume設定的大小。它也會因您在其他qtree內的寫入活動或背景儲存效率活動而有所不同。

說明的空間使用範例 `df` 命令和配額報告

下列配額報告顯示qtree Alice1 GB的磁碟限制、qtree bob 2 GB的磁碟限制、qtree project1的磁碟限制為無上限：

```
C1_vsim1::> quota report -vserver vs0
Vserver: vs0
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol2     alice     tree    1
                                   502.0MB    1GB       2       -   alice
vol2     bob       tree    2
                                    1003MB    2GB       2       -   bob
vol2     project1  tree    3
                                   200.8MB      -       2       -
project1
vol2               tree    *           0B      -       0       -   *
4 entries were displayed.
```

在下列範例中、的輸出 `df` qtree 上的命令 Alice 和 bob 會報告與配額報告相同的已用空間、以及與磁碟限制相同的總大小（以 1M 區塊為準）。這是因為qtree Aliceand bob的配額規則具有已定義的磁碟限制、而Volume可用空間（1211 MB）大於qtree Alice（523 MB）和qtree bob（1045 MB）的剩餘樹狀配額空間。

```
linux-client1 [~]$ df -m /mnt/vol2/alice
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1024   502       523  50% /mnt/vol2

linux-client1 [~]$ df -m /mnt/vol2/bob
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2048  1004      1045  50% /mnt/vol2
```

在下列範例中、的輸出 `df` qtree project1 上的命令會報告與配額報告相同的已用空間、但總大小會透過將磁碟區中的可用空間（ 1211 MB ）新增至 qtree project1 （ 201 MB ）的配額使用量、以提供總共 1412 MB 的空間來合成。這是因為qtree project1的配額規則沒有磁碟限制。

```
linux-client1 [~]$ df -m /mnt/vol2/project1
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      1412   201      1211  15% /mnt/vol2
```

下列範例顯示的輸出方式 `df` 整個捲上的命令會回報與 project1 相同的可用空間。

```
linux-client1 [~]$ df -m /mnt/vol2
Filesystem          1M-blocks  Used Available Use% Mounted on
172.21.76.153:/vol2      2919  1709      1211  59% /mnt/vol2
```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

DU 命令與空間使用配額報告之間的差異

當您執行時 du 命令若要檢查掛載於 UNIX 用戶端的 qtree 或 FlexVol 磁碟區的磁碟空間使用量、使用值可能會高於 qtree 或磁碟區配額報告所顯示的值。

的輸出 du 命令包含從發出命令的目錄層級開始、透過目錄樹狀結構的所有檔案的組合空間使用量。因為使用率值是由所顯示 du 命令也包含目錄的資料區塊、比配額報告所顯示的值還要高。

DU命令與配額報告所說明的空間使用量差異範例

下列配額報告顯示qtree Q1的上限為10 MB：

```
                                        ----Disk----  ----Files-----   Quota
  Volume   Tree       Type    ID         Used  Limit    Used   Limit
Specifier
  -------  ---------  ------  --------  -----  -----  ------  ------
---------
  vol1     q1         tree    user1     10MB   10MB   1       -        q1

...
```

在下列範例中、磁碟空間使用量是的輸出 du 命令會顯示超過配額限制的較高值：

```
[user1@lin-sys1 q1]$ du -sh
**11M**     q1
```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

配額組態範例

這些範例可協助您瞭解如何設定配額和讀取配額報告。

關於這些範例

對於以下示例，假設您的存儲系統包括 SVM ， `vs1`其中一個 `Volume` ， `vol1`。

1. 若要開始設定配額、請為 SVM 建立新的配額原則：

   ```
   cluster1::>volume quota policy create -vserver vs1 -policy-name
   quota_policy_vs1_1
   ```

2. 因為配額原則是新的、所以您可以將它指派給 SVM ：

```
cluster1::>vserver modify -vserver vs1 -quota-policy quota_policy_vs1_1
```

範例1：預設使用者配額

1. 您決定對中的每位使用者強制限制 50MB `vol1` ：

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 50MB
-qtree ""
```

2. 若要啟動新規則、請在磁碟區上初始化配額：

```
cluster1::>volume quota on -vserver vs1 -volume vol1 -foreground
```

3. 您可以檢視配額報告：

```
cluster1::>volume quota report
```

產生的配額報告類似於下列報告：

```
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     49MB   50MB      37       -   *
vol1               user    root        0B      -       1       -
```

第一行顯示您建立的預設使用者配額、包括磁碟限制。如同所有預設配額、此預設使用者配額不會顯示磁碟或檔案使用量的相關資訊。除了建立的配額之外、還會出現另外兩個配額。目前擁有上檔案的每位使用者都有一個配額 `vol1`。這些額外配額是自動衍生自預設使用者配額的使用者配額。使用者的衍生使用者配額 `jsmith`與預設使用者配額具有相同的 50MB 磁碟限制。根使用者的衍生使用者配額為追蹤配額（無限制）。

如果系統上的任何使用者（ root 使用者以外的使用者）嘗試執行超過 50MB 的動作 `vol1`（例如、從編輯器寫入檔案）、則該動作會失敗。

範例2：明確的使用者配額會覆寫預設的使用者配額

1. 如果您需要爲 `vol1`**用戶提供更多的卷空間** `jsmith`，請輸入以下命令：

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree ""
```

這是明確的使用者配額、因為使用者明確列為配額規則的目標。

這是對現有配額限制的變更、因為它會變更 `jsmith`磁碟區上使用者的衍生使用者配額磁碟限制。因此、您不需要重新初始化磁碟區上的配額、即可啟動變更。

2. 若要調整配額大小：

```
cluster1::>volume quota resize -vserver vs1 -volume vol1 -foreground
```

配額會在您調整大小時維持有效、而調整大小的程序也很短。

產生的配額報告類似於下列報告：

```
cluster1::> volume quota report
Vserver: vs1
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith     50MB   80MB      37       -   jsmith
vol1               user    root        0B      -       1       -
3 entries were displayed.
```

第二行現在顯示的磁碟限制 `80MB`和配額指定符號 `jsmith`。

因此、 `jsmith`vol1`即使所有其他使用者仍限於 50MB 、仍可在上使用高達 80MB 的空間。

範例3：臨界值

假設您想要在使用者達到其磁碟限制的5 MB以內時收到通知。

1. 若要為所有使用者建立 45MB 的臨界值、並為建立 75MB `jsmith` 的臨界值、請變更現有的配額規則：

```
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target "" -qtree ""
-threshold 45MB
cluster1::>volume quota policy rule modify -vserver vs1 -policy
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -qtree ""
-threshold 75MB
```

由於現有規則的大小已變更、因此您可以調整磁碟區上的配額大小、以啟動變更。您需要等待調整大小程序完成。

2. 若要查看具有臨界值的配額報告、請新增 `-thresholds` 的參數 `volume quota report` 命令：

```
cluster1::>volume quota report -thresholds
Vserver: vs1
                                     ----Disk----  ----Files-----
Volume   Tree      Type    ID        Used  Limit   Used    Limit  Quota
                                          (Thold)
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               user    *           0B   50MB       0       -  *
                                         (45MB)
vol1               user    jsmith     59MB   80MB      55       -  jsmith
                                         (75MB)
vol1               user    root        0B      -       1       -
                                         ( -)
3 entries were displayed.
```

臨界值會顯示在「磁碟限制」欄的括弧中。

如"指令參考資料ONTAP"需詳細 `volume quota report`資訊，請參閱。

範例4：qtree上的配額

假設您需要分割兩個專案的空間。您可以建立兩個 qtree `proj1` 、分別命名為和 `proj2`、以便在中容納這些專案 `vol1`。

目前、使用者可以在qtree中使用與分配給整個Volume相同的空間（前提是使用root或其他qtree中的空間不會超過Volume的限制）。此外、每個qtree都可以擴充以使用整個Volume。

1. 如果您想要確保兩個qtree的成長都超過20 GB、您可以在磁碟區上建立預設的樹狀結構配額：

```
cluster1:>>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type tree -target "" -disk-limit 20GB
```

正確的類型是 _tree 、而非 qtree 。

2. 由於這是新的配額、因此您無法透過調整大小來啟動配額。您可以重新初始化磁碟區上的配額：

```
cluster1:>>volume quota off -vserver vs1 -volume vol1
cluster1:>>volume quota on -vserver vs1 -volume vol1 -foreground
```

您必須確保在重新啟動每個受影響磁碟區上的配額之前等待約五分鐘，因為在執行命令之後，幾乎立即嘗試啟動配額 `volume quota off`可能會導致錯誤。或者、您也可以執行命令、從包含特定磁碟區的節點重新初始化磁碟區的配額。如"指令參考資料ONTAP"需詳細 `volume quota off`資訊，請參閱。

在重新初始化程序期間不會強制執行配額、這比調整大小程序所需的時間更長。

當您顯示配額報告時、它有幾行新的資料行。有些線條用於樹狀目錄配額、有些線條用於衍生的使用者配額。

以下是樹狀結構配額的新行：

```
                                     ----Disk----  ----Files-----   Quota
Volume   Tree       Type    ID        Used  Limit    Used   Limit
Specifier
-------  ---------  ------  -------  -----  -----  ------  ------
---------
...
vol1                tree    *           0B   20GB       0       -   *
vol1     proj1      tree    1           0B   20GB       1       -   proj1
vol1     proj2      tree    2           0B   20GB       1       -   proj2
...
```

您所建立的預設樹狀結構配額會出現在第一行的「ID」欄位中、其中有星號（*）。為了回應磁碟區上的預設樹狀結構配額、ONTAP 所以針對磁碟區中的每個qtree自動建立衍生的樹狀結構配額。這些項目會顯示在 `proj1` `proj2` `Tree`欄中的位置和顯示位置。

下列新行適用於衍生的使用者配額：

```
                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
...
vol1     proj1     user    *           0B   50MB       0       -
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
...
```

如果為qtree啟用配額、則會自動為該磁碟區所包含的所有qtree繼承磁碟區上的預設使用者配額。當您新增第一個qtree配額時、會在qtree上啟用配額。因此、會為每個qtree建立衍生的預設使用者配額。這些欄位會顯示在ID為星號（*）的行中。

由於root使用者是檔案的擁有者、因此在為每個qtree建立預設使用者配額時、也會針對每個qtree上的root使用者建立特殊的追蹤配額。這些資訊會顯示在ID為root的行中。

範例**5**：**qtree**上的使用者配額

1. 您決定限制使用者在 `proj1` qtree 中的空間、使其小於整個 Volume 中的空間。您想要防止他們在 `proj1` qtree 中使用超過 10MB 的任何資料。因此、您可以為qtree建立預設的使用者配額：

   ```
   cluster1::>volume quota policy rule create -vserver vs1 -policy-name
   quota_policy_vs1_1 -volume vol1 -type user -target "" -disk-limit 10MB
   -qtree proj1
   ```

   這是對現有配額的變更、因為它會變更從磁碟區上預設使用者配額衍生的proj1 qtree預設使用者配額。因此、您可以調整配額大小來啟動變更。調整大小程序完成後、您可以檢視配額報告。

   配額報告中會出現下列新行、顯示qtree的新明確使用者配額：

   ```
                                        ----Disk----  ----Files-----   Quota
   Volume   Tree      Type    ID        Used  Limit    Used   Limit
   Specifier
   -------  --------  ------  -------  -----  -----  ------  ------
   ---------
   vol1     proj1     user    *           0B   10MB       0       -   *
   ```

   但是、 `jsmith`**由於您建立的配額會覆寫磁碟區上的預設使用者配額（以提供更多空間）、使用者無法將更多資料寫入** `proj1 qtree` **。當您在** `proj1` qtree 上新增預設使用者配額時、會套用該配額、並限制該 qtree 中所有使用者的空間 `jsmith`、包括。

2. 若要為使用者提供更多空間 `jsmith`、您可以為 qtree 新增明確的使用者配額規則、並在其中加入 80MB 磁碟限制、以覆寫 qtree 的預設使用者配額規則：

```
cluster1::>volume quota policy rule create -vserver vs1 -policy-name
quota_policy_vs1_1 -volume vol1 -type user -target jsmith -disk-limit
80MB -qtree proj1
```

由於這是已存在預設配額的明確配額、因此您可以調整配額大小來啟動變更。當調整大小程序完成時、您會顯示配額報告。

配額報告中會出現下列新行：

```
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
```

最後一份配額報告類似於下列報告：

```
cluster1::>volume quota report
Vserver: vs1
                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
vol1               tree    *           0B   20GB       0       -   *
vol1               user    *           0B   50MB       0       -   *
vol1               user    jsmith    70MB   80MB      65       -   jsmith
vol1     proj1     tree    1           0B   20GB       1       -   proj1
vol1     proj1     user    *           0B   10MB       0       -   *
vol1     proj1     user    root        0B      -       1       -
vol1     proj2     tree    2           0B   20GB       1       -   proj2
vol1     proj2     user    *           0B   50MB       0       -
vol1     proj2     user    root        0B      -       1       -
vol1               user    root        0B      -       3       -
vol1     proj1     user    jsmith    61MB   80MB      57       -   jsmith
11 entries were displayed.
```

使用者 `jsmith`必須達到下列配額限制、才能寫入中的檔案 `proj1`：

1. `proj1`qtree 的樹狀目錄配額。
2. `proj1`qtree 上的使用者配額。

3. 磁碟區上的使用者配額。

在**SVM**上設定配額

您可以在新的 SVM 上設定配額、以管理及監控資源使用率。

關於這項工作

在較高層級、設定配額時需要執行幾個步驟、包括：

1. 建立配額原則
2. 將配額規則新增至原則
3. 將原則指派給 SVM
4. 初始化 SVM 上每個 FlexVol volume 的配額

步驟

1. 輸入命令 `vserver show -instance` 顯示建立 SVM 時自動建立的預設配額原則名稱。

   如果在建立SVM時未指定名稱、則名稱為「預設」。您可以使用 `vserver quota policy rename` 命令、為預設原則命名。

   您也可以使用建立新原則 `volume quota policy create` 命令。

2. 使用 `volume quota policy rule create` 命令可為 SVM 上的每個磁碟區建立下列任何配額規則：
   - 所有使用者的預設配額規則
   - 針對特定使用者的明確配額規則
   - 所有群組的預設配額規則
   - 特定群組的明確配額規則
   - 所有qtree的預設配額規則
   - 特定qtree的明確配額規則
3. 使用 `volume quota policy rule show` 檢查配額規則是否正確設定的命令。
4. 如果您正在制定新原則、請使用 `vserver modify` 命令將新原則指派給 SVM 。
5. 使用 `volume quota on` 用於初始化 SVM 上每個磁碟區的配額的命令。

   您可以使用下列方式監控初始化程序：
   - 當您使用時 `volume quota on` 您可以新增 `-foreground` 在工作前景執行配額的參數。（依預設、工作會在背景執行。）

     當工作在背景執行時、您可以使用監控其進度 `job show` 命令。
   - 您可以使用 `volume quota show` 用於監控配額初始化狀態的命令。
6. 使用 `volume quota show -instance` 用於檢查初始化錯誤的命令、例如無法初始化的配額規則。
7. 使用 `volume quota report` 顯示配額報告的命令、以確保強制配額符合您的期望。

相關資訊

- "Vserver展示"
- "Vserver修改"
- "工作展示"
- "Volume 配額"

修改或調整配額限制大小

您可以變更或調整所有受影響磁碟區上的配額大小、比重新初始化這些磁碟區上的配額更快。

關於這項工作

您的儲存虛擬機器（SVM、先前稱為Vserver）具有強制配額、您想要變更現有配額的大小限制、或是新增或刪除已有衍生配額的目標配額。

步驟

1. 使用 `vserver show` 命令 `-instance` 用於確定當前分配給 SVM 的策略名稱的參數。
2. 執行下列任一動作來修改配額規則：
   - 使用 `volume quota policy rule modify` 修改現有配額規則磁碟或檔案限制的命令。
   - 使用 `volume quota policy rule create` 命令可為目前已衍生配額的目標（使用者、群組或 qtree ）建立明確的配額規則。
   - 使用 `volume quota policy rule delete` 用於刪除具有預設配額之目標（使用者、群組或 qtree ）的明確配額規則的命令。
3. 使用 `volume quota policy rule show` 檢查配額規則是否正確設定的命令。
4. 使用 `volume quota resize` 命令、在您變更配額的每個磁碟區上啟動每個磁碟區上的變更。

   您可以使用下列任一方法來監控調整大小程序：

   - 當您使用時 `volume quota resize` 您可以新增 `-foreground` 在前景執行調整工作的參數。（依預設、工作會在背景執行。）

     當工作在背景執行時、您可以使用監控其進度 `job show` 命令。

   - 您可以使用 `volume quota show` 用於監控調整大小狀態的命令。
5. 使用 `volume quota show -instance` 用於檢查大小調整錯誤的命令、例如無法調整大小的配額規則。

   特別是、針對尚未有衍生配額的目標、新增明確配額後、重新調整配額大小時、請檢查「'new definition」錯誤。

6. 使用 `volume quota report` 顯示配額報告的命令，以確保強制配額符合您的需求。

相關資訊

- "Volume 配額原則規則"
- "Volume 配額"

- "工作展示"

進行廣泛變更後、重新初始化配額

在對現有配額定義進行大量變更之後、您必須重新初始化所有受影響磁碟區上的配額。這類變更的範例之一是新增或刪除沒有強制配額的目標配額。

關於這項工作

您擁有具有強制配額的儲存虛擬機器（SVM）、而且想要進行需要重新初始化配額的變更。

步驟

1. 使用 `vserver show` 命令 `-instance` 用於確定當前分配給 SVM 的策略名稱的參數。
2. 執行下列任一動作來修改配額規則：

如果您想要...	然後...
建立新的配額規則	使用 `volume quota policy rule create` 命令
修改現有配額規則的設定	使用 `volume quota policy rule modify` 命令
刪除現有的配額規則	使用 `volume quota policy rule delete` 命令

3. 使用 `volume quota policy rule show` 檢查配額規則是否正確設定的命令。
4. 在每個變更配額的磁碟區上重新初始化配額、方法是關閉配額、然後開啟這些磁碟區的配額。
   a. 使用 `volume quota off` 在每個受影響的磁碟區上執行命令、以停用該磁碟區上的配額。
   b. 使用 `volume quota on` 命令在每個受影響的磁碟區上啟動配額。

   > 您必須確保在重新啟動每個受影響磁碟區上的配額之前、等待大約五分鐘、因為在執行之後、您幾乎會立即嘗試啟動配額 `volume quota off` 命令可能會導致錯誤。
   >
   > 或者、您也可以執行命令、從包含特定磁碟區的節點重新初始化磁碟區的配額。

   您可以使用下列任一方法來監控初始化程序：

   - 當您使用時 `volume quota on` 您可以新增 `-foreground` 在工作前景執行配額的參數。（依預設、工作會在背景執行。）

     當工作在背景執行時、您可以使用監控其進度 `job show` 命令。

   - 您可以使用 `volume quota show` 用於監控配額初始化狀態的命令。
5. 使用 `volume quota show -instance` 用於檢查初始化錯誤的命令、例如無法初始化的配額規則。
6. 使用 `volume quota report` 顯示配額報告的命令、以確保強制配額符合您的期望。

相關資訊

- "Vserver展示"
- "Volume 配額原則規則"
- "Volume 配額"
- "工作展示"

用於管理配額規則和配額原則的命令

這些 `volume quota policy rule`命令可讓您設定配額規則、而 `volume quota policy`命令和某些 `vserver`命令可讓您設定配額原則。視您需要執行的動作而定、請使用下列命令來管理配額規則和配額原則：

您只能在FlexVol 下列指令上執行：

用於管理配額規則的命令

如果您想要...	使用此命令...
建立新的配額規則	`volume quota policy rule create`
刪除現有的配額規則	`volume quota policy rule delete`
修改現有的配額規則	`volume quota policy rule modify`
顯示有關已設定配額規則的資訊	`volume quota policy rule show`

用於管理配額原則的命令

如果您想要...	使用此命令...
複製配額原則及其所包含的配額規則	`volume quota policy copy`
建立新的空白配額原則	`volume quota policy create`
刪除目前未指派給儲存虛擬機器（SVM）的現有配額原則	`volume quota policy delete`
重新命名配額原則	`volume quota policy rename`
顯示配額原則的相關資訊	`volume quota policy show`
將配額原則指派給 SVM	`vserver modify -quota-policy` *`policy_name`*

如果您想要...	使用此命令...
顯示指派給 SVM 的配額原則名稱	`vserver show`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "Volume 配額原則"
- "vserver modify -quota 原則名稱"
- "Vserver展示"

在 **ONTAP** 中啟動及修改配額的命令

`volume quota`命令可讓您變更配額狀態、並設定配額的訊息記錄。視您需要執行的動作而定、您可以使用下列命令來啟動和修改配額：

如果您想要...	使用此命令...
開啟配額（也稱為_初始化_）	`volume quota on`
調整現有配額的大小	`volume quota resize`
關閉配額	`volume quota off`
變更配額的訊息記錄、開啟配額、關閉配額或調整現有配額的大小	`volume quota modify`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "Volume配額開啟"
- "Volume配額大小調整"
- "Volume配額關閉"
- "Volume配額修改"

使用重複資料刪除技術、資料壓縮及資料壓縮技術來提高儲存效率

重複資料刪除、資料壓縮、資料壓縮及儲存效率

您可以一起執行重複資料刪除、資料壓縮及資料壓縮、或是獨立執行、以在FlexVol 一個影像區上實現最佳的空間節約效益。重複資料刪除技術可消除重複的資料區塊資料壓縮會壓縮資料區塊、以減少所需的實體儲存容量。資料壓縮可在較少空間中儲存更多資料、以提升儲存效率。

所有內聯儲存效率功能（例如內聯重複資料刪除和內聯壓縮）在AFF磁碟區上預設為啟用。

在磁碟區上啟用重複資料刪除

您可以在FlexVol 支援重複資料刪除技術的過程中、在一個支援重複資料刪除的磁碟區上啟用、您可以在所有磁碟區上啟用後處理重複資料刪除功能、並在AFF 駐留在NetApp或Flash Pool Aggregate上的磁碟區上啟用即時重複資料刪除功能。

如果您要在其他類型的磁碟區上啟用內嵌重複資料刪除，請參閱"NetApp知識庫：如何在非AFF （全快閃FAS）聚合上啟用卷內聯重複資料刪除"。

開始之前

對於某個Set功能 磁碟區、您必須已確認磁碟區和集合體中有足夠的可用空間可用於重複資料刪除中繼資料。FlexVol重複資料刪除中繼資料需要集合體中的最小可用空間量。此金額等於FlexVol 所有重複資料刪除的所有非重複資料的實體資料總量的3%、或是集合體內的資料成分。每FlexVol 個實體磁碟區或資料組成部份應佔實體資料總可用空間的4%、總計應佔7%。

AFF系統預設啟用內聯重複資料刪除。

選擇

- 使用 `volume efficiency on`命令啟用後處理重複資料刪除。如"指令參考資料ONTAP"需詳細 `volume efficiency on`資訊，請參閱。

  下列命令可在Volume Vola上啟用後處理重複資料刪除：

  ```
  volume efficiency on -vserver vs1 -volume VolA
  ```

- 使用 `volume efficiency on`命令後加上 `volume efficiency modify`選項設定為的 `true`命令 `-inline-deduplication`，即可同時啟用後處理重複資料刪除和內嵌重複資料刪除。如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

  下列命令可在Volume Vola上同時啟用後處理重複資料刪除和即時重複資料刪除：

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -inline-dedupe true
  ```

- 使用 `volume efficiency on` 命令後面接著 `volume efficiency modify` 命令 `-inline-deduplication` 選項設為 `true` 和 `-policy` 選項設為 `inline-only` 僅啟用即時重複資料刪除。

  下列命令僅在Volume Vola上啟用即時重複資料刪除：

  ```
  volume efficiency on -vserver vs1 -volume VolA

  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only -inline-dedupe true
  ```

完成後

檢視 Volume EffEffEffEffEff需 的設定、確認設定已變更：

```
volume efficiency show -instance
```

如"指令參考資料ONTAP"需詳細 `volume efficiency show -instance`資訊，請參閱。

停用磁碟區上的重複資料刪除功能

您可以在磁碟區上獨立停用後處理重複資料刪除和即時重複資料刪除。

開始之前

停止目前在磁碟區上作用中的任何Volume效率作業： `volume efficiency stop`

如"指令參考資料ONTAP"需詳細 `volume efficiency stop`資訊，請參閱。

關於這項工作

如果您已在捲上啟用資料壓縮，執行命令會停用資料壓縮 `volume efficiency off`。如"指令參考資料ONTAP"需詳細 `volume efficiency off`資訊，請參閱。

選擇

- 使用 `volume efficiency off` 命令可停用後處理重複資料刪除和內嵌重複資料刪除。

  下列命令可停用Volume Vola上的後處理重複資料刪除和即時重複資料刪除功能：

  ```
  volume efficiency off -vserver vs1 -volume VolA
  ```

- 使用 `volume efficiency modify` 命令 `-policy` 選項設為 `inline only` 若要停用後處理重複資料刪除、但即時重複資料刪除功能仍保持啟用狀態。

  下列命令會停用後處理重複資料刪除、但Volume Vola仍會啟用即時重複資料刪除：

  ```
  volume efficiency modify -vserver vs1 -volume VolA -policy inline-only
  ```

- 使用 `volume efficiency modify` 命令 `-inline-deduplication` 選項設為 `false` 僅停用即時重複資料刪除。

  下列命令僅會停用Volume Vola上的即時重複資料刪除功能：

  ```
  volume efficiency modify -vserver vs1 -volume VolA -inline-deduplication false
  ```

  如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

AFF 系統上的自動磁碟區層級背景重複資料刪除技術

從 ONTAP 9.3 開始、您可以設定磁碟區層級的背景重複資料刪除功能、以使用預先定義的方式自動執行 `auto` AFF 原則。不需要手動設定排程。。 `auto` 原則會在背景執行持續的重複資料刪除。

。 `auto` 所有新建立的磁碟區和所有尚未手動設定背景重複資料刪除的升級磁碟區都會設定原則。您可以 "變更原則" 至 `default` 或任何其他原則來停用此功能。

如果某個 Volume 從非 AFF 系統移至 AFF 系統、則 `auto` 預設會在目的地節點上啟用原則。如果某個 Volume

從 AFF 節點移至非 AFF 節點、則會移至 `auto` 目的地節點上的原則會由取代 `inline-only` 原則預設。

在 AFF 上、系統會監控所有具有的磁碟區 `auto` 原則和排定磁碟區的優先順序、以減少節省成本或頻繁覆寫的磁碟區。已取消優先順序的磁碟區不再參與自動背景重複資料刪除。停用已取消優先順序之磁碟區上的變更記錄、且磁碟區上的中繼資料會被刪減。

使用者可以升級已取消優先順序的磁碟區、以便使用重新參與自動背景重複資料刪除 `volume efficiency promote` 進階權限層級可用的命令。

如"指令參考資料ONTAP"需詳細 `volume efficiency promote`資訊，請參閱。

在**AFF** 不完善的系統上管理集合體層級的即時重複資料刪除技術

Aggregate層級的重複資料刪除技術可在屬於同一個Aggregate的各磁碟區之間消除重複區

您可以在AFF系統上執行聚合級重複資料刪除。此功能預設會針對所有新建立的磁碟區和所有已升級的磁碟區啟用、並開啟Volume即時重複資料刪除功能。

關於這項工作

重複資料刪除作業可在資料寫入磁碟之前、先消除重複的區塊。只有具有的 Volume `space guarantee` 設定為 `none` 可參與 Aggregate 層級的內嵌重複資料刪除。這是AFF 在整個系統上的預設設定。

Aggregate層級的即時重複資料刪除技術有時稱為跨磁碟區即時重複資料刪除技術。

步驟

1. 在AFF 下列情況下、管理位於下列系統上的集合體層級即時重複資料刪除：

如果您想要...	使用此命令
啟用Aggregate層級的即時重複資料刪除技術	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe true`
停用Aggregate層級的即時重複資料刪除	`volume efficiency modify -vserver vserver_name -volume vol_name -cross -volume-inline-dedupe false`
顯示Aggregate層級的即時重複資料刪除狀態	`volume efficiency config -volume vol_name`

範例

下列命令會顯示Aggregate層級的即時重複資料刪除狀態：

```
wfit-8020-03-04::> volume efficiency config -volume choke0_wfit_8020_03_0
Vserver:                                    vs0
Volume:                                     choke0_wfit_8020_03_0
Schedule:                                   -
Policy:                                     choke_VE_policy
Compression:                                true
Inline Compression:                         true
Inline Dedupe:                              true
Data Compaction:                            true
Cross Volume Inline Deduplication:          false
```

在**AFF** 不完善的系統上管理集合體層級的背景重複資料刪除技術

Aggregate層級的重複資料刪除技術可在屬於同一個Aggregate的各磁碟區之間消除重複區

從功能介紹9.3開始ONTAP 、您可以在AFF 幕後執行Aggregate層級的重複資料刪除技術。此功能預設會針對所有新建立的磁碟區和所有已升級且已開啟Volume背景重複資料刪除功能的磁碟區啟用。

關於這項工作

當填入足夠大的變更記錄百分比時、系統會自動觸發此作業。沒有與作業相關的排程或原則。

從使用者執行的功能為物件9.4開始ONTAP 、AFF 使用者也可以執行Aggregate層級的重複資料刪除掃描程式、以消除集合體中各磁碟區之間現有資料的重複資料。您可以使用 `storage aggregate efficiency cross-volume-dedupe start` 命令 `-scan-old-data=true` 啟動掃描器的選項：

```
cluster-1::> storage aggregate efficiency cross-volume-dedupe start
-aggregate aggr1 -scan-old-data true
```

重複資料刪除掃描可能相當耗時。您可能想要在非尖峰時間執行作業。

Aggregate層級的背景重複資料刪除技術有時稱為跨Volume背景重複資料刪除技術。

如"指令參考資料ONTAP"需詳細 `storage aggregate efficiency cross-volume-dedupe start`資訊，請參閱。

步驟

1. 管理AFF 位於整個系統上的Aggregate層級背景重複資料刪除技術：

如果您想要...	使用此命令
啟用Aggregate層級的背景重複資料刪除	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe true`

如果您想要...	使用此命令
停用Aggregate層級的背景重複資料刪除	`volume efficiency modify -vserver <vserver_name\> -volume <vol_name\> -cross-volume-background-dedupe false`
顯示Aggregate層級的背景重複資料刪除狀態	`aggregate efficiency cross-volume-dedupe show`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "Volume效率修改"
- "彙總效率跨磁碟區重複資料刪除顯示"

了解**ONTAP**溫度敏感型儲存效率

ONTAP透過評估磁碟區資料的存取頻率並將該頻率對應到應用於該資料的壓縮程度來提供溫度敏感儲存效率 (TSSE) 優勢。對於不經常存取的冷數據，壓縮較大的數據塊；對於經常存取和覆蓋的熱數據，壓縮較小的數據塊，從而使處理更加高效。

TSSE 在ONTAP 9.8 中引入，並在新建立的精簡配置AFF磁碟區上自動啟用。您可以對現有的精簡配置AFF磁碟區和精簡配置的非AFF DP 磁碟區啟用溫度敏感儲存效率。TSSE 不支援在厚置備卷上執行。

以下平台不適用溫度敏感儲存效率：

平台	版本**ONTAP**
• AFF A1K • AFF A90 • AFF A70 • FAS90 • FAS70	9.15.1 或更新版本
• AFF C80 • AFF C60 • AFF C30 • AFF A50 • AFF A30	9.16.1 或更新版本

這些平台使用"CPU 或專用卸載處理器儲存效率"。壓縮是使用主 CPU 或專用卸載處理器執行的，並不是基於熱數據或冷數據。

隨著時間的推移，與 8K 自適應壓縮相比，TSSE 佔用的捲空間量可能會更加明顯。由於 TSSE 和 8K 自適應壓縮之間的架構差異，這種行為是可以預期的。

引進「預設」和「有效率」模式

從 ONTAP 9 。 10.1 開始、 *default* 和 *Effive* 磁碟區層級的儲存效率模式僅適用於 AFF 系統。這兩種模式可選擇檔案壓縮（預設），這是建立新 AFF 磁碟區時的預設模式，或是對溫度敏感的儲存效率（效率），這兩種模式使用自動調適式壓縮技術，可在不常存取的冷資料上，提供更高的壓縮節省。

升級至 ONTAP 9.10.1 及更新版本時、會根據目前在磁碟區上啟用的壓縮類型、為現有磁碟區指派儲存效率模式。在升級期間、已啟用壓縮的磁碟區會被指派預設模式、而已啟用溫度敏感儲存效率的磁碟區則會被指派效率模式。如果未啟用壓縮、儲存效率模式會保持空白。

搭配 ONTAP 9 。 10.1 、"必須明確設定溫度敏感的儲存效率"可啟用自動調適式壓縮。不過、 AFF 平台預設會啟用其他儲存效率功能、例如資料壓縮、自動重複資料刪除排程、內嵌重複資料刪除、跨磁碟區內嵌重複資料刪除、以及跨磁碟區背景重複資料刪除、以提供預設模式和高效率模式。

啟用 FabricPool 的集合體和所有分層原則類型都支援兩種儲存效率模式（預設和有效率）。

在 **C** 系列平台上啟用對溫度敏感的儲存效率

在AFF C 系列平台上，溫度敏感儲存效率 (TSSE) 預設為啟用；當使用磁碟區移動或SnapMirror將精簡配置磁碟區從非 TSSE 平台遷移到啟用 TSSE 的 C 系列平台時，如果目標平台上安裝了以下版本，則也會啟用 TSSE：

- ONTAP 9.12.1P4 及更新版本
- ONTAP 9.13.1 及更新版本

如需更多資訊、請參閱 "Volume Move 和 SnapMirror 作業的儲存效率行為"。

對於現有的精簡配置卷，溫度敏感儲存效率不會自動啟用；但是，您可以... "修改儲存效率模式" 手動切換到高效率模式。

將儲存效率模式變更為「有效率」後、您就無法將其變更回來。

連續包裝實體區塊、提升儲存效率

從 ONTAP 9.13.1 開始、對溫度敏感的儲存效率可增加連續實體區塊的連續包裝、進一步改善儲存效率。當您將系統升級至 ONTAP 9.13.1 時、已啟用溫度敏感儲存效率的磁碟區會自動啟用連續封裝。啓用連續打包後"手動重新包裝現有資料"，您必須。

Volume Move 和 **SnapMirror** 作業的儲存效率行為

儲存效率的行為可能會受到其他作用中或同時啟動的儲存作業影響。您應該瞭解這些作業對儲存效率的影響。

在某些情況下"對溫度敏感的儲存效率（ TSSE ）"，磁碟區上的儲存效率可能會受到其他作業的影響，包括 Volume Moves ， SnapMirror 關係， FabricPool Volume 和。

FabricPool

`all`資料保護磁碟區通常會使用分層原則，以立即將資料標記為冷資料，並儘快分層。在資料變得冷且分層之前，無需等待至少幾天的時間。

由於分層原則會盡快分層資料，因此 `all`仰賴背景處理程序（例如 32K 高效調適式壓縮（ TSSE ））的儲存效率，沒有足夠的時間來應用。像 8K 壓縮一樣的即時儲存效率，也會正常套用。

下表說明執行其中一項作業時、來源 Volume 和目的地 Volume 的行為。

來源 Volume 效率	目的地 Volume 預設行為			手動啟用 TSSE 後的預設行為（ SnapMirror 中斷後）		
	* 儲存效率類型 *	* 新的寫入 *	* 冷資料壓縮 *	* 儲存效率類型 *	* 新的寫入 *	* 冷資料壓縮 *
無儲存效率（可能是 FAS ）	檔案壓縮	在新寫入的資料上嘗試即時壓縮檔案	不壓縮冷資料、資料仍保持不變	TSSE 採用 ZSTD 的冷資料掃描演算法	嘗試使用 TSSE 格式進行 8K 內嵌壓縮	* 檔案壓縮資料 * ：不適用 * 未壓縮資料 * ：達到臨界天數後嘗試 32K 壓縮 * 新寫入的資料 * ：達到臨界天數後嘗試 32K 壓縮
無儲存效率（可能是 FAS ）	在使用 ONTAP 9.11.1P10 或 ONTAP 9.12.1P3 的 C 系列平台上進行檔案壓縮	沒有啟用 TSSE-的冷資料壓縮	* 檔案壓縮資料 * ：不適用	TSSE 採用 ZSTD 的冷資料掃描演算法	8K 內嵌壓縮	* 檔案壓縮資料 * ：不適用 * 未壓縮資料 * ：達到臨界天數後嘗試 32K 壓縮 * 新寫入的資料 * ：達到臨界天數後嘗試 32K 壓縮
無儲存效率（可能是 FAS ）	使用 ONTAP 9.12.1P4 及更新版本或 ONTAP 9.13.1 及更新版本的 C 系列平台上的 TSSE	嘗試使用 TSSE 格式進行 8K 內嵌壓縮	* 檔案壓縮資料 * ：不適用 * 未壓縮資料 * ：達到臨界天數後嘗試 32K 壓縮 * 新寫入的資料 * ：達到臨界天數後嘗試 32K 壓縮	TSSE 採用 ZSTD 的冷資料掃描演算法	嘗試使用 TSSE 格式進行 8K 內嵌壓縮	* 檔案壓縮資料 * ：不適用 * 未壓縮資料 * ：達到臨界天數後嘗試 32K 壓縮 * 新寫入的資料 * ：達到臨界天數後嘗試 32K 壓縮

檔案壓縮群組	與來源相同	在新寫入的資料上嘗試即時壓縮檔案	不壓縮冷資料、資料仍保持不變	TSSE 採用 ZSTD 的冷資料掃描演算法	嘗試使用 TSSE 格式進行 8K 內嵌壓縮	* 檔案壓縮資料 * ：未壓縮 * 未壓縮資料 * ：達到臨界天數後會嘗試 32K 壓縮 * 新寫入的資料 * ：達到臨界天數後、會嘗試 32K 壓縮
TSSE 冷資料掃描	TSSE 使用與來源 Volume 相同的壓縮演算法（ LZOPro→LZOPro 和 ZSTD→ZSTD ）	嘗試 TSSE 格式的 8K 內嵌壓縮	在現有資料和新寫入的資料達到臨界天數的冷度後、與 LzoPro 嘗試 32K 壓縮。	TSSE 已啟用。附註：LZOPro 冷資料掃描演算法可變更為 ZSTD 。	嘗試使用 TSSE 格式進行 8K 內嵌壓縮	在現有資料和新寫入的資料達到臨界天數冷度之後、會嘗試 32K 壓縮。

在磁碟區建立期間設定儲存效率模式

從ONTAP 功能更新到功能更新AFF 到功能更新到功能更新到功能更新到功能更新到功能更新的功能更新到功能更新到功能更新的功能、您可以設定儲存效率模式。

關於這項工作

您可以使用下列參數控制新AFF磁碟區的儲存效率模式 `-storage-efficiency-mode`。您可以選擇以下兩種選項來設定儲存效率模式： `default` 或者 `efficient`。您選擇的儲存效率模式取決於您想要更高的效能還是更高的儲存效率。參數 `-storage-efficiency-mode` 在非AFF磁碟區或資料保護磁碟區上不受支援。

建立新的AFF區時，如果啟用儲存效率模式，則預設為效能模式。

"深入瞭解對溫度敏感的儲存效率和儲存效率模式"。

步驟

1. 建立新磁碟區並設定效率模式：

```
volume create -vserver <vserver name> -volume <volume name> -aggregate
<aggregate name> -size <volume size> -storage-efficiency-mode
<efficient|default>
```

放 `-storage-efficiency-mode` 到 `efficient` 為了提高效率模式或 `default` 用於性能模式。

在以下範例中，aff_vol1 是以效率模式建立的。

```
volume create -vserver vs1 -volume aff_vol1 -aggregate aff_aggr1 -storage
-efficiency-mode efficient -size 10g
```

變更 **ONTAP** 中的 **Volume** 非使用中資料壓縮臨界值

您可以變更 ONTAP 執行冷資料掃描的頻率、方法是使用溫度敏感的儲存效率、修改磁碟區的冷度臨界值。

開始之前

您必須是叢集或 SVM 管理員、並使用 ONTAP CLI 進階權限等級。

關於這項工作

冷限值可以是 1 到 60 天。預設臨界值為 14 天。

步驟

1. 設定權限等級：

   ```
   set -privilege advanced
   ```

2. 修改磁碟區上的非作用中資料壓縮：

   ```
   volume efficiency inactive-data-compression modify -vserver <vserver_name>
   -volume <volume_name> -threshold-days <integer>
   ```

如"指令參考資料ONTAP"需詳細 `volume efficiency inactive-data-compression modify`資訊，請參閱。

檢查**Volume Eff**效率 模式

您可以使用 `volume-efficiency-show` 命令 AFF 磁碟區、檢查是否已設定效率、以及檢視目前的效率模式。

步驟

1. 檢查磁碟區的效率模式：

   ```
   volume efficiency show -vserver <vserver name> -volume <volume name> -fields
   storage-efficiency-mode
   ```

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

變更**Volume Eff**效率 模式

從ONTAP 9.10.1 開始，磁碟區級儲存效率模式 *default* 和 *efficient* 僅對AFF系統支援。這些模式提供了兩種選擇：檔案壓縮（預設），這是建立新AFF磁碟區時的預設模式；或溫度敏感儲存效率（高效），它啟用溫度敏感儲存效率 (TSSE)。

TSSE 僅在精簡配置磁碟區上支援。"了解更多關於TSSE的信息"。

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 來執行此工作。

系統管理員

從《支援範圍》9.10.1開始ONTAP 、您可以使用System Manager、利用對溫度敏感的儲存效率功能來提升儲存效率。效能型儲存效率預設為啟用。

1. 按一下「儲存設備>磁碟區」。
2. 找到要啟用或停用儲存效率的磁碟區、然後按一下 ⋮。
3. 按一下 * 編輯 > 磁碟區 * 、然後捲動至 * 儲存效率 * 。
4. 選取*「啟用更高的儲存效率」*。

CLI

你可以使用 `volume efficiency modify` 用於更改AFF卷儲存效率模式的命令 `default` 到 `efficient` 或者，當音量效率尚未設定時，您可以設定效率模式。

1. 變更Volume Eff效率 模式：

```
volume efficiency modify -vserver <vserver name> -volume <volume
name> -storage-efficiency-mode <default|efficient>
```

如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

檢視儲存容量的儲存效率、無論是否對溫度敏感、都能節省佔用空間

視 ONTAP 版本而定、您可以檢視每個磁碟區的實體佔用空間節約效益。您可以這樣做來評估管理程序的有效性、或是作為容量規劃的一部分。

關於這項工作

從 ONTAP 9 。 11.1 開始、您可以使用命令 `volume show-footprint`來檢視已啟用溫度敏感儲存效率（ TSSe ）的磁碟區實體佔用空間節約效益。從 ONTAP 9 。 13.1 開始、您可以使用相同的命令來檢視未啟用 TSSE 的磁碟區、可節省實體佔用空間。

步驟

1. 檢視大容量佔用空間的節約效益：

```
volume show-footprint
```

啟用 **TSSE** 的輸出範例

```
      Vserver : vs0
      Volume  : vol_tsse_75_per_compress

      Feature                                    Used       Used%
      --------------------------------        ----------    -----
      Volume Data Footprint                      10.15GB      13%
      Volume Guarantee                               0B       0%
      Flexible Volume Metadata                   64.25MB       0%
      Delayed Frees                              235.0MB       0%
      File Operation Metadata                        4KB       0%

      Total Footprint                            10.45GB      13%

      Footprint Data Reduction                    6.85GB       9%
           Auto Adaptive Compression              6.85GB       9%
      Effective Total Footprint                   3.59GB       5%
```

未啟用 **TSSE** 的輸出範例

```
      Vserver : vs0
      Volume  : vol_file_cg_75_per_compress

      Feature                                    Used       Used%
      --------------------------------        ----------    -----
      Volume Data Footprint                       5.19GB       7%
      Volume Guarantee                               0B       0%
      Flexible Volume Metadata                   32.12MB       0%
      Delayed Frees                              90.17MB       0%
      File Operation Metadata                        4KB       0%

      Total Footprint                             5.31GB       7%

      Footprint Data Reduction                    1.05GB       1%
           Data Compaction                        1.05GB       1%
      Effective Total Footprint                   4.26GB       5%
```

相關資訊

- "在磁碟區建立期間設定儲存效率模式"

在磁碟區上啟用資料壓縮

您可以使用命令在 FlexVol volume 上啟用資料壓縮，以節省空間 `volume efficiency modify`。如果您不想使用預設的壓縮類型、也可以指派壓縮類型給Volume。如"指令參考

資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

開始之前

您必須在磁碟區上啟用重複資料刪除功能。

- 重複資料刪除只需啟用、不需要在磁碟區上執行。
- 壓縮掃瞄器必須用於壓縮AFF 位於各種不同平台上的磁碟區上的現有資料。

"在磁碟區上啟用重複資料刪除"

關於這項工作

- 在HDD Aggregate和Flash Pool Aggregate中、您可以同時啟用即時和後處理壓縮、也可以只在磁碟區上啟用後處理壓縮。

  如果您同時啟用這兩項功能、則必須先在磁碟區上啟用後處理壓縮、才能啟用內嵌壓縮。

- 在支援的支援平台中、僅支援即時壓縮。AFF

  在啟用即時壓縮之前、您必須在磁碟區上啟用後處理壓縮。不過AFF 、由於不支援在流程後壓縮的功能、因此這些磁碟區不會發生後處理壓縮、而且會產生一則EMS訊息、通知您已跳過後處理壓縮。

- 對溫度敏感的儲存效率已在ONTAP 介紹過程中介紹。有了這項功能、儲存效率會根據資料是熱的還是冷的而有所不同。對於冷資料而言、較大的資料區塊會被壓縮、而熱資料會被覆寫的頻率較高、較小的資料區塊會被壓縮、使程序更有效率。對溫度敏感的儲存效率會在新建立的精簡配置AFF 的功能區上自動啟用。
- 壓縮類型會根據Aggregate平台自動指派：

平台/集合體	壓縮類型
AFF	自適應壓縮
Flash Pool Aggregate	自適應壓縮
HDD集合體	二線壓縮

選擇

- 使用 `volume efficiency modify` 以預設壓縮類型啟用資料壓縮的命令。

  下列命令可在SVM VS1的Volume Vola上啟用後處理壓縮：

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true
  ```

  下列命令可在SVM VS1的Volume Vola上啟用後處理和即時壓縮：

  ```
  volume efficiency modify -vserver vs1 -volume VolA -compression true -inline
  -compression true
  ```

- 使用 `volume efficiency modify` 進階權限層級的命令、可啟用特定壓縮類型的資料壓縮。

a. 使用 `set -privilege advanced` 命令將權限等級變更為進階。

b. 使用 `volume efficiency modify` 命令將壓縮類型指派給磁碟區。

下列命令可啟用後處理壓縮、並將調適性壓縮類型指派給SVM VS1的Volume Vola：

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive
```

下列命令可啟用後處理和內嵌壓縮、並將調適性壓縮類型指派給SVM VS1的Volume Vola：

```
volume efficiency modify -vserver vs1 -volume VolA -compression true
-compression-type adaptive -inline-compression true
```

a. 使用 `set -privilege admin` 命令將權限等級變更為 admin 。

在二線壓縮和調適性壓縮之間移動

視資料讀取量而定、您可以在二線壓縮和調適性壓縮之間切換。如果系統隨機讀取量很大、而且需要較高的效能、則建議使用調適性壓縮。如果資料是循序寫入、而且需要更高的壓縮節約量、則偏好使用二線壓縮。

關於這項工作

預設的壓縮類型是根據您的Aggregate與平台而選擇。

步驟

1. 停用磁碟區的效率：

```
volume efficiency off
```

例如、下列命令會停用 Volume vol1 的效率：

```
volume efficiency off -vserver vs1 -volume vol1
```

2. 變更為進階權限層級：

```
set -privilege advanced
```

3. 解壓縮壓縮資料：

```
volume efficiency undo
```

例如、下列命令會解壓縮 Volume vol1 上的壓縮資料：

```
volume efficiency undo -vserver vs1 -volume vol1 -compression true
```

您必須驗證磁碟區中是否有足夠的空間來容納解壓縮的資料。

4. 變更為管理權限層級：

```
set -privilege admin
```

5. 確認作業狀態為閒置：

   `volume efficiency show`

   例如、下列命令會顯示 Volume vol1 上效率作業的狀態：

   `volume efficiency show -vserver vs1 -volume vol1`

6. 提高 Volume 效率：

   `volume efficiency on` 例如、下列命令可提高 Volume vol1 的效率：

   `volume efficiency on -vserver vs1 -volume vol1`

7. 啟用資料壓縮、然後設定壓縮類型：

   `volume efficiency modify`

   例如、下列命令可啟用資料壓縮、並將壓縮類型設定為 Volume vol1 的次要壓縮：

   ```
   volume efficiency modify -vserver vs1 -volume vol1 -compression true
   -compression-type secondary
   ```

   此步驟只會啟用磁碟區的二次壓縮、而不會壓縮磁碟區上的資料。

   - 若要壓縮AFF 現有的資料至非資料系統、您必須執行背景壓縮掃描程式。
   - 若要壓縮Flash Pool Aggregate或HDD Aggregate上的現有資料、您必須執行背景壓縮。

8. 選用：啟用即時壓縮：

   `volume efficiency modify`

   例如、下列命令可在 Volume vol1 上啟用即時壓縮：

   `volume efficiency modify -vserver vs1 -volume vol1 -inline-compression true`

停用**Volume**上的資料壓縮

您可以使用命令停用磁碟區上的資料壓縮 `volume efficiency modify`。如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

關於這項工作

若要停用後處理壓縮、必須先停用Volume上的內嵌壓縮。

步驟

1. 停止目前在磁碟區上作用中的任何Volume效率作業：

   `volume efficiency stop`

2. 停用資料壓縮：

   `volume efficiency modify`

   現有的壓縮資料會在磁碟區上保持壓縮狀態。只有進入磁碟區的新寫入作業不會被壓縮。

範例

下列命令會停用Volume Vola上的即時壓縮：

```
volume efficiency modify -vserver vs1 -volume VolA -inline-compression false
```

下列命令會停用Volume Vola上的後處理壓縮和即時壓縮：

```
volume efficiency modify -vserver vs1 -volume VolA -compression false -inline
-compression false
```

如"指令參考資料ONTAP"需詳細 `volume efficiency stop`資訊，請參閱。

管理**AFF** 適用於不實系統的即時資料精簡

您可以使用在 Volume 層級控制 AFF 系統上的即時資料壓縮 `volume efficiency modify` 命令。根據預設AFF 、資料壓縮功能會針對整個系統上的所有磁碟區啟用。

開始之前

資料壓縮需要將磁碟區空間保證設定為 `none`。這是AFF 不適用於整個系統的預設值。

非AFF資料保護磁碟區的預設空間保證設定為無。

步驟

1. 若要驗證磁碟區的空間保證設定：

   ```
   volume show -vserver vserver_name -volume volume_name -fields space-guarantee
   ```

2. 若要啟用資料壓縮：

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction true
   ```

3. 若要停用資料壓縮：

   ```
   volume efficiency modify -vserver vserver_name -volume volume_name -data
   -compaction false
   ```

4. 若要顯示資料精簡狀態：

   ```
   volume efficiency show -instance
   ```

範例

```
cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data-compaction
```

```
true cluster1::> volume efficiency modify -vserver vs1 -volume vol1 -data
-compaction false
```

為FAS 不實系統啟用即時資料壓縮功能

您可以使用叢集 Shell 命令，在 FAS 系統上啟用快閃集區（混合式）集合體或磁碟區層級的 HDD 集合體的內嵌資料壓縮 `volume efficiency`功能。FAS 系統上建立的磁碟區預設會停用資料壓縮功能。如"指令參考資料ONTAP"需詳細 `volume efficiency`資訊，請參閱。

關於這項工作

若要在磁碟區上啟用內嵌資料壓縮，其 `-space-guarantee`選項必須設定為 `none`。在HDD Aggregate上的磁碟區上啟用資料壓縮功能、會使用額外的CPU資源。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

   如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

2. 檢查所需節點的磁碟區和集合體資料壓縮狀態：

   ```
   volume efficiency show -volume <volume_name>
   ```

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

3. 在 Volume 上執行資料壓縮：

   ```
   volume efficiency modify -volume <volume_name> -data-compaction true
   ```

   如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

   > ⓘ 如果將 Aggregate 或 Volume 的資料壓縮設為 `false` 、則壓縮作業會失敗。啟用壓縮並不會壓縮現有資料、只會壓縮新的系統寫入內容。此 `volume efficiency start`命令包含有關如何壓縮現有資料的詳細資訊。如"指令參考資料ONTAP"需詳細 `volume efficiency start`資訊，請參閱。

4. 檢視壓縮統計資料：

   ```
   volume efficiency show -volume <volume_name>
   ```

根據預設**AFF** 、可在不支援的系統上實現即時儲存效率

儲存效率功能預設會在 AFF 系統上所有新建立的磁碟區上啟用。所有AFF系統上所有現有和新建立的磁碟區均預設啟用所有內聯儲存效率功能。

儲存效率功能包括即時重複資料刪除、即時跨磁碟區重複資料刪除和即時壓縮、而且預設會在AFF 如表所示的各種系統上啟用。

預設情況下， AFF磁碟區上的資料壓縮行為處於啟用狀態。

Volume條件	預設啟用儲存效率功能		
	即時重複資料刪除技術	即時跨Volume重複資料刪除技術	即時壓縮
叢集升級	是的	是的	是的
將7-Mode移轉至叢集式VMware ONTAP ONTAP	是的	是的	是的
Volume搬移	是的	是的	是的
完整配置的Volume	是的	否	是的
加密磁碟區	是的	否	是的

下列例外情況適用於一或多項內嵌儲存效率功能：

- 只有讀寫磁碟區才能支援預設的內嵌儲存效率功能。
- 在啟用即時壓縮時、會忽略壓縮節約的Volume。
- 啟用即時資料壓縮時、會忽略已開啟後置處理重複資料刪除功能的磁碟區。
- 在已關閉Volume效率的磁碟區上、系統會覆寫現有的Volume效率原則設定、並將其設定為啟用純內嵌原則。

儲存效率視覺化

使用 `storage aggregate show-efficiency`命令顯示有關係統中所有聚合的儲存效率的資訊。

。 `storage aggregate show-efficiency` 命令有三種不同的檢視、可透過傳遞命令選項來叫用。

詳細了解 `storage aggregate show-efficiency`在"指令參考資料ONTAP" 。

預設檢視

預設檢視會顯示每個集合體的整體比率。

```
cluster1::> storage aggregate show-efficiency
```

詳細檢視

使用叫用詳細檢視 `-details` 命令選項。此檢視會顯示下列項目：

- 每個集合體的整體效率比率。
- 無快照的整體比率。
- 下列效率技術的比率分割： Volume 重複資料刪除， Volume 壓縮，快照，複本，資料壓縮及 Aggregate 內嵌重複資料刪除。

```
cluster1::> storage aggregate show-efficiency -details
```

進階檢視

進階檢視類似於詳細檢視、並同時顯示邏輯和實體使用的詳細資料。

您必須在進階權限層級執行此命令。使用切換至進階權限 `set -privilege advanced` 命令。

命令提示字元會變更為 `cluster::*>`。

```
cluster1::> set -privilege advanced
```

使用叫用進階檢視 `-advanced` 命令選項。

```
cluster1::*> storage aggregate show-efficiency -advanced
```

若要個別檢視單一集合體的比率、請叫用 `-aggregate` *`aggregate_name`* 命令。此命令可在管理層級以及進階權限層級執行。

```
cluster1::> storage aggregate show-efficiency -aggregate aggr1
```

如"指令參考資料ONTAP"需詳細 `set -privilege advanced`資訊，請參閱。

建立**Volume**效率原則以執行效率作業

建立 **Volume** 效率原則

您可以建立磁碟區效率原則來執行重複資料刪除或資料壓縮、然後在磁碟區上執行重複資料刪除、並使用指定工作排程 `volume efficiency policy create` 命令。

開始之前

您必須使用命令建立 cron 排程 `job schedule cron create`。如需管理 cron 排程的詳細資訊，請參閱"系統管理參考資料"。如"指令參考資料ONTAP"需詳細 `job schedule cron create`資訊，請參閱。

關於這項工作

具有預設預先定義角色的SVM管理員無法管理重複資料刪除原則。不過、叢集管理員可以使用任何自訂角色、修改指派給SVM管理員的權限。如需SVM管理員功能的詳細資訊、請參閱 "系統管理員驗證與RBAC"。

您可以在排定的時間執行重複資料刪除或資料壓縮作業、或建立具有特定持續時間的排程、或指定臨界值百分比、以等待新資料超過臨界值、然後觸發重複資料刪除或資料壓縮作業。此臨界值是磁碟區中使用之區塊總數的百分比。例如、當磁碟區上使用的區塊總數為50%時、如果您將磁碟區上的臨界值設定為20%、則當寫入磁碟區的新資料達到10%時、資料重複資料刪除或資料壓縮會自動觸發（使用50%區塊的20%）。如有需要、您可以從取得使用的區塊總數 `df` 命令輸出。

步驟

1. 使用 `volume efficiency policy create` 命令以建立 Volume 效率原則。

範例

下列命令會建立名為pol1的Volume Eff效率 原則、每天觸發效率作業：

```
volume efficiency policy create -vserver vs1 -policy pol1 -schedule daily
```

下列命令會建立名為pol2的Volume Effency原則、在臨界值百分比達到20%時觸發效率作業：

```
volume efficiency policy create -vserver vs1 -policy pol2 -type threshold -start
-threshold-percent 20%
```

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

將**Volume**效率原則指派給磁碟區

您可以使用 `volume efficiency modify`命令將效率原則指派給磁碟區、以執行重複資料刪除或資料壓縮作業。

開始之前

請務必做到 "建立 Volume 效率原則" 將其指派給磁碟區之前。

關於這項工作

如果將效率原則指派給SnapVault 某個不二重磁碟區、則在執行Volume Efficity作業時、只會考慮Volume Efficity優先順序屬性。工作排程會被忽略、重複資料刪除作業會在SnapVault 對靜態次要Volume進行遞增更新時執行。

步驟

1. 使用 `volume efficiency modify` 命令將原則指派給磁碟區。

範例

下列命令會指派名為的 Volume 效率原則 `new_policy` 至 Volume `VolA`：

```
volume efficiency modify -vserver vs1 -volume VolA -policy new_policy
```

如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

修改**Volume**效率原則

您可以修改磁碟區效率原則，以在不同的期間執行重複資料刪除和資料壓縮，或使用命令變更工作排程 `volume efficiency policy modify`。如"指令參考資料ONTAP"需詳

細 `volume efficiency policy modify`資訊，請參閱。

步驟

1. 使用 `volume efficiency policy modify` 修改 Volume 效率原則的命令。

範例

下列命令會修改名為policy1的Volume Eff效率 原則、以每小時執行一次：

```
volume efficiency policy modify -vserver vs1 -policy policy1 -schedule hourly
```

下列命令會將名為pol2的Volume Effency原則修改為臨界值30%：

```
volume efficiency policy modify -vserver vs1 -policy pol1 -type threshold -start
-threshold-percent 30%
```

在 ONTAP 中檢視 Volume 效率原則

您可以檢視 Volume 效率原則、包括名稱、排程、持續時間和說明。

關於這項工作

此命令 `volume efficiency policy show`用於顯示 Volume 效率原則。當您在叢集範圍中執行命令時、不會顯示叢集範圍原則。不過、您可以在 SVM 內容中檢視叢集範圍的原則。如"指令參考資料ONTAP"需詳細 `volume efficiency policy show`資訊，請參閱。

步驟

1. 使用 `volume efficiency policy show` 命令以檢視有關 Volume 效率原則的資訊。

   輸出取決於您指定的參數。如"指令參考資料ONTAP"需詳細 `volume efficiency policy show`資訊，請參閱。

範例

下列命令會顯示為 SVM VS1 建立的原則相關資訊：

```
volume efficiency policy show -vserver vs1
```

下列命令會顯示將持續時間設為 10 小時的原則：

```
volume efficiency policy show -duration 10
```

解除磁碟區效率原則與磁碟區的關聯

您可以取消磁碟區效率原則與磁碟區之間的關聯、以停止在磁碟區上執行任何進一步的排程型重複資料刪除和資料壓縮作業。一旦取消磁碟區效率原則的關聯、就必須手動觸發。

步驟

1. 使用 `volume efficiency modify` 命令、將 Volume 效率原則與磁碟區解除關聯。

範例

下列命令會取消 Volume 效率原則與 Volume Vola 的關聯：`volume efficiency modify -vserver vs1 -volume VolA -policy -`

如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

刪除Volume效率原則

您可以使用刪除 Volume 效率原則 `volume efficiency policy delete` 命令。

開始之前

您必須確保要刪除的原則不會與任何Volume相關聯。

您無法刪除_inline-only和_default_預先定義的效率原則。

步驟

1. 使用 `volume efficiency policy delete` 命令刪除 Volume EffEff可使用 原則。

範例

下列命令會刪除名為 policy1 的 Volume Eff可使用 原則： `volume efficiency policy delete -vserver vs1 -policy policy1`

如"指令參考資料ONTAP"需詳細 `volume efficiency policy delete`資訊，請參閱。

手動管理Volume效率作業

手動管理Volume效率作業總覽

您可以手動執行效率作業、來管理在磁碟區上執行效率作業的方式。

您也可以根據下列條件來控制效率作業的執行方式：

- 使用檢查點或不使用檢查點
- 對現有資料或只對新資料執行效率作業
- 必要時停止效率作業

您可以使用 `volume efficiency show` 命令 `schedule` 做為的價值 `-fields` 選項以檢視指派給磁碟區的排程。

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

手動執行效率作業

您可以手動在磁碟區上執行效率作業。當排程效率作業不適當時、您可以這麼做。

開始之前

視您想要手動執行的效率作業而定、您必須在磁碟區上啟用重複資料刪除、或同時啟用資料壓縮和重複資料刪除。

關於這項工作

此作業是使用 `volume efficiency start`命令來執行。當磁碟區上的溫度敏感儲存效率已啟用時、重複資料刪除功能會先執行、然後再執行資料壓縮。

重複資料刪除是一種背景程序、會在系統資源執行時耗用資源。如果磁碟區中的資料不經常變更、最好是減少重複資料刪除的執行頻率。在儲存系統上執行多項並行重複資料刪除作業、可提高系統資源的使用量。

每個節點最多可執行八個並行重複資料刪除或資料壓縮作業。如果排定更多效率作業、則會排入作業佇列。

從 ONTAP 9.13.1 開始、如果在磁碟區上啟用了對溫度敏感的儲存效率、您就可以對現有資料執行 Volume 效率、以利用連續包裝來進一步改善儲存效率。

手動執行效率

步驟

1. 在磁碟區上啟動效率作業： `volume efficiency start`

範例

+ 下列命令可讓您手動啟動重複資料刪除或重複資料刪除、然後在 Volume Vola 上執行邏輯壓縮和容器壓縮

+

```
volume efficiency start -vserver vs1 -volume VolA
```

重新入侵現有資料

若要利用 ONTAP 9.13.1 中針對已啟用溫度敏感儲存效率的磁碟區所推出的連續資料打包功能、您可以重新封裝現有資料。您必須處於進階權限模式才能使用此命令。

步驟

1. 設定權限等級： `set -privilege advanced`
2. 重新包裝現有資料： `volume efficiency inactive-data-compression start -vserver` *`vserver_name`* `-volume` *`volume_name`* `-scan-mode extended_recompression`

範例

```
volume efficiency inactive-data-compression start -vserver vs1 -volume
vol1 -scan-mode extended_recompression
```

相關資訊

- "在現有資料上手動執行效率作業"

檢查點和效率作業

檢查點用於內部記錄效率作業的執行程序。當效率作業因任何原因而停止（例如系統停止、系統中斷、重新開機、或是因為上次效率作業失敗或停止）且存在檢查點資料時、效率作業可以從最新的檢查點檔案恢復。

建立檢查點：

- 在作業的每個階段或子階段
- 當您執行時 `sis stop` 命令
- 當期間到期時

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

恢復暫停的效率作業

如果效率作業因系統停止、系統中斷或重新開機而停止、您可以從停止的同一點恢復效率作業。這有助於節省時間和資源、因為不需要從頭重新啟動作業。

關於這項工作

如果您只在磁碟區上啟用重複資料刪除、則重複資料刪除功能會在資料上執行。如果您在磁碟區上同時啟用重複資料刪除和資料壓縮、則資料壓縮會先執行、然後再執行重複資料刪除。

您可以使用命令來檢視磁碟區的檢查點詳細資料 `volume efficiency show`。如"指令參考資料ONTAP"需詳細 `volume efficiency show`資訊，請參閱。

根據預設、效率作業會從檢查點恢復。不過、如果檢查點對應於先前的效率作業（當 `volume efficiency start`-scan-old-data' 命令運行時間超過 24 小時，則效率操作不會自動從先前的檢查點恢復。在這種情況下、效率作業從一開始就開始。不過、如果您知道自上次掃描以來、 Volume 中並未發生重大變更、則可以使用強制從先前的檢查點繼續 `-use-checkpoint` 選項。

步驟

1. 使用 `volume efficiency start` 命令 `-use-checkpoint` 恢復效率作業的選項。

   下列命令可讓您恢復Volume Vola上新資料的效率作業：

   ```
   volume efficiency start -vserver vs1 -volume VolA -use-checkpoint true
   ```

   下列命令可讓您恢復Volume Vola上現有資料的效率作業：

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true -use
   -checkpoint true
   ```

   如"指令參考資料ONTAP"需詳細 `volume efficiency start`資訊，請參閱。

手動對現有資料執行效率作業

在啟用重複資料刪除、資料壓縮或資料壓縮之前、您可以手動對非溫度敏感儲存效率磁碟區中的資料執行效率作業。您可以使用 ONTAP 9 8 之前的 ONTAP 版本來執行這些作業。

關於這項工作

此作業是使用 `volume efficiency start`命令搭配 `-scan-old-data`參數來執行。此 `-compression` 選項不適用於 `-scan-old-data` 對溫度敏感的儲存效率磁碟區。非作用中的資料壓縮會自動在 ONTAP 9.8 及更新版本中、針對溫度敏感的儲存效率磁碟區、在預先存在的資料上執行。

如果您只在磁碟區上啟用重複資料刪除、則重複資料刪除功能會在資料上執行。如果您在磁碟區上啟用重複資料刪除、資料壓縮及資料壓縮、則資料壓縮會先執行、然後再執行重複資料刪除和資料壓縮。

在現有資料上執行資料壓縮時，資料壓縮作業預設會跳過重複資料刪除所共用的資料區塊，以及快照所鎖定的資料區塊。如果您選擇在共用區塊上執行資料壓縮、則會關閉最佳化功能、並擷取指紋資訊並再次用於共用。您可以在壓縮現有資料時變更資料壓縮的預設行為。

每個節點最多可同時執行八項重複資料刪除、資料壓縮或資料壓縮作業。其餘作業會排入佇列。

後處理程序壓縮無法在 AFF 平台上執行。系統會產生一則EMS訊息、通知您已跳過此作業。

如"指令參考資料ONTAP"需詳細 `volume efficiency start`資訊，請參閱。

步驟

1. 使用 `volume efficiency start -scan-old-data` 可手動在現有資料上執行重複資料刪除、資料壓縮或資料壓縮的命令。

   下列命令可讓您在Volume Vola中的現有資料上手動執行這些作業：

   ```
   volume efficiency start -vserver vs1 -volume VolA -scan-old-data true [-
   compression | -dedupe | -compaction ] true
   ```

相關資訊

- "手動執行效率作業"

使用排程來管理**Volume**效率作業

根據寫入的新資料量執行效率作業

您可以修改效率作業排程、以便在前一次效率作業超過指定臨界值百分比後、寫入磁碟區的新區塊數超過指定臨界值百分比時、執行重複資料刪除或資料壓縮。無論先前的效率作業是手動執行還是排程執行、都適用此選項。

關於這項工作

如果是 `schedule` 選項設定為 `auto`，排程的效率作業會在新資料量超過指定百分比時執行。預設臨界值為20%。此臨界值是效率作業已處理之區塊總數的百分比。

步驟

1. 使用 `volume efficiency modify` 命令 `auto@num` 修改臨界值百分比值的選項。

   `num` 為兩位數的數字、用於指定百分比。

範例

下列命令會將Volume Vola的臨界值百分比值修改為30%：

```
volume efficiency modify -vserver vs1 -volume -VolA -schedule auto@30
```

相關資訊

- "使用排程來執行效率作業"
- "Volume效率修改"

使用排程執行效率作業

您可以修改磁碟區上重複資料刪除或資料壓縮作業的排程。排程和磁碟區效率原則的組態選項是互不相容的。

關於這項工作

此作業是使用 `volume efficiency modify`命令來執行。如"指令參考資料ONTAP"需詳細 `volume efficiency modify`資訊，請參閱。

步驟

1. 使用 `volume efficiency modify` 修改捲上重複資料刪除或資料壓縮作業排程的命令。

範例

下列命令會修改Vola的效率作業排程、以便在星期一至星期五的晚上11點執行：

```
volume efficiency modify -vserver vs1 -volume VolA -schedule mon-fri@23
```

相關資訊

- "視寫入的新資料量而定、執行效率作業"

監控Volume效率作業

檢視效率作業和狀態

您可以檢視磁碟區是否啟用重複資料刪除或資料壓縮。您也可以檢視磁碟區上效率作業的狀態、狀態、壓縮類型和進度。

有兩項工作可供使用。兩者都使用命令 `volume efficiency show`。

檢視效率狀態

步驟

1. 檢視磁碟區上效率作業的狀態： `volume efficiency show`

   下列命令會顯示指派自適性壓縮類型之Volume Vola的效率作業狀態：

   ```
   volume efficiency show -instance -vserver vs1 -volume VolA
   ```

   如果已在Volume Vola上啟用效率作業、且作業閒置、則您可以在系統輸出中看到下列內容：

   ```
   cluster1::> volume efficiency show -vserver vs1 -volume VolA

     Vserver Name: vs1
      Volume Name: VolA
      Volume Path: /vol/VolA
            State: Enabled
           Status: Idle
         Progress: Idle for 00:03:20
   ```

判斷磁碟區是否包含依序打包的資料

您可以顯示已啟用連續封裝的磁碟區清單、例如當您需要還原至早於 9.13.1 的 ONTAP 版本時。您必須處於進

階權限模式才能使用此命令。

步驟

1. 設定權限等級： `set -privilege advanced`
2. 列出已啟用連續封裝的磁碟區：

```
volume efficiency show -extended-auto-adaptive-compression true
```

檢視效率空間節約效益

您可以檢視磁碟區上重複資料刪除和資料壓縮所節省的空間量。您可以這樣做來評估管理程序的有效性、或是作為容量規劃的一部分。

關於這項工作

您需要使用命令 `volume show`來顯示磁碟區上的空間節約。請注意，在計算磁碟區上所節省的空間時，快照空間並不包含在內。使用重複資料刪除技術不會影響磁碟區配額。配額會在邏輯層級報告、並保持不變。

步驟

1. 使用 `volume show` 命令、檢視使用重複資料刪除和資料壓縮在磁碟區上節省的空間。

範例

下列命令可讓您檢視在 Volume Vola 上使用重複資料刪除和資料壓縮所節省的空間： `volume show -vserver vs1 -volume VolA`

```
cluster1::> volume show -vserver vs1 -volume VolA

                                Vserver Name: vs1
                                 Volume Name: VolA

...
            Space Saved by Storage Efficiency: 115812B
       Percentage Saved by Storage Efficiency: 97%
                 Space Saved by Deduplication: 13728B
            Percentage Saved by Deduplication: 81%
                Space Shared by Deduplication: 1028B
                   Space Saved by Compression: 102084B
        Percentage Space Saved by Compression: 97%

...
```

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

檢視**FlexVol** 關於某個方面的效率統計資料

您可以檢視在 FlexVol volume 上執行的效率作業詳細資料。您可以這樣做來評估管理程序的有效性、或是作為容量規劃的一部分。

步驟

1. 使用 `volume efficiency stat` 用於查看 FlexVol 捲上效率操作統計資料的命令。

範例

下列命令可讓您檢視 Volume Vola 上效率作業的統計資料：
`volume efficiency stat -vserver vs1 -volume VolA`

```
cluster1::> volume efficiency stat -vserver vs1 -volume VolA

               Vserver Name: vs1
                Volume Name: VolA
                Volume Path: /vol/VolA
Inline Compression Attempts: 0
```

如"指令參考資料ONTAP"需詳細 `volume efficiency stat`資訊，請參閱。

停止**Volume**效率作業

您可以停止重複資料刪除或程序後壓縮作業。

關於這項工作

此操作使用命令 `volume efficiency stop`。此命令會自動產生檢查點。

步驟

1. 使用 `volume efficiency stop` 停止作用中重複資料刪除或後處理壓縮作業的命令。

   如果您指定 `-all` 選項會中止作用中和佇列中的效率作業。

範例

下列命令會停止Volume Vola目前作用中的重複資料刪除或後處理壓縮作業：

```
volume efficiency stop -vserver vs1 -volume VolA
```

下列命令會中止Volume Vola上的作用中和佇列重複資料刪除或後處理壓縮作業：

```
volume efficiency stop -vserver vs1 -volume VolA -all true
```

如"指令參考資料ONTAP"需詳細 `volume efficiency stop`資訊，請參閱。

有關從 **Volume** 中移除空間節約的其他資訊

您可以選擇移除在磁碟區上執行效率作業所節省的空間。不過、您必須有足夠的空間來容納反轉。

有幾種相關資源可協助您規劃及實作空間節約的移除作業。

相關資訊

- "如何在ONTAP 支援資料刪除技術、壓縮技術和實壓技術的過程中、查看如何節省空間。9"
- "如何在ONTAP 還原中復原儲存效率節約效益"

將一個磁碟區從一個SVM重新裝載到另一個SVM

準備將磁碟區從一個 SVM 重新裝載到另一個 SVM

Volume 重組作業可讓您將 NAS 或 SAN 磁碟區從一個 SVM 重新指派給另一個 SVM 、而不需要 SnapMirror 複本。確切的重新託管程序取決於所使用的用戶端存取傳輸協定和磁碟區類型。磁碟區重組是一項中斷營運的作業、可用於資料存取和磁碟區管理。

必須先符合下列條件、才能將磁碟區從一個 SVM 重新託管到另一個 SVM ：

- 磁碟區必須在線上
- Volume 傳輸協定必須是 SAN 或 NAS
  - 對於 NAS 傳輸協定磁碟區，該磁碟區不應是交會路徑的一部分，而且必須卸載
- 如果磁碟區處於 SnapMirror 關係中，則必須刪除關係，然後僅釋放關係資訊，或在磁碟區重新主機之前中斷關係
  - 您可以在磁碟區重新主機作業之後重新同步 SnapMirror 關係
- 來源和目的地 SVM 的 Vserver 子類型應相同
  - 磁碟區只能在同一子類型的 SVM 之間重新裝載
- 磁碟區不可為 FlexClone 或 FlexClone Parent
  - 必須先分割 FlexClones ，才能重新裝載父或複製 Volume

重新裝載 SMB Volume

您可以使用 SMB 通訊協定重新託管提供資料的磁碟區。若要允許用戶端在重新裝載作業之後繼續存取資料、您必須手動設定原則和相關規則。

關於這項工作

- 重新託管是一項顛覆性的作業。
- 如果重新託管作業失敗、您可能需要重新設定來源Volume上的Volume原則和相關規則。
- 如果來源SVM和目的地SVM Active Directory網域不同、您可能無法存取磁碟區上的物件。
- 從 ONTAP 9.8 開始，支援使用 NetApp Volume Encryption （ NVE ）重新裝載 Volume 。如果您使用內建金鑰管理程式、加密的中繼資料將會在重新主機作業期間修改。使用者資料不會變更。

  如果您使用的是 ONTAP 9.8 或更早版本、則必須在執行重新託管作業之前先取消對磁碟區的加密。

- 當來源SVM擁有本機使用者和群組時、設定的檔案和目錄（ACL）權限在磁碟區重新裝載作業之後將不再有效。

  稽核ACL（SACL）也是如此

- 重新裝載作業之後、下列磁碟區原則、原則規則和組態會從來源磁碟區遺失、必須在重新裝載的磁碟區上手

動重新設定：

- Volume與qtree匯出原則
- 防毒原則
- Volume效率原則
- 服務品質（QoS）原則
- Snapshot原則
- 配額規則
- NS-SWITCH與名稱服務組態匯出原則與規則
- 使用者和群組ID

開始之前

- Volume必須在線上。
- Volume管理作業（例如Volume Move或LUN Move）不得執行。
- 必須停止對正在重新託管的磁碟區的資料存取。
- 目標SVM的ns交換器和名稱服務組態必須設定為支援重新託管Volume的資料存取。
- 來源SVM和目的地SVM必須具有相同的Active Directory和重新分配DNS網域。
- 磁碟區的使用者ID和群組ID必須在目標SVM中可用、或在託管Volume上變更。

> 如果已設定本機使用者和群組、而且該磁碟區上有檔案和目錄、且已針對這些使用者或群組設定權限、則這些權限將不再有效。

步驟

1. 記錄CIFS共用的相關資訊、以免在磁碟區重新主機作業失敗時遺失CIFS共用的資訊。
2. 從父Volume卸載磁碟區：

   ```
   volume unmount
   ```

3. 切換至進階權限層級：

   ```
   set -privilege advanced
   ```

4. 在目的地SVM上重新裝載磁碟區：

   ```
   volume rehost -vserver source_svm -volume vol_name -destination-vserver
   destination_svm
   ```

5. 將磁碟區掛載到目的地SVM中適當的交會路徑下：

   ```
   volume mount
   ```

6. 為重新託管的Volume建立CIFS共用：

   ```
   vserver cifs share create
   ```

7. 如果來源SVM和目的地SVM之間的DNS網域不同、請建立新的使用者和群組。
8. 使用新的目的地SVM LIF及連線路徑、更新CIFS用戶端至重新裝載的Volume。

完成後

您必須手動重新設定重新裝載磁碟區上的原則和相關規則。

"SMB 組態"

"SMB與NFS多重傳輸協定組態"

重新裝載 **NFS Volume**

您可以使用 NFS 傳輸協定重新裝載資料的磁碟區。若要允許用戶端在重新裝載作業之後繼續存取資料、您必須將該磁碟區與 SVM 的匯出原則建立關聯、並手動設定原則和相關規則。

關於這項工作

- 重新託管是一項顛覆性的作業。
- 如果重新託管作業失敗、您可能需要重新設定來源Volume上的Volume原則和相關規則。
- 從 ONTAP 9.8 開始，支援使用 NetApp Volume Encryption （ NVE ）重新裝載 Volume 。如果您使用內建金鑰管理程式、加密的中繼資料將會在重新主機作業期間修改。使用者資料不會變更。

  如果您使用的是 ONTAP 9.8 或更早版本、則必須在執行重新託管作業之前先取消對磁碟區的加密。

- 重新裝載作業之後、下列磁碟區原則、原則規則和組態會從來源磁碟區遺失、必須在重新裝載的磁碟區上手動重新設定：
  - Volume與qtree匯出原則
  - 防毒原則
  - Volume效率原則
  - 服務品質（QoS）原則
  - Snapshot原則
  - 配額規則
  - NS-SWITCH與名稱服務組態匯出原則與規則
  - 使用者和群組ID

開始之前

- Volume必須處於線上狀態。
- Volume管理作業（例如Volume搬移或LUN搬移）不得執行。
- 必須停止對正在重新託管的磁碟區的資料存取。
- 目標SVM的ns交換器和名稱服務組態必須設定為支援重新託管Volume的資料存取。
- 磁碟區的使用者ID和群組ID必須在目標SVM中可用、或在託管Volume上變更。

步驟

1. 記錄NFS匯出原則的相關資訊、避免在磁碟區重新主機作業失敗時遺失NFS原則的相關資訊。
2. 從父Volume卸載磁碟區：

   ```
   volume unmount
   ```

3. 切換至進階權限層級：

   ```
   set -privilege advanced
   ```

4. 在目的地SVM上重新裝載磁碟區：

   ```
   volume rehost -vserver source_svm -volume volume_name -destination-vserver
   destination_svm
   ```

   目的地SVM的預設匯出原則會套用至重新裝載的Volume。

5. 建立匯出原則：

   ```
   vserver export-policy create
   ```

6. 將重新裝載磁碟區的匯出原則更新為使用者定義的匯出原則：

   ```
   volume modify
   ```

7. 將磁碟區掛載到目的地SVM中適當的交會路徑下：

   ```
   volume mount
   ```

8. 確認NFS服務正在目的地SVM上執行。
9. 恢復NFS對重新託管磁碟區的存取。
10. 更新NFS用戶端認證和LIF組態、以反映目的地SVM LIF。

    這是因為磁碟區存取路徑（LIF和接合路徑）已發生變更。

完成後

您必須手動重新設定重新裝載磁碟區上的原則和相關規則。如需詳細資訊、請參閱 "NFS 組態" 。

重新裝載 **SAN** 磁碟區

您可以重新託管 SAN 磁碟區、透過對應的 LUN 來提供資料。在目的地 SVM 中重新建立啟動器群組（ igroup ）之後、 Volume 重組作業可以自動重新對應同一 SVM 上的磁碟區。

關於這項工作

- 重新託管是一項顛覆性的作業。
- 如果重新託管作業失敗、您可能需要重新設定來源Volume上的Volume原則和相關規則。
- 從 ONTAP 9.8 開始，支援使用 NetApp Volume Encryption （ NVE ）重新裝載 Volume 。如果您使用內建金鑰管理程式、加密的中繼資料將會在重新主機作業期間修改。使用者資料不會變更。

如果您使用的是 ONTAP 9.8 或更早版本、則必須在執行重新託管作業之前先取消對磁碟區的加密。

- 重新裝載作業之後、下列Volume原則、原則規則和組態會從來源Volume遺失、必須在重新裝載的Volume上手動重新設定：
  - 防毒原則
  - Volume效率原則
  - 服務品質（QoS）原則
  - Snapshot原則
  - NS-SWITCH與名稱服務組態匯出原則與規則
  - 使用者和群組ID

開始之前

- Volume必須處於線上狀態。
- Volume管理作業（例如Volume搬移或LUN搬移）不得執行。
- 磁碟區或LUN上不得有作用中的I/O。
- 您必須確認目的地SVM沒有名稱相同但啟動器不同的igroup。

  如果igroup的名稱相同、則您必須在任一SVM（來源或目的地）中重新命名igroup。

- 您必須已啟用 `force-unmap-luns` 選項。
  - 的預設值 `force-unmap-luns` 選項是 `false`。
  - 設定時不會顯示警告或確認訊息 `force-unmap-luns` 選項 `true`。

步驟

1. 記錄目標Volume上的LUN對應資訊：

   `lun mapping show volume` *`volume`* `vserver` *`source_svm`*

   這是一個預防步驟、可避免在磁碟區重組失敗時遺失LUN對應的相關資訊。

   如"指令參考資料ONTAP"需詳細 `lun mapping show volume`資訊，請參閱。

2. 刪除與目標Volume相關的igroup。
3. 將目標磁碟區重新裝載至目的地SVM：

   `volume rehost -vserver` *`source_svm`* `-volume` *`volume_name`* `-destination-vserver` *`destination_svm`*

4. 將目標磁碟區上的 LUN 對應至適當的 igroup ：
   - Volume rehost 會在目標磁碟區上保留 LUN 、但 LUN 仍未對應。
   - 在對應LUN時使用目的地SVM連接埠集。
   - 如果是 `auto-remap-luns` 選項設定為 `true`， LUN 會在重新主機後自動對應。

重新託管 **SnapMirror** 關係中的 **Volume**

您可以重新託管定義為 SnapMirror 關係一部分的 Volume 。在重新建立關係之前、您需要考量幾個問題。

關於這項工作

- 重新託管是一項顛覆性的作業。
- 如果重新託管作業失敗、您可能需要重新設定來源Volume上的Volume原則和相關規則。
- 重新裝載作業之後、下列Volume原則、原則規則和組態會從來源Volume遺失、必須在重新裝載的Volume上手動重新設定：
  - Volume與qtree匯出原則
  - 防毒原則
  - Volume效率原則
  - 服務品質（QoS）原則
  - Snapshot原則
  - 配額規則
  - NS-SWITCH與名稱服務組態匯出原則與規則
  - 使用者和群組ID

開始之前

- Volume必須處於線上狀態。
- Volume管理作業（例如Volume搬移或LUN搬移）不得執行。
- 必須停止對正在重新託管的磁碟區的資料存取。
- 目標SVM的ns交換器和名稱服務組態必須設定為支援重新託管Volume的資料存取。
- 磁碟區的使用者ID和群組ID必須在目標SVM中可用、或在託管Volume上變更。

步驟

1. 記錄SnapMirror關係類型：

   ```
   snapmirror show
   ```

   這是預防步驟、可避免在磁碟區重組失敗時遺失SnapMirror關係類型的相關資訊。

2. 從目的地叢集刪除SnapMirror關係：

   ```
   snapmirror delete
   ```

   請勿中斷 SnapMirror 關係；否則，目的地磁碟區的資料保護功能將會遺失，而且在重新託管作業之後，無法重新建立關係。

3. 從來源叢集移除SnapMirror關係資訊：

   ```
   snapmirror release -relationship-info-only true
   ```

設定 `-relationship-info-only`參數以 `true`移除來源關係資訊，而不刪除快照。

4. 如果已掛載磁碟區，請將其卸載：

   ```
   volume unmount -vserver <source_svm> -volume <vol_name>
   ```

5. 切換至進階權限層級：

   ```
   set -privilege advanced
   ```

6. 在目的地SVM上重新裝載磁碟區：

   ```
   volume rehost -vserver <source_svm> -volume <vol_name> -destination-vserver
   <destination_svm>
   ```

7. 如果SVM對等關係不存在、請在來源SVM和目的地SVM之間建立SVM對等關係：

   ```
   vserver peer create
   ```

8. 在來源Volume與目的地Volume之間建立SnapMirror關係：

   ```
   snapmirror create
   ```

   您必須執行 `snapmirror create` 主控 DP Volume 的 SVM 命令。重新託管的Volume可以是SnapMirror關係的來源或目的地。

9. 重新同步SnapMirror關係。

相關資訊

- "設定"
- "SnapMirror"
- "Volume重新裝載"
- "Volume卸載"
- "Vserver對等端點建立"

ONTAP 中的 **Volume Rehost** 不支援的功能

有幾項 ONTAP 功能不支援 Volume Rehost 。在嘗試重新主機作業之前、您應該瞭解這些功能。

Volume Rehost 不支援下列功能：

- SVM DR
- 內部組態MetroCluster

  MetroCluster 組態也不支援將 Volume 複製為不同 SVM 上的 FlexClone Volume 。

- 資料量SnapLock

- NetApp Volume Encryption （ NVE ） Volume （ 9.8 之前版本的 ONTAP ）

  在 9.8 之前的 ONTAP 版本中、您必須先取消加密磁碟區、然後再重新裝載。Volume加密金鑰取決於SVM金鑰。如果將磁碟區移至另一個SVM、且在來源或目的地SVM上啟用多租戶金鑰組態、則磁碟區和SVM金鑰將不相符。

  從 ONTAP 9.8 開始，您可以使用 NVE 重新裝載磁碟區。

- 資料量FlexGroup
- 複製磁碟區

建議的**Volume**與檔案或**LUN**組態組合

建議的磁碟區和檔案或 **LUN** 組態組合總覽

根據您的應用程式和管理需求、FlexVol 您可以使用特定的功能組合來搭配使用。瞭解這些組合的效益和成本、有助於判斷適合您環境的組態。

建議使用下列磁碟區和LUN組態組合：

- 保留空間的檔案或LUN、具有完整磁碟區資源配置
- 非空間保留的檔案或LUN、採用精簡磁碟區資源配置
- 使用半厚磁碟區資源配置的空間保留檔案或LUN

您可以在LUN上搭配任何這些組態組合使用SCSI精簡配置。

保留空間的檔案或**LUN**、具有完整磁碟區資源配置

效益：

- 保證空間保留檔案內的所有寫入作業、不會因為空間不足而失敗。
- 磁碟區上的儲存效率和資料保護技術沒有任何限制。

成本與限制：

- 必須在Aggregate up Front預留足夠的空間、以支援最厚的已配置磁碟區。
- 在LUN建立時、從磁碟區配置的空間大小為LUN大小的兩倍。

非空間保留的檔案或**LUN**、採用精簡磁碟區資源配置

效益：

- 磁碟區上的儲存效率和資料保護技術沒有任何限制。
- 空間只會在使用時分配。

成本與限制：

- 寫入作業無法保證；如果磁碟區的可用空間不足、則寫入作業可能會失敗。

- 您必須有效管理Aggregate中的可用空間、以避免Aggregate耗盡可用空間。

使用半厚磁碟區資源配置的空間保留檔案或**LUN**

效益：

前端保留空間比大型磁碟區資源配置少、而且仍提供盡力寫入保證。

成本與限制：

- 使用此選項時、寫入作業可能會失敗。

  您可以適當平衡磁碟區中的可用空間與資料波動性、藉此降低此風險。

- 您無法仰賴資料保護物件的保留，例如快照， FlexClone 檔案和 LUN 。
- 您無法使用ONTAP 無法自動刪除的功能、包括重複資料刪除、壓縮及ODX/Copy卸載。

根據您的需求、判斷正確的磁碟區和 **LUN** 組態

回答幾個有關您環境的基本問題、有助於判斷FlexVol 最適合您環境的支援功能。

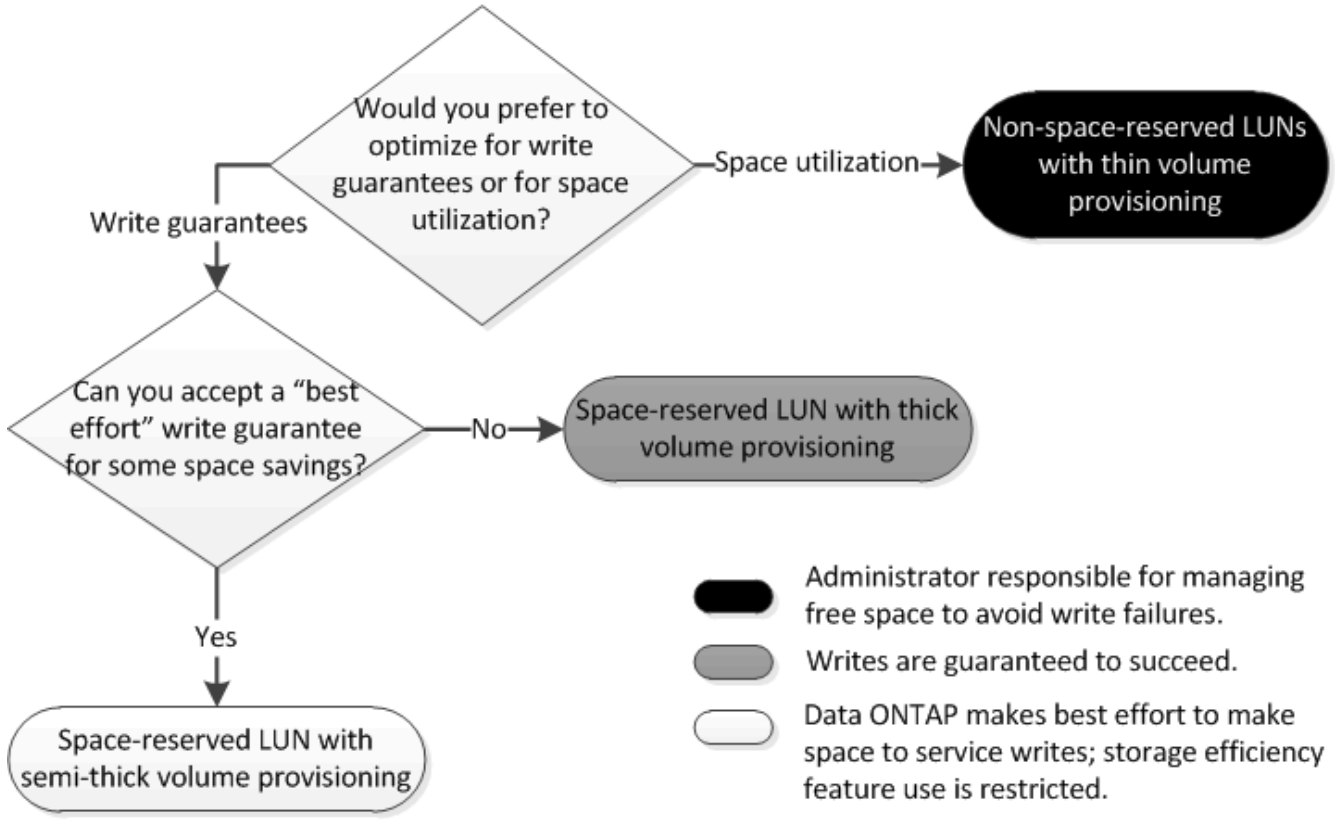
關於這項工作

您可以最佳化LUN和Volume組態、以達到最大的儲存使用率、或是保證寫入安全。根據您對儲存使用率的需求、以及您快速監控及補充可用空間的能力、您必須判斷FlexVol 適合您安裝的適用的版本。

您不需要為每個LUN分別建立磁碟區。

步驟

1. 請使用下列診斷樹來判斷環境的最佳Volume與LUN組態組合：



空間保留檔案的組態設定、或是具有完整配置磁碟區的**LUN**

您可以使用 FlexVol volume 和檔案或 LUN 組態的數種組態組合。這種以完整配置磁碟區為基礎的組合、可提供使用儲存效率技術的能力、而且不需要主動監控可用空間、因為前端已分配足夠的空間。

若要使用完整資源配置、在磁碟區中設定空間保留檔案或LUN、必須執行下列設定：

Volume設定	價值
保證	Volume
部分保留	100
Snapshot保留	任何
Snapshot自動刪除	選用
自動擴充	選用；如果啟用、則必須主動監控Aggregate可用空間。

檔案或**LUN**設定	價值
保留空間	已啟用

相關資訊

- "建議的Volume與檔案或LUN組態組合總覽"

非空間保留檔案或具有精簡配置磁碟區的 **LUN** 的設定

此一實體磁碟區與檔案或LUN組態組合需要最少的儲存容量預先配置、但需要主動式可用空間管理、以避免空間不足造成錯誤。FlexVol

若要在精簡配置的Volume中設定非空間保留的檔案或LUN、必須執行下列設定：

Volume設定	價值
保證	無
部分保留	0%
Snapshot保留	任何
Snapshot自動刪除	選用
自動擴充	選用

檔案或**LUN**設定	價值
保留空間	已停用

其他考量

當磁碟區或Aggregate空間不足時、寫入檔案或LUN的作業可能會失敗。

如果您不想主動監控磁碟區和Aggregate的可用空間、則應針對磁碟區啟用「自動擴充」、並將磁碟區的最大大小設為集合體的大小。在此組態中、您必須主動監控Aggregate可用空間、但不需要監控磁碟區中的可用空間。

空間保留檔案或**LUN**的組態設定、含半厚磁碟區資源配置

您可以使用 FlexVol volume 和檔案或 LUN 組態的數種組態組合。這種以半厚磁碟區資源配置為基礎的組合、需要比完全資源配置的組合更少的儲存設備才能預先配置。但它限制了您可以用於 Volume 的效率技術。此組態組合會盡力執行覆寫。

若要使用半厚資源配置、在磁碟區中設定空間保留LUN、必須執行下列設定：

Volume設定	價值
保證	Volume
部分保留	0%

Volume設定	價值
Snapshot保留	0%
Snapshot自動刪除	在上、只要承諾銷毀層級、就會顯示一個銷毀清單、其中包含所有物件、設定為Volume的觸發程序、以及所有啟用自動刪除的FlexClone LUN和FlexClone檔案。
自動擴充	選用；如果啟用、則必須主動監控Aggregate可用空間。

檔案或LUN設定	價值
保留空間	已啟用

技術限制

您無法將下列Volume儲存效率技術用於此組態組合：

- 壓縮
- 重複資料刪除
- ODX與FlexClone複製卸載
- FlexClone LUN和FlexClone檔案未標示為自動刪除（作用中複本）
- FlexClone子檔案
- ODX/Copy卸載

其他考量

使用此組態組合時、必須考量下列事實：

- 當支援該 LUN 的磁碟區空間不足時，保護資料（ FlexClone LUN 和檔案，快照）就會遭到銷毀。
- 當磁碟區的可用空間不足時、寫入作業可能會逾時並失敗。

根據預設AFF 、對不支援的平台啟用壓縮。您必須明確停用壓縮任何想要在AFF 某個平台上使用半厚資源配置的Volume。

相關資訊

- "建議的Volume與檔案或LUN組態組合總覽"

變更檔案或目錄容量時的注意事項與考量

ONTAP中**FlexVol**磁碟區允許的預設檔案數和最大檔案數

FlexVol磁碟區具有其可包含的預設檔案數和最大檔案數。如果您的資料需要大量文件，您可以將磁碟區上允許的使用者可見文件的數量增加到最大值。在繼續之前您應該了解限制

和注意事項。

磁碟區可以包含的使用者可見檔案的數量由該磁碟區的可用 inode 容量決定。 inode 是一種包含有關文件資訊的資料結構。

ONTAP會根據新建立的磁碟區的大小自動設定其預設和最大可用 inode 數，如下所示。

預設 **inode** 數量	最大 **inode** 數量
每 32 KB 卷大小 1 個	每 4 KB 卷大小 1 個

當磁碟區的大小增加時（無論是由管理員手動增加還是由 ONTAP 的自動調整大小功能自動增加）， ONTAP也會增加（如有必要）可用的 inode 數量，以便每 32 KB 磁碟區大小至少有 1 個 inode，直到磁碟區大小達到約 680 GB。

在ONTAP 9.12.1 及更早版本中，建立新磁碟區或調整現有磁碟區的大小（大於 680 GB）不會自動產生額外的 inode 容量。如果您需要的檔案數量超過任何大小卷的預設數量，則可以使用 `volume modify`指令將磁碟區的可用 inode 數量增加到最大值。

從ONTAP 9.13.1 開始，建立新磁碟區或調整現有磁碟區的大小時，即使磁碟區大於 680 GB，可用 inode 的預設數量也會設定為每 32 KB 磁碟區空間 1 個 inode。此比率將持續存在，直到磁碟區達到絕對 inode 最大值 2,040,109,451。

您還可以減少可用的 inode 數量。這不會改變分配給 inode 的空間量，但會降低公用 inode 檔案可以消耗的最大空間量。為 inode 分配空間後，該空間將永遠不會返回磁碟區。因此，不可能將最大 inode 數量降低到低於目前分配的 inode 數量。

更多資訊

- 確定卷的文件和 inode 使用情況
- "NetApp知識庫：常見問題 - ONTAP預設和最大檔案數（inode）"

FlexVol 磁碟區的最大目錄大小

您可以使用下列方法增加特定FlexVol volume的預設最大目錄大小： `-maxdir-size`選項 `volume modify`命令，但這樣做可能會影響系統效能。查看"NetApp知識庫：什麼是 maxdirsize？"。

如需深入瞭解FlexVol 依賴於機型的最大目錄大小、請造訪 "NetApp Hardware Universe"。

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

對節點根磁碟區和根集合體的限制

您應該瞭解管理節點根磁碟區和根 Aggregate 的限制。

節點的根磁碟區包含節點的特殊目錄和檔案。根 Volume 包含在根 Aggregate 中。

節點的根Volume FlexVol 是指由原廠安裝或安裝軟體安裝的一個現象。它保留給系統檔案、記錄檔和核心檔案。目錄名稱為 `/mroot`，只有技術支援人員才能透過系統 Shell 存取。節點根磁碟區的最小大小取決於平台模型。

- 下列規則管理節點的根Volume：
  - 除非技術支援人員指示您這麼做、否則請勿修改根磁碟區的組態或內容。
  - 請勿將使用者資料儲存在根Volume中。

    將使用者資料儲存在根磁碟區中、會增加HA配對中節點之間的儲存恢復時間。

  - 您可以將根磁碟區移至其他Aggregate。

    "將根磁碟區重新部署到新的Aggregate"

- 根Aggregate僅專供節點的根Volume使用。

  無法在根Aggregate中建立其他磁碟區。ONTAP

"NetApp Hardware Universe"

將根磁碟區重新定位至新的集合體

根置換程序會將目前的根Aggregate移轉到另一組磁碟、而不會造成中斷。您可能需要在磁碟更換或預防性維護程序中執行此動作。

關於這項工作

您可以在下列案例中、將根磁碟區的位置變更為新的Aggregate：

- 當根集合體不在您偏好的磁碟上時
- 當您想要重新排列連接至節點的磁碟時
- 當您執行更換EOS磁碟櫃的磁碟櫃時

步驟

1. 重新部署根Aggregate：

   ```
   system node migrate-root -node node_name -disklist disk_list -raid-type
   raid_type
   ```

   - 節點

     指定擁有您要移轉之根Aggregate的節點。

   - 磁碟清單

     指定要在其中建立新根Aggregate的磁碟清單。所有磁碟都必須是備援磁碟、且必須由同一個節點擁有。所需的磁碟數目下限取決於RAID類型。

   - * RAID類型*

     指定根Aggregate的RAID類型。預設值為 `raid-dp`。這是在進階模式中唯一支援的類型。

2. 監控工作進度：

```
job show -id jobid -instance
```

結果

如果所有的預先檢查都成功、命令會啟動根磁碟區置換工作並結束。

FlexClone 檔案和 FlexClone LUN 支援的功能

FlexClone 檔案和 FlexClone LUN 支援的功能

FlexClone 檔案和 FlexClone LUN 可搭配不同的 ONTAP 功能使用，例如重複資料刪除，快照，配額和 Volume SnapMirror 。

FlexClone 檔案和 FlexClone LUN 支援下列功能：

- 重複資料刪除
- 快照
- 存取控制清單
- 配額
- FlexClone Volume
- NDMP
- Volume SnapMirror
- 。 `volume move` 命令
- 保留空間
- HA 組態

使用 FlexClone 檔案和 FlexClone LUN 進行重複資料刪除

您可以在啟用重複資料刪除的磁碟區中、建立父檔案的FlexClone檔案或FlexClone LUN、以及父LUN、有效地使用資料區塊的實體儲存空間。

FlexClone檔案和LUN所使用的區塊共用機制也會用於重複資料刪除。您可以FlexVol 在磁碟區上啟用重複資料刪除功能、然後複製啟用重複資料刪除的磁碟區、以最大程度地節省整個實體磁碟區的空間。

> 執行時 `sis undo` 命令在啟用重複資料刪除的磁碟區上、您無法為位於該磁碟區的父檔案和父 LUN 建立 FlexClone 檔案和 FlexClone LUN 。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

快照如何與 FlexClone 檔案和 FlexClone LUN 搭配運作

快照與 FlexClone 檔案和 FlexClone LUN 之間有協同作用。如果您使用這些技術、您應該瞭解可能發生的情況、以及相關的限制。

建立 FlexClone 檔案和 LUN

您可以從現有的快照建立 FlexClone 檔案或 FlexClone LUN 。複本是以 FlexVol volume 中包含的父檔案和父 LUN 為基礎。

刪除快照

您無法手動刪除目前正在建立 FlexClone 檔案或 FlexClone LUN 的快照。快照會保持鎖定狀態，直到背景區塊共用程序完成為止。如果您嘗試刪除鎖定的快照，系統會顯示一則訊息，要求您在一段時間後重試該作業。在這種情況下、您需要繼續重新嘗試刪除作業。您可以在區塊共用完成後刪除快照。

依 **FlexClone** 檔案和 **FlexClone LUN** 繼承存取控制清單

FlexClone檔案和FlexClone LUN會繼承其父檔案和LUN的存取控制清單。

如果父檔案包含Windows NT串流、FlexClone檔案也會繼承串流資訊。但是、無法複製包含六個以上串流的父檔案。

配額如何與**FlexClone**檔案和**FlexClone LUN**搭配使用

您應該熟悉配額如何在使用 FlexClone 檔案和 FlexClone LUN 之前運作。

配額限制會套用至FlexClone檔案或FlexClone LUN的總邏輯大小。即使複製作業導致配額超出、也不會使區塊共用失敗。

當您建立FlexClone檔案或FlexClone LUN時、配額無法辨識任何空間節約效益。例如、如果您為父檔案建立10 GB的FlexClone檔案、則只會使用10 GB的實體空間、但配額使用率會記錄為20 GB（父檔案為10 GB 、FlexClone檔案為10 GB）。

如果建立FlexClone檔案或LUN導致超出群組或使用者配額、則只要FlexVol 該實體磁碟區有足夠空間容納該實體複本的中繼資料、即會成功完成複製作業。不過、該使用者或群組的配額已超額訂閱。

FlexClone 磁碟區及相關的 **FlexClone** 檔案和 **FlexClone LUN**

您可以為FlexVol 包含FlexClone檔案和FlexClone LUN及其父檔案或LUN的實體磁碟區建立FlexClone Volume。

FlexClone檔案或FlexClone LUN及其父檔案或位於FlexClone Volume中的LUN、仍會以其在父FlexVol 實體磁碟區中的相同方式、繼續共用區塊。事實上、所有FlexClone實體及其父實體都共用相同的基礎實體資料區塊、將實體磁碟空間使用量降至最低。

如果FlexClone磁碟區是從其父磁碟區分割而來、FlexClone檔案或FlexClone LUN及其父檔案或LUN會停止共用FlexClone磁碟區複製中的區塊。之後它們會以獨立檔案或LUN的形式存在。這表示磁碟區的實體複本所使用的空間比分割作業之前還要多。

NDMP如何與**FlexClone**檔案和**FlexClone LUN**搭配使用

NDMP可在邏輯層級與FlexClone檔案和FlexClone LUN搭配運作。所有FlexClone檔案或LUN都會備份為個別檔案或LUN。

當您使用NDMP服務來備份包含FlexVol FlexClone檔案或FlexClone LUN的qtree或支援的支援磁碟區時、父實體與複製實體之間的區塊共用不會保留、而且複製實體會以個別檔案或LUN的形式備份到磁帶。節省空間已遺失。因此、您要備份的磁帶應有足夠空間來儲存擴充的資料量。還原時、所有FlexClone檔案和FlexClone LUN都會還原為個別的實體檔案和LUN。您可以在磁碟區上啟用重複資料刪除、以還原區塊共用的優點。

從 FlexVol volume 的現有快照建立 FlexClone 檔案和 FlexClone LUN 時，除非在背景中執行區塊共用程序，否則您無法將磁碟區備份至磁帶。如果在進行區塊共用程序時、您在磁碟區上使用NDMP、系統會顯示一則訊息、要求您在一段時間後重試該作業。在這種情況下、您必須持續重試磁帶備份作業、以便在區塊共用完成之後成功。

Volume SnapMirror如何搭配**FlexClone**檔案和**FlexClone LUN**運作

將 Volume SnapMirror 與 FlexClone 檔案和 FlexClone LUN 搭配使用、有助於維持空間節約、因為複製的實體僅複寫一次。

如果FlexVol 某個實體磁碟區是Volume SnapMirror來源、且包含FlexClone檔案或FlexClone LUN、則Volume SnapMirror只會將共用實體區塊和少量中繼資料傳輸至Volume SnapMirror目的地。目的地只儲存實體區塊的一個複本、而此區塊會在父實體與複製實體之間共用。因此、目的地磁碟區是來源磁碟區的確切複本、而目的地磁碟區上的所有實體複本檔案或LUN則共用相同的實體區塊。

空間保留與**FlexClone**檔案和**FlexClone LUN**的搭配運作方式

使用 FlexClone 檔案和 FlexClone LUN 時、您應該瞭解 space reservation 屬性的運作方式。

根據預設、 FlexClone 檔案和 LUN 會分別從父檔案和父 LUN 繼承空間保留屬性。不過、如果 FlexVol volume 缺少空間、您可以在停用空間保留的情況下建立 FlexClone 檔案和 FlexClone LUN 。即使個別父項中的屬性已啟用、也可能發生這種情況。

請注意、如果 FlexVol volume 沒有足夠的空間來建立 FlexClone 檔案或 FlexClone LUN 、且其保留空間與父 LUN 相同、則複製作業將會失敗。

HA組態如何搭配**FlexClone**檔案和**FlexClone LUN**運作

HA組態支援FlexClone檔案與FlexClone LUN作業。

在HA配對中、您無法在進行接管或恢復作業時、在合作夥伴上建立FlexClone檔案或FlexClone LUN。在接管或恢復作業完成後、會恢復合作夥伴上所有擱置的區塊共用作業。

資料區管理FlexGroup

透過 CLI 瞭解 ONTAP FlexGroup Volume 管理

您可以設定、管理FlexGroup 及保護不只是為了擴充性和效能而建置的功能。支援垂直擴充的功能是提供高效能及自動負載分配的功能。FlexGroup

如果符合下列條件、您可以設定FlexGroup 此功能：

- 您想要使用最佳實務做法、而非探索每個可用選項。
- 您擁有叢集管理員權限、而非SVM管理員權限。

從 ONTAP 9.5 開始， FlexGroup Volume 取代 ONTAP 9.5 或更新版本不支援的 Infinite Volumes 。

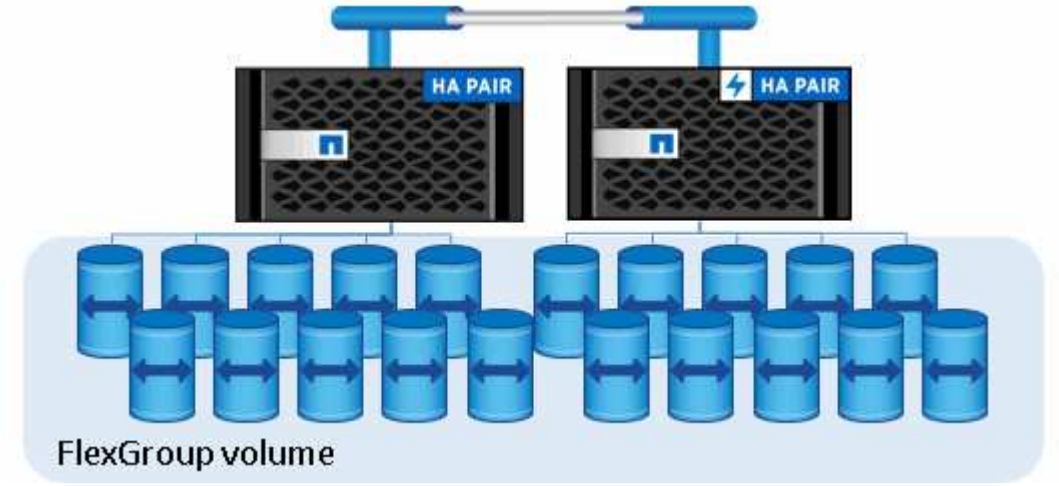
請參閱 "FlexGroup 磁碟區支援和不支援的組態" 以取得更多資訊。

相關資訊

關於功能的概念資訊FlexVol 適用於FlexGroup 功能區。關於「支援功能」和「功能」技術的資訊FlexVol 、請參閱《參考資料庫》和《技術報告》（TR）ONTAP ONTAP 。

瞭解 ONTAP FlexGroup Volume

支援垂直擴充的NAS容器、可提供高效能、以及自動分配負載和擴充性。FlexGroupFlexGroup Volume 包含多個成員磁碟區（組成區），可自動且透明地共用流量。_Member Volumes 是組成 FlexGroup Volume 的基礎 FlexVol Volume 。



NetApp提供下列優點：FlexGroup

- 高擴充性

  只要成員磁碟區數量不超過節點或叢集限制，就可以在叢集上佈建多個 FlexGroup 磁碟區。

  從 ONTAP 9.12.1P2 開始，單一 FlexGroup 磁碟區的最大容量為 60PB ， 10 節點叢集上有 4000 億個檔案"已啟用大容量支援"。如果不支援大容量磁碟區，則單一 FlexGroup 磁碟區的最大容量為 20PB 。

  > 雖然單一 FlexGroup 磁碟區的最大容量為 60PB （ 200 個成員磁碟區 x 300TB = 60PB ），但當成員磁碟區的使用容量維持在 80% 以下（ 200 個成員磁碟區 x 240TB = 48PB ）時，則可達到最佳效能。

- 高效能

  FlexGroup 磁碟區可以使用叢集的資源來處理具有高處理量和低延遲的工作負載。

- 簡化管理

  這個解決方法是將一個名稱空間容器當作一個容器來管理、其管理方式與支援的方式類似。FlexGroup FlexVol

ONTAP FlexGroup 磁碟區支援和不支援的組態

您應該注意ONTAP 到支援且FlexGroup 不支援ONTAP 的功能、這些功能可在支援的地方使用、而且不能在支援的地方使用。

ONTAP 9.18.1 及更高版本支援的功能

- 嵌套 QoS 策略支援以下對象對：
  - SVM 和FlexGroup磁碟區包含在 SVM 中
  - FlexGroup捲和卷內的 qtree

ONTAP 9.16.1 開始支援的功能

- 進階容量平衡

ONTAP 9.15.1 開始支援的功能

- 自動資源配置增強功能

ONTAP 9.14.1 開始支援的功能

- Snapshot 標記：支援使用命令在 FlexGroup 磁碟區上建立，修改及刪除快照標記（ SnapMirror 標籤和註解） `volume snapshot`。

ONTAP 9.13.1 開始支援的功能

- 自主勒索軟體保護（Arp）對於 FlexGroup Volume ，包括下列支援功能：
  - FlexGroup 擴充作業：新的成員磁碟區會繼承自主勒索軟體保護屬性。
  - FlexVol 轉 FlexGroup 轉換：使用主動式勒索軟體保護的 FlexVols 可轉換。
  - FlexGroup 重新平衡：在中斷和不中斷營運的重新平衡作業中、支援自主勒索軟體保護。
- 排程單一 FlexGroup 重新平衡作業。
- SnapMirror 扇出與 FlexGroup 磁碟區上的 SVM DR 的關係。支援展開至八個站台。

支援功能、從**ONTAP** 功能部件支援的版本起、從功能部件支援的版本

- 重新平衡FlexGroup
- 適用於本產品的SnapLock SnapVault
- SnapMirror雲端
- FabricPool 、 FlexGroup 和 SVM DR 搭配運作。（在早於 ONTAP 9.12.1 的版本中、其中任何兩項功能都能一起運作、但並非全部三項功能都能一起運作。）
- 大容量支援將 FlexGroup Volume 成員大小從最大 100TB 增加至最大 300TB 。

支援功能、從**ONTAP** 功能部件支援的版本起、從功能部件支援的版本

- 資料量SnapLock

不支援下列功能搭配使用下列功能的功能：SnapLock FlexGroup

- 合法持有
- 以事件為基礎的保留
- 適用於本產品的SnapLock SnapVault

您可以在SnapLock 整個過程中設定不一樣的功能。FlexGroup您無法在成員磁碟區層級設定 SnapLock 。

- 用戶端非同步目錄刪除

支援功能、從**ONTAP** 功能部件支援的版本從功能部件支援的版本

- 在 SVM DR 關係中，將 FlexVol volume 轉換為 FlexGroup Volume
- SVM DR FlexClone 支援 FlexGroup Volume

支援功能、從**ONTAP** 支援的功能僅從支援的功能

- SVM 災難恢復

  不支援複製 SVM DR 關係中的 FlexGroup Volume 。

- SnapMirror可將2個以上的關係（A到B、A到C）展開、最多可有8個扇出式分支。

  為 FlexGroup 磁碟區建立 SnapMirror 串聯和展開關係的考量事項

- SnapMirror將關係串聯至兩個層級（A至B至C）

  為 FlexGroup 磁碟區建立 SnapMirror 串聯和展開關係的考量事項

支援功能、從**ONTAP** 功能介紹到功能介紹

- 從FlexGroup SnapMirror資料庫或從udp目的地還原單一檔案
  - 還原作業可從FlexGroup 任何幾何的不還原量、到FlexGroup 任何幾何的不還原量
  - 每個還原作業只支援一個檔案
- 將磁碟區從 7-Mode 系統轉換為 FlexGroup 磁碟區

  欲了解更多信息，請參閱"NetApp知識庫：如何將過渡的FlexVol轉換為FlexGroup"。

- NFSv4.2
- 非同步刪除檔案和目錄
- 檔案系統分析（FSA）
- VMware vSphere資料存放區FlexGroup
- 其他支援使用NDMP備份及還原磁帶、包括下列功能：
  - NDMP可重新設定的備份擴充（RBE）和Snapshot Management Extension（SSME）
  - 環境變數exclude、而多重樹狀結構名稱支援FlexGroup 還原備份

- 引進ignore _CTIM_mtime環境變數以FlexGroup 進行還原備份
- 使用副檔名 0x2050 的 NDMP 快照恢復訊息、在 FlexGroup 中進行個別檔案還原傾印和還原工作階段會在升級或還原期間中止。

支援功能、從**ONTAP** 支援的功能從支援的功能

- FlexClone Volume
- NFSv4 和 NFSv4.1
- pNFS
- 使用NDMP進行磁帶備份與還原

  您必須注意FlexGroup 下列事項、才能在支援的情況下支援支援有關的功能：

  - 副檔名類別0x2050中的NDMP快照恢復訊息僅可用於恢復整個FlexGroup 整個整個版本。

    無法恢復使用無法恢復的個別檔案。FlexGroup

  - 不支援FlexGroup NDMP可重新啓動備份擴充（RBE）以供支援。
  - 不支援FlexGroup 環境變數exclude、也不支援多重樹狀結構名稱。
  - 。 `ndmpcopy` FlexVol 與 FlexGroup 磁碟區之間的資料傳輸支援命令。

    如果您從Data ONTAP 還原9.7回復至舊版、先前傳輸的遞增傳輸資訊將不會保留、因此您必須在還原後執行基礎複本。

- 適用於陣列整合的VMware vStorage API（VAAI）
- 將一個不只是一個的功能、更能將一個功能性的功能轉化FlexVol 為FlexGroup 一個功能
- 以作爲來源的來源卷的功能FlexGroup FlexCache

支援功能、從**ONTAP** 支援的功能僅從支援的功能

- 持續可用的SMB共用
- "內部組態MetroCluster"
- 重新命名 FlexGroup Volume (`volume rename` 命令）
- 縮減或縮減 FlexGroup Volume 的大小 (`volume size` 命令）
- 彈性調整規模
- NetApp Aggregate加密（NAE）
- Cloud Volumes ONTAP

支援功能、從**ONTAP** 支援的功能從支援的版本起算

- ODX複本卸載
- 儲存層級存取保護
- 增強功能、可變更SMB共用的通知

變更通知會針對變更傳送至父目錄的變更 `changenotify` 內容已設定、並用於變更該父目錄中的所有子目錄。

- FabricPool
- 配額強制執行
- qtree統計資料
- 適用於包含在Sfor文件的Adaptive QoS FlexGroup
- 僅快取；支援來源於支援的來源於支援的來源於支援的來源於支援的來源FlexCache FlexGroup ONTAP

支援功能、從**ONTAP** 支援的功能僅從支援的功能

- FPolicy
- 檔案稽核
- 適用於FlexGroup 整個過程的處理量層（QoS下限）和調適性QoS
- 處理量上限（QoS上限）和處理量層（QoS下限）、用於FlexGroup 支援包含在內的檔案

  您可以使用 `volume file modify` 用於管理與檔案相關聯的 QoS 原則群組的命令。

- 放寬SnapMirror限制
- SMB 3.x多通道

ONTAP 9.3 及更早版本支援的功能

- 防毒組態
- 變更SMB共用的通知

  只會針對變更的父目錄而傳送通知 `changenotify` 內容已設定。變更通知不會針對父目錄中子目錄的變更傳送。

- qtree
- 處理量上限（QoS上限）
- 在FlexGroup SnapMirror關係中、擴充來源的不只是資料來源的部分和目的地FlexGroup 的不只是資料
- 支援備份與還原SnapVault
- 統一化資料保護關係
- 自動擴充選項和自動縮小選項
- 擷取時納入的inode數
- Volume加密
- Aggregate即時重複資料刪除技術（跨Volume重複資料刪除技術）
- NetApp Volume加密（NVE）
- SnapMirror技術
- 快照
- 數位顧問

- 即時調適壓縮
- 即時重複資料刪除技術
- 即時資料精簡
- AFF
- 配額報告
- NetApp Snapshot技術
- 軟件（僅限部分）SnapRestore FlexGroup
- 混合式Aggregate
- 成員磁碟區移動
- 後處理重複資料刪除
- NetApp RAID-TEC 技術
- 每個Aggregate一致性點
- 在FlexGroup 同一個SVM中使用FlexVol SVM共享這個功能

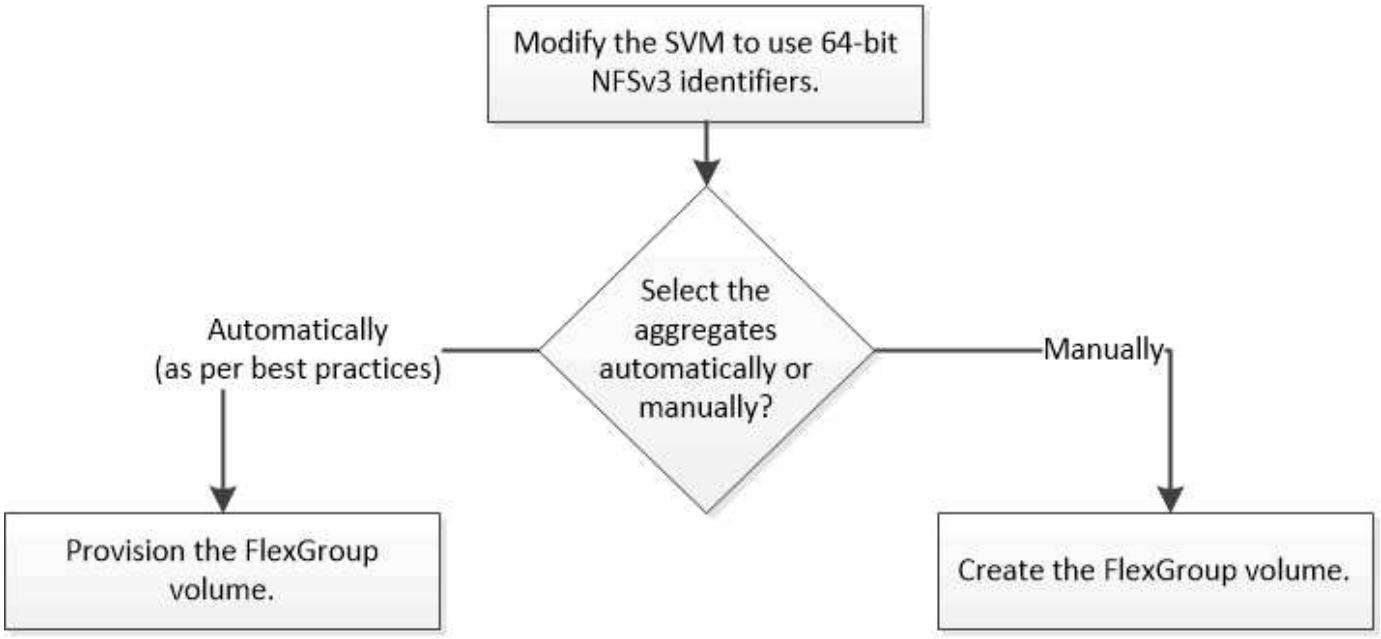
ONTAP 9 中不支援的 **FlexGroup Volume** 組態

不支援的傳輸協定	不支援的資料保護功能	其他不受支援ONTAP 的功能
• pNFS （ ONTAP 9 6 及更早版本） • SMB 1.0 • SMB 透明容錯移轉 （ ONTAP 9 技術及更早版本） • SAN	• 資料量SnapLock （ ONTAP 9 ： 10.1 及更早版本） • SM磁帶 • SnapMirror 同步 • 包含 FabricPools （ ONTAP 9.11.1 及更早版本）的 FlexGroup 磁碟區 SVM DR	• 遠端Volume陰影複製服務（VSS） • SVM資料移動性

設定流通量FlexGroup

ONTAP FlexGroup Volume 設定工作流程

您可以根據FlexGroup 最佳實務做法、在ONTAP 其中配置一個由VMware自動選取集合體的功能、以達到最佳效能、或FlexGroup 是手動選取集合體並將其設定為資料存取、以建立一個流通量。



開始之前

您必須在SVM允許的傳輸協定清單中新增NFS和SMB的SVM。

關於這項工作

您只能在FlexGroup 具有四個節點或更少節點的叢集上自動配置一個不含任何功能的資源。在具有四個以上節點的叢集上、您必須FlexGroup 手動建立一個流通量。

使用 **FlexGroups** 在 **ONTAP SVM** 上啟用 **64** 位元 **NFSv3** 標識符

若要支援FlexGroup 高檔案數的現象、並避免檔案ID衝突、您應該在必須FlexGroup 建立此現象磁碟區的SVM上啟用64位元檔案識別碼。

步驟

1. 登入進階權限層級： `set -privilege advanced`
2. 修改 SVM 以使用 64 位元 NFSv3 FSID 和檔案 ID ： `vserver nfs modify -vserver svm_name -v3-64bit-identifiers enabled`

```
cluster1::*> vserver nfs modify -vserver vs0 -v3-64bit-identifiers
enabled

Warning: You are attempting to increase the number of bits used for
NFSv3
         FSIDs and File IDs from 32 to 64 on Vserver "vs0". This could
         result in older client software no longer working with the
volumes
         owned by Vserver "vs0".
Do you want to continue? {y|n}: y

Warning: Based on the changes you are making to the NFS server on
Vserver
         "vs0", it is highly recommended that you remount all NFSv3
clients
         connected to it after the command completes.
Do you want to continue? {y|n}: y
```

完成後

所有用戶端都必須重新掛載。這是必要的、因為檔案系統ID會變更、而且用戶端在嘗試NFS作業時可能會收到過時的檔案處理訊息。

自動配置 ONTAP FlexGroup Volume

建立 FlexGroup Volume 時，您可以選擇讓 ONTAP 透過選取基礎本機層（集合體）來自動佈建 FlexGroup Volume 。本機層是根據最佳實務做法來選擇，以達到最佳效能和容量。

開始之前

叢集中的每個節點必須至少有一個本機層。

> 建立將分層儲存非使用中資料的 FlexGroup Volume 時，每個節點必須至少有一個本機層，且已啟用 FabricPool 。

關於這項工作

ONTAP 會選取兩個本機層，每個節點上可用空間最大，以建立 FlexGroup Volume 。如果兩個本機層不可用，ONTAP 會為每個節點選取一個本機層，以建立 FlexGroup Volume 。

從 ONTAP 9.15.1 開始，當您自動配置 FlexGroup Volume 時， ONTAP 會使用平衡放置（ BP ）來選擇本機層和 FlexGroup 成員（組成） Volume 配置。BP 的一個層面是在建立「無」保證（精簡配置）的 FlexGroup 磁碟區時，它如何限制過度資源配置的本機層。整體 FlexGroup 磁碟區的大小受限於本機層的可用空間量，但限制高於保證「 Volume 」（磁碟區）（完整配置）的 FlexGroup 磁碟區。當您使用 REST API 或 ONTAP CLI 建立 FlexGroup Volume `auto-provision-as` 時、資源配置可能會因為空間不足而失敗、因為這種限制。您可以建立較小的 FlexGroup 磁碟區、或使用參數來避免這種 "建立 FlexGroup Volume 並手動選取本機層" `aggr-list` 情況。

步驟

1. 配置FlexGroup 供應功能：

```
volume create -vserver svm_name -volume fg_vol_name -auto-provision-as
flexgroup -size fg_size [-encrypt true] [-qos-policy-group
qos_policy_group_name] [-support-tiering true] [-granular-data advanced]
```

從 ONTAP 9.16.1 開始，您可以 (`-granular-data advanced`在 CLI 中啟用"進階容量平衡"），在檔案大於 10GB 時，在多個 FlexGroup 成員磁碟區中寫入資料。

從 ONTAP 9.5 開始，您可以在啟用 FabricPool 的本機層上建立 FlexGroup 磁碟區。若要在啟用 FabricPool 的本機層上自動佈建 FlexGroup Volume ，您必須將參數設定 `-support-tiering`為 `true`。磁碟區保證一律必須設定為 `none` for FabricPool 。您也可以指定FlexGroup 針對該卷的分層原則和分層最低冷卻期。

"磁碟與Aggregate管理"

您可以指定 FlexGroup 磁碟區的處理量上限（ QoS 上限）。這會限制 FlexGroup 磁碟區所能耗用的效能資源。從ONTAP S得9.4開始、您可以指定處理量層（QoS下限）和適用於FlexGroup 整個過程的調適QoS。

"效能管理"

如果您想要在 FlexGroup 磁碟區上啟用加密，可以將參數設定 `-encrypt`為 `true`。若要建立加密磁碟區、您必須安裝Volume加密授權和金鑰管理程式。

> ⓘ 您必須在FlexGroup 建立時啟用對靜止磁碟區的加密。您無法在現有FlexGroup 的支援資料區啟用加密功能。

"加密閒置的資料"

。 `size` 參數指定 FlexGroup 磁碟區大小、單位為 KB 、 MB 、 GB 、 TB 或 PB 。

以下範例說明如何配置大小為 400 TB 的 FlexGroup Volume ：

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

以下範例說明如何建立QoS原則群組、以利處理量上限、以及如何將其套用FlexGroup 至某個流通量：

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

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -qos-policy-group pg-vs1
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

以下範例說明如何在啟用 FabricPool 的本機層上，配置大小為 400 TB 的 FlexGroup Volume ：

```
cluster-1::> volume create -vserver vs0 -volume fg -auto-provision-as
flexgroup -size 400TB -support-tiering true -tiering-policy auto
Warning: The FlexGroup "fg" will be created with the following number of
constituents of size 25TB: 16.
The constituents will be created on the following aggregates:
aggr1,aggr2
Do you want to continue? {y|n}: y
[Job 34] Job succeeded: Successful
```

FlexGroup 磁碟區是在叢集中的每個節點上建立，每個節點上有八個成員磁碟區。成員磁碟區會在每個節點上兩個最大的本機層之間平均分配。

根據預設、 FlexGroup Volume 是使用建立的 `volume` 空間保證設定、 AFF 系統除外。對於 AFF 系統、依預設會使用建立 FlexGroup Volume `none` 空間保證。

2. 使用連接路徑掛載 FlexGroup Volume ：

   `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg2
```

完成後

您應該從FlexGroup 用戶端掛載此功能。

如果您執行ONTAP 的是32位或更早版本的版本、而且儲存虛擬機器（SVM）同時設定了NFSv3和NFSv4、FlexGroup 則從用戶端安裝此支援卷可能會失敗。在這種情況FlexGroup 下、您必須在從用戶端掛載完這個版本時、明確指定NFS版本。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg2 /mnt/fg2
# ls /mnt/fg2
file1  file2
```

相關資訊

- "建立QoS原則群組"

建立 **ONTAP FlexGroup Volume**

您可以手動選取必須在其中建立 FlexGroup 磁碟區的本機層（集合體），然後指定每個本機層上的成員磁碟區（組成）數量，來建立 FlexGroup 磁碟區。

或者，您也可以選擇 ONTAP "自動配置"the FlexGroup Volume ，方法是選取本機層，並讓 ONTAP 根據最佳實務做法來設定成員磁碟區的數量，以達到最佳效能和容量。

關於這項工作

您必須知道在本機層中建立 FlexGroup Volume 所需的空間。

建立FlexGroup 一套用於FlexGroup 實現最佳效能結果的功能集區時、您必須考量下列準則：

- FlexGroup 磁碟區應使用位於相同硬體系統上的本機層。

  使用相同的硬體系統有助於在整個FlexGroup磁碟區中提供可預測的效能。注意：C 系列 r1 和 C 系列 r2 系統不是相同的系統。例如， AFF C80 r1 和AFF C80 r2 並不相同。

- FlexGroup 磁碟區應使用相同的磁碟類型和 RAID 群組組組態跨越本機層。

  為了達到一致的效能，您必須確保所有的本機層都是由所有 SSD ，所有 HDD 或所有 Flash Pool （混合式）本機層所組成。此外，本機層在 FlexGroup 磁碟區中的磁碟機和 RAID 群組數量應相同。

- 一個可跨越叢集的部分的供應量。FlexGroup

  不需要將一個穩定磁碟區設定為橫跨整個叢集、但這樣做可以更充分地利用可用的硬體資源。FlexGroup

- 建立 FlexGroup Volume 時，最好是部署 FlexGroup Volume 的本機層具有下列特性：
  - 在多個本機層中，可用空間應大致相同，尤其是在使用精簡配置時。
  - 在建立 FlexGroup Volume 之後，應保留約 3% 的可用空間給本機層中繼資料。
- 對於 FAS 系統，最好每個節點有兩個本機層，對於 AFF 系統，每個節點必須有一個本機層，才能用於 FlexGroup Volume 。
- 對於每個 FlexGroup Volume ，您應該建立至少八個成員磁碟區，這些磁碟區分佈在 FAS 系統上的兩個或多個本機層，以及 AFF 系統上的一或多個本機層上。
- 從ONTAP 支援的範圍僅為0.9.9.1開始、SnapMirror會展開兩FlexGroup 個以上的支援範圍、最多可支援八個扇形區。System Manager不支援SnapMirror串聯FlexGroup 式的等量資料磁碟區關係。
- 當您使用系統管理員建立FlexGroup區時， ONTAP會自動選擇建立FlexGroup磁碟區所需的本機層。
- 從ONTAP 供應儲存設備開始、預設會啟用QoS。您可以在資源配置程序期間或稍後時間停用 QoS 、或選擇自訂 QoS 原則。

開始之前

- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

系統管理員

使用系統管理器，您可以建立 FlexGroup 磁碟區。

步驟

1. 導航至“儲存”>“磁碟區”並選擇 + Add 。
2. 在*新增磁碟區*視窗中，輸入磁碟區名稱和大小，然後選擇*更多選項*。
3. 在*儲存和最佳化*部分中，選擇*在叢集中分發磁碟區資料（FlexGroup）*。

   如果您執行的是 ONTAP 9.8 或更新版本、而且想要停用 QoS 或選擇自訂 QoS 原則、請按一下 * 更多選項 * 、然後在 * 儲存與最佳化 * 下、選取 * 效能服務層級 * 。

4. 完成捲的剩餘資訊並選擇*儲存*。

CLI

1. 建立 FlexGroup Volume ：

```
volume create -vserver <svm_name> -volume <flexgroup_name> -aggr
-list aggr1,aggr2,.. -aggr-list-multiplier <constituents_per_aggr>
-size <fg_size> [-encrypt true] [-qos-policy-group
qos_policy_group_name] [-granular-data advanced]
```

   - 此 `-aggr-list`參數指定用於 FlexGroup 成員磁碟區的本機層清單。

     為了在 FlexGroup 磁碟區中保持一致的效能，所有本機層都必須使用相同的磁碟類型和 RAID 群組組態。

   - 此 `-aggr-list-multiplier`參數指定將在每個與參數一起列出的本機層上建立的成員磁碟區數量 `-aggr-list`。

     的預設值 `-aggr-list-multiplier` 參數為 4 。

   - 。 `size` 參數指定 FlexGroup 磁碟區大小、單位為 KB 、 MB 、 GB 、 TB 或 PB 。
   - 從 ONTAP 9.16.1 開始，您可以 (`-granular-data advanced`在 CLI 中啟用"進階容量平衡") ，在檔案大於 10GB 時，在多個 FlexGroup 成員磁碟區中寫入資料。
   - 從 ONTAP 9.5 開始，您可以使用啟用 FabricPool 的本機層來建立 FlexGroup Volume 。

     若要為 FabricPool 建立 FlexGroup Volume ，使用參數指定的所有本機層都 `-aggr-list`必須啟用 `FabricPool` 。使用 `FabricPool` 時，必須一律將 `Volume` 保證設定為 `none`。您也可以指定FlexGroup 針對該卷的分層原則和分層最低冷卻期。

     磁碟與Aggregate管理

   - 從ONTAP S得9.4開始、您可以指定處理量層（QoS下限）和適用於FlexGroup 整個過程的調適QoS。

     "效能管理"

- 您可以為FlexGroup磁碟區指定吞吐量上限 (QoS Max)，從而限制FlexGroup磁碟區可以消耗的效能資源。
- 如果您想要在 FlexGroup 磁碟區上啟用加密，可以將參數設定 `-encrypt`為 `true`。

  若要建立加密磁碟區、您必須安裝Volume加密授權和金鑰管理程式。

  > 您必須在FlexGroup 建立時啟用對靜止磁碟區的加密。您無法在現有FlexGroup 的支援資料區啟用加密功能。

  "加密閒置的資料"

```
cluster-1::> volume create -vserver vs0 -volume fg2 -aggr-list
aggr1,aggr2,aggr3,aggr1 -aggr-list-multiplier 2 -size 500TB

Warning: A FlexGroup "fg2" will be created with the following number
of constituents of size 62.50TB: 8.
Do you want to continue? {y|n}: y

[Job 43] Job succeeded: Successful
```

在上一個範例中，如果您要為 FabricPool 建立 FlexGroup Volume ，則所有本機層（ aggr1 ， aggr2 和 aggr3 ）都必須啟用 FabricPool 。使用連接路徑掛載 FlexGroup Volume ： `volume mount -vserver vserver_name -volume vol_name -junction-path junction_path`

```
cluster1::> volume mount -vserver vs0 -volume fg2 -junction-path /fg
```

完成後

您應該從FlexGroup 用戶端掛載此功能。

如果您執行ONTAP 的是32位或更早版本的版本、而且儲存虛擬機器（SVM）同時設定了NFSv3和NFSv4、FlexGroup 則從用戶端安裝此支援卷可能會失敗。在這種情況FlexGroup 下、您必須在從用戶端掛載完這個版本的時、明確指定NFS版本。

```
# mount -t nfs -o vers=3 192.53.19.64:/fg /mnt/fg2
# ls /mnt/fg2
file1  file2
```

相關資訊

"NetApp技術報告4571：NetApp FlexGroup 《最佳實務做法與實作指南》"

管理FlexGroup 功能

監控 ONTAP FlexGroup 磁碟區的空間使用量

您可以檢視FlexGroup 一個「不景區」及其構成部分、並監控FlexGroup 由「不景區」使用的空間。

關於這項工作

從支援的不只是功能性的9.6、ONTAP 還能靈活調整規模。如果某個現象正在耗盡空間、則會自動擴充一個包含在該問題上的資料、將該問題的任何其他部分壓縮成同等數量的可用空間。ONTAP FlexGroup FlexGroup彈性調整規模可避免因空間FlexGroup 不足而產生的空間不足錯誤。

> 從供應到支援的版本號為0.9.9.1、ONTAP 我們也提供邏輯空間報告與執行FlexGroup 功能、適用於各種版本的資料。如需更多資訊、請參閱 "磁碟區的邏輯空間報告與強制"。

步驟

1. 檢視 FlexGroup Volume 使用的空間及其組成： `volume show -vserver vserver_name -volume -style-extended [flexgroup | flexgroup-constituent]`

```
cluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1          -            online     RW        500GB
207.5GB   56%
```

```
ccluster-2::> volume show -vserver vs1 -volume-style-extended flexgroup-
constituent
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs1       fg1__0001    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0002    aggr1        online     RW      31.25GB
12.98GB   56%
vs1       fg1__0003    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0004    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0005    aggr1        online     RW      31.25GB
13.00GB   56%
vs1       fg1__0006    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0007    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0008    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0009    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0010    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0011    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0012    aggr1        online     RW      31.25GB
13.01GB   56%
vs1       fg1__0013    aggr3        online     RW      31.25GB
12.95GB   56%
vs1       fg1__0014    aggr3        online     RW      31.25GB
12.97GB   56%
vs1       fg1__0015    aggr3        online     RW      31.25GB
12.88GB   56%
vs1       fg1__0016    aggr1        online     RW      31.25GB
13.01GB   56%
16 entries were displayed.
```

您可以使用可用的空間和百分比空間來監控FlexGroup 使用的空間。

增加 **ONTAP FlexGroup** 磁碟區的大小

您可以透過在FlexGroup磁碟區的所有現有成員磁碟區（組成部分）中新增更多容量或透

過使用新成員磁碟區來擴充FlexGroup區來增加FlexGroup磁碟區的大小。 FlexGroup磁碟區不能有超過 200 個成員磁碟區。

如果需要，您也可以增加FlexGroup區中單一磁碟區的大小。

開始之前

集合體中必須有足夠的可用空間。

關於這項工作

如果您想要增加更多空間、可以增加FlexGroup 整個現象的整體大小。增加 FlexGroup 磁碟區的大小會調整 FlexGroup 磁碟區現有成員磁碟區的大小。

如果您想要提升效能、可以擴充FlexGroup 《不只是要用的功能、在下列情況下，您可能會想要擴充 FlexGroup Volume 並新增成員磁碟區：

- 新節點已新增至叢集。
- 已在現有節點上建立新的本機層（集合體）。
- FlexGroup 磁碟區的現有成員磁碟區已達到硬體的最大 FlexVol 大小（如果已啟用，則為 100TB 或 300TB "大容量支援"），因此 FlexGroup 磁碟區必須新增其他成員磁碟區，才能調整大小。

> ⓘ 如果您修改 FlexGroup 磁碟區以包含更多成員，則先前建立的快照將被視為“部分”，並且只能由來自 `.snapshot`目錄或“以前的版本”選項卡。
>
> 如果快照被視為“部分”，則不能用於 SnapRestore 操作。但是，部分快照可用於從 `.snapshot`目錄或“以前的版本”選項卡。

在早於 ONTAP 9.3 的版本中，建立 SnapMirror 關係後，請勿擴充 FlexGroup Volume 。如果FlexGroup 您在ONTAP 更新版本早於版本的SnapMirror關係之後擴充來源的來源的sels在於 版本9.3、則必須FlexGroup 再次執行基準傳輸至目的地的s0 Volume。從ONTAP 功能區9.3開始、您可以擴充FlexGroup SnapMirror關係中的功能區。

步驟

1. 視需要增加容量或效能以增加FlexGroup VMware FlexGroup Volume的大小：

如果您想要增加…	然後執行此動作…
功能FlexGroup	調整FlexGroup磁碟區的所有成員磁碟區的大小： `volume modify -vserver <svm_name> -volume <fg_name> -size <new_size>`

效能提升FlexGroup 至整個過程	新增成員磁碟區（組成）以擴充 FlexGroup 磁碟區： `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]` 的預設值 `-aggr-list-multiplier` 參數為 1 。 使用擴充 FlexGroup Volume "FabricPool"時，所有本機層（集合體）都必須附加到同一個雲端層。

假設現有的集合體（本機層）或成員磁碟區尚未達到其最大容量（每個 100 / 300 TB 或 20 億個檔案），最好是增加 FlexGroup 磁碟區的整體大小，而非增加額外的成員磁碟區。

只有當增加現有的磁碟區大小或檔案數不是選項，或 FlexGroup 正在擴充至新硬體時，才使用 Volume Expand 。應將相同數量的成員磁碟區新增至所有節點，以確保一致的效能。例如，如果現有的 FlexGroup 磁碟區有 8 個成員磁碟區，每個節點有四個成員磁碟區，則每個節點新增兩個成員會產生 12 個成員磁碟區，每個節點有六個成員磁碟區。

將新成員新增至新節點時，請嘗試維持現有節點中每個節點的成員磁碟區數量一致。例如，如果現有的 FlexGroup 磁碟區有 8 個成員磁碟區，每個節點有四個成員磁碟區，則如果 FlexGroup 磁碟區擴充至新節點，則應新增四個成員磁碟區，從而產生 12 個成員的 FlexGroup 磁碟區。

將新成員新增至 FlexGroup 磁碟區會變更擷取功能，以利新的空成員磁碟區，並影響新資料擷取的整體系統效能，直到新成員磁碟區與現有成員磁碟區達到平衡為止。

範例

- 增加現有成員磁碟區容量的範例 *

以下範例說明如何將20 TB空間新增至FlexGroup 一套功能不全的volX磁碟區：

```
cluster1::> volume modify -vserver svm1 -volume volX -size +20TB
```

如果 FlexGroup 磁碟區有 16 個成員磁碟區，則每個成員磁碟區的空間會增加 1.25 TB 。

- 新增成員磁碟區來改善效能的範例 *

以下範例顯示如何為 FlexGroup 磁碟區新增四個額外的成員卷，每個底層本機層（聚合）新增兩個 `fg1` ：

```
cluster1::> volume expand -vserver svm1 -volume fg1 -aggr-list aggr1,aggr2
-aggr-list-multiplier 2
```

新成員磁碟區的大小與現有成員磁碟區的大小相同。

增加單一卷的大小

如果要增加FlexGroup區中單一成員磁碟區的大小，可以使用 `volume resize`命令。

步驟

1. 增加單一FlexGroup成員磁碟區的大小：

   ```
   volume size -volume <volume_name> -vserver <svm1> -new-size <new_size>
   ```

   以下範例將FlexGroup成員磁碟區 FG_0003 的大小增加到 3.7GB：

   ```
   volume size -volume FG__0003 -vserver svm1 -new-size 3.7GB
   vol size: Volume "svm1:FG__0003" size set to 3.70g.
   ```

減少 **ONTAP FlexGroup** 磁碟區的大小

從ONTAP 功能性的9.6開始、FlexGroup 您可以將一個不符合目前大小的值重新調整成低於目前大小的值、以便從磁碟區中釋出未使用的空間。當您縮小FlexGroup 一個等量資料量時ONTAP 、系統會自動重新調整FlexGroup 所有的候數資料。

步驟

1. 檢查目前FlexGroup 的動態區大小：「Volume size -vserver *vserver_name*-volume *fa_name*」
2. 縮小FlexGroup 不必要的資料量：`volume size -vserver` *`vserver_name`* `-volume` *`fg_name new_size`*

   當您指定新的大小時、可以使用減號（-）來指定低於目前大小的值、或使用減號（-）來減少FlexGroup 目前的大小。

   > ⓘ 如果磁碟區已啟用自動壓縮 (`volume autosize` 命令）、將最小自動調整大小設為新的Volume 大小。

   下列範例顯示FlexGroup 名為volX的目前流通量大小、並將磁碟區大小重新調整為10TB：

   ```
   cluster1::> volume size -vserver svm1 -volume volX
   (volume size)
   vol size: FlexGroup volume 'svm1:volX' has size 15TB.

   cluster1::> volume size -vserver svm1 -volume volX 10TB
   (volume size)
   vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
   ```

   下列範例顯示FlexGroup 名為volX的目前流通量大小、並將此磁碟區的大小減少5TB：

```
cluster1::> volume size -vserver svm1 -volume volX
(volume size)
vol size: FlexGroup volume 'svm1:volX' has size 15TB.

cluster1::> volume size -vserver svm1 -volume volX -5TB
(volume size)
vol size: FlexGroup volume 'svm1:volX' size set to 10TB.
```

設定 **ONTAP FlexGroup** 磁碟區，以自動擴充和縮小其大小

從ONTAP 功能介紹9.3開始、您可以根據FlexGroup 目前所需的空間、將功能區設定為自動擴充和縮小。

開始之前

此版本必須在線上。FlexGroup

關於這項工作

您可以FlexGroup 在兩種模式中自動調整尺寸：

- 自動增加磁碟區大小 (`grow` 模式）

  如果FlexGroup Aggregate能夠提供更多空間、自動擴充功能有助於防止使用完這個功能。您可以設定磁碟區的最大大小。根據寫入磁碟區的資料量、相對於目前已用空間量和任何臨界值集、會自動觸發增加。

  根據預設、磁碟區可成長為啟用自動擴充的大小的120%。如果您需要確保磁碟區的大小可以大於該磁碟區、則必須據此設定磁碟區的最大大小。

- 自動縮小磁碟區大小 (`grow_shrink` 模式）

  自動壓縮可防止磁碟區大於所需的容量、釋放集合體中的空間供其他磁碟區使用。

  自動壓縮只能搭配自動擴充一起使用、以滿足不斷變化的空間需求、而且無法單獨使用。啟用自動壓縮功能時ONTAP 、支援使用者可自動管理磁碟區的縮減行為、以避免自動擴充和自動縮小動作的循環。

隨著磁碟區的成長、可以包含的檔案數量上限可能會自動增加。當磁碟區縮小時、其可包含的檔案數量上限將維持不變、而且磁碟區無法自動縮減至與其目前最大檔案數相對應的大小。因此、可能無法自動將磁碟區縮小至原始大小。

步驟

1. 設定磁碟區以自動擴充及縮小其大小： `volume autosize -vserver vserver_name -volume vol_name -mode [grow | grow_shrink]`

   您也可以指定用於擴充或縮減磁碟區的最大大小、最小大小和臨界值。

   以下命令啟用名為 `fg1` 。當磁碟區已滿70%時、該磁碟區的最大容量可擴充至5 TB。

```
cluster1::> volume autosize -volume fg1 -mode grow -maximum-size 5TB
-grow-threshold-percent 70
vol autosize: volume "vs_src:fg1" autosize settings UPDATED.
```

從**ONTAP FlexGroup**卷非同步刪除目錄

從ONTAP 9.8 開始，您可以非同步（即在背景）從 Linux 和 Windows 用戶端共用中刪除目錄。叢集和 SVM 管理員可以在FlexVol和FlexGroup磁碟區上執行非同步刪除操作。

關於這項工作

您必須是叢集管理員或使用進階權限模式的 SVM 管理員。

從 ONTAP 9 8 開始、您可以使用 ONTAP CLI 使用非同步刪除功能。從功能支援的9.9開始ONTAP 、您可以搭配System Manager使用此功能。如需此程序的詳細資訊，請參閱"根據 FSA 中的 ONTAP 分析採取糾正措施"。

從功能更新9.11.1開始ONTAP 、儲存管理員可以授予磁碟區的權限、讓NFS和SMB用戶端執行非同步刪除作業。如需更多資訊、請參閱 "管理用戶端權限、以非同步方式刪除目錄"。

您可以使用 `volume file async-delete show`指令檢查正在進行的非同步刪除作業的狀態，並且從ONTAP 9.17.1開始，也會顯示從客戶端發出的非同步刪除作業的狀態。

非同步刪除目錄

您可以使用 System Manager 或ONTAP CLI 非同步刪除目錄。

系統管理員

從**ONTAP** 功能上開始。**9.10.1**	在**ONTAP 9.9.1** 中
1. 選擇“儲存 **>** 磁碟區”並選擇所需的磁碟區名稱。 2. 在單一磁碟區頁面中，選擇「檔案系統」選項卡，然後選擇「資源管理器」標籤。 3. 在*Explorer*視圖中，選擇所需的目錄。 4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除 選項出現。 一次只能刪除一個物件。 刪除目錄和檔案時、新的儲存容量值不會立即顯示。	1. 選擇*儲存>磁碟區*。 2. 選取所需的磁碟區，然後選取 * 檔案總管 * 。 3. 在*Explorer*視圖中，選擇所需的目錄。 4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除 選項出現。

CLI

- 使用 CLI 執行非同步刪除 *

1. 進入進階權限模式：

   ```
   set -privilege advanced
   ```

2. 刪除 FlexVol 或 FlexGroup 磁碟區上的目錄：

   ```
   volume file async-delete start -vserver <SVM_name> -volume <volume_name>
   -path <file_path> -throttle <throttle>
   ```

   最小節流值為 10，最大值為 100,000，預設值為 5000。較低的節流值使用較少的資源，這會導致較慢的刪除速度，而較高的節流值使用較多的資源，但會導致較快的刪除速度。

   下列範例會刪除名為D2的目錄、該目錄位於名為D1的目錄中。

   ```
   cluster::*> volume file async-delete start -vserver vs1 -volume
   vol1 -path d1/d2
   ```

3. （可選）檢查正在進行的非同步刪除作業的狀態：

   ```
   volume file async-delete show
   ```

4. 確認目錄已刪除：

   ```
   event log show
   ```

   下列範例顯示成功刪除目錄時事件記錄的輸出。

```
cluster::*> event log show

Time                 Node              Severity      Event
-------------------- ----------------- -------------
---------------------------
7/7/2025 09:04:04    cluster-vsim      NOTICE
asyncDelete.message.success: Async delete job on path d1/d2 of
volume (MSID: 2162149232) was completed. Number of files deleted: 7,
Number of directories deleted: 5. Total number of bytes deleted:
135168.
```

+
如"指令參考資料ONTAP"需詳細 `event log show`資訊，請參閱。

取消目錄刪除作業

1. 進入進階權限模式：

   ```
   set -privilege advanced
   ```

2. 確認正在刪除目錄：

   ```
   volume file async-delete show
   ```

   如果顯示SVM、Volume、JobID和目錄路徑、您可以取消工作。

3. 取消目錄刪除：

   ```
   volume file async-delete cancel -vserver <SVM_name> -volume <volume_name>
   -jobid <job_id>
   ```

管理用戶端權限以使用 **FlexGroups** 非同步刪除 **ONTAP** 目錄

從ONTAP 9.11.1 開始，儲存管理員可以授予磁碟區上的權限，以允許 NFS 和 SMB 用戶端執行非同步刪除操作。當叢集啟用非同步刪除時，Linux 用戶端使用者可以使用 `mv`命令和 Windows 用戶端用戶可以使用 `rename`命令透過將目錄移至預設名為 .ontaptrashbin 的隱藏目錄來刪除指定磁碟區上的目錄。

權利是按卷授予的。 NFS 用戶端使用者應該在 NFS 用戶端上具有 root 存取權限，並在 NFS 匯出上具有超級使用者存取權限。

您只能移動目錄。您不能將檔案移至 .ontaptrashbin 目錄。

"了解如何使用ONTAP從FlexGroup卷非同步刪除目錄" 。

步驟

1. 從叢集 CLI 進入進階權限模式： `-privilege advance`
2. 在磁碟區的掛載點啟用用戶端非同步刪除，並且如果需要，為垃圾桶目錄提供備用名稱：

   `volume file async-delete client enable volume` *volname* `vserver` *vserverName* `trashbinname` *name*

   使用預設垃圾桶名稱的範例：

   ```
   cluster1::*> volume file async-delete client enable -volume v1 -vserver
   vs0

   Info: Async directory delete from the client has been enabled on volume
   "v1" in
         Vserver "vs0".
   ```

   指定替代垃圾桶名稱的範例：

   ```
   cluster1::*> volume file async-delete client enable -volume test
   -trashbin .ntaptrash -vserver vs1

   Success: Async directory delete from the client is enabled on volume
   "v1" in
         Vserver "vs0".
   ```

3. 確認已啟用用戶端非同步刪除：

   `volume file async-delete client show`

   範例：

   ```
   cluster1::*> volume file async-delete client show

   Vserver Volume      async-delete client TrashBinName
   ------------ ------------ ---------------------- -------------
   vs1          vol1         Enabled          .ntaptrash
   vs2          vol2         Disabled          -

   2 entries were displayed.
   ```

停用用戶端非同步目錄刪除

步驟

1. 在叢集CLI中、停用用戶端非同步目錄刪除：

   `volume file async-delete client disable volume *volname* vserver *vserverName*`

   範例：

```
cluster1::*> volume file async-delete client disable -volume vol1
-vserver vs1

       Success: Asynchronous directory delete client disabled
successfully on volume.
```

2. 確認用戶端非同步刪除已停用：

   `volume file async-delete client show`

   範例：

```
cluster1::*> volume file async-delete client show

Vserver      Volume      async-delete client      TrashBinName
------------ ------------ ----------------------- -------------
vs1          vol1         Disabled                -
vs2          vol2         Disabled                -

2 entries were displayed.
```

使用 **ONTAP FlexGroup** 磁碟區建立 **qtree**

從ONTAP 使用者名「0、3、3、3、3、2、3、2、3、3、2、3、FlexGroupqtree可讓FlexGroup 您將您的需求區塊分割成較小的區段、以便個別管理。

關於這項工作

- 如果來源FlexGroup 的SnapMirror Volume有qtree與SnapMirror的關係、則目的地叢集必須執行ONTAP 更新版本的《支援ONTAP qtree的支援》（一種版本的《支援qtree的》）。
- 從ONTAP 版本S9.5開始、FlexGroup 支援qtree統計資料以供支援使用。

步驟

1. 在 FlexGroup Volume 中建立 qtree ：

```
volume qtree create -vserver <vserver_name> -volume <volume_name> -qtree
<qtree_name>
```

您可以選擇性地指定qtree的安全樣式、SMB oplocks、UNIX權限及匯出原則。

```
cluster1::> volume qtree create -vserver vs0 -volume fg1 -qtree qtree1
-security-style mixed
```

相關資訊

"邏輯儲存管理"

使用 **ONTAP FlexGroup** 磁碟區配額

在僅供報告之用的情形下、您可以在適用配額規則的情形下、僅將配額規則套用至不適用配額限制的情形。ONTAP FlexGroup從功能介紹9.5開始ONTAP 、您可以對FlexGroup 套用至功能介紹區的配額規則強制限制。

關於這項工作

- 從功能表9.5開始ONTAP 、您可以指定FlexGroup 硬、軟和臨界值的等量配額、以供支援各種功能。

  您可以指定這些限制來限制空間量、特定使用者、群組或qtree可以建立的檔案數量、或兩者。配額限制會在下列情況下產生警告訊息：

  - 當使用量超過設定的軟體限制時ONTAP 、功能性功能會發出警告訊息、但仍允許進一步的流量。

    如果稍後使用量再次低於設定的軟體限制、系統會發出一則完全清除的訊息。

  - 當使用量超過設定的臨界值上限時ONTAP 、功能不均會發出第二則警告訊息。

    當使用量稍後低於設定的臨界值限制時、不會發出「完全清除」的管理訊息。

  - 如果使用量達到設定的硬限制、ONTAP 則無法拒絕流量、藉此防止資源進一步耗用。
- 在SnapMirror 9.5中ONTAP 、配額規則無法在FlexGroup SnapMirror關係的目的地SnapMirror磁碟區上建立或啟動。
- 在配額初始化期間、不會強制執行配額、而且配額初始化之後不會收到違反配額的通知。

  若要檢查配額初始化期間是否違反配額、您可以使用 `volume quota report` 命令。

配額目標和類型

配額有一種類型：可以是使用者、群組或樹狀結構。配額目標會指定套用配額限制的使用者、群組或qtree。

下表列出配額目標的類型、每個配額目標關聯的配額類型、以及每個配額目標的呈現方式：

配額目標	配額類型	目標的呈現方式	附註

使用者	使用者配額	UNIX使用者名稱UNIX UID Windows 2000之前版本的Windows使用者名稱 Windows SID	使用者配額可套用至特定磁碟區或qtree。
群組	群組配額	UNIX群組名稱UNIX Gid	群組配額可套用至特定磁碟區或qtree。 不適用以Windows ID為基礎的群組配額。ONTAP
qtree	樹狀結構配額	qtree名稱	樹狀結構配額會套用至特定的磁碟區、不會影響其他磁碟區中的qtree。
""	使用者配額 樹狀結構配額	雙引號（""）	配額目標為「」表示預設配額_。對於預設配額、配額類型取決於類型欄位的值。

超出配額限制時的現象**FlexGroup**

從功能介紹9.5開始ONTAP 、FlexGroup 支援在功能區上設定配額限制。在FlexGroup 執行配額限制的方式上、與FlexVol 使用此功能的整個過程相比、在這個過程中、存在一些差異。

超過配額限制時、可能會顯示下列行為：FlexGroup

- 在強制執行配額限制之前、由於拒絕更多流量、所以在使用完這個配額之前、使用於一個流通量的空間和檔案FlexGroup 可能會比設定的硬限制高出5%。

  為了提供最佳效能、ONTAP 在開始執行配額之前、使用的空間量可能會超過設定的硬限制、只有一小段距離。這項額外的空間使用量不會超過設定硬限制（1 GB或65536個檔案）的5%、以較低者為準。

- 達到配額上限後、如果使用者或系統管理員刪除部分檔案或目錄、使配額使用量低於上限、則後續的耗用配額檔案作業可能會以延遲的方式恢復（可能需要5秒才能恢復）。
- 當某個現象磁碟區的總空間和檔案使用量FlexGroup 超過設定的配額限制時、記錄事件記錄訊息可能會略有延遲。
- 如果某些部分包含整個流程、可能會出現「no space'」錯誤FlexGroup 、但無法達到配額限制。
- 配額目標上的作業、例如重新命名檔案或目錄、或在qtree之間移動檔案、而配額目標上已設定配額硬限制、相較FlexVol 於類似的功能、可能需要更長的時間。

執行配額的範例**FlexGroup**

您可以使用範例來瞭解如何在ONTAP 更新版本的版本中設定限制配額。

範例**1**：以磁碟限制強制執行配額規則

1. 您應該建立類型的配額原則規則 `user` 可達成的軟碟限制和硬碟限制。

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
default -volume FG -type user -target "" -qtree "" -disk-limit 1T -soft
-disk-limit 800G
```

2. 您可以檢視配額原則規則：

```
cluster1::> volume quota policy rule show -vserver vs0 -policy-name
default -volume FG

Vserver: vs0               Policy: default           Volume: FG

                                          Soft             Soft
                        User         Disk     Disk   Files    Files
Type   Target    Qtree  Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   ""        ""      off           1TB    800GB       -        -
-
```

3. 若要啟動新的配額規則、請在磁碟區上初始化配額：

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 您可以使用配額報告來檢視FlexGroup 有關此問題的磁碟使用量和檔案使用資訊。

```
cluster1::> volume quota report -vserver vs0 -volume FG
Vserver: vs0

                                    ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    root      50GB      -       1       -
FG                 user    *         800GB    1TB      0       -   *
2 entries were displayed.
```

在達到硬碟限制之後、配額原則規則目標（在此情況下為使用者）將無法寫入更多資料至檔案。

範例2：為多個使用者強制執行配額規則

1. 您應該建立類型的配額原則規則 `user`，其中在配額目標中指定多個使用者（ UNIX 使用者、 SMB 使用者或兩者的組合），且規則同時具有可達成的軟碟限制和硬碟限制。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target "rdavis,ABCCORP\RobertDavis" -qtree ""
-disk-limit 1TB -soft-disk-limit  800GB
```

2. 您可以檢視配額原則規則：

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user   "rdavis,ABCCORP\RobertDavis"  "" off  1TB  800GB  -  -
```

3. 若要啟動新的配額規則、請在磁碟區上初始化配額：

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 您可以驗證配額狀態是否為作用中：

```
cluster1::> volume quota show -vserver vs0 -volume FG
               Vserver Name: vs0
                Volume Name: FG
                Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. 您可以使用配額報告來檢視FlexGroup 有關此問題的磁碟使用量和檔案使用資訊。

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis,ABCCORP\RobertDavis
```

配額限制會在配額目標中列出的所有使用者之間共用。

達到硬碟限制後、配額目標中所列的使用者將無法寫入更多資料至檔案。

範例3：啟用使用者對應來強制執行配額

1. 您應該建立類型的配額原則規則 `user`下，使用指定 `UNIX` 使用者或 `Windows` 使用者做為配額目標 `user-mapping` 設定為 `on`並建立規則、同時設定可達成的軟碟限制和硬碟限制。

   UNIX 與 Windows 使用者之間的對應必須先使用設定 `vserver name-mapping create` 命令。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type user -target rdavis -qtree "" -disk-limit 1TB -soft
-disk-limit  800GB -user-mapping on
```

2. 您可以檢視配額原則規則：

```
cluster1::> quota policy rule show -vserver vs0 -policy-name default
-volume FG

Vserver: vs0               Policy: default           Volume: FG

                                                 Soft             Soft
                         User         Disk       Disk    Files    Files
Type    Target    Qtree  Mapping      Limit      Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
user    rdavis    ""     on            1TB    800GB       -        -
-
```

3. 若要啟動新的配額規則、請在磁碟區上初始化配額：

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

4. 您可以驗證配額狀態是否為作用中：

```
cluster1::> volume quota show -vserver vs0 -volume FG
              Vserver Name: vs0
               Volume Name: FG
               Quota State: on
                Scan Status: -
          Logging Messages: on
          Logging Interval: 1h
          Sub Quota Status: none
  Last Quota Error Message: -
Collection of Quota Errors: -
```

5. 您可以使用配額報告來檢視FlexGroup 有關此問題的磁碟使用量和檔案使用資訊。

```
cluster1::> quota report -vserver vs0 -volume FG
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
FG                 user    rdavis,ABCCORP\RobertDavis  0B  1TB  0  -
rdavis
```

配額限制會在配額目標中所列的使用者與其對應的Windows或UNIX使用者之間共用。

在達到硬碟限制之後、配額目標中列出的使用者及其對應的Windows或UNIX使用者都會遭到封鎖、無法將更多資料寫入檔案。

範例4：啟用配額時驗證qtree大小

1. 您應該建立類型的配額原則規則 `tree` 以及規則同時具有可達成的軟碟限制和硬碟限制。

```
cluster1::> quota policy rule create -vserver vs0 -policy-name default
-volume FG -type tree -target tree_4118314302 -qtree "" -disk-limit 48GB
-soft-disk-limit 30GB
```

2. 您可以檢視配額原則規則：

```
cluster1::> quota policy rule show -vserver vs0

Vserver: vs0               Policy: default           Volume: FG

                                              Soft             Soft
                         User         Disk     Disk   Files    Files
Type   Target    Qtree   Mapping     Limit    Limit   Limit    Limit
Threshold
-----  --------  ------- -------  --------  -------  ------  -------
---------
tree   tree_4118314302  "" -          48GB        -      20        -
```

3. 若要啟動新的配額規則、請在磁碟區上初始化配額：

```
cluster1::> volume quota on -vserver vs0 -volume FG -foreground true
[Job 49] Job succeeded: Successful
```

a. 您可以使用配額報告來檢視FlexGroup 有關此問題的磁碟使用量和檔案使用資訊。

```
cluster1::> quota report -vserver vs0
Vserver: vs0
----Disk---- ----Files----- Quota
Volume Tree Type ID Used Limit Used Limit Specifier
------- -------- ------ ------- ----- ----- ------ ------ ---------
FG tree_4118314302 tree 1 30.35GB 48GB 14 20 tree_4118314302
```

配額限制會在配額目標中所列的使用者與其對應的Windows或UNIX使用者之間共用。

4. 從 NFS 用戶端、使用 `df` 命令以檢視總空間使用量、可用空間和已用空間。

```
scsps0472342001# df -m /t/10.53.2.189/FG-3/tree_4118314302
Filesystem 1M-blocks Used Available Use% Mounted on
10.53.2.189/FG-3 49152 31078 18074 63% /t/10.53.2.189/FG-3
```

使用硬限制時、空間使用量會從NFS用戶端計算、如下所示：

- 總空間使用量=樹狀結構的硬限制
- 可用空間 = 硬限制減去 qtree 空間使用量
  在沒有硬限制的情況下、空間使用量會從 NFS 用戶端計算、如下所示：
- 空間使用量=配額使用量
- 總空間=磁碟區中配額使用量和實體可用空間的總和

5. 在SMB共用區中、使用Windows檔案總管來檢視總空間使用量、可用空間和已用空間。

在SMB共用區中、計算空間使用量時、您應注意下列考量事項：

- 使用者和群組的使用者配額硬限制會納入計算總可用空間的考量。
- 樹狀結構配額規則、使用者配額規則和群組配額規則的可用空間中、最小值會被視為SMB共用的可用空間。
- SMB的總空間使用量是可變的、取決於對應於樹狀結構、使用者和群組之間最小可用空間的硬限制。

在 **FlexGroup** 磁碟區上套用規則和限制

步驟

1. 爲目標創建配額規則： `volume quota policy rule create -vserver vs0 -policy-name quota_policy_of_the_rule -volume flexgroup_vol -type {tree|user|group} -target target_for_rule -qtree qtree_name [-disk-limit hard_disk_limit_size] [-file-limit hard_limit_number_of_files] [-threshold threshold_disk_limit_size] [-soft-disk-limit soft_disk_limit_size] [-soft-file-limit soft_limit_number_of_files]`
   - 配額目標類型可以是 `user`， `group`或 `tree`是 FlexGroup Volume 。

- 建立FlexGroup 適用於整個過程的配額規則時、路徑不支援作為目標路徑。
- 從ONTAP 功能表9.5開始、您可以指定硬碟限制、硬碟檔案限制、軟碟限制、軟式檔案限制、FlexGroup 以及針對功能表磁碟區的臨界值限制配額。

  在《支援範圍》9.4及更早版本中、當您建立適用於此功能的配額規則時、無法指定磁碟限制、檔案限制、磁碟限制臨界值、軟碟限制或軟式檔案限制。ONTAP FlexGroup

下列範例顯示要為使用者目標類型建立的預設配額規則：

```
cluster1::> volume quota policy rule create -vserver vs0 -policy-name
quota_policy_vs0_1 -volume fg1 -type user -target "" -qtree ""
```

以下範例顯示正在為qtree命名為qtree1建立樹狀結構配額規則：

```
cluster1::> volume quota policy rule create -policy-name default -vserver
vs0 -volume fg1 -type tree -target "qtree1"
```

1. 啟動指定 FlexGroup Volume 的配額：`volume quota on -vserver svm_name -volume flexgroup_vol -foreground true`

```
cluster1::> volume quota on -vserver vs0 -volume fg1 -foreground true
```

1. 監控配額初始化的狀態：`volume quota show -vserver svm_name`

FlexGroup Volume 可能會顯示 `mixed` 狀態、表示所有組成 Volume 尚未處於相同狀態。

```
cluster1::> volume quota show -vserver vs0
                                        Scan
Vserver    Volume        State          Status
---------  ------------  -------------  ------
vs0        fg1           initializing       95%
vs0        vol1          off                 -
2 entries were displayed.
```

1. 檢視具有作用中配額的 FlexGroup Volume 配額報告：`volume quota report -vserver svm_name -volume flexgroup_vol`

   您無法使用指定路徑 `volume quota report` FlexGroup Volume 的命令。

   以下範例顯示了 FlexGroup 磁碟區的使用者配額 `fg1` ：

```
cluster1::> volume quota report -vserver vs0 -volume fg1
  Vserver: vs0
                                       ----Disk----  ----Files-----
Quota
  Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
  -------  --------  ------  -------  -----  -----  ------  ------
---------
  fg1                user    *           0B      -       0       -   *
  fg1                user    root       1GB      -       1       -   *
  2 entries were displayed.
```

以下範例顯示了 FlexGroup 磁碟區的樹配額 `fg1` ：

```
cluster1::> volume quota report -vserver vs0 -volume fg1
Vserver: vs0

                                     ----Disk----  ----Files-----   Quota
Volume   Tree      Type    ID        Used  Limit    Used   Limit
Specifier
-------  --------  ------  -------  -----  -----  ------  ------
---------
fg1      qtree1  tree      1         68KB      -      18       -
qtree1
fg1              tree      *           0B      -       0       -   *
2 entries were displayed.
```

結果

配額規則和限制會套用至 FlexGroup 磁碟區。

使用量可能會比設定的硬限制高出5%、ONTAP 而在執行此配額之前、會拒絕更多流量。

相關資訊

- "指令參考資料ONTAP"

在 ONTAP FlexGroup 磁碟區上實現儲存效率

您可以一起執行重複資料刪除和資料壓縮、或是獨立在FlexGroup 某個支援區上執行、以達到最佳的空間節約效益。

開始之前

此版本必須在線上。FlexGroup

步驟

1. 在 FlexGroup 磁碟區上實現儲存效率： `volume efficiency on -vserver svm_name -volume volume_name`

   儲存效率作業可在FlexGroup 所有的功能上啟用。

   如果FlexGroup 在磁碟區上啟用儲存效率之後、擴充了一個支援功能、則新的成員會自動啟用儲存效率。

2. 使用在 FlexGroup 磁碟區上啟用所需的儲存效率操作 `volume efficiency modify` 命令。

   您可以在FlexGroup 支援即時重複資料刪除技術、後置重複資料刪除技術、即時資料壓縮、以及在支援後置處理的情況下、在支援內嵌資料刪除技術的情況下您也可以設定壓縮類型（次要或調適）、並為FlexGroup 該磁碟區指定排程或效率原則。

3. 如果您未使用排程或效率原則來執行儲存效率作業、請開始效率作業： `volume efficiency start -vserver svm_name -volume volume_name`

   如果在磁碟區上啟用重複資料刪除和資料壓縮、則資料壓縮會先執行、然後再執行重複資料刪除。如果FlexGroup 任何效率作業已在該磁碟區上啟用、則此命令會失敗。

4. 驗證 FlexGroup 磁碟區上啟用的效率作業： `volume efficiency show -vserver svm_name -volume volume_name`

```
cluster1::> volume efficiency show -vserver vs1 -volume fg1
             Vserver Name: vs1
              Volume Name: fg1
              Volume Path: /vol/fg1
                    State: Enabled
                   Status: Idle
                 Progress: Idle for 17:07:25
                     Type: Regular
                 Schedule: sun-sat@0

...

             Compression: true
      Inline Compression: true
Incompressible Data Detection: false
      Constituent Volume: false
Compression Quick Check File Size: 524288000
           Inline Dedupe: true
         Data Compaction: false
```

使用快照保護 **ONTAP FlexGroup** 磁碟區

您可以建立自動管理快照建立的快照原則，也可以手動建立 FlexGroup 磁碟區的快照。只有在 ONTAP 能夠為 FlexGroup Volume 的每個組成部份成功建立快照之後，才會為 FlexGroup Volume 建立有效的快照。

關於這項工作

- 如果您有多個 FlexGroup 磁碟區與快照原則相關聯，則應確保 FlexGroup 磁碟區排程不會重疊。
- 從 ONTAP 9.8 開始， FlexGroup 磁碟區支援的最大快照數為 1023 。

> 從 ONTAP 9.8 開始， `volume snapshot show` FlexGroup Volume 命令會使用邏輯區塊來報告快照大小，而非計算最年輕的擁有區塊。這種新的大小計算方法可能會使快照大小看起來大於舊版 ONTAP 的計算。

步驟

1. 建立快照原則或手動建立快照：

如果您想要建立…	輸入此命令…
Snapshot原則	`volume snapshot policy create` 與 FlexGroup 磁碟區快照原則相關的排程，間隔必須大於 30 分鐘。 建立 FlexGroup Volume 時， `default`快照原則會套用至 FlexGroup Volume 。
手動快照	`volume snapshot create` 為 FlexGroup Volume 建立快照之後，您就無法修改快照的屬性。如果您想要修改屬性，您必須刪除快照，然後重新建立快照。

建立快照時，用戶端對 FlexGroup Volume 的存取會短暫停頓。

1. 確認已為 FlexGroup Volume 建立有效的快照： `volume snapshot show -volume volume_name -fields state`

```
cluster1::> volume snapshot show -volume fg -fields state
vserver volume snapshot                state
------- ------ ---------------------- -----
fg_vs   fg     hourly.2016-08-23_0505 valid
```

2. 檢視 FlexGroup Volume 組成要素的快照： `volume snapshot show -is-constituent true`

```
cluster1::> volume snapshot show -is-constituent true

---Blocks---
Vserver  Volume   Snapshot                                  Size Total%
Used%
-------- -------- ------------------------------------ -------- ------
-----
fg_vs    fg__0001
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0002
                  hourly.2016-08-23_0505                    72MB     0%
27%
         fg__0003
                  hourly.2016-08-23_0505                    72MB     0%
27%
...
         fg__0016
                  hourly.2016-08-23_0505                    72MB     0%
27%
```

從 **ONTAP FlexGroup** 磁碟區移除組成區

您可以將 FlexGroup Volume 的組成要素從一個集合移到另一個集合、以便在某些組成要素遇到更多流量時、平衡負載。移動成員也有助於釋出集合體上的空間、以調整現有成員的大小。

開始之前

若要移動FlexGroup SnapMirror關係中的某個部分、您必須已初始化SnapMirror關係。

關於這項工作

當擴充了整個過程的內容時、您無法執行Volume Move作業FlexGroup 。

步驟

1. 識別您要移動的 FlexGroup Volume 組成：

   ```
   volume show -vserver svm_name -is-constituent true
   ```

```
cluster1::> volume show -vserver vs2 -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vs2       fg1          -            online     RW        400TB
15.12TB   62%
vs2       fg1__0001    aggr1        online     RW         25TB
8.12MB   59%
vs2       fg1__0002    aggr2        online     RW         25TB
2.50TB   90%
...
```

2. 識別可將 FlexGroup Volume 組成移至的集合體：

   `volume move target-aggr show -vserver svm_name -volume vol_constituent_name`

   您選取的Aggregate中的可用空間必須大於FlexGroup 您正在移動的各個版本的大小。

```
cluster1::> volume move target-aggr show -vserver vs2 -volume fg1_0002
Aggregate Name   Available Size   Storage Type
--------------   --------------   ------------
aggr2            467.9TB          hdd
node12a_aggr3    100.34TB         hdd
node12a_aggr2    100.36TB         hdd
node12a_aggr1    100.36TB         hdd
node12a_aggr4    100.36TB         hdd
5 entries were displayed.
```

3. 驗證 FlexGroup Volume 組成是否可以移至預期的 Aggregate ：

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name -perform-validation-only true`

```
cluster1::> volume move start -vserver vs2 -volume fg1_0002 -destination
-aggregate node12a_aggr3 -perform-validation-only true
Validation succeeded.
```

4. 移動 FlexGroup Volume 組成：

   `volume move start -vserver svm_name -volume vol_constituent_name -destination -aggregate aggr_name [-allow-mixed-aggr-types {true|false}]`

   磁碟區移動作業會以背景程序的形式執行。

從 ONTAP 9.5 開始、您可以將 FlexGroup Volume 組成要素從 Fabric Pool 移至非 Fabric Pool 、或是透過設定來將其移至非 Fabric Pool `-allow-mixed-aggr-types` 參數至 `true`。依預設 `-allow-mixed-aggr-types` 選項設定為 `false`。

您無法使用 `volume move` 在 FlexGroup 磁碟區上啟用加密的命令。

```
cluster1::> volume move start -vserver vs2 -volume fg1_002 -destination
-aggregate node12a_aggr3
```

如果磁碟區移動作業因使用中的 SnapMirror 作業而失敗，您應該使用命令來中止 SnapMirror 作業 `snapmirror abort -h`。在某些情況下、SnapMirror中止作業也可能失敗。在這種情況下、您應該中止Volume Move作業、然後稍後再試一次。如"指令參考資料ONTAP"需詳細 `snapmirror abort`資訊，請參閱。

5. 驗證Volume Move作業的狀態：

   `volume move show -volume vol_constituent_name`

   以下範例顯示FlexGroup 完成複寫階段且處於Volume Move作業轉換階段的各個不完整磁碟區狀態：

```
cluster1::> volume move show -volume fg1_002
Vserver   Volume     State    Move Phase  Percent-Complete Time-To-
Complete
--------- ---------- -------- ----------  ----------------
----------------
vs2       fg1_002    healthy  cutover     -                -
```

在 **FabricPool** 中使用集合體來處理現有的 **ONTAP FlexGroup** 磁碟區

從ONTAP 功能支援的版本起、FabricPool 支援從功能9.5開始FlexGroup 的功能。如果您想要在FabricPool 現有FlexGroup 的流通區使用aggregate in整個功能、您可以將FlexGroup 駐留在該功能區的集合體轉換成FabricPool 集合體、或是將FlexGroup 流通區的成員資料移轉到FabricPool 流通區、以利在流通區內集合體。

開始之前

- FlexGroup 磁碟區必須將空間保證設定為 `none`。
- 如果您想要將FlexGroup 駐留在該實體磁碟區的集合體轉換成FabricPool 在元資料中的集合體、則集合體必須使用所有的SSD磁碟。

關於這項工作

如果現有FlexGroup 的流通區位於非SSD集合體上、您必須移轉FlexGroup 供應區內的功能區、才能將其整合到FabricPool 流通區中。

選擇

- 若要將FlexGroup 駐留在該磁碟區上的集合體轉換成FabricPool 在整個過程中的集合體、請執行下列步驟：

  a. 在現有的 FlexGroup 磁碟區上設定分層原則： `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. 識別 FlexGroup 磁碟區所在的集合體： `volume show -volume flexgroup_name -fields aggr-list`

  ```
  cluster-2::> volume show -volume fg1 -fields aggr-list
  vserver volume aggr-list
  ------- ------ -----------
  vs1     fg1    aggr1,aggr3
  ```

  c. 將物件存放區附加至集合清單中列出的每個集合： `storage aggregate object-store attach -aggregate aggregate name -name object-store-name -allow-flexgroup true`

  您必須將所有集合體附加至物件存放區。

```
cluster-2::> storage aggregate object-store attach -aggregate aggr1
-object-store-name Amazon01B1
```

- 若要移轉FlexGroup 將整個過程的對象組成到FabricPool 整個過程中的集合體、請執行下列步驟：

  a. 在現有的 FlexGroup 磁碟區上設定分層原則： `volume modify -volume flexgroup_name -tiering-policy [auto|snapshot|none|backup]`

  ```
  cluster-2::> volume modify -volume fg1 -tiering-policy auto
  ```

  b. 將 FlexGroup Volume 的每個組成要素移至同一個叢集中 FabricPool 中的集合： `volume move start -volume constituent-volume -destination-aggregate FabricPool_aggregate -allow-mixed-aggr-types true`

  您必須將FlexGroup 所有的「不穩定」Volume成員移至FabricPool 「不穩定」（如果FlexGroup 「不穩定」磁碟區成員為混合式Aggregate類型）、並確保所有成員在叢集中的節點之間取得平衡。

```
cluster-2::> volume move start -volume fg1_001 -destination-aggregate
FP_aggr1 -allow-mixed-aggr-types true
```

相關資訊

- "磁碟與Aggregate管理"

- "存儲聚合物件存儲附加"

重新分配檔案資料以平衡 **ONTAP FlexGroup** 磁碟區

從 ONTAP 9 。 16.1 開始，您可以啟用進階容量平衡，以便在一個成員磁碟區上的大型檔案增加和佔用空間時，在 FlexGroup 成員磁碟區之間進行資料發佈。

進階容量平衡功能可擴充 ONTAP 9 。 12.1 中引進的精細資料功能，讓 ONTAP 能夠"重新平衡 FlexGroup 磁碟區"將檔案移至其他成員。從 ONTAP 9 。 16.1 開始，當使用選項啟用進階容量平衡時 `-granular-data advanced`，「基本」檔案重新平衡功能和進階容量功能都會啟動。

預設會停用檔案重新平衡和進階容量平衡。啟用這些功能後，就無法停用這些功能。如果您需要停用容量平衡，則必須從啟用進階容量平衡之前所建立的快照進行還原。

進階容量平衡是由高達 10GB 或 1% 磁碟區可用空間的新寫入所觸發。

檔案的散佈方式

如果建立或擴充足夠大的檔案來觸發進階容量平衡，則檔案會在成員 FlexGroup 磁碟區中以介於 1GB 和 10GB 之間的分段形式散佈。

啟用進階容量平衡時， ONTAP 不會追溯等量分割現有的大型檔案。如果在啟用進階容量平衡之後，現有的大型檔案仍會繼續成長，則現有大型檔案中的新內容可能會根據檔案大小和可用空間，跨成員 FlexGroup 磁碟區進行等量分割。

進階容量平衡的一種方式是使用成員磁碟區上的可用空間量來決定等量區塊寬度。進階容量平衡功能可建立檔案等量磁碟區，其可用空間為可用空間的 1% 。這表示如果有更多可用空間，條紋就會開始變大，而隨著 FlexGroup 的填滿，條紋也會變小。

支援的傳輸協定

下列通訊協定支援進階容量平衡：

- NFSv3 、 NFSv4 、 NFSv4.1
- pNFS
- 中小企業

啟用進階容量平衡

預設會停用進階容量平衡。您必須啟用進階容量平衡，才能自動平衡 FlexGroup 容量。請記住，啟用此功能後，您就無法停用此功能，但您可以從啟用進階容量平衡之前建立的快照中還原。

開始之前

- 叢集中的所有節點都必須執行ONTAP 版本不符合要求的9.16.1或更新版本。
- 如果已啟用進階容量平衡，則無法還原至早於 ONTAP 9 的版本。 16.1 。如果您需要還原，則必須先從啟用進階容量平衡之前所建立的快照還原。
- 如果已(`vserver nfs -vstorage enabled`在 SVM 上啟用 NFS 複製卸載），您就無法在 FlexGroup 磁碟區上啟用進階容量平衡。同樣地，如果您在 SVM 中的任何 FlexGroup 磁碟區上啟用進階容量平衡，就無法啟用 NFS 複製卸載。

- FlexCache 回寫不支援進階容量平衡。
- 如果在執行 ONTAP 9.16.1 或更新版本的叢集中的磁碟區上啟用進階容量平衡，則 ONTAP 9.16.1 之前的 ONTAP 版本不支援 SnapMirror 傳輸。
- 啟用進階容量平衡之前，請先停用 SMB Multichannel。將 SMB Multichannel 與進階容量重新平衡搭配使用可能會導致高延遲。如需詳細資訊，請參閱 "CONTAP-400433：在啟用 SMB Multichannel 的用戶端上使用 FlexGroup Rebalancing/GDD 時，讀取/寫入延遲較高"。

關於這項工作

在使用其中一個精細資料選項（基本或進階）建立 DP 目的地 Volume 期間，目的地會將設定顯示為「停用」，直到 SnapMirror 傳輸完成為止。傳輸完成後， DP 目的地會將精細資料顯示為「啟用」。

在 **FlexGroup** 建立期間啟用進階容量平衡

步驟

建立新的 FlexGroup Volume 時，您可以使用系統管理員或 ONTAP CLI 來啟用進階容量平衡。

系統管理員

1. 瀏覽至 * 儲存 > 磁碟區 * + Add ，然後按一下。
2. 在 * 新增 Volume * 視窗中，輸入磁碟區名稱和大小。然後按一下「 * 更多選項 * 」。
3. 在 * 儲存與最佳化 * 下，選取 * 在叢集（ FlexGroup ） * 之間散佈磁碟區資料。
4. 選取 * 進階容量平衡 * 。
5. 完成磁碟區設定，然後按一下 * 儲存 * 。

CLI

1. 建立已啟用進階容量平衡的磁碟區：

```
volume create -vserver <svm name> -volume <volume name>-size <volume
size> -auto-provision-as flexgroup -junction-path /<path> -granular
-data advanced
```

範例：

```
volume create -vserver vs0 -volume newvol-size 1TB -auto-provision
-as flexgroup -junction-path /newvol -granular-data advanced
```

在現有的 **FlexGroup** 磁碟區上啟用進階容量平衡

步驟

您可以使用系統管理員或 ONTAP CLI 來啟用進階容量平衡。

系統管理員

1. 瀏覽至 * 儲存 > 磁碟區 * ，按一下⋮，然後選擇 * 編輯 > 磁碟區 * 。
2. 在 * 編輯 Volume * 視窗的 * 儲存與最佳化 * 下，選取 * 進階容量平衡 * 。
3. 按一下「 * 儲存 * 」。

CLI

1. 修改現有的 FlexGroup Volume 以啟用進階容量平衡：

```
volume modify -vserver <svm name> -volume <volume name> -granular
-data advanced
```

範例：

```
volume modify -vserver vs0 -volume newvol  -granular-data advanced
```

透過移動檔案重新平衡 **ONTAP FlexGroup** 磁碟區

從功能完整的9.12.1開始ONTAP 、您可以FlexGroup 在不中斷營運的情況下、將檔案從FlexGroup 某個部分的一個部分移至另一個部分、藉此重新平衡功能。

由於新增檔案和檔案增長、導致長期不平衡時、可利用此功能重新平衡功能來重新分配容量。FlexGroup手動啟動重新平衡作業之後ONTAP 、即可選擇檔案、並在不中斷營運的情況下自動移動。

> ⓘ 您應該知道、當大量檔案被移作單一重新平衡事件的一部分、或是因為建立多個部分 inode 而導致多個重新平衡事件時、 FlexGroup 重新平衡會降低系統效能。每個作爲重新平衡事件一部分移動的文件都有 2 個與該文件相關聯的多部分 inode 。在 FlexGroup 中、多個部分 inode 的檔案數量佔檔案總數的百分比越多、效能影響就越大。某些使用案例（例如 FlexVol 到 FlexGroup 的轉換）可能會導致大量的多部分 inode 創建。

只有叢集中的所有節點都執行 ONTAP 9.12.1 或更新版本時、才能使用重新平衡。您必須在執行重新平衡作業的任何 FlexGroup 磁碟區上啟用精細資料功能。啟用該功能後，除非您刪除此磁碟區，或從啟用設定之前建立的快照中還原，否則無法還原至 ONTAP 9.11.1 及更早版本。

從 ONTAP 9.14.1 開始、 ONTAP 引進一種演算法、可在不需使用者互動的情況下、不中斷運作且主動地移動已啟用精細資料的磁碟區中的檔案。此演算法在非常特定且目標明確的案例中運作、以減輕效能瓶頸。 此演算法可能會執行的案例包括叢集中某個節點上特定檔案集的嚴重寫入負載、或是在非常熱的父目錄中持續成長的檔案。

從 ONTAP 9 。 16.1 開始，您也可以"進階容量平衡"在 FlexGroup 成員磁碟區之間重新分配大型檔案的資料。

重新平衡考量**FlexGroup**

您應該瞭FlexGroup 解到如何使用還原功能、以及它如何與ONTAP 其他的功能進行互動。

- 從系統轉換為FlexVol FlexGroup

  建議您在FlexVol到FlexGroup轉換後不要使用自動FlexGroup重新平衡。相反，您可以使用 `volume rebalance file-move start`指令，在ONTAP 9.10.1 及更高版本中可用。預設情況下，此操作不會造成中斷 (-is-disruptive false`）。如果某些繁忙檔案無法移動，您可以以中斷模式重新執行命令(`-is-disruptive true`) 在計畫的維護時段內。詳細了解 `volume rebalance file-move start`在"指令參考資料ONTAP" 。

  使用自動 FlexGroup 重新平衡功能重新平衡可能會在移動大量檔案時降低效能、例如執行 FlexVol 至 FlexGroup 轉換時、 FlexVol 磁碟區上最多有 50% 至 85% 的資料會移至新的組成項目。

- 最小和最大檔案大小

  自動重新平衡的檔案選擇是根據已儲存的區塊而來。 根據預設、重新平衡所考慮的檔案大小下限為 100 MB （使用以下所示的最小檔案大小參數、可設定為低至 20 MB ）、檔案大小上限為 100 GB 。

- 快照中的檔案

  您可以將 FlexGroup 重新平衡設定為僅考慮要移動的檔案，而這些檔案目前不存在於任何快照中。重新平衡啟動時，如果在重新平衡作業期間隨時排程快照作業，則會顯示通知。

  如果檔案正在移動，且正在目的地進行框架架構，則快照會受到限制。檔案重新平衡進行中，不允許執行快照還原作業。

  啟用此選項之後建立的任何快照，都 `granular-data`無法複寫至執行 ONTAP 9.11.1 及更早版本的系統，因為 ONTAP 9.11.1 及更早版本不支援多個部分的 inode 。

- SnapMirror作業

  應在排定的SnapMirror作業之間進行資訊重新平衡。FlexGroup如果在SnapMirror操作開始之前重新定位某個檔案、如果該檔案移動在24分鐘SnapMirror重試期間內未完成、SnapMirror作業可能會失敗。在SnapMirror傳輸開始之後開始的任何新檔案重新配置都不會失敗。

- 檔案型壓縮儲存效率

  使用檔案型壓縮儲存效率時、檔案會在移至目的地之前解壓縮、因此壓縮節約效益會遺失。手動啟動的背景掃描儀FlexGroup 在重新平衡後、在該磁碟區上執行後、便可重新獲得壓縮節約效益。但是，如果任何檔案與任何磁碟區上的快照相關聯，則會忽略檔案進行壓縮。

- 重複資料刪除

  移動刪除重複資料的檔案可能會增加FlexGroup 整個使用率。在檔案重新平衡期間、只會將唯一的區塊移至目的地、以釋放來源上的該容量。共享區塊會保留在來源上、並複製到目的地。雖然如此一來、我們的目標是在接近完整的來源中減少已用容量、但FlexGroup 由於新目的地上的共享區塊複本、也可能導致整個使用率增加。當屬於快照一部分的檔案被移動時，也可能發生這種情況。在快照排程資源回收，且快照中不再有檔案複本之前，無法完全辨識所節省的空間。

- FlexClone Volume

  如果在建立FlexClone磁碟區時正在進行檔案重新平衡、則不會在FlexClone磁碟區上執行重新平衡。FlexClone磁碟區的重新平衡應在建立之後執行。

- 檔案搬移

當檔案在FlexGroup 重新平衡作業期間移動時、檔案大小會在來源和目的地構成區塊上報告為配額會計的一部分。 完成移動後、配額會計會恢復正常、而且只會在新目的地上報告檔案大小。

- 自主勒索軟體保護

  從 ONTAP 9.13.1 開始、在中斷和不中斷營運的重新平衡作業中、均支援自動勒索軟體保護。

- 物件儲存區 Volume

  磁碟區容量重新平衡不支援物件儲存區磁碟區、例如 S3 儲存區。

啟用**FlexGroup** 支援功能重新平衡

從 ONTAP 9.12.1 開始、您可以啟用自動不中斷營運的 FlexGroup Volume 重新平衡、以便在 FlexGroup 元件之間重新分配檔案。

從 ONTAP 9.13.1 開始、您可以排程單一 FlexGroup 重新平衡作業、以在未來的日期和時間開始。

開始之前

您必須已啟用 `granular-data` 在啟用功能不均衡之前、請先在FlexGroup 支援FlexGroup 功能不均衡的情況下、選擇使用支援功能。您可以使用下列其中一種方法來啟用：

- 當您FlexGroup 使用建立完這個功能時 `volume create` 命令
- 藉由修改現有FlexGroup 的支援功能、以啟用使用的設定 `volume modify` 命令
- 使用初始化還原平衡時、會自動設定此功能FlexGroup `volume rebalance` 命令

> 如果您使用的是 ONTAP 9 。 16.1 或更新版本，並且"FlexGroup 進階容量平衡"是使用 ONTAP CLI 中的選項或使用系統管理員來啟用 `granular-data advanced`，則 FlexGroup 重新平衡也會啟用。

步驟

您可以FlexGroup 使用ONTAP VMware System Manager或ONTAP VMware CLI來管理不均衡的功能。

系統管理員

1. 瀏覽至* Storage > Volumes *、找到FlexGroup 要重新平衡的S復原 磁碟區。
2. 選取 ⌄ 以檢視 Volume 詳細資料。
3. 在 * Balance Status* （ FlexGroup 餘額狀態 * ）下選擇 * Rebalanc* （重新平衡）

   只有當 FlexGroup 狀態超出平衡時、才能使用 * 重新平衡 * 選項。

4. 在*重新平衡Volume *視窗中、視需要變更預設設定。
5. 若要排程重新平衡作業、請選取 * 稍後重新平衡 * 、然後輸入日期和時間。

CLI

1. 開始自動重新平衡：

   ```
   volume rebalance start -vserver <SVM name> -volume <volume name>
   ```

   您也可以指定下列選項：

   [[-max-runtime] <time interval>] 最大執行時間

   [-max-threshold <percent>] 每個組成單位的最大不平衡臨界值

   [-min-threshold <percent> （最低閾值）] 每個組成單位的最小不平衡臨界值

   [-max-file-Moves <integer> （最大檔案移動量）] 每個組成單位的最大並行檔案移動量

   [-min-file-size ｛ <integer> [kb|MB|GB|TB|PB]｝] 最小檔案大小

   [- 開始時間 <mm/dd/yyyy-00:00:00>] 排程重新平衡開始日期和時間

   [-excluse-snapshots ｛ true|false ｝] 排除快照中的檔案

   範例：

   ```
   volume rebalance start -vserver vs0 -volume fg1
   ```

修改**FlexGroup** 重新平衡組態

您可以變更 FlexGroup 重新平衡組態，以更新不平衡臨界值，並行檔案數量會移動最小檔案大小，最大執行時間，以及包含或排除快照。從 ONTAP 9.13.1 開始、您可以選擇修改 FlexGroup 重新平衡排程。

系統管理員

1. 瀏覽至* Storage > Volumes *、找到FlexGroup 要重新平衡的S復原 磁碟區。
2. 選取 ⌄ 以檢視 Volume 詳細資料。
3. 在 * Balance Status* （ FlexGroup 餘額狀態 * ）下選擇 * Rebalanc* （重新平衡）

   只有當 FlexGroup 狀態超出平衡時、才能使用 * 重新平衡 * 選項。

4. 在*重新平衡Volume *視窗中、視需要變更預設設定。

CLI

1. 修改自動重新平衡：

   ```
   volume rebalance modify -vserver <SVM name> -volume <volume name>
   ```

   您可以指定下列一或多個選項：

   [[-max-runtime] <time interval>] 最大執行時間

   [-max-threshold <percent>] 每個組成單位的最大不平衡臨界值

   [-min-threshold <percent> （最低閾值）] 每個組成單位的最小不平衡臨界值

   [-max-file-Moves <integer> （最大檔案移動量）] 每個組成單位的最大並行檔案移動量

   [-min-file-size ｛ <integer> [kb|MB|GB|TB|PB]｝] 最小檔案大小

   [- 開始時間 <mm/dd/yyyy-00:00:00>] 排程重新平衡開始日期和時間

   [-excluse-snapshots ｛ true|false ｝] 排除快照中的檔案

停止**FlexGroup** 重新平衡

啟用或排程 FlexGroup 重新平衡之後、您可以隨時停止。

系統管理員

1. 瀏覽至* Storage > Volumes *、找到FlexGroup 《不確定的問題》（英文）。
2. 選取 以檢視 Volume 詳細資料。
3. 選取 * 停止重新平衡 * 。

CLI

1. 停止FlexGroup 重新平衡：

```
volume rebalance stop -vserver <SVM name> -volume <volume name>
```

檢視**FlexGroup** 重新平衡狀態

您可以顯示FlexGroup 有關以下項目的狀態：重新平衡作業、FlexGroup 重新平衡組態、重新平衡作業時間、以及重新平衡執行個體詳細資料。

系統管理員

1. 瀏覽至* Storage > Volumes *、找到FlexGroup 《不確定的問題》（英文）。
2. 選取 以檢視 FlexGroup 詳細資料。
3. *此「平衡狀態」*會顯示在詳細資料窗格底部附近。FlexGroup
4. 若要檢視上次重新平衡作業的相關資訊、請選取 * 上次 Volume 重新平衡狀態 * 。

CLI

1. 檢視FlexGroup 畫面重新平衡作業的狀態：

```
volume rebalance show
```

重新平衡狀態範例：

```
> volume rebalance show
Vserver: vs0
                                                                  Target
Imbalance
Volume       State                  Total      Used     Used
Size     %
------------ ------------------ --------- --------- ---------
--------- -----
fg1          idle                     4GB   115.3MB         -
8KB    0%
```

重新平衡組態詳細資料的範例：

```
> volume rebalance show -config
Vserver: vs0
                     Max            Threshold         Max
Min          Exclude
Volume               Runtime        Min     Max       File Moves
File Size    Snapshot
---------------      ------------   -----   -----     ----------
---------    ---------
fg1                  6h0m0s         5%      20%          25
4KB          true
```

重新平衡時間詳細資料範例：

```
> volume rebalance show -time
Vserver: vs0
Volume               Start Time                    Runtime
Max Runtime
---------------     -------------------------     -----------
-----------
fg1                  Wed Jul 20 16:06:11 2022      0h1m16s
6h0m0s
```

重新平衡執行個體詳細資料範例：

```
    > volume rebalance show -instance
    Vserver Name: vs0
    Volume Name: fg1
    Is Constituent: false
    Rebalance State: idle
    Rebalance Notice Messages: -
    Total Size: 4GB
    AFS Used Size: 115.3MB
    Constituent Target Used Size: -
    Imbalance Size: 8KB
    Imbalance Percentage: 0%
    Moved Data Size: -
    Maximum Constituent Imbalance Percentage: 1%
    Rebalance Start Time: Wed Jul 20 16:06:11 2022
    Rebalance Stop Time: -
    Rebalance Runtime: 0h1m32s
    Rebalance Maximum Runtime: 6h0m0s
    Maximum Imbalance Threshold per Constituent: 20%
    Minimum Imbalance Threshold per Constituent: 5%
    Maximum Concurrent File Moves per Constituent: 25
    Minimum File Size: 4KB
    Exclude Files Stuck in snapshots: true
```

資料保護**FlexGroup** 功能

ONTAP FlexGroup Volume 資料保護工作流程摘要

您可以建立FlexGroup SnapMirror災難恢復（DR）關係、以利解決此問題。您也可以使用 SnapVault 技術來備份和還原 FlexGroup 磁碟區，也可以建立統一化的資料保護關係，將相同的目的地用於備份和災難恢復。

關於這項工作

SnapMirror 關係類型一律 `XDP`適用於 FlexGroup Volume 。SnapMirror關係所提供的資料保護類型、取決於您使用的複寫原則。您可以針對您要建立的複寫關係、使用預設原則或所需類型的自訂原則。

1 對等叢集和 **SVM**

如果叢集和 SVM 尚未對等執行，請建立"叢集對等端點"和"SVM 對等端點"。

2 建立工作排程

您必須"建立工作排程"決定何時進行 SnapMirror 更新。

3 根據資料保護的類型，請遵循下列其中一種路徑：

- * 如果 SnapMirror DR ： *

  "建立SnapMirror關係。"建立關聯時，您可以選取預設原則或類型的自訂 `async-mirror`原則 `MirrorAllSnapshots`。

- * 如果 SnapMirror 資料保險箱： *

  "建立 SnapMirror 資料保險箱關係。"建立關聯時，您可以選取預設原則或類型的自訂 `vault`原則 `XDPDefault`。

- * 如果統一化資料保護： *

  "建立統一化的資料保護關係。"建立關聯時，您可以選取預設原則或類型的自訂 `mirror-vault`原則 `MirrorAndVault`。

為 **ONTAP FlexGroup** 磁碟區建立 **SnapMirror** 關係

您可以在FlexGroup 連接的SVM上、在來源Sf2 Volume和目的地FlexGroup Sfvolume之間建立SnapMirror關係、以便複寫資料以進行災難恢復。發生災難時、您可以使用FlexGroup鏡射複本的現象來恢復資料。

開始之前

您必須建立叢集對等關係和SVM對等關係。

"叢集與SVM對等關係"

關於這項工作

- 從 ONTAP 9.9.1 開始，您可以使用 ONTAP CLI 為 FlexGroup 磁碟區建立 SnapMirror 串聯和展開關係。如需詳細資訊、請參閱 "為 FlexGroup 磁碟區建立 SnapMirror 串聯和展開關係的考量事項"。
- 您可以建立FlexGroup 叢集間的SnapMirror關係、以及針對各個磁碟區建立叢集內的叢集SnapMirror關係。
- 從ONTAP 功能區9.3開始、您可以擴充FlexGroup SnapMirror關係中的功能區。

  如果您使用的 ONTAP 版本早於 ONTAP 9.3 ，請勿在建立 SnapMirror 關係後擴充 FlexGroup Volume ；不過，您可以在建立 SnapMirror 關係後增加 FlexGroup Volume 的容量。如果FlexGroup 您在ONTAP 更新版

本早於版本的SnapMirror關係之後、擴充來源的聲音量、則必須執行基準傳輸至目的地FlexGroup 的聲音量。

步驟

1. 建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 的組成數量相同：

   a. 從來源叢集中、判斷來源 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

   b. 從目的地叢集建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 相同。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

   c. 從目的地叢集、確認目的地 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume        Aggregate    State      Type       Size
Available  Used%
--------- ------------  ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     DP         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     DP         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     DP         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     DP         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     DP         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     DP         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     DP         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     DP         25TB
10.63TB   57%
...
```

2. 建立工作排程： `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   適用於 `-month`、 `-dayofweek`和 `-hour` 選項、您可以指定 `all` 每個月、每週的每一天、每小時執行一次工作。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. 建立類型的自訂原則 `async-mirror` 對於 SnapMirror 關係： `snapmirror policy create -vserver SVM -policy snapmirror_policy -type async-mirror`

   如果您未建立自訂原則、則應指定 `MirrorAllSnapshots` SnapMirror 關係原則。

4. 從目的地叢集、在來源 FlexGroup Volume 和目的地 FlexGroup Volume 之間建立 SnapMirror 關係： `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -policy snapmirror_policy -schedule sched_name`

   FlexGroup 磁碟區的 SnapMirror 關係必須屬於類型 `XDP`。

如果您為FlexGroup SnapMirror關係指定一個流向值、則每個組成部分都會使用相同的節流值。節流值不會分成多個部分。

> 您無法為 FlexGroup Volume 使用快照的 SnapMirror 標籤。

在 ONTAP 9.4 及更早版本中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAllSnapshots` 原則預設為使用。在 ONTAP 9.5 中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAndVault` 原則預設為使用。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -policy MirrorAllSnapshots -schedule hourly
Operation succeeded: snapmirror create for the relationship with
destination "vsd:dstFG".
```

5. 從目的地叢集執行基準傳輸、以初始化 SnapMirror 關係： `snapmirror initialize -destination -path dest_svm:dest_flexgroup`

   基礎傳輸完成後、目的地FlexGroup 的E動磁 碟區會根據SnapMirror關係的排程定期更新。

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

> 如果FlexGroup 您已在來源叢集執行ONTAP 版本為9.3的來源叢集與執行ONTAP 版本為9.2或更早版本的目的地叢集之間建立任何SnapMirror關係、而且如果您在來源FlexGroup 版本為0、SnapMirror更新就會失敗。若要從這種情況中恢復，您必須刪除 FlexGroup Volume 中的所有非預設 qtree ，停用 FlexGroup 磁碟區上的 qtree 功能，然後刪除使用 qtree 功能啟用的所有快照。

完成後

您應設定必要的組態、例如lifs和匯出原則、以設定目的地SVM進行資料存取。

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略創建"
- "SnapMirror 更新"

為 **ONTAP FlexGroup** 磁碟區建立 **SnapVault** 關係

您可以設定SnapVault 一個靜態關係、並為SnapVault 該關係指派一個不支援的原則、以建立SnapVault 一個不支援的備份。

開始之前

您必須瞭解建立SnapVault 有關本區的不景點關係的考量FlexGroup 事項。

步驟

1. 建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 的組成數量相同：

   a. 從來源叢集中、判斷來源 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume src* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vss       src          -            online     RW         400TB
172.86GB  56%
vss       src__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       src__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       src__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       src__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       src__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       src__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       src__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

   b. 從目的地叢集建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 相同。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dst

Warning: The FlexGroup volume "dst" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

   c. 從目的地叢集、確認目的地 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dst* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     RW         400TB
172.86GB  56%
vsd       dst__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dst__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dst__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dst__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dst__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dst__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dst__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. 建立工作排程： `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. 建立SnapVault 一套不規則的原則、然後定義SnapVault 一套適用於該決策的規則：

   a. 建立類型的自訂原則 `vault` 對於 SnapVault 關係： `snapmirror policy create -vserver svm_name -policy policy_name -type vault`

   b. 為 SnapVault 原則定義規則，以決定在初始化和更新作業期間傳輸哪些快照： `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   如果您未建立自訂原則、則應指定 `XDPDefault` SnapVault 關係原則。

4. 建立 SnapVault 關係： `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name`

`-policy XDPDefault`

在 ONTAP 9.4 及更早版本中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAllSnapshots` 原則預設為使用。在 ONTAP 9.5 中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAndVault` 原則預設為使用。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy XDPDefault
```

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

5. 從目的地叢集執行基準傳輸來初始化 SnapVault 關係： `snapmirror initialize -destination -path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dst
Operation is queued: snapmirror initialize of destination "vsd:dst".
```

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略新增規則"
- "SnapMirror 策略創建"

為 **ONTAP FlexGroup** 磁碟區建立統一化的資料保護關係

從ONTAP 使用支援功能支援功能9.3開始、您可以建立及設定SnapMirror統一化資料保護關係、以便在同一個目的地磁碟區上設定災難恢復與歸檔。

開始之前

您必須瞭解建立FlexGroup 統一化資料保護關係以利建立有關本區的考量。

"建立SnapVault 不支援的備份關係和FlexGroup 統一資料保護關係的考量事項"

步驟

1. 建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 的組成數量相同：
   a. 從來源叢集中、判斷來源 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster1::> volume show  -volume srcFG* -is-constituent true
Vserver   Volume         Aggregate    State      Type       Size
Available  Used%
--------- ------------   ------------ ---------- ---- ----------
---------- -----
vss       srcFG          -            online     RW         400TB
172.86GB  56%
vss       srcFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vss       srcFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vss       srcFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vss       srcFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vss       srcFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vss       srcFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vss       srcFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

b. 從目的地叢集建立類型的目的地 FlexGroup Volume `DP` 其組成數量與來源 FlexGroup Volume 相同。

```
cluster2::> volume create -vserver vsd -aggr-list aggr1,aggr2 -aggr
-list-multiplier 8 -size 400TB -type DP dstFG

Warning: The FlexGroup volume "dstFG" will be created with the
following number of constituents of size 25TB: 16.
Do you want to continue? {y|n}: y
[Job 766] Job succeeded: Successful
```

c. 從目的地叢集、確認目的地 FlexGroup Volume 中的組成數量： `volume show -volume volume_name* -is-constituent true`

```
cluster2::> volume show  -volume dstFG* -is-constituent true
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dstFG          -            online     RW         400TB
172.86GB  56%
vsd       dstFG__0001    Aggr_cmode   online     RW         25GB
10.86TB   56%
vsd       dstFG__0002    aggr1        online     RW         25TB
10.86TB   56%
vsd       dstFG__0003    Aggr_cmode   online     RW         25TB
10.72TB   57%
vsd       dstFG__0004    aggr1        online     RW         25TB
10.73TB   57%
vsd       dstFG__0005    Aggr_cmode   online     RW         25TB
10.67TB   57%
vsd       dstFG__0006    aggr1        online     RW         25TB
10.64TB   57%
vsd       dstFG__0007    Aggr_cmode   online     RW         25TB
10.63TB   57%
...
```

2. 建立工作排程： `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   適用於 `-month`、 `-dayofweek`和 `-hour` 選項、您可以指定 `all` 每個月、每週的每一天、每小時執行一次工作。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

   ```
   cluster1::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

3. 建立類型的自訂原則 `mirror-vault`, 然後定義鏡射和資料保險箱原則的規則 :

   a. 建立類型的自訂原則 `mirror-vault` 針對統一化的資料保護關係： `snapmirror policy create -vserver svm_name -policy policy_name -type mirror-vault`

   b. 定義鏡射和資料保險箱原則的規則，以決定在初始化和更新作業期間傳輸哪些快照： `snapmirror policy add-rule -vserver svm_name -policy policy_for_rule - snapmirror-label snapmirror-label -keep retention_count -schedule schedule`

   如果您未指定自訂原則、請使用 `MirrorAndVault` 原則用於統一化資料保護關係。

4. 建立統一化的資料保護關係： `snapmirror create -source-path src_svm:src_flexgroup -destination-path dest_svm:dest_flexgroup -type XDP -schedule schedule_name`

`-policy MirrorAndVault`

在 ONTAP 9.4 及更早版本中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAllSnapshots` 原則預設為使用。在 ONTAP 9.5 中、如果原則未使用指定 `snapmirror create` 命令 `MirrorAndVault` 原則預設為使用。

```
cluster2::> snapmirror create -source-path vss:srcFG -destination-path
vsd:dstFG -type XDP -schedule Daily -policy MirrorAndVault
```

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

5. 從目的地叢集執行基準傳輸、以初始化統一化資料保護關係： `snapmirror initialize -destination-path dest_svm:dest_flexgroup`

```
cluster2::> snapmirror initialize -destination-path vsd:dstFG
Operation is queued: snapmirror initialize of destination "vsd:dstFG".
```

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略新增規則"
- "SnapMirror 策略創建"

為 **ONTAP FlexGroup** 磁碟區建立 **SVM** 災難恢復關係

從ONTAP Sf19.9.1開始、您可以使用FlexGroup 支援的功能區建立SVM災難恢復（SVM DR）關係。SVM DR 關係可同步及複寫 SVM 組態及其資料，提供備援功能，並在發生災難時恢復 FlexGroup Volume 。SVM DR需要SnapMirror授權。

開始之前

您 _ 無法 _ 建立符合下列條件的 FlexGroup SVM DR 關係。

- 存在FlexClone FlexGroup 功能組態
- FlexGroup Volume 是串聯關係的一部分
- FlexGroup Volume 是扇出關係的一部分、您的叢集執行的 ONTAP 版本早於 ONTAP 9.12.1 。（從 ONTAP 9.13.1 開始、支援展開關係。）

關於這項工作

- 兩個叢集中的所有節點都必須執行與ONTAP 新增SVM DR支援的節點相同的版本（ONTAP 更新版本為《SVM DR》）。
- 一線站台和二線站台之間的SVM DR關係應該健全、而且在一線和二線SVM上應有足夠的空間來支援FlexGroup 該等磁碟區。
- 從 ONTAP 9.12.1 開始、 FabricPool 、 FlexGroup 和 SVM DR 可以搭配使用。在版本早於ONTAP 《支

援》9.12.1的版本中、這兩項功能可以搭配使用、但三項功能不能同時搭配使用。

- 當您建立 FlexGroup SVM DR 關係、其中 FlexGroup Volume 是扇出關係的一部分時、您應該瞭解下列需求：
  - 來源叢集和目的地叢集必須執行 ONTAP 9.13.1 或更新版本。
  - SVM DR 搭配 FlexGroup 磁碟區、可支援與八個站台的 SnapMirror 扇出關係。

如需建立 SVM DR 關係的相關資訊，請參閱"管理SnapMirror SVM複寫"。

步驟

1. 建立SVM DR關係、或使用現有關係。

   "複寫整個SVM組態"

2. 在FlexGroup 主站台建立包含所需數量成分的功能區。

   "建立FlexGroup 一個功能不全的功能"。

   請等到FlexGroup 建立完所有的成員後再繼續。

3. 若要複寫 FlexGroup Volume 、請在次要站台更新 SVM ： `snapmirror update -destination-path destination_svm_name: -source-path source_svm_name:`

   您也可以輸入以下命令來檢查排程的 SnapMirror 更新是否已存在 `snapmirror show -fields schedule`

4. 從次要站台驗證 SnapMirror 關係是否健全： `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                     Idle           -         true    -
```

5. 從次要站台、確認新的 FlexGroup Volume 及其組成成分存在： `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                    Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                             Snapmirrored
                                    Idle           -         true    -
6 entries were displayed.
```

相關資訊

- "SnapMirror 顯示"
- "SnapMirror 更新"

將 **ONTAP FlexGroup SnapMirror** 關係移轉至 **SVM DR**

您可以FlexGroup 轉換現有FlexGroup 的SnapMirror磁碟區關係、建立一套SVM DR關係。

開始之前

- 此功能與本系統的SnapMirror關係狀況良好。FlexGroup
- 來源FlexGroup 和目的地的不一致名稱。

步驟

1. 從 SnapMirror 目的地重新同步 FlexGroup 層級的 SnapMirror 關係： `snapmirror resync`
2. 建立FlexGroup SVM DR SnapMirror關係。使用在 FlexGroup Volume SnapMirror 關係上設定的相同 SnapMirror 原則： `snapmirror create -destination-path dest_svm: -source-path src_svm: -identity-preserve true -policy MirrorAllSnapshots`

   您必須使用 `-identity-preserve true` 的選項 `snapmirror create` 建立複寫關係時的命令。

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

3. 確認關係已中斷： `snapmirror show -destination-path dest_svm: -source-path src_svm:`

```
snapmirror show -destination-path fg_vs_renamed: -source-path fg_vs:


Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
fg_vs:        XDP  fg_vs1_renamed:     Broken-off
                                      Idle           -         true    -
```

4. 停止目的地SVM： `vserver stop -vserver vs_name`

```
vserver stop -vserver fg_vs_renamed
[Job 245] Job is queued: Vserver Stop fg_vs_renamed.
[Job 245] Done
```

5. 重新同步 SVM SnapMirror 關係： `snapmirror resync -destination-path dest_svm: -source -path src_svm:`

```
snapmirror resync -destination-path fg_vs_renamed: -source-path fg_vs:
Warning: This Vserver has volumes which are the destination of FlexVol
or FlexGroup SnapMirror relationships. A resync on the Vserver
SnapMirror relationship will cause disruptions in data access
```

6. 確認 SVM DR 層級 SnapMirror 關係達到健全的閒置狀態： `snapmirror show -expand`
7. 驗證 FlexGroup SnapMirror 關係是否處於正常狀態： `snapmirror show`

相關資訊

- "SnapMirror建立"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

將 **ONTAP FlexVol Volume** 轉換為 **SVM-DR** 關係中的 **FlexGroup Volume**

從ONTAP SVM-DR FlexVol 來源開始、您可以將一個Svm-DR Volume轉換成FlexGroup 一個Svm-DR Volume。

開始之前

- 正在轉換的這個版本必須在線上。FlexVol
- 在這個過程中、執行的操作和設定FlexVol 必須與轉換程序相容。

  如果FlexVol 現象不一致、而且取消了Volume轉換、就會產生錯誤訊息。您可以採取修正行動、然後重試轉換。
  如需詳細資料、請參閱 "將FlexVol 功能區轉換FlexGroup 為功能區的考量事項"

步驟

1. 使用進階權限模式登入： `set -privilege advanced`
2. 從目的地更新SVM-DR關係：

   ```
   snapmirror update -destination-path <destination_svm_name>: -source-path
   <source_svm_name>:
   ```

   您必須在選項中的 SVM 名稱之後輸入一個冒號（：） `-destination-path` 。

3. 確保SVM-DR關係處於Snapor不可 中斷的狀態：

   ```
   snapmirror show
   ```

4. 從目的地SVM、確認FlexVol 支援的不只是支援轉換的功能：

   ```
   volume conversion start -vserver <svm_name> -volume <vol_name> -check
   -only true
   ```

   如果此命令產生「這是目的地SVMDR Volume」以外的任何錯誤、您可以採取適當的修正行動、再次執行命令、然後繼續轉換。

5. 從目的地停用SVM-DR關係上的傳輸：

```
snapmirror quiesce -destination-path <dest_svm>:
```

您必須在選項中的 SVM 名稱之後輸入一個冒號（：） `-destination-path` 。

6. 從來源叢集開始轉換：

```
volume conversion start -vserver <svm_name> -volume <vol_name>
```

7. 確認轉換成功：

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state    volume-style-extended
-------  ---------  ------   ---------------------
vs0      my_volume  online   flexgroup
```

8. 從目的地叢集繼續傳輸關係：

```
snapmirror resume -destination-path <dest_svm>:
```

您必須在選項中的 SVM 名稱之後輸入一個冒號（：） `-destination-path` 。

9. 從目的地叢集執行更新、將轉換傳播到目的地：

```
snapmirror update -destination-path <dest_svm>:
```

您必須在選項中的 SVM 名稱之後輸入一個冒號（：） `-destination-path` 。

10. 確保SVM-DR關係處於Snap/快照狀態、且不會中斷：

```
snapmirror show
```

11. 確保轉換發生在目的地：

```
volume show <vol_name> -fields volume-style-extended,state
```

```
cluster-2::*> volume show my_volume -fields volume-style-extended,state

vserver  volume     state   volume-style-extended
-------  -------    ------  ---------------------
vs0_dst  my_volume  online  flexgroup
```

相關資訊

- "SnapMirror 履歷"
- "SnapMirror靜止"
- "SnapMirror 顯示"
- "SnapMirror 更新"

為 **ONTAP FlexGroup** 磁碟區建立 **SnapMirror** 串聯和展開關係的考量事項

在建立FlexGroup SnapMirror串聯和針對SnapMirror磁碟區的扇出關係時、請謹記支援考量和限制。

建立串聯關係的考量

- 每種關係都可以是叢集間關係或叢集內關係。
- 這兩種關係都支援所有非同步原則類型、包括非同步鏡射、鏡射保存庫和保存庫。
- 僅支援「MirrorAllSnapshots」、而非「MirrorLatest」非非同步鏡射原則。
- 不支援長期保留快照。

  詳細了解"長期保留快照"。

- 支援同步更新串聯的XDP關係。
- 支援移除 A 至 B 和 B 至 C 、並重新同步 A 至 C 或重新同步 C 至 A
- A和B FlexGroup 版的支援功能也可在所有節點執行ONTAP 版本的支援版本號為b、9.9.1或更新版本時進行。
- 支援從B或C FlexGroup 等磁碟區還原作業。
- 不支援在不支援之間傳輸FlexGroup 資料、而目的地則是還原關係的來源。
- 無法將還原目的地FlexGroup 作為任何其他FlexGroup 關聯的目的地。
- 還原檔案作業的限制與一般的還原作業相同。FlexGroup FlexGroup
- 叢集中FlexGroup B和C等功能區所在的所有節點、都必須執行ONTAP 版本號為「版本號」的版本號為「版本號」的版本號。
- 支援所有擴充和自動擴充功能。
- 在串聯組態（例如A到B到C）中、如果A到B和B到C的組成SnapMirror關係數量不同、則B到C SnapMirror關係不支援來源的中止作業。
- 無論 ONTAP 版本為何，系統管理員都不支援串聯關係。

- 將A轉B轉B轉C組FlexVol 的不景點關係轉換為FlexGroup 不景點關係時、您必須先將B轉換為C躍點。
- REST API也支援所有的與REST支援之原則類型關係的支援、可在串聯式功能表組態中使用。FlexGroup FlexGroup
- 如同 FlexVol 關係、 FlexGroup 串聯不受支援 `snapmirror protect` 命令。

建立扇出關係的考量事項

- 支援兩FlexGroup 個或更多的「橫向」關係、例如A到B、A到C、最多8個「扇形」雙腳。
- 每種關係都可以是叢集間或叢集內的關係。
- 這兩種關係都支援並行更新。
- 支援所有擴充和自動擴充功能。
- 如果關係的扇形分支具有不同數量的組成SnapMirror關係、則來源的中止作業不支援A對B和A對C關係。
- 來源和目的地 FlexGroup 磁碟區所在叢集中的所有節點都必須執行 ONTAP 9.9.1 或更新版本。
- 目前支援FlexGroup 的所有非同步原則類型均可用於Fanout關係。
- 您可以執行從 B 到 C FlexGroup 磁碟區的還原作業。
- 所有具有REST支援之原則類型的扇出組態、FlexGroup 也支援在支援的靜態組態中使用REST API。

相關資訊

- "SnapMirror保護"

為 **ONTAP FlexGroup** 磁碟區建立 **SnapVault** 備份關係和統一資料保護關係的考量事項

您必須瞭解建立SnapVault 一套適用於FlexGroup 整個過程的還原功能備份關係和統一化資料保護關係的考量事項。

- 您可以使用選項重新同步 SnapVault 備份關係和統一化資料保護關係，以便 `-preserve`在比最新通用快照更新的目的地磁碟區上保留快照。
- 不支援FlexGroup 使用不支援的長期保留。

  長期保留功能可直接在目的地磁碟區上建立快照，而無需將快照儲存在來源磁碟區上。

- 。 `snapshot` 命令 `expiry-time` FlexGroup Volume 不支援此選項。
- 儲存效率無法在目的地FlexGroup 的仰賴資料保護SnapVault 關係的不一致之處進行設定。
- 您無法重新命名 SnapVault 備份關係的快照，也無法為 FlexGroup 磁碟區重新命名統一化的資料保護關係。
- 一個支援區只能是一個備份關係或還原關係的來源磁碟區。FlexGroup

  無法從兩個方面建立起穩固的關係、兩個還原關係、或是一個還原關係和還原關係。FlexGroup SnapVault SnapVault

- 如果您刪除來源 FlexGroup 磁碟區上的快照，並以相同名稱重新建立快照，則如果目的地磁碟區具有相同名稱的快照，則下次傳送至目的地 FlexGroup 磁碟區的更新作業將會失敗。

  這是因為無法為 FlexGroup Volume 重新命名快照。

監控 ONTAP FlexGroup 磁碟區的 SnapMirror 資料傳輸

您應該定期監控FlexGroup 「SnapMirror Volume」關係的狀態、以確認目的地FlexGroup 的VMware磁碟區會根據指定的排程定期更新。

關於這項工作

您必須從目的地叢集執行此工作。

步驟

1. 查看所有 FlexGroup Volume 關係的 SnapMirror 關係狀態： `snapmirror show -relationship -group-type flexgroup`

```
cluster2::> snapmirror show -relationship-group-type flexgroup

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:d        Snapmirrored
                                     Idle           -         true    -
vss:s2      XDP  vsd:d2       Uninitialized
                                     Idle           -         true    -
2 entries were displayed.
```

相關資訊

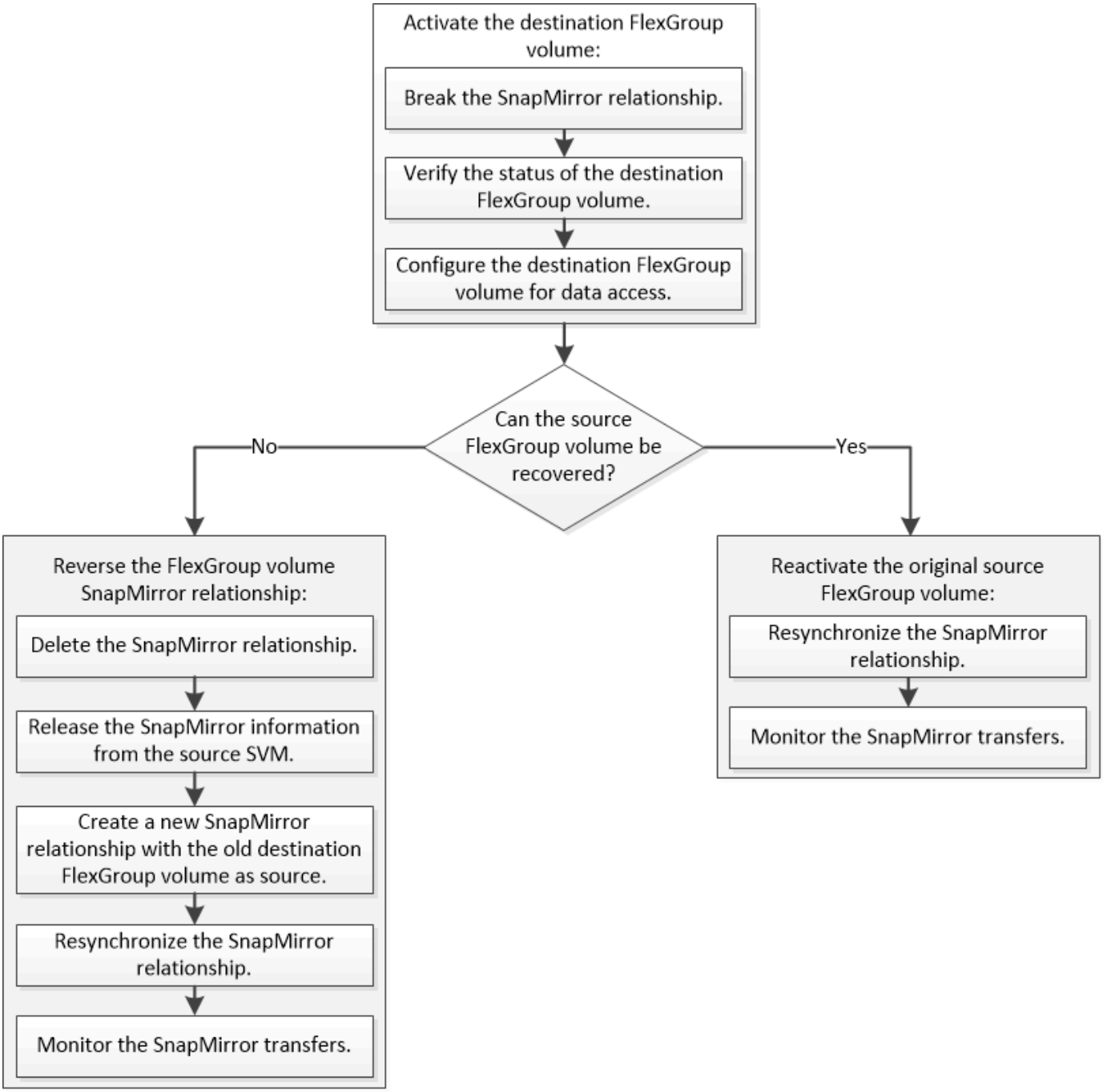
- "SnapMirror 顯示"

管理FlexGroup 資料保護作業、以利執行不中斷的作業

適用於支援功能區的災難恢復FlexGroup

ONTAP FlexGroup Volume 的災難恢復工作流程

當災難發生在來源FlexGroup 的供應區時、您應該啟動目的地FlexGroup 的供應區、並重新導向用戶端存取。視來源FlexGroup 的來源供應區是否可以恢復而定、您應該重新啟動來源FlexGroup 供應區、或是反轉SnapMirror關係。



關於這項工作

當FlexGroup 某些SnapMirror作業（例如SnapMirror中斷和重新同步）正在執行時、用戶端對目的地的存取功能會在短時間內遭到封鎖。如果SnapMirror作業失敗、部分成分可能仍處於這種狀態、FlexGroup 無法存取到此磁碟區。在此情況下、您必須重試SnapMirror作業。

啟動目的地 **ONTAP FlexGroup Volume**

當來源FlexGroup 供應資料時、由於資料毀損、意外刪除或離線狀態等事件而無法提供資料時、您必須啟動目的地FlexGroup 的穩定區才能存取資料、直到您在來源FlexGroup 的穩定區上恢復資料為止。啟動作業包括停止未來的SnapMirror資料傳輸、以及打破SnapMirror關係。

關於這項工作

您必須從目的地叢集執行此工作。

步驟

1. 停用 FlexGroup Volume SnapMirror 關係的未來傳輸： `snapmirror quiesce dest_svm:dest_flexgroup`

```
cluster2::> snapmirror quiesce -destination-path vsd:dst
```

2. 中斷 FlexGroup Volume SnapMirror 關係： `snapmirror break dest_svm:dest_flexgroup`

```
cluster2::> snapmirror break -destination-path vsd:dst
```

3. 查看 SnapMirror 關係的狀態： `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Broken-off
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Broken-off
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Broken-off
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Broken-off
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Broken-off
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Broken-off
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Broken-off
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Broken-off
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Broken-off
                                    Idle           -         true    -
...
```

每個組成要素的 SnapMirror 關係狀態為 `Broken-off`。

4. 確認目的地 FlexGroup Volume 為讀取 / 寫入： `volume show -vserver svm_name`

```
cluster2::> volume show -vserver vsd
Vserver   Volume       Aggregate    State      Type       Size
Available Used%
--------- ------------ ------------ ---------- ---- ----------
---------- -----
vsd       dst          -            online     **RW**          2GB
1.54GB   22%
vsd       d2           -            online     DP           2GB
1.55GB   22%
vsd       root_vs0     aggr1        online     RW         100MB
94.02MB    5%
3 entries were displayed.
```

5. 將用戶端重新導向至目的地FlexGroup 的不確定磁碟區。

相關資訊

- "SnapMirror中斷"
- "SnapMirror靜止"
- "SnapMirror 顯示"

災難後重新啟動原始來源 **ONTAP FlexGroup Volume**

當來源FlexGroup 供應時、您可以重新同步原始來源FlexGroup 和原始目的地的資料。目的地FlexGroup 的任何新資料都會遺失。

關於這項工作

目的地磁碟區上的任何作用中配額規則都會停用、而且配額規則會在執行重新同步之前刪除。

您可以使用 `volume quota policy rule create` 和 `volume quota modify` 在重新同步作業完成後建立及重新啟動配額規則的命令。

步驟

1. 從目的地叢集重新同步 FlexGroup Volume SnapMirror 關係： `snapmirror resync -destination -path dst_svm:dest_flexgroup`
2. 查看 SnapMirror 關係的狀態： `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vss:s       XDP  vsd:dst        Snapmirrored
                                    Idle           -         true    -
vss:s__0001 XDP  vsd:dst__0001  Snapmirrored
                                    Idle           -         true    -
vss:s__0002 XDP  vsd:dst__0002  Snapmirrored
                                    Idle           -         true    -
vss:s__0003 XDP  vsd:dst__0003  Snapmirrored
                                    Idle           -         true    -
vss:s__0004 XDP  vsd:dst__0004  Snapmirrored
                                    Idle           -         true    -
vss:s__0005 XDP  vsd:dst__0005  Snapmirrored
                                    Idle           -         true    -
vss:s__0006 XDP  vsd:dst__0006  Snapmirrored
                                    Idle           -         true    -
vss:s__0007 XDP  vsd:dst__0007  Snapmirrored
                                    Idle           -         true    -
vss:s__0008 XDP  vsd:dst__0008  Snapmirrored
                                    Idle           -         true    -
...
```

每個組成要素的 SnapMirror 關係狀態為 `Snapmirrored`。

相關資訊

- "SnapMirror 重新同步"
- "SnapMirror 顯示"

在災難恢復期間，反轉 **ONTAP FlexGroup** 磁碟區之間的 **SnapMirror** 關係

當災難停用FlexGroup SnapMirror關係的來源等量資料時、您可以在FlexGroup 修復或更換來源FlexGroup 的等量資料時、使用目的地的等量資料。在來源FlexGroup 供應資料的來源供應上線後、您可以將原始來源FlexGroup 供應資料的來源供應區變成唯讀目的地、並反轉SnapMirror關係。

關於這項工作

目的地磁碟區上的任何作用中配額規則都會停用、而且配額規則會在執行重新同步之前刪除。

您可以使用 `volume quota policy rule create` 和 `volume quota modify` 在重新同步作業完成後建立及重新啟動配額規則的命令。

步驟

1. 在原始目的地 FlexGroup 磁碟區上、移除來源 FlexGroup 磁碟區與目的地 FlexGroup 磁碟區之間的資料保護鏡射關係： `snapmirror delete -destination-path svm_name:volume_name`

```
cluster2::> snapmirror delete -destination-path vsd:dst
```

2. 在原始來源 FlexGroup 磁碟區上、從來源 FlexGroup 磁碟區移除關係資訊： `snapmirror release -destination-path svm_name:volume_name -relationship-info-only`

   刪除SnapMirror關係之後、您必須先從來源FlexGroup 的SnapMirror Volume移除關係資訊、然後再嘗試重新同步作業。

```
cluster1::> snapmirror release -destination-path vsd:dst -relationship
-info-only true
```

3. 在新的目的地 FlexGroup 磁碟區上、建立鏡射關係： `snapmirror create -source-path src_svm_name:volume_name -destination-path dst_svm_name:volume_name -type XDP -policy MirrorAllSnapshots`

```
cluster1::> snapmirror create -source-path vsd:dst -destination-path
vss:src -type XDP -policy MirrorAllSnapshots
```

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

4. 在新的目的地 FlexGroup 磁碟區上、重新同步來源 FlexGroup ： `snapmirror resync -source-path svm_name:volume_name`

```
cluster1::> snapmirror resync -source-path vsd:dst
```

5. 監控 SnapMirror 傳輸： `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vsd:dst       XDP  vss:src        Snapmirrored
                                      Idle           -         true    -
vss:dst__0001 XDP  vss:src__0001  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0002 XDP  vss:src__0002  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0003 XDP  vss:src__0003  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0004 XDP  vss:src__0004  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0005 XDP  vss:src__0005  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0006 XDP  vss:src__0006  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0007 XDP  vss:src__0007  Snapmirrored
                                      Idle           -         true    -
vsd:dst__0008 XDP  vss:src__0008  Snapmirrored
                                      Idle           -         true    -
...
```

每個成分的 SnapMirror 關係狀態顯示為 `Snapmirrored` 這表示重新同步已成功。

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror版本"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

在FlexGroup SnapMirror關係中擴充功能區

在 SnapMirror 關係中展開 ONTAP FlexGroup Volume

從ONTAP 功能介紹9.3開始、您可以FlexGroup 在磁碟區中加入新的成分、以擴

充FlexGroup SnapMirror關係中的來源供應區和目的地供應區。您可以手動或自動擴充目的地磁碟區。

關於這項工作

- 此任務不適用於 SVM-DR 關係，SVM-DR 關係會自動管理 FlexGroup 磁碟區的擴充。
- 擴充之後FlexGroup 、SnapMirror關係的來源等量磁碟區和目的地FlexGroup 的等量資料必須相符。

  如果磁碟區中的成員數量不相符、SnapMirror傳輸就會失敗。

- 擴充程序進行中時、您不應執行任何SnapMirror作業。
- 如果在擴充程序完成之前發生災難、您必須中斷SnapMirror關係、並等待作業成功。

> 當擴充程序只在發生災難時才進行時、您應該中斷SnapMirror關係。發生災難時、中斷作業可能需要一些時間才能完成。執行重新同步作業之前、您應等待中斷作業順利完成。如果中斷作業失敗、您必須重試中斷作業。如果中斷作業失敗、FlexGroup 在中斷作業之後、部分新的成分可能仍留在目的地的景點。最好先手動刪除這些成分、然後再繼續。

展開 **SnapMirror** 關係的來源 **ONTAP FlexGroup Volume**

從功能更新9.3開始ONTAP 、您可以FlexGroup 在來源Volume中加入新的成分、以擴充SnapMirror關係的來源功能。您可以使用擴充一般FlexGroup 的邊量（讀寫磁碟區）的相同方式來擴充來源磁碟區。

步驟

1. 展開來源 FlexGroup Volume ：`volume expand -vserver vserver_name -volume fg_src -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster1::> volume expand -volume src_fg -aggr-list aggr1 -aggr-list
-multiplier 2 -vserver vs_src

Warning: The following number of constituents of size 50GB will be added
to FlexGroup "src_fg": 2.
Expanding the FlexGroup will cause the state of all Snapshot copies to
be set to "partial".
Partial Snapshot copies cannot be restored.
Do you want to continue? {y|n}: Y
[Job 146] Job succeeded: Successful
```

在將磁碟區擴充為部分之前所拍攝的所有快照狀態。

展開 **SnapMirror** 關係的目的地 **ONTAP FlexGroup Volume**

您可以FlexGroup 自動或手動擴充目的地的聲音量、並重新建立SnapMirror關係。根據預設、SnapMirror關係會設定為自動擴充、而來源FlexGroup Volume擴充時、目的地的還原Volume會自動擴充。

開始之前

- 來源FlexGroup 的流通量必須已經擴大。
- SnapMirror 關係必須在中 `SnapMirrored` 州/省。

  SnapMirror關係不得中斷或刪除。

關於這項工作

- 建立目的地FlexGroup 時、預設會將Volume設定為自動擴充。

  如有需要、您可以修改目的地FlexGroup 的聲音量、以手動擴充。

  最佳實務做法是FlexGroup 自動擴充目的地的景點。

- 所有SnapMirror作業都會失敗、直到來源FlexGroup 的Setrror Volume和目的地FlexGroup 的Setrror Volume都已擴充、而且擁有相同數量的成分為止。
- 如果FlexGroup 您在SnapMirror關係中斷或刪除之後擴充目的地的聲音區、就無法再次重新同步原始關係。

  如果您想要重複使用目的地 FlexGroup Volume ，請勿在刪除 SnapMirror 關係之後展開該 Volume 。

選擇

- 執行更新傳輸FlexGroup 以自動擴充目的地的更新磁碟區：

  a. 執行 SnapMirror 更新傳輸： `snapmirror update -destination-path svm:vol_name`

  b. 驗證 SnapMirror 關係的狀態是否在中 `SnapMirrored` 州： `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

  根據Aggregate的大小和可用度、會自動選取Aggregate、FlexGroup 並將符合來源版的組成要素的新成分新增至目的地FlexGroup 版的流通量。擴充之後、系統會自動觸發重新同步作業。

- 手動擴充目的地FlexGroup 的目標區域：

a. 如果 SnapMirror 關係處於自動展開模式、請將 SnapMirror 關係設定為手動展開模式： `snapmirror modify -destination-path svm:vol_name -is-auto-expand-enabled false`

```
cluster2::> snapmirror modify -destination-path vs_dst:dst_fg -is
-auto-expand-enabled false
Operation succeeded: snapmirror modify for the relationship with
destination "vs_dst:dst_fg".
```

b. 使 SnapMirror 關係不再運作： `snapmirror quiesce -destination-path svm:vol_name`

```
cluster2::> snapmirror quiesce -destination-path vs_dst:dst_fg
Operation succeeded: snapmirror quiesce for destination
"vs_dst:dst_fg".
```

c. 展開目的地 FlexGroup Volume ： `volume expand -vserver vserver_name -volume fg_name -aggr-list aggregate name,... [-aggr-list-multiplier constituents_per_aggr]`

```
cluster2::> volume expand -volume dst_fg -aggr-list aggr1 -aggr-list
-multiplier 2  -vserver vs_dst

Warning: The following number of constituents of size 50GB will be
added to FlexGroup "dst_fg": 2.
Do you want to continue? {y|n}: y
[Job 68] Job succeeded: Successful
```

d. 重新同步 SnapMirror 關係： `snapmirror resync -destination-path svm:vol_name`

```
cluster2::> snapmirror resync -destination-path vs_dst:dst_fg
Operation is queued: snapmirror resync to destination
"vs_dst:dst_fg".
```

e. 驗證 SnapMirror 關係的狀態 `SnapMirrored`： `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress
Healthy Updated
----------- ---- ------------ ------- -------------- ---------
------- --------
vs_src:src_fg
            XDP  vs_dst:dst_fg
                              Snapmirrored
                                      Idle           -         true
-
```

相關資訊

- "SnapMirror靜止"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

從 **ONTAP FlexGroup** 磁碟區執行 **SnapMirror** 單一檔案還原

從ONTAP 功能不完整的9.8開始、您可以從FlexGroup SnapMirror保存庫或從udp目的地還原單一檔案。

關於這項工作

- 您可以從任何幾何形狀的FlexGroup磁碟區恢復到任何幾何形狀的FlexGroup磁碟區。
- 每個還原操作僅支援一個檔案。
- 您可以還原到原始來源FlexGroup磁碟區或新的FlexGroup區。
- 不支援遠端隔離檔案查詢。

  如果來源檔案設有保護區、則單一檔案還原會失敗。

- 您可以重新啟動或清理中止的單一檔案復原。
- 您應該使用 `clean-up-failure`選項 `snapmirror restore`命令。

  如"指令參考資料ONTAP"需詳細 `snapmirror restore`資訊，請參閱。

- 當FlexGroup單一檔案還原正在進行或處於中止狀態時，支援擴充FlexGroup磁碟區。

步驟

1. 從 FlexGroup 磁碟區還原檔案： `snapmirror restore -destination-path destination_path -source-path source_path -file-list /f1 -throttle throttle -source-snapshot snapshot`

以下是FlexGroup 一個關於使用單一檔案還原功能的範例。

```
vserverA::> snapmirror restore -destination-path vs0:fg2 -source-path
vs0:fgd -file-list /f1 -throttle 5 -source-snapshot snapmirror.81072ce1-
d57b-11e9-94c0-005056a7e422_2159190496.2019-09-19_062631
[Job 135] Job is queued: snapmirror restore from source "vs0:fgd" for
the snapshot snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631.
vserverA::> snapmirror show

Source              Destination Mirror   Relationship
Total Last
Path       Type   Path            State    Status           Progress
Healthy Updated
---------- ----      ------------     -------    ---------
----- --------- ------- --------
vs0:v1d RST    vs0:v2          -           Transferring Idle 83.12KB
true 09/19 11:38:42

vserverA::*> snapmirror show vs0:fg2

Source Path: vs0:fgd
Source Cluster: -
Source Vserver: vs0
Source Volume: fgd
Destination Path: vs0:fg2
Destination Cluster: -
Destination Vserver: vs0
Destination Volume: fg2
Relationship Type: RST
Relationship Group Type: none
Managing Vserver: vs0
SnapMirror Schedule: -
SnapMirror Policy Type: -
SnapMirror Policy: -
Tries Limit: -
Throttle (KB/sec): unlimited
Current Transfer Throttle (KB/sec): 2
Mirror State: -
Relationship Status: Transferring
File Restore File Count: 1
File Restore File List: f1
Transfer Snapshot: snapmirror.81072ce1-d57b-11e9-94c0-
005056a7e422_2159190496.2019-09-19_062631
Snapshot Progress: 2.87MB
Total Progress: 2.87MB
```

```
Network Compression Ratio: 1:1
Snapshot Checkpoint: 2.97KB
Newest Snapshot: -
Newest Snapshot Timestamp: -
Exported Snapshot: -
Exported Snapshot Timestamp: -
Healthy: true
Physical Replica: -
Relationship ID: e6081667-dacb-11e9-94c0-005056a7e422
Source Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Destination Vserver UUID: 81072ce1-d57b-11e9-94c0-005056a7e422
Current Operation ID: 138f12e6-dacc-11e9-94c0-005056a7e422
Transfer Type: cg_file_restore
Transfer Error: -
Last Transfer Type: -
Last Transfer Error: -
Last Transfer Error Codes: -
Last Transfer Size: -
Last Transfer Network Compression Ratio: -
Last Transfer Duration: -
Last Transfer From: -
Last Transfer End Timestamp: -
Unhealthy Reason: -
Progress Last Updated: 09/19 07:07:36
Relationship Capability: 8.2 and above
Lag Time: -
Current Transfer Priority: normal
SMTape Operation: -
Constituent Relationship: false
Destination Volume Node Name: vserverA
Identity Preserve Vserver DR: -
Number of Successful Updates: 0
Number of Failed Updates: 0
Number of Successful Resyncs: 0
Number of Failed Resyncs: 0
Number of Successful Breaks: 0
Number of Failed Breaks: 0
Total Transfer Bytes: 0
Total Transfer Time in Seconds: 0
Source Volume MSIDs Preserved: -
OpMask: ffffffffffffffff
Is Auto Expand Enabled: -
Source Endpoint UUID: -
Destination Endpoint UUID: -
Is Catalog Enabled: false
```

相關資訊

- "SnapMirror 顯示"

從 **SnapVault** 備份還原 **ONTAP FlexGroup** 磁碟區

您可以從 SnapVault 次要 Volume 中的快照，執行 FlexGroup Volume 的完整磁碟區還原作業。您可以將FlexGroup 還原成原始來源Volume或新FlexGroup 的還原成新的版本。

開始之前

當您從SnapVault 還原為FlexGroup 還原為還原為資料的功能時、必須注意某些考量事項。

- 只有 SnapVault 備份的部分快照才支援基礎還原。目的地 Volume 中的組成數量必須符合擷取快照時來源 Volume 中的組成數量。
- 如果還原作業失敗、則在還原作業完成之前、不允許執行其他作業。
  您可以重試還原作業、或使用執行還原作業 `cleanup` 參數。
- 一個支援區只能是一個備份關係或還原關係的來源磁碟區。FlexGroup
  不能將一個資料區做為兩個相依關係的來源、兩個還原關係、或是一個相依關係與還原關係。FlexGroup SnapVault SnapVault
- 無法並行執行還原與備份作業。SnapVault
  當正在執行基準還原作業或遞增還原作業時、您應該停止備份作業。
- 您必須從目的地 FlexGroup Volume 中止部分快照的還原作業。您無法從來源磁碟區中止部分快照的還原作業。
- 如果您中止還原作業，則必須使用先前還原作業所使用的相同快照來重新啟動還原作業。

關於這項工作

在執行FlexGroup 還原之前、會停用目的地聲音區上的任何作用中配額規則。

您可以使用 `volume quota modify` 還原作業完成後重新啟動配額規則的命令。

步驟

1. 還原 FlexGroup Volume ： `snapmirror restore -source-path` *`src_svm:src_flexgroup`* `-destination-path` *`dest_svm:dest_flexgroup`* `-snapshot` *`snapshot_name`*
   `snapshot_name`是要從來源磁碟區還原至目的地磁碟區的快照。如果未指定快照，則會從最新的快照還原目的地磁碟區。

```
vserverA::> snapmirror restore -source-path vserverB:dstFG -destination
-path vserverA:newFG -snapshot daily.2016-07-15_0010
Warning: This is a disruptive operation and the volume vserverA:newFG
will be read-only until the operation completes
Do you want to continue? {y|n}: y
```

相關資訊

- "SnapMirror還原"

停用 ONTAP FlexGroup 磁碟區上的 SVM 保護

當 SVM DR 旗標設定為時 `protected` 在 FlexGroup 磁碟區上、您可以將旗標設為「未受保護」、以停用 SVM DR `protection` 在 FlexGroup 磁碟區上。

開始之前

- 一線與二線之間的SVM DR關係是健全的。
- SVM DR 保護參數設為 `protected`。

步驟

1. 使用停用保護 `volume modify` 變更的命令 `vserver-dr-protection` FlexGroup Volume 的參數 `unprotected`。

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection unprotected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. 更新次要站台的 SVM ： `snapmirror update -destination-path destination_svm_name: -source-path Source_svm_name:`
3. 驗證 SnapMirror 關係是否健全： `snapmirror show`
4. 驗證 FlexGroup SnapMirror 關係是否已移除： `snapmirror show -expand`

相關資訊

- "SnapMirror 顯示"
- "SnapMirror 更新"

在 ONTAP FlexGroup 磁碟區上啟用 SVM 保護

當 SVM DR 保護旗標設定為時 `unprotected` 在 FlexGroup 磁碟區上、您可以將旗標設定為 `protected` 以啟用 SVM DR 保護。

開始之前

- 一線與二線之間的SVM DR關係是健全的。
- SVM DR 保護參數設為 `unprotected`。

步驟

1. 使用啟用保護 `volume modify` 以變更 `vserver-dr-protection` FlexGroup Volume 的參數 `protected`。

```
cluster2::> volume modify -vserver vs1 -volume fg_src -vserver-dr
-protection protected
[Job 5384] Job is queued: Modify fg_src.
[Job 5384] Steps completed: 4 of 4.
cluster2::>
```

2. 更新次要站台的 SVM ： `snapmirror update -destination-path destination_svm_name -source-path source_svm_name`

```
snapmirror update -destination-path vs1_dst: -source-path vs1:
```

3. 驗證 SnapMirror 關係是否健全： `snapmirror show`

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                Idle           -         true    -
```

4. 驗證 FlexGroup SnapMirror 關係是否健全： `snapmirror show -expand`

```
cluster2::> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs1:        XDP  vs1_dst:     Snapmirrored
                                    Idle           -         true    -
vs1:fg_src  XDP  vs1_dst:fg_src
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0001
            XDP  vs1_dst:fg_src__0001
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0002
            XDP  vs1_dst:fg_src__0002
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0003
            XDP  vs1_dst:fg_src__0003
                             Snapmirrored
                                    Idle           -         true    -
vs1:fg_src__0004
            XDP  vs1_dst:fg_src__0004
                             Snapmirrored
                                    Idle           -         true    -
6 entries were displayed.
```

相關資訊

- "SnapMirror 顯示"

將功能區轉換為FlexVol 功能區FlexGroup

瞭解如何將 ONTAP FlexVol Volume 轉換為 FlexGroup Volume

如果您想要將FlexVol 一個不超過空間限制的範圍擴大到一個範FlexVol 圍、可以將該範圍內的整個過程轉換成FlexGroup 一個地方。從ONTAP NetApp 9.7開始、您可以將FlexVol SnapMirror關係中的獨立式SnapMirror Volume或FlexVol SnapMirror Volume、轉換成FlexGroup SnapMirror Volume。

將**FlexVol** 功能區轉換**FlexGroup** 為功能區的考量事項

您應該意識到"支援的功能和操作"在您決定將FlexVol磁碟區轉換為FlexGroup磁碟區之前。

轉換期間不支援作業

進行Volume轉換時、不允許執行下列作業：

- Volume搬移
- Aggregate重新配置
- 在高可用度組態中進行計畫性接管與恢復
- 以高可用度組態手動和自動還原
- 叢集升級與還原
- FlexClone Volume分割
- Volume重新裝載
- Volume修改與自動調整大小
- Volume重新命名
- 將物件存放區附加至Aggregate
- 協調MetroCluster 以進行交換、以進行不協調的組態設定
- SnapMirror作業
- 從快照還原
- 配額作業
- 儲存效率作業

您可以FlexGroup 在成功轉換後、在整個流程中執行這些作業。

不支援**FlexGroup** 的組態

- 離線或受限Volume
- SVM根Volume
- SAN
- SMB 1.0
- NVMe命名空間
- 遠端Volume陰影複製服務（VSS）

將 **ONTAP FlexVol Volume** 轉換為 **ONTAP FlexGroup Volume**

從功能升級至功能區9.7開始ONTAP 、FlexVol 您可以在不FlexGroup 需要資料複本或額外磁碟空間的情況下、就地將一個功能區轉換成一個功能區。

開始之前

- 從 ONTAP 9.8 開始，可將轉換的磁碟區轉換為 FlexGroup 磁碟區。

- 正在轉換的這個版本必須在線上。FlexVol
- 在這個過程中、執行的操作和設定FlexVol 必須與轉換程序相容。

  請檢查是否有下列情況、以避免轉換成功：

  - FlexVol Volume 是使用 7MTT （ ONTAP 9.7 ）從 7-Mode 轉換而來。

    轉換後的磁碟區可以從 ONTAP 9.8 開始轉換。

  - 磁碟區啟用了 FlexGroup 磁碟區尚未支援的功能；例如，SAN LUN、Windows NFS、SMB1、快照命名/自動刪除、vmalign 設定、早於 ONTAP 9.11.1 版本的 SnapLock（從 ONTAP 9.11.1 開始支援 SnapLock）、空間 SLO 或邏輯空間強制執行/報表。如需更多資訊、請參閱 "支援且不支援FlexGroup的功能組態"。
  - 要轉換的 FlexVol Volume 所在的 SVM 目前使用 SVM DR 。
  - NetApp FlexClone 磁碟區存在、 FlexVol 磁碟區是父磁碟區。正在轉換的磁碟區不能是父磁碟區或複製磁碟區。
  - Volume 是 NetApp FlexCache 原始 Volume 。
  - 對於 ONTAP 9.7 及更早版本， NetApp 快照不得超過 255 個。ONTAP 9.8 及更新版本支援 1023 個快照。
  - 實現儲存效率。這些必須停用、且可在轉換後重新啟用。
  - Volume 是 SnapMirror 關係的來源、目的地尚未轉換。
  - Volume 是主動（非停止） SnapMirror 關係的一部分。
  - 該卷上的自主勒索軟體防護 (ARP) 已停用。轉換完成前，請勿再次啟用該功能。
  - 配額已啟用。這些必須停用、且可在轉換後重新啟用。
  - Volume 名稱長度超過 197 個字元。
  - 磁碟區與應用程式相關聯。

    這僅適用於 ONTAP 9.7 。ONTAP 9.8 中已移除此限制。

  - ONTAP 程序正在執行、例如鏡射、工作、 wafliron 、 NDMP 備份、 及處理中的 inode 轉換。
  - 該 Volume 是 SVM 根 Volume 。
  - 音量太大。

    如果存在任何這些不相容的情況、則會在 FlexVol Volume 終止時產生錯誤訊息、且 Volume 轉換也會中止。您可以採取修正行動、然後重試轉換。

- 如果 FlexVol Volume 目前的最大容量為 80% 或更高、請考慮將資料複製到新建立的 FlexGroup Volume 、而非執行就地轉換。雖然 FlexGroup 成員磁碟區會隨著時間自然重新平衡、但將大容量 FlexVol 磁碟區轉換為 FlexGroup 磁碟區可能會產生效能或平衡問題、而這些問題不會在成員磁碟區之間快速重新平衡。

  轉換非常大FlexGroup 的版次時、FlexGroup 會產生非常完整的版次成員組成、進而造成效能問題。如需更多資訊、請參閱FlexGroup TR中的「當不建立一套功能時」一節 "《英文版-最佳實務做法與實作指南》FlexGroup"。

步驟

1. 驗證 FlexVol Volume 是否在線上：`volume show -fields vol_name volume-style-extended,state`

```
cluster-1::> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexvol
```

2. 驗證FlexVol 是否可在不發生問題的情況下轉換此功能：

   a. 登入進階權限模式：`set -privilege advanced`

   b. 驗證轉換程序：`volume conversion start -vserver vs1 -volume flexvol -check -only true`

   在轉換磁碟區之前、您必須先修正所有錯誤。

   ⓘ 您無法將FlexGroup 某個不全的功能區轉換回FlexVol 一個不全的功能區。

3. 開始轉換：`volume conversion start -vserver svm_name -volume vol_name`

```
cluster-1::*> volume conversion start -vserver vs0 -volume my_volume

Warning: Converting flexible volume "my_volume" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion Snapshot copies cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

4. 確認轉換成功：`volume show vol_name -fields volume-style-extended,state`

```
cluster-1::*> volume show my_volume -fields volume-style-extended,state
vserver volume    state  volume-style-extended
------- --------- ------ ---------------------
vs0     my_volume online flexgroup
```

結果

將此功能轉換成單一成員的《不完整的不完整影像：FlexVol FlexGroup

完成後

您可以視需要擴充FlexGroup 「功能區」。

若要將FlexVol 位於FlexGroup SnapMirror中的SnapMirror與不景區的SnapMirror關係轉換成不景區的SnapMirror關係ONTAP 、您必須先轉換目的地FlexVol 的SnapMirror Volume、再轉換來源FlexVol 的不景區。

關於這項工作

- 在SnapMirror/ SnapVault關係中，除了轉換流程之外，不支援將 FlexGroups 與FlexVol磁碟區混合使用。
- FlexGroup 轉換僅支援 SnapMirror 非同步關係。
- SnapMirror雲端關係不支援FlexGroup轉換。
- 轉換時間取決於多個變數。其中一些變數包括：
  - 控制器的 CPU
  - 其他應用程式 CPU 的使用率
  - 初始快照中的資料量
  - 網路頻寬
  - 其他應用程式使用的頻寬

開始之前

- 正在轉換的這個版本必須在線上。FlexVol
- SnapMirror關係中的來源FlexVol 供應區不可以是多個SnapMirror關係的來源磁碟區。

  從ONTAP 支援的範圍僅為0.9.1.1開始、FlexGroup 即可支援針對SnapMirror的範圍。如需更多資訊、請參閱 "為 FlexGroup 磁碟區建立 SnapMirror 串聯和展開關係的考量事項"。

- 在這個過程中、執行的操作和設定FlexVol 必須與轉換程序相容。

  如果FlexVol 現象不一致、而且中止了Volume轉換、就會產生錯誤訊息。您可以採取修正行動、然後重試轉換。

步驟

1. 驗證 SnapMirror 關係是否健全：

   ```
   snapmirror show
   ```

   只能轉換XDP類型的鏡射關係。

   範例：

```
cluster2::> snapmirror show

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:src_dpv DP   vs2:dst_dpv  Snapmirrored
                                     Idle           -         true    -
vs0:src_xdp XDP  vs2:dst_xdp  Snapmirrored
                                     Idle           -         true    -
```

2. 確認來源Volume是否相容於轉換：

   a. 登入進階權限模式：

      ```
      set -privilege advanced
      ```

   b. 驗證轉換程序：

      ```
      volume conversion start -vserver <src_svm_name> -volume <src_vol>
      -check-only true
      ```

      範例：

```
volume conversion start -vserver vs1 -volume src_vol -check-only true
```

+
在轉換磁碟區之前、您必須先修正所有錯誤。

3. 將目的地FlexVol 的聲音量轉換為FlexGroup 聲音量。

   a. 使 FlexVol SnapMirror 關係不再運作：

      ```
      snapmirror quiesce -destination-path <dest_svm:dest_volume>
      ```

      範例：

      ```
      cluster2::> snapmirror quiesce -destination-path vs2:dst_xdp
      ```

b. 開始轉換：

```
volume conversion start -vserver <dest_svm> -volume <dest_volume>
```

範例：

```
cluster-1::> volume conversion start -vserver vs2 -volume dst_xdp

Warning: After the volume is converted to a FlexGroup, it will not be
possible
to change it back to a flexible volume.
Do you want to continue? {y|n}: y

[Job 510] Job succeeded: SnapMirror destination volume "dst_xdp" has
been successfully converted to a FlexGroup volume.
You must now convert the relationship's source volume, "vs0:src_xdp", to
a FlexGroup.
Then, re-establish the SnapMirror relationship using the "snapmirror
resync" command.
```

4. 將來源 FlexVol Volume 轉換為 FlexGroup Volume ：`

```
volume conversion start -vserver <src_svm_name> -volume <src_vol_name>
```

範例：

```
cluster-1::> volume conversion start -vserver vs0 -volume src_xdp

Warning: Converting flexible volume "src_xdp" in Vserver "vs0" to a
FlexGroup
         will cause the state of all Snapshot copies from the volume to
be set
         to "pre-conversion". Pre-conversion snapshots cannot be
         restored.
Do you want to continue? {y|n}: y
[Job 57] Job succeeded: success
```

5. 重新同步關係：

```
snapmirror resync -destination-path dest_svm_name:dest_volume
```

範例：

```
cluster2::> snapmirror resync -destination-path vs2:dst_xdp
```

完成後

您必須確保當來源FlexGroup 的供應區擴大以包含更多成分時、目的地Volume也會隨之擴充。

相關資訊

- "SnapMirror靜止"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

資料區管理FlexCache

瞭解 ONTAP FlexCache Volume

NetApp FlexCache 技術可加速資料存取、減少 WAN 延遲、並降低讀取密集工作負載的 WAN 頻寬成本、尤其是用戶端需要重複存取相同資料的地方。當您建立 FlexCache Volume 時、會建立已存在（來源） Volume 的遠端快取、該磁碟區只包含來源 Volume 的主動存取資料（熱資料）。

當 FlexCache 磁碟區收到其所包含之熱資料的讀取要求時、其回應速度可能會比原始磁碟區快、因為資料不需要傳輸至最遠的範圍即可到達用戶端。 如果 FlexCache 磁碟區收到不常讀取資料（冷資料）的讀取要求、它會從原始磁碟區擷取所需資料、然後在處理用戶端要求之前儲存資料。隨後對該資料的讀取要求會直接從 FlexCache 磁碟區傳送。在第一次要求之後、資料不再需要在網路上傳輸、也不需要從負載沉重的系統中傳輸。例如、假設您在叢集內的單一存取點遇到瓶頸、而這些資料是經常要求的資料。 您可以在叢集中使用 FlexCache 磁碟區、為熱資料提供多個掛載點、藉此減少瓶頸並提高效能。另一個例子是、假設您需要減少從多個叢集存取的磁碟區的網路流量。您可以使用 FlexCache Volume 在網路中的叢集之間、從來源磁碟區散佈熱資料。 如此可讓使用者更接近存取點、進而減少 WAN 流量。

您也可以使用 FlexCache 技術來改善雲端和混合雲環境的效能。FlexCache Volume 可將內部部署資料中心的資料快取至雲端、協助您將工作負載移轉至混合雲。 您也可以使用 FlexCache 磁碟區、將資料從一個雲端供應商快取至另一個雲端供應商、或是在同一個雲端供應商的兩個區域之間、來移除雲端封閉環境。

從功能升級到功能升級到ONTAP 功能升級 "啟用全域檔案鎖定" 橫跨所有 FlexCache Volume 。全域檔案鎖定可防止使用者存取已由其他使用者開啟的檔案。 然後、原始磁碟區的更新會同時發佈到所有 FlexCache 磁碟區。

從 ONTAP 9.9.1 開始、 FlexCache Volume 會保留找不到的檔案清單。 這有助於減少網路流量、因為當用戶端搜尋不存在的檔案時、不再需要傳送多通電話給來源伺服器。

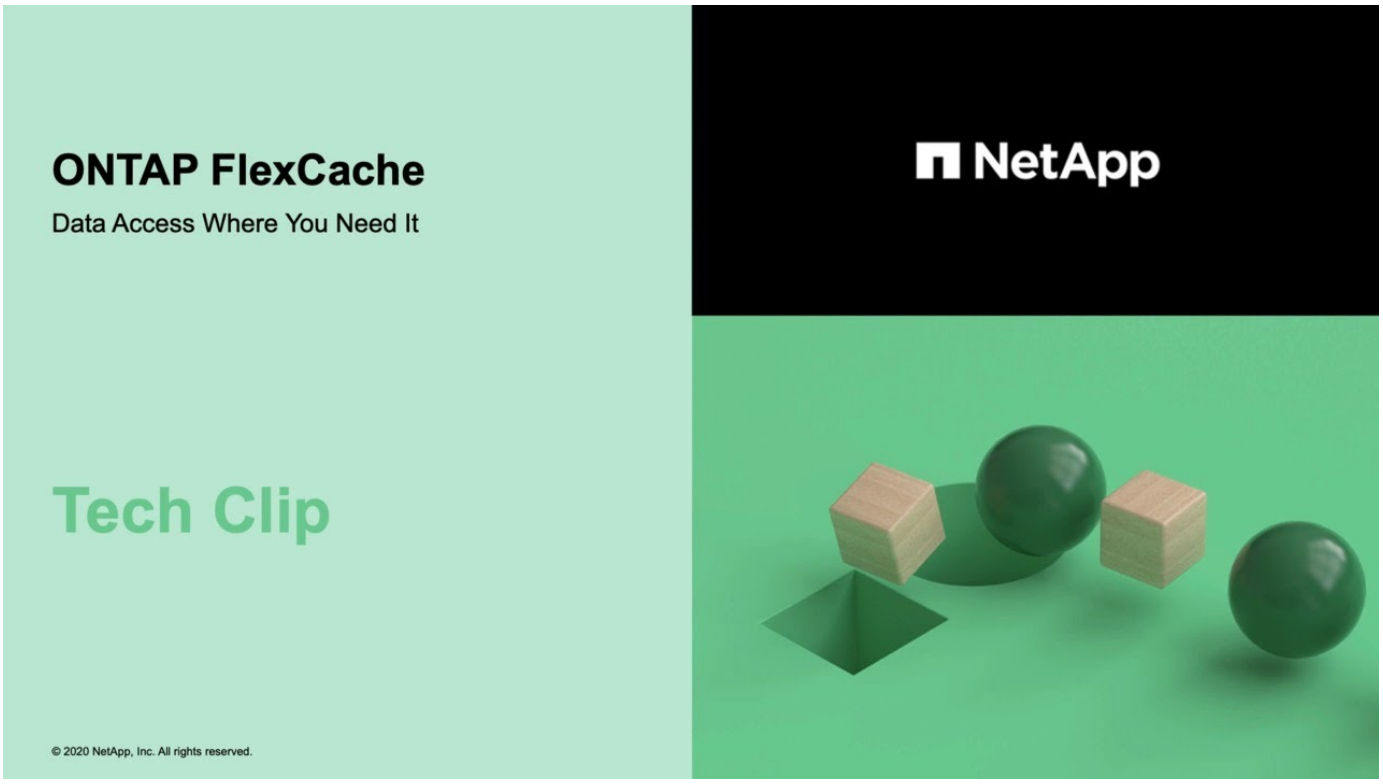
其他清單 "FlexCache Volume 及其原始磁碟區支援的功能"也提供 ONTAP 版本支援的通訊協定清單。

您可以在中深入瞭解 ONTAP FlexCache 技術的架構 "TR-4743：FlexCache 《不ONTAP 實的"。

影片

如何減少**WAN**延遲、縮短全域資料的讀取時間**FlexCache**

深入瞭**ONTAP FlexCache** 解**VMware**的效能優勢！



ONTAP FlexCache Volume 支援和不支援的功能

從 ONTAP 9.5 開始，您可以設定 FlexCache Volume 。支援 FlexVol Volume 做為原始磁

碟區、並支援 FlexGroup 磁碟區做為 FlexCache 磁碟區。從 ONTAP 9.7 開始， FlexVol Volume 和 FlexGroup Volume 都支援做為原始 Volume 。來源 Volume 和 FlexCache Volume 支援的功能和傳輸協定會有所不同。

只要快取磁碟區和原始磁碟區都在支援的 ONTAP 版本上執行、就能互通。請記住、只有在快取和原始伺服器至少執行支援所在的 ONTAP 版本或更新的 ONTAP 版本時、才能支援這些功能。

FlexCache 磁碟區與原始磁碟區之間的 **ONTAP** 版本支援

原始磁碟區與快取磁碟區之間支援的建議 ONTAP 版本，不超過四個版本的舊版或四個版本。例如，如果快取使用的是 ONTAP 9.14.1 ，則原始伺服器可以使用的最早版本是 ONTAP 9.10.1 。

支援的傳輸協定

傳輸協定	支援來源磁碟區？	支援的功能是什麼？FlexCache
NFSv3.	是的	是的
NFSv4.	是的 若要使用 NFSv4.x 通訊協定存取快取磁碟區、來源叢集和快取叢集都必須使用 ONTAP 9.10.1 或更新版本。原始叢集和 FlexCache 叢集可以有不同的 ONTAP 版本、但兩者都應該是 ONTAP 9.10.1 和更新版本、例如、原始伺服器可以有 ONTAP 9.10.1 、而且快取可以有 ONTAP 9.11.1 。	是的 從 ONTAP 9.10.1 開始支援。 若要使用 NFSv4.x 通訊協定存取快取磁碟區、來源叢集和快取叢集都必須使用 ONTAP 9.10.1 或更新版本。原始叢集和 FlexCache 叢集可以有不同的 ONTAP 版本、但兩者都應該是 ONTAP 9.10.1 和更新版本、例如、原始伺服器可以有 ONTAP 9.10.1 、而且快取可以有 ONTAP 9.11.1 。
NFSv4.2	是的	否
中小企業	是的	是的 支援從ONTAP 功能9.8開始。

支援的功能

功能	支援來源磁碟區？	支援的功能是什麼？FlexCache

自主勒索軟體保護	是的 支援以 ONTAP 9.10.1 開頭的 FlexVol 原始磁碟區、並支援以 ONTAP 9.13.1 開頭的 FlexGroup 原始磁碟區。請參閱 "自主勒索軟體保護的使用案例和考量"。	否
防毒軟體	是的 從 ONTAP 9.7 開始支援。	不適用 如果您在原始伺服器上設定防毒掃描、則快取中不需要。無論寫入來源為何、原始防毒掃描都會在寫入前偵測感染病毒的檔案。如需搭配 FlexCache 使用防毒掃描的詳細資訊、請參閱 "FlexCache with ONTAP 技術報告"。
稽核	是的 從 ONTAP 9.7 開始支援。 您可以使用原生 ONTAP 稽核來稽核 FlexCache 關聯中的 NFS 檔案存取事件。 如需詳細資訊、請參閱 稽核FlexCache 功能的考量	是的 從 ONTAP 9.7 開始支援。 您可以使用原生 ONTAP 稽核來稽核 FlexCache 關聯中的 NFS 檔案存取事件。 如需詳細資訊、請參閱 稽核FlexCache 功能的考量
Cloud Volumes ONTAP	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始
壓實	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始	是的 支援從ONTAP 支援的功能從支援的功能9.7開始
壓縮	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始

重複資料刪除	是的	是的 從功能支援從功能支援到功能支援到功能的9.6開始、可支援FlexCache 即時重複資料刪除技術。ONTAP從NetApp 9.7開始、支援從各個磁FlexCache 碟區開始的各個磁碟區重複資料刪除技術ONTAP 。
FabricPool	是的	是的 支援從ONTAP 支援的功能從支援的功能9.7開始 您可以建立一個FlexCache磁碟區作為啟用了FabricPool分層功能的來源磁碟區的緩存，但FlexCache磁碟區本身不能分層。
解決災難恢復問題FlexCache	是的	是的 僅支援ONTAP 從支援NFSv3傳輸協定的版本S9.9開始。不能將資料區放在獨立的SVM或獨立的叢集內。FlexCache
流通量FlexGroup	是的 支援從ONTAP 支援的功能從支援的功能9.7開始	是的
流通量FlexVol	是的	否
FPolicy	是的 支援從ONTAP 支援的功能從支援的功能9.7開始	是的 從 ONTAP 9.7 開始支援 NFS 。從 ONTAP 9.14.1 開始支援中小企業。
組態MetroCluster	是的 支援從ONTAP 支援的功能從支援的功能9.7開始	是的 支援從ONTAP 支援的功能從支援的功能9.7開始

Microsoft卸載資料傳輸（ODX）	是的	否
NetApp Aggregate Encryption（NAE）	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始
NetApp Volume Encryption（NVE）	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始	是的 支援ONTAP 從支援的功能為從支援的功能9.6開始
ONTAP S3 NAS 貯體	是的 從 ONTAP 9.12.1 開始支援	是的 從 ONTAP 9.18.1 版本開始支援
QoS	是的	是的 不支援FlexCache 檔案層級的QoS以供支援使用。
qtree	是的 從 ONTAP 9.6 開始、您可以建立和修改 qtree 。在來源上建立的 qtree 可在快取中存取。	否
配額	是的 從 ONTAP 9.6 開始、使用者、群組和 qtree 都支援 FlexCache 原始磁碟區的配額強制。	否 使用 FlexCache 寫入模式（預設模式）時、快取上的寫入會轉送到原始磁碟區。配額會在原點強制執行。 從ONTAP 功能支援的不只是功能性的9.6、FlexCache 還能在功能區上支援遠端配額（rquota）。
SMB變更通知	是的	是的 從 ONTAP 9.14.1 開始、快取支援 SMB 變更通知。

資料量SnapLock	否	否
SnapMirror 非同步關係 *	是的	否
	• FlexCache 起源： • 您可以使用來源 FlexVol 的 FlexCache Volume • 您可以使用來源 FlexGroup 的 FlexCache Volume • 您可以在FlexCache SnapMirror關係中、從來源主要Volume取得一個解決功能區。 • 從功能不全的9.8開始ONTAP、SnapMirror次要Volume可以是FlexCache 一個來源不全的Volume。SnapMirror 次要磁碟區必須閒置、而且沒有主動式 SnapMirror 更新；否則、FlexCache 建立將會失敗。	SnapMirror 同步關係
否	否	SnapRestore
是的	否	快照
是的	否	SVM DR組態
是的 從ONTAP 9.5 開始支援。SVM DR關係的主 SVM 可以具有來源磁碟區；但是，如果您執行的是ONTAP ONTAP之前的版本，當 SVM DR關係中斷時，必須使用新的來源磁碟區重新建立FlexCache關係。 從ONTAP 9.18.1 開始，當來源 SVM 發生故障轉移時，DR 站點的快取會自動切換到來源。無需手動恢復步驟。 了解如何建立FlexCache磁碟區。	否 您可以FlexCache 在主要SVM中使用支援功能、但不能在次要SVM中使用。在主要SVM中的FlexCache任何一個SVM Volume都不會複寫、因為它是SVM DR關係的一部分。	儲存層級存取保護（slag）
否	否	資源隨需配置

是的	是的 支援從ONTAP 支援的功能從支援的功能9.7開始	Volume複製
是的 支援從ONTAP 功能上的支援從還原9.6開始、複製來源磁碟區和來源磁碟區中的檔案。	否	Volume搬移
是的	是（僅適用於Volume成員） ONTAP 9.6 及更新版本支援 FlexCache Volume 的移動 Volume 成分。	Volume重新裝載
否	否	適用於陣列整合的 VStorage API （ VAAI ）

在9.5版之前的版本中、來源地不僅僅能將資料提供給執行以7-Mode運作的VMware 8.2.x系統上所建立的不實資料。ONTAP FlexVol FlexCache Data ONTAP從推出版的S25 9.5開始ONTAP 、來源FlexVol 地的不穩定區也能在FlexCache 功能區上提供資料給ONTAP 功能區上的不穩定區。有關從 7-Mode FlexCache 移轉至 ONTAP 9 FlexCache 的資訊、請參閱"NetApp 技術報告 4743 ： FlexCache in ONTAP"。

ONTAP FlexCache Volume 規模調整準則

在開始配置磁碟區之前、您必須瞭解FlexCache 到有關使用功能的限制。

一個來源Volume的大小限制FlexVol 適用於來源Volume。一個不符合原點的Volume大小FlexCache 可以小於或等於原始Volume。最佳實務做法FlexCache 是讓整個範本大小至少達到原點Volume大小的10%。

您也必須瞭解FlexCache 下列有關《關於》的額外限制：

限制	更新版本ONTAP	更新ONTAP	ONTAP 9.6 - 9.5
您可以從來源Volume建立的FlexCache 最大數量的不全區資料	100	10.	10.
建議的每個節點原始磁碟區數量上限	100	100	10.
建議FlexCache 的每個節點的最大數量的不均資料量	100	100	10.
建議的每個節點的每個共享區的最大FlexGroup 數量FlexCache	800	800	40.
每個節點每FlexCache 個個個個元區的最大構成數	32.	32.	32.

相關資訊

- "NetApp互通性"

建立 ONTAP FlexCache Volume

您可以在同一 ONTAP 叢集中建立 FlexCache 磁碟區，以提高存取熱點物件時的效能。如果您在不同位置擁有資料中心，則可以在遠端 ONTAP 叢集上建立 FlexCache 磁碟區，以加快資料存取速度。

關於這項工作

- 從 ONTAP 9.18.1 開始，您可以在建立磁碟區時將 `-is-s3-enabled`選項設定為 `true`，以在 FlexCache 磁碟區上啟用 NAS S3 儲存桶存取權限。此選項預設為停用狀態。
- 從ONTAP 9.18.1 開始， FlexCache支援為具有 SVM-DR 關係的 SVM 的來源磁碟區建立快取磁碟區。

  如果您執行的是ONTAP 9.18.1 或更高版本，則儲存管理員必須先將快取 SVM 與 SVM-DR 關係中的主來源 SVM 和輔助來源 SVM 建立對等關係，然後再建立屬於 SVM-DR 關係的來源磁碟區的快取磁碟區。
- 從 ONTAP 9.14.0 開始、您可以從加密來源建立未加密的 FlexCache Volume 。
- 從 ONTAP 9.7 開始，FlexVol 磁碟區和 FlexGroup 磁碟區都支援作為來源磁碟區。
- 從 ONTAP 9.5 開始、 FlexCache 支援 FlexVol Volume 做為原始磁碟區、 FlexGroup 磁碟區做為 FlexCache 磁碟區。

開始之前

- 您必須執行ONTAP 的是版本不含更新版本的版本。
- 如果您執行的是 ONTAP 9 6 或更早版本"新增 FlexCache 授權"、則必須。

  ONTAP 9.7 或更新版本不需要 FlexCache 授權。從 ONTAP 9.7 開始、 FlexCache 功能隨附於 ONTAP 、不再需要授權或啟動。

如果HA配對正在使用 "加密SAS或NVMe磁碟機（SED、NSE、FIPS）"、您必須遵循主題中的指示 "將FIPS磁碟機或SED恢復為無保護模式" 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

範例 **12.** 步驟

系統管理員

1. 如果 FlexCache 磁碟區與來源磁碟區位於不同的 ONTAP 叢集上，請建立叢集對等關係：
   a. 在本機叢集中、按一下*保護>總覽*。
   b. 展開 * 叢集間設定 * 、按一下 * 新增網路介面 * 、然後新增叢集的叢集間網路介面。

      在遠端叢集上重複此步驟。

   c. 在遠端叢集中、按一下*保護>總覽*。按一下 ⋮ 「叢集對等點」區段、然後按一下「 * 產生複雜密碼 * 」。
   d. 複製產生的通關密碼、然後貼到本機叢集中。
   e. 在本機叢集的「叢集對等端點」下、按一下「對等叢集」、然後對等本機和遠端叢集。
2. 建立 SVM 對等關係：

   在 Storage VM Peers 下、按一下、然後按一下 ⋮ * Peer Storage VMS* 來對等儲存 VM 。
3. 選擇*儲存>磁碟區*。
4. 選取*「Add*」。
5. 選取 * 更多選項 * 、然後選取 * 新增為遠端磁碟區的快取 * 。

   如果您執行的是 ONTAP 9.8 或更新版本、而且想要停用 QoS 或選擇自訂 QoS 原則、請按一下 * 更多選項 * 、然後在 * 儲存與最佳化 * 下、選取 * 效能服務層級 * 。

CLI

1. 如果FlexCache 要建立的實體磁碟區位於不同的叢集、請建立叢集對等關係：
   a. 在目的地叢集上、與資料保護來源叢集建立對等關係：

      ```
      cluster peer create -generate-passphrase -offer-expiration
      MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
      <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
      -ipspace <ipspace_name>
      ```

      從ONTAP 功能支援的9.6開始、建立叢集對等關係時、預設會啟用TLS加密。支援TLS加密、以便在來源FlexCache 與實體磁碟區之間進行叢集間通訊。您也可以視需要停用叢集對等關係的TLS加密。

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. 在來源叢集上、驗證來源叢集到目的地叢集的驗證：

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. 如果 FlexCache 磁碟區與原始磁碟區位於不同的 SVM 、請與建立 SVM 對等關係 `flexcache` 應用程式：

a. 如果 SVM 位於不同的叢集中、請為對等 SVM 建立 SVM 權限：

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

下列範例說明如何建立適用於所有本機SVM的SVM對等權限：

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. 建立 SVM 對等關係：

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. 建立FlexCache 一個流通量：

```
volume flexcache create -vserver <cache_svm> -volume
<cache_vol_name> -auto-provision-as flexgroup -size <vol_size>
-origin-vserver <origin_svm> -origin-volume <origin_vol_name> -is-s3
-enabled true|false
```

以下範例建立FlexCache 一個現象區、並自動選取現有的集合體進行資源配置：

```
cluster1::> volume flexcache create -vserver vs_1 -volume fc1 -auto
-provision-as flexgroup -origin-volume vol_1 -size 160MB -origin
-vserver vs_1
[Job 443] Job succeeded: Successful
```

下列範例建立FlexCache 一個聲音量、並設定交會路徑：

```
cluster1::> volume flexcache create -vserver vs34 -volume fc4 -aggr
-list aggr34,aggr43 -origin-volume origin1 -size 400m -junction-path
/fc4
[Job 903] Job succeeded: Successful
```

以下範例啟用對 FlexCache 磁碟區的 S3 存取：

```
cluster1::> volume flexcache create -vserver vs3 -volume
cache_vs3_vol33 -origin-volume vol33 -origin-vserver vs3 -junction
-path /cache_vs3_vol33 -is-s3-enabled true
```

4. 驗證FlexCache 從「聲音量」和「原始」磁碟區的「聲音」關係FlexCache 。
   a. 檢視叢集中的 FlexCache 關係：

```
volume flexcache show
```

```
cluster1::> volume flexcache show
Vserver Volume      Size       Origin-Vserver Origin-Volume
Origin-Cluster
------- ----------- ---------- -------------- -------------
--------------
vs_1    fc1         160MB      vs_1           vol_1
cluster1
```

   b. 檢視來源叢集中的所有 FlexCache 關係：

```
volume flexcache origin show-caches
```

```
cluster::> volume flexcache origin show-caches
Origin-Vserver Origin-Volume   Cache-Vserver    Cache-Volume
Cache-Cluster
-------------- --------------- ---------------  --------------
---------------
vs0            ovol1           vs1              cfg1
clusA
vs0            ovol1           vs2              cfg2
clusB
vs_1           vol_1           vs_1             fc1
cluster1
```

結果

成功建立了這個功能。FlexCache用戶端可以使用FlexCache 解決方案開發區的交會路徑來掛載磁碟區。

相關資訊

"叢集與SVM對等關係"

FlexCache 回寫

瞭解 ONTAP FlexCache 回寫功能

FlexCache 回寫是 ONTAP 9.15.1 推出的另一種寫入快取的作業模式。回寫功能可將寫入內容提交至快取的穩定儲存設備、並將其確認給用戶端、而無需等待資料傳送至原始伺服器。資料會以非同步方式重新排清回來源。因此、全球分散式檔案系統可讓寫入作業以接近本機的速度執行特定工作負載和環境、提供顯著的效能效益。

ONTAP 9.12.1 推出回寫功能作為公開預覽。這稱為回寫版本 1 （ wbv1 ）、不應視為 ONTAP 9.15.1 中的回寫版本 2 （ wbv2 ）。

回寫與回寫

自從 ONTAP 9.5 引進 FlexCache 以來、它一直是可讀寫的快取、但卻是以寫入模式運作。快取中的寫入資料會傳送至原始伺服器、以用於穩定儲存設備。原始伺服器成功將寫入內容提交至穩定儲存設備後、就會確認寫入快取。然後快取會確認寫入用戶端。如此一來、每次寫入都會被罰在快取和原始伺服器之間穿越網路。FlexCache 回寫會變更此項目。

升級至 ONTAP 9.15.1 之後、您可以將傳統的繞過寫入快取轉換為回寫快取、並在必要時回復為回寫式快取。不過、如果發生問題、讀取診斷記錄可能會更困難。

	繞過寫入	回寫
版本ONTAP	超過 9.6 個	9.15.1+
使用案例	讀取繁重的工作負載	大量寫入工作負載
資料提交時間	來源	快取
客戶體驗	類似 WAN	類似 LAN
限制	每個來源 100 個	每個來源 10 個
"CAP Theorem"	可用且可容錯分割區	可用且一致

FlexCache 回寫詞彙

瞭解使用 FlexCache 回寫功能的關鍵概念和詞彙。

期限	定義
*O變 髒的資料 *	已提交至快取穩定儲存區、但尚未排清至來源區的資料。
* 獨家鎖定委派（ XLD ） *	以每個檔案為基礎、授予快取的通訊協定層級鎖定權限。此權限可讓快取將專屬寫入鎖定交給用戶端、而無需聯絡來源。
* 共用鎖定委派（ SLD ） *	以每個檔案為基礎、授予快取的通訊協定層級鎖定權限。此權限可讓快取將共用讀取鎖定分發給用戶端、而無需聯絡原始伺服器。
* 回寫式 *	一種 FlexCache 作業模式、寫入快取的資料會被提交至該快取的穩定儲存設備、並立即確認給用戶端。資料會以非同步方式寫入來源。

期限	定義
* 繞過寫入 *	一種 FlexCache 作業模式、將寫入快取的資料轉送至原始伺服器、以提交至穩定的儲存設備。提交後、原始伺服器會確認寫入快取、快取會確認寫入用戶端。
* 不良資料記錄系統（ DDR ） *	一種專屬機制、可針對每個檔案、追蹤啟用回寫式快取中的髒資料。
* 來源 *	包含所有 FlexCache 快取磁碟區之來源資料的 FlexGroup 或 FlexVol 。它是唯一的事實來源、協調鎖定、並確保 100% 資料一致性、貨幣和一致性。
* 快取 *	FlexGroup 、 FlexCache 原始伺服器的稀疏快取磁碟區。

一致、最新且一致的

FlexCache 是 NetApp 的解決方案、可隨時隨地擁有正確的資料。FlexCache 100% 一致、即時且一致的 100% 時間：

- * 一致： * 無論資料在何處存取、資料都是相同的。
- * 目前： * 資料永遠保持在最新狀態。
- * 一致： * 資料正確 / 未毀損。

ONTAP FlexCache 回寫準則

FlexCache寫回涉及來源伺服器和快取伺服器之間的許多複雜互動。為了獲得最佳效能，您應該確保您的環境遵循以下準則。這些指南是基於內容創建時可用的最新主要ONTAP版本（ONTAP 9.17.1）。

最佳實務做法是在非正式作業環境中測試您的正式作業工作負載。如果您在這些準則之外實作 FlexCache 回寫，這就更重要了。

以下準則已在 NetApp 內部經過充分測試。建議您留在這些範圍內。否則可能會發生非預期的行為。

- ONTAP 9.17.1P1 引進了對FlexCache回寫功能的重大增強。強烈建議您在來源叢集和快取叢集上，在 9.17.1P1 版本之後運行目前建議版本。如果您無法執行 9.17.1 程式碼線，建議使用最新的 P 版本 9.16.1 。ONTAP 9.15.1 尚未包含FlexCache回寫所需的全部修復和改進，因此不建議用於生產工作負載。
- 在目前的迭代中， FlexCache 回寫式快取應設定為整個 FlexCache Volume 的單一組成要素。多成分 FlexCaches 可能會導致不必要的資料從快取區移出。
- 測試針對小於 100GB 的檔案進行，快取和來源之間的 WAN 往返時間不超過 200ms。超出這些限制的任何工作負載都可能導致意想不到的效能特性。
- 寫入 SMB 替代資料串流會導致主檔案被從快取中移出。主檔案的所有髒資料都必須先清除至來源，才能在該檔案上執行任何其他作業。替代資料串流也會轉送至來源。
- 重新命名檔案會使檔案從快取中移出。檔案的所有髒資料都必須先清除至來源，才能在該檔案上執行任何其他作業。
- 目前，唯一可在啟用回寫的 FlexCache 磁碟區上變更或設定的屬性為：
  - 時間戳記
  - 模式位元

- NT ACL
- 擁有者
- 群組
- 尺寸

  任何其他變更或設定的屬性都會轉寄至原始伺服器，這可能會導致檔案從快取中移除。如果您需要在快取中變更或設定其他屬性，請要求您的帳戶團隊開啟 PVR 。

- 在來源處拍攝的快照會叫出與來源磁碟區相關聯的每個啟用回寫快取中所有未處理的髒資料。如果有大量的回寫活動正在進行中，這可能需要多次重試作業，因為這些髒檔案的移轉可能需要一些時間。
- 啟用回寫功能的FlexCache磁碟區不支援 SMB 機會鎖（Oplocks）寫入。
- 原點必須保持在 80% 的滿量以下。如果原始磁碟區中沒有至少 20% 的剩餘空間，則不會授予快取磁碟區獨佔鎖定委派。在這種情況下，對啟用回寫式快取的通話會轉接至來源。這有助於防止來源空間不足，導致在啟用回寫的快取中留下髒資料孤立。
- 低頻寬和/或有損的群集間網路會對FlexCache寫回效能產生顯著的負面影響。雖然沒有特定的頻寬要求，因為它很大程度上取決於您的工作負載，但強烈建議您確保快取和來源之間的叢集間連結的健康狀況。

ONTAP FlexCache 回寫式架構

FlexCache 的設計具有強烈的一致性、包括兩種寫入作業模式：回寫和繞過寫入。ONTAP 9.15.1 採用的傳統寫入操作模式和新的回寫操作模式、都能保證存取的資料永遠保持 100% 一致、一致、最新且一致。

以下概念詳述 FlexCache 回寫作業的方式。

委派

鎖定委派和資料委派有助於 FlexCache 保持寫入和寫入快取資料的一致性、一致性和最新狀態。來源協調兩個委派。

鎖定委派

鎖定委派是一種通訊協定層級的鎖定權限、原始伺服器會根據每個檔案授予快取、以視需要向用戶端發出通訊協定鎖定。其中包括 獨家鎖定委派（ XLD ） 和 共用鎖定委派（ SLD ）。

XLD 和回寫

為了確保 ONTAP 永遠不需要協調衝突的寫入、會將 XLD 授予用戶端要求寫入檔案的快取。重要的是、任何檔案都只能有一個 XLD 、這表示每次只能有一個寫入檔案的寫入器。

當寫入檔案的要求進入啟用回寫的快取時、會執行下列步驟：

1. 快取會檢查它是否已有 XLD 用於要求的檔案。如果是這樣、只要另一個用戶端未寫入快取的檔案、它就會將寫入鎖定授予用戶端。如果快取沒有 XLD 可用於要求的檔案、它會向來源要求一個。這是一個專屬的呼叫、會穿越叢集間網路。
2. 從快取接收 XLD 要求時、原始伺服器會檢查另一個快取中的檔案是否有未處理的 XLD 。如果是這樣、它將會回收該檔案的 XLD 、這會觸發從該快取中的任何快取項目清除 不良資料 回原始伺服器。
3. 一旦從該快取中清除髒資料、並將其歸入原始伺服器的穩定儲存設備、原始伺服器就會將該檔案的 XLD 授予要求的快取。

4. 收到檔案的 XLD 後、快取會將鎖定授予用戶端、並開始寫入。

順序圖中會說明一些步驟的高階順序圖 [write-back-sequence-diagram] 。

從用戶端的角度來看、所有鎖定都會像寫入標準 FlexVol 或 FlexGroup 一樣運作、而且在要求寫入鎖定時可能會有小延遲。

在目前的迭代中、如果啟用回寫的快取保留檔案的 XLD 、 ONTAP 會在其他快取中封鎖 * 任何 * 對該檔案的存取、包括 `READ` 作業。

每個原點組成的 XLDs 上限為 170 個。

資料委派

資料委派是原始伺服器提供的每個檔案保證、該檔案的資料快取是最新的。只要快取具有檔案的資料委派、它就能將該檔案的快取資料提供給用戶端、而無需聯絡來源。如果快取沒有檔案的資料委派、則必須聯絡來源、以接收用戶端要求的資料。

在回寫模式中、如果在另一個快取或來源中為檔案取得 XLD 、則檔案的資料委派將會撤銷。如此可有效地從所有其他快取和原始伺服器的用戶端關閉檔案、即使是讀取也沒問題。這是一項交易、必須確保永遠不會存取舊資料。

在啟用回寫式快取中讀取通常會像在寫入快取中讀取一樣運作。在具有寫入和回寫功能的快取中、當要求的檔案在啟用回寫功能的快取上具有專屬寫入鎖定、而非發出讀取的快取時、可能會發生初始 `READ` 效能受限。必須撤銷 XLD 、而且必須先將髒資料提交至來源、才能在其他快取中進行讀取。

追蹤不良資料

從快取回寫至原始伺服器的作業會非同步進行。這表示不實的資料不會立即寫回來源。ONTAP 採用不乾淨的資料記錄系統來追蹤每個檔案的不乾淨資料。每個髒資料記錄（ DDR ）代表特定檔案的約 20MB 髒資料。當檔案正在主動寫入時、 ONTAP 會在填入兩個 DDP 並寫入第三個 DDR 之後、開始將髒資料重新排清。這會在寫入期間、在快取中留下大約 40MB 的髒資料。對於有狀態的通訊協定（ NFSv4.x 、 SMB ）、其餘 40MB 的資料會在檔案關閉時重新排清至來源。對於無狀態通訊協定（ NFSv3 ）、當要求在不同的快取中存取檔案、或在檔案閒置兩分鐘以上（最多五分鐘）後、 40MB 的資料將會重新排清。如需計時器觸發或空間觸發的不乾淨資料排清的詳細資訊，請參閱 快取 Scubers。

除了 DDP 和 Scubers 之外、某些前端 NAS 作業也會觸發檔案的所有髒資料清空：

- `SETATTR`
  - 「只修改 mtime 、 atime 和 / 或 ctime 的 ETATTR 可在快取中處理、避免 WAN 的罰則。
- `CLOSE`
- `OPEN` 在另一個快取中
- `READ` 在另一個快取中
- `READDIR` 在另一個快取中
- `READDIRPLUS` 在另一個快取中
- `WRITE` 在另一個快取中

中斷連線

當檔案的 XLD 存放在繞過寫入快取中、且快取從來源中斷連線時、其他快取和來源仍允許讀取該檔案。當 XLD 被啟用回寫式快取所保留時、此行為會有所不同。在這種情況下、如果快取中斷連線、對檔案的讀取將會隨處掛起。這有助於確保 100% 一致性、貨幣和一致性得以維持。寫入模式允許讀取、因為原始伺服器保證有所有已寫入確認給用戶端的可用資料。在中斷連線期間的回寫模式中、原始伺服器無法保證寫入啟用回寫式快取的所有資料、都會在中斷連線發生之前、將資料寫入原始伺服器。

如果檔案的 XLD 快取已長時間中斷連線、系統管理員可以手動撤銷來源的 XLD 。如此可讓 IO 傳至檔案、在存續的快取和原始伺服器上繼續執行。

手動撤銷 XLD 會導致檔案在中斷連線的快取中遺失任何髒資料。只有在快取和原始伺服器之間發生災難性中斷時、才應手動撤銷 XLD 。

快取 **Scubers**

ONTAP 中有 Scubers 會針對特定事件執行、例如計時器過期或空間臨界值遭到違反。清理程序會對正在清理的檔案進行專屬鎖定、有效地將 IO 凍結至該檔案、直到清理完成為止。

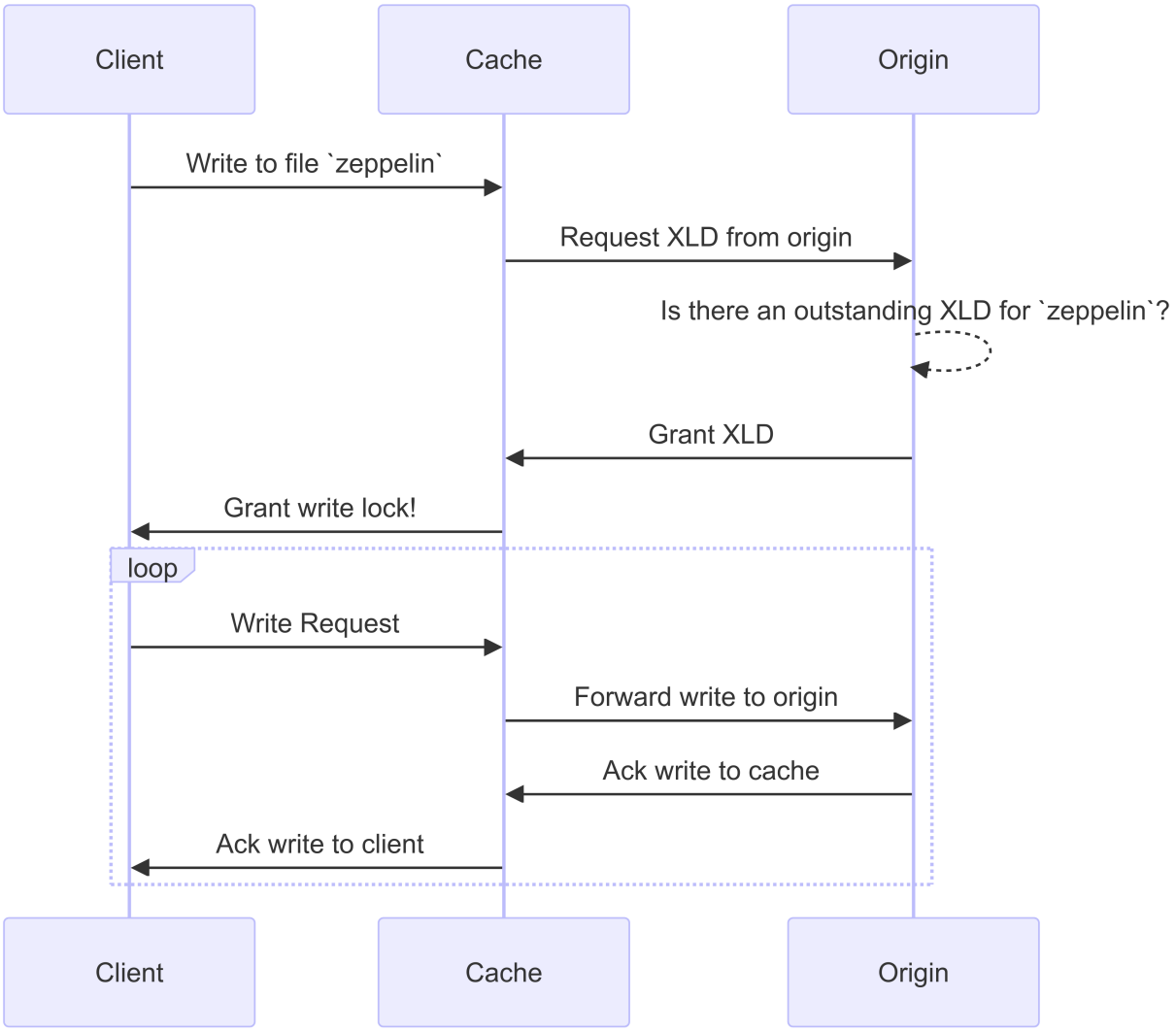
洗滌器包括：

- * 快取記憶體上的時間型 Scrub橡膠 ： * 這種 Scrubrub 每五分鐘啟動一次、並將任何未經修改的檔案擦去兩分鐘。如果檔案的任何髒資料仍在快取中、該檔案的 IO 將會靜止、並觸發回寫。IO 將在回寫完成後恢復。
- * 基於時間的來源 Sc橡膠 ： * 與快取中的 mtime 型 Sc橡膠 非常相似、這種情形也會每五分鐘執行一次。不過、它會將未經修改的任何檔案擦去 15 分鐘、並叫出 inode 的委派。此 Sc橡膠 不會啟動任何回寫。
- * 來源上的 rw 限制型 Scr橡膠 ： * ONTAP 會監控每個來源組成的 RW 鎖定委派數量。如果這個數字超過 170 、 ONTAP 就會開始以最少使用（ LRU ）為基礎來執行資料清理寫入鎖定委派。
- * 快取上的空間型 Scruber:* 如果 FlexCache 磁碟區達到 90% 滿、快取會被擦洗、以 LRU 為基礎。
- * 來源上的空間型 Scruber:* 如果 FlexCache 原始磁碟區滿 90% 、快取會被擦洗、以 LRU 為基礎。

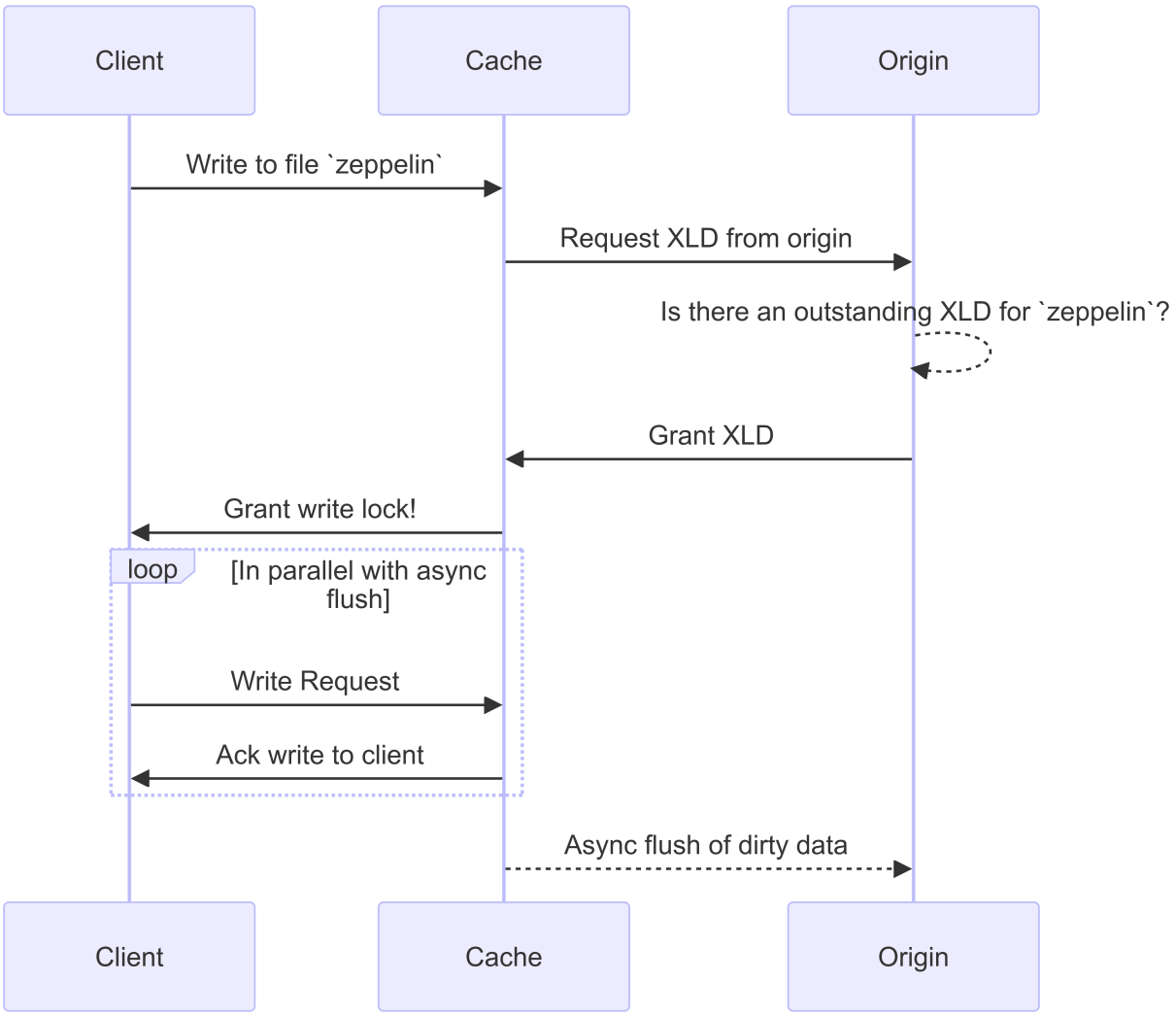
序列圖

這些順序圖描述了繞寫模式和回寫模式之間的寫入確認差異。

繞過寫入


Client
Cache
Origin
Write to file `zeppelin`
Request XLD from origin
Is there an outstanding XLD for `zeppelin`?
Grant XLD
Grant write lock!
loop
Write Request
Forward write to origin
Ack write to cache
Ack write to client
Client
Cache
Origin

回寫



ONTAP FlexCache 回寫式使用案例

這些寫入設定檔最適合啟用回寫的 FlexCache 。您應該測試工作負載、以瞭解回寫或繞過寫入是否能提供最佳效能。

回寫並不取代回寫功能。雖然回寫是針對大量寫入工作負載所設計、但回寫仍是許多工作負載的最佳選擇。

目標工作負載

檔案大小

檔案大小比與呼叫檔案之間所發出的寫入次數來得小 `OPEN CLOSE` 。小型檔案本來就有較少的 `WRITE` 通話、因此不太適合回寫。大型檔案在與通話之間可能有更多寫入 `OPEN CLOSE` 、但這並不保證。

請參閱"FlexCache 回寫準則"頁面，以取得最新的檔案大小建議。

寫入大小

從用戶端寫入時，除了寫入呼叫之外，還會涉及其他修改 NAS 呼叫。其中包括但不限於：

- CREATE
- OPEN
- CLOSE
- SETATTR
- SET_INFO

SETATTR`以及 `SET_INFO owner`在快取中處理的設定， `atime， ctime， group`或 `size`呼叫 `mtime。其餘的通話必須在原始伺服器處理，並觸發寫入已啟用回寫快取的任何髒資料的回寫。檔案的 IO 將會停止、直到回寫完成為止。

知道這些通話必須經過 WAN 、有助於識別適合回寫的工作負載。一般而言、在 OPEN `CLOSE`不發出上述其中一個通話的情況下、在與通話之間所能完成的寫入次數越多、效能回寫所提供的效能就越高。

寫入後讀取

寫入後讀取工作負載在 FlexCache 的執行效能一向不佳。這是由於 9.15.1 之前的繞過寫入操作模式所致。WRITE`對檔案的呼叫必須在原始伺服器上進行、後續的 `READ 通話則必須將資料拉回快取。這會導致這兩種作業都會受到 WAN 的影響。因此、 FlexCache 在寫入模式中不建議使用寫入後讀取工作負載。在 9.15.1 中引入回寫功能後、資料現在會在快取中提交、並可立即從快取中讀取、免除 WAN 的麻煩。如果您的工作負載在 FlexCache 磁碟區中包含讀取後寫入、則應將快取設定為以回寫模式運作。

如果寫入後讀取是工作負載的關鍵部分、您應該將快取設定為以回寫模式運作。

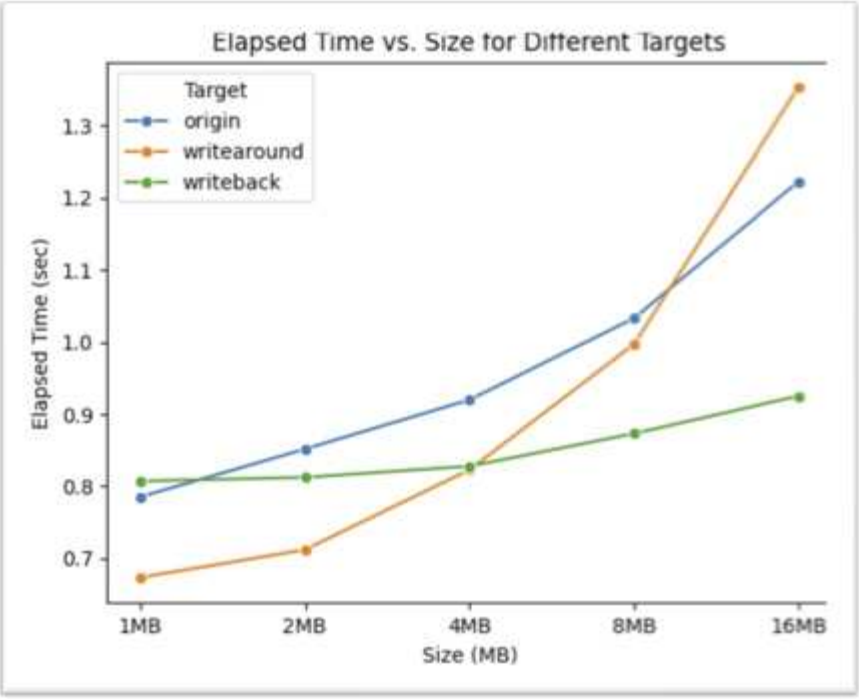
寫入後寫入

當檔案在快取中累積髒資料時、快取會以非同步方式將資料重新寫入來源。這自然會導致用戶端關閉檔案、但仍有髒資料等待重新排清來源。如果剛關閉且仍有髒資料的檔案有其他開啟或寫入資料、寫入作業將會暫停、直到所有髒資料都已排清至來源。

延遲考量

當 FlexCache 以回寫模式運作時、延遲增加對 NAS 用戶端更有幫助。不過、回寫的成本、有一點比低延遲環境中所獲得的優勢還要高。在某些 NetApp 測試中，回寫效益是從快取與原始伺服器之間的最低延遲開始，時間為 8 毫秒。這種延遲會因工作負載而異，因此請務必測試以瞭解工作負載的報酬點。

下圖顯示 NetApp 實驗室測試中回寫的退回點。 x`軸為檔案大小、 `y 軸為經過時間。此測試使用 NFSv3 、以 256 KB 和 64 毫秒的 WAN 延遲進行掛載 rsize wsize 。此測試是使用小型 ONTAP Select 執行個體來執行快取和原始伺服器、以及單一執行緒寫入作業。您的結果可能有所不同。



回寫不應用於叢集快取。當原始伺服器和快取位於同一個叢集中時、就會發生叢集內快取。

ONTAP FlexCache 回寫必要條件

在回寫模式下部署 FlexCache 之前，請先確定您已符合這些效能，軟體，授權和系統組態需求。

CPU與記憶體

強烈建議每個原始叢集節點至少具有 128GB 的 RAM 和 20 個 CPU 來吸收啟用回寫功能的快取發起的回寫訊息。這相當於 A400 或更高版本。如果原始叢集是多個啟用回寫的 FlexCaches 的來源，則需要更多 CPU 和 RAM 。

針對工作負載使用較小的原始伺服器，可能會對啟用回寫式快取或原始伺服器的效能造成深遠影響。

版本**ONTAP**

- 原始伺服器 *_m必 _ * 執行 ONTAP 9.15.1 或更新版本。
- 任何需要以回寫模式操作的快取叢集 * 必須 _ * 執行 ONTAP 9.15.1 或更新版本。
- 任何不需要以回寫模式操作的快取叢集，都可以執行任何一般支援的 ONTAP 版本。

授權

FlexCache （包括回寫操作模式）隨附於您購買的 ONTAP 產品中。不需要額外授權。

對等關係

- 來源叢集和快取叢集必須是 "叢集已對等執行"

- 原始伺服器和快取叢集上的伺服器虛擬機器（ SVM ）必須 "vserver 已被人使用" 具有 FlexCache 選項。

您不需要將快取叢集與另一個快取叢集對等。也不需要將快取 SVM 與另一個快取 SVM 對等。

ONTAP FlexCache 回寫互通性

在回寫模式下部署 FlexCache 時、請瞭解這些互通性考量事項。

版本**ONTAP**

若要使用回寫式作業模式、快取和原始伺服器 * 必須 * 執行 ONTAP 9.15.1 或更新版本。

不需要啟用回寫式快取的叢集可以執行舊版 ONTAP 、但該叢集只能以繞寫模式運作。

您可以在環境中混合使用 ONTAP 版本。

叢集	版本**ONTAP**	是否支援回寫？
* 來源 *	ONTAP 9.15.1.1	不適用†
* 叢集 1*	ONTAP 9.15.1.1	是的
* 叢集 2 *	ONTAP 9.14.1.	否

叢集	版本**ONTAP**	是否支援回寫？
* 來源 *	ONTAP 9.14.1.	不適用†
* 叢集 1*	ONTAP 9.15.1.1	否
* 叢集 2 *	ONTAP 9.15.1.1	否

† _ 來源不是快取、因此不適用回寫或繞過寫入支援。 _

在 [example2-table]中、兩個叢集都無法啟用回寫模式、因為原始伺服器並未執行 ONTAP 9.15.1 或更新版本、這是一項嚴格的要求。

用戶端互通性

ONTAP 通常支援的任何用戶端都可以存取 FlexCache Volume 、無論它是以寫入或回寫模式運作。有關受支持客戶端的最新列表，請參閱 NetApp 的 "互通性對照表"。

雖然用戶端版本並不重要、但用戶端必須是新的、足以支援 NFSv3 、 NFSv4.0 、 NFSv4.1 、 SMB2.x 或 SMB3.xSMB1 和 NFSv2 是過時的通訊協定、不受支援。

寫回和寫回

如所示 [example1-table]、以回寫模式操作的 FlexCache 可以與以繞寫模式操作的快取共存。我們建議您將繞過寫入與回寫與您的特定工作負載進行比較。

如果工作負載在回寫和回寫之間的效能相同、請使用繞寫功能。

ONTAP 功能互通性

如需 FlexCache 功能互通性的最新清單、請參閱 "FlexCache Volume 支援和不支援的功能"。

啟用及管理 ONTAP FlexCache 回寫

從 ONTAP 9.15.1 開始、您可以在 FlexCache 磁碟區上啟用 FlexCache 回寫模式、為邊緣運算環境和具有大量寫入工作負載的快取提供更好的效能。您也可以決定是否在 FlexCache 磁碟區上啟用回寫功能、或在必要時停用磁碟區上的回寫功能。

在快取磁碟區上啟用回寫時、寫入要求會傳送至本機快取、而非原始磁碟區。

開始之前

您必須處於進階權限模式。

建立啟用回寫功能的新 FlexCache Volume

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 、在啟用回寫功能的情況下建立新的 FlexCache Volume 。

系統管理員

1. 如果 FlexCache 磁碟區與原始磁碟區位於不同的叢集、請建立叢集對等關係：
   a. 在本機叢集上、按一下 * 保護 > 概述 * 。
   b. 展開 * 叢集間設定 * 、按一下 * 新增網路介面 * 、然後將叢集間介面新增至叢集。

      在遠端叢集上重複此步驟。

   c. 在遠端叢集上、按一下 * 保護 > 概述 * 。按一下 ⋮ 「叢集對等點」區段、然後按一下「 * 產生複雜密碼 * 」。
   d. 複製產生的通關密碼、然後貼到本機叢集中。
   e. 在本機叢集上、按一下叢集對等項下的 * 對等叢集 * 、然後對本機叢集和遠端叢集進行對等處理。
2. 如果 FlexCache 磁碟區與原始磁碟區位於不同的叢集、請建立 SVM 對等關係：

   在 * 儲存 VM Peers * 下、按一下、然後按一下 ⋮ * Peer Storage VMS* 來對等儲存 VM 。

   如果 FlexCache 磁碟區位於同一個叢集、則無法使用系統管理員建立 SVM 對等關係。

3. 選擇*儲存>磁碟區*。
4. 選取*「Add*」。
5. 選取 * 更多選項 * 、然後選取 * 新增為遠端磁碟區的快取 * 。
6. 選取 * 啟用 FlexCache 回寫 * 。

CLI

1. 如果FlexCache 要建立的實體磁碟區位於不同的叢集、請建立叢集對等關係：
   a. 在目的地叢集上、與資料保護來源叢集建立對等關係：

      ```
      cluster peer create -generate-passphrase -offer-expiration
      MM/DD/YYYY HH:MM:SS|1...7days|1...168hours -peer-addrs
      <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name>,..|*
      -ipspace <ipspace_name>
      ```

      從ONTAP 功能支援的9.6開始、建立叢集對等關係時、預設會啟用TLS加密。支援TLS加密、以便在來源FlexCache 與實體磁碟區之間進行叢集間通訊。您也可以視需要停用叢集對等關係的TLS加密。

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
              Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: *
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

a. 在來源叢集上、驗證來源叢集到目的地叢集的驗證：

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship,
use a phrase or sequence of characters that would be hard to
guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

2. 如果 FlexCache 磁碟區與原始磁碟區位於不同的 SVM 、請與建立 SVM 對等關係 `flexcache` 應用程式：

a. 如果 SVM 位於不同的叢集中、請為對等 SVM 建立 SVM 權限：

```
vserver peer permission create -peer-cluster <cluster_name>
-vserver <svm-name> -applications flexcache
```

下列範例說明如何建立適用於所有本機SVM的SVM對等權限：

```
cluster1::> vserver peer permission create -peer-cluster cluster2
-vserver "*" -applications flexcache

Warning: This Vserver peer permission applies to all local Vservers.
After that no explict
"vserver peer accept" command required for Vserver peer relationship
creation request
from peer cluster "cluster2" with any of the local Vservers. Do you
want to continue? {y|n}: y
```

a. 建立 SVM 對等關係：

```
vserver peer create -vserver <local_SVM> -peer-vserver
<remote_SVM> -peer-cluster <cluster_name> -applications flexcache
```

3. 建立啟用回寫功能的 FlexCache Volume ：

```
volume flexcache create -vserver <cache_vserver_name> -volume
<cache_flexgroup_name> -aggr-list <list_of_aggregates> -origin
-volume <origin flexgroup> -origin-vserver <origin_vserver name>
-junction-path <junction_path> -is-writeback-enabled true
```

在現有的 **FlexCache** 磁碟區上啟用 **FlexCache** 回寫

您可以使用 ONTAP 系統管理員或 ONTAP CLI 、在現有的 FlexCache 磁碟區上啟用 FlexCache 回寫功能。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取現有的 FlexCache 磁碟區。
2. 在磁碟區的「總覽」頁面上、按一下右上角的 * 編輯 * 。
3. 在 * 編輯 Volume * 視窗中、選取 * 啟用 FlexCache 回寫 * 。

CLI

1. 在現有的 FlexCache 磁碟區上啟用回寫：

```
volume flexcache config modify -volume <cache_flexgroup_name> -is
-writeback-enabled true
```

檢查 **FlexCache** 回寫功能是否已啟用

步驟

您可以使用系統管理員或 ONTAP CLI 來判斷 FlexCache 回寫功能是否已啟用。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取一個磁碟區。
2. 在卷 * Overview （概述） * 中，找到 FlexCache details* ，然後檢查 FlexCache 捲上的 FlexCache 回寫是否設置爲 **Enabled** （已啓用 * ）。

CLI

1. 檢查是否啟用 FlexCache 回寫：

```
volume flexcache config show -volume <cache_flexgroup_name> -fields
is-writeback-enabled
```

停用 **FlexCache** 磁碟區的回寫功能

在刪除 FlexCache 磁碟區之前、您需要停用 FlexCache 回寫功能。

步驟

您可以使用系統管理員或 ONTAP CLI 來停用 FlexCache 回寫功能。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取已啟用 FlexCache 回寫功能的現有 FlexCache 磁碟區。
2. 在磁碟區的「總覽」頁面上、按一下右上角的 * 編輯 * 。
3. 在 * 編輯 Volume * 視窗中、取消選取 * 啟用 FlexCache 回寫 * 。

CLI

1. 停用回寫：

```
volume flexcache config modify -volume <cache_vol_name> -is
-writeback-enabled false
```

關於 **ONTAP FlexCache** 回寫的常見問題集

如果您正在尋找問題的快速解答，這個常見問題集將有助於您解決問題。

我想使用回寫功能。我需要執行哪個版本的 **ONTAP** ？

快取和原始伺服器都必須執行 ONTAP 9.15.1 或更新版本。建議您執行最新的 P 版本。工程設計持續改善啟用回寫式快取的效能與功能。

存取原始伺服器的用戶端是否會影響存取啟用回寫式快取的用戶端？

是的。原始伺服器對資料擁有與任何快取相同的權限。如果在需要將檔案從快取中移出的檔案上執行作業，或是要撤銷鎖定 / 資料委派，快取中的用戶端可能會看到存取檔案的延遲。

我是否可以將 **QoS** 套用至啟用回寫功能的 **FlexCaches** ？

是的。每個快取和來源都可以套用個別的 QoS 原則。這對任何回寫啟動的叢集間流量沒有直接影響。間接來說，您可以透過 QoS 限制啟用回寫式快取的前端流量，來減緩叢集間回寫式流量。

啟用回寫式 **FlexCaches** 是否支援多重傳輸協定 **NAS** ？

是的。啟用回寫式 FlexCaches 可完整支援多重傳輸協定。目前，以寫入或回寫模式操作的 FlexCache 不支援 NFSv4.2 和 S3 。

啟用回寫式 **FlexCaches** 是否支援 **SMB** 替代資料串流？

支援 SMB 替代資料串流（ ADS ），但不會透過回寫來加速。寫給廣告的內容會轉寄給來源，導致 WAN 延遲的損失。寫入也會從快取中移出廣告所在的主檔案。

建立快取後，是否可以在寫入模式和回寫模式之間切換快取？

是的。您只需要切換連結中的旗標即可 `is-writeback-enabled`： ../../e-writeback FlexCache / FlexCache-writeback-enable-task.html[`flexcache modify` 命令] 。

對於快取和來源伺服器之間的叢集間鏈路，我應該注意哪些頻寬方面的因素？

是的。FlexCache 的寫回功能高度依賴快取和來源之間的叢集間連結。低頻寬和/或丟包網路會對效能產生顯著的負面影響。沒有特定的頻寬要求，因為它很大程度上取決於您的工作負載。

FlexCache 二元性

關於 **FlexCache** 二元性的常見問題

本常見問題解答了有關 ONTAP 9.18.1 中引入的 FlexCache 對偶性的常見問題。

常見問題

什麼是「二元性」？

雙功能允許使用檔案（NAS）和物件（S3）協定統一存取相同資料。ONTAP 9.12.1 引入了雙功能，但當時並未提供 FlexCache 支援，ONTAP 9.18.1 擴展了雙功能，使其支援 FlexCache 磁碟區，從而允許使用 S3 協定存取快取在 FlexCache 磁碟區中的 NAS 檔案。

FlexCache S3 儲存貯體支援哪些 **S3** 作業？

標準 S3 NAS 儲存區支援的 S3 作業在 FlexCache S3 NAS 儲存區上也受到支援，但 `COPY` 作業除外。如需標準 S3 NAS 儲存區不支援的作業的最新清單，請造訪 "互通性文件"。

我可以在寫回模式下使用 **FlexCache** 與 **FlexCache** 雙重性嗎？

不。如果在 FlexCache 磁碟區上建立 FlexCache S3 NAS 儲存桶，則該 FlexCache 磁碟區*必須*處於寫入繞過模式。如果嘗試在寫回模式的 FlexCache 磁碟區上建立 FlexCache S3 NAS 儲存桶，則操作將會失敗。

由於硬體限制，我無法將其中一個叢集升級到 **ONTAP 9.18.1**。如果只有快取叢集執行 **ONTAP 9.18.1**，**duality** 在我的叢集中還能正常運作嗎？

不。快取叢集和來源叢集的有效叢集版本都必須至少為 9.18.1。如果您嘗試在與執行 ONTAP 版本低於 9.18.1 的來源叢集建立對等連線的快取叢集上建立 FlexCache S3 NAS 儲存桶，則操作將會失敗。

我有一個 **MetroCluster** 配置。我可以使用 **FlexCache** 雙重性嗎？

否。FlexCache 二元性在 MetroCluster 組態中不受支援。

我可以審核對 **FlexCache S3 NAS** 儲存桶中檔案的 **S3** 存取嗎？

S3 審計功能由 NAS 審計功能提供，FlexCache 磁碟區使用此功能。有關 NAS 審計 FlexCache 磁碟區的更多資訊，請參閱"深入瞭解 FlexCache 稽核"。

如果快取叢集與來源叢集中斷連線，我應該預期會發生什麼情況？

如果快取叢集與來源叢集斷開連接，則向 FlexCache S3 NAS 儲存桶發出的 S3 請求將失敗並出現 `503 Service Unavailable`錯誤。

我能否使用具有 **FlexCache** 雙重性的多部分 **S3** 操作？

若要讓多部分 S3 操作正常運作，底層 FlexCache 磁碟區的粒度資料欄位必須設定為「進階」。此欄位的值與來源磁碟區的值相同。

FlexCache duality 是否支援 **HTTP** 和 **HTTPS** 存取？

是的。預設情況下，必須使用 HTTPS。如有需要，您可以設定 S3 服務以允許 HTTP 存取。

啟用對 **NAS FlexCache** 磁碟區的 **S3** 存取

從 ONTAP 9.18.1 開始，您可以啟用對 NAS FlexCache 磁碟區的 S3 存取，也稱為「雙重性」。這允許用戶端使用 S3 傳輸協定存取儲存在 FlexCache 磁碟區中的資料，以及 NFS 和 SMB 等傳統 NAS 傳輸協定。您可以使用以下資訊來設定 FlexCache 雙重性。

先決條件

在開始之前、您必須確保完成下列先決條件：

- 確保 S3 協議和所需的 NAS 協議（NFS、SMB 或兩者）已獲得授權並在 SVM 上進行設定。
- 請確認 DNS 及其他所需服務均已配置。
- 叢集和 SVM 對等
- FlexCache Volume 建立
- 已建立資料 LIF

> 有關 FlexCache 雙重性的更詳細文件，請參閱 "ONTAP S3 多重傳輸協定支援"。

步驟 **1**：建立並簽署憑證

若要啟用對 FlexCache 磁碟區的 S3 存取，您需要為託管 FlexCache 磁碟區的 SVM 安裝憑證。本範例使用自我簽署憑證，但在正式作業環境中，您應該使用由受信任的憑證授權單位（CA）簽署的憑證。

1. 建立 SVM 根 CA：

```
security certificate create -vserver <svm> -type root-ca -common-name
<arbitrary_name>
```

2. 產生憑證簽署要求：

```
security certificate generate-csr -common-name <dns_name_of_data_lif>
-dns-name <dns_name_of_data_lif> -ipaddr <data_lif_ip>
```

範例輸出：

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

私密金鑰範例：

```
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

請保留憑證申請和私密金鑰的副本，以供日後參考。

3. 簽署憑證：

`root-ca`是您在<<anchor1-step,建立 SVM 根 CA>>中建立的。

```
certificate sign -ca <svm_root_ca> -ca-serial <svm_root_ca_sn> -expire
-days 364 -format PEM -vserver <svm>
```

4. 貼上在產生憑證簽署要求中產生的憑證簽署請求 (CSR)。

範例：

```
-----BEGIN CERTIFICATE REQUEST-----
MIICzjCCAbYCAQAwHzEdMBsGA1UEAxMUY2FjaGUxZy1kYXRhLm5hcy5sYWIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCusJk075O8Uh329cHI6x+BaRS2
w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK1CI2VEkrXGUg
...
vMIGN351+FgzLQ4X5lKfoMXCV70NqIakxzEmkTIUDKv7n9EVZ4b5DTTlrL03X/nK
+Bim2y2y180PaFB3NauZHTnIIzIc8zCp2IEqmFWyMDcdBjP9KS0+jNm4QhuXiM8F
D7gm3g/O70qa5OxbAEal5o4NbOl95U0T0rwqTaSzFG0XQnK2PmA1OIwS5ET35p3Z
dLU=
-----END CERTIFICATE REQUEST-----
```

這會將已簽署的憑證列印到主控台，類似於以下範例。

已簽署憑證範例：

```
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

5. 複製憑證以供下一步使用。
6. 在 SVM 上安裝伺服器憑證：

```
certificate install -type server -vserver <svm> -cert-name flexcache-
duality
```

7. 從 簽署憑證 貼上已簽署的憑證。

範例：

```
Please enter Certificate: Press <Enter> [twice] when done
-----BEGIN CERTIFICATE-----
MIIDdzCCAl+gAwIBAgIIGHolbgv5DPowDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjIxNTU4WhcNMjYxMTIwMjIxNTU4WjAfMR0wGwYDVQQDExRjYWNoZTFnLWRhdGEu
bmFzLmxhYjCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK6wmTTvk7xS
...
qS7zhj3ikWE3Gp9s+QijKWXx/0HDd1UuGqy0QZNqNm/M0mqVnokJNk5F4fBFxMiR
1o63BxL8xGIRdtTCjjb2Gq2Wj7EClUw6CykEkxAcVk+XrRtArGkNtcYdtHfUsKVE
wswvv0rNydrNnWhJLhSl8TW5Tex+OMyTXgk9/3K8kB0mAMrtxxYjt8tm+gztkivf
J0eo1uDJhaNxqwEZRzFyGaa4k1+56oFzRfTc
-----END CERTIFICATE-----
```

8. 貼上在 產生憑證簽署要求 中產生的私鑰。

   範例：

```
Please enter Private Key: Press <Enter> [twice] when done
-----BEGIN PRIVATE KEY-----
MIIEvAIBADANBgkqhkiG9w0BAQEFAASCBKYwggSiAgEAAoIBAQCusJk075O8Uh32
9cHI6x+BaRS2w5wrqvzoYlidXtYmdCH3m1DDprBiAyfIwBC0/iU3Xd5NpB7nc1wK
1CI2VEkrXGUgwBtx1K4IlrCTB829Q1aLGAQXVyWnzhQc4tS5PW/DsQ8t7olZ9zEI
W/gaEIajgpXIwGNWZ+weKQK+yoolxC+gy4IUE7WvnEUiezaIdoqzyPhYq5GC4XWf
0johpQugOPe0/w2nVFRWJoFQp3ZP3NZAXc8H0qkRB6SjaM243XV2jnuEzX2joXvT
wHHH+IBAQ2JDs7s1TY0I20e49J2Fx2+HvUxDx4BHao7CCHA1+MnmEl+9E38wTaEk
NLsU724ZAgMBAAECggEABHUy06wxcIk5hO3S9Ik1FDZV3JWzsu5gGdLSQOHRd5W+
...
rXGEdDaqp7jQGNXUGlbxO3zcBil1/A9Hc6oalNECgYBKwe3PeZamiwhIHLy9ph7w
dJfFCshsPalMuAp2OuKIAnNa9l6fT9y5kf9tIbskT+t5Dth8bmV9pwe8UZaK5eC4
Svxm19jHT5QqloDaZVUmMXFKyKoqPDdfvcDk2Eb5gMfIIb0a3TPC/jqqpDn9BzuH
TO02fuRvRR/G/HUz2yRd+A==
-----END PRIVATE KEY-----
```

9. 輸入構成伺服器憑證憑證鏈的憑證授權單位（CA）的憑證。

   這從伺服器憑證的發行 CA 憑證開始，最多可到根 CA 憑證。

```
Do you want to continue entering root and/or intermediate certificates
{y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.

The installed certificate's CA and serial number for reference:
CA: cache-164g-svm-root-ca
serial: 187A256E0BF90CFA
```

10. 取得 SVM 根 CA 的公開金鑰：

```
security certificate show -vserver <svm> -common-name <root_ca_cn> -ca
<root_ca_cn> -type root-ca -instance

-----BEGIN CERTIFICATE-----
MIIDgTCCAmmgAwIBAgIIGHokTnbsHKEwDQYJKoZIhvcNAQELBQAwLjEfMB0GA1UE
AxMWY2FjaGUtMTY0Zy1zdm0tcm9vdC1jYTELMAkGA1UEBhMCVVMwHhcNMjUxMTIx
MjE1NTIzWhcNMjYxMTIxMjE1NTIzWjAuMR8wHQYDVQQDExZjYWNoZS0xNjRnLXN2
bS1yb290LWNhMQswCQYDVQQGEwJVUzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
...
DoOL7vZFFt44xd+rp0DwafhSnLH5HNhdIAfa2JvZW+eJ7rgevH9wmOzyc1vaihl3
Ewtb6cz1a/mtESSYRNBmGkIGM/SFCy5v1ROZXCzF96XPbYQN4cW0AYI3AHYBZP0A
HlNzDR8iml4k9IuKf6BHLFA+VwLTJJZKrdf5Jvjgh0trGAbQGI/Hp2Bjuiopkui+
n4aa5Rz0JFQopqQddAYnMuvcq10CyNn7S0vF/XLd3fJaprH8kQ==
-----END CERTIFICATE-----
```

這是設定客戶端信任由 SVM root-ca 簽署的憑證所必需的。公開金鑰會列印到主控台。複製並儲存公開金鑰。此命令中的值與您在 建立 SVM 根 CA 中輸入的值相同。

步驟 2：設定 S3 伺服器

1. 啟用 S3 協定存取：

```
vserver show -vserver <svm> -fields allowed-protocols
```

預設情況下，在 SVM 層級允許 S3。

2. 複製現有原則：

```
network interface service-policy clone -vserver <svm> -policy default-
data-files -target-vserver <svm> -target-policy <any_name>
```

3. 將 S3 加入複製的原則：

```
network interface service-policy add-service -vserver <svm> -policy
<any_name> -service data-s3-server
```

4. 將新原則新增至資料 LIF ：

```
network interface modify -vserver <svm> -lif <data_lif> -service-policy
duality
```

> 修改現有 LIF 的服務原則可能會造成中斷。這需要先關閉 LIF，然後再重新啟動，並啟用新服務的接聽程式。TCP 應該 很快就能從這種中斷中恢復，但請注意潛在的影響。

5. 在 SVM 上建立 S3 物件儲存伺服器：

```
vserver object-store-server create -vserver <svm> -object-store-server
<dns_name_of_data_lif> -certificate-name flexcache-duality
```

6. 在 FlexCache 磁碟區上啟用 S3 功能：

必須先將 `flexcache config`選項 `-is-s3-enabled`設定為 `true`，才能建立儲存桶。您還必須將選項 `-is-writeback-enabled`設定為 `false`。

以下命令可修改現有的 FlexCache：

```
flexcache config modify -vserver <svm> -volume <fcache_vol> -is
-writeback-enabled false -is-s3-enabled true
```

7. 建立 S3 儲存桶：

```
vserver object-store-server bucket create -vserver <svm> -bucket
<bucket_name> -type nas -nas-path <flexcache_junction_path>
```

8. 建立儲存區原則：

```
vserver object-store-server bucket policy add-statement -vserver <svm>
-bucket <bucket_name> -effect allow
```

9. 建立 S3 使用者：

```
vserver object-store-server user create -user <user> -comment ""
```

範例輸出：

```
    Vserver: <svm>>
       User: <user>>
 Access Key: WCOT7...Y7D6U
 Secret Key: 6143s...pd__P
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

10. 為 root 使用者重新產生金鑰：

```
vserver object-store-server user regenerate-keys -vserver <svm> -user
root
```

範例輸出：

```
    Vserver: <svm>>
       User: root
 Access Key: US791...2F1RB
 Secret Key: tgYmn...8_3o2
    Warning: The secret key won't be displayed again. Save this key for
future use.
```

步驟 **3**：設定用戶端

有許多 S3 用戶端可供使用。AWS CLI 是一個不錯的入門選擇。如需更多資訊、請參閱 "安裝 AWS CLI"。

管理 FlexCache Volume

瞭解如何稽核 ONTAP FlexCache Volume

從ONTAP 使用Sf9.7開始、您可以使用FlexCache 原生ONTAP 的功能、以FPolicy稽核及檔案原則管理、來稽核彼此之間關係中的NFS檔案存取事件。

從 ONTAP 9.14.1 開始、具有 NFS 或 SMB 的 FlexCache Volume 支援 FPolicy 。以前、 FlexCache Volume 不支援使用 SMB 的 FPolicy 。

原生稽核與FPolicy的設定與管理方式與FlexVol 使用相同的CLI命令進行、這些命令可用於解決各種問題。不過FlexCache 、使用現象不一樣。

- 原生稽核
  - 您無法使用FlexCache 一個不完整的Volume做為稽核記錄的目的地。
  - 如果您想要稽核FlexCache 在Sforsvolume上的讀取和寫入、則必須在快取SVM和來源SVM上設定稽核。

    這是因為檔案系統作業會在處理時進行稽核。也就是在快取SVM上稽核讀取、然後在來源SVM上稽核寫入。

  - 若要追蹤寫入作業的來源、稽核記錄中會附加SVM UUID和MSID、以識別FlexCache 產生寫入的來源來源於哪個SVM Volume。
- * FPolicy*
  - 雖然寫入FlexCache 到某個卷的作業是在來源捲上進行、但是FPolicy組態會監控快取磁碟區上的寫入作業。這與原生稽核不同、原生稽核會在原始磁碟區上稽核寫入內容。
  - 雖然在快取和來源SVM上不需要相同的FPolicy組態、但建議您部署兩個類似的組態。ONTAP您可以為快取建立新的FPolicy原則、設定方式與來源SVM相同、但新原則的範圍僅限於快取SVM。
  - FPolicy 組態中的副檔名大小限制為 20KB （ 20480 位元組）。當 FlexCache 磁碟區上 FPolicy 組態中使用的擴充功能大小超過 20KB 時，就會觸發 EMS 訊息 `nblade.fpolicy.extn.failed`。

從原始磁碟區同步 **ONTAP FlexCache** 磁碟區的內容

部分的聲音量屬性FlexCache 必須與原始Volume的部分內容同步。如果FlexCache 在原點Volume修改屬性後、無法自動同步化某個sorize Volume的Volume內容、您可以手動同步這些內容。

關於這項工作

下列的聲音量屬性FlexCache 必須一律與來源Volume的內容同步：

- 安全風格 (`-security-style`)
- Volume名稱 (`-volume-name`)
- 目錄大小上限 (`-maxdir-size`)
- 預先讀取的最小值 (`-min-readahead`)

步驟

1. 從這個功能區、同步Volume內容：FlexCache

   `volume flexcache sync-properties -vserver svm_name -volume flexcache_volume`

   ```
   cluster1::> volume flexcache sync-properties -vserver vs1 -volume fc1
   ```

更新 ONTAP FlexCache 關聯的組態

在發生磁碟區移動、集合體重新配置或儲存容錯移轉等事件之後、會FlexCache 自動更新來源磁碟區和流通磁碟區上的磁碟區組態資訊。如果自動更新失敗、系統會產生一則EMS訊息、然後您必須手動更新組態、以利FlexCache 實現此關係。

如果來源Volume和FlexCache 聲音不相連模式、您可能需要執行一些額外的作業FlexCache 、以手動更新一個不相連的關係。

關於這項工作

如果您想要更新FlexCache 某個版本的組態、必須從原始磁碟區執行命令。如果您想要更新來源Volume的組態、必須從FlexCache 這個版本執行命令。

步驟

1. 更新FlexCache 關於這個問題的組態：

```
volume flexcache config-refresh -peer-vserver peer_svm -peer-volume
peer_volume_to_update -peer-endpoint-type [origin | cache]
```

在 ONTAP FlexCache 磁碟區上啟用檔案存取時間更新

從 ONTAP 9.11.1 開始、您可以啟用 `-atime-update` FlexCache 捲上的欄位、以允許檔案存取時間更新。您也可以使用設定存取時間更新期間 `-atime-update-period` 屬性。。 `-atime-update-period` 屬性可控制存取時間更新的發生頻率、以及更新可傳播到原始磁碟區的時間。

總覽

ONTAP 提供一個稱為的 Volume 層級欄位 `-atime-update`，用於管理使用讀取、 readlink 和 READDIR 讀取的檔案和目錄的存取時間更新。atime用於不常存取的檔案和目錄的資料生命週期決策。不常存取的檔案最終會移轉至歸檔儲存設備、之後通常會移至磁帶。

在現有和新建立FlexCache 的版本中、預設會停用atim-update欄位。如果您在早於 9.11.1 版的 ONTAP 上使用 FlexCache Volume ，則應將 atime-update 欄位保持停用，以便在原始磁碟區上執行讀取作業時，不會不必要地清除快取。然而、有了大量FlexCache 的支援資料的快取、系統管理員可以使用特殊工具來管理資料、並確保熱資料保留在快取中、並清除冷資料。停用atime-update時無法執行此動作。不過，從 ONTAP 9.11.1 開始，您可以啟用 `-atime-update`及 `-atime-update-period,`使用管理快取資料所需的工具。

開始之前

- 所有FlexCache 的不完整資料區都必須執行ONTAP 更新版本的更新版本。
- 您必須使用 `advanced`權限模式。

關於這項工作

設定 `-atime-update-period` 至 86400 秒、無論檔案上執行的類似讀取作業次數為何、每 24 小時期間都不允許進行一次以上的存取時間更新。

設定 `-atime-update-period` 至 0 會傳送訊息給每個讀取存取的來源。然後、來源會通知每FlexCache 個VMware Volume、該atime已經過時、影響效能。

步驟

1. 將權限模式設定為 `advanced`：

   ```
   set -privilege advanced
   ```

2. 啟用檔案存取時間更新並設定更新頻率：

   ```
   volume modify -volume vol_name -vserver <SVM name> -atime-update true -atime
   -update-period <seconds>
   ```

   以下範例啟用 `-atime-update` 和套件 `-atime-update-period` 至 86400 秒或 24 小時：

   ```
   c1: volume modify -volume origin1 vs1_c1 -atime-update true -atime
   -update-period 86400
   ```

3. 請確認 `-atime-update` 已啟用：

   ```
   volume show -volume vol_name -fields atime-update,atime-update-period
   ```

   ```
   c1::*> volume show -volume cache1_origin1 -fields atime-update,atime-
   update-period
   vserver volume         atime-update atime-update-period
   ------- -------------- ------------ -------------------
   vs2_c1  cache1_origin1 true         86400
   ```

4. 啟用之後，`-atime-update`您可以指定是否可以自動清理 FlexCache 磁碟區上的檔案，以及清理時間間隔：

   ```
   volume flexcache config modify -vserver <SVM name> -volume <volume_name> -is
   -atime-scrub-enabled <true|false> -atime-scrub-period <integer>
   ```

如需參數的詳細 `-is-atime-scrub-enabled`"指令參考資料ONTAP"資訊，請參閱。

在 **ONTAP FlexCache** 磁碟區上啟用全域檔案鎖定

從ONTAP 功能完整的1.10.1開始、您可以套用全域檔案鎖定功能、以防止讀取所有相關的快取檔案。

啟用全域檔案鎖定後、原始磁碟區的修改會暫停、直到所有 FlexCache 磁碟區都上線為止。只有當FlexCache 您控制快取與來源之間的連線可靠性時、才應啟用全域檔案鎖定、因為當停用時、可能會有修改逾時、而且當停用完時。

開始之前

- 全域檔案鎖定功能要求包含來源和所有相關快取的叢集執行ONTAP 版本為《更新版本的指南：可在新FlexCache 的或現有的支援區啟用全域檔案鎖定。此命令可在一個磁碟區上執行、並套用至所有相關聯的 FlexCache 磁碟區。

- 您必須處於進階權限層級、才能啟用全域檔案鎖定。
- 如果還原為早於 9.9.1 的 ONTAP 版本、則必須先在原始伺服器和相關快取上停用全域檔案鎖定。若要停用來源 Volume 、請執行： `volume flexcache prepare-to-downgrade -disable-feature-set 9.10.0`
- 啟用全域檔案鎖定的程序取決於原始伺服器是否有現有的快取：
  - [enable-gfl-new]
  - [enable-gfl-existing]

在新**FlexCache** 的支援區啟用全域檔案鎖定

步驟

1. 使用建立 FlexCache Volume `-is-global-file-locking` 設為true：

   ```
   volume flexcache create volume volume_name -is-global-file-locking-enabled
   true
   ```

   > 的預設值 `-is-global-file-locking` 為 "`FALSE" 。之後的任何時候 `volume flexcache create` 命令是在磁碟區上執行、必須與一起傳遞 `-is-global-file -locking enabled` 設為「 'true' 」 。

在現有**FlexCache** 的支援區上啟用全域檔案鎖定

步驟

1. 必須從來源磁碟區設定全域檔案鎖定。
2. 來源不能有任何其他現有關係（例如SnapMirror）。任何現有的關係都必須取消關聯。執行命令時、必須連接所有快取和磁碟區。若要檢查連線狀態、請執行：

   ```
   volume flexcache connection-status show
   ```

   所有列出的磁碟區的狀態應顯示為 `connected`. 如需詳細資訊、請參閱 "檢視FlexCache 彼此之間的關係狀態" 或 "從FlexCache 來源同步處理一個不同步的資料區的屬性"。

3. 在快取上啟用全域檔案鎖定：

   ```
   volume flexcache origin config show/modify -volume volume_name -is-global-file
   -locking-enabled true
   ```

相關資訊

- "指令參考資料ONTAP"

預先填入 **ONTAP FlexCache Volume**

您可以預先填入FlexCache 一個現象區、以縮短存取快取資料所需的時間。

開始之前

- 您必須是進階權限層級的叢集管理員

- 預先填入的路徑必須存在、否則預先填入作業將會失敗。

關於這項工作

- 預先填入只讀取檔案、並在目錄中搜尋
- 。 `-isRecursion` 此旗標會套用至傳遞給預先填入的目錄的完整清單

步驟

1. 預先填入FlexCache 一個資料流通量：

   ```
   volume flexcache prepopulate -cache-vserver vserver_name -cache-volume -path
   -list path_list -isRecursion true|false
   ```

   - 。 `-path-list` 參數指出您要從來源根目錄開始預先填入的相對目錄路徑。例如、如果來源根目錄命名為/origin、其中包含目錄/orige/dir1和/orige/dir2、您可以如下指定路徑清單： `-path-list dir1, dir2` 或 `-path-list /dir1, /dir2`。
   - 的預設值 `-isRecursion` 參數為True。

     此範例預先填入單一目錄路徑：

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1
       (volume flexcache prepopulate start)
     [JobId 207]: FlexCache prepopulate job queued.
     ```

     此範例預先填入多個目錄中的檔案：

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1,/dir2,/dir3,/dir4
       (volume flexcache prepopulate start)
     [JobId 208]: FlexCache prepopulate job queued.
     ```

     此範例預先填入單一檔案：

     ```
     cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
     -volume fg_cachevol_1 -path-list /dir1/file1.txt
       (volume flexcache prepopulate start)
     [JobId 209]: FlexCache prepopulate job queued.
     ```

     此範例預先填入來源的所有檔案：

```
cluster1::*> flexcache prepopulate start -cache-vserver vs2 -cache
-volume fg_cachevol_1 -path-list / -isRecursion true
  (volume flexcache prepopulate start)
[JobId 210]: FlexCache prepopulate job queued.
```

此範例包含預先填入的無效路徑：

```
cluster1::*> flexcache prepopulate start -cache-volume
vol_cache2_vs3_c2_vol_origin1_vs1_c1 -cache-vserver vs3_c2 -path-list
/dir1, dir5, dir6
  (volume flexcache prepopulate start)

Error: command failed: Path(s) "dir5, dir6" does not exist in origin
volume
       "vol_origin1_vs1_c1" in Vserver "vs1_c1".
```

2. 顯示讀取的檔案數：

   ```
   job show -id job_ID -ins
   ```

相關資訊

- "工作展示"

刪除 **ONTAP FlexCache** 關聯

如果不再需要使用此功能、您可以刪除FlexCache 一個「不相關」和FlexCache 「不相關」的功能。FlexCache

開始之前

如果啟用了 FlexCache 回寫功能，則必須先停用該功能才能刪除 FlexCache 磁碟區。請參閱 "停用 FlexCache 磁碟區的回寫功能"。

步驟

1. 從擁有FlexCache 此功能的叢集、FlexCache 將此功能離線：

   ```
   volume offline -vserver svm_name -volume volume_name
   ```

2. 刪除FlexCache 此功能：

   ```
   volume flexcache delete -vserver svm_name -volume volume_name
   ```

   從原始Volume和《不知如何使用的功能」中移除「不使用的功能」的相關詳細資料。FlexCache FlexCache

用於熱點修復的 FlexCache

利用 ONTAP FlexCache Volume 修正高效能運算工作負載的熱點

許多高效能運算工作負載（例如動畫呈現或 EDA ）的常見問題是熱點發現。當叢集或網路的特定部分比其他區域的負載大幅增加時，會發生熱點現象，導致效能瓶頸，並因為該位置集中的資料流量過多而降低整體效率。例如，檔案或多個檔案對執行中的工作需求很高，導致 CPU 瓶頸，用於（透過 Volume 關聯性）處理該檔案的要求。FlexCache 可協助減輕此瓶頸，但必須正確設定。

本文件說明如何設定 FlexCache 以修正熱點。

自 2024 年 7 月起、先前以 PDF 格式發佈的技術報告內容已與 ONTAP 產品文件整合。此 ONTAP 熱點補救技術報告內容自發表之日起即為全新內容，且從未製作過任何舊版格式。

主要概念

規劃熱點補救時，請務必瞭解這些基本概念。

- * 高密度 FlexCache （ HDF ） * ：一種精簡化的 FlexCache ，只要快取容量需求允許，就能跨越幾個節點
- * HDF Array （ HDFA ） * ：一組 HDFS ，位於同一來源的快取區，散佈於叢集中
- * SVM 間 HDFA* ：每部伺服器虛擬機器（ SVM ）的 HDFA 中有一個 HDF
- * SVM 內部 HDFA* ： HDFA 中的所有 HDFS 都在一個 SVM 中
- * 東西部流量 * ：從間接資料存取產生的叢集後端流量

下一步

- "瞭解如何使用高密度 FlexCache 建構架構，以協助補救熱點"
- "決定 FlexCache 陣列密度"
- "判斷 HDFS 的密度，並決定是否要使用 NFS 搭配 SVM 間 HDFAs 和 SVM 內部 HDFAs 來存取 HDFS"
- "設定 HDFA 和資料生命週期，以實現搭配 ONTAP 組態使用叢集快取的效益"
- "瞭解如何設定用戶端，以使用用戶端組態來散佈 ONTAP NAS 連線"

建構 ONTAP FlexCache 熱點補救解決方案

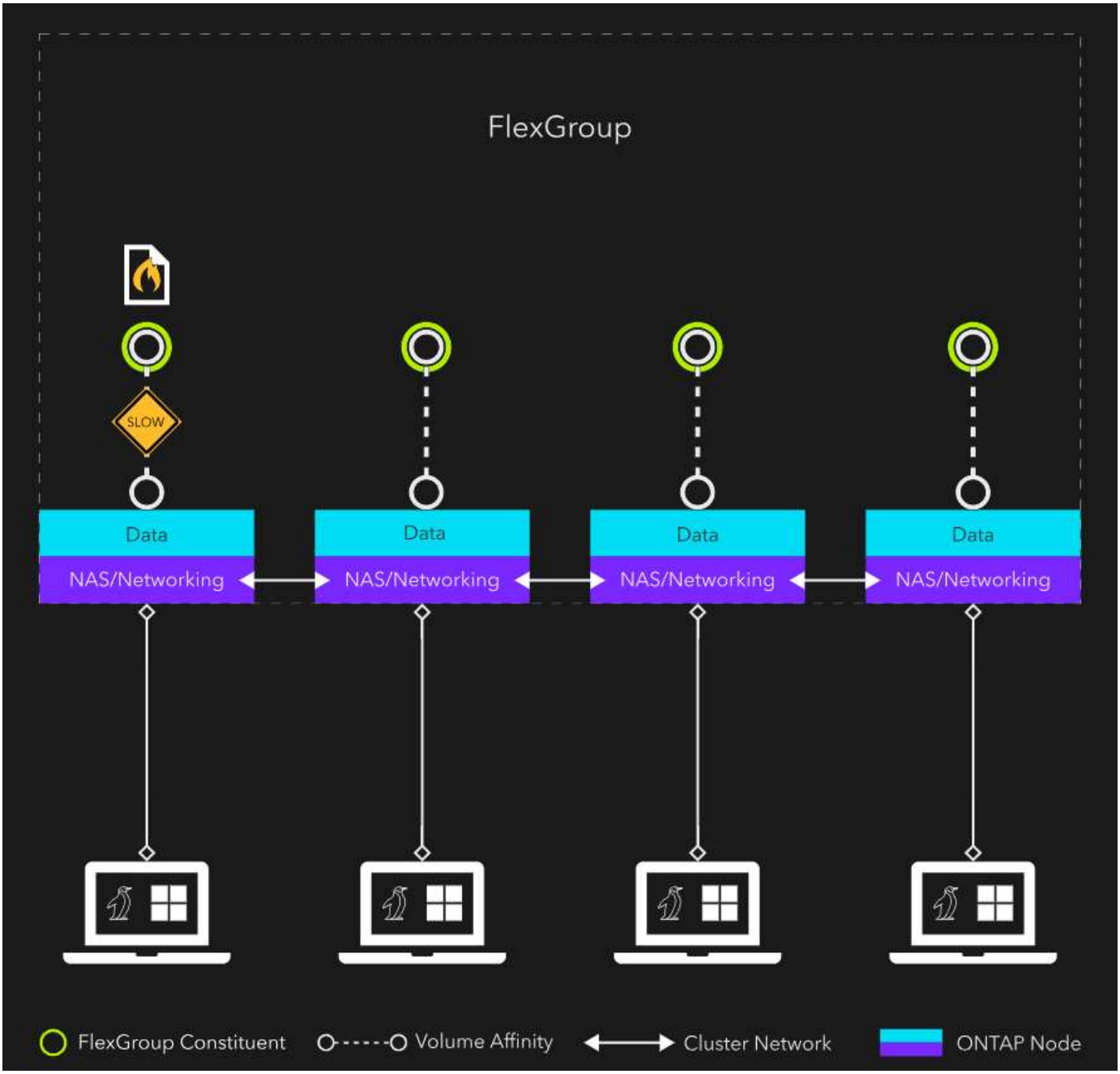
若要修正熱點，請探索瓶頸的根本原因，為何自動佈建 FlexCache 不夠充分，以及有效建構 FlexCache 解決方案所需的技術詳細資料。透過瞭解並實作高密度 FlexCache 陣列（ HDFAs ），您可以最佳化效能，消除高需求工作負載的瓶頸。

瞭解瓶頸

以下映像是典型的單一檔案熱點分析案例。磁碟區是 FlexGroup ，每個節點都有單一組成，檔案位於節點 1 上。

如果您將所有 NAS 用戶端的網路連線分散到叢集中的不同節點，則仍會在 CPU 上產生瓶頸，而 CPU 則會為熱檔案所在的磁碟區相關性提供服務。您也會將叢集網路流量（東西部流量）引入來自連接至檔案所在節點以外節點之用戶端的通話。東西部的流量負荷通常很小，但對於高效能運算工作負載而言，每個小位元都很重要。

圖 1 ： FlexGroup 單一檔案熱點案例

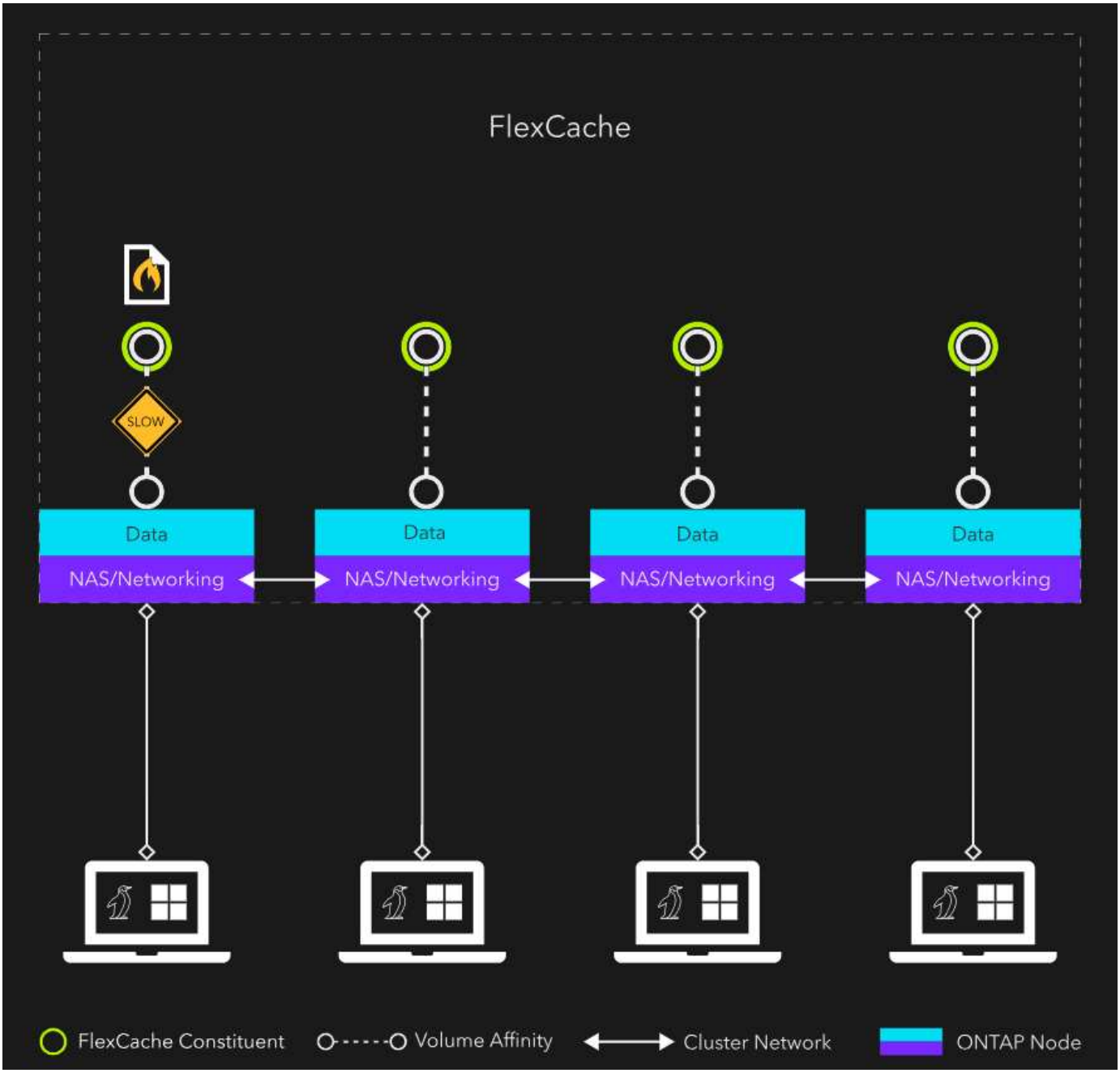


為何自動佈建的 **FlexCache** 不是答案

若要補救熱點現象，請消除 CPU 瓶頸，最好是東西部流量。如果設定正確， FlexCache 可以提供協助。

在下列範例中， FlexCache使用系統管理員、 NetApp控制台或預設 CLI 參數自動設定。圖 1.和圖 2.乍看之下它們是一樣的：都是四節點、單成分 NAS 容器。唯一的差異是，圖 1 的 NAS 容器是FlexGroup，而圖 2 的 NAS 容器是FlexCache。每個圖都描述了相同的瓶頸：節點 1 的 CPU 用於卷親和性服務存取熱文件，以及導致延遲的東西向流量。自動配置的FlexCache並未消除瓶頸。

圖 2 ：自動佈建的 **FlexCache** 案例



FlexCache 的解剖構造

若要有效建構 FlexCache 以進行熱點修復，您必須瞭解 FlexCache 的一些技術詳細資料。

FlexCache 始終是稀疏 FlexGroup 。FlexGroup 由多個 FlexVols 組成。這些 FlexVols 稱為 FlexGroup 成分。在預設的 FlexGroup 配置中，叢集中的每個節點都有一或多個組成。組成要素是在抽象層下方「縫製」，並以單一大型 NAS 容器的形式呈現給用戶端。當檔案寫入 FlexGroup 時，擷取啟發式系統會判斷檔案將儲存在哪個組成要素上。它可能是包含用戶端 NAS 連線的組成要素，也可能是不同的節點。位置無關緊要，因為所有作業都在抽象層下運作，而且對用戶端而言是不可見的。

讓我們將 FlexGroup 的這項瞭解應用到 FlexCache 。由於 FlexCache 是建立在 FlexGroup 上，因此默認情況下，您只有一個 FlexCache ，它在羣集中的所有節點上都具有組成部分圖 1.，如所示。在大多數情況下，這是一件好事。您正在使用叢集中的所有資源。

不過，為了修正 Hot 檔案，這並不理想，因為有兩個瓶頸：單一檔案的 CPU 和東西部流量。如果您為 Hot 檔案

在每個節點上建立具有組成成分的 FlexCache ，則該檔案仍只會位於其中一個組成要素上。這表示只有一個 CPU 可為所有存取 Hot 檔案的服務。您也想要限制到達 Hot 檔案所需的東西部流量。

解決方案是一系列高密度 FlexCaches 。

高密度 **FlexCache** 的解剖構造

高密度 FlexCache （ HDF ）在快取資料的容量需求允許的節點數量範圍內，會有多個組成節點。目標是讓快取在單一節點上運作。如果容量需求使得這種情況變得不可能，您只能在少數幾個節點上建立成員。

例如， 24 節點叢集可能有三個高密度 FlexCaches ：

- 一個跨節點 1 至 8
- 跨越節點 9 到 16 的第二個節點
- 跨越節點 17 到 24 的第三個節點

這三個 HDFS 將組成一個高密度 FlexCache 陣列（ HDFA ）。如果檔案平均分散在每個 HDF 中，您將有機會將用戶端要求的檔案存放在前端 NAS 連線的本機位置，達到八分之一。如果您的 12 個 HDFS 只橫跨兩個節點，則檔案有 50% 的可能是本機檔案。如果您可以將 HDF 向下收合至單一節點，並建立其中 24 個節點，則您可以保證檔案是本機檔案。

此組態可消除所有東西部流量，最重要的是，將提供 24 個 CPU/ 磁碟區關聯性，以供存取 Hot 檔案。

接下來呢？

"決定 FlexCache 陣列密度"

相關資訊

"FlexGroup 和 TR 的文件"

判斷 **ONTAP FlexCache** 密度

您的第一個熱點補救設計決策是找出 FlexCache 密度。下列範例為四節點叢集。假設檔案數平均分佈在每個 HDF 的所有成分之間。也假設所有節點之間的前端 NAS 連線都會平均分配。

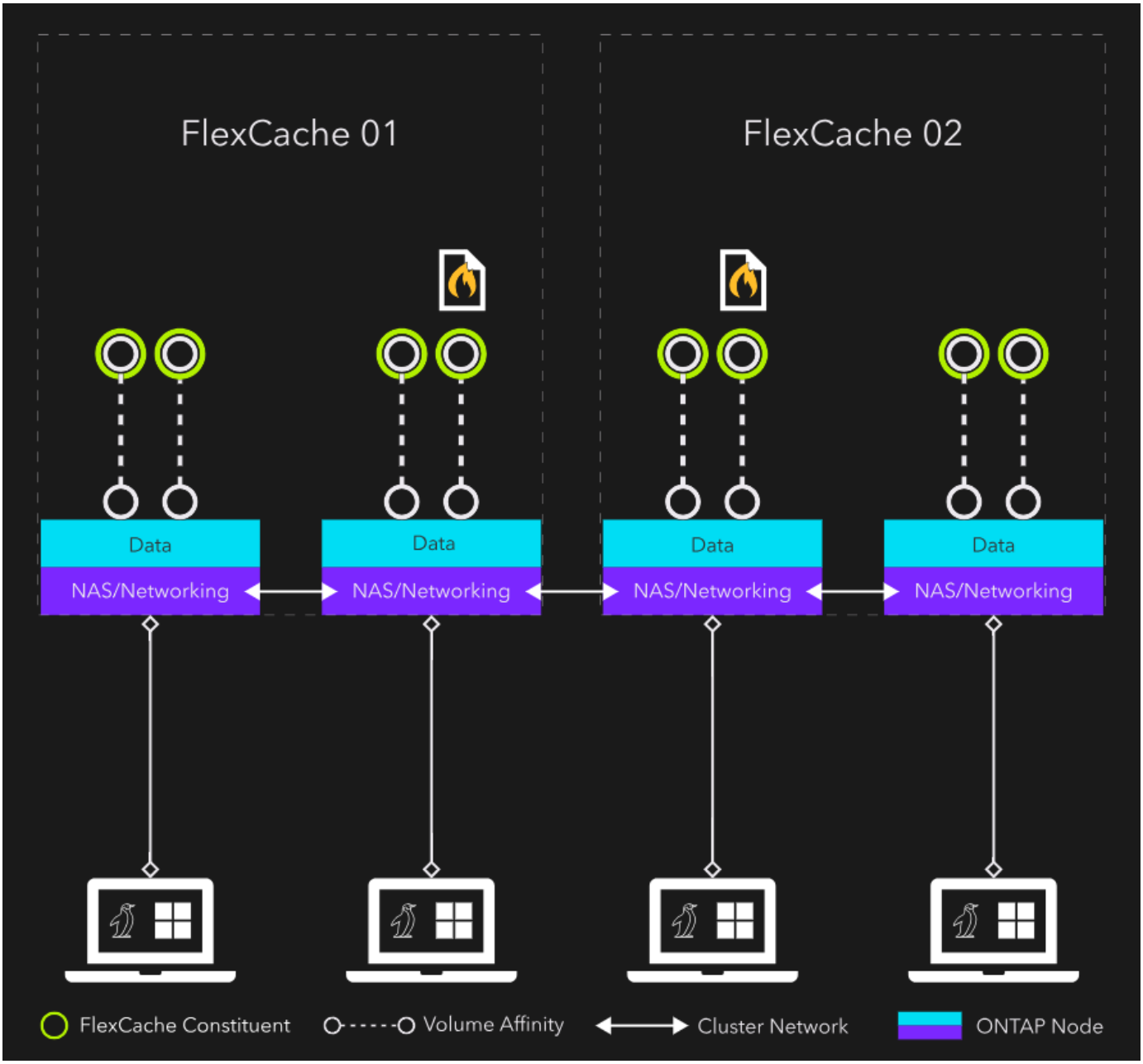
雖然這些範例並非您唯一可以使用的組態，但您應該瞭解導引設計原則，以便在空間需求和可用資源允許的情況下，製作盡可能多的 HDFS 。

HDFAs 使用下列語法表示： `HDFs per HDFA x nodes per HDF x constituents per node per HDF`

2x2x2 HDFA 組態

圖 1.為 2x2x2 HDFA 組態的範例：兩個 HDFS ，每個 HDFS 跨越兩個節點，每個節點包含兩個組成 Volume 。在此範例中，每個用戶端都有 50% 的機會可以直接存取 Hot 檔案。四個用戶端中有兩個具有東西部流量。重要的是，現在有兩個 HDFS ，這表示熱檔案有兩個不同的快取。現在有兩個 CPU/ 磁碟區關聯性，可提供熱檔案的存取。

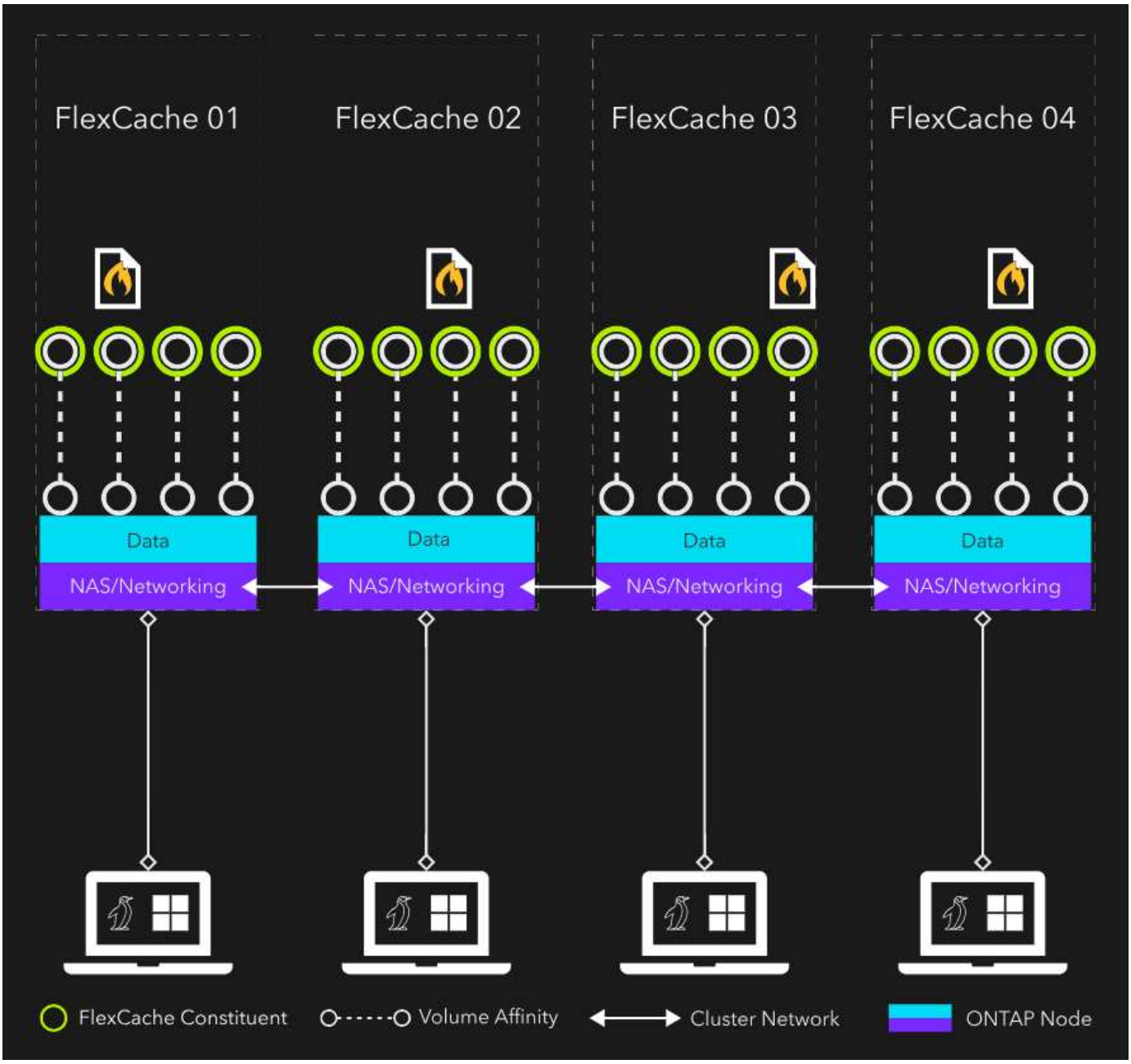
圖 **1** ： **2x2x2 HDFA** 組態



4x1x4 HDFA 組態

圖 2.代表最佳組態。這是 4x1x4 HDFA 組態的範例：四個 HDFS ，每個都包含在單一節點，每個節點包含四個成分。在此範例中，每個用戶端都保證能夠直接存取 Hot 檔案的快取。由於四個不同節點上有四個快取檔案，因此四個不同的 CPU/ 磁碟區關聯性有助於服務存取 Hot 檔案。此外，也不會產生東西部流量。

圖 **2** ： **4x1x4 HDFA** 組態



下一步

在您決定要設定 HDFS 的密度後，如果您要使用來存取 HDFS "SVM 間 HDFAs 和 SVM 內部 HDFAs"，就必須做出另一項設計決定。

決定 **ONTAP Inter-SVM** 或 **SVM** 內部 **HDFA** 選項

確定 HDFS 的密度之後，請決定是否要使用 NFS 存取 HDFS ，並瞭解 SVM 間 HDFA 和 SVM 內部 HDFA 選項。

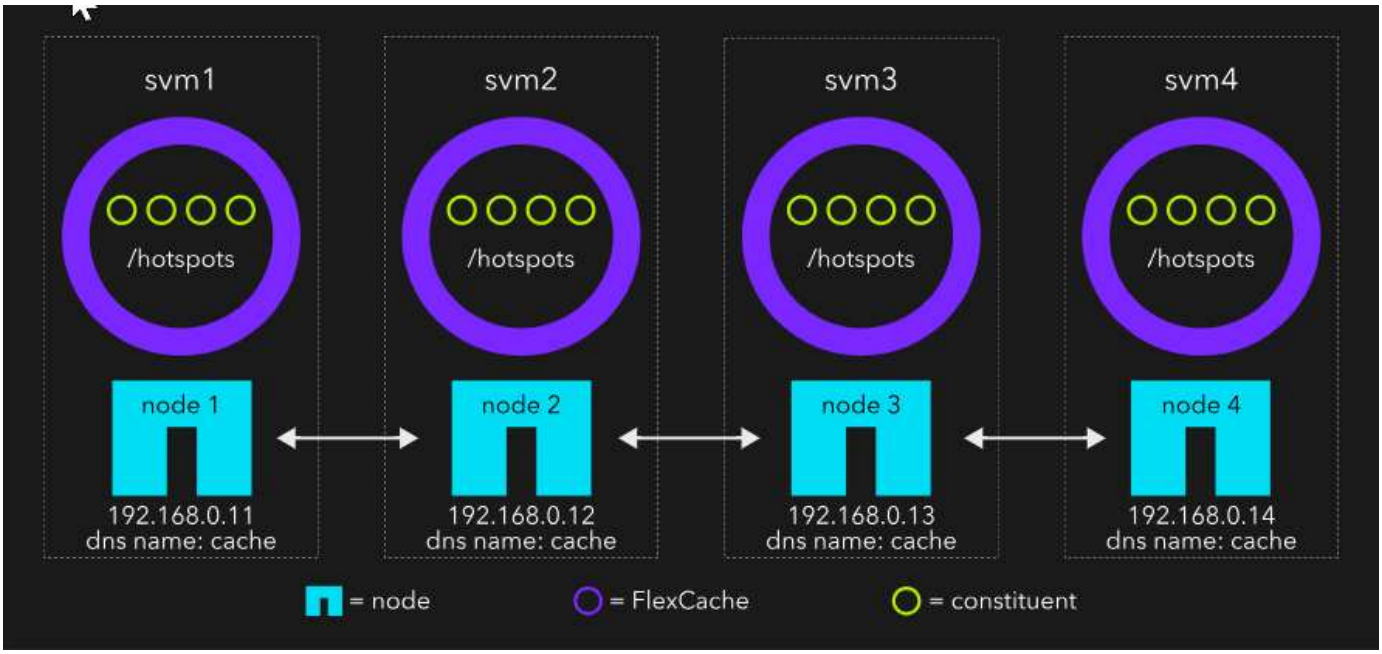
如果只有 SMB 用戶端會存取 HDFS ，您應該在單一 SVM 中建立所有 HDFS 。請參閱 Windows 用戶端組態，瞭解如何使用 DFS 目標來進行負載平衡。

SVM 間 HDFA 部署

SVM 間 HDFA 需要為 HDFA 中的每個 HDF 建立 SVM 。如此一來， HDFA 內的所有 HDFS 都能擁有相同的交會路徑，讓用戶端更容易設定。

在範例中圖 1.，每個 HDF 都位於自己的 SVM 中。這是 SVM 間 HDFA 部署。每個 HDF 都有 / 熱點的交會路徑。此外，每個 IP 都有 DNS A 主機名稱快取記錄。此組態會利用 DNS 循環配置資源，在不同的 HDFS 之間裝載平衡負載。

圖 1 ： 4x1x4 SVM 間 HDFA 組態

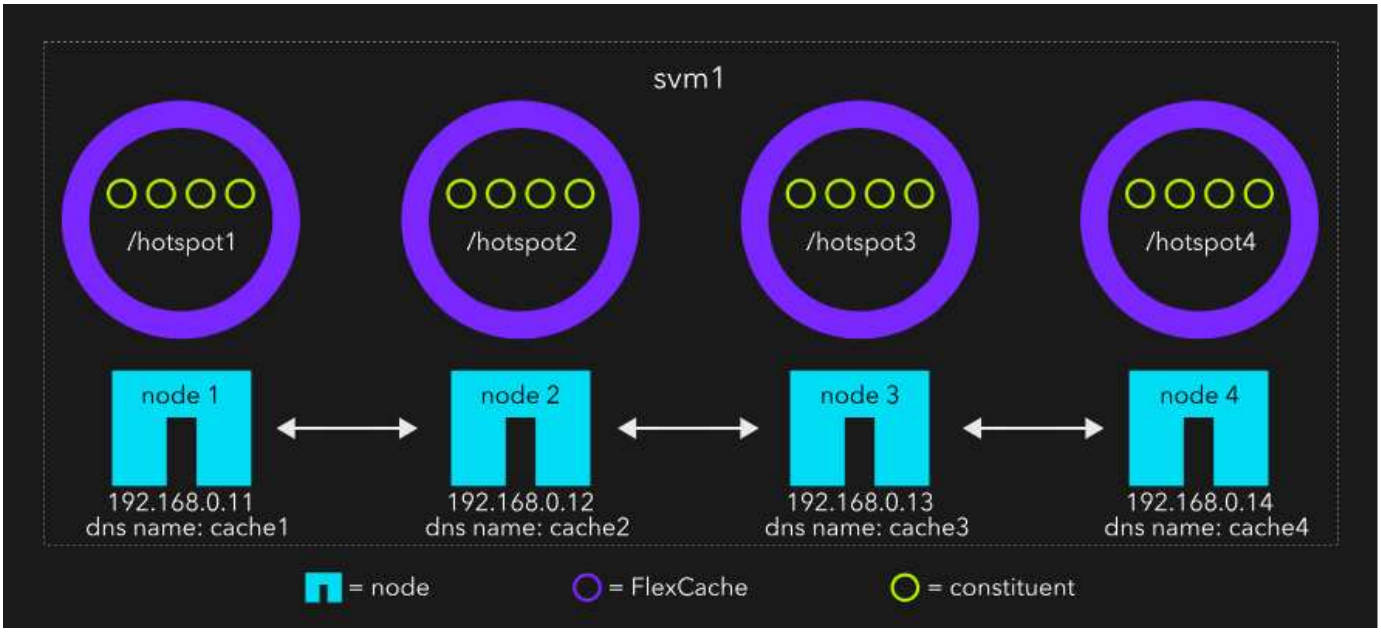


SVM 內部 HDFA 部署

SVM 內部需要每個 HDF 都有唯一的交會路徑，但所有 HDFS 都在一個 SVM 中。ONTAP 中的這項設定較為簡單，因為它只需要一個 SVM ，但它需要在 Linux 端進行更進階的組態 `autofs`，並將資料 LIF 置於 ONTAP 中。

在範例中圖 2.，每個 HDF 都位於同一個 SVM 中。這是 SVM 內部 HDFA 部署，需要交會路徑是唯一的。若要讓負載平衡正常運作，您需要為每個 IP 建立唯一的 DNS 名稱，並將主機名稱解析為的資料生命負載僅放置在 HDF 所在的節點上。您也需要依照中所述設定 `autofs`多個項目"Linux 用戶端組態"。

圖 2 ： 4x1x4 SVM 內部 HDFA 組態



下一步

現在您已經瞭解如何部署您的 HDFA, "部署 HDFA 並設定用戶端以分散式方式存取"。

設定 **HDFAs** 和 **ONTAP** 資料生命

您必須適當設定 HDFA 和資料生命週期，才能實現此熱點補救解決方案的效益。此解決方案在同一個叢集中使用同一個來源和 HDFA 的叢集內建快取功能。

以下是兩種 HDFA 範例組態：

- 2x2x2 SVM 間 HDFA
- 4x1x4 SVM 內部 HDFA

關於這項工作

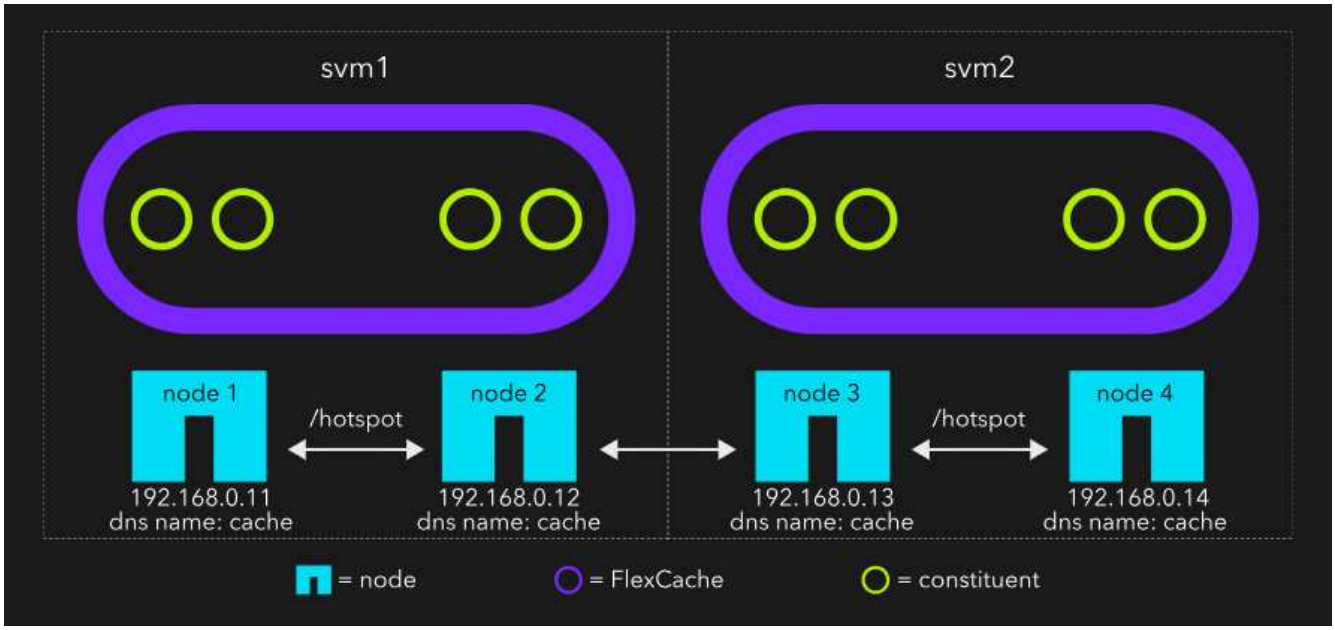
使用 ONTAP CLI 執行此進階組態。您必須在命令中使用兩種組態 `flexcache create`，而且必須確定其中一種組態尚未設定：

- `-aggr-list`：提供集合體或集合體清單，這些集合體位於您要限制 HDF 的節點或節點子集上。
- `-aggr-list-multiplier`：確定選項中列出的每個集合將創建多少個組成 `aggr-list`。如果列出兩個集合體，並將此值設為 `2`，則最後會有四個組成。NetApp 建議每個集合最多 8 個組成單位，但 16 個也足夠。
- `-auto-provision-as`：如果選中此選項卡， CLI 將嘗試自動填寫並將值設置爲 `flexgroup`。請確定尚未設定。如果出現，請將其刪除。

建立 **2x2x2** 的 **SVM** 間 **HDFA** 組態

1. 如圖 1 所示，若要協助設定 2x2x2 的 SVM 間 HDFA ，請填寫準備表。

   圖 **1** ： **2x2x2 SVM** 內部 **HDFA** 配置



SVM	每個 HDF 的節點數	集合體	每個節點的組成	交會路徑	資料 LIF IP
svm1	node1 、 node2	aggr1 、 aggr2	2.	/HotSpot	192 · 168 · 0 · 11 · 0 · 12
svm2	node3 、 node4	aggr3 、 aggr4	2.	/HotSpot	192 · 168 · 0 · 13 · 0 · 14

2. 建立 HDFS 。執行下列命令兩次，準備工作表中的每一列各執行一次。請務必調整 `vserver`第二次迭代的和 `aggr-list`值。

```
cache::> flexcache create -vserver svm1 -volume hotspot -aggr-list
aggr1,aggr2 -aggr-list-multiplier 2 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot
```

3. 建立資料生命。執行命令四次，在準備工作表中列出的節點上，為每個 SVM 建立兩個資料生命週期。請務必針對每次迭代適當調整值。

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

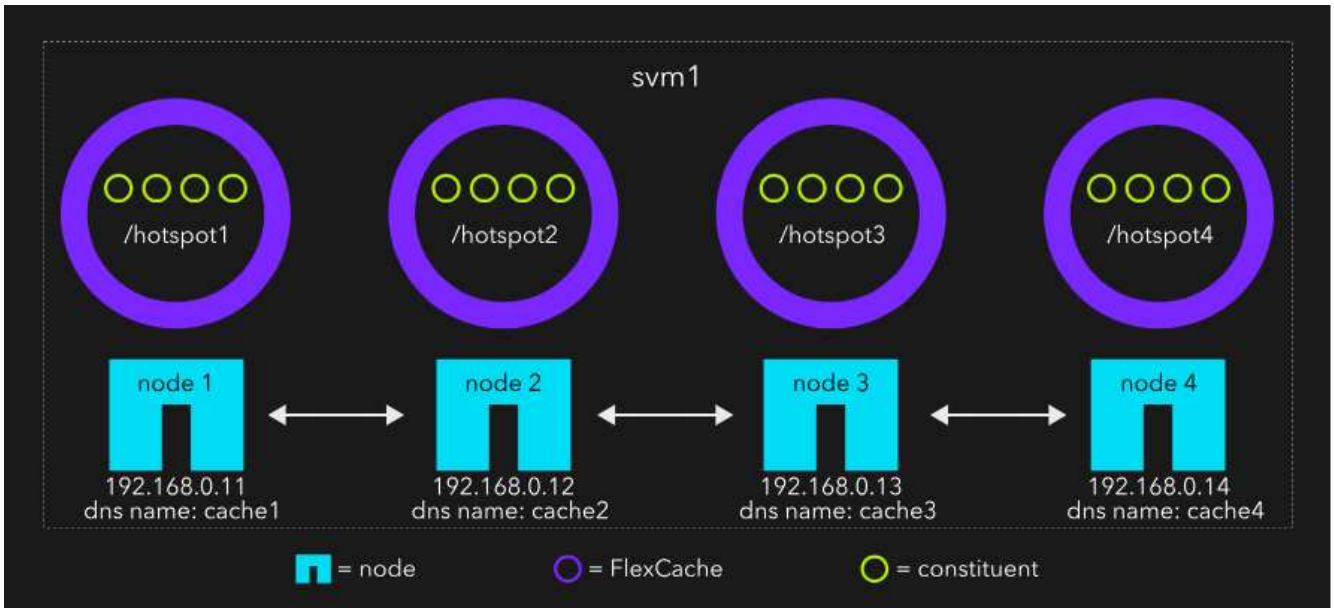
下一步

現在您需要設定用戶端，以適當地使用 HDFA 。請參閱。 "用戶端組態"

建立 **4x1x4 SVM** 內部 **HDFA**

1. 如圖 2 所示，若要協助設定 4x1x4 SVM 間 HDFA ，請填寫準備表。

圖 **2** ： **4x1x4 SVM** 內部 **HDFA** 配置



SVM	每個 HDF 的節點數	集合體	每個節點的組成	交會路徑	資料 LIF IP
svm1	節點1	aggr1	4.	/hotspot1.	192.168.0.11
svm1	節點2	aggr2	4.	/hotspot2.	192.168.0.12
svm1	node3	aggr3	4.	/hotspot3.	192.168.0.13
svm1	node4	aggr4	4.	/hotspot4.	192.168.0.14

2. 建立 HDFS 。執行下列命令四次，準備工作表中的每一列各執行一次。請務必調整 `aggr-list`每次迭代的和 `junction-path`值。

```
cache::> flexcache create -vserver svm1 -volume hotspot1 -aggr-list
aggr1 -aggr-list-multiplier 4 -origin-volume <origin_vol> -origin
-vserver <origin_svm> -size <size> -junction-path /hotspot1
```

3. 建立資料生命。執行命令四次，在 SVM 中總共建立四個資料生命週期。每個節點應有一個資料 LIF 。請務必針對每次迭代適當調整值。

```
cache::> net int create -vserver svm1 -home-port e0a -home-node node1
-address 192.168.0.11 -netmask-length 24
```

下一步

現在您需要設定用戶端，以適當地使用 HDFA 。請參閱。 "用戶端組態"

設定用戶端以散佈 **ONTAP NAS** 連線

若要補救熱點現象，請正確設定用戶端，以避免 CPU 瓶頸。

Linux 用戶端組態

無論您選擇 SVM 內部部署或 SVM 內部 HDFA 部署，您都應該在 Linux 中使用 `autofs`，以確保用戶端在不同的 HDFS 之間進行負載平衡。 `autofs`SVM 之間和 SVM 內部的組態將有所不同。

開始之前

您需要 `autofs`安裝適當的相依性。如需相關說明，請參閱 Linux 文件。

關於這項工作

所述步驟將使用範例 `/etc/auto_master`檔案搭配下列項目：

```
/flexcache auto_hotspot
```

這會設定 `autofs`為在程序嘗試存取目錄時，隨時尋找目錄 `/flexcache`中所 `/etc`呼叫的檔案 `auto_hotspot`。檔案的內容 `auto_hotspot`會決定要在目錄中掛載哪個 `NFS` 伺服器和連接路徑 `/flexcache`。所述範例為檔案的不同組態 `auto_hotspot`。

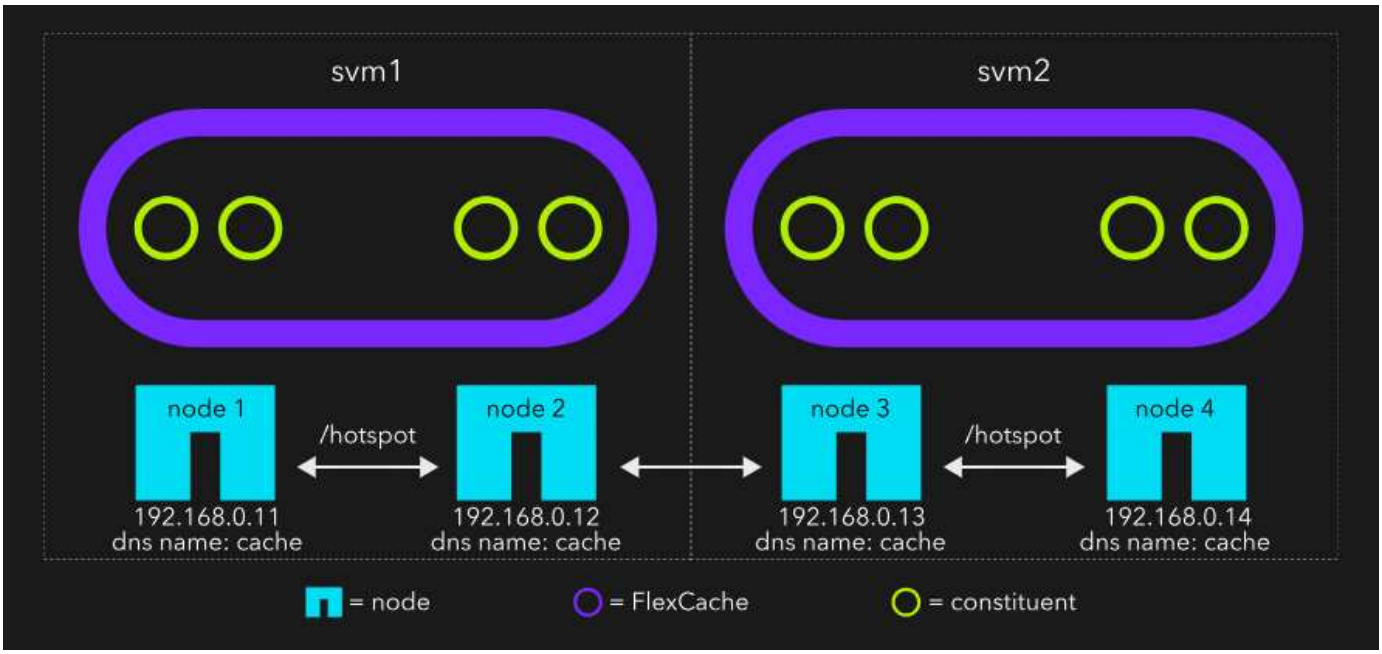
SVM 內部 **HDFA** 自動設定

在下列範例中，我們將在中建立 `autofs`圖表的對應圖 1.。因為每個快取都有相同的交會路徑，而且主機名稱有四個 DNS A 記錄，所以 `cache`我們只需要一行：

```
hotspot cache:/hotspot
```

這一簡單行將導致 NFS 客戶端對主機名執行 DNS 查詢 `cache`。DNS 設定為以循環方式傳回 IP 。這將導致前端 NAS 連線的平均分配。用戶端收到 IP 之後，會將連接路徑掛載 `/hotspot`到 `/flexcache/hotspot`。它可以連線至 SVM1 ， SVM2 ， SVM3 或 SVM4 ，但特定的 SVM 並不重要。

圖 **1** ： **2x2x2 SVM** 間 **HDFA**



SVM 內部 HDFA 自動設定

在下列範例中，我們將在中建立 `autofs`圖表的對應圖 2.。我們需要確保 NFS 用戶端裝載屬於 HDF 交會路徑部署一部分的 IP 。換句話說，我們不想使用 IP 192 · 168 · 0 · 11 以外的任何設備進行掛載 `/hotspot1。為達此目的，我們可以列出對應中一個本機裝載位置的四個 IP/ 交會路徑配對 auto_hotspot。

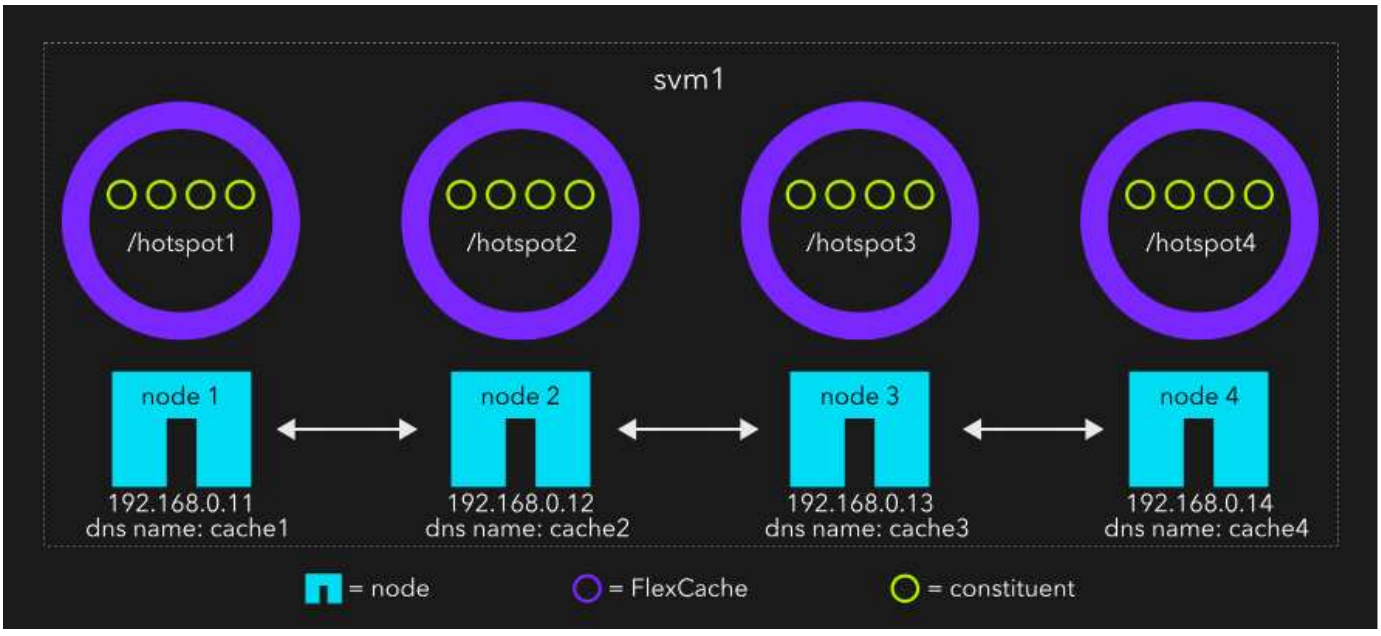
(`\`以下示例中的反斜槓）將繼續輸入下一行，使讀取更容易。

```
hotspot     cache1:/hostspot1 \
            cache2:/hostspot2 \
            cache3:/hostspot3 \
            cache4:/hostspot4
```

當用戶端嘗試存取 `/flexcache/hotspot`時， `autofs`將會對所有四個主機名稱執行轉送查詢。假設所有四個 IP 都位於用戶端所在的同一子網路或不同的子網路中， `autofs`則會對每個 IP 發出 NFS NULL ping 。

此 NULL ping 需要 ONTAP 的 NFS 服務處理封包，但不需要任何磁碟存取。第一個要傳回的 ping 將是 IP 和連接路徑 `autofs`選擇掛載。

圖 2 ： 4x1x4 SVM 內部 HDFA



Windows 用戶端組態

使用 Windows 用戶端時，您應該使用 SVM 內部 HDFA 。若要在 SVM 中的不同 HDFS 之間平衡負載，您必須在每個 HDF 中新增唯一的共用名稱。之後，請依照中的步驟"Microsoft文件"，為同一個資料夾實作多個 DFS 目標。

網路管理

開始使用

使用系統管理員視覺化 **ONTAP** 網路

從 ONTAP 9 開始、您可以使用系統管理員來顯示一個圖形、顯示網路的元件和組態、讓您查看主機、連接埠、 SVM 、 Volume 等各主機之間的網路連線路徑。從 ONTAP 9 。12.1 開始、您可以在網路介面網格上檢視 LIF 和子網路關聯。

當您選取 * 網路 > 總覽 * 或從儀表板的 * 網路 * 區段中選取時、圖形會顯示出來 → 。

下圖顯示下列元件類別：

- 主機
- 儲存連接埠
- 網路介面
- 儲存VM
- 資料存取元件

每個區段都會顯示其他詳細資料、您可以將滑鼠游標暫留或選取以執行網路管理和組態工作。

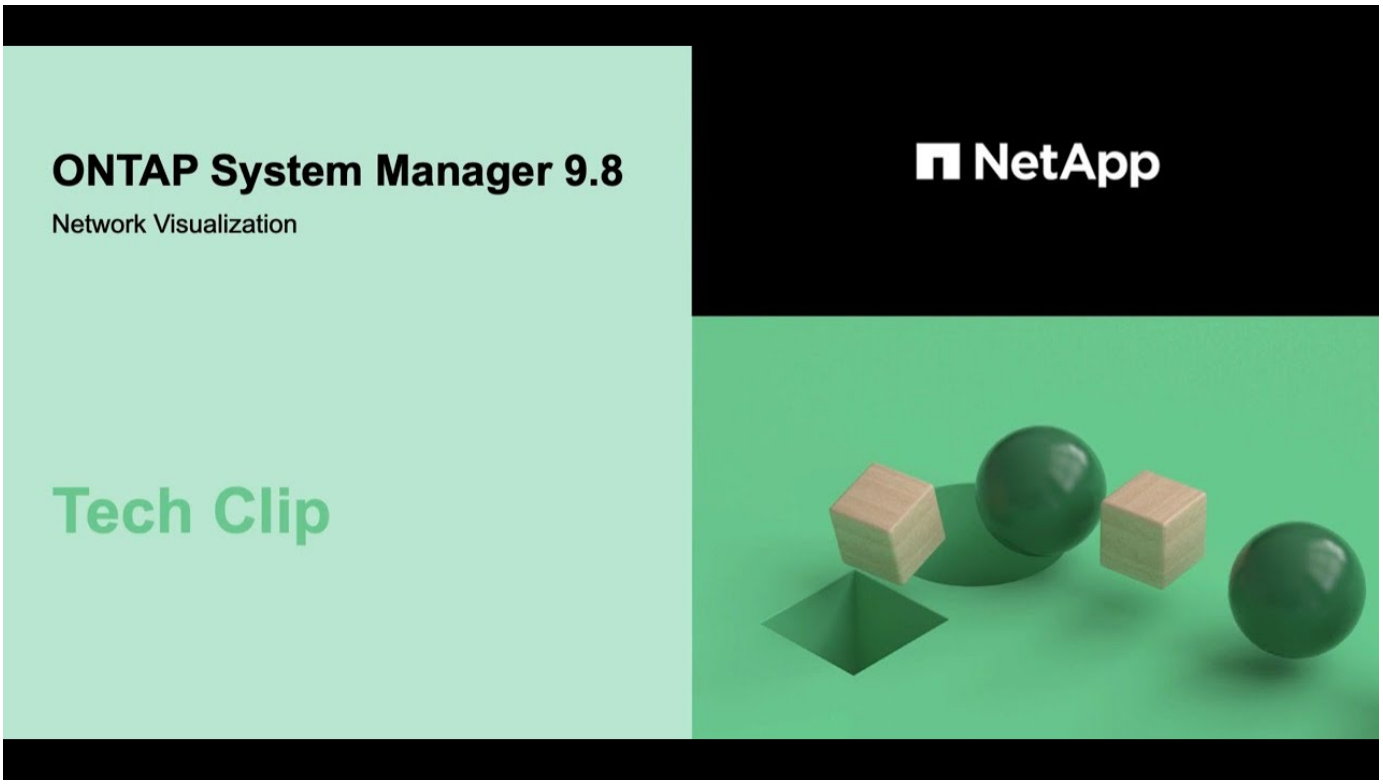
如果您使用的是傳統系統管理程式（僅適用於 ONTAP 9 7 及更早版本）、請參閱"管理網路"。

範例

以下是您可以與圖形互動的多種方式範例、用以檢視每個元件的詳細資料、或是啟動管理網路的行動：

- 按一下主機即可查看其組態：連接埠、網路介面、儲存 VM 及與其相關的資料存取元件。
- 將滑鼠游標移到儲存VM中的磁碟區數目上、即可選取磁碟區以檢視其詳細資料。
- 選取iSCSI介面以檢視其上週的效能。
- 按一下 ⋮ 元件旁的、即可啟動修改該元件的動作。
- 快速判斷網路中可能發生的問題所在位置、不正常元件旁會顯示「X」。

System Manager網路視覺化影片



瞭解 ONTAP 叢集的網路元件

在設定叢集之前、您應該先熟悉叢集的網路元件。將叢集的實體網路元件組態為邏輯元件、可在ONTAP 畫面上提供靈活度和多租戶功能。

叢集中的各種網路元件如下：

- 實體連接埠

  網路介面卡（NIC）和主機匯流排介面卡（HBA）可提供實體（乙太網路和光纖通道）連線、從每個節點連至實體網路（管理和資料網路）。

  如需站台需求、交換器資訊、連接埠纜線資訊、以及控制器內建連接埠纜線、請參閱Hardware Universe 上的《》（英文） "hwu.netapp.com"。

- 邏輯連接埠

  虛擬區域網路（VLAN）和介面群組構成邏輯連接埠。介面群組將多個實體連接埠視為單一連接埠、而VLAN則將實體連接埠細分為多個獨立連接埠。

- IPspaces

  您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

- 廣播網域

  廣播網域位於IPspace中、包含一組網路連接埠、這些連接埠可能來自叢集中的許多節點、屬於同一個第2層網路。群組中的連接埠用於SVM中的資料流量。

- 子網路

  子網路是在廣播網域內建立、其中包含屬於同一第3層子網路的IP位址集區。此IP位址集區可簡化LIF建立期間的IP位址配置。

- 邏輯介面

  邏輯介面（LIF）是與連接埠相關聯的IP位址或全球連接埠名稱（WWPN）。它與容錯移轉群組、容錯移轉規則及防火牆規則等屬性相關聯。LIF會透過目前繫結的連接埠（實體或邏輯）透過網路進行通訊。

  叢集中的不同類型生命體包括資料生命量、叢集範圍內的管理生命體、節點範圍內的管理生命體、叢集間生命體及叢集生命體。生命生命的所有權取決於LIF所在的SVM。資料生命體歸資料SVM所有、節點範圍內的管理生命體、叢集範圍內的管理、以及叢集間生命體歸管理SVM所有、叢集生命體歸叢集SVM所有。

- DNS區域

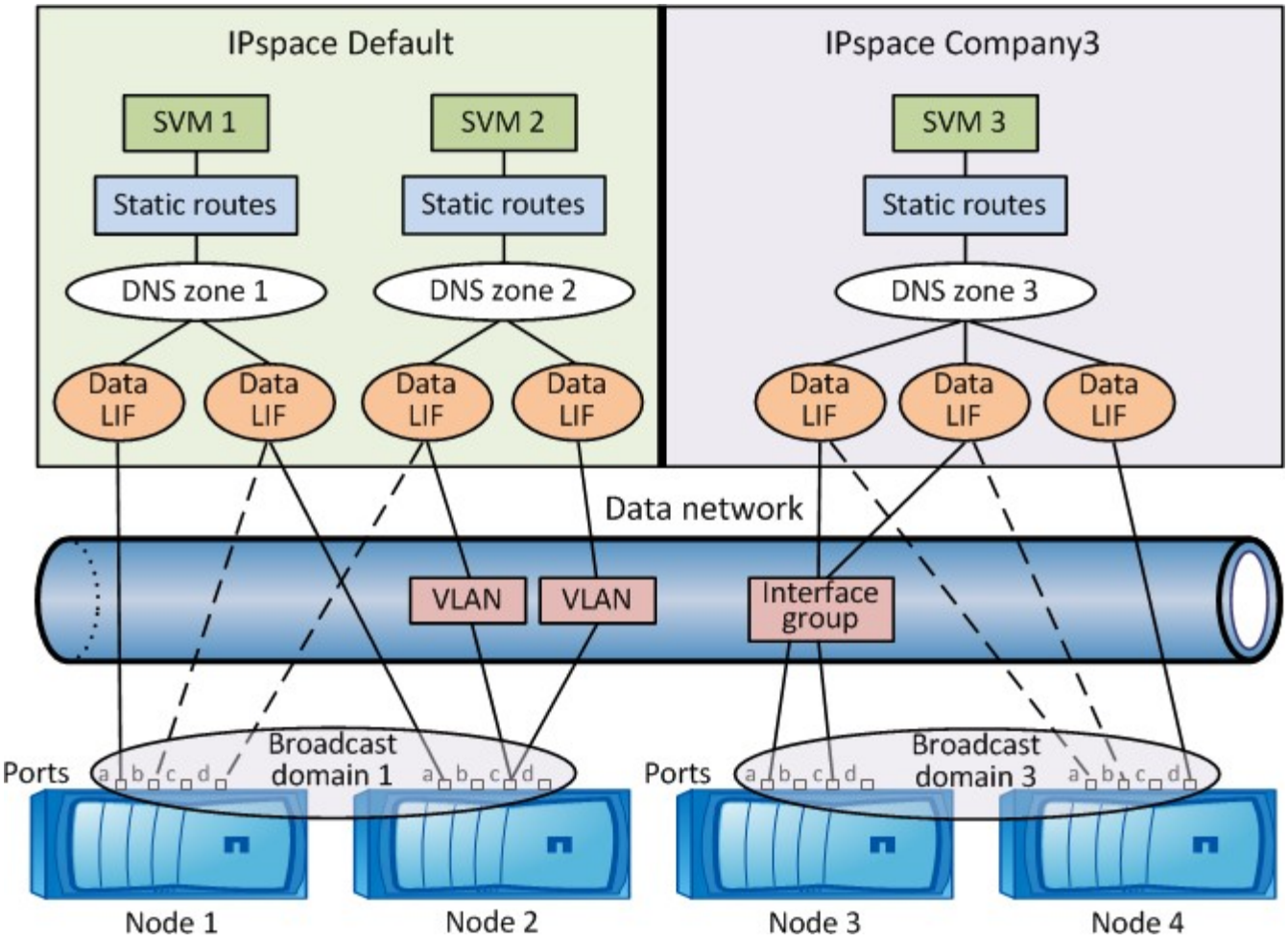
  DNS區域可在LIF建立期間指定、提供透過叢集DNS伺服器匯出LIF的名稱。多個LIF可以共用相同的名稱、讓DNS負載平衡功能根據負載來分配名稱的IP位址。

  SVM可以有多個DNS區域。

- 路由

  每個SVM在網路方面都是自給自足的。SVM擁有可連線至每個已設定外部伺服器的生命和路由。

  下圖說明不同的網路元件在四節點叢集中的關聯方式：

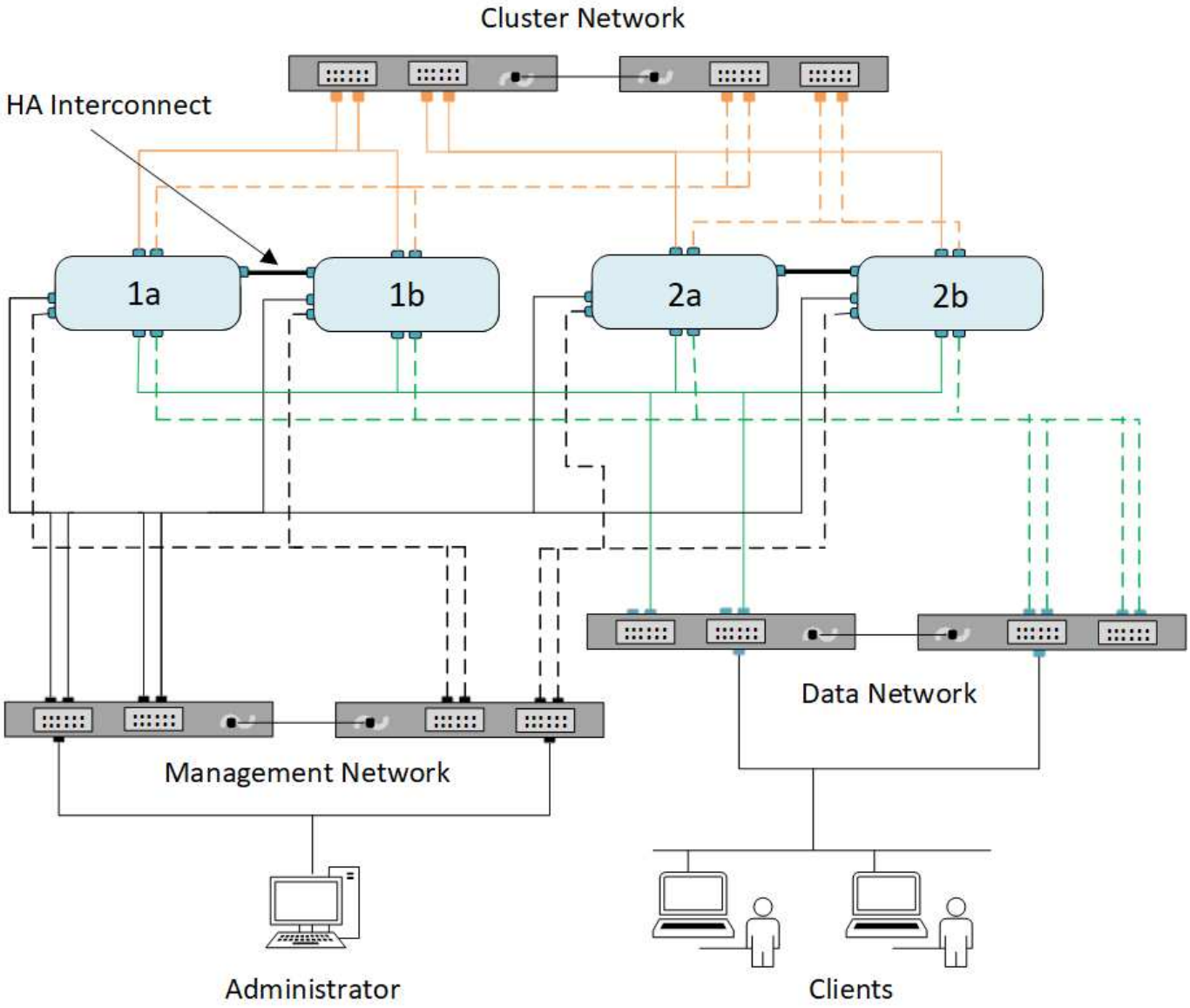


ONTAP 網路纜線的最佳實務做法

網路佈線最佳實務做法可將流量分隔至下列網路：叢集、管理和資料。

您應該連接叢集、使叢集流量與所有其他流量位於不同的網路上。這是一種選擇性做法、但建議您將網路管理流量與資料和叢集內流量分開。藉由維護個別的網路、您可以獲得更好的效能、更容易管理、並改善節點的安全性與管理存取。

下圖說明包含三個獨立網路的四節點HA叢集的網路佈線：



在佈線網路連線時、您應遵循特定準則：

- 每個節點都應連線至三個不同的網路。

  一個網路用於管理、一個用於資料存取、一個用於叢集內通訊。管理和資料網路可以邏輯分隔。

- 您可以將多個資料網路連線至每個節點、以改善用戶端（資料）流量傳輸。
- 建立叢集時無需資料網路連線、但必須包含叢集互連連連線。
- 每個節點都應有兩個或多個叢集連線。

如需網路纜線的詳細資訊、請參閱 "系統文件中心AFF FAS" 和 "Hardware Universe"。

判斷 ONTAP 網路中要使用的 LIF 容錯移轉原則

廣播網域、容錯移轉群組及容錯移轉原則可共同運作、以判斷在設定LIF的節點或連接埠發生故障時、哪個連接埠會接管。

廣播網域會列出同一層乙太網路中所有可連線的連接埠。從其中一個連接埠傳送的乙太網路廣播封包會被廣播網域中的所有其他連接埠所看到。廣播網域的這項通用可到達性特性對lifs很重要、因為如果LIF要容錯移轉至廣播網域中的任何其他連接埠、它仍可連線到從原始連接埠可連線的每個本機和遠端主機。

容錯移轉群組可定義廣播網域內的連接埠、以提供彼此的LIF容錯移轉涵蓋範圍。每個廣播網域都有一個容錯移轉群組、其中包含所有連接埠。此容錯移轉群組包含廣播網域中的所有連接埠、是LIF的預設及建議容錯移轉群組。您可以使用所定義的較小子集建立容錯移轉群組、例如在廣播網域中具有相同連結速度的連接埠容錯移轉群組。

容錯移轉原則決定LIF在節點或連接埠當機時、如何使用容錯移轉群組的連接埠。將容錯移轉原則視為套用至容錯移轉群組的篩選器類型。LIF的容錯移轉目標（LIF可容錯移轉的一組連接埠）是透過將LIF的容錯移轉原則套用至廣播網域中LIF的容錯移轉群組來決定。

您可以使用下列CLI命令檢視LIF的容錯移轉目標：

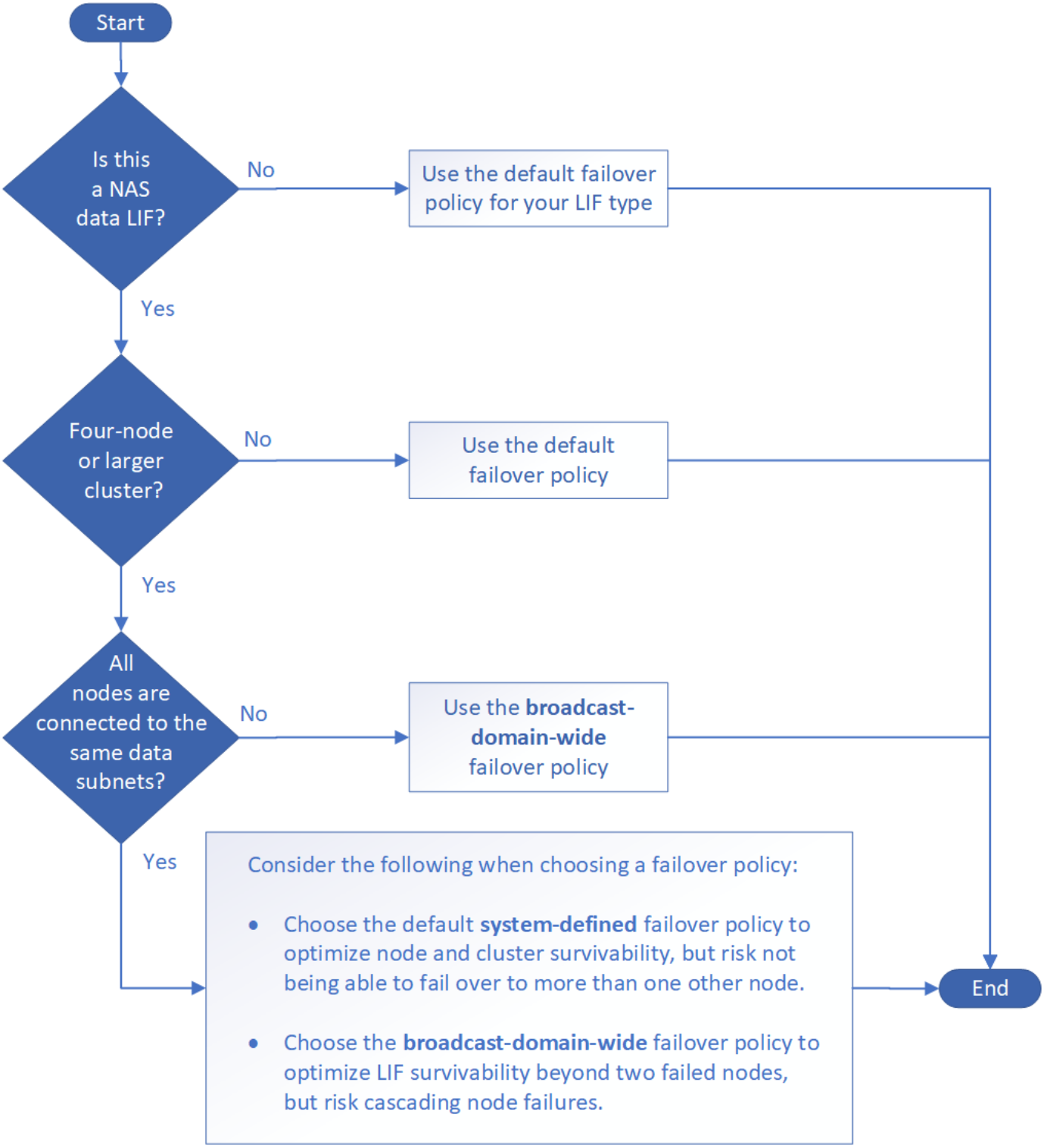
```
network interface show -failover
```

NetApp強烈建議針對LIF類型使用預設的容錯移轉原則。

決定要使用哪個**LIF**容錯移轉原則

決定是使用建議的預設容錯移轉原則、還是根據LIF類型和環境來變更。

容錯移轉原則決策樹狀結構



依**LIF**類型的預設容錯移轉原則

LIF類型	預設容錯移轉原則	說明
BGP lifs	已停用	LIF不會容錯移轉至其他連接埠。
叢集生命	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
叢集管理LIF	整個廣播網域	LIF會容錯移轉至同一個廣播網域中的連接埠、以及叢集中的任何節點。

叢集間LIF	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
NAS資料生命量	系統定義	LIF容錯移轉至另一個非HA合作夥伴的節點。
節點管理生命里	僅限本機	LIF只會容錯移轉至同一個節點上的連接埠。
SAN 資料生命	已停用	LIF不會容錯移轉至其他連接埠。

「僅限SFO合作夥伴」容錯移轉原則並非預設值、但只有當您希望LIF容錯移轉至主節點或SFO合作夥伴上的連接埠時、才可使用此原則。

相關資訊

- "網路介面顯示"

NAS 路徑容錯移轉工作流程

在 ONTAP 網路上設定 NAS 路徑容錯移轉

如果您已經熟悉基本的網路概念、可以檢閱NAS路徑容錯移轉組態的「實際操作」工作流程、以節省設定網路的時間。

ONTAP 9.7 和舊版中的 NAS 路徑容錯移轉設定工作流程不同。如果您需要在運行 ONTAP 9.7 及更早版本的網絡上配置 NAS 故障切換"NAS 路徑容錯移轉工作流程（ ONTAP 9.7 及更早版本）"，請參閱工作流程。

NAS LIF會在目前連接埠的連結失敗後、自動移轉至正常運作的網路連接埠。您可以仰賴ONTAP 「恢復」預設值來管理路徑容錯移轉。

SAN LIF不會移轉（除非您在連結失敗後手動移動它）。相反地、主機上的多重路徑技術會將流量轉移到不同的LIF。如需詳細資訊、請參閱 "SAN管理"。

1. "填寫工作表單"

請使用工作表規劃 NAS 路徑容錯移轉。

2. "建立IPspaces"

為叢集中的每個 SVM 建立不同的 IP 位址空間。

3. "將廣播網域移至IPspaces"

將廣播網域移至 IPspace 。

4. "建立SVM"

建立 SVM 以將資料提供給用戶端。

5 "建立生命"

在您要用來存取資料的連接埠上建立生命。

6 "設定 SVM 的 DNS 服務"

建立 NFS 或 SMB 伺服器之前，請先設定 SVM 的 DNS 服務。

ONTAP 網路上的 NAS 路徑容錯移轉工作表

在設定NAS路徑容錯移轉之前、您應該先完成工作表的所有區段。

ONTAP 網路上的 NAS 容錯移轉資訊在 ONTAP 9.7 和舊版中有所不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上配置 NAS 故障切換，請"NAS 路徑容錯移轉組態工作表（ ONTAP 9.7 及更早版本）"參閱。

IPSpace組態

您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

資訊	必要？	您的價值
IPSpace名稱 IPspace 的唯一識別碼。	是的	

廣播網域組態

廣播網域會將屬於同一個第2層網路的連接埠分組、並設定廣播網域連接埠的MTU。

廣播網域會指派給IPspace。IPspace可包含一或多個廣播網域。

LIF容錯移轉的連接埠必須是LIF的容錯移轉群組成員。對於ONTAP 由Isname建立的每個廣播網域、也會建立名稱相同的容錯移轉群組、其中包含廣播網域中的所有連接埠。

資訊	必要？	您的價值
IPSpace名稱 指派廣播網域的IPspace。 此IPspace必須存在。	是的	
廣播網域名稱 廣播網域的名稱。 此名稱在IPspace中必須是唯一的。	是的	

MTU 廣播網域的最大傳輸單位值，通常設定為 **1500** 或 **9000** 。 MTU值會套用至廣播網域中的所有連接埠、以及稍後新增至廣播網域的任何連接埠。 MTU值應與連接至該網路的所有裝置相符。請注意、e0M連接埠處理管理和服務處理器流量應將MTU設定為不超過1500位元組。	是的	
連接埠 連接埠會根據連線能力指派給廣播網域。連接埠指派完成後、請執行來檢查連線能力 `network port reachability show` 命令。 這些連接埠可以是實體連接埠、VLAN或介面群組。 如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。	是的	

子網路組態

子網路包含IP位址集區和預設閘道、可指派給IP空間中的SVM所使用的生命區。

- 在SVM上建立LIF時、您可以指定子網路的名稱、而非提供IP位址和子網路。
- 由於子網路可以設定為預設閘道、因此在建立SVM時、您不需要在個別步驟中建立預設閘道。
- 廣播網域可以包含一或多個子網路。
- 您可以將多個子網路與IPspace的廣播網域建立關聯、以設定位於不同子網路上的SVM LIF。
- 每個子網路都必須包含IP位址、而不應與指派給相同IPspace中其他子網路的IP位址重疊。
- 您可以將特定的IP位址指派給SVM資料生命期、並為SVM建立預設閘道、而非使用子網路。

資訊	必要？	您的價值
IPSpace名稱 子網路指派的IPspace。 此IPspace必須存在。	是的	
子網路名稱 子網路名稱。 此名稱在IPspace中必須是唯一的。	是的	

廣播網域名稱 要指派子網路的廣播網域。 此廣播網域必須位於指定的IPspace中。	是的	
子網路名稱和遮罩 IP位址所在的子網路和遮罩。	是的	
閘道 您可以指定子網路的預設閘道。 如果您在建立子網路時未指派閘道、可以稍後指派一個閘道。	否	
IP位址範圍 您可以指定IP位址範圍或特定IP位址。 例如、您可以指定一個範圍、例如： `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` 如果未指定IP位址範圍、則指定子網路中的IP位址範圍將可指派給LIF。	否	
強制更新LIF關聯 指定是否強制更新現有LIF關聯。 根據預設、如果任何服務處理器介面或網路介面使用所提供範圍內的IP位址、則建立子網路會失敗。 使用此參數可將任何手動定址的介面與子網路建立關聯、並允許命令成功執行。	否	

SVM 組態

您可以使用SVM將資料提供給用戶端和主機。

您記錄的值是建立預設資料SVM。如果您要建立MetroCluster 一個SVM的不確定來源、請參閱 "Fabric附加MetroCluster 的《安裝與組態指南》" 或 "延伸MetroCluster 《安裝與組態指南》"。

資訊	必要？	您的價值
SVM名稱 SVM 的完整網域名稱（ FQDN ）。 此名稱必須在各叢集聯盟中都是唯一的名稱。	是的	

根Volume名稱 SVM根Volume的名稱。	是的	
Aggregate名稱 擁有SVM根磁碟區的集合體名稱。 此Aggregate必須存在。	是的	
安全風格 SVM根磁碟區的安全樣式。 可能的值包括* ntf*、* UNIX*和*混合*。	是的	
IPSpace名稱 指派SVM的IPspace。 此IPspace必須存在。	否	
SVM語言設定 SVM及其磁碟區的預設語言。 如果未指定預設語言、預設SVM語言會設為* 。UTF-8*。 SVM語言設定可決定用於顯示SVM中所有NAS磁碟區的檔案名稱和資料的字元集。 您可以在建立SVM之後修改語言。	否	

LIF 組態

SVM透過一或多個網路邏輯介面（LIF）、為用戶端和主機提供資料服務。

資訊	必要？	您的價值
SVM名稱 LIF的SVM名稱。	是的	
LIF 名稱 LIF 的名稱。 您可以為每個節點指派多個資料生命期、而且只要節點有可用的資料連接埠、就可以將生命期指派給叢集中的任何節點。 若要提供備援、您應該為每個子網路建立至少兩個資料生命期、並在不同節點上指派指派指派給特定子網路的生命期為主連接埠。 *重要事項：*如果您將SMB伺服器設定為以SMB代管Hyper-V或SQL Server、以提供不中斷營運的解決方案、則叢集中每個節點上的SVM必須至少有一個資料LIF。	是的	

服務原則 LIF 的服務原則。 服務原則會定義哪些網路服務可以使用LIF。內建的服務和服務原則可用於管理資料和系統SVM上的資料和管理流量。	是的	
允許的傳輸協定 IP 型的生命體不需要允許的通訊協定、請改用服務原則列。 指定在Fibre Channel連接埠上允許的SAN生命體傳輸協定。這些是可以使用該LIF的傳輸協定。在建立LIF之後、無法修改使用LIF的傳輸協定。設定LIF時、您應該指定所有的傳輸協定。	否	
主節點 LIF還原至其主連接埠時、LIF傳回的節點。 您應該記錄每個資料LIF的主節點。	是的	
主連接埠或廣播網域 請選擇下列其中一項： **Port** ：指定邏輯介面在 LIF 還原至其主連接埠時傳回的連接埠。這僅適用於IPspace子網路中的第一個LIF、否則不需要。 廣播網域：指定廣播網域、系統會在LIF還原至其主連接埠時、選取邏輯介面傳回的適當連接埠。	是的	
子網路名稱 要指派給SVM的子網路。 用於建立應用程式伺服器的持續可用SMB連線的所有資料生命期、必須位於相同的子網路上。	是（如果使用子網路）	

DNS 組態

在建立NFS或SMB伺服器之前、您必須在SVM上設定DNS。

資訊	必要？	您的價值
SVM名稱 您要在其中建立NFS或SMB伺服器的SVM名稱。	是的	
DNS網域名稱 執行主機對IP名稱解析時要附加到主機名稱的網域名稱清單。 請先列出本機網域、然後列出最常進行DNS查詢的網域名稱。	是的	

DNS 伺服器的 IP 位址 將為 NFS 或 SMB 伺服器提供名稱解析的 DNS 伺服器 IP 位址清單。 列出的DNS伺服器必須包含所需的服務位置記錄（SRV),才能找到SMB伺服器要加入之網域的Active Directory LDAP伺服器和網域控制器。 「服務」記錄用於將服務名稱對應至提供該服務之伺服器的DNS電腦名稱。如果ONTAP 無法透過本機DNS查詢取得服務位置記錄、則無法建立SMB伺服器。 確保ONTAP 功能完整的Active Directory SRVs記錄、最簡單的方法就是將Active Directory整合的DNS伺服器設定為SVM DNS伺服器。 您可以使用非Active Directory整合的DNS伺服器、前提是DNS管理員已手動將含有Active Directory網域控制器相關資訊的SRV記錄新增至DNS區域。 如需Active Directory整合式SRV記錄的相關資訊、請參閱主題 "Microsoft TechNet上的DNS Active Directory支援運作方式"。	是的	

動態**DNS**組態

您必須先在SVM上設定動態DNS（DDNS）、才能使用動態DNS自動將DNS項目新增至Active Directory整合的DNS伺服器。

系統會為SVM上的每個資料LIF建立DNS記錄。透過在SVM上建立多個資料LIF、您可以在用戶端連線與指派的資料IP位址之間取得負載平衡。DNS負載會以循環配置資源的方式、平衡使用主機名稱對指派IP位址所建立的連線。

資訊	必要？	您的價值
SVM名稱 您要在其中建立NFS或SMB伺服器的SVM。	是的	
是否使用DDNS 指定是否使用DDNS。 SVM上設定的DNS伺服器必須支援DDNS。預設會停用DDNS。	是的	

是否使用安全的DDNS 只有Active Directory整合的DNS才支援安全DDNS。 如果Active Directory整合的DNS只允許安全的DDNS更新、則此參數的值必須為true。 根據預設、安全DDNS會停用。 只有在為SVM建立SMB伺服器或Active Directory帳戶之後、才能啟用安全DDNS。	否	
DNS網域的FQDN DNS網域的FQDN。 您必須使用在SVM上為DNS名稱服務設定的相同網域名稱。	否	

網路連接埠

瞭解 **ONTAP** 網路連接埠組態

連接埠是實體連接埠（NIC）或虛擬化連接埠、例如介面群組或VLAN。

虛擬區域網路（VLAN）和介面群組構成虛擬連接埠。介面群組將多個實體連接埠視為單一連接埠、而VLAN則將實體連接埠細分為多個獨立的邏輯連接埠。

- 實體連接埠：可直接在實體連接埠上設定LIF。
- 介面群組：連接埠Aggregate、包含兩個以上的實體連接埠、做為單一主幹連接埠。介面群組可以是單一模式、多重模式或動態多重模式。
- VLAN：接收和傳送VLAN標記（IEEE 802.1Q標準）流量的邏輯連接埠。VLAN連接埠特性包括連接埠的VLAN ID。基礎實體連接埠或介面群組連接埠被視為VLAN主幹連接埠、且連接的交換器連接埠必須設定為主幹VLAN ID。

  VLAN連接埠的基礎實體連接埠或介面群組連接埠可繼續裝載傳輸區、以傳輸和接收無標記流量。

- 虛擬IP（VIP）連接埠：作為VIP LIF主連接埠的邏輯連接埠。VIP連接埠是由系統自動建立、僅支援有限數量的作業。支援VIP連接埠、從ONTAP 功能表9.5開始。

連接埠命名慣例為_enumberletter：

- 第一個字元說明連接埠類型。
  「E」代表乙太網路。
- 第二個字元表示連接埠介面卡所在的編號插槽。
- 第三個字元表示連接埠在多端口介面卡上的位置。
  「A」表示第一個連接埠、「b」表示第二個連接埠、依此類推。

例如、 `e0b` 表示乙太網路連接埠是節點主機板上的第二個連接埠。

VLAN 必須使用語法命名 `port_name-vlan-id`。

`port_name` 指定實體連接埠或介面群組。

`vlan-id` 指定網路上的 VLAN 識別。例如、 `e1c-80` 為有效的 VLAN 名稱。

設定網路連接埠

結合實體連接埠以建立 **ONTAP** 介面群組

介面群組也稱為「連結集合群組（ LAG ）」、是透過將同一個節點上的兩個或多個實體連接埠合併為單一邏輯連接埠而建立。邏輯連接埠可提供更高的恢復能力、更高的可用度和負載共享。

介面群組類型

儲存系統支援三種類型的介面群組：單一模式、靜態多重模式和動態多重模式。每個介面群組提供不同層級的容錯能力。多重模式介面群組提供負載平衡網路流量的方法。

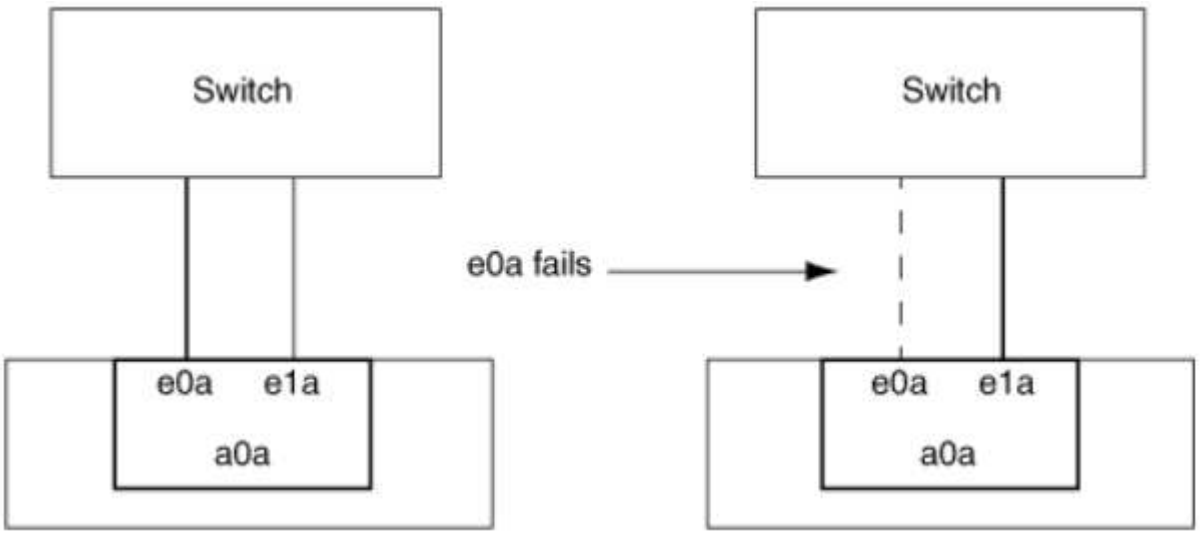
單一模式介面群組的特性

在單一模式介面群組中、介面群組中只有一個介面處於作用中狀態。其他介面處於待命狀態、可在作用中介面故障時接管。

單一模式介面群組的特性：

- 對於容錯移轉、叢集會監控主動式連結並控制容錯移轉。
  由於叢集會監控主動式連結、因此不需要交換器組態。
- 在單一模式介面群組中、待命的介面可以有多個。
- 如果單一模式介面群組橫跨多個交換器、則必須使用交換器間連結（ISL）來連接交換器。
- 對於單一模式介面群組、交換器連接埠必須位於相同的廣播網域中。
- 來源位址為0.00.0的連結監控Arp封包會透過連接埠傳送、以驗證連接埠是否位於同一個廣播網域中。

下圖是單一模式介面群組的範例。在圖中、e0a和e1a是a0a單一模式介面群組的一部分。如果作用中介面e0a故障、待命e1a介面會接管並維持與交換器的連線。



若要完成單一模式功能、建議改用容錯移轉群組。使用容錯移轉群組時、第二個連接埠仍可用於其他生命週期、不需保留未使用的狀態。此外、容錯移轉群組可跨越兩個以上的連接埠、並可跨越多個節點上的連接埠。

靜態多重模式介面群組的特性

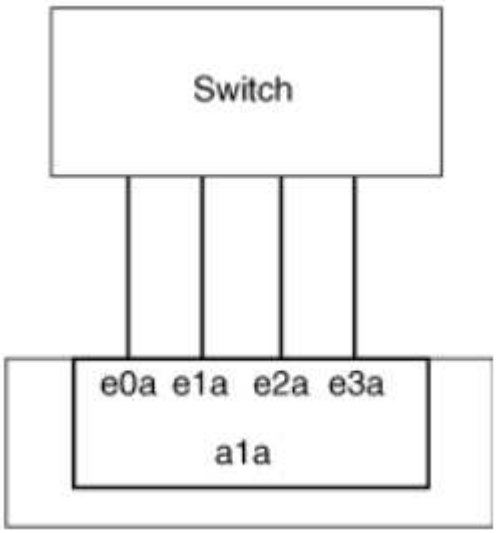
靜態多重模式介面群組實作ONTAP 功能符合IEEE 802.3ad（靜態）。任何支援Aggregate但沒有設定Aggregate的控制封包交換的交換器、都可以搭配靜態多重模式介面群組使用。

靜態多重模式介面群組不符合IEEE 802.3ad（動態）、也稱為「連結集合控制傳輸協定（LACP）」。LACP相當於連接埠集合傳輸協定（PAgP）、這是Cisco專屬的連結集合傳輸協定。

以下是靜態多重模式介面群組的特性：

- 介面群組中的所有介面都處於作用中狀態、並共用一個MAC位址。
  - 介面群組中的介面之間會分散多個個別連線。
  - 每個連線或工作階段都會在介面群組中使用一個介面。
    當您使用循序負載平衡方案時、所有工作階段都會以每個封包為基礎散佈在可用的連結之間、而且不會繫結到介面群組中的特定介面。
- 靜態多重模式介面群組最多可從「n-1」介面故障中恢復、其中n是組成介面群組的介面總數。
- 如果某個連接埠故障或拔除、則會自動將流經故障連結的流量重新分配至其餘的其中一個介面。
- 靜態多重模式介面群組可偵測到連結中斷、但無法偵測到與用戶端或交換器的連線中斷、進而影響連線能力和效能。
- 靜態多重模式介面群組需要支援多個交換器連接埠連結集合的交換器。
  交換器已設定成介面群組連結所連接的所有連接埠都是單一邏輯連接埠的一部分。某些交換器可能不支援設定用於巨型框架的連接埠連結集合。如需詳細資訊、請參閱交換器廠商的文件。
- 有多種負載平衡選項可供在靜態多重模式介面群組的介面之間分配流量。

下圖是靜態多重模式介面群組的範例。介面e0a、e1a、E2A和e3a是A1A多重模式介面群組的一部分。A1A多重模式介面群組中的所有四個介面都處於作用中狀態。



有幾項技術可讓單一集合式連結中的流量分散在多個實體交換器上。啟用此功能的技術因網路產品而異。靜態多

重模式介面群組ONTAP 的功能符合IEEE 802.3標準。如果某種特定的多重交換器連結集合技術據說可與IEEE 802.3標準互通或符合該標準、則應搭配ONTAP 使用。

IEEE 802.3標準指出、彙總連結中的傳輸裝置會決定傳輸的實體介面。因此ONTAP 、只有在分配傳出流量時、才能控制傳入訊框的傳入方式。如果您想要管理或控制集合式連結的傳入流量傳輸、則必須在直接連線的網路裝置上修改該傳輸。

動態多重模式介面群組

動態多重模式介面群組實作連結集合控制傳輸協定（LACP）、將群組成員資格與直接連接的交換器通訊。LACP可讓您偵測失去連結狀態、以及節點無法與直接附加交換器連接埠通訊。

Dynamic多重模式介面群組實作ONTAP 在整個過程中均符合IEEE 802.3 AD（802.1 AX）標準。不支援連接埠集合傳輸協定（PAgP）、這是Cisco專屬的連結集合傳輸協定。ONTAP

動態多重模式介面群組需要支援LACP的交換器。

在不可設定的主動模式中執行LACP、可與設定為主動或被動模式的交換器搭配運作。ONTAP根據IEEE 802.3 AD（802.1AX）的規定、執行長和短LACP定時器（搭配不可設定的值使用3秒和90秒）ONTAP 。

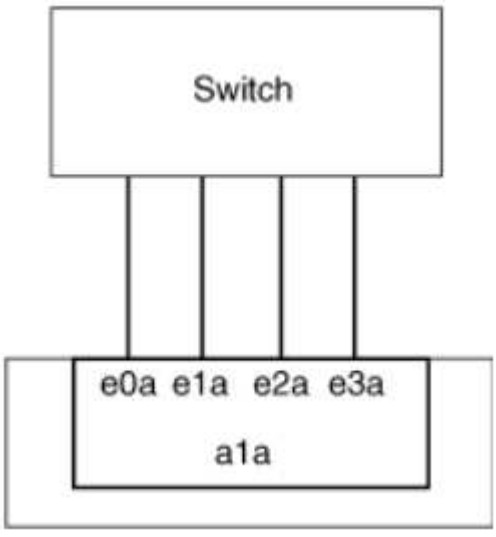
此功能可判斷用於傳輸傳出流量的成員連接埠、但無法控制接收傳入訊框的方式。ONTAP交換器會根據交換器連接埠通道群組中設定的負載平衡演算法、決定其連接埠通道群組的成員（個別實體連接埠）以供傳輸。因此、交換器組態會決定儲存系統的成員連接埠（個別實體連接埠）來接收流量。如需設定交換器的詳細資訊、請參閱交換器廠商的文件。

如果個別介面無法接收連續的LACP傳輸協定封包、則在「ifgrp STATUS」命令的輸出中、該個別介面會標示為「lid_inactive」。現有流量會自動重新路由至任何剩餘的作用中介面。

使用動態多重模式介面群組時、適用下列規則：

- 動態多重模式介面群組應設定為使用連接埠型、IP型、MAC型或循環配置資源負載平衡方法。
- 在動態多重模式介面群組中、所有介面都必須處於作用中狀態、並共用一個MAC位址。

下圖為動態多重模式介面群組的範例。介面e0a、e1a、E2A和e3a是A1A多重模式介面群組的一部分。A1A動態多重模式介面群組中的所有四個介面都處於作用中狀態。



多重模式介面群組中的負載平衡

您可以使用 IP 位址， MAC 位址，循序或連接埠型負載平衡方法，在多重模式介面群組的網路連接埠上平均分配網路流量，確保多重模式介面群組的所有介面都能用於傳出流量。

只有在建立介面群組時、才能指定多重模式介面群組的負載平衡方法。

最佳實務：建議盡可能使用連接埠型負載平衡。除非網路中有特定的原因或限制可防止負載平衡、否則請使用連接埠型負載平衡。

連接埠型負載平衡

建議使用連接埠型負載平衡。

您可以使用連接埠型負載平衡方法、根據傳輸層（TCP/IP）連接埠、將多重模式介面群組上的流量等化。

連接埠型負載平衡方法使用快速雜湊演算法來處理來源和目的地IP位址、以及傳輸層連接埠號碼。

IP位址和**MAC**位址負載平衡

IP位址和MAC位址負載平衡是在多重模式介面群組上平衡流量的方法。

這些負載平衡方法使用快速雜湊演算法來處理來源位址和目的地位址（IP位址和MAC位址）。如果雜湊演算法的結果對應到不在UP連結狀態的介面、則會使用下一個作用中介面。

> 在直接連線至路由器的系統上建立介面群組時、請勿選取MAC位址負載平衡方法。在這樣的設定中、每個傳出IP訊框的目的MAC位址都是路由器的MAC位址。因此、只會使用介面群組的一個介面。

IP位址負載平衡的運作方式與IPv6位址相同。

連續負載平衡

您可以使用循序負載平衡、使用循環配置資源演算法、在多個連結之間平均分配封包。您可以使用連續選項來平衡單一連線在多個連結之間的流量負載、以增加單一連線處理量。

不過、由於連續負載平衡可能導致封包交付順序不正常、因此可能導致效能極差。因此、一般不建議使用循序負載平衡。

建立介面群組或**LAG**

您可以建立介面群組或LAG（單一模式、靜態多重模式或動態多重模式（LACP））、結合彙總網路連接埠的功能、將單一介面呈現給用戶端。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式建立LAG *

步驟

1. 選擇*網路>乙太網路連接埠>+連結集合群組*以建立LAG。
2. 從下拉式清單中選取節點。
3. 請從下列選項中選擇：
   a. 自動選擇廣播網域（建議）。ONTAP
   b. 手動選取廣播網域。
4. 選擇要形成 LAG 的連接埠。
5. 選取模式：
   a. 單一：一次只使用一個連接埠。
   b. 多個：所有連接埠都可以同時使用。
   c. LACP：LACP傳輸協定決定可使用的連接埠。
6. 選擇負載平衡：
   a. IP型
   b. Mac型
   c. 連接埠
   d. 連續的
7. 儲存您的變更。

CLI

使用**CLI**建立介面群組

建立多重模式介面群組時、您可以指定下列任一種負載平衡方法：

- `port`：網路流量是根據傳輸層（ TCP/UDP ）連接埠來分配。這是建議的負載平衡方法。
- `mac`：網路流量是根據 MAC 位址來分配。
- `ip`：網路流量是根據 IP 位址來分配。
- `sequential`：網路流量會在收到時隨之分佈。

> ⓘ 介面群組的MAC位址取決於基礎連接埠的順序、以及這些連接埠在開機期間的初始化方式。因此、您不應假設在重新開機或ONTAP 進行升級時、ifgrp MAC位址會持續存在。

步驟

使用 `network port ifgrp create` 用於建立介面群組的命令。

介面群組必須使用語法命名 `a<number><letter>`。例如、a0a、a0b、a1C和a2a是有效的介面群組名稱。

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

以下範例說明如何建立名為a0a的介面群組、其中包含連接埠的發佈功能和多重模式：

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

將連接埠新增至介面群組或**LAG**

您最多可將16個實體連接埠新增至介面群組或LAG、以獲得所有連接埠速度。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式將連接埠新增至LAG *

步驟

1. 選擇*網路>乙太網路連接埠> LAG*以編輯LAG。
2. 在同一個節點上選取其他連接埠以新增至LAG。
3. 儲存您的變更。

CLI

使用**CLI**將連接埠新增至介面群組

步驟

將網路連接埠新增至介面群組：

```
network port ifgrp add-port
```

下列範例說明如何將連接埠e0c新增至名為a0a的介面群組：

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

從ONTAP 功能更新到功能更新的版本開始、介面群組會在介面群組新增第一個實體連接埠約一分鐘後、自動放入適當的廣播網域。如果您不想讓 ONTAP 這麼做、而偏好手動將 ifgrp 放入廣播網域、請指定 `-skip -broadcast-domain-placement` 參數為的一部分 `ifgrp add-port` 命令。

深入瞭解 `network port ifgrp add-port`和設定中適用於連接埠介面群組"指令參考資料ONTAP"的限制。

從介面群組或**LAG**中移除連接埠

只要連接埠不是介面群組中的最後一個連接埠、您就可以從裝載lifs的介面群組中移除該連接埠。由於您並未從介面群組中移除最後一個連接埠、因此不需要介面群組不可裝載lifs、也不需要介面群組不可是LIF的主連接埠。不過、如果您要移除最後一個連接埠、則必須先移轉或移除介面群組中的LIF。

關於這項工作

您最多可從介面群組或LAG移除16個連接埠（實體介面）。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式從LAG *移除連接埠

步驟

1. 選擇*網路>乙太網路連接埠> LAG*以編輯LAG。
2. 從LAG中選取要移除的連接埠。
3. 儲存您的變更。

CLI

*使用CLI從介面群組*移除連接埠

步驟

從介面群組移除網路連接埠：

```
network port ifgrp remove-port
```

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

下列範例說明如何從名為a0a的介面群組移除連接埠e0c：

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

刪除介面群組或**LAG**

如果要直接在基礎實體連接埠上設定LIF、或決定變更介面群組、LAG模式或發佈功能、您可以刪除介面群組或LAG。

開始之前

- 介面群組或LAG不得裝載LIF。
- 介面群組或LAG不能是LIF的主連接埠或容錯移轉目標。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*使用系統管理程式刪除LAG *

步驟

1. 選擇*網路>乙太網路連接埠> LAG *以刪除LAG。
2. 選取您要移除的 LAG 。
3. 刪除 LAG 。

CLI

使用**CLI**刪除介面群組

步驟

使用 `network port ifgrp delete` 用於刪除介面群組的命令。

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

下列範例說明如何刪除名為a0b的介面群組：

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

透過實體連接埠設定 **ONTAP VLAN**

您可以在 ONTAP 中使用 VLAN 來提供網路的邏輯區段、方法是建立獨立的廣播網域、這些網域是以交換器連接埠為基礎定義、而非以實體邊界定義的傳統廣播網域。

一個VLAN可以跨越多個實體網路區段。屬於VLAN的終端站台會依功能或應用程式而定。

例如、VLAN中的終端站台可能會依部門（例如工程和會計）或專案（例如releasease1和release2）進行分組。由於終端站台的實體鄰近性在VLAN中並不重要、因此您可以將終端站台分散到不同的地理位置、並將廣播網域保留在交換式網路中。

在ONTAP 9.14.1 和 9.13.1 中，未被任何邏輯介面 (LIF) 使用且在所連接的交換器上缺少本機 VLAN 連線的未標記連接埠被標記為已降級。這有助於識別未使用的端口，並不表示中斷。本機 VLAN 允許 ifgrp 基本連接埠上未標記的流量，例如ONTAP CFM 廣播。在交換器上設定本機 VLAN 以防止阻止未標記的流量。

您可以建立、刪除或顯示有關VLAN的資訊來管理VLAN。

> 您不應該在網路介面上建立與交換器原生VLAN相同識別碼的VLAN。例如、如果網路介面e0b位於原生VLAN 10、則不應在該介面上建立VLAN e0b-10。

建立 **VLAN**

您可以使用 System Manager 或建立 VLAN 、以維護同一個網路網域內的個別廣播網域 `network port vlan create` 命令。

開始之前

確認已符合下列要求：

- 部署在網路中的交換器必須符合IEEE 802.1Q標準、或是具有廠商專屬的VLAN實作。
- 若要支援多個VLAN、端點必須靜態設定為屬於一個或多個VLAN。
- VLAN未附加至裝載叢集LIF的連接埠。
- VLAN未連接至指派給叢集IPspace的連接埠。
- VLAN並非在不含成員連接埠的介面群組連接埠上建立。

關於這項工作

建立VLAN會將VLAN附加至叢集中指定節點上的網路連接埠。

當您第一次透過連接埠設定VLAN時、連接埠可能會關閉、導致網路暫時中斷連線。後續新增至相同連接埠的VLAN不會影響連接埠狀態。

> 您不應該在網路介面上建立與交換器原生VLAN相同識別碼的VLAN。例如、如果網路介面e0b位於原生VLAN 10、則不應在該介面上建立VLAN e0b-10。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**建立**VLAN**

從ONTAP 功能更新9.12.0開始、您可以自動選取廣播網域、或從清單中手動選取。之前、廣播網域一律會根據第2層連線功能自動選取。如果您手動選取廣播網域、會出現一則警告訊息、指出手動選取廣播網域可能會導致連線中斷。

步驟

1. 選擇*網路>乙太網路連接埠>+ VLAN*。
2. 從下拉式清單中選取節點。
3. 請從下列選項中選擇：
   a. 自動選擇廣播網域（建議）。ONTAP
   b. 可從列表中手動選擇廣播域。
4. 選取要形成VLAN的連接埠。
5. 指定VLAN ID。
6. 儲存您的變更。

CLI

使用**CLI**建立**VLAN**

在某些情況下、如果您想要在效能降低的連接埠上建立 VLAN 連接埠、而不修正硬體問題或任何軟體組態錯誤、則可以設定 `-ignore-health-status` 的參數 `network port modify` 命令為 `true`。

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

步驟

1. 使用 `network port vlan create` 建立 VLAN 的命令。
2. 您必須指定 `vlan-name` 或 `port` 和 `vlan-id` 建立 VLAN 的選項。
   VLAN名稱是連接埠（或介面群組）名稱與網路交換器VLAN識別碼的組合、中間有連字號。例如、`e0c-24` 和 `e1c-80` 為有效的 VLAN 名稱。

以下範例說明如何建立 VLAN `e1c-80` 已連接至網路連接埠 `e1c` 在節點上 `cluster-1-01`：

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

從ONTAP 功能更新到功能更新的版本開始、VLAN會在建立後約一分鐘自動放入適當的廣播網域。如果您不想讓 ONTAP 這麼做、而偏好手動將 VLAN 放入廣播網域、請指定 `-skip-broadcast-domain-placement` 參數為的一部分 `vlan create` 命令。

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

編輯 VLAN

您可以變更廣播網域或停用VLAN。

使用System Manager編輯VLAN

從ONTAP 功能更新9.12.0開始、您可以自動選取廣播網域、或從清單中手動選取。先前的廣播網域一律會根據第2層連線功能自動選取。如果您手動選取廣播網域、會出現一則警告訊息、指出手動選取廣播網域可能會導致連線中斷。

步驟

1. 選擇*網路>乙太網路連接埠> VLAN*。
2. 選取編輯圖示。
3. 執行下列其中一項：
   - 從清單中選取不同的廣播網域、以變更廣播網域。
   - 清除*已啟用*核取方塊。
4. 儲存您的變更。

刪除 VLAN

從插槽中移除NIC之前、您可能必須先刪除VLAN。當您刪除VLAN時、它會自動從所有使用它的容錯移轉規則和群組中移除。

開始之前

請確定沒有任何與VLAN相關的生命里數。

關於這項工作

從連接埠刪除最後一個VLAN可能會導致網路暫時中斷與連接埠的連線。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**刪除**VLAN**

步驟

1. 選擇*網路>乙太網路連接埠> VLAN*。
2. 選取您要移除的VLAN。
3. 按一下*刪除*。

CLI

使用**CLI**刪除**VLAN**

步驟

使用 `network port vlan delete` 刪除 VLAN 的命令。

以下範例說明如何刪除 VLAN `e1c-80` 從網路連接埠 `e1c` 在節點上 `cluster-1-01`：

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

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

修改 **ONTAP** 網路連接埠屬性

您可以修改實體網路連接埠的自動協商、雙工、流程控制、速度和健全狀況設定。

開始之前

您要修改的連接埠不得裝載任何LIF。

關於這項工作

- 不建議修改100 GbE、40 GbE、10 GbE或1 GbE網路介面的管理設定。

  您為雙工模式和連接埠速度設定的值稱為管理設定。視網路限制而定、管理設定可能會與操作設定有所不同（亦即、雙工模式和連接埠實際使用的速度）。

- 不建議修改介面群組中基礎實體連接埠的管理設定。

  。 `-up-admin` 參數（可在進階權限層級使用）會修改連接埠的管理設定。

- 不建議設定 `-up-admin` 對於節點上的所有連接埠、或是節點上最後一個可運作叢集 LIF 所在的連接埠、系統管理設定為 false 。
- 不建議修改管理連接埠的 MTU 大小、 `e0M`。
- 廣播網域中連接埠的MTU大小無法從為廣播網域設定的MTU值變更。
- VLAN的MTU大小不得超過其基礎連接埠的MTU大小值。

步驟

1. 修改網路連接埠的屬性：

   `network port modify`

2. 您可以設定 `-ignore-health-status` 欄位為 true 、指定系統可以忽略指定連接埠的網路連接埠健全狀況狀態。

   網路連接埠健全狀況狀態會自動從降級變更為健全狀態、而此連接埠現在可用於裝載lifs。您應該將叢集連接埠的流量控制設定為 `none`。依預設、流程控制設定為 `full`。

下列命令會將流程控制項設定為「無」、以停用連接埠e0b上的流程控制：

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

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

轉換 **40GbE NIC** 連接埠，為 **ONTAP** 網路建立 **10GbE** 連接埠

您可以將X1144A-R6和X91440A-R6 40GbE網路介面卡（NIC）轉換成支援四個10GbE連接埠。

如果您要將支援其中一個NIC的硬體平台連接至支援10GbE叢集互連和客戶資料連線的叢集、則必須轉換NIC以提供必要的10GbE連線。

開始之前

您必須使用支援的中斷連接線。

關於這項工作

如需支援NIC的平台完整清單、請參閱 "Hardware Universe"。

> 在X1144A-R6 NIC上、只能轉換連接埠A來支援四個10GbE連線。轉換連接埠A後、連接埠e便無法使用。

步驟

1. 進入維護模式。
2. 將NIC從40GbE支援轉換為10GbE支援。

   ```
   nicadmin convert -m [40G | 10G] [port-name]
   ```

3. 使用convert命令後、停止節點。
4. 安裝或更換纜線。
5. 視硬體機型而定、請使用SP（服務處理器）或BMC（基礎板管理控制器）將節點關機後再開機、以使轉換生效。

為 ONTAP 網路設定 UTA X1143A-R6 連接埠

根據預設， X1143A-R6 統一化目標介面卡是以 FC 目標模式設定，但您可以將其連接埠設定為 10 Gb 乙太網路和 FCoE （ CNA ）連接埠，或設定為 16 Gb FC 啟動器或目標連接埠。這需要不同的SFP+介面卡。

當X1143A-R6介面卡設定為乙太網路和FCoE時、可在相同的10-GbE連接埠上支援並行NIC和FCoE目標流量。如果設定為FC、則可針對FC目標或FC啟動器模式個別設定每個共用相同ASIC的雙埠配對。這表示單一X1143A-R6介面卡可在一個雙埠配對上支援FC目標模式、在另一個雙埠配對上支援FC啟動器模式。 連接至相同ASIC的連接埠配對必須設定為相同模式。

在FC模式中、X1143A-R6介面卡的運作速度就像任何現有的FC裝置一樣、最高可達16 Gbps。在CNA模式中、您可以使用X1143A-R6介面卡來同時處理NIC和FCoE流量、並共用相同的10 GbE連接埠。CNA模式僅支援FC目標模式的FCoE功能。

若要設定統一化目標介面卡（X1143A-R6）、您必須在相同的特性設定模式下、在同一個晶片上設定兩個鄰近的連接埠。

步驟

1. 檢視連接埠組態：

```
system hardware unified-connect show
```

2. 視需要設定光纖通道（ FC ）或融合式網路介面卡（ CNA ）的連接埠：

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. 連接FC或10 Gb乙太網路適用的纜線。
4. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

   對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該使用8 GB SFP或16 GB SFP、視所連接的FC架構而定。

轉換 UTA2 連接埠以用於 ONTAP 網路

您可以將 UTA2 連接埠從融合式網路介面卡（ CNA ）模式轉換為光纖通道（ FC ）模式，反之亦然。

當您需要變更連接埠與其網路的實體媒體，或是支援 FC 啟動器和目標時，您應該將 UTA2 特性設定從 CNA 模式變更為 FC 模式。

從 **CNA** 模式到 **FC** 模式

步驟

1. 使介面卡離線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 變更連接埠模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. 重新啟動節點、然後將介面卡上線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 請通知您的管理員或VIF管理程式、視情況刪除或移除連接埠：
   - 如果連接埠作為LIF的主連接埠、介面群組（ifgrp）或主機VLAN的成員、則管理員應執行下列動作：
     - 移動LIF、從ifgrp移除連接埠、或分別刪除VLAN。
     - 執行命令以手動刪除連接埠 `network port delete`。如果 `network port delete`命令失敗，系統管理員應解決錯誤，然後再次執行命令。
   - 如果連接埠不是LIF的主連接埠、不是ifgrp的成員、也不是主控VLAN、則VIF管理程式應在重新開機時從記錄中移除連接埠。如果 VIF 管理程式未移除連接埠，則管理員必須在重新開機後使用命令手動移除該連接埠 `network port delete`。

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

5. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

   對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該先使用8 GB SFP或16 GB SFP、再變更節點上的組態。

從 **FC** 模式到 **CNA** 模式

步驟

1. 使介面卡離線：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 變更連接埠模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. 重新啟動節點
4. 確認您已安裝正確的 SFP+ 。

   對於CNA、您應該使用10Gb乙太網路SFP。

轉換 **ONTAP** 網路的 **CNA/UTA2** 光學模組

您應該變更統一化目標介面卡（CNA/UTA2）上的光學模組、以支援您為介面卡選取的特性設定模式。

步驟

1. 驗證卡中使用的目前SFP+。接著、將目前的SFP+替換為適當的SFP+、以符合偏好的特性設定（FC或CNA）。
2. 從X1143A-R6介面卡移除目前的光纖模組。
3. 針對您偏好的個人化模式（FC或CNA）光纖插入正確的模組。
4. 確認您已安裝正確的SFP+：

```
network fcp adapter show -instance -node -adapter
```

   支援的SFP+模組和Cisco品牌銅線（雙軸纜線）纜線列於中 "NetApp Hardware Universe"。

從 **ONTAP** 叢集節點移除 **NIC**

您可能必須從插槽中移除故障的NIC、或將NIC移至其他插槽以進行維護。

移除 NIC 的程序與 ONTAP 9.7 和舊版不同。如果需要從運行 ONTAP 9.7 及更早版本的 ONTAP 羣集節點中刪除 NIC ，請參閱過程"從節點移除 NIC （ ONTAP 9.7 或更早版本）"。

步驟

1. 關閉節點電源。
2. 從插槽中實際移除NIC。
3. 開啟節點電源。
4. 確認連接埠已刪除：

```
network port show
```

自動從任何介面群組移除連接埠。ONTAP如果連接埠是介面群組的唯一成員、介面群組就會刪除。如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

5. 如果連接埠上已設定任何VLAN、就會被取代。您可以使用下列命令來檢視已移出的VLAN：

```
cluster controller-replacement network displaced-vlans show
```

。 `displaced-interface show`、 `displaced-vlans show`和 `displaced-vlans restore` 命令是唯一的，不需要以開頭的完整命令名稱 `cluster controller-replacement network`。

6. 這些VLAN會被刪除、但可以使用下列命令還原：

```
displaced-vlans restore
```

7. 如果連接埠上已設定任何LIF、ONTAP 則在同一個廣播網域的另一個連接埠上、會自動為這些LIF選擇新的主連接埠。如果在同一個檔案管理器上找不到合適的主連接埠、則這些生命區會被視為已取代。您可以使用下列命令來檢視已移出的LIF：

```
displaced-interface show
```

8. 將新連接埠新增至同一個節點上的廣播網域時、便會自動還原該LIF的主連接埠。或者、您也可以使用設定主連接埠 `network interface modify -home-port -home-node or use the displaced-interface restore` 命令。

相關資訊

- "叢集控制器更換網路置換介面刪除"
- "修改網路介面"

監控網路連接埠

監控 **ONTAP** 網路連接埠的健全狀況

網路連接埠的支援管理包括自動健全狀況監控和一組健全狀況監控、可協助您識別可能不適合裝載生命設備的網路連接埠。ONTAP

關於這項工作

如果健全狀況監視器判定網路連接埠不健全、它會透過EMS訊息警告系統管理員、或將連接埠標記為降級。如果該LIF有健全的替代容錯移轉目標、則可避免在降級的網路連接埠上裝載LIF。ONTAP連接埠可能會因為軟性故障事件而降級、例如連結跳轉（上下快速跳轉連結）或網路分割：

- 當叢集IPspace中的網路連接埠遇到連結Flapping或失去與廣播網域中其他網路連接埠的第2層（L2）連線能力時、它們會標示為降級。

- 非叢集IPspaces中的網路連接埠遇到連結Flapping時、會標示為降級。

您必須瞭解降級連接埠的下列行為：

- 降級的連接埠無法包含在VLAN或介面群組中。

  如果介面群組的成員連接埠已標示為降級、但介面群組仍標示為健全、則該介面群組可裝載lifs。

- LIF會自動從降級的連接埠移轉至正常的連接埠。
- 在容錯移轉事件期間、降級的連接埠不會被視為容錯移轉目標。如果沒有可用的正常連接埠、則降級的連接埠會根據正常的容錯移轉原則來主機生命期。
- 您無法建立、移轉LIF或將其還原為降級連接埠。

  您可以修改 `ignore-health-status` 將網路連接埠設定為 `true`。然後、您可以在健全的連接埠上裝載LIF。

步驟

1. 登入進階權限模式：

   ```
   set -privilege advanced
   ```

2. 檢查啟用哪些健全狀況監視器來監控網路連接埠健全狀況：

   ```
   network options port-health-monitor show
   ```

   連接埠的健全狀況狀態取決於健全狀況監視器的值。

   下列健全狀況監視器預設ONTAP 可在支援中使用：

   - 連結Flapping健全狀況監視器：監控連結Flapping

     如果連接埠在五分鐘內有一次以上的連結Flapping、則此連接埠會標示為降級。

   - L2可到達性健全狀況監視器：監控同一個廣播網域中設定的所有連接埠是否彼此具有L2可到達性

     此健全狀況監視器會報告所有IPspace中的L2可連線性問題、但只會將叢集IPspace中的連接埠標記為降級。

   - crc監控：監控連接埠上的crc統計資料

     此健全狀況監視器不會將連接埠標記為降級、但會在觀察到極高的CRC故障率時產生EMS訊息。

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

3. 使用啟用或停用 IPspace 的任何健全狀況監視器 `network options port-health-monitor modify` 命令。

   如"指令參考資料ONTAP"需詳細 `network options port-health-monitor modify`資訊，請參閱。

4. 檢視連接埠的詳細健全狀況：

```
network port show -health
```

命令輸出會顯示連接埠的健全狀況狀態、 `ignore health status` 設定、以及連接埠標示為降級的原因清單。

連接埠健全狀況狀態可以是 `healthy` 或 `degraded`。

如果是 `ignore health status` 設定為 `true`、表示連接埠健全狀況狀態已從修改 `degraded` 至 `healthy` 由管理員提供。

如果是 `ignore health status` 設定為 `false`，連接埠健全狀況狀態會由系統自動決定。

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

監控 ONTAP 網路連接埠的連線能力

可到達性監控功能已內建ONTAP 於更新版本的更新版本中。使用此監控功能來識別實體網路拓撲與ONTAP 該功能組態不相符的情況。在某些情況下ONTAP 、無法連線的連接埠可修復。在其他情況下、需要採取其他步驟。

關於這項工作

使用這些命令來驗證、診斷及修復ONTAP 因不符合實體纜線或網路交換器組態的物件組態而產生的網路錯誤組態。

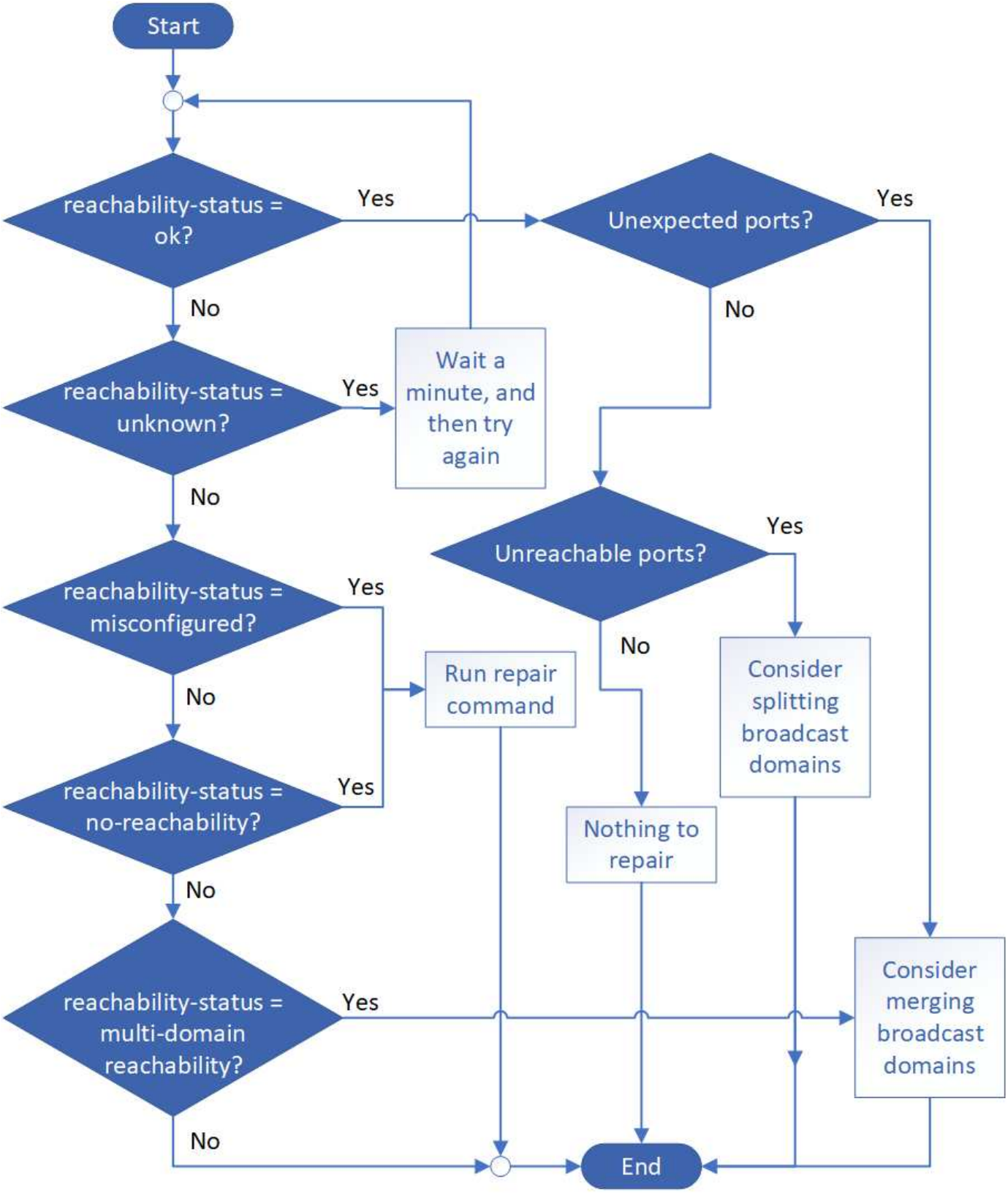
步驟

1. 檢視連接埠連線性：

```
network port reachability show
```

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

2. 請使用下列決策樹狀結構和表格來判斷下一個步驟（如果有）。


Start
reachability-status = ok?
Yes
Unexpected ports?
Yes
No
No
reachability-status = unknown?
Yes
Wait a minute, and then try again
No
Unreachable ports?
Yes
reachability-status = misconfigured?
Yes
No
Run repair command
Consider splitting broadcast domains
No
Nothing to repair
reachability-status = no-reachability?
Yes
No
reachability-status = multi-domain reachability?
Yes
Consider merging broadcast domains
No
End

連線狀態	說明

好的	連接埠可連線至其指派的廣播網域的第2層。 如果連線狀態為「正常」、但有「非預期的連接埠」、請考慮合併一或多個廣播網域。如需詳細資訊、請參閱下列_Unexpected連接埠_資料列。 如果連線狀態為「正常」、但有「無法連線的連接埠」、請考慮分割一或多個廣播網域。如需詳細資訊、請參閱下列_Unreachable連接埠_資料列。 如果連線狀態為「正常」、而且沒有非預期或無法連線的連接埠、表示您的組態正確。
非預期的連接埠	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷其是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
無法連線的連接埠	如果單一廣播網域已分割成兩個不同的連線能力集、您可以分割廣播網域、將ONTAP 此功能與實體網路拓撲進行同步。 一般而言、無法連線的連接埠清單會定義在您確認實體和交換器組態正確之後、應分割成另一個廣播網域的一組連接埠。 如需詳細資訊、請參閱 "分割廣播網域"。
設定錯誤的連線能力	連接埠無法連線至其指派的廣播網域的第2層；不過連接埠確實可連線至不同的廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給可連線的廣播網域： `network port reachability repair -node -port` 如需詳細資訊、請參閱 "修復連接埠連線能力"。
不可到達性	連接埠無法連線至任何現有廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給預設IPspace中自動建立的新廣播網域： `network port reachability repair -node -port`如需更多資訊"修復連接埠連線能力"，請參閱。如"指令參考資料ONTAP"需詳細 `network port reachability repair`資訊，請參閱。
多網域連線能力	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷其是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域" 或 "修復連接埠連線能力"。

不明	如果連線狀態為「未知」、請稍候幾分鐘、然後再試一次命令。

修復連接埠之後、您需要檢查並解決已移轉的LIF和VLAN。如果連接埠是介面群組的一部分、您也需要瞭解該介面群組發生了什麼事。如需詳細資訊、請參閱 "修復連接埠連線能力"。

瞭解 **ONTAP** 網路上的連接埠使用情形

有幾個知名連接埠是專為 ONTAP 與特定服務的通訊所保留。如果儲存網路環境中的連接埠值與 ONTAP 連接埠上的值相同，就會發生連接埠衝突。

傳入流量

ONTAP 儲存設備上的傳入流量使用下列通訊協定和連接埠：

傳輸協定	連接埠	目的
所有 ICMP	全部	Ping 執行個體
TCP	22	安全 Shell 存取叢集管理 LIF 或節點管理 LIF 的 IP 位址
TCP	80	網頁存取叢集管理 LIF 的 IP 位址
TCP/UDP	111.	rpcbind ，遠端程序呼叫 NFS
UDP	123.	NTP ，網路時間傳輸協定
TCP	135.	MSRPC ， Microsoft 遠端程序呼叫
TCP	139.	NetBIOS-SSN ，適用於 CIFS 的 NetBios 服務工作階段
TCP/UDP	161-162	SNMP ，簡易網路管理傳輸協定
TCP	443.	安全的網頁存取叢集管理 LIF 的 IP 位址
TCP	445.	MS Active Domain Services ， Microsoft SMB/CIFS over TCP 搭配 NetBIOS 架構
TCP/UDP	635	NFS 裝載可與遠端檔案系統互動，就像是本機檔案系統一樣
TCP	749.	Kerberos
UDP	953.	名稱精靈
TCP/UDP	2049.	NFS 伺服器精靈
TCP	2050.	NRV ， NetApp 遠端 Volume 傳輸協定
TCP	3260	透過 iSCSI 資料 LIF 存取 iSCSI
TCP/UDP	4045	NFS 鎖定精靈
TCP/UDP	4046	NFS 的網路狀態監控
UDP	4049	NFS RPC Rquotad
UDP	4444.	KRB524 ， Kerberos 524

UDP	5353.	多點傳送DNS
TCP	10000.	使用網路資料管理傳輸協定（ NDMP ）進行備份
TCP	11104.	叢集對等，雙向管理 SnapMirror 的叢集間通訊工作階段
TCP	11105.	叢集對等，雙向 SnapMirror 資料傳輸，使用叢集間的生命週期
SSL/TLS	30000	透過安全通訊端 (SSL/TLS) 接受 DMA 和 NDMP 伺服器之間的 NDMP 安全控制連線。安全掃描器可以報告連接埠 30000 上的漏洞。

傳出流量

您可以根據業務需求，使用基本或進階規則來設定 ONTAP 儲存設備上的輸出流量。

基本傳出規則

所有連接埠都可用於透過 ICMP ， TCP 和 UDP 傳輸協定的所有輸出流量。

傳輸協定	連接埠	目的
所有 ICMP	全部	所有傳出流量
所有 TCP	全部	所有傳出流量
所有的 udp	全部	所有傳出流量

進階傳出規則

如果您需要嚴格的輸出流量規則，可以使用下列資訊，只開啟 ONTAP 輸出通訊所需的連接埠。

Active Directory

傳輸協定	連接埠	來源	目的地	目的
TCP	88.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ， iSCSI ）	Active Directory 樹系	Kerberos V 驗證
UDP	137.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 名稱服務
UDP	138.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 資料報服務
TCP	139.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	NetBios 服務工作階段
TCP	389.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	LDAP
UDP	389.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	LDAP
TCP	445.	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	Microsoft SMB/CIFS over TCP 搭配 NetBios 架構

TCP	464	節點管理 LIF ，資料 LIF （ NFS ， CIFS ）	Active Directory 樹系	變更並設定 Kerberos V 密碼（ set_change ）
UDP	464	節點管理 LIF ， Data LIF （ NFS ， CIFS ）	Active Directory 樹系	Kerberos 金鑰管理
TCP	749.	節點管理 LIF ， Data LIF （ NFS ， CIFS ）	Active Directory 樹系	變更並設定 Kerberos V 密碼（ RPCSEC_GSS ）

AutoSupport

傳輸協定	連接埠	來源	目的地	目的
TCP	80	節點管理 LIF	support.netapp.com	僅當傳輸傳輸傳輸傳輸傳輸傳輸協定從HTTPS變更為HTTP時、AutoSupport

SNMP

傳輸協定	連接埠	來源	目的地	目的
TCP/UDP	162.	節點管理 LIF	監控伺服器	透過 SNMP 設陷進行監控

SnapMirror

傳輸協定	連接埠	來源	目的地	目的
TCP	11104.	叢集間 LIF	叢集間 LIF ONTAP	管理 SnapMirror 的叢集間通訊工作階段

其他服務

傳輸協定	連接埠	來源	目的地	目的
TCP	25.	節點管理 LIF	郵件伺服器	可以使用 SMTP 警示 AutoSupport 來執行功能
UDP	53.	節點管理 LIF 與資料 LIF （ NFS 、 CIFS ）	DNS	DNS
UDP	67.	節點管理 LIF	DHCP	DHCP伺服器
UDP	68.	節點管理 LIF	DHCP	第一次設定的 DHCP 用戶端
UDP	514	節點管理 LIF	系統記錄伺服器	系統記錄轉送訊息
TCP	5010.	叢集間 LIF	備份端點或還原端點	備份與還原備份至 S3 功能的作業
TCP	18600 至 18699	節點管理 LIF	目的地伺服器	NDMP 複本

瞭解 **ONTAP** 內部連接埠

下表列出了 ONTAP 內部使用的連接埠及其功能。 ONTAP使用這些連接埠執行各種功能，

例如建立叢集內 LIF 通訊。

此列表並不詳盡，並且可能在不同環境中有所不同。

連接埠/傳輸協定	組件/功能
514	系統記錄
900	NetApp叢集RPC
902.	NetApp叢集RPC
904	NetApp叢集RPC
905)	NetApp叢集RPC
910	NetApp叢集RPC
911	NetApp叢集RPC
913	NetApp叢集RPC
914	NetApp叢集RPC
159.15	NetApp叢集RPC
918	NetApp叢集RPC
920	NetApp叢集RPC
921.	NetApp叢集RPC
924	NetApp叢集RPC
925	NetApp叢集RPC
927	NetApp叢集RPC
928	NetApp叢集RPC
929	NetApp叢集RPC
930	核心服務與管理功能（KSMF）
931	NetApp叢集RPC
932.	NetApp叢集RPC
933	NetApp叢集RPC
934	NetApp叢集RPC
935	NetApp叢集RPC
936.	NetApp叢集RPC
937	NetApp叢集RPC
939	NetApp叢集RPC
940	NetApp叢集RPC
951.	NetApp叢集RPC
954	NetApp叢集RPC

95	NetApp叢集RPC
956.	NetApp叢集RPC
958	NetApp叢集RPC
961.	NetApp叢集RPC
963,	NetApp叢集RPC
969.64	NetApp叢集RPC
9666	NetApp叢集RPC
967	NetApp叢集RPC
975	金鑰管理互通性傳輸協定（KMIP）
982.	NetApp叢集RPC
983.	NetApp叢集RPC
5125.	磁碟的備用控制連接埠
5133	磁碟的備用控制連接埠
51444.	磁碟的備用控制連接埠
65502	節點範圍SSH
65503	LIF共用
7700	叢集會話管理器 (CSM)
7810.	NetApp叢集RPC
7811.	NetApp叢集RPC
7812.	NetApp叢集RPC
7813.	NetApp叢集RPC
7814	NetApp叢集RPC
（—	NetApp叢集RPC
7816	NetApp叢集RPC
7817.	NetApp叢集RPC
7818.	NetApp叢集RPC
7819	NetApp叢集RPC
7820	NetApp叢集RPC
7821	NetApp叢集RPC
7822.	NetApp叢集RPC
7823	NetApp叢集RPC
7824	NetApp叢集RPC
7835-7839 及 7845-7849	用於集群內通訊的 TCP 連接埠
8023.	節點範圍Telnet

8443	適用於 Amazon FSx 的 ONTAP S3 NAS 連接埠
8514.	節點範圍RSH
9877	KMIP用戶端連接埠（僅限內部本機主機）
10006	用於 HA 互連通訊的 TCP 連接埠

IPspaces

瞭解 **ONTAP IPspace** 組態

IPspaces可讓您設定單ONTAP 一的支援叢集、讓用戶端從多個管理性獨立的網路網域存取、即使這些用戶端使用相同的IP位址子網路範圍也一樣。如此可將用戶端流量區隔、以確保隱私與安全。

IPspace可定義儲存虛擬機器（SVM）所在的獨特IP位址空間。為IPspace定義的連接埠和IP位址僅適用於該IPspace。IPspace內的每個SVM都會有一個不同的路由表、因此不會發生跨SVM或跨IPspace流量路由傳送。

IPspace可在其路由網域上同時支援IPv6位址。

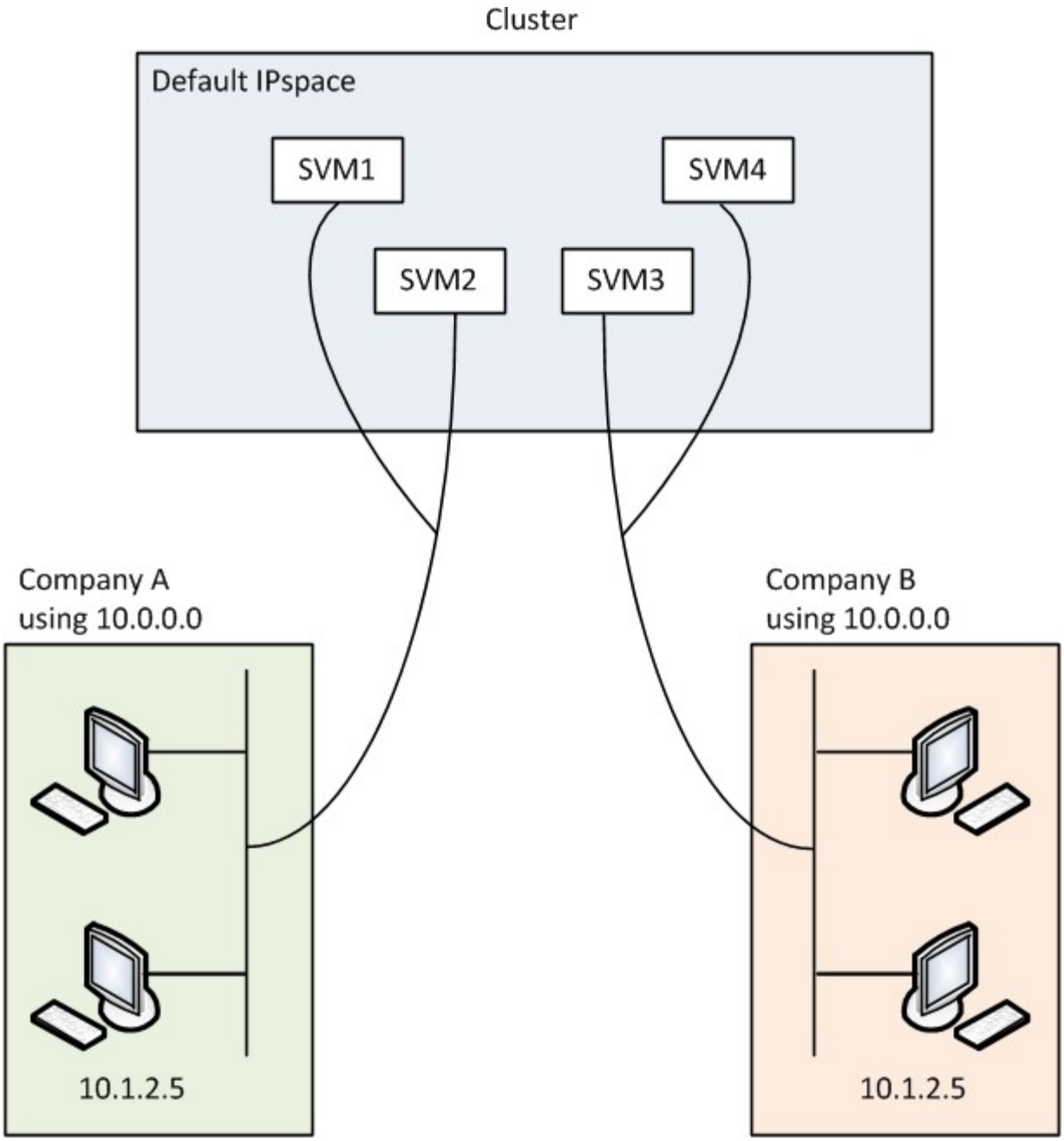
如果您要管理單一組織的儲存設備、則不需要設定IPspaces。如果您要在單ONTAP 一的一套叢集上管理多家公司的儲存設備、而且您確定您的客戶都沒有衝突的網路組態、那麼您也不需要使用IPspaces。在許多情況下、使用儲存虛擬機器（SVM）及其各自獨特的IP路由表、可用來分隔獨特的網路組態、而非使用IPspace。

使用**IPspaces**的範例

使用IPspaces的常見應用程式、是儲存服務供應商（SSP）需要將公司A和B的客戶連接ONTAP 到SSP內部部署上的一個支援叢集、而兩家公司都使用相同的私有IP位址範圍。

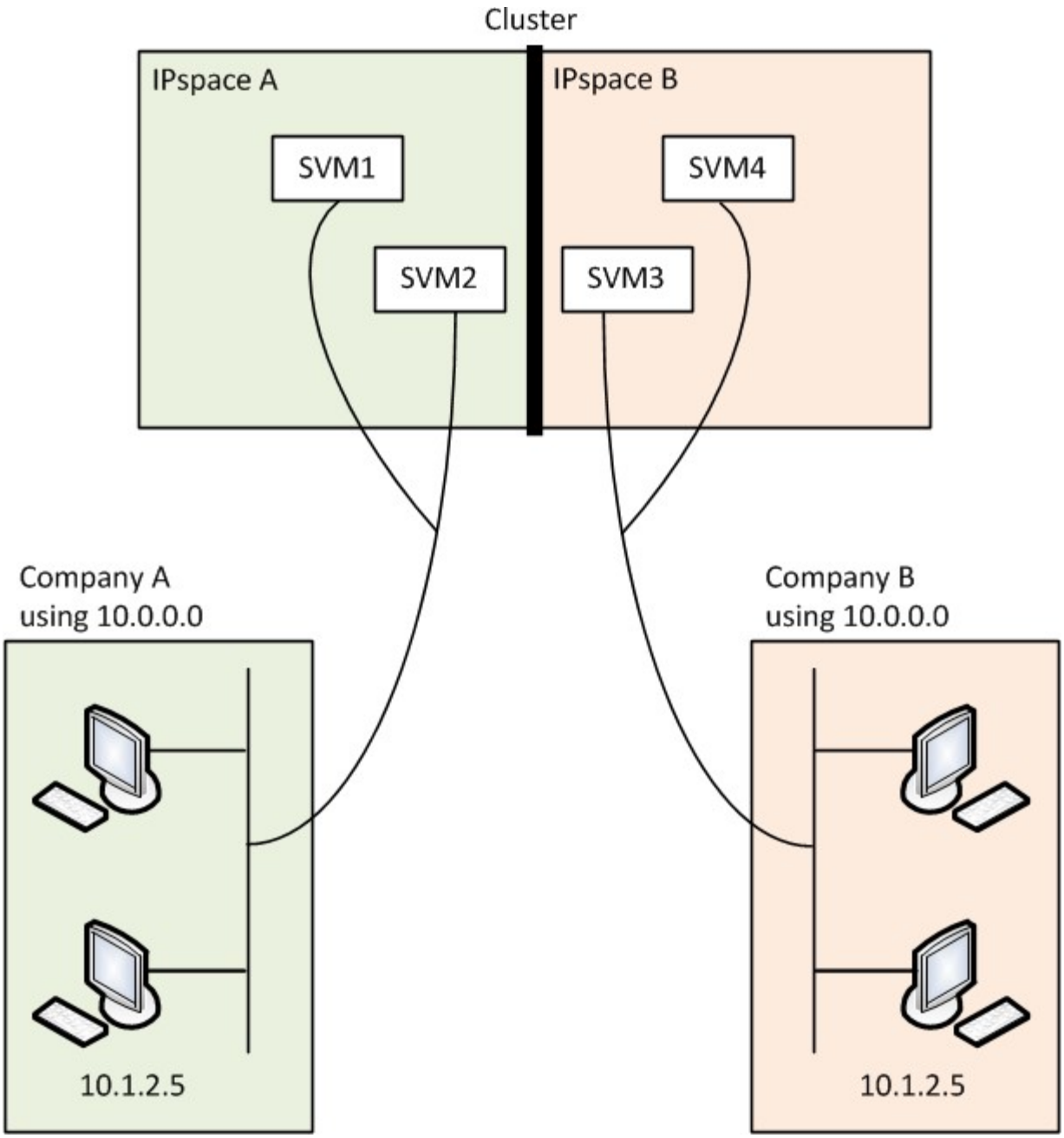
SSP會在叢集上為每位客戶建立SVM、並提供從兩個SVM到公司A網路的專用網路路徑、以及從其他兩個SVM到公司B網路的專用網路路徑。

下圖顯示這種部署類型、如果兩家公司都使用非私有IP位址範圍、就能正常運作。不過、圖例顯示兩家公司使用相同的私有IP位址範圍、這會造成問題。



兩家公司都使用私有IP位址子網路10.0.0.0、造成下列問題：

- 如果兩家公司決定為其各自的SVM使用相同的IP位址、則位於SSP位置之叢集中的SVM會有衝突的IP位址。
- 即使兩家公司同意使用不同的IP位址來處理SVM、也可能發生問題。
- 例如，如果網路中的任何用戶端與B網路中的用戶端具有相同的IP位址，則發往A位址空間中用戶端的封包可能會路由傳送到B位址空間中的用戶端，反之亦然。
- 如果兩家公司決定使用互不相容的位址空間（例如、A使用10.0.0.0、網路遮罩為255.128.0.0、B使用10.128.0.0、網路遮罩為255.128.8.0）、 SSP需要在叢集上設定靜態路由、以便將流量適當路由傳送到A和B的網路。
- 此解決方案既不可擴充（因為靜態路由）、也不安全（廣播流量會傳送至叢集的所有介面）。為了克服這些問題、SSP會在叢集上定義兩個IPspace、每個公司一個。由於不路由跨IP空間的流量、因此即使所有SVM都設定在10.0.0.0位址空間中、每家公司的資料仍會安全地路由至其各自的網路、如下圖所示：



此外、各種組態檔案（例如）所參照的 IP 位址 `/etc/ hosts` 檔案 `/etc/hosts.equiv` 檔案、和 `the /etc/rc` 檔案、與該 IPspace 相關。因此、IPspaces可讓SSP針對多個SVM的組態和驗證資料、設定相同的IP位址、而不會發生衝突。

IPspaces的標準屬性

首次建立叢集時、預設會建立特殊的IPspaces。此外、還會針對每個IPspace建立特殊的儲存虛擬機器（SVM）。

初始化叢集時會自動建立兩個IPspace：

- 「預設」IPspace

  此IPspace是連接埠、子網路和SVM的容器、用於提供資料。如果您的組態不需要用戶端個別的IPspace、則可在此IPspace中建立所有SVM。此IPspace也包含叢集管理和節點管理連接埠。

- 「叢集」IPspace

  此IPspace包含叢集中所有節點的所有叢集連接埠。它會在建立叢集時自動建立。可連線至內部私有叢集網路。當其他節點加入叢集時、這些節點的叢集連接埠會新增至「叢集」IPspace。

每個IPspace都有一個「系統」SVM。當您建立IPspace時、會建立名稱相同的預設系統SVM：

- 「叢集」IPspace的系統SVM會在內部私有叢集網路上的叢集節點之間傳輸叢集流量。

  它由叢集管理員管理、名稱為「叢集」。

- 「預設」IPspace的系統SVM會傳輸叢集和節點的管理流量、包括叢集之間的叢集間流量。

  它由叢集管理員管理、使用與叢集相同的名稱。

- 您所建立的自訂IPspace系統SVM會承載該SVM的管理流量。

  它由叢集管理員管理、使用與IPspace相同的名稱。

一個IPspace中可以存在一個或多個用於用戶端的SVM。每個用戶端SVM都有自己的資料磁碟區和組態、並獨立管理其他SVM。

為 ONTAP 網路建立 IPspace

IPspaces是儲存虛擬機器（SVM）所在的不同IP位址空間。當您需要SVM擁有自己的安全儲存、管理和路由時、可以建立IPspaces。您可以使用IPspace為叢集中的每個SVM建立不同的IP位址空間。這樣做可讓管理性分隔網路網域中的用戶端存取叢集資料、同時使用相同IP位址子網路範圍中重疊的IP位址。

關於這項工作

整個叢集的IP空間上限為512個。對於包含具有 6 GB RAM 的節點的叢集、叢集範圍限制會減至 256 個 IPspace。請參閱Hardware Universe 《參考資訊（英文）：判斷您的平台是否有其他限制。

"NetApp Hardware Universe"

IPspace名稱不能為「ALL」、因為「ALL」是系統保留的名稱。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立IPspace：

   ```
   network ipspace create -ipspace ipspace_name
   ```

   `ipspace_name` 為您要建立的 IPspace 名稱。下列命令會在叢集上建立IPspace ipspace1：

```
network ipspace create -ipspace ipspace1
```

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

2. 顯示 IPspaces ：

   `network ipspace show`

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ----------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

IPspace隨系統SVM一起建立、用於IPspace。系統SVM可傳輸管理流量。

完成後

如果您在MetroCluster 具有不含任何組態的叢集中建立IPspace、則必須手動將IPspace物件複寫到合作夥伴叢集。在IPspace複寫之前建立並指派給IPspace的任何SVM、將不會複寫到合作夥伴叢集。

廣播網域會自動在「預設」IPspace中建立、並可使用下列命令在IPspaces之間移動：

```
network port broadcast-domain move
```

例如、如果您想要使用下列命令、將廣播網域從「預設」移至「ips1」：

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

檢視 **ONTAP** 網路上的 **IPspace**

您可以顯示叢集中存在的IPspaces清單、也可以檢視指派給每個IPspace的儲存虛擬機器（SVM）、廣播網域和連接埠。

步驟

顯示叢集中的IPspaces和SVM：

```
network ipspace show [-ipspace ipspace_name]
```

下列命令會顯示叢集中的所有IPspaces、SVM和廣播網域：

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  -----------------------  ------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

下列命令會顯示屬於IPspace ipspace1的節點和連接埠：

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

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

從 **ONTAP** 網路刪除 **IPspace**

如果不再需要IPspace、您可以將其刪除。

開始之前

不得有廣播網域、網路介面或SVM與您要刪除的IPspace相關聯。

系統定義的「預設」和「叢集」IPspaces無法刪除。

步驟

刪除IPspace：

```
network ipspace delete -ipspace ipspace_name
```

下列命令會從叢集刪除IPspace ipspace1：

```
network ipspace delete -ipspace ipspace1
```

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

廣播網域

瞭解 ONTAP 廣播網域

廣播網域的目的是將屬於同一層網路的網路連接埠分組。然後、儲存虛擬機器（SVM）便可使用群組中的連接埠來處理資料或管理流量。

ONTAP 9.7 和舊版中的廣播網域管理方式有所不同。如果您需要在運行 ONTAP 9.7 及更早版本的網絡上管理廣播域，請"廣播網域總覽（ ONTAP 9.7 及更早版本）"參閱。

廣播網域位於IPspace中。在叢集初始化期間、系統會建立兩個預設廣播網域：

- 「預設」廣播網域包含「預設」IPspace中的連接埠。

  這些連接埠主要用於提供資料。叢集管理和節點管理連接埠也位於此廣播網域中。

- 「叢集」廣播網域包含「叢集」IPspace中的連接埠。

  這些連接埠用於叢集通訊、並包含叢集中所有節點的所有叢集連接埠。

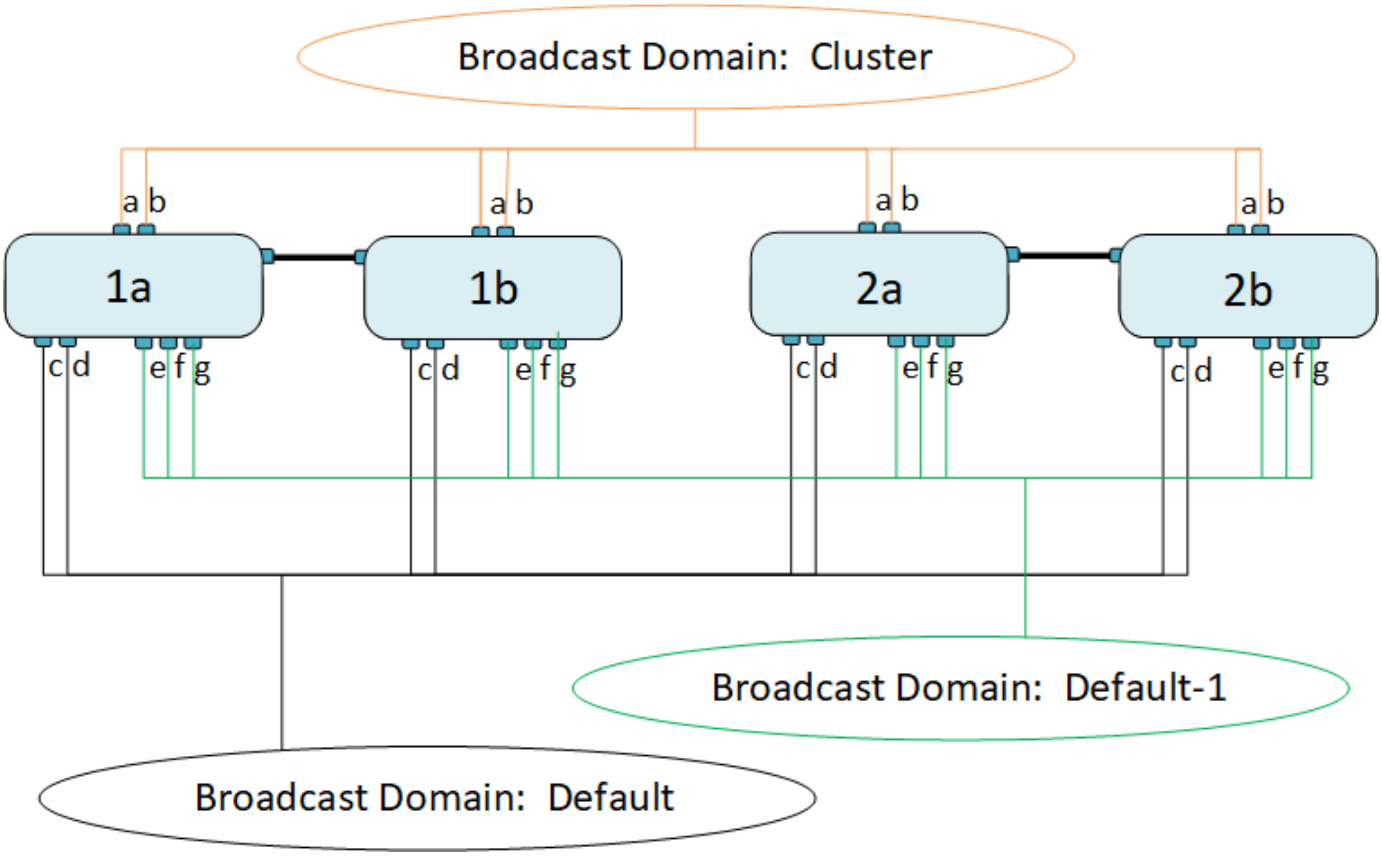
  必要時、系統會在預設IPspace中建立額外的廣播網域。「預設」廣播網域包含管理LIF的主連接埠、以及任何其他連接埠具有該連接埠第2層可連線性的連接埠。其他廣播網域的名稱為「預設值-1」、「預設值-2」等。

使用廣播網域的範例

廣播網域是同一個IPspace中的一組網路連接埠、也能彼此連接第2層、通常包括叢集中許多節點的連接埠。

下圖顯示指派給四節點叢集中三個廣播網域的連接埠：

- 叢集初始化期間會自動建立「叢集」廣播網域、其中包含叢集中每個節點的連接埠a和b。
- 叢集初始化期間也會自動建立「預設」廣播網域、其中包含叢集中每個節點的連接埠c和d。
- 系統會根據第2層網路連線能力、在叢集初始化期間自動建立任何其他廣播網域。這些額外的廣播網域命名為「預設-1」、「預設-2」等。



系統會自動建立名稱相同且與每個廣播網域具有相同網路連接埠的容錯移轉群組。此容錯移轉群組是由系統自動管理、也就是說、當連接埠從廣播網域新增或移除時、它們會自動從這個容錯移轉群組中新增或移除。

建立 ONTAP 廣播網域

廣播網域會將叢集中屬於同一個第2層網路的網路連接埠分組。然後、SVM便可使用這些連接埠。

廣播網域會在叢集建立或加入作業期間自動建立。從ONTAP 功能更新9.12.0開始、除了自動建立的廣播網域之外、您也可以在System Manager中手動新增廣播網域。

建立廣播網域的程序與 ONTAP 9.7 和舊版不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上創建廣播域，請"建立廣播網域（ ONTAP 9.7 及更早版本）"參閱。

開始之前

您打算新增至廣播網域的連接埠不得屬於其他廣播網域。如果您要使用的連接埠屬於另一個廣播網域、但未使用、請從原始廣播網域移除這些連接埠。

關於這項工作

- 所有廣播網域名稱在IPspace內必須是唯一的。
- 新增至廣播網域的連接埠可以是實體網路連接埠、VLAN或連結集合群組/介面群組（LAG / ifgrps）。
- 如果您要使用的連接埠屬於另一個廣播網域、但未使用、請先將它們從現有的廣播網域中移除、再將它們新增至新的廣播網域。
- 新增至廣播網域之連接埠的最大傳輸單元（MTU）會更新為廣播網域中設定的MTU值。

- MTU值必須符合連接至該層2網路的所有裝置、但e0M連接埠處理管理流量除外。
- 如果您未指定IPspace名稱、則會在「預設」IPspace中建立廣播網域。

為了簡化系統組態、系統會自動建立同名的容錯移轉群組、其中包含相同的連接埠。

系統管理員

步驟

1. 選擇*網路>總覽>廣播網域*。
2. 按一下 + Add
3. 命名廣播網域。
4. 設定MTU。
5. 選取IPspace。
6. 儲存廣播網域。

您可以在新增廣播網域之後編輯或刪除該網域。

CLI

如果您使用的是 ONTAP 9.8 及更新版本、則會根據第 2 層的連線能力、自動建立廣播網域。如需詳細資訊、請參閱 "修復連接埠連線能力"。

您也可以手動建立廣播網域。

步驟

1. 檢視目前未指派給廣播網域的連接埠：

   ```
   network port show
   ```

   如果顯示器很大、請使用 `network port show -broadcast-domain` 僅檢視未指派連接埠的命令。

2. 建立廣播網域：

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` 是您要建立的廣播網域名稱。

   b. `mtu_value` 為 IP 封包的 MTU 大小； 1500 和 9000 為典型值。

      此值會套用至新增至此廣播網域的所有連接埠。

   c. `ipspace_name` 是要新增此廣播網域的 IPspace 名稱。

      除非您指定此參數的值、否則會使用「預設」IPspace。

   d. `ports_list` 是要新增至廣播網域的連接埠清單。

      連接埠會以格式新增 `node_name:port_number`例如、 `node1:e0c`。

3. 確認已視需要建立廣播網域：

   ```
   network port show -instance -broadcast-domain new_domain
   ```

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

範例

下列命令會在預設IPspace中建立廣播網域bcast1、將MTU設為1500、並新增四個連接埠：

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain create`資訊，請參閱。

完成後

您可以透過建立子網路來定義廣播網域中可用的IP位址集區、或是現在可以將SVM和介面指派給IPspace。如需更多資訊、請參閱 "叢集與SVM對等關係"。

如果您需要變更現有廣播網域的名稱、請使用 `network port broadcast-domain rename` 命令。

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain rename`資訊，請參閱。

從 ONTAP 廣播網域新增或移除連接埠

廣播網域會在叢集建立或加入作業期間自動建立。您不需要從廣播網域手動移除連接埠。

如果網路連接埠連線能力已變更、無論是透過實體網路連線或交換器組態、而且網路連接埠屬於不同的廣播網域、請參閱下列主題：

"修復連接埠連線能力"

新增或移除廣播網域連接埠的程序與 ONTAP 9.7 和舊版不同。如果您需要在執行 ONTAP 9.7 及更早版本的網路上，從廣播網域新增或移除連接埠"從廣播網域新增或移除連接埠（ ONTAP 9.7 及更早版本）"，請參閱。

系統管理員

從 ONTAP 9.14.1 開始、您可以使用系統管理員在廣播網域之間重新指派乙太網路連接埠。建議您將每個乙太網路連接埠指派給廣播網域。因此、如果您從廣播網域取消指派乙太網路連接埠、則必須將其重新指派給不同的廣播網域。

步驟

若要重新指派乙太網路連接埠、請執行下列步驟：

1. 選擇 * 網路 > 總覽 * 。
2. 在 * 廣播網域 * 區段中、選取 ⋮ 網域名稱旁的。
3. 在下拉式功能表中、選取*編輯*。
4. 在 * 編輯廣播網域 * 頁面上、取消選取您要重新指派給其他網域的乙太網路連接埠。
5. 對於每個取消選取的連接埠、會顯示 * 重新指派乙太網路連接埠 * 視窗。選取您要重新指派連接埠的廣播網域，然後選取 * 重新指派 * 。
6. 選取您要指派給目前廣播網域的所有連接埠、然後儲存變更。

CLI

如果網路連接埠連線能力已變更、無論是透過實體網路連線或交換器組態、而且網路連接埠屬於不同的廣播網域、請參閱下列主題：

"修復連接埠連線能力"

或者、您也可以使用手動新增或移除廣播網域的連接埠 `network port broadcast-domain add-ports` 或 `network port broadcast-domain remove-ports` 命令。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您打算新增至廣播網域的連接埠不得屬於其他廣播網域。
- 已屬於介面群組的連接埠無法個別新增至廣播網域。

關於這項工作

新增和移除網路連接埠時、適用下列規則：

新增連接埠時…	移除連接埠時…
連接埠可以是網路連接埠、VLAN或介面群組（ifgrps）。	不適用
這些連接埠會新增至廣播網域的系統定義容錯移轉群組。	這些連接埠會從廣播網域中的所有容錯移轉群組中移除。
連接埠的MTU會更新為廣播網域中設定的MTU值。	連接埠的MTU不變。
連接埠的IPspace會更新為廣播網域的IPspace值。	這些連接埠會移至「預設」IPspace、且不含廣播網域屬性。

如果使用命令移除介面群組的最後一個成員連接埠 `network port ifgrp remove-port`，則會導致介面群組連接埠從廣播網域中移除，因為廣播網域中不允許使用空的介面群組連接埠。如"指令參考資料ONTAP"需詳細 `network port ifgrp remove-port`資訊，請參閱。

步驟

1. 使用顯示目前指派或未指派給廣播網域的連接埠 `network port show` 命令。
2. 從廣播網域新增或移除網路連接埠：

如果您想要…	使用…
新增連接埠至廣播網域	`network port broadcast-domain add-ports`
從廣播網域移除連接埠	`network port broadcast-domain remove-ports`

3. 確認已從廣播網域新增或移除連接埠：

   `network port show`

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

新增和移除連接埠的範例

下列命令會將節點叢集上的連接埠e0g與節點叢集上的連接埠e0g新增至預設IPspace中的廣播網域bcast1：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

下列命令會在叢集IPspace中新增兩個叢集連接埠以廣播網域叢集：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

下列命令會從預設IPspace的廣播網域bcast1中移除節點叢集1上的連接埠e0e：

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

如"指令參考資料ONTAP"需詳細 `network port broadcast-domain remove-ports`資訊，請參閱。

相關資訊

- "指令參考資料ONTAP"

修復 ONTAP 連接埠連線能力

系統會自動建立廣播網域。但是、如果連接埠已重新標記、或交換器組態變更、則可能需要將連接埠修復至不同的廣播網域（新的或現有的）。

根據廣播網域成員（乙太網路連接埠）的第2層連通性、可自動偵測並建議網路線路問題的解決方案。ONTAP

錯誤的佈線可能會導致非預期的廣播網域連接埠指派。從ONTAP 版本號《21：1：2》（《2：2：2）開始、叢集會在叢集設定後或新節點加入現有叢集時、透過驗證連接埠可連線性、自動檢查網路配線問題。

系統管理員

如果偵測到連接埠連線性問題、System Manager會建議您執行修復作業來解決問題。

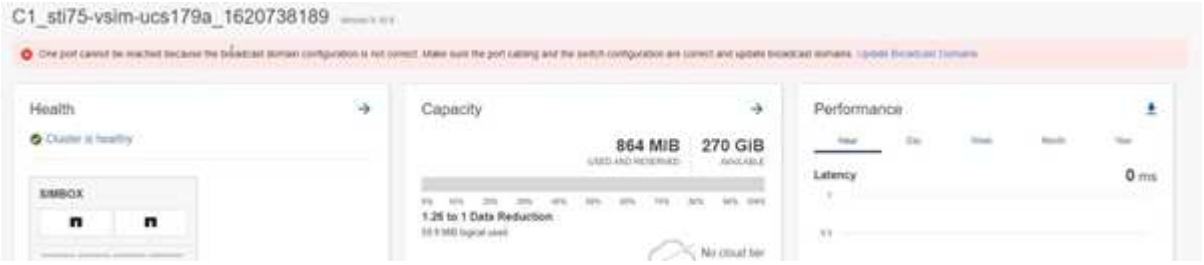
設定叢集之後、儀表板上會報告網路配線問題。

將新節點加入叢集之後、「節點」頁面上會出現網路配線問題。

您也可以在網路圖上檢視網路配線健全狀況。連接埠連線能力問題會在網路圖中以紅色的錯誤圖示表示。

叢集後設定

設定叢集之後、如果系統偵測到網路配線問題、儀表板上會出現一則訊息。



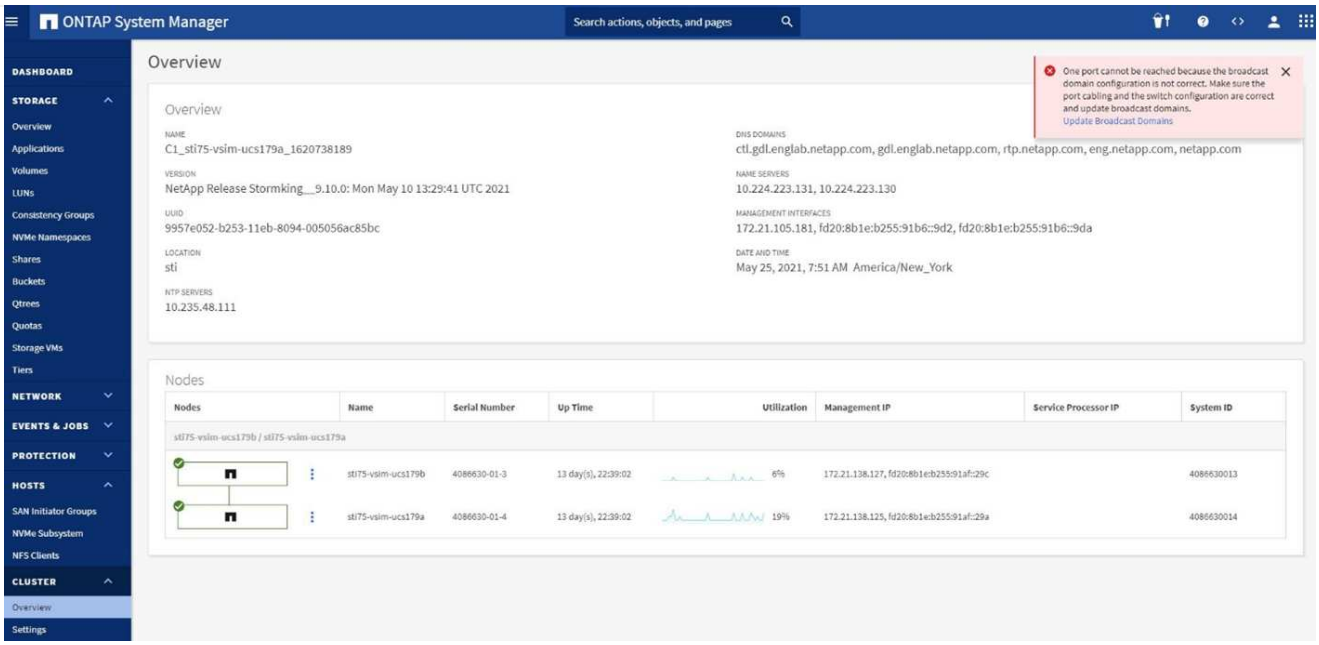
步驟

1. 按照訊息中的建議修正線路。
2. 按一下連結以啟動「更新廣播網域」對話方塊。
   「更新廣播網域」對話方塊隨即開啟。

3. 檢閱連接埠的相關資訊、包括節點、問題、目前的廣播網域及預期的廣播網域。
4. 選取您要修復的連接埠、然後按一下「修復」。
   系統會將連接埠從目前的廣播網域移至預期的廣播網域。

POST節點加入

將新節點加入叢集之後、如果系統偵測到網路配線問題、節點頁面上會出現一則訊息。



步驟

1. 按照訊息中的建議修正線路。
2. 按一下連結以啟動「更新廣播網域」對話方塊。
   「更新廣播網域」對話方塊隨即開啟。

3. 檢閱連接埠的相關資訊、包括節點、問題、目前的廣播網域及預期的廣播網域。
4. 選取您要修復的連接埠、然後按一下「修復」。
   系統會將連接埠從目前的廣播網域移至預期的廣播網域。

CLI

開始之前

您必須是叢集管理員才能執行此工作。

關於這項工作

您可以使用命令、根據ONTAP 由停止偵測到的第2層可到達性、自動修復連接埠的廣播網域組態。

步驟

1. 檢查交換器組態和纜線。

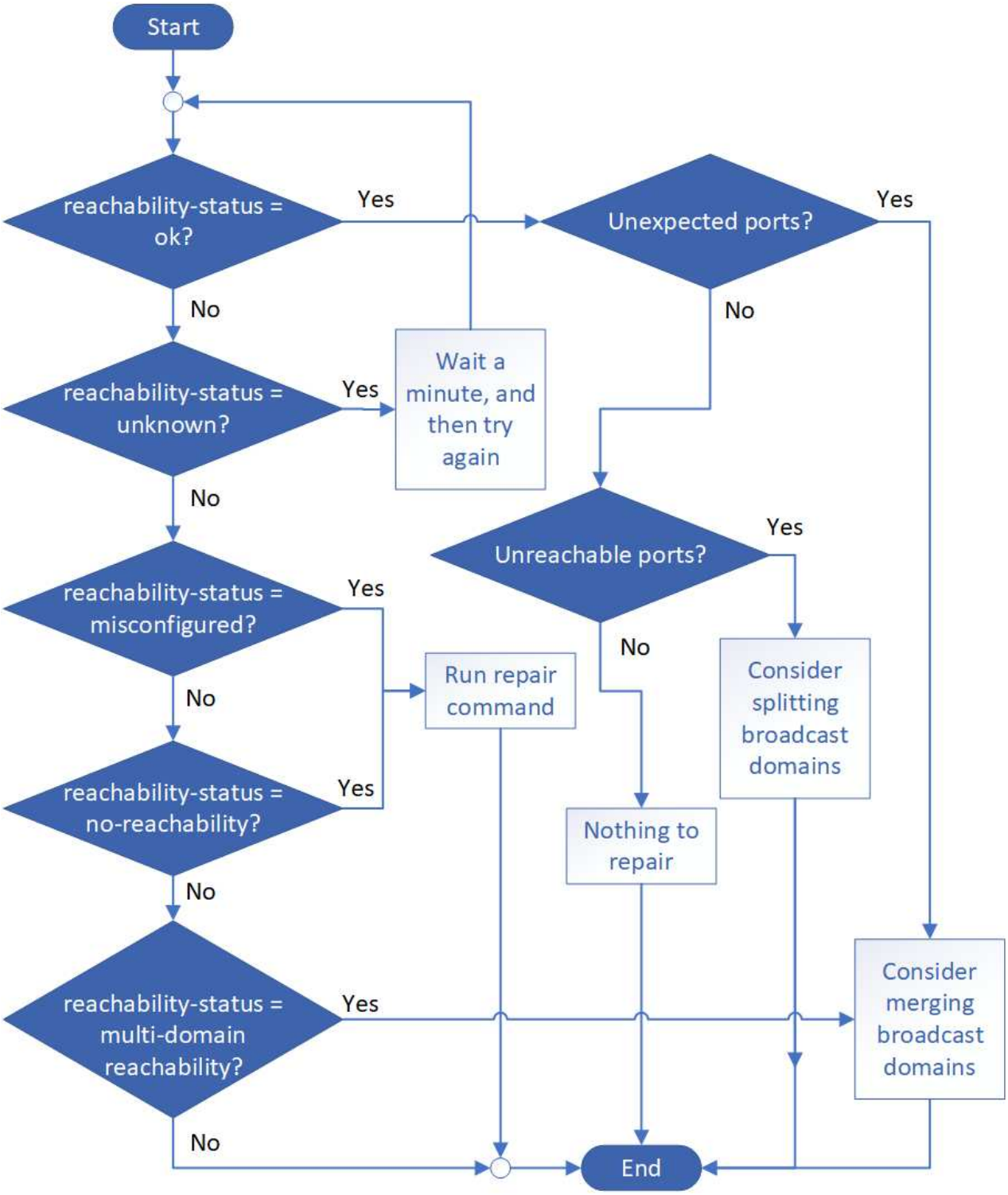
2. 檢查連接埠的可連線性：

   `network port reachability show -detail -node -port`

   命令輸出包含可到達性結果。

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

3. 請使用下列決策樹狀結構和表格來瞭解可連線性結果、並判斷接下來要做什麼（如果有的話）。



連線狀態	說明
好的	連接埠可連線至其指派的廣播網域的第2層。 如果連線狀態為「正常」、但有「非預期的連接埠」、請考慮合併一或多個廣播網域。如需詳細資訊、請參閱下列_Unexpected連接埠_資料列。 如果連線狀態為「正常」、但有「無法連線的連接埠」、請考慮分割一或多個廣播網域。如需詳細資訊、請參閱下列_Unreachable連接埠_資料列。 如果連線狀態為「正常」、而且沒有非預期或無法連線的連接埠、表示您的組態正確。
非預期的連接埠	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
無法連線的連接埠	如果單一廣播網域已分割成兩個不同的連線能力集、您可以分割廣播網域、 將ONTAP 此功能與實體網路拓撲進行同步。 一般而言、無法連線的連接埠清單會定義在您確認實體和交換器組態正確之後、應分割成另一個廣播網域的一組連接埠。 如需詳細資訊、請參閱 "分割廣播網域"。
設定錯誤的連線能力	連接埠無法連線至其指派的廣播網域的第2層；不過連接埠確實可連線至不同的廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給可連線的廣播網域： `network port reachability repair -node -port`
不可到達性	連接埠無法連線至任何現有廣播網域的第2層。 您可以修復連接埠連線能力。執行下列命令時、系統會將連接埠指派給預設IPspace中自動建立的新廣播網域： `network port reachability repair -node -port` • 注意：* 如果所有介面群組（ ifgrp ）成員連接埠都報告 `no-reachability`、執行 `network port reachability repair` 每個成員連接埠上的命令都會導致從 ifgrp 移除每個連接埠、並置入新的廣播網域、最後導致移除 ifgrp 本身。執行之前 `network port reachability repair` 命令、根據實體網路拓撲、確認連接埠的可連線廣播網域符合您的預期。 如"指令參考資料ONTAP"需詳細 `network port reachability repair`資訊，請參閱。

多網域連線能力	連接埠可到達其指派的廣播網域的第2層連通性、但它也可到達至少一個其他廣播網域的第2層連通性。 檢查實體連線能力和交換器組態、判斷是否不正確、或連接埠指派的廣播網域是否需要與一或多個廣播網域合併。 如需詳細資訊、請參閱 "合併廣播網域"。
不明	如果連線狀態為「未知」、請稍候幾分鐘、然後再試一次命令。

修復連接埠之後、請檢查是否有已移位的LIF和VLAN。如果連接埠是介面群組的一部分、您也需要瞭解該介面群組發生了什麼事。

生命

當某個連接埠修復並移至不同的廣播網域時、在修復連接埠上設定的任何LIF都會自動指派新的主連接埠。如果可能、該主連接埠會從同一個節點上的相同廣播網域中選取。或者、也會選取另一個節點的主連接埠、或者、如果沒有適當的主連接埠、主連接埠就會清除。

如果 LIF 的主連接埠移至另一個節點、或已清除、則 LIF 會被視為「已移轉」。您可以使用下列命令來檢視這些已移出的LIF：

```
displaced-interface show
```

如果有任何需要更換的生命、您必須：

- 還原已移出的LIF的主場：

  ```
  displaced-interface restore
  ```

- 手動設定LIF的主目錄：

  ```
  network interface modify -home-port -home-node
  ```

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

- 如果您對LIF目前設定的主目錄感到滿意、請從「失所介面」表格中移除該項目：

  ```
  displaced-interface delete
  ```

VLAN

如果修復的連接埠有VLAN、這些VLAN會自動刪除、但也會記錄為「已移除」。您可以檢視這些已移離的VLAN：

```
displaced-vlans show
```

如果有任何已被取代的VLAN、您必須：

- 將VLAN還原至其他連接埠：

  ```
  displaced-vlans restore
  ```

- 從「Valler-VLANs」表中移除項目：

```
displaced-vlans delete
```

介面群組

如果修復的連接埠是介面群組的一部分、則會從該介面群組中移除。如果它是唯一指派給介面群組的成員連接埠、則介面群組本身就會移除。

相關資訊

- "升級後驗證您的網路組態"
- "監控網路連接埠的連線能力"
- "指令參考資料ONTAP"

將 ONTAP 廣播網域移至 IPspace

從 ONTAP 9.8 開始，您可以將系統根據第 2 層連線能力所建立的廣播網域移至您建立的 IPspace 。

在移動廣播網域之前、您必須確認廣播網域中連接埠的可連線性。

自動掃描連接埠可判斷哪些連接埠可以彼此連線、並將它們放在同一個廣播網域中、但此掃描無法判斷適當的IPspace。如果廣播網域屬於非預設IPspace、則您必須使用本節中的步驟手動移動它。

開始之前

廣播網域會自動設定為叢集建立和加入作業的一部分。此「預設」廣播網域定義為連接第2層連接至叢集第一個節點上管理介面的主連接埠的連接埠集。ONTAP如有必要、會建立其他廣播網域、並命名為*預設值-1*、*預設值-2*等。

當節點加入現有叢集時、其網路連接埠會根據其第2層可到達性自動加入現有的廣播網域。如果連接埠無法連線至現有的廣播網域、則連接埠會放置在一個或多個新的廣播網域中。

關於這項工作

- 具有叢集生命的連接埠會自動置入「叢集」IPspace。
- 可連線至節點管理LIF主連接埠的連接埠、會置於「預設」廣播網域中。
- 其他廣播網域則由ONTAP 不受限制的功能自動建立、作為叢集建立或加入作業的一部分。
- 當您新增VLAN和介面群組時、這些VLAN和介面群組會在建立後約一分鐘自動放入適當的廣播網域。

步驟

1. 驗證廣播網域中連接埠的可連線性。自動監控第2層連線能力。ONTAP使用下列命令來驗證每個連接埠是否已新增至廣播網域、且具有「OK」連線能力。

   ```
   network port reachability show -detail
   ```

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

2. 如有必要、請將廣播網域移至其他IPspaces：

```
network port broadcast-domain move
```

例如、如果您要將廣播網域從「預設」移至「ips1」：

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default
-to-ipspace ips1
```

相關資訊

- "網路連接埠廣播網域移動"

分割 ONTAP 廣播網域

如果透過實體網路連線或交換器組態變更了網路連接埠連線能力、 先前在單一廣播網域中設定的一組網路連接埠已分割成兩個不同的連線能力集、您可以分割廣播網域、將ONTAP此「更新」組態與實體網路拓撲進行同步。

分割廣播網域的程序與 ONTAP 9.7 和舊版不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上分割廣播域，請"分割廣播網域（ ONTAP 9.7 或更早版本）"參閱。

若要判斷網路連接埠廣播網域是否分割成多個連線能力集，請使用 `network port reachability show -details`命令並注意哪些連接埠無法彼此連線（「無法連線的連接埠」）。一般而言、無法連線的連接埠清單會在您確認實體和交換器組態正確之後、定義應分割成另一個廣播網域的連接埠集。如"指令參考資料ONTAP"需詳細 `network port reachability show`資訊，請參閱。

步驟

將廣播網域分割成兩個廣播網域：

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` 是廣播網域所在 IPSpace 的名稱。
- `-broadcast-domain` 是要分割的廣播網域名稱。
- `-new-broadcast-domain` 是要建立的新廣播網域名稱。
- `-ports` 是要新增至新廣播網域的節點名稱和連接埠。

相關資訊

- "網路連接埠廣播網域分割"

合併 ONTAP 廣播網域

如果網路連接埠可連線性已變更、無論是透過實體網路連線或交換器組態、或是先前在多個廣播網域中設定的兩組網路連接埠、現在都能共用可連線性、則可以使用合併兩個廣播網域、將ONTAP 此二元組態與實體網路拓撲進行同步。

ONTAP 9.7 和舊版中的廣播網域合併程序不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上合併廣播域，請"合併廣播網域（ ONTAP 9.7 或更早版本）"參閱。

若要確定多個廣播域是否屬於可達性集，請使用 `network port reachability show -details`命令並注意在另一個廣播網域中配置的哪些連接埠實際上彼此具有連接（“意外連接埠”）。通常、非預期連接埠清單會定義在您驗證實體和交換器組態是否正確之後、應合併到廣播網域的連接埠集。

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

步驟

將一個廣播網域的連接埠合併到現有的廣播網域：

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` 是廣播網域所在 IPSpace 的名稱。
- `-broadcast-domain` 是要合併的廣播網域名稱。
- `-into-broadcast-domain` 是將接收其他連接埠的廣播網域名稱。

相關資訊

- "網路連接埠 broadcast-domain-merge"

變更 ONTAP 廣播網域中連接埠的 MTU 值

您可以修改廣播網域的MTU值、以變更該廣播網域中所有連接埠的MTU值。這可以用來支援網路中的拓撲變更。

在 ONTAP 9.7 和更早版本中，變更廣播網域連接埠 MTU 值的程序有所不同。如果您需要變更執行 ONTAP 9.7 及更早版本之網路上廣播網域連接埠的 MTU 值，請參閱"變更廣播網域中連接埠的 MTU 值（ ONTAP 9.7 及更早版本）"。

系統管理員

從 ONTAP 9.12.1 開始，您可以使用 System Manager 修改廣播網域的 MTU 值，從而變更該廣播網域中所有連接埠的 MTU 值。

步驟

1. 選擇 **Network > Broadcast Domains** 。
2. 在 **Broadcast Domains** 部分，選擇要變更 MTU 值的廣播網域的名稱。
3. 系統會彈出提示，詢問您是否要變更廣播網域中所有連接埠的 MTU 值。按一下 **Yes** 繼續變更。
4. 根據需要修改 MTU 值並儲存變更。

   系統會將新的 MTU 值套用至廣播網域中的所有連接埠，這會導致這些連接埠的流量短暫中斷。

CLI

開始之前

MTU值必須符合連接至該層2網路的所有裝置、但e0M連接埠處理管理流量除外。

關於這項工作

更改 MTU 值會導致受影響連接埠上的流量短暫中斷。系統會顯示提示，您必須輸入 **y** 才能變更 MTU。

步驟

變更廣播網域中所有連接埠的MTU值：

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

其中：

- `broadcast_domain` 是廣播網域的名稱。
- `mtu` 為 IP 封包的 MTU 大小； 1500 和 9000 為典型值。
- `ipspace` 是此廣播域所在的 IPspace 的名稱。除非您為此選項指定值，否則將使用「Default」IPspace。

  以下命令將廣播網域 bcast1 中所有連接埠的 MTU 變更為 9000：

```
network port broadcast-domain modify -broadcast-domain <Default-1>
-mtu < 9000 >
Warning: Changing broadcast domain settings will cause a momentary
data-serving interruption.
Do you want to continue? {y|n}: <y>
```

相關資訊

- "修改網路連接埠廣播網域"

檢視 ONTAP 廣播網域

您可以顯示叢集中每個IPspace內的廣播網域清單。輸出也會顯示每個廣播網域的連接埠清單和MTU值。

ONTAP 9.7 和舊版中顯示廣播網域的程序有所不同。如果需要在運行 ONTAP 9.7 及更早版本的網絡上顯示廣播域，請"顯示廣播網域（ ONTAP 9.7 或更早版本）"參閱。

步驟

顯示叢集中的廣播網域和相關連接埠：

```
network port broadcast-domain show
```

下列命令會顯示叢集中的所有廣播網域和相關連接埠：

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        Default-1    1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

下列命令會顯示預設廣播網域中的連接埠、其更新狀態為「錯誤」、表示連接埠無法正確更新：

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ------------ -----  ---------------------- --------------
Default Default-1    1500
                            cluster-1-02:e0g       error
```

相關資訊

- "網路連接埠廣播網域show"

刪除 ONTAP 廣播網域

如果不再需要廣播網域、您可以將其刪除。這會將與該廣播網域相關的連接埠移至「預設」IPspace。

開始之前

不得有任何子網路、網路介面或SVM與您要刪除的廣播網域相關聯。

關於這項工作

- 無法刪除系統建立的「叢集」廣播網域。
- 刪除廣播網域時、會移除與廣播網域相關的所有容錯移轉群組。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**刪除廣播網域

當廣播網域包含連接埠或與子網路相關聯時、不會顯示刪除選項。

步驟

1. 選擇*網路>總覽>廣播網域*。
2. 在您要移除的廣播網域旁邊選取 * > 刪除 * 。

CLI

使用**CLI**刪除廣播網域

步驟

刪除廣播網域：

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

下列命令會刪除IPspace ipspace1中的廣播網域預設值1：

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

相關資訊

- "網路連接埠廣播網域刪除"

容錯移轉群組和原則

瞭解 **ONTAP** 網路上的 **LIF** 容錯移轉

LIF容錯移轉是指自動將LIF移轉至不同的網路連接埠、以因應LIF目前連接埠上的連結故障。這是提供高可用度以連線至SVM的關鍵元件。設定LIF容錯移轉包括建立容錯移轉群組、修改LIF以使用容錯移轉群組、以及指定容錯移轉原則。

容錯移轉群組包含一組來自叢集中一或多個節點的網路連接埠（實體連接埠、VLAN和介面群組）。容錯移轉群組中的網路連接埠可定義LIF可用的容錯移轉目標。容錯移轉群組可以指派叢集管理、節點管理、叢集間及NAS資料生命期給它。

如果LIF設定為沒有有效的容錯移轉目標、則LIF嘗試容錯移轉時會發生中斷。您可以使用 `network interface show -failover`命令來驗證容錯移轉組態。如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。

建立廣播網域時、系統會自動建立同名的容錯移轉群組、其中包含相同的網路連接埠。此容錯移轉群組是由系統自動管理、也就是說、當連接埠從廣播網域新增或移除時、它們會自動從這個容錯移轉群組中新增或移除。對於不想管理自己的容錯移轉群組的系統管理員而言、這是一種效率。

建立 ONTAP 容錯移轉群組

您可以建立網路連接埠的容錯移轉群組、以便LIF在LIF的目前連接埠發生連結故障時、自動移轉至不同的連接埠。這可讓系統將網路流量重新路由至叢集中的其他可用連接埠。

關於這項工作

您可以使用 `network interface failover-groups create` 命令以建立群組並將連接埠新增至群組。

- 新增至容錯移轉群組的連接埠可以是網路連接埠、VLAN或介面群組（ifgrps）。
- 新增至容錯移轉群組的所有連接埠都必須屬於同一個廣播網域。
- 單一連接埠可位於多個容錯移轉群組中。
- 如果您在不同的VLAN或廣播網域中有LIF、則必須為每個VLAN或廣播網域設定容錯移轉群組。
- 容錯移轉群組不適用於SAN iSCSI或FC環境。

步驟

建立容錯移轉群組：

`network interface failover-groups create -vserver` *`vserver_name`* `-failover-group` *`failover_group_name`* `-targets` *`ports_list`*

- *`vserver_name`* 是可以使用容錯移轉群組的 SVM 名稱。
- *`failover_group_name`* 為您要建立的容錯移轉群組名稱。
- *`ports_list`* 是要新增至容錯移轉群組的連接埠清單。
  連接埠的新增格式為_node_name>:<port_number>_、例如node1:e0c。

下列命令會針對SVM VS3建立容錯移轉群組fg3、並新增兩個連接埠：

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

完成後

- 在建立容錯移轉群組之後、您應該將容錯移轉群組套用至LIF。
- 套用不為LIF提供有效容錯移轉目標的容錯移轉群組、會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 如"指令參考資料ONTAP"需詳細 `network interface failover-groups create`資訊，請參閱。

在 LIF 上設定 ONTAP 容錯移轉設定

您可以將容錯移轉原則和容錯移轉群組套用至LIF、將LIF設定為容錯移轉至特定的網路連接埠群組。您也可以停用LIF、使其無法容錯移轉至其他連接埠。

關於這項工作

- 建立LIF時、預設會啟用LIF容錯移轉、可用的目標連接埠清單則由預設的容錯移轉群組和容錯移轉原則根據LIF類型和服務原則來決定。

  從9.5開始、您可以為LIF指定服務原則、以定義哪些網路服務可以使用LIF。有些網路服務會對LIF強制容錯移轉限制。

  如果LIF的服務原則變更後會進一步限制容錯移轉、則系統會自動更新LIF的容錯移轉原則。

- 您可以在network interface modify命令中指定-容 錯移轉群組和-容 錯移轉原則參數的值、以修改I生命 體的容錯移轉行為。
- 修改LIF會導致LIF沒有有效的容錯移轉目標、因此會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 從 ONTAP 9.11.1 開始、在 All Flash SAN Array （ASA）平台上、 iSCSI LIF 容錯移轉會自動在新建立的儲存 VM 上、於新建立的 iSCSI 生命週期中啟用。

  此外、您也可以 "在預先存在的 iSCSI 生命體上手動啟用 iSCSI LIF 容錯移轉"、意指在升級至 ONTAP 9.11.1 或更新版本之前建立的生命。

- 下列清單說明容錯移轉原則設定如何影響從容錯移轉群組選取的目標連接埠：

  對於 iSCSI LIF 容錯移轉、只有容錯移轉原則 `local-only`、 `sfo-partner-only` 和 `disabled` 支援。

- `broadcast-domain-wide` 適用於容錯移轉群組中所有節點上的所有連接埠。
- `system-defined` 僅適用於 LIF 主節點上的連接埠、以及叢集中的另一個節點、通常是非 SFO 合作夥伴（如果存在）。
- `local-only` 僅適用於 LIF 主節點上的連接埠。
- `sfo-partner-only` 僅適用於 LIF 主節點及其 SFO 合作夥伴上的連接埠。
- `disabled` 表示 LIF 未設定為容錯移轉。

步驟

設定現有介面的容錯移轉設定：

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

設定容錯移轉設定及停用容錯移轉的範例

下列命令會將容錯移轉原則設定為廣播網域範圍、並使用容錯移轉群組fg3中的連接埠做為SVM VS3上LIF資料1的容錯移轉目標：

```
network interface modify -vserver vs3 -lif data1 -failover-policy
broadcast-domain-wide -failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1          broadcast-domain-wide  fg3
```

下列命令會停用SVM VS3上LIF資料1的容錯移轉：

```
network interface modify -vserver vs3 -lif data1 -failover-policy disabled
```

相關資訊

- "網路介面"

用於管理容錯移轉群組和原則的 ONTAP 命令

您可以使用 `network interface failover-groups` 管理容錯移轉群組的命令。您可以使用 `network interface modify` 用於管理套用至 LIF 的容錯移轉群組和容錯移轉原則的命令。

如果您想要...	使用此命令...
將網路連接埠新增至容錯移轉群組	`network interface failover-groups add-targets`
從容錯移轉群組移除網路連接埠	`network interface failover-groups remove-targets`
修改容錯移轉群組中的網路連接埠	`network interface failover-groups modify`
顯示目前的容錯移轉群組	`network interface failover-groups show`
在LIF上設定容錯移轉	`network interface modify -failover -group -failover-policy`
顯示每個LIF所使用的容錯移轉群組和容錯移轉原則	`network interface show -fields failover-group, failover-policy`

重新命名容錯移轉群組	`network interface failover-groups rename`
刪除容錯移轉群組	`network interface failover-groups delete`

修改容錯移轉群組、使其無法為叢集中的任何LIF提供有效的容錯移轉目標、可能會在LIF嘗試容錯移轉時造成中斷。

相關資訊

- "網路介面"

子網路（僅限叢集管理員）

瞭解 ONTAP 網路的子網路

子網路可讓您分配特定區塊或集區IP位址、以供ONTAP 您進行支援所需的網路組態。這可讓您指定子網路名稱、而不必指定IP位址和網路遮罩值、更輕鬆地建立lifs。

子網路是在廣播網域內建立、其中包含屬於同一第3層子網路的IP位址集區。子網路中的IP位址會在建立LIF時分配給廣播網域中的連接埠。移除LIF時、IP位址會傳回子網路集區、可供未來的LIF使用。

建議您使用子網路、因為子網路可讓IP位址的管理更輕鬆、而且能簡化生命週期的建立程序。此外、如果您在定義子網路時指定閘道、則當使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。

為 ONTAP 網路建立子網路

您可以建立子網路、以配置稍後為SVM建立LIF時所使用的特定IPv4或IPv6位址區塊。

這可讓您更輕鬆地建立lifs、方法是指定子網路名稱、而非為每個LIF指定IP位址和網路遮罩值。

開始之前

您必須是叢集管理員才能執行此工作。

您要新增子網路的廣播網域和IPspace必須已經存在。

關於這項工作

- 所有子網路名稱在IPspace內必須是唯一的。
- 將IP位址範圍新增至子網路時、您必須確保網路中沒有重疊的IP位址、以免不同的子網路或主機嘗試使用相同的IP位址。
- 如果您在定義子網路時指定閘道、則當使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。如果您不使用子網路、或是定義子網路時未指定閘道、則需要使用 `route create` 手動將路由新增至 SVM 的命令。
- NetApp 建議為資料 SVM 上的所有生命建立子網路物件。這對 MetroCluster 組態尤其重要，因為每個子網路物件都有相關的廣播網域，因此子網路物件可讓 ONTAP 判斷目的地叢集上的容錯移轉目標。

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 建立子網路。

系統管理員

從ONTAP 功能性版本的0：9.12.0開始、您可以使用System Manager建立子網路。

步驟

1. 選擇*網路>總覽>子網路*。
2. 按一下 + Add 以建立子網路。
3. 命名子網路。
4. 指定子網路IP位址。
5. 設定子網路遮罩。
6. 定義組成子網路的IP位址範圍。
7. 如果有用、請指定閘道。
8. 選取子網路所屬的廣播網域。
9. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

使用CLI建立子網路。

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 為您要建立的第 3 層子網路名稱。

  名稱可以是像「Mgmt」這樣的文字字串、也可以是特定的子網路IP值、例如192.0/24。

- `broadcast_domain_name` 是子網路所在的廣播網域名稱。
- `ipspace_name` 是廣播網域所屬的 IPspace 名稱。

  除非您指定此選項的值、否則會使用「預設」IPspace。

- `subnet_address` 是子網路的 IP 位址和遮罩、例如 192.0.2.0/24 。
- `gateway_address` 是子網路預設路由的閘道、例如 192.0.2.1 。
- `ip_address_list` 是將分配給子網路的 IP 位址清單或範圍。

  IP位址可以是個別位址、IP位址範圍、或是以逗號分隔的清單組合。

- 價值 `true` 可設定為 `-force-update-lif-associations` 選項。

  如果任何服務處理器或網路介面目前正在使用指定範圍內的IP位址、則此命令會失敗。將此值設為true、可將任何手動定址的介面與目前子網路建立關聯、並允許命令成功執行。

下列命令會在預設IPspace的廣播網域預設-1中建立子網路子網路1。它會新增一個IPV4子網路IP位址和遮罩、閘道和一系列IP位址：

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

下列命令會在「預設」IPspace的廣播網域預設中建立子網路子網路2。它新增多種IPv6位址：

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

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

完成後

您可以使用子網路中的位址、將SVM和介面指派給IPspace。

如果您需要變更現有子網路的名稱、請使用 `network subnet rename` 命令。

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

從 **ONTAP** 網路的子網路新增或移除 **IP** 位址

您可以在最初建立子網路時新增IP位址、或是將IP位址新增至已存在的子網路。您也可以從現有子網路移除IP位址。如此一來、您只能為SVM分配所需的IP位址。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

*從ONTAP 版本S59.12.0開始、您可以使用System Manager在子網路*中新增或移除IP位址

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要變更的子網路旁選取 ⋮ * > 編輯 * 。
3. 新增或移除IP位址。
4. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

*使用CLI在子網路*中新增或移除IP位址

關於這項工作

新增IP位址時、如果有任何服務處理器或網路介面使用所新增範圍內的IP位址、您將會收到錯誤訊息。如果您想要將任何手動定址的介面與目前的子網路建立關聯、您可以設定 `-force-update-lif-associations` 選項 `true`。

移除IP位址時、如果有任何服務處理器或網路介面使用要移除的IP位址、您將會收到錯誤訊息。如果您希望介面在從子網路移除後繼續使用 IP 位址、您可以設定 `-force-update-lif-associations` 選項 `true`。

步驟

新增或移除子網路中的IP位址：

如果您想要…	使用此命令…
新增IP位址至子網路	網路子網路新增範圍
從子網路移除IP位址	網路子網路移除範圍

下列命令會將IP位址192.0.2.82到192.0.2.85新增至子網路子網路1：

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

下列命令會從子網路子網路3移除IP位址198.51.1009：

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

如果目前範圍包括1到10、20到40、而您想要新增11到19、41到50（基本上允許1到50）、您可以使用下列命令來重疊現有的位址範圍。此命令只會新增新位址、不會影響現有位址：

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

深入瞭解 `network subnet add-ranges`及 `network subnet remove-ranges` "指令參考資料ONTAP"。

變更 ONTAP 網路的子網路內容

您可以變更現有子網路中的子網路位址和遮罩值、閘道位址或IP位址範圍。

關於這項工作

- 修改IP位址時、您必須確保網路中沒有重疊的IP位址、以免不同的子網路或主機嘗試使用相同的IP位址。
- 如果您新增或變更閘道IP位址、當使用子網路在新的SVM中建立LIF時、修改的閘道會套用至新的SVM。如果路由尚未存在、則會為SVM建立通往閘道的預設路由。變更閘道IP位址時、您可能需要手動新增新路由至SVM。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**來變更子網路內容

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要變更的子網路旁選取 * > 編輯 * 。
3. 進行變更。
4. 儲存您的變更。
   a. 如果輸入的 IP 位址或範圍已被介面使用、則會顯示下列訊息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 當您按一下「確定」時、現有的LIF將會與子網路相關聯。

CLI

使用**CLI**變更子網路內容

步驟

修改子網路內容：

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 是您要修改的子網路名稱。
- `ipspace` 是子網路所在 IPspace 的名稱。
- `subnet` 為子網路的新位址和遮罩（如果適用）、例如 192.0.2.0/24 。
- `gateway` 是子網路的新閘道（如果適用）、例如 192.0.2.1 。輸入*「*」*會移除閘道項目。
- `ip_ranges` 為 IP 位址的新清單或範圍、如果適用、將會分配給子網路。IP位址可以是個別位址、範圍或IP位址、或是以逗號分隔的清單組合。此處指定的範圍會取代現有的IP位址。
- `force-update-lif-associations` 變更 IP 位址範圍時為必填。修改IP位址範圍時、您可以將此選項的值設為* true*。如果任何服務處理器或網路介面使用指定範圍內的IP位址、則此命令會失敗。將此值設為* true*可將任何手動定址的介面與目前的子網路建立關聯、並允許命令成功執行。

下列命令會修改子網路子網路3的閘道IP位址：

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

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

檢視 ONTAP 網路的子網路

您可以顯示IP空間內分配給每個子網路的IP位址清單。輸出也會顯示每個子網路可用的IP位址總數、以及目前使用的位址數目。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**來顯示子網路

步驟

1. 選擇*網路>總覽>子網路*。
2. 檢視子網路清單。

CLI

使用**CLI**顯示子網路

步驟

顯示子網路清單及這些子網路中使用的相關IP位址範圍：

```
network subnet show
```

下列命令會顯示子網路和子網路內容：

```
network subnet show

IPspace: Default
Subnet                  Broadcast               Avail/
Name    Subnet          Domain    Gateway       Total    Ranges
------  --------------- --------- ------------ --------
------------------------
sub1    192.0.2.0/24     bcast1   192.0.2.1     5/9      192.0.2.92-
192.0.2.100
sub3    198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

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

從 ONTAP 網路刪除子網路

如果您不再需要子網路、而想要取消分配指派給子網路的IP位址、您可以將其刪除。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**刪除子網路

步驟

1. 選擇*網路>總覽>子網路*。
2. 在您要移除的子網路旁選取 ⋮ * > 刪除 * 。
3. 儲存您的變更。

CLI

使用**CLI**刪除子網路

關於這項工作

如果任何服務處理器或網路介面目前使用指定範圍內的IP位址、您將會收到錯誤訊息。如果希望介面在刪除子網路之後仍繼續使用IP位址、您可以將-force-update-lif-associations-true選項設定為true、以移除子網路與lifs的關聯。

步驟

刪除子網路：

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

下列命令會刪除IPspace ipspace1中的子網路子網路1：

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

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

為 ONTAP 網路建立 SVM

您必須建立SVM、才能將資料提供給用戶端。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須知道SVM根磁碟區的安全樣式。

  如果您計畫在此SVM上實作Hyper-V或SQL Server over SMB解決方案、則根磁碟區應該使用NTFS安全樣式。包含Hyper-V檔案或SQL資料庫檔案的磁碟區在建立時必須設定為NTFS安全性。將根磁碟區安全樣式設定為NTFS、可確保您不會不慎建立UNIX或混合式安全型資料磁碟區。

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

系統管理員

您可以使用System Manager來建立儲存VM。

步驟

1. 選擇*儲存VMS*。
2. 按一下 + Add 以建立儲存 VM 。
3. 命名儲存VM。
4. 選取存取傳輸協定：
   - SMB/CIFS、NFS
   - iSCSI
   - FC
   - NVMe
     i. 如果您選取*啟用SMB/CIFS*、請完成下列組態：

欄位或核取方塊	說明
系統管理員名稱	指定SMB/CIFS儲存VM的系統管理員使用者名稱。
密碼	指定SMB/CIFS儲存VM的管理員密碼。
伺服器名稱	指定SMB/CIFS儲存VM的伺服器名稱。
Active Directory網域	指定Active Directory網域、為SMB/CIFS儲存VM提供使用者驗證。
組織單位	指定Active Directory網域中與SMB/CIFS伺服器相關聯的組織單位。「cn=computers"是預設值、可以修改。
存取儲存VM中的共享區時、加密資料	選取此核取方塊可使用SMB 3.0加密資料、以防止對SMB/CIFS儲存VM中共用區的未授權檔案存取。
網域	新增、移除或重新排列SMB / CIFS儲存VM所列的網域。
名稱伺服器	新增、移除或重新排序SMB/CIFS儲存VM的名稱伺服器。
預設語言	指定儲存VM及其磁碟區的預設語言編碼設定。使用CLI變更儲存VM內個別磁碟區的設定。

網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用NFS*、請完成下列組態：

欄位或核取方塊	說明
允許NFS用戶端存取核取方塊	如果NFS儲存VM上建立的所有磁碟區都應該使用根磁碟區路徑「/」來掛載及周遊、請選取此核取方塊。將規則新增至匯出原則「預設」、以允許不中斷的掛載周遊。
規則	按一下 + Add 以建立規則。 • 用戶端規格：指定主機名稱、IP位址、網路群組或網域。 • 存取傳輸協定：選取下列選項的組合： ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3. ▪ NFSv4. • 存取詳細資料：針對每種類型的使用者、指定存取層級（唯讀、讀取/寫入器或超級使用者）。使用者類型包括： ◦ 全部 ◦ 全部（匿名使用者） ◦ UNIX ◦ Kerberos 5. ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM 儲存規則。

預設語言	指定儲存VM及其磁碟區的預設語言編碼設定。使用CLI變更儲存VM內個別磁碟區的設定。
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用iSCSI*、請完成下列組態：

欄位或核取方塊	說明
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取 * 啟用 FC* 、請完成下列組態：

欄位或核取方塊	說明
設定FC連接埠	在要納入儲存VM的節點上選取網路介面。建議每個節點使用兩個網路介面。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取*啟用NVMe/FC*、請完成下列組態：

欄位或核取方塊	說明

設定FC連接埠	在要納入儲存VM的節點上選取網路介面。建議每個節點使用兩個網路介面。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 如果您選取 * 啟用 NVMe / TCP * 、請完成下列組態：

欄位或核取方塊	說明
網路介面	對於您為儲存VM設定的每個網路介面、請選取現有的子網路（如果至少有一個子網路）、或指定*不含子網路*、並填寫* IP位址*和*子網路遮罩*欄位。 如果有用、請選取「對下列所有介面使用相同的子網路遮罩和閘道」核取方塊。 您可以讓系統自動選取主連接埠、或從清單中手動選取您要使用的連接埠。
管理系統管理員帳戶	如果您要管理儲存VM系統管理員帳戶、請選取此核取方塊。選取此選項時、請指定使用者名稱、密碼、確認密碼、並指出您是否要新增網路介面以進行儲存VM管理。

1. 儲存您的變更。

CLI

使用ONTAP CLI建立子網路。

步驟

1. 判斷哪些Aggregate是包含SVM根磁碟區的候選集合體。

   ```
   storage aggregate show -has-mroot false
   ```

   您必須選擇至少有1 GB可用空間的集合體、才能包含根磁碟區。如果您打算在SVM上設定NAS稽核、則必須在根Aggregate上至少有3 GB的額外可用空間、並在啟用稽核功能時、使用額外空間來建立稽核接移磁碟區。

   > 如果已在現有SVM上啟用NAS稽核、則會在成功完成集合建立之後、立即建立Aggregate的接移Volume。

2. 記錄您要在其上建立SVM根Volume的集合體名稱。
3. 如果您打算在建立SVM時指定語言、但不知道要使用的值、請識別並記錄您要指定的語言值：

   ```
   vserver create -language ?
   ```

4. 如果您計畫在建立 SVM 時指定快照原則，但不知道原則名稱，請列出可用的原則，並識別並記錄您要

使用的快照原則名稱：

```
volume snapshot policy show -vserver vserver_name
```

5. 如果您打算在建立SVM時指定配額原則、但不知道原則名稱、請列出可用的原則、並識別並記錄您要使用的配額原則名稱：

```
volume quota policy show -vserver vserver_name
```

6. 建立SVM：

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. 驗證SVM組態是否正確。

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.UTF-8
Snapshot Policy: default
Comment:
Quota Policy: default
List of Aggregates Assigned: -
Limit on Maximum Number of Volumes allowed: unlimited
Vserver Admin State: running
Vserver Operational State: running
Vserver Operational State Stopped Reason: -
Allowed Protocols: nfs, cifs, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

在此範例中、命令會在IPspace「ipspace1」中建立名為「VS1」的SVM。根磁碟區的名稱為「VS1_root」、建立於具有NTFS安全樣式的aggr3上。

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

邏輯介面（LIF）

LIF 總覽

瞭解 ONTAP 叢集的 LIF 組態

LIF（邏輯介面）代表叢集中節點的網路存取點。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。

叢集管理員可以建立、檢視、修改、移轉、還原、 或刪除lifs。SVM管理員只能檢視與SVM相關聯的LIF。

LIF是具有相關特性的IP位址或WWPN、例如服務原則、主連接埠、主節點、容錯移轉至的連接埠清單、以及防

火牆原則。您可以在叢集透過網路傳送和接收通訊的連接埠上設定LIF。

> 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

LIF可裝載於下列連接埠：

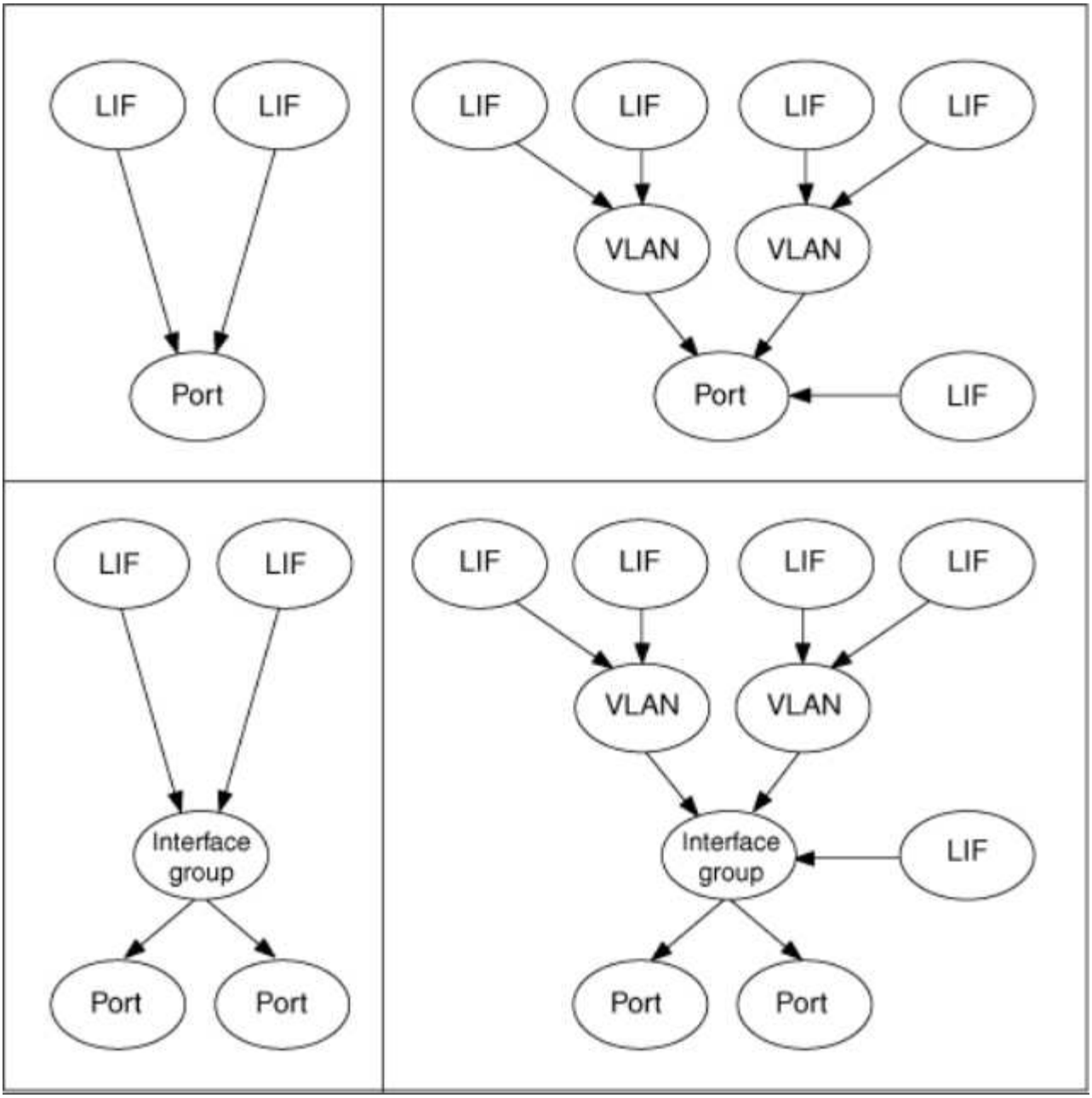
- 不屬於介面群組的實體連接埠
- 介面群組
- VLAN
- 裝載VLAN的實體連接埠或介面群組
- 虛擬IP（VIP）連接埠

  從支援的版本起、VIP LIF就會在VIP連接埠上提供支援。ONTAP

在LIF上設定FC等SAN傳輸協定時、它會與WWPN相關聯。

"SAN管理"

下圖說明ONTAP 了一個作業系統中的連接埠階層架構：



LIF 容錯移轉與恢復

LIF 會在 LIF 從其主節點或連接埠移至其 HA 合作夥伴節點或連接埠時進行容錯移轉。LIF 容錯移轉可由 ONTAP 自動觸發、或由叢集管理員手動針對某些事件觸發、例如實體乙太網路連結中斷或節點從複寫資料庫（ RDB ）仲裁中刪除。發生 LIF 容錯移轉時、 ONTAP 會繼續在合作夥伴節點上執行正常作業、直到容錯移轉的原因解決為止。當主節點或連接埠恢復健全狀況時、 LIF 會從 HA 合作夥伴還原回其主節點或連接埠。 此還原稱為贈品。

對於 LIF 容錯移轉和恢復、每個節點的連接埠都必須屬於同一個廣播網域。若要檢查每個節點上的相關連接埠是否屬於同一個廣播網域、請參閱下列內容：

- ONTAP 9.8 及更新版本： "修復連接埠連線能力"
- ONTAP 9.7 及更早版本："新增或移除廣播網域中的連接埠"

若為已啟用 LIF 容錯移轉的生命（自動或手動）、則適用下列項目：

- 對於使用資料服務原則的生命、您可以檢查容錯移轉原則限制：
  - ONTAP 9.6 及更新版本： "更新版本中的生命與服務政策ONTAP"
  - ONTAP 9.5 及更早版本："LIF角色在ONTAP 更新版本的版本中"
- 當自動還原設定為時、會自動還原生命 `true` 當 LIF 的主連接埠健全且能夠裝載 LIF 時、
- 在計畫性或非計畫性節點接管上、接管節點上的 LIF 會容錯移轉至 HA 合作夥伴。LIF容錯移轉的連接埠由VIF Manager決定。
- 容錯移轉完成後、 LIF 會正常運作。
- 啟動恢復時、如果將自動還原設定為、 LIF 會還原回其主節點和連接埠 `true`。
- 當乙太網路連結在裝載一或多個生命體的連接埠上中斷時、 VIF Manager 會將生命體從停機連接埠移轉到同一個廣播網域中的不同連接埠。新連接埠可能位於同一個節點或其HA合作夥伴中。連結還原後、如果自動還原設為 `true`、 VIF Manager 會將生命恢復回其主節點和主連接埠。
- 當節點從複寫資料庫（ RDB ）仲裁中移出時、 VIF Manager 會將生命從仲裁節點移出移轉至其 HA 合作夥伴。當節點恢復為仲裁、且自動還原設為時 `true`、 VIF Manager 會將生命恢復回其主節點和主連接埠。

瞭解 **ONTAP LIF** 與連接埠類型的相容性

LIF可以具有不同的特性、以支援不同的連接埠類型。

當叢集間和管理生命體設定在同一個子網路中時、外部防火牆可能會封鎖管理流量、AutoSupport而且可能會導致無法透過不中斷的功能進行。您可以執行來恢復系統 `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` 切換叢集間 LIF 的命令。不過、您應該在不同的子網路中設定叢集間LIF和管理LIF、以避免此問題。

LIF	說明
資料LIF	與儲存虛擬機器（SVM）相關聯的LIF、用於與用戶端通訊。 您可以在一個連接埠上擁有多個資料生命量。這些介面可在整個叢集內進行移轉或容錯移轉。您可以將資料LIF修改成SVM管理LIF、將其防火牆原則修改為管理。 建立至NIS、LDAP、Active Directory、WINS和DNS伺服器的工作階段會使用資料生命期。
叢集LIF	LIF用於在叢集中的節點之間傳輸叢集內的流量。必須始終在叢集連接埠上建立叢集LIF。 叢集LIF可在同一個節點上的叢集連接埠之間容錯移轉、但無法移轉或容錯移轉至遠端節點。當新節點加入叢集時、會自動產生IP位址。不過、如果您想要手動指派IP位址給叢集LIF、則必須確保新的IP位址與現有的叢集LIF位於相同的子網路範圍內。
叢集管理LIF	LIF可為整個叢集提供單一管理介面。 叢集管理LIF可容錯移轉至叢集中的任何節點。它無法容錯移轉至叢集或叢集間連接埠

叢集間 LIF	用於跨叢集通訊、備份和複寫的LIF。您必須在叢集中的每個節點上建立叢集間LIF、才能建立叢集對等關係。 這些LIF只能容錯移轉至同一個節點中的連接埠。它們無法移轉或容錯移轉至叢集中的其他節點。
節點管理 LIF	提供專屬IP位址以管理叢集中的特定節點的LIF。節點管理生命期是在建立或加入叢集時建立的。例如、當節點無法從叢集存取時、這些生命量會用於系統維護。
VIP LIF	VIP LIF是在VIP連接埠上建立的任何資料LIF。若要深入瞭解"設定虛擬IP（VIP）LIF"、請參閱。

相關資訊

- "修改網路介面"

ONTAP 版本支援的 **LIF** 服務原則和角色

隨著時間的推移、 ONTAP 管理生命負載所支援流量類型的方式也隨之改變。

- ONTAP 9 的同一版本和更早的版本使用 LIF 角色和防火牆服務。
- ONTAP 9 6 及更新版本使用 LIF 服務原則：
  - ONTAP 9 簡介推出 LIF 服務原則。
  - ONTAP 9 6 中以 LIF 服務原則取代 LIF 角色。
  - ONTAP 9 。 10.1 以 LIF 服務原則取代防火牆服務。

您設定的方法取決於您所使用的 ONTAP 版本。

若要深入瞭解：

- 防火牆原則請"命令： firewall-police-show"參閱。
- LIF 角色、請參閱"LIF 角色（ ONTAP 9.5 及更早版本）"。
- LIF 服務原則，請"生命與服務原則（ ONTAP 9.6 及更新版本）"參閱。

瞭解 **ONTAP** 生命與服務原則

您可以將服務原則（而非LIF角色或防火牆原則）指派給生命期、以決定生命期所支援的流量類型。服務原則定義LIF支援的網路服務集合。提供一組可與LIF相關聯的內建服務原則。ONTAP

ONTAP 9.7 和舊版的網路流量管理方法不同。如果您需要管理運行 ONTAP 9.7 及更早版本的網絡上的流量，請"LIF 角色（ ONTAP 9.5 及更早版本）"參閱。

FCP 和 NVMe/FCP 協定目前不需要服務原則。

您可以使用下列命令來顯示服務原則及其詳細資料：

```
network interface service-policy show
```

如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。

未繫結至特定服務的功能、將會使用系統定義的行為來選取輸出連線的生命。

具有空服務原則的 LIF 上的應用程式可能會在非預期的情況下運作。

系統**SVM**的服務原則

管理SVM和任何系統SVM都包含可用於該SVM中的LIF的服務原則、包括管理和叢集間LIF。系統會在建立IPspace時自動建立這些原則。

下表列出從 ONTAP 9.12.1 開始的系統 SVM 中生命週期的內建原則。對於其他版本、請使用下列命令顯示服務原則及其詳細資料：

```
network interface service-policy show
```

原則	隨附服務	等效角色	說明
預設叢集間	叢集間核心、管理-https	叢集間	用於傳輸叢集間流量的lifs。 附註：ONTAP 服務叢集間核心可從名稱為net-intercluster服務原則的版本中取得。
default-route-聲明	管理- BGP	-	由承載 BGP 對等連線的生命所使用 附註：可從 ONTAP 9.5 取得、名稱為 net-route-note 服務原則。
預設管理	管理核心、管理https、管理http、管理ssh、管理自動支援、 管理- EMS、管理- DNS用戶端、管理- ad用戶端、管理-LDAP用戶端、管理-NIS用戶端、 管理層NTP用戶端、管理層記錄轉送	節點管理或叢集管理	使用此系統範圍內的管理原則、建立系統SVM擁有的節點和叢集範圍管理生命期。這些LIF可用於連往DNS、AD、LDAP或NIS伺服器的傳出連線、以及一些額外連線、以支援代表整個系統執行的應用程式。從 ONTAP 9.12.1 開始，您可以使用該 `management-log-forwarding`服務來控制將稽核記錄轉送到遠端系統記錄伺服器的生命週期。

下表列出從 ONTAP 9.11.1 開始，在系統 SVM 上可使用的服務：

服務	容錯移轉限制	說明
叢集間核心	僅限主節點	核心叢集間服務
管理核心	-	核心管理服務
管理- ssh	-	SSH管理存取服務
管理-http	-	HTTP 管理存取服務

管理- https	-	HTTPS 管理存取服務
管理自動支援	-	發佈AutoSupport 功能的相關服務
管理- BGP	僅限主連接埠	與BGP對等互動相關的服務
備份NDMP控制	-	NDMP備份控制服務
管理- EMS	-	管理訊息存取服務
管理- NTP用戶端	-	推出於本文件的版本。ONTAP NTP用戶端存取服務。
管理- NTP伺服器	-	推出於本文件的版本。ONTAP NTP伺服器管理存取服務
管理-連接埠對應	-	portmap管理服務
管理伺服器	-	rsh伺服器管理服務
管理SNMP伺服器	-	SNMP伺服器管理服務
管理- Telnet-server	-	用於Telnet伺服器管理的服務
管理記錄轉送	-	推出於本文件的版本為ONTAP 稽核記錄轉送服務

資料**SVM**的服務原則

所有資料SVM都包含服務原則、可供該SVM中的LIF使用。

下表列出以 ONTAP 9.11.1 開頭的資料 SVM 中的生命週期內建原則。對於其他版本、請使用下列命令顯示服務原則及其詳細資料：

```
network interface service-policy show
```

原則	隨附服務	等效資料傳輸協定	說明
預設管理	資料核心，管理-https ，管理 -http ，管理 -ssh ，管理 -DNS-Client ，管理 -ad-Client ，管理 -LDAP-Client ，管理 -NIS-Client	無	使用此SVM範圍內的管理原則來建立資料SVM擁有的SVM管理生命期。這些LIF可用於提供SSH或HTTPS存取給SVM管理員。必要時、這些LIF可用於連往外部DNS、AD、LDAP或NIS伺服器的傳出連線。

預設資料區塊	資料核心、資料iSCSI	iSCSI	用於傳輸區塊導向SAN資料流量的生命體。從 ONTAP 9.10.1 開始，「 default-data-blocks 」原則已過時。改用「預設資料iSCSI」服務原則。
預設資料檔案	資料核心， data-fpolice-client ， data-dnS-server ， FlexCache ， data-CIFS ， data-nfs ， management -dnS -client ， management -ad -client ， management -ldap -client ， management -nis 用戶端	NFS、CIFS、fcache	使用預設資料檔案原則來建立支援檔案型資料傳輸協定的NAS lifs。有時SVM中只有一個LIF、因此此原則允許LIF用於外部DNS、AD、LDAP或NIS伺服器的傳出連線。如果您偏好這些連線只使用管理階層的生命，則可以從此原則移除這些服務。
預設資料iSCSI	資料核心、資料iSCSI	iSCSI	用於傳輸iSCSI資料流量的LIF。
預設資料-NVMe -TCP	資料核心、資料 -NVMe-TCP	NVMe TCP	用於傳輸NVMe/TCP資料流量的生命生命量。

下表列出可用於資料 SVM 的服務，以及從 ONTAP 9.11.1 開始的 LIF 容錯移轉原則所施加的任何限制：

服務	容錯移轉限制	說明
管理- ssh	-	SSH管理存取服務
管理-http	-	在 ONTAP 9.10.1 中推出 HTTP 管理存取服務
管理- https	-	HTTPS 管理存取服務
管理-連接埠對應	-	portmap管理存取服務
管理SNMP伺服器	-	在 ONTAP 9.10.1 中推出 用於 SNMP 伺服器管理存取的服務
資料核心	-	核心資料服務
資料NFS	-	NFS資料服務
資料CIFS	-	CIFS 資料服務

資料FlexCache	-	資料服務FlexCache
資料iSCSI	僅適用於 AFF/FAS 的主連接埠；僅適用於 ASA 的 SFO 合作夥伴	iSCSI資料服務
備份NDMP控制	-	在 ONTAP 9.10.1 中推出 備份NDMP可控制資料服務
資料DNS伺服器	-	在 ONTAP 9.10.1 中推出 DNS伺服器資料服務
資料fpolice-client	-	檔案篩選原則資料服務
資料-NVMe-TCP	僅限主連接埠	在 ONTAP 9.10.1 中推出 NVMe TCP資料服務
資料S3伺服器	-	簡易儲存服務（S3）伺服器資料服務

您應該瞭解如何將服務原則指派給資料SVM中的LIF：

- 如果使用資料服務清單建立資料SVM、則會使用指定的服務來建立該SVM中的內建「預設資料檔案」和「預設資料區塊」服務原則。
- 如果在建立資料SVM時未指定資料服務清單、則會使用預設的資料服務清單來建立該SVM中的內建「預設資料檔案」和「預設資料區塊」服務原則。

  預設的資料服務清單包括iSCSI、NFS、NVMe、SMB及FlexCache 支援服務。

- 如果LIF是以資料傳輸協定清單建立、則會將相當於指定資料傳輸協定的服務原則指派給LIF。
- 如果不存在等效的服務原則、則會建立自訂服務原則。
- 如果在沒有服務原則或資料傳輸協定清單的情況下建立LIF、預設會將預設資料檔案服務原則指派給LIF。

資料核心服務

資料核心服務可讓先前使用LIF搭配資料角色的元件、在已升級的叢集上正常運作、以使用服務原則來管理LIF角色（ONTAP 在S32 9.6中已過時）。

將資料核心指定為服務並不會開啟防火牆中的任何連接埠、但該服務應包含在資料SVM的任何服務原則中。例如、預設的資料檔案服務原則會包含下列服務：

- 資料核心
- 資料NFS
- 資料CIFS
- 資料FlexCache

資料核心服務應包含在原則中、以確保使用LIF的所有應用程式都能如預期般運作、但其他三項服務則可視需要

移除。

用戶端LIF服務

從推出支援支援多種應用程式的支援服務起、支援客戶端LIF服務。ONTAP ONTAP這些服務可控制代表每個應用程式用於傳出連線的LIF。

下列新服務可讓系統管理員控制哪些LIF是用於特定應用程式的來源位址。

服務	SVM限制	說明
管理-廣告用戶端	-	從《支援支援》9.11.1開始ONTAP 、ONTAP 支援Active Directory用戶端服務、以進行外部AD伺服器的傳出連線。
管理DNS用戶端	-	從功能支援的版本起、功能支援DNS用戶端服務、以便連線至外部DNS伺服器。ONTAP ONTAP
管理- LDAP用戶端	-	從功能支援的版本起、支援LDAP用戶端服務、以進行外部LDAP伺服器的傳出連線。ONTAP ONTAP
管理NIS用戶端	-	從功能支援的版本起、功能支援NIS用戶端服務、以進行外部NIS伺服器的傳出連線。ONTAP ONTAP
管理- NTP用戶端	僅限系統	從功能支援的版本起、支援NTP用戶端服務、以便連線至外部NTP伺服器。ONTAP ONTAP
資料fpolice-client	純資料	從功能不全的9.8開始ONTAP 、支援用戶端服務輸出FPolicy連線。ONTAP

某些內建服務原則會自動包含每項新服務、但系統管理員可以將其從內建原則中移除、或將其新增至自訂原則中、以控制代表每個應用程式用於傳出連線的LIF。

相關資訊

- "網路介面服務原則顯示"

管理生命

設定 ONTAP 叢集的 LIF 服務原則

您可以設定LIF服務原則、以識別將使用LIF的單一服務或服務清單。

為lifs建立服務原則

您可以為lifs建立服務原則。您可以將服務原則指派給一或多個LIF、讓LIF能夠傳輸單一服務或服務清單的流量。

您需要進階權限才能執行 `network interface service-policy create` 命令。

關於這項工作

內建的服務和服務原則可用於管理資料和系統SVM上的資料和管理流量。大部分的使用案例都是使用內建服務原則而非建立自訂服務原則來滿足。

您可以視需要修改這些內建服務原則。

步驟

1. 檢視叢集中可用的服務：

```
network interface service show
```

服務代表LIF存取的應用程式、以及叢集所服務的應用程式。每項服務都包含零個或多個應用程式正在偵聽的TCP和udp連接埠。

提供下列額外的資料與管理服務：

```
cluster1::> network interface service show

Service                     Protocol:Ports
-------                     --------------
cluster-core                -
data-cifs                   -
data-core                   -
data-flexcache              -
data-iscsi                  -
data-nfs                    -
intercluster-core           tcp:11104-11105
management-autosupport      -
management-bgp              tcp:179
management-core             -
management-https            tcp:443
management-ssh              tcp:22
12 entries were displayed.
```

2. 檢視叢集中的服務原則：

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

7 entries were displayed.
```

3. 建立服務原則：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- 「service_name」指定應包含在原則中的服務清單。
- "ip_address/mask"指定允許存取服務原則中服務之位址的子網路遮罩清單。根據預設、所有指定的服務都會新增預設允許位址清單0.00.0.0/0、以允許來自所有子網路的流量。如果提供了非預設允許的位址清單、則使用該原則的LIF會設定為封鎖所有來源位址不符合任何指定遮罩的要求。

  下列範例說明如何針對包含_NFS_和_SMB_服務的SVM建立資料服務原則（*svm1_data_policy_*）：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver svm1
-policy svm1_data_policy -services data-nfs,data-cifs,data-core
```

  下列範例顯示如何建立叢集間服務原則：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. 確認已建立服務原則。

```
cluster1::> network interface service-policy show
```

  下列輸出顯示可用的服務原則：

```
cluster1::> network interface service-policy show

Vserver   Policy                       Service: Allowed Addresses
--------- --------------------------
---------------------------------------
cluster1
          default-intercluster         intercluster-core: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          intercluster1                intercluster-core: 0.0.0.0/0

          default-management           management-core: 0.0.0.0/0
                                       management-autosupport: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          default-route-announce       management-bgp: 0.0.0.0/0

Cluster
          default-cluster              cluster-core: 0.0.0.0/0

vs0
          default-data-blocks          data-core: 0.0.0.0/0
                                       data-iscsi: 0.0.0.0/0

          default-data-files           data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0
                                       data-flexcache: 0.0.0.0/0

          default-management           data-core: 0.0.0.0/0
                                       management-ssh: 0.0.0.0/0
                                       management-https: 0.0.0.0/0

          svm1_data_policy             data-core: 0.0.0.0/0
                                       data-nfs: 0.0.0.0/0
                                       data-cifs: 0.0.0.0/0

9 entries were displayed.
```

完成後

在建立時或修改現有LIF、將服務原則指派給LIF。

將服務原則指派給LIF

您可以在建立LIF時或修改LIF、將服務原則指派給LIF。服務原則會定義可與LIF搭配使用的服務清單。

關於這項工作

您可以在管理VM和資料SVM中指派生命權的服務原則。

步驟

視您要將服務原則指派給LIF的時間而定、請執行下列其中一項動作：

如果您...	指派服務原則...
建立LIF	網路介面create -vserver Svm_name -lIF <lif_name>-home-node<node_name>-home-port <port_name> ｛（-address <ip_address>-netMask<ip_address>）-subnet-name <subnet_name>-service-policy <service_policy_name>
修改LIF	網路介面修改-vserver <Svm_name>-lif<lif_name>-service-policy <service_policy_name>

當您為LIF指定服務原則時、不需要指定LIF的資料傳輸協定和角色。也支援透過指定角色和資料傳輸協定來建立LIF。

服務原則只能由建立服務原則時所指定之相同SVM中的LIF使用。

範例

下列範例說明如何修改LIF的服務原則、以使用預設管理服務原則：

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

管理LIF服務原則的命令

使用 `network interface service-policy` 管理 LIF 服務原則的命令。

如"指令參考資料ONTAP"需詳細 `network interface service-policy`資訊，請參閱。

開始之前

在主動 SnapMirror 關係中修改 LIF 的服務原則會中斷複寫排程。如果您將 LIF 從叢集間轉換為非叢集間（反之亦然）、則這些變更不會複寫至對等叢集。若要在修改 LIF 服務原則之後更新對等叢集、請先執行 `snapmirror abort` 然後操作 重新同步複寫關係。

如果您想要...	使用此命令...
建立服務原則（需要進階權限）	`network interface service-policy create`
新增其他服務項目至現有的服務原則（需要進階權限）	`network interface service-policy add-service`

如果您想要...	使用此命令...
複製現有的服務原則（需要進階權限）	`network interface service-policy clone`
修改現有服務原則中的服務項目（需要進階權限）	`network interface service-policy modify-service`
從現有的服務原則移除服務項目（需要進階權限）	`network interface service-policy remove-service`
重新命名現有的服務原則（需要進階權限）	`network interface service-policy rename`
刪除現有的服務原則（需要進階權限）	`network interface service-policy delete`
將內建服務原則還原為原始狀態（需要進階權限）	`network interface service-policy restore-defaults`
顯示現有的服務原則	`network interface service-policy show`

相關資訊

- "網路介面服務展示"
- "網路介面服務原則"
- "SnapMirror中止"

建立 **ONTAP** 生命

SVM透過一或多個網路邏輯介面（LIF）、為用戶端提供資料服務。您必須在您要用來存取資料的連接埠上建立LIF。LIF （網路介面）是與實體或邏輯連接埠相關聯的 IP 位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

最佳實務做法

連接至 ONTAP 的交換器連接埠應設定為跨距樹狀目錄邊緣連接埠、以減少 LIF 移轉期間的延遲。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 基礎實體或邏輯網路連接埠必須設定為管理UP狀態。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用 System Manager 或建立的 `network subnet create` 命令。

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

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您無法將NAS和SAN傳輸協定指派給相同的LIF。

  支援的傳輸協定包括SMB、NFS、FlexCache 支援功能、iSCSI和FC； iSCSI和FC無法與其他傳輸協定結合使用。不過、NAS和乙太網路型SAN傳輸協定可以存在於同一個實體連接埠上。

  - 您不應設定承載SMB流量的生命期、以自動還原至其主節點。如果SMB伺服器要裝載解決方案、以便透過Hyper-V或SQL Server透過SMB進行不中斷營運、則此建議為必填。
- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- SVM使用的所有名稱對應和主機名稱解析服務、例如DNS、NIS、LDAP和Active Directory、 必須至少有一個LIF處理SVM的資料流量。
- 處理節點之間叢集內流量的LIF、不應與處理管理流量的LIF或處理資料流量的LIF位於相同的子網路上。
- 建立沒有有效容錯移轉目標的LIF會產生警告訊息。
- 如果叢集中有大量的生命量、您可以驗證叢集上支援的LIF容量：
  - System Manager：從ONTAP 功能完善的9.12.0,開始檢視網路介面網格的處理量。
  - CLI ：使用 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

    深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。
- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他LIF。ONTAP

  從ONTAP 支援FFC-NVMe的支援功能到支援的功能表9.4開始。如果您要建立FC-NVMe LIF、應該注意下列事項：

  - NVMe傳輸協定必須受到建立LIF的FC介面卡支援。
  - FC-NVMe是資料生命中唯一的資料傳輸協定。
- 必須為每個支援SAN的儲存虛擬機器（SVM）設定一個LIF處理管理流量。
- NVMe LIF和命名空間必須裝載在同一個節點上。
- 每個 SVM 每個節點最多可設定兩個處理資料流量的 NVMe 生命。
- 當您建立具有子網路的網路介面時ONTAP 、ENetApp會自動從所選子網路選取可用的IP位址、並將其指派給網路介面。如果有多個子網路、您可以變更子網路、但無法變更IP位址。
- 建立（新增）SVM時、您無法為網路介面指定位於現有子網路範圍內的IP位址。您會收到子網路衝突錯誤。此問題發生在網路介面的其他工作流程中、例如在SVM設定或叢集設定中建立或修改叢集間網路介面。
- 從 ONTAP 9.10.1 開始， `network interface` CLI 命令包含 `-rdma-protocols`透過 RDMA 組態的 NFS 參數。從 ONTAP 9.12.1 開始，系統管理員支援透過 RDMA 組態建立 NFS 的網路介面。如需更多資訊、請參閱 透過RDMA設定NFS的LIF。
- 從 ONTAP 9.11.1 開始、全快閃 SAN 陣列（ASA）平台可自動進行 iSCSI LIF 容錯移轉。

iSCSI LIF 容錯移轉會自動啟用（容錯移轉原則設為 `sfo-partner-only` 且自動還原值設為 `true`）如果指定 SVM 中不存在 iSCSI 生命負載、或指定 SVM 中所有現有的 iSCSI 生命負載均已透過 iSCSI LIF 容錯移轉啟用、則新建立的 iSCSI 生命負載。

如果您升級至 ONTAP 9.11.1 或更新版本後、 SVM 中現有的 iSCSI 生命體尚未啟用 iSCSI LIF 容錯移轉功能、且您在同一個 SVM 中建立新的 iSCSI 生命體、則新的 iSCSI 生命體將採用相同的容錯移轉原則 (`disabled`） SVM 中現有的 iSCSI 生命。

"適用於ASA 各種平台的iSCSI LIF容錯移轉"

從ONTAP 支援支援的版本9.7開始、ONTAP 只要IPspace的同一子網路中至少已存在一個LIF、則該產品就會自動選擇LIF的主連接埠。在同一個廣播網域中選擇一個主連接埠、以作為該子網路中的其他LIF。ONTAP您仍可指定主連接埠、但不再需要主連接埠（除非該子網路在指定的IPspace中尚不存在任何生命區）。

從ONTAP 功能性的9.12.0開始、您所遵循的程序取決於您所使用的介面-系統管理員或CLI：

系統管理員

使用**System Manager**新增網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 選取 + Add 。
3. 選取下列其中一個介面角色：
   a. 資料
   b. 叢集間
   c. SVM管理
4. 選取傳輸協定：
   a. SMB/CIFS與NFS
   b. iSCSI
   c. FC
   d. NVMe / FC
   e. NVMe / TCP
5. 命名LIF或接受先前選擇所產生的名稱。
6. 接受主節點、或使用下拉式選單選取一個節點。
7. 如果在所選SVM的IPspace中至少設定一個子網路、則會顯示子網路下拉式清單。
   a. 如果您選取子網路、請從下拉式清單中選擇該子網路。
   b. 如果您在沒有子網路的情況下繼續、則會顯示「廣播網域」下拉式清單：
      i. 指定IP位址。如果IP位址正在使用中、則會顯示警告訊息。
      ii. 指定子網路遮罩。
8. 從廣播網域中選取主連接埠、可以是自動（建議）或從下拉式功能表中選取一個。主連接埠控制項會根據廣播網域或子網路選擇來顯示。
9. 儲存網路介面。

CLI

- 使用 CLI 建立 LIF*

步驟

1. 確定要用於LIF的廣播網域連接埠。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List     Status Details
ipspace1
            default       1500
                                node1:e0d     complete
                                node1:e0e     complete
                                node2:e0d     complete
                                node2:e0e     complete
```

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

2. 驗證要用於lifs的子網路是否包含足夠的未使用IP位址。

   `network subnet show -ipspace` *`ipspace1`*

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

3. 在您要用來存取資料的連接埠上建立一個或多個生命體。

   NetApp 建議為資料 SVM 上的所有生命建立子網路物件。這對 MetroCluster 組態尤其重要，因為每個子網路物件都有相關的廣播網域，因此子網路物件可讓 ONTAP 判斷目的地叢集上的容錯移轉目標。有關說明，請參閱"建立子網路"。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

     您也可以使用-autom-revert選項、指定LIF是否應自動還原為主節點和主連接埠。

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

   - `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
   - 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
   - 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
   - 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。如"指令參考資料ONTAP"需詳細 `network route create`資訊，請參閱。
   - `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下

自動還原至其主節點。預設設定為 `false`但您可以將其設定為 `true` 視環境中的網路管理原則而定。

- `-service-policy` 從 ONTAP 9.5 開始、您可以使用指派 LIF 的服務原則 `-service-policy` 選項。
  當為LIF指定服務原則時、該原則會用來建構LIF的預設角色、容錯移轉原則和資料傳輸協定清單。在支援的過程中、服務原則僅適用於叢集間和BGP對等服務。ONTAP在NetApp 9.6中ONTAP 、您可以建立多種資料與管理服務的服務原則。
- `-data-protocol` 可讓您建立支援 FCP 或 NVMe / FC 傳輸協定的 LIF 。建立IP LIF時不需要此選項。

4. 選用：在-address選項中指派IPv6位址：

   a. 使用 `network ndp prefix show` 用於查看在各種接口上學習的 RA 前綴列表的命令。

      - `network ndp prefix show` 命令可在進階權限層級使用。

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

   b. 使用格式 `prefix::id` 手動建構 IPv6 位址。

      `prefix` 是在各種介面上學習的首碼。

   用於導出 `id`，選擇隨機 64 位元十六進位數字。

5. 驗證LIF介面組態是否正確。

   ```
   network interface show -vserver vs1
   ```

   ```
             Logical    Status     Network          Current   Current Is
   Vserver   Interface  Admin/Oper Address/Mask     Node      Port
   Home
   --------- ---------- ---------- ---------------- --------- -------
   ----
   vs1
              lif1       up/up      10.0.0.128/24    node1     e0d
   true
   ```

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

6. 確認容錯移轉群組組態符合需求。

   ```
   network interface show -failover -vserver vs1
   ```

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
--------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	網路ping
IPv6位址	網路ping6.

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

下列命令會建立一個 NVMe / FC LIF 並指定 `nvme-fc` 資料傳輸協定：

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

修改 **ONTAP** 生命

您可以變更主節點或目前節點、管理狀態、IP位址、網路遮罩、容錯移轉原則、 防火牆原則和服務原則。您也可以將LIF的位址系列從IPV4變更為IPV6。

關於這項工作

- 將LIF的管理狀態修改為「關機」時、任何未完成的NFSv4鎖定都會保留、直到LIF的管理狀態恢復為「開機」為止。

為了避免其他生命週期嘗試存取鎖定檔案時發生鎖定衝突、您必須先將NFSv4用戶端移至不同的LIF、再將管理狀態設為向下。

- 您無法修改FC LIF所使用的資料傳輸協定。不過、您可以修改指派給服務原則的服務、或變更指派給IP LIF的服務原則。

  若要修改FC LIF所使用的資料傳輸協定、您必須刪除並重新建立LIF。若要變更IP LIF的服務原則、更新期間會短暫中斷。

- 您無法修改主節點或節點範圍管理LIF的目前節點。
- 使用子網路變更LIF的IP位址和網路遮罩值時、會從指定的子網路分配IP位址；如果LIF的先前IP位址來自不同的子網路、則IP位址會傳回該子網路。
- 若要將 LIF 的位址系列從 IPv4 修改為 IPv6 、您必須使用冒號表示法來表示 IPv6 位址、並為新增值 `-netmask-length` 參數。
- 您無法修改自動設定的連結本機IPv6位址。
- 修改LIF會導致LIF沒有有效的容錯移轉目標、因此會產生警告訊息。

  如果沒有有效容錯移轉目標的LIF嘗試進行容錯移轉、可能會發生中斷。

- 從功能介紹9.5開始ONTAP 、您可以修改與LIF相關的服務原則。

  在支援的過程中、服務原則僅適用於叢集間和BGP對等服務。ONTAP在NetApp 9.6中ONTAP 、您可以建立多種資料與管理服務的服務原則。

- 從 ONTAP 9.11.1 開始、自動 iSCSI LIF 容錯移轉功能可在 All Flash SAN Array （ASA）平台上使用。

  對於預先存在的 iSCSI 生命體（即升級至 9.11.1 或更新版本之前建立的生命體）、您可以將容錯移轉原則修改為 "啟用自動 iSCSI LIF 容錯移轉"。

- ONTAP利用網路時間協定 (NTP) 來同步整個叢集的時間。變更 LIF IP 位址後，您可能需要更新 NTP 設定以防止同步失敗。欲了解更多信息，請參閱"NetApp知識庫：LIF IP 變更後 NTP 同步失敗"。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

從**ONTAP** 版本**S59.12.0**開始、您可以使用**System Manager**編輯網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁選取 ⋮ * > 編輯 * 。
3. 變更一或多個網路介面設定。如需詳細資訊、請參閱 "建立LIF"。
4. 儲存您的變更。

CLI

使用**CLI**修改**LIF**

步驟

1. 使用修改 LIF 屬性 `network interface modify` 命令。

   下列範例說明如何使用IP位址和子網路client1_sub的網路遮罩值來修改LIF datalif2的IP位址和網路遮罩：

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   下列範例說明如何修改LIF的服務原則。

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

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

2. 驗證IP位址是否可連線。

如果您使用…	然後使用…
IPV4位址	`network ping`
IPv6位址	`network ping6`

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

移轉 **ONTAP** 生命

如果連接埠故障或需要維護、您可能必須將LIF移轉至同一個節點或叢集中的不同節點上的不同連接埠。移轉LIF與LIF容錯移轉類似、但LIF移轉是手動作業、而LIF容錯移轉則是LIF

的自動移轉、以因應LIF目前網路連接埠上的連結故障。

開始之前

- 必須已為lifs設定容錯移轉群組。
- 目的地節點和連接埠必須正常運作、而且必須能夠存取與來源連接埠相同的網路。

關於這項工作

- BGP LIF位於主連接埠上、無法移轉至任何其他節點或連接埠。
- 從節點移除NIC之前、您必須先將屬於NIC的連接埠上裝載的LIF移轉至叢集中的其他連接埠。
- 您必須執行命令、從裝載叢集LIF的節點移轉叢集LIF。
- 節點範圍的LIF（例如節點範圍管理LIF、叢集LIF、叢集間LIF）無法移轉至遠端節點。
- 當NFSv4 LIF在節點之間移轉時、新連接埠上的LIF可用前、延遲最多可達45秒。

  若要解決此問題、請在沒有延遲的情況下使用NFSv4.1。

- 您可以在執行 ONTAP 9.11.1 或更新版本的 All Flash SAN Array （ ASA ）平台上移轉 iSCSI 生命體。

  移轉iSCSI LIF僅限於主節點或HA合作夥伴上的連接埠。

- 如果您的平台不是執行 ONTAP 9.11.1 版或更新版本的 All Flash SAN Array （ ASA ）平台、則無法將 iSCSI 生命體從一個節點移轉至另一個節點。

  若要解決此限制、您必須在目的地節點上建立iSCSI LIF。瞭解 "建立iSCSI LIF"。

- 如果您想要透過RDMA移轉LIF（網路介面）for NFS、則必須確保目的地連接埠具有RoCE功能。您必須執行ONTAP 版本S廳9.10.1或更新版本、才能使用CLI移轉LIF、ONTAP 或使用System Manager移轉版本。在System Manager中、一旦您選取了具備RoCE功能的目的地連接埠、就必須勾選*使用roce連接埠*旁的方塊、才能成功完成移轉。深入瞭解 "透過RDMA設定NFS的LIF"。
- 當您移轉來源或目的地LIF時、VMware VAAI複製卸載作業會失敗。深入瞭解卸載複本：
  - "NFS 環境"
  - "SAN環境"

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**移轉網路介面

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁邊選取 ⋮ * > Migrate* 。

   對於 iSCSI LIF 、請在 * 移轉介面 * 對話方塊中、選取 HA 合作夥伴的目的地節點和連接埠。

   如果您要永久移轉 iSCSI LIF 、請選取核取方塊。iSCSI LIF 必須先離線、才能永久移轉。此外、一旦iSCSI LIF永久移轉、就無法復原。沒有還原選項。

3. 按一下*移轉*。
4. 儲存您的變更。

CLI

使用**CLI**移轉**LIF**

步驟

視您要移轉特定LIF或所有LIF而定、請執行適當的動作：

如果您想要移轉...	輸入下列命令...
特定LIF	`network interface migrate`
節點上的所有資料和叢集管理生命體	`network interface migrate-all`
連接埠上的所有生命	`network interface migrate-all -node <node> -port <port>`

下列範例說明如何移轉名為的LIF `datalif1` 在SVM上 `vs0` 連接埠 `e0d` 開啟 `node0b`：

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

以下範例說明如何從目前（本機）節點移轉所有資料與叢集管理生命週期：

```
network interface migrate-all -node local
```

相關資訊

- "網路介面移轉"

在 **ONTAP** 節點容錯移轉或連接埠移轉之後，將 **LIF** 還原至其主連接埠

您可以在LIF容錯移轉或手動或自動移轉至其他連接埠之後、將其還原至主連接埠。如果特定LIF的主連接埠無法使用、則LIF會保留在目前的連接埠、不會還原。

關於這項工作

- 如果您在設定自動還原選項之前、以管理方式將LIF的主連接埠移至「UP」狀態、則LIF不會傳回主連接埠。
- 除非「自動回復」選項的值設為true、否則LIF不會自動回復。
- 您必須確保已啟用「自動還原」選項、以便讓I生命 回復到主連接埠。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**將網路介面還原為其主連接埠

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁選取 ⋮ * > Revert * 。
3. 選取*還原*可將網路介面還原至其主連接埠。

CLI

使用**CLI**將**LIF**還原為其主連接埠

步驟

手動或自動將LIF還原至主連接埠：

如果您想要將LIF還原至其主連接埠…	然後輸入下列命令…
手動	`network interface revert -vserver vserver_name -lif lif_name`
自動	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

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

恢復設定不正確的 **ONTAP LIF**

叢集網路連線至交換器時、無法建立叢集、但叢集IPspace中設定的所有連接埠、都無法連線至叢集IPspace中設定的其他連接埠。

關於這項工作

在交換式叢集中、如果叢集網路介面（ LIF ）設定在錯誤的連接埠上、或是叢集連接埠連接到錯誤的網路、則為

`cluster create` 命令可能會失敗、並出現下列錯誤：

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

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

命令的結果 `network port show`可能會顯示數個連接埠已新增至叢集 IPspace ，因為它們已連線至使用叢集 LIF 設定的連接埠。然而， `network port reachability show -detail`指令顯示哪些連接埠彼此之間沒有連線。

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

若要從連接埠上設定的叢集LIF還原、而該連接埠無法連線至使用叢集lifs設定的其他連接埠、請執行下列步驟：

步驟

1. 將叢集LIF的主連接埠重設為正確的連接埠：

   ```
   network port modify -home-port
   ```

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

2. 從叢集廣播網域中移除未設定叢集lifs的連接埠：

   ```
   network port broadcast-domain remove-ports
   ```

   如"指令參考資料ONTAP"需詳細 `network port broadcast-domain remove-ports`資訊，請參閱。

3. 建立叢集：

   ```
   cluster create
   ```

結果

當您完成叢集建立時、系統會偵測到正確的組態、並將連接埠放入正確的廣播網域。

相關資訊

- "網路連接埠連線能力顯示"

刪除 **ONTAP** 生命

您可以刪除不再需要的網路介面（LIF）。

開始之前

要刪除的生命期不得在使用中。

步驟

1. 使用以下命令將要刪除的生命期標記爲管理性關閉：

```
network interface modify -vserver vserver_name -lif lif_name -status
-admin down
```

2. 使用 `network interface delete` 刪除一或所有生命的命令：

如果您要刪除...	輸入命令...
特定LIF	`network interface delete -vserver vserver_name -lif lif_name`
所有生命	`network interface delete -vserver vserver_name -lif *`

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

下列命令會刪除LIF mgmtlif2：

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. 使用 `network interface show` 確認 LIF 已刪除的命令。

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

設定 ONTAP 虛擬 IP （ VIP ）生命

有些新一代資料中心使用第 3 層（ IP ）網路機制，需要在子網路之間容錯移轉。ONTAP 支援虛擬 IP （ VIP ）資料生命體，以及相關的路由傳輸協定，邊界閘道傳輸協定（ BGP ），以滿足這些新一代網路的容錯移轉需求。

關於這項工作

VIP資料LIF並非任何子網路的一部分、可從以相同IPspace裝載BGP LIF的所有連接埠存取。VIP資料LIF可消除主機對個別網路介面的相依性。由於多個實體介面卡會傳輸資料流量、因此整個負載不會集中在單一介面卡和相關子網路上。VIP資料LIF是透過路由傳輸協定邊界閘道傳輸協定（BGP）通告給對等路由器。

VIP資料生命量具備下列優點：

- LIF可攜性超越廣播網域或子網路：VIP資料LIF可透過BGP向路由器宣告每個VIP資料LIF的目前位置、容錯移轉至網路中的任何子網路。
- Aggregate處理量：VIP資料生命量可支援超過任何個別連接埠頻寬的Aggregate處理量、因為VIP生命量可以同時從多個子網路或連接埠傳送或接收資料。

設定邊界閘道傳輸協定（BGP）

在建立VIP生命期之前、您必須先設定BGP、這是用於向對等路由器宣告VIP LIF存在的路由傳輸協定。

從 ONTAP 9 9.1 開始， VIP 提供選用的預設路由自動化功能，使用 BGP 對等群組來簡化組態。

當BGP對等端點位於同一子網路時、使用BGP對等端點做為下一跳路由器、即可輕鬆學習預設路由。ONTAP若要使用此功能、請設定 `-use-peer-as-next-hop` 屬性至 `true`。依預設、此屬性為 `false`。

如果您已設定靜態路由、則這些路由仍會優先於這些自動預設路由。

開始之前

對等路由器必須設定為接受來自BGP LIF的BGP連線、以取得所設定的自治系統編號（ASN）。

> 不處理來自路由器的任何傳入路由宣告、因此您應該設定對等路由器、使其不傳送任何路由更新到叢集。ONTAP如此可縮短與對等通訊完全正常運作所需的時間，並減少 ONTAP 內部的記憶體使用量。

關於這項工作

設定BGP包括選擇性地建立BGP組態、建立BGP LIF、以及建立BGP對等群組。當在指定節點上建立第一個BGP對等群組時、使用預設值自動建立預設BGP組態。ONTAP

BGP LIF用於與對等路由器建立BGP TCP工作階段。對於對等路由器而言、BGP LIF是下一跳、可到達VIP LIF。BGP LIF已停用容錯移轉。BGP 對等群組會在對等群組使用的 IPspace 中，為所有 SVM 通告 VIP 路由。對等群組使用的 IPspace 是從 BGP LIF 繼承而來。

從 ONTAP 9 。 16.1 開始， BGP 對等群組支援 MD5 驗證，以保護 BGP 工作階段。啟用 MD5 時， BGP 工作階段只能在獲授權的對等點之間建立和處理，以防止未獲授權的使用者可能中斷工作階段。

下列欄位已新增至 `network bgp peer-group create`和 `network bgp peer-group modify`命令：

- `-md5-enabled <true/false>`
- `-md5-secret <md5 secret in string or hex format>`

這些參數可讓您使用 MD5 簽章來設定 BGP 對等群組，以增強安全性。下列需求適用於使用 MD5 驗證：

- 您只能在參數設定為 `true`**時指定** `-md5-secret`**參數** `-md5-enabled`。
- 您必須先全域啟用 IPsec ，才能啟用 MD5 BGP 驗證。BGP LIF 不一定要有作用中的 IPsec 組態。請參閱 "透過有線加密設定IP安全性（IPsec）"。
- NetApp 建議您先在路由器上設定 MD5, 然後再在 ONTAP 控制器上進行設定。

從功能變數9.9開始ONTAP 、新增了下列欄位：

- `-asn`**或** `-peer-asn`（ 4 位元組值）屬性本身不是新的，但現在使用 4 位元組整數。
- `-med`
- `-use-peer-as-next-hop`

您可以利用多重出口鑑別器（MED-）支援、針對路徑優先順序進行進階路由選擇。BGP更新訊息中的選用屬性Medion、可讓路由器為流量選取最佳路由。MEDA是無符號32位元整數（0 - 4294967295）、偏好較低的

值。

從 ONTAP 9.8 開始、這些欄位已新增至 `network bgp peer-group` 命令：

- `-asn-prepend-type`
- `-asn-prepend-count`
- `-community`

這些BGP屬性可讓您設定BGP對等群組的AS路徑和社群屬性。

> 雖然 ONTAP 支援上述 BGP 屬性，但路由器不需要遵守這些屬性。NetApp 強烈建議您確認路由器支援哪些屬性，並據此設定 BGP 對等群組。如需詳細資料、請參閱路由器提供的BGP文件。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 選用：執行下列其中一項動作、建立BGP組態或修改叢集的預設BGP組態：

   a. 建立BGP組態：

   ```
   network bgp config create -node {node_name | local} -asn <asn_number>
   -holdtime
   <hold_time> -routerid <router_id>
   ```

   > - 此 `-routerid`參數接受點分十進制 `32` 位元值，只需在 `AS` 網域內唯一即可。`NetApp` 建議您使用保證唯一性的節點管理 `IP` （ `v4` ）位址 `<router_id>`。
   > - 雖然 ONTAP BGP 支援 32 位元 ASN 數字，但僅支援標準十進位標記法。不支援私有 ASN 的點狀 ASN 表示法，例如 65000.1 ，而非 4259840001 。

   2位元組ASN的範例：

   ```
   network bgp config create -node node1 -asn 65502 -holdtime 180
   -routerid 1.1.1.1
   ```

   使用4位元組ASN的範例：

   ```
   network bgp config create -node node1 -asn 85502 -holdtime 180 -routerid
   1.1.1.1
   ```

   a. 修改預設BGP組態：

```
network bgp defaults modify -asn <asn_number> -holdtime <hold_time>
network bgp defaults modify -asn 65502 -holdtime 60
```

- `<asn_number>`指定 ASN 編號。從支援BGP的ASN 9.8開始ONTAP 、支援2位元組非負整數。這是一個 16 位元數字（ 1 到 65534 個可用值）。從 ONTAP 9 9.1 開始， BGP 的 ASN 支援 4 位元組非負整數（ 1 至 4294967295 ）。預設ASN為65501。ASN 23456保留用於ONTAP 建立不宣告4位元組ASN功能的對等端點、以供建立不含
- `<hold_time>`指定保留時間（以秒為單位）。預設值為 180s 。

ONTAP 僅支援一個全域 `<asn_number>`， `<hold_time>`，和 `<router_id>`，即使您為多個 IPspace 設定 BGP 也一樣。BGP 和所有 IP 路由資訊完全隔離在一個 IPspace 內。IPspace 相當於虛擬路由和轉送（ VRF ）執行個體。

3. 為系統SVM建立BGP LIF：

   對於預設 IPspace ， SVM 名稱是叢集名稱。對於其他 IPspace ， SVM 名稱與 IPspace 名稱相同。

```
network interface create -vserver <system_svm> -lif <lif_name> -service
-policy default-route-announce -home-node <home_node> -home-port
<home_port> -address <ip_address> -netmask <netmask>
```

   您可以使用 `default-route-announce` BGP LIF 的服務原則或任何包含「管理 BGP 」服務的自訂服務原則。

```
network interface create -vserver cluster1 -lif bgp1 -service-policy
default-route-announce -home-node cluster1-01 -home-port e0c -address
10.10.10.100 -netmask 255.255.255.0
```

4. 建立BGP對等群組、用於與遠端對等路由器建立BGP工作階段、並設定通告給對等路由器的VIP路由資訊：

   範例1：建立沒有自動預設路由的對等群組

   在這種情況下，管理員需要建立通往 BGP 對等點的靜態路由。

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-route-preference <integer>} {-asn-prepend-
type <ASN_prepend_type>} {-asn-prepend-count <integer>} {-med <integer>}
{-community BGP community list <0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -route-preference 100
-asn-prepend-type local-asn -asn-prepend-count 2 -med 100 -community
9000:900,8000:800
```

範例2：使用自動預設路由建立對等群組

```
network bgp peer-group create -peer-group <group_name> -ipspace
<ipspace_name> -bgp-lif <bgp_lif> -peer-address <peer-router_ip_address>
-peer-asn <peer_asn_number> {-use-peer-as-next-hop true} {-route-
preference <integer>} {-asn-prepend-type <ASN_prepend_type>} {-asn-
prepend-count <integer>} {-med <integer>} {-community BGP community list
<0-65535>:<0-65535>}
```

```
network bgp peer-group create -peer-group group1 -ipspace Default -bgp
-lif bgp1 -peer-address 10.10.10.1 -peer-asn 65503 -use-peer-as-next-hop
true -route-preference 100 -asn-prepend-type local-asn -asn-prepend
-count 2 -med 100 -community 9000:900,8000:800
```

範例 3 ：建立啟用 MD5 的對等群組

a. 啟用IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

b. 建立啟用 MD5 的 BGP 對等群組：

   ```
   network bgp peer-group create -ipspace Default -peer-group
   <group_name> -bgp-lif bgp_lif -peer-address <peer_router_ip_address>
   {-md5-enabled true} {-md5-secret <md5 secret in string or hex format>}
   ```

   使用十六進位金鑰的範例：

   ```
   network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
   -lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret
   0x746573742073656372657
   ```

   使用字串的範例：

```
network bgp peer-group create -ipspace Default -peer-group peer1 -bgp
-lif bgp_lif1 -peer-address 10.1.1.100 -md5-enabled true -md5-secret "test
secret"
```

建立 BGP 對等群組之後，執行命令時會列出虛擬乙太網路連接埠（以 v0a.v0z ， v1a… 開頭）`network port show`。此介面的 MTU 一律以 1500 報告。用於流量的實際 MTU 是從實體連接埠（ BGP LIF ）衍生而來，此連接埠是在流量傳送時決定的。如"指令參考資料ONTAP"需詳細`network port show`資訊，請參閱。

建立虛擬IP（VIP）資料LIF

VIP資料LIF是透過路由傳輸協定邊界閘道傳輸協定（BGP）通告給對等路由器。

開始之前

- 必須設定BGP對等群組、且要建立LIF的SVM之BGP工作階段必須處於作用中狀態。
- 必須為 SVM 的任何傳出 VIP 流量建立通往 BGP 路由器或 BGP LIF 子網路中任何其他路由器的靜態路由。
- 您應該開啟多重路徑路由，以便傳出的 VIP 流量可以使用所有可用的路由。

  如果未啟用多重路徑路由、則所有傳出的VIP流量都會從單一介面發出。

步驟

1. 建立VIP資料LIF：

```
network interface create -vserver <svm_name> -lif <lif_name> -role data
-data-protocol
{nfs|cifs|iscsi|fcache|none|fc-nvme} -home-node <home_node> -address
<ip_address> -is-vip true -failover-policy broadcast-domain-wide
```

   如果您未使用指定主連接埠、則會自動選取 VIP 連接埠 `network interface create` 命令。

   根據預設、VIP資料LIF屬於系統建立的每個IPspace名為「VIP」的廣播網域。您無法修改VIP廣播網域。

   VIP資料LIF可同時在裝載BGP LIF IP空間的所有連接埠上存取。如果本機節點上的VIP SVM沒有作用中的BGP工作階段、則VIP資料LIF會容錯移轉至節點上已針對該SVM建立BGP工作階段的下一個VIP連接埠。

2. 驗證BGP工作階段是否處於VIP資料LIF SVM的UP狀態：

```
network bgp vserver-status show

Node        Vserver  bgp status
          ----------  -------- ---------
          node1       vs1      up
```

如果 BGP 狀態為 `down` 對於節點上的 SVM 、 VIP 資料 LIF 會容錯移轉至另一個節點、而該節點的 BGP 狀態是 SVM 的正常狀態。如果 BGP 狀態為 `down` 在所有節點上、 VIP 資料 LIF 無法在任何位置託管、且 LIF 狀態為「關閉」。

管理**BGP**的命令

從 ONTAP 9.5 開始、您可以使用 `network bgp` 用於管理 ONTAP 中 BGP 工作階段的命令。

管理**BGP**組態

如果您想要…	使用此命令…
建立BGP組態	`network bgp config create`
修改BGP組態	`network bgp config modify`
刪除BGP組態	`network bgp config delete`
顯示BGP組態	`network bgp config show`
顯示VIP LIF SVM的BGP狀態	`network bgp vserver-status show`

管理**BGP**預設值

如果您想要…	使用此命令…
修改BGP預設值	`network bgp defaults modify`
顯示BGP預設值	`network bgp defaults show`

管理**BGP**對等群組

如果您想要…	使用此命令…
建立BGP對等群組	`network bgp peer-group create`
修改BGP對等群組	`network bgp peer-group modify`
刪除BGP對等群組	`network bgp peer-group delete`
顯示BGP對等群組資訊	`network bgp peer-group show`
重新命名BGP對等群組	`network bgp peer-group rename`

使用 **MD5** 管理 **BGP** 對等群組

從 ONTAP 9 。 16.1 開始，您可以在現有的 BGP 對等群組上啟用或停用 MD5 驗證。

> 如果您在現有的 BGP 對等群組上啟用或停用 MD5 ，則 BGP 連線會終止並重新建立，以套用 MD5 組態變更。

如果您想要…	使用此命令…

在現有的 BGP 對等群組上啟用 MD5	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -peer-address <peer_router_ip_address> -md5-enabled true -md5-secret <md5 secret in string or hex format>`
在現有的 BGP 對等群組上停用 MD5	`network bgp peer-group modify -ipspace Default -peer-group <group_name> -bgp -lif <bgp_lif> -md5-enabled false`

相關資訊

- "指令參考資料ONTAP"
- "網路 BGP"
- "網路介面"
- "安全性IPsec組態修改"

平衡網路負載

使用 **DNS** 負載平衡最佳化 **ONTAP** 網路流量

您可以將叢集設定為從適當載入的lifs處理用戶端要求。如此一來、生命與連接埠的使用率就會更加平衡、進而提升叢集的效能。

DNS負載平衡有助於選擇適當負載的資料LIF、並平衡所有可用連接埠（實體、介面群組和VLAN）之間的使用者網路流量。

透過DNS負載平衡、LIF會與SVM的負載平衡區域建立關聯。站台範圍的DNS伺服器已設定為轉送所有DNS要求、並根據網路流量和連接埠資源的可用度（CPU使用率、處理量、開放式連線等）、傳回負載最低的LIF。DNS負載平衡具有下列優點：

- 新的用戶端連線在可用資源之間取得平衡。
- 無需手動介入、即可決定在掛載特定SVM時要使用哪些LIF。
- DNS 負載平衡支援 NFSv3 、 NFSv4 、 NFSv4.1 、 SMB 2.0 、 SMB 2.1 、 SMB 3.0 和 S3 。

瞭解 **ONTAP** 網路的 **DNS** 負載平衡

用戶端可藉由指定IP位址（與LIF關聯）或主機名稱（與多個IP位址關聯）來掛載SVM。依預設、整個站台的DNS伺服器會以循環配置資源的方式選取生命體、以平衡所有生命體的工作負載。

循環資源負載平衡可能會導致部分生命量過載、因此您可以選擇使用DNS負載平衡區域來處理SVM中的主機名稱解析。使用DNS負載平衡區域、可確保新用戶端連線在可用資源之間取得更好的平衡、進而提升叢集的效能。

DNS負載平衡區域是叢集內的DNS伺服器、可動態評估所有LIF上的負載、並傳回適當載入的LIF。在負載平衡區域中、DNS會根據負載、為每個LIF指派權重（度量）。

每個LIF都會根據其主節點的連接埠負載和CPU使用率來指派一個權重。負載較少的連接埠上的LIF在DNS查詢中傳回的機率較高。您也可以手動指派權重。

為 ONTAP 網路建立 DNS 負載平衡區域

您可以建立DNS負載平衡區域、以便根據負載（即LIF上掛載的用戶端數目）、動態選擇LIF。您可以在建立資料LIF時建立負載平衡區域。

開始之前

站台範圍DNS伺服器上的DNS轉寄站必須設定為將負載平衡區域的所有要求轉送到設定的LIF。

這"NetApp知識庫：如何在叢集模式下設定 DNS 負載平衡"包含有關使用條件轉送配置 DNS 負載平衡的詳細資訊。

關於這項工作

- 任何資料LIF都能回應DNS查詢、以取得DNS負載平衡區域名稱。
- DNS負載平衡區域在叢集中必須有唯一的名稱、而且區域名稱必須符合下列需求：
  - 不得超過256個字元。
  - 其中應至少包含一段期間。
  - 第一個和最後一個字元不應為句點或任何其他特殊字元。
  - 字元之間不得包含任何空格。
  - DNS名稱中的每個標籤不得超過63個字元。

    標籤是指在期間之前或之後出現的文字。例如、名稱為storage.company.com的DNS區域有三個標籤。

步驟

使用 `network interface create`命令搭配 `dns-zone`選項來建立 DNS 負載平衡區域。如"指令參考資料ONTAP"需詳細 `network interface create`資訊，請參閱。

如果負載平衡區域已存在、則會將LIF新增至該區域。

下列範例示範如何在建立 LIF 時建立名為 storage.company.com 的 DNS 負載平衡區域 `lif1`：

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

從負載平衡區域新增或移除 ONTAP LIF

您可以從虛擬機器（SVM）的DNS負載平衡區域新增或移除LIF。您也可以從負載平衡區域同時移除所有的LIF。

開始之前

- 負載平衡區域中的所有LIF都應該屬於同一個SVM。

- LIF只能是一個DNS負載平衡區域的一部分。
- 如果生命體屬於不同的子網路、則必須設定每個子網路的容錯移轉群組。

關於這項工作

處於管理中斷狀態的LIF會從DNS負載平衡區域中暫時移除。當LIF返回管理UP狀態時、LIF會自動新增至DNS負載平衡區域。

步驟

在負載平衡區域中新增LIF或移除LIF：

如果您想要...	輸入...

新增LIF	`network interface modify -vserver vserver_name -lif lif_name -dns-zone zone_name`
	範例：
	`network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

移除單一LIF	`network interface modify -vserver vserver_name -lif lif_name -dns-zone none`
	範例：
	`network interface modify -vserver vs1 -lif data1 -dns -zone none`

移除所有生命	`network interface modify -vserver vserver_name -lif * -dns-zone none`
	範例：
	`network interface modify -vserver vs0 -lif * -dns-zone none`
	您可以從負載平衡區域移除 SVM 中的所有生命負載、以移除 SVM 中的 SVM 。

相關資訊

- "修改網路介面"

設定 ONTAP 網路的 DNS 服務

在建立NFS或SMB伺服器之前、您必須先為SVM設定DNS服務。一般而言、DNS名稱伺服器是NFS或SMB伺服器要加入之網域的Active Directory整合式DNS伺服器。

關於這項工作

Active Directory整合式DNS伺服器包含網域LDAP和網域控制器伺服器的服務位置記錄（SRV),如果SVM找不到Active Directory LDAP伺服器和網域控制器、NFS或SMB伺服器設定就會失敗。

SVM使用主機名稱服務ns-交換器資料庫來判斷要使用哪些名稱服務、以及在查詢主機資訊時的順序。主機資料庫支援的兩種名稱服務為檔案和DNS。

在建立SMB伺服器之前、您必須確定DNS是其中一個來源。

若要檢視mgwd程序和SecD程序的DNS名稱服務統計資料、請使用統計資料UI。

步驟

1. 判斷主機名稱服務資料庫目前的組態為何。在此範例中、主機名稱服務資料庫會使用預設設定。

   `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 如有必要、請執行下列動作。

   a. 依所需順序將DNS名稱服務新增至主機名稱服務資料庫、或重新排序來源。

      在此範例中、主機資料庫會設定為依該順序使用DNS和本機檔案。

      `vserver services name-service *ns-switch* modify -vserver *vs1* -database *hosts* -sources *dns,files*`

   b. 驗證名稱服務組態是否正確。

      `vserver services name-service *ns-switch* show -vserver *vs1* -database *hosts*`

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. 設定DNS服務。

   `vserver services name-service dns create -vserver *vs1* -domains *example.com,example2.com* -name-servers *10.0.0.50,10.0.0.51*`

   vserver services name-service DNS create命令會執行自動組態驗證、並在ONTAP 無法聯絡名稱伺服器時回報錯誤訊息。

4. 確認DNS組態正確、且服務已啟用。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. 驗證名稱伺服器的狀態。

```
vserver services name-service dns check -vserver vs1
```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

在SVM上設定動態DNS

如果您想要Active Directory整合式DNS伺服器在DNS中動態登錄NFS或SMB伺服器的DNS記錄、則必須在SVM上設定動態DNS（DDNS）。

開始之前

必須在SVM上設定DNS名稱服務。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器、而且必須為SVM建立NFS或SMB伺服器或Active Directory帳戶。

關於這項工作

指定的完整網域名稱（FQDN）必須是唯一的：

指定的完整網域名稱（FQDN）必須是唯一的：

- 若為 NFS 、則為中指定的值 `-vserver-fqdn` 作為的一部分 `vserver services name-service dns dynamic-update` 命令會成為已註冊的 FQDN 。
- 對於SMB、指定為CIFS伺服器的NetBios名稱和CIFS伺服器完整網域名稱的值、會成為該LIF的註冊FQDN。這在ONTAP 不進行設定的情況下無法進行。在下列案例中、LIF FQDN為「CIFS_VS1.EXAMPLE.COM":」

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

若要避免SVM FQDN組態失敗、但不符合DDNS更新的RFC規則、請使用符合RFC規範的FQDN名稱。如需詳細資訊、請參閱 "RFC 1123"。

步驟

1. 在SVM上設定DDNS：

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   星號無法作為自訂FQDN的一部分使用。例如、 `*.netapp.com` 無效。

2. 確認DDNS組態正確：

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

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

設定 **ONTAP** 網路的動態 **DNS** 服務

如果您想要Active Directory整合式DNS伺服器在DNS中動態登錄NFS或SMB伺服器的DNS記錄、則必須在SVM上設定動態DNS（DDNS）。

開始之前

必須在SVM上設定DNS名稱服務。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器、而且必須為SVM建立NFS或SMB伺服器或Active Directory帳戶。

關於這項工作

指定的FQDN必須是唯一的。

> 若要避免SVM FQDN組態失敗、但不符合DDNS更新的RFC規則、請使用符合RFC規範的FQDN名稱。

步驟

1. 在SVM上設定DDNS：

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   星號無法作為自訂FQDN的一部分使用。例如、 `*.netapp.com` 無效。

2. 確認DDNS組態正確：

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

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

主機名稱解析

瞭解 ONTAP 網路的主機名稱解析

必須能夠將主機名稱轉譯為數字IP位址、才能存取用戶端及存取服務。ONTAP您必須設定儲存虛擬機器（SVM）、才能使用本機或外部名稱服務來解析主機資訊。支援設定外部DNS伺服器、或設定本機主機檔案以進行主機名稱解析。ONTAP

使用外部DNS伺服器時、您可以設定動態DNS（DDNS）、它會自動將新的或變更的DNS資訊從儲存系統傳送到DNS伺服器。如果沒有動態DNS更新、您必須在新系統上線或現有DNS資訊變更時、手動將DNS資訊（DNS名稱和IP位址）新增至識別的DNS伺服器。此程序緩慢且容易出錯。在災難恢復期間、手動設定可能會導致長時間停機。

設定 DNS 以進行 ONTAP 網路的主機名稱解析

您可以使用DNS存取本機或遠端來源以取得主機資訊。您必須設定DNS、才能存取其中一個或兩個來源。

必須能夠查詢主機資訊、才能正確存取用戶端。ONTAP您必須設定名稱服務、才能啟用ONTAP 支援功能、以存取本機或外部DNS服務來取得主機資訊。

ONTAP 會將名稱服務組態資訊儲存在相當於的表格中 `/etc/nsswitch.conf` UNIX 系統上的檔案。

使用外部**DNS**伺服器設定**SVM**和資料**LIF**以進行主機名稱解析

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。。 `vserver services name-service dns create` 如果只輸入一個 DNS 伺服器名稱、命令會發出警告。

關於這項工作

請參閱 設定動態DNS服務 如需在SVM上設定動態DNS的詳細資訊、

步驟

1. 在SVM上啟用DNS：

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

下列命令可啟用SVM VS1上的外部DNS伺服器：

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

ⓘ ° `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com
                                    Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

如需與 DNS 相關的服務原則資訊、請參閱 "更新版本中的生命與服務政策ONTAP"。

設定名稱服務交換器表以進行主機名稱解析

您必須正確設定名稱服務交換器表、才能啟用ONTAP 支援功能、以參考本機或外部名稱服務來擷取主機資訊。

開始之前

您必須決定要在環境中使用哪種名稱服務來進行主機對應。

步驟

1. 將必要的項目新增至名稱服務交換器表：

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. 驗證名稱服務交換器表格是否包含所需順序的預期項目：

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

範例

以下範例修改名稱服務交換器表格中的項目、讓 SVM VS1 先使用本機主機檔案、然後使用外部 DNS 伺服器來解析主機名稱：

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

用於管理 **ONTAP Hosts** 表的 **ONTAP** 命令

叢集管理員可以新增、修改、刪除及檢視管理儲存虛擬機器（SVM）主機表中的主機名稱項目。SVM管理員只能為指派的SVM設定主機名稱項目。

用於管理本機主機名稱項目的命令

您可以使用 `vserver services name-service dns hosts` 建立、修改或刪除 DNS 主機表格項目的命令。

當您建立或修改DNS主機名稱項目時、可以指定多個以逗號分隔的別名位址。

如果您想要...	使用此命令...
建立DNS主機名稱項目	`vserver services name-service dns hosts create`
修改DNS主機名稱項目	`vserver services name-service dns hosts modify`
刪除DNS主機名稱項目	`vserver services name-service dns hosts delete`

如需命令的詳細資訊 `vserver services name-service dns hosts` ，請參閱 "指令參考資料ONTAP"。

保護您的網路安全

使用 **FIPS** 為所有 **SSL** 連線設定 **ONTAP** 網路安全性

ONTAP 的所有 SSL 連線均符合聯邦資訊處理標準 (FIPS) 140-2。您可以開啟和關閉 SSL FIPS 模式，全域設定 SSL 協議，並關閉ONTAP中的任何弱密碼。

根據預設， ONTAP 上的 SSL 設為停用 FIPS 相容性，並啟用下列 TLS 通訊協定：

- TLSv1.3 （從 ONTAP 9.11.1 開始）
- TLSv1.2

先前的 ONTAP 版本預設啟用下列 TLS 通訊協定：

- TLSv1.1 （從 ONTAP 9.12.1 開始預設為停用）
- TLSv1 （從 ONTAP 9.8 開始預設為停用）

啟用SSL FIPS模式時、ONTAP 從靜止到外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

如果您想要系統管理員帳戶使用SSH公開金鑰來存取SVM、則必須先確認主機金鑰演算法受到支援、才能啟用SSL FIPS模式。

附註： ONTAP 主機金鑰演算法支援已在更新版本的版本中變更。

發行版ONTAP	支援的金鑰類型	不支援的金鑰類型
9.11.1 及更新版本	ECDSA-SHA2-nistp256	RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	SSH-DSS SSH-RSA

沒有支援金鑰演算法的現有SSH公開金鑰帳戶、必須先以支援的金鑰類型重新設定、才能啟用FIPS、否則系統管理員驗證將會失敗。

如需詳細資訊、請參閱 "啟用SSH公開金鑰帳戶"。

ONTAP 9.18.1 引入了對 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法的支持，用於 SSL，從而為抵禦未來潛在的量子電腦攻擊提供了額外的安全保障。這些演算法僅在以下情況下可用FIPS 已停用。當 FIPS 被停用且對等方支援時，將協商後量子加密演算法。

啟用 **FIPS**

建議所有安全的使用者在系統安裝或升級之後、立即調整其安全組態。啟用SSL FIPS模式時、ONTAP 從靜止到外部用戶端或ONTAP 伺服器元件的SSL通訊、將使用FIPS相容的SSL加密。

啟用FIPS時、您無法安裝或建立RSA金鑰長度為4096的憑證。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 啟用 FIPS ：

   ```
   security config modify * -is-fips-enabled true
   ```

3. 當系統提示您繼續時、請輸入 `y`

4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。

範例

如果您執行ONTAP 的是更新版本的版本、則不會看到警告訊息。

```
security config modify -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

如"指令參考資料ONTAP"需有關及 SSL FIPS 模式組態的詳細 `security config modify`資訊，請參閱。

停用**FIPS**

從ONTAP 9.18.1 開始， ONTAP中的 SSL 支援 ML-KEM、ML-DSA 和 SLH-DSA 後量子計算加密演算法。只有在禁用 FIPS 且對等方支援這些演算法時，這些演算法才可用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令來停用FIPS：

   ```
   security config modify -is-fips-enabled false
   ```

3. 當系統提示您繼續時、請輸入 `y`。
4. 從ONTAP 9.9.1 開始，不需要重新啟動。如果您執行的是ONTAP 9.8 或更早版本，請手動重新啟動叢集中的每個節點。

如果您需要使用 SSLv3 協議，則必須依照上述步驟停用 FIPS。只有在停用 FIPS 的情況下才能啟用 SSLv3。

您可以使用以下命令啟用 SSLv3。如果您執行的是ONTAP 9.9.1 或更高版本，則不會看到此警告訊息。

```
security config modify -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

檢視**FIPS**法規遵循狀態

您可以查看整個叢集是否正在執行目前的安全性組態設定。

步驟

1. 如果您執行的是ONTAP 9.8 或更早版本，請手動逐一重新啟動叢集中的每個節點。
2. 檢視目前的法規遵循狀態：

   `security config show`

   ```
   cluster1::> security config show
   Cluster    Supported
   FIPS Mode  Protocols Supported Cipher Suites
   ---------- ---------
   ------------------------------------------------------------
   false      TLSv1.3,  TLS_RSA_WITH_AES_128_CCM,
   TLS_RSA_WITH_AES_128_CCM_8,
              TLSv1.2   TLS_RSA_WITH_AES_128_GCM_SHA256,
                        TLS_RSA_WITH_AES_128_CBC_SHA,
                        TLS_RSA_WITH_AES_128_CBC_SHA256,
   TLS_RSA_WITH_AES_256_CCM,
                        TLS_RSA_WITH_AES_256_CCM_8,
                        ...
   ```

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

相關資訊

- "FIPS 203：基於模組格的金鑰封裝機制標準（ML-KEM）"
- "FIPS 204：基於模組格的數位簽章標準（ML-DSA）"

- "FIPS 205：無狀態雜湊數位簽章標準 (SLH-DSA)"

設定 IPsec 在線上加密

準備在 ONTAP 網路上使用 IP 安全性

從 ONTAP 9 8 開始，您可以選擇使用 IP 安全性（ IPsec ）來保護網路流量。IPsec 是 ONTAP 提供的數種資料傳輸或傳輸中加密選項之一。在正式作業環境中使用 IPsec 之前，您應該做好設定的準備。

ONTAP 中的 IP 安全實作

IPsec 是由 IETF 維護的網際網路標準。它提供資料加密與完整性，以及 IP 層級網路端點之間流量傳輸的驗證。

使用 ONTAP 時， IPsec 可保護 ONTAP 和各種用戶端之間的所有 IP 流量，包括 NFS ， SMB 和 iSCSI 傳輸協定。除了隱私權和資料完整性之外，網路流量還能防範多種攻擊，例如重播和攔截式攻擊。ONTAP 使用 IPsec 傳輸模式實作。它利用網際網路金鑰交換（ IKE） 傳輸協定第 2 版，在 ONTAP 和使用 IPv4 或 IPv6 的用戶端之間協商金鑰資料。

當叢集上啟用 IPsec 功能時，網路需要 ONTAP 安全性原則資料庫（ SPD ）中的一或多個項目，才能符合各種流量特性。這些項目會對應至處理及傳送資料所需的特定保護詳細資料（例如密碼套件和驗證方法）。每個用戶端也需要對應的 SPD 項目。

對於某些類型的流量，最好使用另一個資料傳輸加密選項。例如，對於 NetApp SnapMirror 和叢集對等流量的加密，一般建議使用傳輸層安全性（ TLS ）傳輸協定，而非 IPsec 。這是因為 TLS 在大多數情況下都能提供更好的效能。

相關資訊

- "網際網路工程工作團隊"
- "RFC 4301-Security Architecture for the Internet Protocol （網際網路傳輸協定的安全架構）"

ONTAP IPsec 實作的演進

IPsec 最初是在ONTAP 9.8 中引入的。該實現在後續ONTAP版本中不斷發展，如下所述。

ONTAP 9.18.1

IPsec硬體卸載支援已擴展到IPv6流量。

ONTAP 9.17.1

IPsec 硬體卸載支援擴充至"鏈路聚合組" 。"後量子預共享密鑰（PPK）"支援 IPsec 預共用金鑰 (PSK) 驗證。

ONTAP 9.16.1.

加密和完整性檢查等多項密碼編譯作業可卸載至支援的 NIC 卡。如需詳細資訊、請參閱 IPsec 硬體卸載功能 。

ONTAP 9.12.1

MetroCluster IP 和 MetroCluster 網路附加組態提供 IPsec 前端主機傳輸協定支援。MetroCluster 叢集所提供的 IPsec 支援僅限於前端主機流量， MetroCluster 叢集間的生命體不受支援。

零點9.10.1 ONTAP

除了 PSK 之外，憑證還可用於 IPsec 驗證。在ONTAP 9.10.1 之前的版本中，僅支援使用 PSK 進行身份驗證。

部分**9.9.1 ONTAP**

IPsec 使用的加密演算法已通過 FIPS 140-2 驗證。這些演算法由 ONTAP 中的 NetApp 密碼編譯模組處理，該模組執行 FIPS 140-2 驗證。

部分**9.8 ONTAP**

根據傳輸模式實作， IPsec 的支援一開始就可用。

IPsec 硬體卸載功能

如果您使用的是 ONTAP 9 。 16.1 或更新版本，您可以選擇將某些運算密集的作業（例如加密和完整性檢查）卸載到儲存節點上安裝的網路介面控制器（ NIC ）卡。卸載到 NIC 卡的作業處理量約為 5% 或更低。這可大幅改善受 IPsec 保護的網路流量的效能和處理量。

要求與建議

在使用 IPsec 硬體卸載功能之前，您應該考量幾項需求。

支援的乙太網路卡

您只需安裝並使用受支援的乙太網路卡。從ONTAP 9.16.1 開始，支援以下乙太網路卡：

- X50131A （ 2p ， 40G/100g/200g/400G 乙太網路控制器）
- X60132A （ 4p ， 10G/25G 乙太網路控制器）

ONTAP 9.17.1 增加了對以下乙太網路卡的支援：

- X50135A（2p，40G/100G乙太網路控制器）
- X60135A（2p，40G/100G乙太網路控制器）

以下平台支援 X50131A 和 X50135A 卡：

- ASA A1K
- ASA A90
- ASA A70
- AFF A1K
- AFF A90
- AFF A70

以下平台支援 X60132A 和 X60135A 卡：

- ASA A50
- ASA A30
- ASA A20
- AFF A50
- AFF A30
- AFF A20

查看"NetApp Hardware Universe"有關支援的平台和卡片的更多資訊。

叢集範圍

IPsec 硬體卸載功能是針對叢集進行全域設定。例如，此命令會 `security ipsec config`套用至叢集中的所有節點。

一致的組態

支援的 NIC 卡應安裝在叢集中的所有節點上。如果支援的 NIC 卡只能在某些節點上使用，則當容錯移轉後，如果部分生命負載未裝載於具有卸載功能的 NIC 上，您就會發現效能大幅降低。

停用反重播

您必須停用 ONTAP （預設組態）和 IPsec 用戶端上的 IPsec 反重新執行保護。如果未停用，將不支援分割和多重路徑（備援路由）。

如果 ONTAP IPsec 組態已從預設變更為啟用反重新執行保護，請使用此命令將其停用：

```
security ipsec config modify -replay-window 0
```

您必須確定用戶端上的 IPsec 反重新執行保護已停用。請參閱用戶端的 IPsec 文件，以停用反重播保護。

限制

在使用 IPsec 硬體卸載功能之前，您應該考慮幾項限制。

IPv6

從ONTAP 9.18.1 開始，IPsec 硬體卸載功能支援 IPv6。在ONTAP 9.18.1 之前的版本中，IPsec 硬體卸載不支援 IPv6。

延伸序號

硬體卸載功能不支援 IPsec 延伸序列號。僅使用正常的 32 位元序列號。

連結集合體

從ONTAP 9.17.1 開始，您可以將 IPsec 硬體卸載功能與"鏈路聚合組" 。

在 9.17.1 之前的版本中，IPsec 硬體卸載功能不支援連結聚合。它不能與通過 `network port ifgrp` ONTAP CLI 中的指令。

ONTAP CLI 中的組態支援

ONTAP 9 。 16.1 中更新了三個現有的 CLI 命令，以支援以下所述的 IPsec 硬體卸載功能。如需詳細資訊，請參閱"在 ONTAP 中設定 IP 安全性"。

指令**ONTAP**	更新
`security ipsec config show`	布林參數 `Offload Enabled`顯示目前的 NIC 卸載狀態。
`security ipsec config modify`	此參數 `is-offload-enabled`可用於啟用或停用 NIC 卸載功能。
`security ipsec config show-ipsecsa`	新增了四個新的計數器，以位元組和封包顯示傳入和傳出流量。

ONTAP REST API 中的組態支援

ONTAP 9 中更新了兩個現有的 REST API 端點。 16.1 可支援 IPsec 硬體卸載功能，如下所述。

REST端點	更新
`/api/security/ipsec`	此參數 `offload_enabled`已新增，可透過修補方法使用。
`/api/security/ipsec/security_association`	新增兩個計數器值，以追蹤卸載功能處理的總位元組和封包數。

從 ONTAP 自動化文件中深入瞭解 ONTAP REST API ，包括 "ONTAP REST API 的新功能"。您也應該檢閱 ONTAP 自動化文件，以取得有關的詳細資訊 "IPsec 端點"。

相關資訊

- "安全 IPSEC"

設定 ONTAP 網路的 IP 安全性

在 ONTAP 叢集上設定及啟動 IPsec 進行中加密需要執行數項工作。

設定 IPsec 之前，請務必先檢閱"準備使用 IP 安全性"。例如，您可能需要決定是否使用以 ONTAP 9 開頭的可用 IPsec 硬體卸載功能。 16.1

在叢集上啟用IPsec

您可以在叢集上啟用 IPsec ，以確保資料在傳輸過程中持續加密且安全。

步驟

1. 探索是否已啟用IPsec：

   ```
   security ipsec config show
   ```

   如果結果包括 `IPsec Enabled: false`，繼續下一步。

2. 啟用IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

   您可以使用布爾參數來啟用 IPsec 硬體卸載功能 `is-offload-enabled`。

3. 再次執行探索命令：

   ```
   security ipsec config show
   ```

   現在的結果包括 `IPsec Enabled: true`。

準備使用憑證驗證建立 IPsec 原則

如果您只使用預先共用金鑰（ PSK ）進行驗證、而且不會使用憑證驗證、則可以略過此步驟。

在建立使用憑證進行驗證的 IPsec 原則之前、您必須確認符合下列先決條件：

- ONTAP 和用戶端都必須安裝另一方的 CA 憑證、以便雙方可驗證終端實體（ ONTAP 或用戶端）憑證
- 系統會為ONTAP 參與該原則的Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the Sfor the

可共享證書的產品。ONTAP不需要在憑證與lifs之間建立一對一對應關係。

步驟

1. 除非已安裝 ONTAP 憑證管理（例如 ONTAP 自我簽署的根 CA ）、否則請將在相互驗證期間使用的所有 CA 憑證（包括 ONTAP 端和用戶端 CA ）安裝到憑證管理。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server-ca
     -cert-name my_ca_cert
     ```
2. 若要確保在驗證期間安裝的 CA 位於 IPsec CA 搜尋路徑內、請使用將 ONTAP 憑證管理 CA 新增至 IPsec 模組 `security ipsec ca-certificate add` 命令。
   - 命令範例 *
     ```
     cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
     my_ca_cert
     ```
3. 建立並安裝認證以供ONTAP 《Sfor the Suse LIF（供《Sfor the Suse：此憑證的發卡行CA必須已安裝ONTAP 至ESA並新增至IPsec。
   - 命令範例 *
     ```
     cluster::> security certificate install -vserver svm_name -type server -cert
     -name my_nfs_server_cert
     ```

如需ONTAP 更多有關資訊、請參閱ONTAP 《》介紹文件中的安全認證命令。

定義安全性原則資料庫（**SPD**）

在允許流量在網路上傳輸之前、IPsec需要SPD項目。無論您使用的是用於驗證的PSK或憑證、都是如此。

步驟

1. 使用 `security ipsec policy create` 命令至：
   a. 選取ONTAP 要參與IPsec傳輸的IP位址或子網路。
   b. 選取要連線ONTAP 至「靜態IP位址」的用戶端IP位址。

      用戶端必須使用預先共用金鑰（PSK）來支援網際網路金鑰交換版本2（IKEv2）。

   c. 可選擇細粒度的流量參數，例如上層協定（UDP、TCP、ICMP 等）、本機連接埠號碼和遠端連接埠號，以保護流量。對應的參數如下 `protocols` ， `local-ports`和 `remote-ports`分別。

      跳過此步驟以保護ONTAP 所有介於整個過程中的資訊流量、例如：靜態IP位址和用戶端IP位址。保護所有流量是預設設定。

   d. 輸入的 PSK 或公開金鑰基礎架構（ PKI ） `auth-method` 所需驗證方法的參數。
      i. 如果您輸入一個 PSK 、請包含參數、然後按 <enter> 鍵提示您輸入並驗證預先共用金鑰。

`local-identity`如果主機和用戶端都使用強化天鵝，而且沒有為主機或用戶端選取萬用字元原則，則和 `remote-identity`參數是選用的。

ii. 如果您輸入 PKI 、也需要輸入 `cert-name`、 `local-identity`、 `remote-identity` 參數。如果遠端端憑證身分不明、或是需要多個用戶端身分識別、請輸入特殊身分識別 `ANYTHING`。

e. 從ONTAP 9.17.1 開始，可以選擇輸入後量子預共享金鑰 (PPK) 身份 `ppk-identity`參數。 PPK提供了額外的安全保障，以抵禦未來潛在的量子電腦攻擊。輸入 PPK 身分時，系統會提示您輸入 PPK 金鑰。PPK僅支援 PSK 身份驗證。

詳細了解 `security ipsec policy create`在"指令參考資料ONTAP" 。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

除非 ONTAP 和用戶端都設定了相符的 IPsec 原則、而且雙方都有驗證認證（可以是 PSK 或憑證）、否則 IP 流量無法在用戶端和伺服器之間傳輸。

使用**IPsec**身分識別

對於預先共用金鑰驗證方法、如果主機和用戶端都使用強化天鵝、而且沒有為主機或用戶端選取萬用字元原則、則本機和遠端身分識別是選用的。

對於公開密碼匙基礎建設/憑證驗證方法、本機和遠端身分識別都是必要的。身分識別會指定在每一方憑證中認證的身分識別、並用於驗證程序。如果遠端身分識別不明、或是可能有許多不同的身分識別、請使用特殊身分識別 `ANYTHING`。

關於這項工作

在不受限的情況下、可透過修改SPD項目或在SPD原則建立期間來指定身分識別。ONTAPSPD可以是IP位址或字串格式身分識別名稱。

步驟

1. 使用下列命令修改現有的 SPD 身分識別設定：

```
security ipsec policy modify
```

命令範例

```
security ipsec policy modify -vserver vs1 -name test34 -local-identity
192.168.134.34 -remote-identity client.fooboo.com
```

IPsec多個用戶端組態

當少數用戶端需要使用IPsec時、每個用戶端只需使用一個SPD項目就足夠了。但是、當數百甚至數千個用戶端需要使用IPsec時、NetApp建議使用IPsec多重用戶端組態。

關於這項工作

支援將多個網路上的多個用戶端連線至單一SVM IP位址、並啟用IPsec。ONTAP您可以使用下列其中一種方法來達成此目的：

- 子網路組態

  若要允許特定子網路上的所有用戶端（例如 192.168.134.0/24 ）使用單一 SPD 原則項目連線到單一 SVM IP 位址、您必須指定 `remote-ip-subnets` 子網路形式。此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。

  > 在子網路組態中使用單一原則項目時、該子網路中的IPsec用戶端會共用IPsec身分識別和預先共用金鑰（PSK）。不過、憑證驗證並不符合此要求。使用憑證時、每個用戶端都可以使用自己的唯一憑證或共用憑證進行驗證。IPsec會根據安裝在本機信任存放區上的CA來檢查憑證的有效性。ONTAP支援憑證撤銷清單（CRL）檢查。ONTAP

- 允許所有用戶端組態

  若要允許任何用戶端連線至 SVM IPsec 啟用的 IP 位址、無論其來源 IP 位址為何、請使用 `0.0.0.0/0` 指定時使用萬用字元 `remote-ip-subnets` 欄位。

  此外、您必須指定 `remote-identity` 具有正確用戶端身分識別的欄位。對於憑證驗證、您可以輸入 `ANYTHING`。

  此外、當 `0.0.0.0/0` 使用萬用字元時、您必須設定要使用的特定本機或遠端連接埠號碼。例如、 `NFS port 2049`。

  步驟

  a. 使用下列其中一個命令來設定多個用戶端的 IPsec 。

     i. 如果您使用 * 子網路組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     命令範例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. 如果您使用 * 允許所有用戶端組態 * 來支援多個 IPsec 用戶端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

命令範例

```
security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
-identity ontap_side_identity -remote-identity client_side_identity
```

顯示 IPsec 統計資料

透過協商、ONTAP 可在「穩定SVM IP位址」和「用戶端IP位址」之間建立稱為「IKE安全性關聯」（SA）的安全通道。兩個端點都安裝了IPsec SAS、以執行實際的資料加密與解密工作。您可以使用統計資料命令來檢查IPsec SAS和IKE SAS的狀態。

如果您使用 IPsec 硬體卸載功能，則會使用命令顯示數個新的計數器 `security ipsec config show-ipsecsa`。

命令範例

IKE SA命令範例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA命令和輸出範例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

相關資訊

- "安全性憑證安裝"
- "安全 IPSEC"

配置ONTAP後端集群網路加密

從ONTAP 9.18.1 開始，您可以為後端叢集網路上的傳輸中資料配置傳輸層安全性 (TLS) 加密。此加密技術可在後端叢集網路上的ONTAP節點之間傳輸客戶資料時，保護儲存在ONTAP中的客戶資料。

關於這項工作

- 後端集群網路加密預設為停用狀態。
- 啟用後端叢集網路加密後，儲存在ONTAP中的所有客戶資料在後端叢集網路上的ONTAP節點之間傳輸時都會被加密。集群網路的部分流量（例如控制路徑資料）未加密。
- 預設情況下，後端叢集網路加密將使用叢集中每個節點自動產生的憑證。你可以[管理集群網路加密證書]每個節點都使用自訂安裝的憑證。

開始之前

- 您必須是ONTAP管理員。 `admin`執行下列任務所需的權限等級。
- 叢集中的所有節點必須執行ONTAP 9.18.1 或更高版本才能啟用後端叢集網路加密。

啟用或停用叢集網路通訊加密

步驟

1. 查看目前集群網路加密狀態：

```
security cluster-network show
```

此命令顯示集群網路加密的目前狀態：

```
Cluster-1::*> security cluster-network show

Enabled: true

Mode: tls

Status: READY
```

2. 啟用或停用TLS後端叢集網路加密：

```
security cluster-network modify -enabled <true|false>
```

此命令啟用或停用後端叢集網路上客戶傳輸資料的加密通訊。

管理集群網路加密證書

1. 查看目前集群網路加密證書資訊：

```
security cluster-network certificate show
```

此命令顯示目前集群網路加密證書資訊：

```
security cluster-network certificate show
Node                  Certificate Name                       CA
--------------------- -------------------------------------
--------------
node1                 -                                      Cluster-
1_Root_CA
node2                 -                                      Cluster-
1_Root_CA
node3                 google_issued_cert1                    Google_CA1
node4                 google_issued_cert2                    Google_CA1
```

叢集中每個節點的憑證和憑證授權單位 (CA) 名稱均已顯示。

2. 修改節點的叢集網路加密證書：

```
security cluster-network certificate modify -node <node_name> -name
<certificate_name>
```

此指令修改特定節點的叢集網路加密證書。在執行此命令之前，必須先安裝憑證並由已安裝的 CA 進行簽署。有關證書管理的更多信息，請參閱"使用系統管理員管理 ONTAP 憑證"。如果 `-name`如果未指定，則使用自動產生的預設憑證。

在 ONTAP 網路中設定生命安全的防火牆原則

設定防火牆可增強叢集的安全性、並有助於防止未獲授權的存取儲存系統。根據預設、內建防火牆會設定為允許遠端存取特定的IP服務集、以供資料、管理及叢集間生命體使用。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。

- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

防火牆原則可用來控制對管理服務傳輸協定的存取、例如SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH、DNS或SNMP。無法為NFS或SMB等資料傳輸協定設定防火牆原則。

您可以使用下列方式來管理防火牆服務和原則：

- 啟用或停用防火牆服務
- 顯示目前的防火牆服務組態
- 使用指定的原則名稱和網路服務建立新的防火牆原則
- 將防火牆原則套用至邏輯介面
- 建立新的防火牆原則、該原則是現有原則的確切複本

  您可以使用這項功能、在同一個SVM中建立具有類似特性的原則、或將原則複製到不同的SVM。

- 顯示防火牆原則的相關資訊
- 修改防火牆原則所使用的IP位址和網路遮罩
- 刪除LIF未使用的防火牆原則

防火牆原則與生命

LIF防火牆原則是用來限制透過每個LIF存取叢集。您需要瞭解預設防火牆原則如何影響每種LIF類型的系統存取、以及如何自訂防火牆原則以提高或降低LIF的安全性。

使用 OR `network interface modify` 命令設定 LIF 時 `network interface create`，為參數指定的值會決定允許存取 LIF 的 `-firewall-policy`服務傳輸協定和 IP 位址。如"指令參考資料ONTAP"需詳細 `network interface`資訊，請參閱。

在許多情況下、您可以接受預設的防火牆原則值。在其他情況下、您可能需要限制特定IP位址和特定管理服務傳輸協定的存取。可用的管理服務傳輸協定包括SSH、HTTP、HTTPS、Telnet、NTP、 NDMP、NDMPS、RSH, DNS及SNMP。

所有叢集生命的防火牆原則預設為 `""` 且無法修改。

下表說明在ONTAP 建立LIF時指派給每個LIF的預設防火牆原則、具體取決於其角色（版本號為9.5或更早）或服務原則ONTAP （版本為9.6及更新版本）：

防火牆原則	預設服務傳輸協定	預設存取	LIF套用至
管理	DNS、http、https、NDMP、ndmps、 NTP、SNMP、ssh	任何位址（0.00.0.0/0）	叢集管理、SVM管理及節點管理生命里

MGMT-NFS	DNS、http、https、NDMP、ndmps、 NTP、portmap、SNMP、ssh	任何位址（0.00.0.0/0）	也支援SVM管理存取的資料生命量
叢集間	HTTPS、NDMP、ndmps	任何位址（0.00.0.0/0）	所有叢集間LIF
資料	DNS、NDMP、ndms、portmap	任何位址（0.00.0.0/0）	所有資料生命量

portmap服務組態

portmap服務會將RPC服務對應至其接聽的連接埠。

Portmap服務可在ONTAP 不間斷的情況下於更新版本中使用、ONTAP 從版本9.4到ONTAP 版本9.6均可設定、並從ONTAP 版本9.7開始自動管理。

- 在更新版本的版本中、連接埠對應服務（rpcbind）一律可在連接埠111上存取、因為網路組態必須仰賴內建的不只是第三方防火牆的功能。ONTAP ONTAP
- 從S得9.4到S得9.6、您可以修改防火牆原則、以控制portmap服務是否可在特定的生命期中存取。ONTAP ONTAP
- 從功能更新至功能更新至功能更新至功能更新至功能更新至功能更新。ONTAP而是會自動為所有支援NFS服務的LIF開啟portmap連接埠。
- Portmap服務可在ONTAP 防火牆內設定、範圍從版本9.4到ONTAP 版本9.6。*

本主題的其餘部分將討論如何設定ONTAP 從版本ONTAP 號至版本號之間的適用效能提升介面防火牆服務。

視組態而定、您可能無法在特定類型的生命期（通常是管理生命期和叢集間生命期）上存取服務。在某些情況下、您甚至可能無法存取資料生命期。

您可以期望的行為

從版本9.4到版本9.6的功能設計、可在升級時提供無縫轉換。ONTAP ONTAP如果已透過特定類型的lifs存取portmap服務、則可透過這些類型的lifs繼續存取。如同在 ONTAP 9.3 及更早版本中、您可以在 LIF 類型的防火牆原則中指定可在防火牆內存取的服務。

叢集中的所有節點都必須執行ONTAP 從功能上到ONTAP 功能上的從功能上的資訊、才能使行為生效。只有傳入流量會受到影響。

新規則如下：

- 升級至9.4到9.6版時ONTAP 、根據預設或自訂、將portmap服務新增至所有現有的防火牆原則。
- 建立新叢集或新的IPspace時ONTAP 、不將portmap服務新增至預設資料原則、而只新增至預設管理或叢集間原則。
- 您可以視需要將portmap服務新增至預設或自訂原則、並視需要移除服務。

如何新增或移除**portmap**服務

若要將portmap服務新增至SVM或叢集防火牆原則（可在防火牆內存取）、請輸入：

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

若要從SVM或叢集防火牆原則中移除portmap服務（使其在防火牆內無法存取）、請輸入：

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

您可以使用網路介面modify命令、將防火牆原則套用至現有的LIF。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立防火牆原則並將其指派給 LIF

當您建立LIF時、預設的防火牆原則會指派給每個LIF。在許多情況下、預設的防火牆設定運作良好、您不需要變更這些設定。如果您想要變更可存取LIF的網路服務或IP位址、可以建立自訂防火牆原則並將其指派給LIF。

關於這項工作

- 您無法使用建立防火牆原則 `policy` 名稱 `data`、 `intercluster`、 `cluster`或 `mgmt`。

  這些值保留給系統定義的防火牆原則。

- 您無法設定或修改叢集I生命 的防火牆原則。

  所有服務類型的叢集LIF防火牆原則都設為0.00.0.0/0。

- 如果您需要從原則中移除服務、則必須刪除現有的防火牆原則並建立新原則。
- 如果叢集上已啟用IPv6、您可以使用IPv6位址建立防火牆原則。

  啟用 IPv6 之後、 `data`、 `intercluster`和 `mgmt` 防火牆原則包括： /0 （ IPv6 萬用字元）在其接受的位址清單中。

- 使用System Manager設定跨叢集的資料保護功能時、您必須確保叢集間LIF IP位址包含在允許的清單中、而且叢集間LIF和公司擁有的防火牆都允許HTTPS服務。

  依預設 `intercluster` 防火牆原則允許從所有 IP 位址（ 0.0.0/0 或： /0 （ IPv6 ））存取、並啟用 HTTPS 、 NDMP 和 NDMPS 服務。如果您修改此預設原則、或是為叢集間LIF建立自己的防火牆原則、則必須將每個叢集間LIF IP位址新增至允許的清單、並啟用HTTPS服務。

- 從支援SJS9.6開始ONTAP 、不支援HTTPS和SSH防火牆服務。

  在 ONTAP 9.6 中 `management-https` 和 `management-ssh` LIF 服務可用於 HTTPS 和 SSH 管理存取。

步驟

1. 建立防火牆原則、讓特定SVM上的LIF可以使用：

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   您可以多次使用此命令、為防火牆原則中的每個服務新增多個網路服務和允許的IP位址清單。

2. 使用確認原則已正確新增 `system services firewall policy show` 命令。

3. 將防火牆原則套用至LIF：

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. 使用確認原則已正確新增至 LIF `network interface show -fields firewall-policy` 命令。

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

建立防火牆原則並將其指派給 **LIF** 的範例

下列命令會建立名為data_http的防火牆原則、以啟用從10.10子網路IP位址存取HTTP和HTTPS傳輸協定、將該原則套用至SVM VS1上名為data1的LIF、然後顯示叢集上的所有防火牆原則：

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

管理防火牆服務和原則的 ONTAP 命令

您可以使用 `system services firewall` 管理防火牆服務的命令 `system services firewall policy` 管理防火牆原則的命令、以及 `network interface modify` 管理生命的防火牆設定的命令。

從功能部分9.10.1開始ONTAP ：

- 防火牆原則已過時、並由LIF服務原則取代。之前、內建防火牆是使用防火牆原則來管理。此功能現在是使用LIF服務原則來完成。
- 所有的防火牆原則都是空的、而且不會開啟基礎防火牆中的任何連接埠。而是必須使用LIF服務原則開啟所有連接埠。
- 升級至9.10.1或更新版本、從防火牆原則轉換至LIF服務原則之後、不需要採取任何行動。系統會自動建構符合先前ONTAP 版本的防火牆原則的LIF服務原則。如果您使用指令碼或其他工具來建立及管理自訂防火牆原則、則可能需要升級這些指令碼、以建立自訂服務原則。

若要深入瞭解、請參閱 "更新版本中的生命與服務政策ONTAP"。

如果您想要...	使用此命令...
啟用或停用防火牆服務	`system services firewall modify`
顯示目前的防火牆服務組態	`system services firewall show`
建立防火牆原則或新增服務至現有的防火牆原則	`system services firewall policy create`
將防火牆原則套用至LIF	`network interface modify -lif lifname -firewall-policy`
修改與防火牆原則相關的IP位址和網路遮罩	`system services firewall policy modify`
顯示防火牆原則的相關資訊	`system services firewall policy show`
建立一個新的防火牆原則、該原則是現有原則的確切複本	`system services firewall policy clone`
刪除LIF未使用的防火牆原則	`system services firewall policy delete`

相關資訊

- "系統服務防火牆"
- "修改網路介面"

QoS 標記（僅限叢集管理員）

瞭解 ONTAP 網路服務品質（ QoS ）

網路服務品質（ QoS ）標記可協助您根據網路狀況，排列不同流量類型的優先順序，以有效使用網路資源。您可以針對每個IPspace所支援的流量類型、設定傳出IP封包的差異化服務程式碼點（Dscp）值。

針對**UC**法規遵循的**DSCP**標示

您可以使用預設或使用者提供的Dscp程式碼、在特定傳輸協定的傳出（出口）IP封包流量上啟用差異化服務程式碼點（Dscp）標記。DSCP標示是一種分類及管理網路流量的機制、也是統一化功能（UC）法規遵循的一項元件。

提供IPspace、傳輸協定及dscp值、即可啟用dscp標記（也稱為_qos標記_或_服務品質標記_）。可套用DSCP標示的傳輸協定為NFS、SMB、iSCSI、SnapMirror、NDMP、 FTP、HTTP/HTTPS、SSH、遠端登入和SNMP。

如果您在啟用指定傳輸協定的dscp標記時未提供dscp值、則會使用預設值：

- 資料傳輸協定/流量的預設值為0X0A（10）。
- 控制傳輸協定/流量的預設值為0x30（48）。

修改 ONTAP 網路 QoS 標記值

您可以針對每個IPspace修改不同傳輸協定的服務品質（QoS）標記值。

開始之前

叢集中的所有節點都必須執行相同版本ONTAP 的Sof the Sof。

步驟

使用修改 QoS 標記值 `network qos-marking modify` 命令。

- 。 `-ipspace` 參數指定要修改 QoS 標記項目的 IPspace 。
- 此 `–protocol`參數指定要修改 QoS 標記項目的通訊協定。
- 。 `-dscp` 參數指定差異化服務代碼點 (DSCP) 值。可能的值範圍從0到63。
- 。 `-is-enabled` 參數用於在提供的 IPspace 中啟用或停用指定傳輸協定的 QoS 標記 `-ipspace` 參數。

下列命令會在預設IPspace中啟用NFS傳輸協定的QoS標記：

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

下列命令會將預設IPspace中NFS傳輸協定的Dscp值設為20：

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

如"指令參考資料ONTAP"需更多關於 `network qos-marking modify`通訊協定的資訊和可能的值，請參閱。

檢視 ONTAP 網路 QoS 標記值

您可以針對每個IPspace顯示不同傳輸協定的QoS標記值。

步驟

使用顯示 QoS 標記值 `network qos-marking show` 命令。

下列命令會顯示預設IPspace中所有傳輸協定的QoS標記：

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
-------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

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

管理 SNMP （僅限叢集管理員）

瞭解 ONTAP 網路上的 SNMP

您可以設定SNMP來監控叢集中的SVM、以避免發生問題、並在問題確實發生時予以回應。管理SNMP包括設定SNMP使用者、以及為所有SNMP事件設定SNMP traphost目的地（管理工作站）。依預設、SNMP會在資料生命量上停用。

您可以在資料SVM中建立及管理唯讀SNMP使用者。資料生命期必須設定為在SVM上接收SNMP要求。

SNMP網路管理工作站（或管理程式）可以查詢SVM SNMP代理程式以取得資訊。SNMP代理程式會收集資訊並將其轉送給SNMP管理程式。SNMP代理程式也會在發生特定事件時產生設陷通知。SVM上的SNMP代理程式具有唯讀權限、無法用於任何設定作業或採取修正行動來回應陷阱。提供與SNMP v1、v2c和v3版本相容的SNMP代理程式。ONTAP使用密碼和加密技術、可提供進階的安全性。

如需ONTAP 更多有關支援SNMP的資訊、請參閱 "TR-4220：Data ONTAP 支援SNMP"。

MIB 總覽

mib（管理資訊庫）是描述SNMP物件和設陷的文字檔。

MIBs說明儲存系統管理資料的結構、並使用包含物件識別碼（OID）的階層式命名空間。每個oid都會識別可透過SNMP讀取的變數。

由於MIBs不是組態檔、ONTAP 而且無法讀取這些檔案、因此SNMP功能不受MIBs影響。提供下列的mib檔案：ONTAP

- NetApp 自訂 MIB (`netapp.mib`)

支援IPv6（RFC 2465）、TCP（RFC 4022）、UDP（RFC 4113）和ICMP（RFC 2466）MIBs（同時顯示IPv6和IPv6資料）ONTAP 。

ONTAP 也會在中的物件識別碼（ OID ）和物件簡短名稱之間提供簡短的交互參照 `traps.dat` 檔案：

> NetApp 支援網站上提供最新版本的 ONTAP MIB 和「traps.dat」檔案。不過、支援網站上的這些檔案版本不一定對應ONTAP 於您的版本的SNMP功能。這些檔案可協助您評估最新ONTAP 版的SNMP功能。

SNMP設陷

SNMP設陷會擷取系統監控資訊、這些資訊會以非同步通知的形式從SNMP代理程式傳送至SNMP管理程式。

SNMP設陷有三種類型：標準、內建及使用者定義。不支援ONTAP 使用者定義的陷阱。

陷阱可用於定期檢查在MIB中定義的操作臨界值或故障。如果達到臨界值或偵測到故障、SNMP代理程式會傳送訊息（設陷）給警示事件的traphosts。

> ONTAP 支援 SNMPv1 和 SNMPv3 設陷。不支援SNMP v2c擷取和通知。ONTAP

標準SNMP設陷

這些陷阱定義於RFC 1215。支援的五種標準SNMP設陷ONTAP ：冷啟動、暖啟動、連結、LinkUp和驗證失敗。

> 驗證失敗設陷預設為停用。您必須使用 `system snmp authtrap` 命令來啟用陷阱。如"指令參考資料ONTAP"需詳細 `system snmp authtrap`資訊，請參閱。

內建SNMP設陷

內建的設陷會預先定義在ONTAP 支援中、並在發生事件時自動傳送至traphost清單上的網路管理站台。這些陷阱（例如diskFailedShutdown, cpuTooBusy和volumeNearlyFull）是在自訂的mib中定義的。

每個內建陷阱都會以獨特的陷阱代碼來識別。

為 ONTAP 網路建立 SNMP 社群

使用SNMP v1和SNMP v2c時、您可以建立SNMP社群、做為管理站與儲存虛擬機器

（SVM）之間的驗證機制。

透過在資料 SVM 中建立 SNMP 社群、您可以執行命令、例如 `snmpwalk` 和 `snmpget` 資料生命。

關於這項工作

- 在全新安裝ONTAP 的功能中、預設會停用SNMPv1和SNMPv2c。

  在建立SNMP社群之後、會啟用SNMP v1和SNMP v2c。

- 支援唯讀社群。ONTAP
- 依預設、指派給資料生命期的「資料」防火牆原則會將 SNMP 服務設為 `deny`。

  您必須建立新的防火牆原則、並將 SNMP 服務設為 `allow` 為資料 SVM 建立 SNMP 使用者時。

  從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- 您可以為管理SVM和資料SVM的SNMP v1和SNMP v2c使用者建立SNMP社群。
- 由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 根 OID （ 1.3.6.1.4.1.789 ）、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

步驟

1. 使用建立 SNMP 社群 `system snmp community add` 命令。下列命令顯示如何在管理SVM叢集1中建立SNMP社群：

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   下列命令顯示如何在資料SVM VS1中建立SNMP社群：

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. 使用系統SNMP community show命令來驗證是否已建立社群。

   下列命令顯示為SNMP v1和SNMP v2c所建立的兩個社群：

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. 使用檢查是否允許 SNMP 作為「資料」防火牆原則中的服務 `system services firewall policy show` 命令。

下列命令顯示預設的「資料」防火牆原則不允許SNMP服務（僅「管理」防火牆原則允許SNMP服務）：

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. 建立允許使用存取的新防火牆原則 `snmp` 使用進行服務 `system services firewall policy create` 命令。

   下列命令會建立一個新的資料防火牆原則「 data1 」、允許使用 `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                      snmp       0.0.0.0/0
vs1
         data1
                      snmp       0.0.0.0/0
```

5. 使用命令搭配 -firewall-policy 參數，將防火牆原則套用至資料 LIF `network interface modify`。

   下列命令會將新的「data1」防火牆原則指派給LIF「dataif1」：

   ```
   network interface modify -vserver vs1 -lif datalif1 -firewall-policy
   data1
   ```

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

在 **ONTAP** 叢集中設定 **SNMPv3** 使用者

相較於SNMPv1和SNMPv2c、v3是一種安全的傳輸協定。若要使用v3、您必須設定一個v3使用者、以便從SNMP管理程式執行SNMP公用程式。

步驟

使用 `security login create`指令建立 SNMPv3 使用者。

系統會提示您提供下列資訊：

- 引擎ID：預設值和建議值為本機引擎ID
- 驗證傳輸協定
- 驗證密碼
- 隱私權傳輸協定
- 隱私權傳輸協定密碼

結果

v3使用者可以使用使用者名稱和密碼、從SNMP管理程式登入、然後執行SNMP公用程式命令。

v3安全參數

v3包含驗證功能、選取時會要求使用者在叫用命令時輸入名稱、驗證傳輸協定、驗證金鑰及其所需的安全層級。

下表列出了v3安全參數：

參數	命令列選項	說明
工程師ID	-e引擎ID	SNMP代理程式的引擎ID。預設值為本機引擎ID（建議使用）。
安全性名稱	-u名稱	使用者名稱不得超過32個字元。
驗證傳輸協定	-A｛NONE	md5

SHA	SHA-256}	驗證類型可以是「無」、「MD5」、「SHa」或「SHA-256」。
驗證金鑰	-A通關密碼	至少八個字元的通關密碼。
安全性層級	I {authNoPrimv	authPrimv
noauthNoPrimiv}	安全層級可以是驗證、無隱私權、驗證、隱私權或無驗證、 無隱私。	私有傳輸協定
-x {nONE	DE	AES128}
隱私權傳輸協定可以是無、DE或AES128	私有密碼	-X密碼

不同安全層級的範例

此範例顯示以不同安全性層級建立的 SNMPv3 使用者如何使用 SNMP 用戶端指令、例如 `snmpwalk`，查詢叢集物件。

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

您必須使用 `snmpwalk` 5.3.1 或更新版本、當驗證傳輸協定為 SHA 時。

安全性層級：**authPrim**

下列輸出顯示使用驗證權限安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS模式

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全性層級：**authNoPrim**

下列輸出顯示使用驗證NoPrimiv安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS模式

FIPS 不允許您為隱私權傳輸協定選擇 * 無 * 。因此、無法在 FIPS 模式中設定驗證 NoPrimv SNMPv3 使用者。

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全性層級：**noAuthNoPrimiv**

下列輸出顯示使用noAuthNoPrimiv安全性層級建立的v3使用者。

```
security login create -user-or-group-name snmpv3user -application snmp
-authmethod usm -role read-only
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS模式

FIPS 不允許您為隱私權傳輸協定選擇 * 無 * 。

snmpwalk.測試

下列輸出顯示執行snmpwalk命令 的v3使用者：

若要獲得更好的效能、您應該擷取資料表中的所有物件、而非從資料表擷取單一物件或數個物件。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

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

在 **ONTAP** 網路上設定用於 **SNMP** 的 **traphosts**

您可以將traphost（SNMP管理程式）設定為在叢集中產生SNMP設陷時接收通知（SNMP設陷PDU）。您可以指定SNMP traphost的主機名稱或IP位址（IPv4或IPv6）。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。

SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。
- 叢集上必須啟用IPv6、才能使用IPv6位址來設定SNMP traphosts。
- 建立 traphosts 時，您必須指定預先定義的使用者型安全模式（ USM ）驗證和隱私權認證。

步驟

新增SNMP traphost：

```
system snmp traphost add
```

只有當至少有一個SNMP管理站台指定為traphost時、才能傳送陷阱。

下列命令會以已知的USM使用者新增名為yyy.example.com的v3 traphost：

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

下列命令會使用主機的IPv6位址來新增traphost：

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

驗證 ONTAP 叢集中的 SNMP 輪詢

設定SNMP之後、您應該確認可以輪詢叢集。

關於這項工作

若要輪詢叢集、您需要使用第三方命令、例如 `snmpwalk`。

步驟

1. 傳送SNMP命令、從不同的叢集輪詢叢集。

   對於執行 SNMPv1 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

   在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 1 -c public 10.11.12.123 system

SNMPv1-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv1-MIB::sysObjectID.0 = OID: SNMPv1-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162644448) 18 days,
19:47:24.48
SNMPv1-MIB::sysContact.0 = STRING:
SNMPv1-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv1-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv1-MIB::sysServices.0 = INTEGER: 72
```

對於執行 SNMPv2c 的系統、請使用 CLI 命令 `snmpwalk -v version -c community_stringip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 2c -c public 10.11.12.123 system

SNMPv2-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
            Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162635772) 18 days,
19:45:57.72
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv2-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv2-MIB::sysServices.0 = INTEGER: 72
```

對於執行 SNMPv3 的系統、請使用 CLI 命令 `snmpwalk -v 3 -a MD5 or SHA -l authnopriv -u username -A passwordip_address_or_host_name system` 探索 MIB （管理資訊庫）的內容。

在此範例中、您要輪詢的叢集管理LIF IP位址為10.11.12.123。此命令會顯示來自以下MIB:

```
C:\Windows\System32>snmpwalk -v 3 -a MD5 -l authnopriv -u snmpv3
       -A password123 10.11.12.123 system

SNMPv3-MIB::sysDescr.0 = STRING: NetApp Release 8.3.0
       Cluster-Mode: Tue Apr 22 16:24:48 EDT 2014
SNMPv3-MIB::sysObjectID.0 = OID: SNMPv3-SMI::enterprises.789.2.5
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (162666569) 18 days,
19:51:05.69
SNMPv3-MIB::sysContact.0 = STRING:
SNMPv3-MIB::sysName.0 = STRING: systemname.testlabs.com
SNMPv3-MIB::sysLocation.0 = STRING: Floor 2 Row B Cab 2
SNMPv3-MIB::sysServices.0 = INTEGER: 72
```

用於管理 **SNMP** ，設陷和 **traphosts** 的 **ONTAP** 命令

您可以使用 `system snmp` 用於管理 SNMP 、設陷和 traphosts 的命令。您可以使用 `security` 用於管理每個 SVM 的 SNMP 使用者的命令。您可以使用 `event` 管理與 SNMP 設陷相關事件的命令。

設定SNMP的命令

如果您想要...	使用此命令...
在叢集上啟用SNMP	`options -option-name snmp.enable -option-value on` SNMP服務必須符合管理（管理）防火牆原則。您可以使用系統服務防火牆原則show命令來驗證是否允許SNMP。
停用叢集上的SNMP	`options -option-name snmp.enable -option-value off`

用於管理SNMP v1、v2c和v3使用者的命令

如果您想要...	使用此命令...
設定SNMP使用者	`security login create`
顯示SNMP使用者	`security snmpusers`和 `security login show -application snmp`
刪除SNMP使用者	`security login delete`

修改SNMP使用者登入方法的存取控制角色名稱	`security login modify`

提供聯絡人和位置資訊的命令

如果您想要…	使用此命令…
顯示或修改叢集的聯絡詳細資料	`system snmp contact`
顯示或修改叢集的位置詳細資料	`system snmp location`

管理**SNMP**社群的命令

如果您想要…	使用此命令…
為SVM或叢集中的所有SVM新增唯讀（RO）社群	`system snmp community add`
刪除社群或所有社群	`system snmp community delete`
顯示所有社群的清單	`system snmp community show`

由於 SVM 不是 SNMP 標準的一部分、因此資料生命體的查詢必須包含 NetApp 根 OID （ 1.3.6.1.4.1.789 ）、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

用於顯示**SNMP**選項值的命令

如果您想要…	使用此命令…
顯示所有SNMP選項的目前值、包括叢集聯絡人、聯絡人位置、叢集是否設定為傳送陷阱、traphosts清單、以及社群和存取控制類型清單	`system snmp show`

用於管理**SNMP**陷阱和**traphosts**的命令

如果您想要…	使用此命令…
啟用從叢集傳送的SNMP設陷	`system snmp init -init 1`
停用從叢集傳送的SNMP設陷	`system snmp init -init 0`
新增接收叢集中特定事件SNMP通知的traphost	`system snmp traphost add`
刪除traphost	`system snmp traphost delete`
顯示traphosts清單	`system snmp traphost show`

用於管理與**SNMP**陷阱相關的事件的命令

如果您想要...	使用此命令...
顯示產生SNMP陷阱（內建）的事件	`event route show` 使用 `-snmp-support true` 僅檢視 SNMP 相關事件的參數。 使用 `instance -messagename <message>` 此參數可檢視事件發生原因的詳細說明、以及任何修正動作。 不支援將個別SNMP設陷事件路由傳送至特定的traphost目的地。所有SNMP設陷事件都會傳送至所有的traphost目的地。
顯示SNMP設陷記錄清單、這是已傳送至SNMP設陷的事件通知	`event snmphistory show`
刪除SNMP設陷歷程記錄	`event snmphistory delete`

相關資訊

- "系統 SNMP"
- "安全性"
- "安全性"
- "活動"
- "安全登入"

管理**SVM**中的路由

瞭解 **ONTAP** 網路上的 **SVM** 路由

SVM的路由表會決定SVM用來與目的地通訊的網路路徑。瞭解路由表的運作方式非常重要、如此一來、您就能在網路問題發生之前先行防範。

路由規則如下：

- 透過最具體的可用路由傳送流量。ONTAP
- 當無法使用更多特定路由時、透過預設閘道路由（網路遮罩為0位元）路由流量。ONTAP

如果路由具有相同目的地、網路遮罩和度量、則無法保證系統在重新開機或升級後會使用相同的路由。如果您已設定多個預設路由、這尤其會造成問題。

最佳做法是僅為 SVM 配置一個預設路由。為了避免中斷，您應該確保預設路由能夠到達任何無法透過更特定的路由到達的網路位址。有關詳細信息，請參閱"NetApp知識庫：SU134 - 叢集ONTAP中的路由配置不正確可能會導致網路存取中斷"

為 ONTAP 網路建立靜態路由

您可以在儲存虛擬機器（SVM）內建立靜態路由、以控制LIF如何將網路用於傳出流量。

當您建立與SVM相關聯的路由項目時、該路由會被指定SVM擁有且與閘道位於同一子網路的所有LIF使用。

步驟

使用 `network route create` 建立路由的命令。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

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

啟用 ONTAP 網路的多重路徑路由

如果多個路由的目的地度量相同、則只會針對傳出流量選取其中一個路由。這會導致其他路由未使用來傳送傳出流量。您可以啟用多重路徑路由、使所有可用路由的負載平衡、以符合其度量、而非 ECMP 路由、後者會在相同度量的可用路由之間平衡負載。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 啟用多重路徑路由：

   ```
   network options multipath-routing modify -is-enabled true
   ```

   叢集中的所有節點均已啟用多重路徑路由。

   ```
   network options multipath-routing modify -is-enabled true
   ```

   如"指令參考資料ONTAP"需詳細 `network options multipath-routing modify`資訊，請參閱。

從 ONTAP 網路刪除靜態路由

您可以從儲存虛擬機器（SVM）刪除不需要的靜態路由。

步驟

使用 `network route delete` 刪除靜態路由的命令。

下列範例會刪除與SVM vs0關聯的靜態路由、閘道為10.63.0.1、目的地IP位址為0.00.0/0：

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

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

檢視 ONTAP 路由資訊

您可以顯示叢集上每個SVM的路由組態資訊。這有助於診斷與用戶端應用程式或服務之間的連線問題有關的路由問題、以及叢集中某個節點上的LIF。

步驟

1. 使用 `network route show` 顯示一或多個 SVM 內路由的命令。下列範例顯示在vs0 SVM中設定的路由：

```
network route show
  (network route show)
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
vs0
                    0.0.0.0/0       172.17.178.1    20
```

2. 使用 `network route show-lifs` 顯示一或多個 SVM 內路由和生命的關聯的命令。

   以下範例顯示vs0 SVM擁有路由的lifs：

```
network route show-lifs
  (network route show-lifs)

Vserver: vs0
Destination             Gateway                 Logical Interfaces
----------------------  --------------          --------------------
0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                LIF-b-01_mgmt1,
                                                LIF-b-02_mgmt1
```

   深入瞭解 `network route show`及 `network route show-lifs` "指令參考資料ONTAP"。

3. 使用 `network route active-entry show` 命令可在一個或多個節點、 SVM 、子網路或具有指定目的地的路由上顯示已安裝的路由。

   下列範例顯示特定SVM上所有已安裝的路由：

```
network route active-entry show -vserver Data0
```

```
Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
11 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `network route active-entry show`資訊，請參閱。

從 ONTAP 網路的路由表中移除動態路由

收到針對IPv6和IPv6的ICMP重新導向時、動態路由會新增至路由表。根據預設、動態路由會在300秒後移除。如果您想要在不同時間內維持動態路由、可以變更逾時值。

關於這項工作

您可以將逾時值從0設定為65,535秒。如果您將值設為0、則路由永遠不會過期。移除動態路由可避免因無效路由持續存在而導致連線中斷。

步驟

1. 顯示目前的逾時值。
   - 對於IPV4：

     ```
     network tuning icmp show
     ```

   - 對於IPv6：

     ```
     network tuning icmp6 show
     ```

2. 修改逾時值。
   - 對於IPV4：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - 對於IPv6：

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. 確認逾時值已正確修改。
   - 對於IPV4：

     ```
     network tuning icmp show
     ```

   - 對於IPv6：

```
network tuning icmp6 show
```

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

ONTAP 網路資訊

檢視 ONTAP 網路資訊

使用 CLI 、您可以檢視與連接埠、生命、路由、容錯移轉規則、容錯移轉群組、 防火牆規則、 DNS 、 NIS 和連線。從 ONTAP 9.8 開始、您也可以下載 System Manager 中顯示的網路相關資料。

此資訊在重新設定網路設定或疑難排解叢集等情況下非常實用。

如果您是叢集管理員、可以檢視所有可用的網路資訊。如果您是SVM管理員、則只能檢視與您指派的SVM相關的資訊。

在 System Manager 中、當您在 *List View* 中顯示資訊時、您可以按一下 * 下載 * 、並下載顯示的物件清單。

- 此清單會以「以逗號分隔的值（CSV）」格式下載。
- 只會下載可見欄中的資料。
- CSV檔案名稱的格式為物件名稱和時間戳記。

檢視 ONTAP 網路連接埠資訊

您可以顯示有關特定連接埠或叢集中所有節點上所有連接埠的資訊。

關於這項工作

將顯示下列資訊：

- 節點名稱
- 連接埠名稱
- IPSpace名稱
- 廣播網域名稱
- 連結狀態（向上或向下）
- MTU設定
- 連接埠速度設定與作業狀態（每秒1 Gb或10 Gb）
- 自動交涉設定（true或假）
- 雙工模式和作業狀態（半雙工或全雙工）
- 連接埠的介面群組（若適用）
- 連接埠的VLAN標記資訊（若適用）

- 連接埠的健全狀況（健全狀況或降級）
- 連接埠標記為降級的原因

如果欄位的資料無法使用（例如、非作用中連接埠的作業雙工和速度將無法使用）、欄位值會列為 -。

步驟

使用顯示網路連接埠資訊 `network port show` 命令。

您可以透過指定來顯示每個連接埠的詳細資訊 `-instance` 或使用指定欄位名稱來取得特定資訊 `-fields` 參數。

```
network port show
Node: node1

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                  Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

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

檢視 ONTAP VLAN 資訊

您可以顯示有關特定VLAN或叢集中所有VLAN的資訊。

關於這項工作

您可以透過指定來顯示每個 VLAN 的詳細資訊 `-instance` 參數。您可以使用指定欄位名稱來顯示特定資訊

`-fields` 參數。

步驟

使用顯示有關 VLAN 的資訊 `network port vlan show` 命令。下列命令會顯示叢集中所有VLAN的相關資訊：

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

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

檢視 ONTAP 介面群組資訊

您可以顯示介面群組的相關資訊、以判斷其組態。

關於這項工作

將顯示下列資訊：

- 介面群組所在的節點
- 介面群組中包含的網路連接埠清單
- 介面群組名稱
- 發佈功能（MAC、IP、連接埠或連續）
- 介面群組的媒體存取控制（MAC）位址
- 連接埠活動狀態；也就是所有彙總連接埠都處於作用中狀態（完全參與）、某些連接埠為作用中狀態（部分參與）、或無作用中狀態

步驟

使用顯示介面群組的相關資訊 `network port ifgrp show` 命令。

您可以透過指定來顯示每個節點的詳細資訊 `-instance` 參數。您可以使用指定欄位名稱來顯示特定資訊 `-fields` 參數。

下列命令會顯示叢集中所有介面群組的相關資訊：

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

下列命令會顯示單一節點的詳細介面群組資訊：

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

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

檢視 ONTAP LIF 資訊

您可以檢視LIF的詳細資訊、以判斷其組態。

您也可能想要檢視此資訊來診斷基本的LIF問題、例如檢查是否有重複的IP位址、或驗證網路連接埠是否屬於正確的子網路。儲存虛擬機器（SVM）管理員只能檢視與SVM相關聯的LIF資訊。

關於這項工作

將顯示下列資訊：

- 與LIF相關的IP位址
- LIF的管理狀態
- LIF的作業狀態

資料生命體的作業狀態取決於資料生命體相關聯的SVM狀態。當SVM停止時、LIF的作業狀態會變更為「關閉」。當SVM再次啟動時、作業狀態會變更為up

- 節點和LIF所在的連接埠

如果欄位的資料無法使用（例如、如果沒有擴充狀態資訊）、欄位值會列為 –。

步驟

使用命令顯示 LIF 資訊 `network interface show`。

您可以指定-instance參數來檢視每個LIF的詳細資訊、或使用-fields參數指定欄位名稱來取得特定資訊。

下列命令會顯示叢集中所有LIF的一般資訊：

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

下列命令顯示單一LIF的詳細資訊：

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                  Data Protocol: nfs,cifs
                      Home Node: node-01
                      Home Port: e0c
                   Current Node: node-03
                   Current Port: e0c
               Operational Status: up
                  Extended Status: -
                          Is Home: false
                  Network Address: 192.0.2.128
                          Netmask: 255.255.192.0
            Bits in the Netmask: 18
                IPv4 Link Local: -
                    Subnet Name: -
             Administrative Status: up
                  Failover Policy: local-only
                  Firewall Policy: data
                      Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                        FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

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

檢視 ONTAP 網路的路由資訊

您可以顯示SVM內的路由資訊。

步驟

視您要檢視的路由資訊類型而定、輸入適當的命令：

若要檢視有關...的資訊	輸入...
靜態路由（每SVM）	`network route show`

每個路由上的LIF（每個SVM）	`network route show-lifs`

您可以透過指定來顯示每個航線的詳細資訊 `-instance` 參數。下列命令會顯示叢集1中SVM內的靜態路由：

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

下列命令會顯示叢集1中所有SVM的靜態路由和邏輯介面（lifs）關聯：

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------

0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

深入瞭解 `network route show`及 `network route show-lifs` "指令參考資料ONTAP"。

檢視 **ONTAP DNS** 主機表格項目

DNS主機表項目會將主機名稱對應至IP位址。您可以針對叢集中的所有SVM顯示主機名稱和別名、以及它們對應的IP位址。

步驟

使用vserver services name-service DNS hosts show命令顯示所有SVM的主機名稱項目。

下列範例顯示主機表格項目：

```
vserver services name-service dns hosts show
Vserver    Address         Hostname        Aliases
---------- --------------- --------------- ---------------------
cluster-1
           10.72.219.36    lnx219-36       -
vs1
           10.72.219.37    lnx219-37       lnx219-37.example.com
```

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

檢視 **ONTAP DNS** 網域組態資訊

您可以在叢集中顯示一或多個儲存虛擬機器（SVM）的DNS網域組態、以驗證其設定是否正確。

步驟

使用檢視 DNS 網域組態 `vserver services name-service dns show` 命令。

下列命令會顯示叢集中所有SVM的DNS組態：

```
vserver services name-service dns show
                                                    Name
Vserver         State     Domains                   Servers
--------------- --------- ------------------------- -------------
cluster-1        enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs1             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs2             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
vs3             enabled   xyz.company.com           192.56.0.129,
                                                    192.56.0.130
```

下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

檢視 ONTAP 容錯移轉群組資訊

您可以檢視容錯移轉群組的相關資訊、包括每個容錯移轉群組中的節點和連接埠清單、是否啟用或停用容錯移轉、以及要套用至每個LIF的容錯移轉原則類型。

步驟

1. 使用顯示每個容錯移轉群組的目標連接埠 `network interface failover-groups show` 命令。

   下列命令會顯示雙節點叢集上所有容錯移轉群組的相關資訊：

```
network interface failover-groups show
                                 Failover
Vserver          Group           Targets
---------------  --------------  --------------------------------
Cluster
                 Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
vs1
                 Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
```

   如"指令參考資料ONTAP"需詳細 `network interface failover-groups show`資訊，請參閱。

2. 使用顯示特定容錯移轉群組的目標連接埠和廣播網域 `network interface failover-groups show` 命令。

   下列命令會顯示SVM VS4容錯移轉群組data12的詳細資訊：

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. 使用顯示所有生命所使用的容錯移轉設定 `network interface show` 命令。

   下列命令會顯示每個LIF所使用的容錯移轉原則和容錯移轉群組：

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  -------------------  ---------------------  --------------
Cluster   cluster1-01_clus_1   local-only             Cluster
Cluster   cluster1-01_clus_2   local-only             Cluster
Cluster   cluster1-02_clus_1   local-only             Cluster
Cluster   cluster1-02_clus_2   local-only             Cluster
cluster1  cluster_mgmt         broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1    local-only             Default
cluster1  cluster1-02_mgmt1    local-only             Default
vs1       data1                disabled               Default
vs3       data2                system-defined         group2
```

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

檢視 ONTAP LIF 容錯移轉目標

您可能必須檢查LIF的容錯移轉原則和容錯移轉群組是否設定正確。為了避免容錯移轉規則組態錯誤、您可以顯示單一LIF或所有LIF的容錯移轉目標。

關於這項工作

顯示LIF容錯移轉目標可讓您檢查下列項目：

- 是否使用正確的容錯移轉群組和容錯移轉原則來設定生命體
- 所產生的容錯移轉目標連接埠清單是否適用於每個LIF
- 資料LIF的容錯移轉目標是否不是管理連接埠（e0M）

步驟

使用顯示 LIF 的容錯移轉目標 `failover` 的選項 `network interface show` 命令。

下列命令會顯示雙節點叢集中所有LIF的容錯移轉目標相關資訊。。 `Failover Targets` 列顯示指定 LIF 的節點連接埠組合（優先順序）清單。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------ --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

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

檢視負載平衡區域中的 ONTAP 生命負載

您可以顯示屬於負載平衡區域的所有生命期、以驗證負載平衡區域是否設定正確。您也可

以檢視特定LIF的負載平衡區域、或檢視所有LIF的負載平衡區域。

步驟

使用下列其中一項命令、顯示所需的生命量與負載平衡詳細資料

若要顯示...	輸入...
特定負載平衡區域中的LIF	`network interface show -dns-zone zone_name` `zone_name` 指定負載平衡區域的名稱。
特定LIF的負載平衡區域	`network interface show -lif lif_name -fields dns-zone`
所有生命區的負載平衡區域	`network interface show -fields dns-zone`

顯示**lifs**負載平衡區域的範例

下列命令會顯示SVM vs0之負載平衡區域storage.company.com中所有LIF的詳細資料：

```
net int show -vserver vs0 -dns-zone storage.company.com

          Logical    Status     Network            Current   Current Is
Vserver   Interface  Admin/Oper Address/Mask       Node      Port    Home
--------- ---------- ---------- ------------------ --------- ------- ----
vs0
          lif3         up/up    10.98.226.225/20   ndeux-11  e0c     true
          lif4         up/up    10.98.224.23/20    ndeux-21  e0c     true
          lif5         up/up    10.98.239.65/20    ndeux-11  e0c     true
          lif6         up/up    10.98.239.66/20    ndeux-11  e0c     true
          lif7         up/up    10.98.239.63/20    ndeux-21  e0c     true
          lif8         up/up    10.98.239.64/20    ndeux-21  e0c     true
```

下列命令會顯示LIF資料3的DNS區域詳細資料：

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

下列命令會顯示叢集中所有LIF及其對應DNS區域的清單：

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

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

檢視 ONTAP 叢集連線

您可以依用戶端、邏輯介面、傳輸協定或服務、顯示叢集中的所有作用中連線、或節點上的作用中連線數。您也可以顯示叢集中的所有聆聽連線。

依用戶端顯示作用中連線（僅限叢集管理員）

您可以檢視用戶端的作用中連線、以驗證特定用戶端所使用的節點、並檢視每個節點的用戶端計數之間可能存在的不平衡。

關於這項工作

用戶端的作用中連線數在下列案例中很有用：

- 尋找忙碌或過載的節點。
- 判斷特定用戶端存取磁碟區的速度緩慢的原因。

  您可以檢視用戶端正在存取之節點的詳細資料、然後將其與磁碟區所在的節點進行比較。如果存取磁碟區需要周遊叢集網路、用戶端可能會因為遠端存取超額訂閱的遠端節點上的磁碟區而遇到效能降低的問題。

- 驗證是否所有節點都能用於資料存取。
- 尋找連線數量異常高的用戶端。
- 驗證特定用戶端是否有連線至節點。

步驟

使用顯示節點上用戶端的作用中連線計數 `network connections active show-clients` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-clients`資訊，請參閱。

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

依傳輸協定顯示作用中連線（僅限叢集管理員）

您可以依節點上的傳輸協定（TCP或udp）顯示作用中連線的計數、以比較叢集內的傳輸協定使用量。

關於這項工作

依傳輸協定的作用中連線數在下列案例中很有用：

- 尋找正在失去連線的udp用戶端。

  如果某個節點接近其連線限制、則會先捨棄UDP用戶端。

- 驗證是否未使用其他通訊協定。

步驟

使用在節點上依通訊協定顯示作用中連線的計數 `network connections active show-protocols` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-protocols`資訊，請參閱。

```
network connections active show-protocols
Node     Vserver Name  Protocol   Count
-------  ------------  ---------  ------
node0
         vs0           UDP            19
         Cluster       TCP            11
node1
         vs0           UDP            17
         Cluster       TCP             8
node2
         vs1           UDP            14
         Cluster       TCP            10
node3
         vs1           UDP            18
         Cluster       TCP             4
```

依服務顯示作用中連線（僅限叢集管理員）

您可以針對叢集中的每個節點、依服務類型（例如NFS、SMB、掛載等）顯示作用中連線的計數。這對於比較叢集內的服務使用量很有用、因為這有助於判斷節點的主要工作負載。

關於這項工作

依服務列出的作用中連線數在下列案例中非常實用：

- 驗證所有節點是否用於適當的服務、以及該服務的負載平衡是否正常運作。
- 驗證是否未使用其他服務。使用顯示節點上依服務顯示作用中連線的計數 `network connections active show-services` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-services`資訊，請參閱。

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
            vs0             mount           3
            vs0             nfs            14
            vs0             nlm_v4          4
            vs0             cifs_srv        3
            vs0             port_map       18
            vs0             rclopcp        27
            Cluster         ctlopcp        60
node1
            vs0             cifs_srv        3
            vs0             rclopcp        16
            Cluster         ctlopcp        60
node2
            vs1             rclopcp        13
            Cluster         ctlopcp        60
node3
            vs1             cifs_srv        1
            vs1             rclopcp        17
            Cluster         ctlopcp        60
```

在節點和**SVM**上顯示**LIF**的作用中連線

您可以依節點和儲存虛擬機器（SVM）顯示每個LIF的作用中連線數、以檢視叢集內LIF之間的連線不平衡。

關於這項工作

LIF的作用中連線數在下列案例中很有用：

- 比較每個LIF上的連線數目、找出過載的LIF。
- 驗證DNS負載平衡是否適用於所有資料LIF。
- 比較不同SVM的連線數目、找出使用最多的SVM。

步驟

使用顯示 SVM 和節點每個 LIF 的作用中連線計數 `network connections active show-lifs` 命令。

如"指令參考資料ONTAP"需詳細 `network connections active show-lifs`資訊，請參閱。

```
network connections active show-lifs
Node      Vserver Name  Interface Name  Count
--------  ------------  --------------- ------
node0
          vs0           datalif1             3
          Cluster       node0_clus_1         6
          Cluster       node0_clus_2         5
node1
          vs0           datalif2             3
          Cluster       node1_clus_1         3
          Cluster       node1_clus_2         5
node2
          vs1           datalif2             1
          Cluster       node2_clus_1         5
          Cluster       node2_clus_2         3
node3
          vs1           datalif1             1
          Cluster       node3_clus_1         2
          Cluster       node3_clus_2         2
```

顯示叢集中的作用中連線

您可以顯示叢集中作用中連線的相關資訊、以檢視個別連線所使用的LIF、連接埠、遠端主機、服務、儲存虛擬機器（SVM）和傳輸協定。

關於這項工作

在下列情況下、檢視叢集中的作用中連線十分有用：

- 驗證個別用戶端是否在正確的節點上使用正確的傳輸協定和服務。
- 如果用戶端無法使用特定的節點、傳輸協定和服務組合來存取資料、您可以使用此命令來尋找類似的用戶端來進行組態或封包追蹤比較。

步驟

使用顯示叢集中的作用中連線 `network connections active show` 命令。

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

下列命令顯示節點節點節點1上的作用中連線：

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

下列命令顯示SVM VS1上的作用中連線：

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ---------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

顯示叢集中的接聽連線

您可以顯示叢集中偵聽連線的相關資訊、以檢視接受特定傳輸協定和服務連線的生命與連接埠。

關於這項工作

檢視叢集中的聆聽連線在下列情況下非常有用：

- 如果與LIF的用戶端連線持續失敗、請確認所需的傳輸協定或服務正在聆聽LIF。
- 如果透過另一個節點上的LIF遠端資料存取某個節點上的磁碟區失敗、請驗證是否在每個叢集LIF上開啟UP/rclipcp接聽程式。
- 如果SnapMirror在同一叢集中的兩個節點之間傳輸失敗、請驗證是否在每個叢集LIF上開啟UP/rclipcp接聽程式。
- 如果SnapMirror在不同叢集的兩個節點之間傳輸失敗、請驗證是否在每個叢集間的LIF上開啟了TCP/IP接聽程式。

步驟

使用顯示每個節點的聆聽連線 `network connections listening show` 命令。

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

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

用於診斷網路問題的 **ONTAP** 命令

您可以使用命令來診斷網路上的問題、例如 `ping`, `traceroute`, `ndp`, 和 `tcpdump`。您也可以使用命令、例如 `ping6` 和 `traceroute6` 診斷 IPv6 問題。

如果您想要...	輸入此命令...
測試節點是否能連線到網路上的其他主機	`network ping`
測試節點是否能連線至IPv6網路上的其他主機	`network ping6`
追蹤將IPv4封包帶到網路節點的路由	`network traceroute`
追蹤IPv6封包通往網路節點的路由	`network traceroute6`
管理鄰近探索傳輸協定（NDP）	`network ndp`
顯示在指定網路介面或所有網路介面上接收和傳送的封包統計資料	`run -node` *`node_name`* `ifstat` * 附註 * ：此命令可從 nodesdesh 取得。
顯示從叢集中每個節點和連接埠探索到的鄰近裝置相關資訊、包括遠端裝置類型和裝置平台	`network device-discovery show`
檢視節點的CDP鄰近節點（ONTAP 僅支援CDPv1廣告）	`run -node` *`node_name`* `cdpd show-neighbors` * 附註 * ：此命令可從 nodesdesh 取得。

追蹤在網路中傳送和接收的封包	`network tcpdump start -node node-name -port port_name` * 附註 * ：此命令可從 nodesdesh 取得。
測量叢集間或叢集內節點之間的延遲和處理量	`network test -path -source-node source_nodename local -destination -cluster destination_clustername -destination-node destination_nodename -session-type Default, AsyncMirrorLocal, AsyncMirrorRemote, SyncMirrorRemote, or RemoteDataTransfer` 如需詳細資訊、請參閱 "效能管理"。

相關資訊

- "指令參考資料ONTAP"
- "網路ping"
- "網路追蹤"
- "網路裝置探索秀"
- "網路 NDP"

檢視與鄰近探索通訊協定的網路連線

檢視 **ONTAP** 與鄰近探索通訊協定的網路連線能力

在資料中心中、您可以使用鄰近探索通訊協定來檢視實體或虛擬系統與其網路介面配對之間的網路連線。支援兩種鄰近探索傳輸協定：Cisco探索傳輸協定（CDP）和連結層探索傳輸協定（LLDP）ONTAP 。

鄰近探索傳輸協定可讓您自動探索及檢視網路中已直接連線之傳輸協定裝置的相關資訊。每個裝置都會通告識別、功能和連線資訊。此資訊會以乙太網路框架傳輸至多點傳送MAC位址、並由所有鄰近的啟用傳輸協定的裝置接收。

若要讓兩個裝置成為鄰近裝置、每個裝置都必須啟用並正確設定傳輸協定。探索傳輸協定功能僅限於直接連線的網路。鄰近設備可包括採用傳輸協定的裝置、例如交換器、路由器、橋接器等。支援兩種鄰近探索通訊協定、可個別或一起使用。ONTAP

- Cisco探索傳輸協定（CDP）*

CDP是Cisco Systems開發的專屬連結層傳輸協定。叢ONTAP 集連接埠的預設功能為啟用、但必須明確啟用資料連接埠。

連結層探索傳輸協定（**LLDP**）

LLDP是標準文件IEEE 802.1AB中指定的廠商中立傳輸協定。所有連接埠都必須明確啟用此功能。

使用CDP偵測網路連線能力、包括審查部署考量、在資料連接埠上啟用、檢視鄰近裝置、以及視需要調整CDP組態值。預設會在叢集連接埠上啟用CDP。

也必須在任何交換器和路由器上啟用CDP、才能顯示鄰近裝置的相關資訊。

發行版ONTAP	說明
9.10.1及更早版本	叢集交換器健全狀況監視器也會使用CDP來自動探索叢集和管理網路交換器。
9.11.1 及更新版本	叢集交換器健全狀況監視器也會使用CDP來自動探索叢集、儲存設備和管理網路交換器。

相關資訊

"系統管理"

使用**CDP**的考量事項

根據預設、符合CDP的裝置會傳送CDPv2通告。CDP相容的裝置僅在收到CDPv1廣告時才會傳送CDPv1廣告。僅支援CDPv1。ONTAP因此ONTAP 、當某個節點傳送CDPv1廣告時、符合CDP的鄰近裝置會傳回CDPv1廣告。

在節點上啟用CDP之前、您應該先考慮下列資訊：

- 所有連接埠均支援CDP。
- CDP通告由處於up狀態的連接埠傳送和接收。
- 必須在傳輸和接收裝置上啟用CDP、才能傳送和接收CDP通告。
- CDP通告會定期傳送、您可以設定時間間隔。
- 當LIF的IP位址變更時、節點會在下一個CDP通告中傳送更新的資訊。
- 更新版本：ONTAP
  - 叢集連接埠上一律會啟用CDP。
  - 預設會在所有非叢集連接埠上停用CDP。
- 更新版本：ONTAP
  - 叢集和儲存連接埠上一律會啟用CDP。
  - 預設會在所有非叢集和非儲存連接埠上停用CDP。

> 有時當節點上的生命區發生變更時、接收裝置端（例如交換器）的CDP資訊不會更新。如果遇到這樣的問題、您應該將節點的網路介面設定為停機狀態、然後再設定為UP狀態。

- CDP通告中只會通告IPv4位址。
- 對於具有VLAN的實體網路連接埠、會通告在該連接埠上VLAN上設定的所有生命體。
- 對於屬於介面群組一部分的實體連接埠、該介面群組上設定的所有IP位址都會在每個實體連接埠上通告。

- 對於裝載VLAN的介面群組、介面群組和VLAN上設定的所有生命體都會在每個網路連接埠上通告。
- 由於端口上的 CDP 封包限制為不超過 1500 位元組
  配置大量的生命流量時、相鄰交換器上只會報告這些 IP 位址的子集。

啟用或停用**CDP**

若要探索及傳送通告至符合CDP的鄰近裝置、必須在叢集的每個節點上啟用CDP。

根據預設ONTAP 、在支援的版本中、CDP會在節點的所有叢集連接埠上啟用、並在節點的所有非叢集連接埠上停用。

根據預設ONTAP 、在更新版本的版本中、CDP會在節點的所有叢集和儲存連接埠上啟用、並在節點的所有非叢集和非儲存連接埠上停用。

關於這項工作

。 `cdpd.enable` 選項可控制是否在節點的連接埠上啟用或停用 CDP ：

- 若為ONTAP 版本不含更新版本的版本、On可在非叢集連接埠上啟用CDP。
- 若為ONTAP 版本的版本、則on會在非叢集和非儲存連接埠上啟用CDP。
- 對於版本不含更新版本的版本、Off會停用非叢集連接埠上的CDP；您無法在叢集連接埠上停用CDP。ONTAP
- 針對版本的版本、Off會停用非叢集和非儲存連接埠上的CDP；您無法在叢集連接埠上停用CDP。ONTAP

如果在連接至CDP相容裝置的連接埠上停用CDP、則可能無法最佳化網路流量。

步驟

1. 顯示節點或叢集中所有節點的目前CDP設定：

若要檢視CDP設定…	輸入…
節點	`run - node <node_name> options cdpd.enable`
叢集中的所有節點	`options cdpd.enable`

2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上啟用或停用CDP：

若要啟用或停用CDP：	輸入…
節點	`run -node node_name options cdpd.enable {on or off}`
叢集中的所有節點	`options cdpd.enable {on or off}`

檢視**CDP**鄰近資訊

只要連接埠連接至符合CDP的裝置、即可檢視連接至叢集節點每個連接埠的鄰近裝置相關資訊。您可以使用 `network device-discovery show -protocol cdp`命令來檢視鄰近的資訊。如"指令參考資料ONTAP"需詳細 `network device-discovery show`資訊，請參閱。

關於這項工作

在版本更新的版本中、由於叢集連接埠一律啟用CDP、因此這些連接埠的CDP鄰近資訊一律會顯示。ONTAP必須在非叢集連接埠上啟用CDP、這些連接埠才會顯示鄰近資訊。

在版本更新的版本中、由於叢集和儲存連接埠一律啟用CDP、因此這些連接埠的CDP鄰近資訊一律會顯示。ONTAP必須在非叢集和非儲存連接埠上啟用CDP、這些連接埠才會顯示鄰近資訊。

步驟

顯示所有連接至叢集中節點上連接埠的CDP相容裝置相關資訊：

```
network device-discovery show -node node -protocol cdp
```

下列命令顯示連接至節點ST2650/212上連接埠的鄰近裝置：

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

輸出會列出連線至指定節點每個連接埠的Cisco裝置。

設定**CDP**訊息的保留時間

保留時間是指CDP通告儲存在鄰近CDP相容裝置快取中的期間。保留時間會在每個CDPv1封包中通告、並在節點收到CDPv1封包時更新。

- 的值 `cdpd.holdtime` 在 HA 配對的兩個節點上、選項應設為相同的值。
- 預設的保留時間值為180秒、但您可以輸入介於10秒到255秒之間的值。
- 如果在保留時間到期之前移除IP位址、則CDP資訊會快取、直到保留時間過期為止。

步驟

1. 顯示節點或叢集中所有節點的目前CDP保留時間：

若要檢視保留時間...	輸入...
節點	`run -node node_name options cdpd.holdtime`
叢集中的所有節點	`options cdpd.holdtime`

2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上設定CDP保留時間：

若要設定保留時間...	輸入...
節點	`run -node node_name options cdpd.holdtime holdtime`
叢集中的所有節點	`options cdpd.holdtime holdtime`

設定傳送**CDP**通告的時間間隔

CDP通告會定期傳送給CDP鄰近裝置。視網路流量和網路拓撲的變更而定、您可以增加或減少傳送CDP通告的時間間隔。

- 的值 `cdpd.interval` 在 HA 配對的兩個節點上、選項應設為相同的值。
- 預設時間間隔為60秒、但您可以輸入5秒到900秒之間的值。

步驟

1. 顯示節點或叢集中所有節點的目前CDP通告時間間隔：

若要檢視時間間隔...	輸入...
節點	`run -node node_name options cdpd.interval`
叢集中的所有節點	`options cdpd.interval`

2. 針對節點的所有連接埠或叢集中所有節點的所有連接埠、設定傳送CDP通告的時間間隔：

若要設定時間間隔...	輸入...
節點	`run -node node_name options cdpd.interval interval`

叢集中的所有節點	`options cdpd.interval interval`

檢視或清除**CDP**統計資料

您可以檢視每個節點上叢集和非叢集連接埠的CDP統計資料、以偵測潛在的網路連線問題。CDP統計資料會從上次清除的時間開始累計。

關於這項工作

在《支援連結埠的CDP》（《支援端口的CDP）中、由於這些連接埠上的流量一律會顯示CDP統計資料。ONTAP必須在連接埠上啟用CDP、才能顯示這些連接埠的統計資料。

在《支援叢集與儲存連接埠的CDP（CDP）9.11.1及更新版本中、由於這些連接埠上的流量一律會顯示CDP統計資料。ONTAP必須在非叢集或非儲存連接埠上啟用CDP、才能顯示這些連接埠的統計資料。

步驟

顯示或清除節點上所有連接埠的目前CDP統計資料：

如果您想要...	輸入...
檢視CDP統計資料	`run -node node_name cdpd show-stats`
清除CDP統計資料	`run -node node_name cdpd zero-stats`

顯示及清除統計資料的範例

下列命令會在清除CDP統計資料之前顯示這些統計資料。輸出會顯示自上次清除統計資料以來、已傳送和接收的封包總數。

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

下列命令會清除CDP統計資料：

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:              0   | Csum Errors:         0   | Unsupported Vers:     0
 Invalid length:       0   | Malformed:           0   | Mem alloc fails:      0
 Missing TLVs:         0   | Cache overflow:      0   | Other errors:         0

TRANSMIT
 Packets:              0   | Xmit fails:          0   | No hostname:          0
 Packet truncated:     0   | Mem alloc fails:     0   | Other errors:         0

OTHER
 Init failures:        0
```

統計資料清除後、會在傳送或接收下一個CDP廣告之後開始累積。

連線至不支援 **CDP** 的乙太網路交換器

一些供應商的交換器不支援 CDP。查看"NetApp知識庫： ONTAP設備發現顯示節點而不是交換機"了解更多詳情。

有兩種方法可以解決此問題：

- 停用 CDP 並啟用 LLDP （如果支援）。請參閱 "使用 LLDP 來偵測網路連線" 以取得更多詳細資料。
- 在交換器上設定 MAC 位址封包篩選器、以捨棄 CDP 通告。

使用 **LLDP** 來偵測 **ONTAP** 網路連線

使用LLDP偵測網路連線能力包括審查部署考量、在所有連接埠上啟用、檢視鄰近裝置、以及視需要調整LLDP組態值。

在顯示鄰近裝置的相關資訊之前、也必須在任何交換器和路由器上啟用LLDP。

目前可報告下列類型長度值結構（TLV）ONTAP ：

- 機箱ID
- 連接埠ID
- 存留時間（TTL）
- 系統名稱

  系統名稱TLV不會傳送至CNA裝置。

某些整合式網路介面卡（CNA）、例如X1143介面卡和UTA2內建連接埠、包含LLDP的卸載支援：

- LLDP卸載用於資料中心橋接（DCB）。
- 叢集與交換器之間顯示的資訊可能有所不同。

  交換器所顯示的機箱ID和連接埠ID資料、可能與CNA和非CNA連接埠不同。

例如：

- 對於非CNA連接埠：
  - 機箱ID是節點上其中一個連接埠的固定MAC位址
  - 連接埠ID是節點上個別連接埠的連接埠名稱
- 對於CNA連接埠：
  - 機箱ID和連接埠ID是節點上個別連接埠的MAC位址。

不過、叢集所顯示的資料對於這些連接埠類型而言是一致的。

LLDP規格定義透過SNMP mib存取所收集的資訊。不過ONTAP 、目前不支援LLDP MIB.

啟用或停用 **LLDP**

若要探索及傳送通告給符合LLDP的鄰近裝置、必須在叢集的每個節點上啟用LLDP。從ONTAP 推出支援支援支援的支援方案開始、在節點的所有連接埠上預設都會啟用LLDP。

關於這項工作

對於 ONTAP 9.10.1 及更早版本、 `lldp.enable` 選項可控制是否在節點的連接埠上啟用或停用 LLDP ：

- `on` 在所有連接埠上啟用 LLDP 。
- `off` 停用所有連接埠上的 LLDP 。

對於 ONTAP 9.11.1 及更新版本、 `lldp.enable` 選項可控制在節點的非叢集和非儲存連接埠上啟用或停用 LLDP ：

- `on` 在所有非叢集和非儲存連接埠上啟用 LLDP 。
- `off` 在所有非叢集和非儲存連接埠上停用 LLDP 。

步驟

1. 顯示節點或叢集中所有節點的目前 LLDP 設定：
   - 單一節點： `run -node node_name options lldp.enable`
   - 所有節點：選項 `lldp.enable`
2. 在節點的所有連接埠或叢集中所有節點的所有連接埠上啟用或停用 LLDP ：

若要在 … 上啟用或停用 LLDP	輸入…
節點	`run -node node_name options lldp.enable {on

off}`	叢集中的所有節點
`options lldp.enable {on	off}`

- 單一節點：

```
run -node node_name options lldp.enable {on|off}
```

- 所有節點：

```
options lldp.enable {on|off}
```

檢視 **LLDP** 鄰近區域資訊

只要連接埠連接至符合LLDP標準的裝置、即可檢視連接至叢集節點每個連接埠的鄰近裝置相關資訊。您可以使用network device-dinDiscovery show命令來檢視鄰近資訊。

步驟

1. 顯示所有與LLDP相容裝置連線至叢集中節點上之連接埠的相關資訊：

```
network device-discovery show -node node -protocol lldp
```

下列命令顯示連接至節點叢集-1_01上連接埠的鄰近節點。輸出會列出連線至指定節點每個連接埠的啟用LLDP的裝置。如果是 `-protocol` 省略選項、輸出也會列出啟用 CDP 的裝置。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

調整傳輸**LLDP**廣告的時間間隔

LLDP廣告會定期傳送給LLDP鄰近裝置。您可以根據網路流量和網路拓撲的變更、增加或減少傳送 LLDP 通告的時間間隔。

關於這項工作

IEEE建議的預設時間間隔為30秒、但您可以輸入5秒到300秒之間的值。

步驟

1. 顯示節點或叢集中所有節點目前的LLDP通告時間間隔：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - 所有節點：

     ```
     options lldp.xmit.interval
     ```

2. 調整為節點的所有連接埠或叢集中所有節點的所有連接埠傳送LLDP通告的時間間隔：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - 所有節點：

     ```
     options lldp.xmit.interval <interval>
     ```

調整**LLDP**廣告的即時時間值

存留時間（TTL）是LLDP廣告儲存在鄰近的LLDP相容裝置快取中的一段時間。TTL會在每個LLDP封包中通告、並在節點收到LLDP封包時進行更新。TTL可在傳出的LLDP框架中修改。

關於這項工作

- TTL 是計算值、即傳輸間隔的乘積 (`lldp.xmit.interval`）和保留倍數 (`lldp.xmit.hold`）再加上一項。
- 預設的保留倍數值為4、但您可以輸入1到100之間的值。
- 因此、根據IEEE的建議、預設TTL為121秒、但調整傳輸時間間隔並保留倍頻值、即可指定傳出訊框的值、從6秒到30001秒。
- 如果在TTL過期之前移除IP位址、則會快取LLDP資訊、直到TTL過期為止。

步驟

1. 顯示節點或叢集中所有節點的目前保留倍數值：
   - 單一節點：

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

◦ 所有節點：

```
options lldp.xmit.hold
```

2. 調整節點的所有連接埠或叢集中所有節點的所有連接埠上的保留倍頻值：
   ◦ 單一節點：

```
run -node <node_name> options lldp.xmit.hold <hold_value>
```

   ◦ 所有節點：

```
options lldp.xmit.hold <hold_value>
```

檢視或清除 **LLDP** 統計資料

您可以檢視每個節點上叢集和非叢集連接埠的 LLDP 統計資料、以偵測潛在的網路連線問題。LLDP 統計資料是從上次清除時開始累積的。

關於這項工作

對於版本9.10.1及更早版本、由於LLDP一律啟用叢集連接埠、因此會針對這些連接埠上的流量顯示LLDP統計資料。ONTAP必須在非叢集連接埠上啟用 LLDP 、這些連接埠的統計資料才會顯示出來。

對於版本僅9.11.1及更新版本、因為LLDP一律啟用叢集與儲存連接埠、因此會針對這些連接埠上的流量顯示LLDP統計資料。ONTAP必須在非叢集和非儲存連接埠上啟用LLDP、才能顯示這些連接埠的統計資料。

步驟

顯示或清除節點上所有連接埠的目前 LLDP 統計資料：

如果您想要...	輸入...
檢視 LLDP 統計資料	`run -node node_name lldp stats`
清除 LLDP 統計資料	`run -node node_name lldp stats -z`

顯示及清除統計資料範例

下列命令會在 LLDP 統計資料被清除之前顯示這些統計資料。輸出會顯示自上次清除統計資料以來、已傳送和接收的封包總數。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

下列命令會清除LLDP統計資料。

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

清除統計資料後、會在傳送或接收下一個LLDP廣告之後開始累積。

NAS儲存管理

使用System Manager管理NAS傳輸協定

了解如何使用 ONTAP System Manager 進行 NAS 管理

本節主題說明如何在ONTAP 更新版本的更新版本中使用System Manager來設定及管理NAS環境。

如果您使用的是經典系統管理程式（僅ONTAP 適用於更新版本的版本）、請參閱下列主題：

- "NFS組態總覽"
- "SMB 組態概觀"

System Manager支援下列工作流程：

- 您打算用於NAS檔案服務的叢集初始組態。
- 針對不斷變化的儲存需求提供額外的Volume資源配置。
- 業界標準驗證與安全設施的組態與維護。

使用System Manager、您可以在元件層級管理NAS服務：

- 傳輸協定 - NFS 、 SMB 或兩者（ NAS 多重傳輸協定）
- 名稱服務 - DNS 、 LDAP 和 NIS
- 名稱服務交換器
- Kerberos 和 TLS 安全性
- 出口與共享
- qtree
- 使用者和群組的名稱對應

使用 ONTAP 系統管理員為 VMware 資料儲存庫配置 NFS 存儲

在使用Virtual Storage Console for VMware vSphere（VSC）為ONTAP ESXi主機在以VMware為基礎的儲存系統上配置NFS磁碟區之前、請使用System Manager for ONTAP VMware 9.7或更新版本來啟用NFS。

建立之後 "支援NFS的儲存VM" 然後在System Manager中、您可以使用VSC來配置NFS磁碟區和管理資料存放區。

從VSC 7.0開始、VSC就是的一部分 "VMware vSphere虛擬應用裝置適用的工具ONTAP"包括VSC、用於儲存感知（VASA）供應商的vStorage API、以及用於VMware vSphere功能的儲存複寫介面卡（SRA）。

請務必檢查 "NetApp 互通性對照表" 以確認您目前ONTAP 的更新版本與VSC版本之間的相容性。

若要使用 System Manager Classic （適用於 ONTAP 9.7 及更早版本）設定 ESXi 主機對資料存放區的 NFS 存

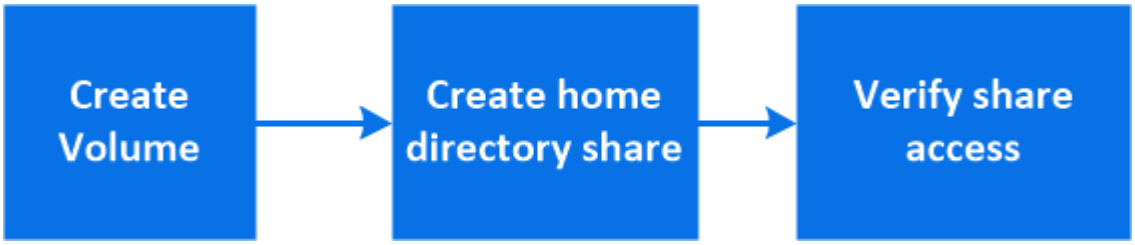
取、請參閱 "使用 VSC 概述的 ESXi NFS 組態"

如需詳細資訊、請參閱 "TR-4597：VMware vSphere ONTAP for VMware" 以及VSC版本的文件。

使用 ONTAP 系統管理員為主目錄設定 NAS 存儲

建立磁碟區、使用SMB傳輸協定為主目錄提供儲存設備。

此程序會為上的主目錄建立新的Volume "現有啟用 SMB 的儲存 VM"。您可以在設定Volume或指定自訂組態時、接受系統預設值。



您可以建立FlexVol卷，或對於具有高效能需求的大型檔案系統，您可以建立FlexGroup區。參見"建立FlexGroup功能區"。

您也可以將本冊的規格儲存至可執行的教戰手冊。如需詳細資料、請前往 "使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"。

步驟

1. 在啟用SMB的儲存VM中新增磁碟區。
   a. 選擇 * 儲存 > 磁碟區 * 、然後按一下 * 新增 * 。
   b. 輸入名稱、選取儲存VM、然後輸入大小。

      只會列出使用 SMB 傳輸協定設定的儲存 VM 。如果只有一個使用 SMB 通訊協定設定的儲存 VM 可用、則不會顯示 * 儲存 VM* 欄位。

      - 如果此時按一下*「Save」（儲存）*、System Manager會使用系統預設值來建立FlexVol 及新增一個「Sof Volume」（資料集）。
      - 您可以按一下*更多選項*來自訂磁碟區的組態、以啟用授權、服務品質及資料保護等服務。 請參閱自訂Volume組態，然後返回此處完成下列步驟。
2. [[step2、Step 2 in the workflow]（工作流程中的步驟2）]單擊* Storage（儲存設備）> Shares*（共享設備）、單擊* Add（添加）、然後選擇 Home Directory（主目錄）*。
3. 在Windows用戶端上、執行下列動作以驗證共用區是否可存取。
   a. 在 Windows 檔案總管中、以下列格式將磁碟機對應至共用區：
      `\\<SMB_Server_Name>\<Share_Name>`

      如果共用名稱是以變數（%w、%d或%u）建立、請務必使用解析名稱來測試存取。
   b. 在新建立的磁碟機上、建立測試檔案、然後刪除該檔案。

自訂**Volume**組態

您可以在新增磁碟區時自訂磁碟區組態、而非接受系統預設值。

步驟

按一下*更多選項*之後、選取您需要的功能、然後輸入所需的值。

- 遠端磁碟區的快取。
- 效能服務層級（服務品質、QoS）。

  從 ONTAP 9.8 開始、您可以指定自訂 QoS 原則或停用 QoS 、以及預設值選擇。

  - 若要停用QoS、請選取*自訂*、現有、然後選取*無*。
  - 如果您選取*自訂*並指定現有的服務層級、則會自動選擇本機層級。
  - 從ONTAP 《支援範圍》9.9.1開始、如果您選擇建立自訂效能服務層級、您可以使用System Manager手動選取您要放置所建立Volume的本機層（手動放置）。

    如果您選擇遠端快取或FlexGroup 是使用「聲音量」選項、則無法使用此選項。

- 供應量（選擇*在叢集內分散磁碟區資料*）FlexGroup 。

  如果您先前在*效能服務層級*下選擇*手動放置*、則無法使用此選項。 否則、您要新增的磁碟區FlexVol 預設會變成一個不全的磁碟區。

- 設定磁碟區之傳輸協定的存取權限。
- 使用SnapMirror（本機或遠端）進行資料保護、然後從下拉式清單中指定目的地叢集的保護原則和設定。
- 選取 * 儲存 * 以建立磁碟區、並將其新增至叢集和儲存 VM 。

儲存磁碟區之後、請返回 [step2] 完成主目錄的資源配置。

使用 **ONTAP** 系統管理器透過 **NFS** 為 **Linux** 伺服器設定 **NAS** 存儲

使用NFS傳輸協定搭配ONTAP 使用NetApp System Manager（9.7及更新版本）、建立Volume以提供Linux伺服器的儲存設備。

此程序會在上建立新的磁碟區 "現有的NFS型儲存VM"。您可以在設定Volume或指定自訂組態時、接受系統預設值。

您可以建立FlexVol卷，或對於具有高效能需求的大型檔案系統，您可以建立FlexGroup區。參見"建立FlexGroup功能區"。

您也可以將本冊的規格儲存至可執行的教戰手冊。如需詳細資料、請前往 "使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"。

如需 ONTAP NFS 通訊協定功能範圍的詳細資訊，請參閱"了解 NFS 協定的 ONTAP 檔案訪問"。

步驟

1. 在啟用 NFS 的儲存 VM 中新增新的 Volume 。

a. 按一下「儲存設備>磁碟區」、然後按一下「新增」。

b. 輸入名稱、選取儲存VM、然後輸入大小。

只會列出使用NFS傳輸協定設定的儲存VM。如果只有一個使用 SMB 通訊協定設定的儲存 VM 可用、則不會顯示 * 儲存 VM* 欄位。

- 如果此時按一下*「Save」（儲存）*、System Manager會使用系統預設值來建立FlexVol 及新增一個「Sof Volume」（資料集）。

  預設匯出原則會授予所有使用者完整存取權。

- 您可以按一下*更多選項*來自訂磁碟區的組態、以啟用授權、服務品質及資料保護等服務。 請參閱自訂Volume組態，然後返回此處完成下列步驟。

2. [[step2-step-prov、Step 2 in the workflow]）]在Linux用戶端上、執行下列動作以驗證存取。

a. 使用儲存VM的網路介面建立及掛載Volume。

b. 在新掛載的磁碟區上、建立測試檔案、將文字寫入其中、然後刪除該檔案。

驗證存取之後、您可以 "使用磁碟區的匯出原則來限制用戶端存取" 並在掛載的磁碟區上設定任何所需的UNIX擁有權和權限。

自訂**Volume**組態

您可以在新增磁碟區時自訂磁碟區組態、而非接受系統預設值。

步驟

按一下*更多選項*之後、選取您需要的功能、然後輸入所需的值。

- 遠端磁碟區的快取。
- 效能服務層級（服務品質、QoS）。

  從 ONTAP 9.8 開始、您可以指定自訂 QoS 原則或停用 QoS 、以及預設值選擇。

  - 若要停用QoS、請選取*自訂*、現有、然後選取*無*。
  - 如果您選取*自訂*並指定現有的服務層級、則會自動選擇本機層級。
  - 從ONTAP 《支援範圍》9.9.1開始、如果您選擇建立自訂效能服務層級、您可以使用System Manager手動選取您要放置所建立Volume的本機層（手動放置）。

    如果您選擇遠端快取或FlexGroup 是使用「聲音量」選項、則無法使用此選項。

- 供應量（選擇*在叢集內分散磁碟區資料*）FlexGroup 。

  如果您先前在*效能服務層級*下選擇*手動放置*、則無法使用此選項。 否則、您要新增的磁碟區FlexVol 預設會變成一個不全的磁碟區。

- 設定磁碟區之傳輸協定的存取權限。
- 使用SnapMirror（本機或遠端）進行資料保護、然後從下拉式清單中指定目的地叢集的保護原則和設定。

- 選取 * 儲存 * 以建立磁碟區、並將其新增至叢集和儲存 VM 。

儲存磁碟區之後、請返回 [step2-complete-prov] 使用NFS完成Linux伺服器的資源配置。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行此工作…	請參閱…
System Manager Classic（ONTAP 僅限版本9.7及更早版本）	"NFS組態總覽"
指令行介面（CLI）ONTAP	"使用 ONTAP CLI 瞭解 NFS 組態"

使用 **ONTAP System Manager** 的匯出策略管理存取

使用匯出原則來啟用Linux用戶端對NFS伺服器的存取。

此程序會建立或修改的匯出原則 "現有的NFS型儲存VM"。

步驟

1. 在System Manager中、按一下* Storage > Volumes *。
2. 按一下NFS啟用的磁碟區、然後按一下*更多*。
3. 按一下「編輯匯出原則」、然後按一下「選取現有原則」或「新增原則」。

使用 **ONTAP** 系統管理員的 **SMB** 為 **Windows** 伺服器設定 **NAS** 存儲

使用System Manager建立磁碟區、使用SMB傳輸協定為Windows伺服器提供儲存設備、ONTAP 此功能可搭配使用支援更新版本的版本。

此程序會在上建立新的磁碟區 "現有啟用 SMB 的儲存 VM" 並建立磁碟區根目錄（/）的共用區。您可以在設定Volume或指定自訂組態時、接受系統預設值。初始SMB組態之後、您也可以建立其他共用區並修改其內容。

您可以建立FlexVol卷，或對於具有高效能需求的大型檔案系統，您可以建立FlexGroup區。參見"建立FlexGroup功能區"。

您也可以將本冊的規格儲存至可執行的教戰手冊。如需詳細資料、請前往 "使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"。

如需 ONTAP SMB 通訊協定功能範圍的詳細資訊，請參閱"參考概述"。

開始之前

- 從 ONTAP 9.13.1 開始，您可以在新磁碟區上預設啟用容量分析和活動追蹤。在 System Manager 中、您可以管理叢集或儲存 VM 層級的預設設定。如需更多資訊、請參閱 "啟用檔案系統分析"。

步驟

1. 在啟用SMB的儲存VM中新增磁碟區。
   a. 按一下「儲存設備>磁碟區」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、然後輸入大小。

只會列出使用 SMB 傳輸協定設定的儲存 VM 。如果只有一個使用 SMB 通訊協定設定的儲存 VM 可用、則不會顯示 * 儲存 VM* 欄位。

- 如果此時選擇 * 儲存 * 、系統管理員會使用系統預設值來建立及新增 FlexVol Volume 。
- 您可以選擇 * 更多選項 * 來自訂磁碟區的組態、以啟用授權、服務品質和資料保護等服務。 請參閱自訂Volume組態，然後返回此處完成下列步驟。

2. [[step2-compl-prov-win, Step 2 in the workflow]切換至Windows用戶端、確認共用區可存取。
   a. 在 Windows 檔案總管中、以下列格式將磁碟機對應至共用區：
   `\\_SMB_Server_Name__Share_Name_`
   b. 在新建立的磁碟機上、建立測試檔案、將文字寫入其中、然後刪除檔案。

驗證存取之後、您可以使用共用ACL限制用戶端存取、並在對應磁碟機上設定任何所需的安全性內容。如需詳細資訊、請參閱 "建立共享" 。

新增或修改共用

您可以在初始SMB組態之後新增其他共用區。共用會以您選取的預設值和屬性建立。稍後可以修改這些項目。

設定共用時、您可以設定下列共用內容：

- 存取權限
- 共用內容
  - 讓包含Hyper-V和SQL Server的共享區能夠透過SMB資料持續可用（從ONTAP 版本號9.10.1開始）。另請參閱：
    - "透過SMB持續提供Hyper-V的共用需求"
    - "SQL Server透過SMB持續可用的共用需求"
  - 使用SMB 3.0加密資料、同時存取此共用區。

初始組態之後、您也可以修改下列內容：

- 符號連結
  - 啟用或停用symlink和wdelinks
- 共用內容
  - 允許用戶端存取快照目錄。
  - 啟用oplocks、允許用戶端在本機上鎖定檔案和快取內容（預設）。
  - 啟用存取型列舉（ABE）、根據使用者的存取權限來顯示共用資源。

步驟

1. 若要在啟用SMB的磁碟區中新增共用區、請按一下「儲存區>共用區」、按一下「新增」、然後選取「**共用」。
2. 若要修改現有的共用區、請按一下「 儲存區 > 共用區 」、然後按一下 ⋮ 並選取「 編輯 」。

自訂**Volume**組態

您可以在新增磁碟區時自訂磁碟區組態、而非接受系統預設值。

步驟

按一下*更多選項*之後、選取您需要的功能、然後輸入所需的值。

- 遠端磁碟區的快取。
- 效能服務層級（服務品質、QoS）。

  從 ONTAP 9.8 開始、您可以指定自訂 QoS 原則或停用 QoS 、以及預設值選擇。

  - 若要停用QoS、請選取*自訂*、現有、然後選取*無*。
  - 如果您選取*自訂*並指定現有的服務層級、則會自動選擇本機層級。
  - 從ONTAP 《支援範圍》9.9.1開始、如果您選擇建立自訂效能服務層級、您可以使用System Manager手動選取您要放置所建立Volume的本機層（手動放置）。

    如果您選擇遠端快取或FlexGroup 是使用「聲音量」選項、則無法使用此選項。

- 供應量（選擇*在叢集內分散磁碟區資料*）FlexGroup 。

  如果您先前在*效能服務層級*下選擇*手動放置*、則無法使用此選項。 否則、您要新增的磁碟區FlexVol 預設會變成一個不全的磁碟區。

- 設定磁碟區之傳輸協定的存取權限。
- 使用SnapMirror（本機或遠端）進行資料保護、然後從下拉式清單中指定目的地叢集的保護原則和設定。
- 選取 * 儲存 * 以建立磁碟區、並將其新增至叢集和儲存 VM 。

儲存磁碟區之後、請返回 [step2-compl-prov-win] 使用SMB完成Windows伺服器的資源配置。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行此工作…	請參閱…
System Manager Classic（ONTAP 僅限版本9.7及更早版本）	"SMB 組態概觀"
指令行介面ONTAP	"使用 CLI 的 SMB 組態概觀"

使用 ONTAP 系統管理器透過 NFS 和 SMB 為 Windows 和 Linux 配置 NAS 存儲

建立磁碟區、使用NFS或SMB傳輸協定為用戶端提供儲存設備。

此程序會在上建立新的磁碟區 "現有的儲存VM同時啟用NFS和SMB傳輸協定"。

NFS 傳輸協定通常用於 Linux 環境。 SMB 通訊協定通常用於 Windows 環境。 不過、 NFS 和 SMB 都可以搭配 Linux 或 Windows 使用。

您可以建立FlexVol卷，或對於具有高效能需求的大型檔案系統，您可以建立FlexGroup區。看"建立FlexGroup功能區"。

您也可以將本冊的規格儲存至可執行的教戰手冊。如需詳細資料、請前往 "使用「可執行教戰手冊」來新增或編輯磁碟區或LUN"。

步驟

1. 在啟用NFS和SMB的儲存VM中新增磁碟區。

   a. 按一下「儲存設備>磁碟區」、然後按一下「新增」。

   b. 輸入名稱、選取儲存VM、然後輸入大小。

      只會列出使用NFS和SMB傳輸協定設定的儲存VM。如果只有一個使用NFS和SMB傳輸協定設定的儲存VM可供使用、則不會顯示「儲存**VM**」欄位。

   c. 單擊 * 更多選項 * 並選擇 * 通過 NFS* 導出。

      預設設定會授予所有使用者完整存取權。您可以稍後在匯出原則中新增更多限制規則。

   d. 選取 * 透過 SMB/CIFS* 分享。

      共享區是以「* Everyon*」群組的預設存取控制清單（ACL）設定為「完全控制」來建立。您可以稍後將限制新增至ACL。

   e. 如果此時按一下*「Save」（儲存）*、System Manager會使用系統預設值來建立FlexVol 及新增一個「Sof Volume」（資料集）。

   或者、您也可以繼續啟用任何其他必要服務、例如授權、服務品質和資料保護。請參閱 自訂Volume組態，然後返回此處完成下列步驟。

2. [[step2-compl-prov-nv-smb, Step 2 in the workrowork]在Linux用戶端上、確認匯出可存取。

   a. 使用儲存VM的網路介面建立及掛載Volume。

   b. 在新掛載的磁碟區上、建立測試檔案、將文字寫入其中、然後刪除該檔案。

3. 在Windows用戶端上、執行下列動作以驗證共用區是否可存取。

   a. 在 Windows 檔案總管中、以下列格式將磁碟機對應至共用區：
      `\\_SMB_Server_Name__Share_Name_`

   b. 在新建立的磁碟機上、建立測試檔案、將文字寫入其中、然後刪除檔案。

   驗證存取權限之後"使用磁碟區的匯出原則限制用戶端存取，使用共用 ACL 限制用戶端存取"，您可以在匯出的和共用的磁碟區上設定任何所需的擁有權和權限。

自訂**Volume**組態

您可以在新增磁碟區時自訂磁碟區組態、而非接受系統預設值。

步驟

按一下*更多選項*之後、選取您需要的功能、然後輸入所需的值。

- 遠端磁碟區的快取。
- 效能服務層級（服務品質、QoS）。

  從 ONTAP 9.8 開始、您可以指定自訂 QoS 原則或停用 QoS 、以及預設值選擇。

  - 若要停用QoS、請選取*自訂*、現有、然後選取*無*。
  - 如果您選取*自訂*並指定現有的服務層級、則會自動選擇本機層級。
  - 從ONTAP 《支援範圍》9.9.1開始、如果您選擇建立自訂效能服務層級、您可以使用System Manager手動選取您要放置所建立Volume的本機層（手動放置）。

    如果您選擇遠端快取或FlexGroup 是使用「聲音量」選項、則無法使用此選項。

- 供應量（選擇*在叢集內分散磁碟區資料*）FlexGroup 。

  如果您先前在*效能服務層級*下選擇*手動放置*、則無法使用此選項。 否則、您要新增的磁碟區FlexVol 預設會變成一個不全的磁碟區。

- 設定磁碟區之傳輸協定的存取權限。
- 使用SnapMirror（本機或遠端）進行資料保護、然後從下拉式清單中指定目的地叢集的保護原則和設定。
- 選取 * 儲存 * 以建立磁碟區、並將其新增至叢集和儲存 VM 。

儲存磁碟區之後、請返回 [step2-compl-prov-nfs-smb] 完成Windows和Linux伺服器的多重傳輸協定資源配置。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作...	請參閱此內容...
System Manager Classic（ONTAP 僅限版本9.7及更早版本）	"SMB與NFS多重傳輸協定組態總覽"
指令行介面ONTAP	• "使用 CLI 的 SMB 組態概觀" • "使用 ONTAP CLI 瞭解 NFS 組態" • "了解安全風格及其影響" • "多重傳輸協定環境中檔案和目錄名稱的區分大小寫"

使用 **ONTAP** 系統管理員透過 **Kerberos** 保護用戶端存取

啟用Kerberos來保護NAS用戶端的儲存存取安全。

此程序會在啟用的現有儲存VM上設定Kerberos "NFS" 或 "中小企業"。

在開始之前、您應該先設定DNS、NTP和 "LDAP" 儲存系統上的。

步驟

1. 在指令行中、設定儲存VM根Volume的UNIX權限。ONTAP

   a. 顯示儲存 VM 根 Volume 的相關權限： `volume show -volume root_vol_name-fields user,group,unix-permissions`。如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

      儲存VM的根Volume必須具有下列組態：

名稱...	正在設定...
UID	root或ID 0
Gid	root或ID 0
UNIX權限	755

   a. 如果未顯示這些值，請使用 `volume modify`命令進行更新。如"指令參考資料ONTAP"需詳細 `volume modify`資訊，請參閱。

2. 設定儲存VM根磁碟區的使用者權限。

   a. 顯示本機 UNIX 使用者： `vserver services name-service unix-user show -vserver vserver_name`。如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-user show`資訊，請參閱。

      儲存VM應設定下列UNIX使用者：

使用者名稱	使用者**ID**	主要群組**ID**
NFS	500	0%
根	0%	0%

+
*附註：*如果NFS用戶端使用者的SPN-UNIX名稱對應存在、則不需要NFS使用者；請參閱步驟5。

   a. 如果未顯示這些值，請使用 `vserver services name-service unix-user modify`命令進行更新。如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-user modify`資訊，請參閱。

3. 設定儲存VM根磁碟區的群組權限。

   a. 顯示本機 UNIX 群組： `vserver services name-service unix-group show -vserver vserver_name`。如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-group show`資訊，請參閱。

      儲存VM應設定下列UNIX群組：

群組名稱	群組**ID**
精靈	1.

群組名稱	群組ID
根	0%

a. 如果未顯示這些值，請使用 `vserver services name-service unix-group modify`命令進行更新。如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-group modify`資訊，請參閱。

4. 切換至System Manager以設定Kerberos
5. 在System Manager中、按一下* Storage > Storage VM*、然後選取儲存VM。
6. 按一下 * 設定 * 。
7. 按一下 → Kerberos 下的。
8. 按一下「Kerberos領域」下的「新增」、然後完成下列各節：
   - 新增Kerberos領域

     視Kdc廠商而定、輸入組態詳細資料。

   - 將網路介面新增至領域

     按一下*「Add*（新增*）」、然後選取網路介面。

9. 如果需要、請將Kerberos主要名稱的對應新增至本機使用者名稱。
   a. 按一下 * 儲存 > 儲存 VM* 、然後選取儲存 VM 。
   b. 按一下 * 設定 * 、然後按一下 → * 名稱對應 * 下的。
   c. 在「* Kerberos到UNIX*」下、使用規則運算式新增模式和替代項目。

使用 ONTAP 系統管理員透過名稱服務提供用戶端訪問

啟用ONTAP 功能支援使用LDAP或NIS來查詢主機、使用者、群組或網路群組資訊、以驗證NAS用戶端。

此程序會在啟用的現有儲存VM上建立或修改LDAP或NIS組態 "NFS" 或 "中小企業"。

對於LDAP組態、您應該擁有環境中所需的LDAP組態詳細資料、而且您應該使用預設ONTAP 的「支援LDAP」架構。

步驟

1. 設定所需的服務：按一下*儲存設備>儲存設備VM*。
2. 選取儲存 VM 、按一下 * 設定 * 、然後按一下 LDAP 或 NIS 。
3. 在名稱服務交換器中加入任何變更：按一下 [名稱服務交換器] 底下的。

使用 ONTAP System Manager 管理目錄和文件

展開System Manager Volume（系統管理器）顯示以查看和刪除目錄和檔案。

從 ONTAP 9 · 9.1 開始、目錄會以低延遲的非同步目錄刪除功能刪除。

如需更多關於在ONTAP 更新版本的資訊中檢視檔案系統、請參閱 "檔案系統分析總覽"。

步驟

1. 選擇*儲存>磁碟區*。展開磁碟區以檢視其內容。

使用 ONTAP System Manager 管理特定於主機的使用者和群組

從ONTAP 版本支援的版本起、您可以使用System Manager來管理UNIX或Windows主機專屬的使用者和群組。

您可以執行下列程序：

Windows	UNIX
• 檢視Windows使用者和群組 • [add-edit-delete-Windows] • [manage-windows-users]	• 檢視UNIX使用者和群組 • [add-edit-delete-UNIX] • [manage-unix-users]

檢視**Windows**使用者和群組

在System Manager中、您可以檢視Windows使用者和群組的清單。

步驟

1. 在System Manager中、按一下* Storage > Storage VM*。
2. 選取儲存VM、然後選取*設定*索引標籤。
3. 捲動至*主機使用者與群組*區域。

   「* Windows *」區段會顯示每個群組中與所選儲存VM相關聯的使用者人數摘要。
4. 按一下 → 「 * Windows* 」區段。
5. 按一下 * 群組 * 索引標籤、然後按一下 ⌄ 群組名稱旁的以檢視該群組的詳細資料。
6. 若要檢視群組中的使用者、請選取該群組、然後按一下「使用者」索引標籤。

新增、編輯或刪除**Windows**群組

在System Manager中、您可以新增、編輯或刪除Windows群組來管理這些群組。

步驟

1. 在System Manager中、檢視Windows群組清單。 請參閱 檢視Windows使用者和群組。
2. 在*群組*索引標籤上、您可以使用下列工作來管理群組：

若要執行此動作…	執行下列步驟…

新增群組	1. 按一下 + Add 。 2. 輸入群組資訊。 3. 指定權限。 4. 指定群組成員（新增本機使用者、網域使用者或網域群組）。
編輯群組	1. 在群組名稱旁、按一下 ⋮、然後按一下 * 編輯 * 。 2. 修改群組資訊。
刪除群組	1. 核取您要刪除的群組旁的方塊。 2. 單擊。 Delete ◦ 注意： * 您也可以按一下群組名稱旁的，然後按一下 * 刪除 * 來刪除單一群組 ⋮ 。

管理**Windows**使用者

在System Manager中、您可以新增、編輯、刪除、啟用或停用Windows使用者、來管理這些使用者。您也可以變更Windows使用者的密碼。

步驟

1. 在System Manager中、檢視群組的使用者清單。 請參閱 檢視Windows使用者和群組。
2. 在*使用者*索引標籤上、您可以使用下列工作來管理使用者：

若要執行此動作...	執行下列步驟...
新增使用者	1. 按一下 + Add 。 2. 輸入使用者資訊。
編輯使用者	1. 在使用者名稱旁、按一下 ⋮、然後按一下 * 編輯 * 。 2. 修改使用者資訊。
刪除使用者	1. 核取您要刪除的使用者旁的方塊。 2. 單擊。 Delete ◦ 注意： * 您也可以按一下使用者名稱旁的、然後按一下 * 刪除 * 來刪除單一使用者 ⋮ 。
變更使用者密碼	1. 在使用者名稱旁、按一下 ⋮、然後按一下 * 變更密碼 * 。 2. 輸入新密碼並加以確認。

啟用使用者	1. 核取您要啟用的每個停用使用者旁的方塊。 2. 單擊。 Enable
停用使用者	1. 核取您要停用的每個啟用的使用者旁的方塊。 2. 單擊。 Disable

檢視**UNIX**使用者和群組

在System Manager中、您可以檢視UNIX使用者和群組的清單。

步驟

1. 在System Manager中、按一下* Storage > Storage VM*。
2. 選取儲存VM、然後選取*設定*索引標籤。
3. 捲動至*主機使用者與群組*區域。

   「* UNIX*」區段會顯示每個群組中與所選儲存VM相關聯的使用者人數摘要。

4. 按一下 → **UNIX** 區段。
5. 按一下*群組*索引標籤、即可檢視該群組的詳細資料。
6. 若要檢視群組中的使用者、請選取該群組、然後按一下「使用者」索引標籤。

新增、編輯或刪除**UNIX**群組

在System Manager中、您可以新增、編輯或刪除UNIX群組來管理這些群組。

步驟

1. 在System Manager中、檢視UNIX群組清單。 請參閱 檢視UNIX使用者和群組。
2. 在*群組*索引標籤上、您可以使用下列工作來管理群組：

若要執行此動作...	執行下列步驟...
新增群組	1. 按一下 + Add 。 2. 輸入群組資訊。 3. （選用）指定相關的使用者。
編輯群組	1. 選取群組。 2. 按一下 Edit 。 3. 修改群組資訊。 4. （選用）新增或移除使用者。

刪除群組	1. 選取您要刪除的群組。 2. 單擊。 Delete

管理**UNIX**使用者

在System Manager中、您可以新增、編輯或刪除Windows使用者、來管理這些使用者。

步驟

1. 在System Manager中、檢視群組的使用者清單。 請參閱 檢視UNIX使用者和群組。
2. 在*使用者*索引標籤上、您可以使用下列工作來管理使用者：

若要執行此動作…	執行下列步驟…
新增使用者	1. 按一下 + Add 。 2. 輸入使用者資訊。
編輯使用者	1. 選取您要編輯的使用者。 2. 按一下 Edit 。 3. 修改使用者資訊。
刪除使用者	1. 選取您要刪除的使用者。 2. 單擊。 Delete

使用 **ONTAP** 系統管理員監控 **NFS** 活動用戶端

從功能不全的9.8開始ONTAP 、System Manager會顯示在叢集上授權NFS時、哪些NFS用戶端連線處於作用中狀態。

這可讓您快速驗證哪些NFS用戶端主動連線至儲存VM、該VM已連線但處於閒置狀態、而且已中斷連線。

對於每個 NFS 用戶端 IP 位址、 **NFS Clients** 顯示畫面會顯示：
* 上次存取時間
* 網路介面 IP 位址
* NFS 連線版本
* 儲存 VM 名稱

此外、在過去48小時內啟用的NFS用戶端清單也會顯示在「儲存設備>磁碟區」顯示中、而「儀表板」顯示中則包含NFS用戶端的數量。

步驟

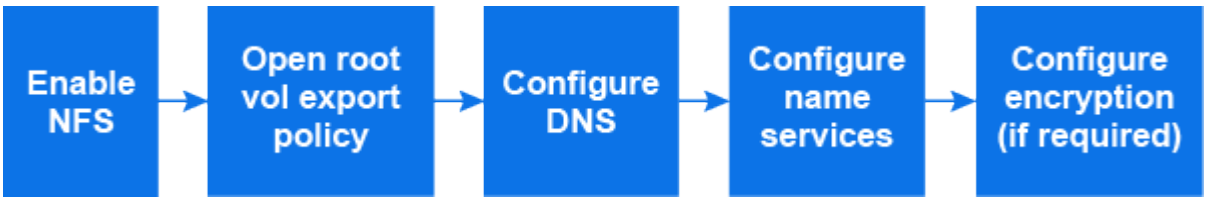
1. 顯示NFS用戶端活動：按一下*主機> NFS用戶端*。

啟用NAS儲存設備

透過 **ONTAP** 系統管理器使用 **NFS** 為 **Linux** 伺服器啟用 **NAS** 存儲

建立或修改儲存VM、以啟用NFS伺服器、將資料提供給Linux用戶端。

使用此程序為 NFS 傳輸協定啟用新的或現有的儲存 VM 。



開始之前

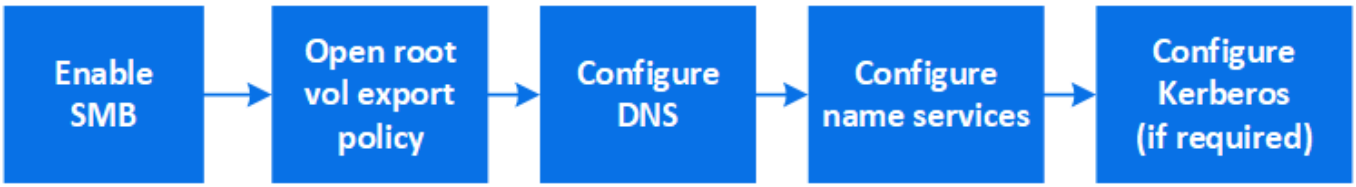
請確定您已記下環境中所需的任何網路、驗證或安全服務的組態詳細資料。

步驟

1. 在儲存 VM 上啟用 NFS 。
   - 對於新的儲存 VM ：按一下 * 儲存 > 儲存 VM* 、按一下 * 新增 * 、輸入儲存 VM 名稱、然後在 **SMB/CIFS** 、 **NFS** 、 **S2** 標籤中、選取 * 啟用 NFS* 。
     i. 確認預設語言。
     ii. 新增網路介面。
     iii. 更新儲存VM管理員帳戶資訊（選用）。
   - 對於現有的儲存 VM ：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * NFS* 下的。
2. 開啟儲存VM根磁碟區的匯出原則：
   a. 按一下「儲存設備>磁碟區」、選取儲存虛擬機器的根磁碟區（預設為_volume名稱__root）、然後按一下「匯出原則」下顯示的原則。
   b. 按一下「新增」以新增規則。
      - 用戶端規格 = `0.0.0.0/0`
      - 存取傳輸協定= NFS
      - 存取詳細資料= UNIX唯讀
3. 設定 DNS 以進行主機名稱解析：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * DNS * 下的。
4. 視需要設定名稱服務。
   a. 按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 LDAP 或 NIS 。
   b. 按一下 「名稱服務交換器」方塊、即可包含任何變更。
5. 如有必要、請設定Kerberos：
   a. 按一下「儲存設備>儲存虛擬機器」、選取儲存虛擬機器、然後按一下「設定」。
   b. 按一下 Kerberos 方塊、然後按一下 * 新增 * 。

建立或修改儲存VM、以啟用SMB伺服器、將資料提供給Windows用戶端。

此程序可為SMB傳輸協定啟用新的或現有的儲存VM。假設您的環境中所需的任何網路、驗證或安全服務都有組態詳細資料可供使用。



步驟

1. 在儲存VM上啟用SMB。
   a. 對於新的儲存虛擬機器：按一下*儲存設備>儲存虛擬機器*、按一下*新增*、輸入儲存虛擬機器名稱、然後在* SMB/CIFS、NFS、S2*索引標籤中、選取*啟用SMB/CIFS*。
      - 輸入下列資訊：
        - 系統管理員名稱與密碼
        - 伺服器名稱
        - Active Directory網域
      - 確認組織單位。
      - 確認DNS值。
      - 確認預設語言。
      - 新增網路介面。
      - 更新儲存VM管理員帳戶資訊（選用）。
   b. 對於現有的儲存 VM ：：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * SMB* 下的。
2. 開啟儲存VM根磁碟區的匯出原則：
   a. 按一下「儲存設備>磁碟區」、選取儲存VM的根磁碟區（預設為_volume名稱_root_）、然後按一下「匯出原則」下顯示的原則。
   b. 按一下「新增」以新增規則。
      - 用戶端規格 = `0.0.0.0/0`
      - 存取通訊協定 = SMB
      - 存取詳細資料 = NTFS 唯讀
3. 設定DNS進行主機名稱解析：
   a. 按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * DNS * 下的。
   b. 切換到DNS伺服器、然後對應SMB伺服器。
      - 建立轉送（A -位址記錄）和反轉（PTTR-指標記錄）查詢項目、將SMB伺服器名稱對應至資料網路介面的IP位址。

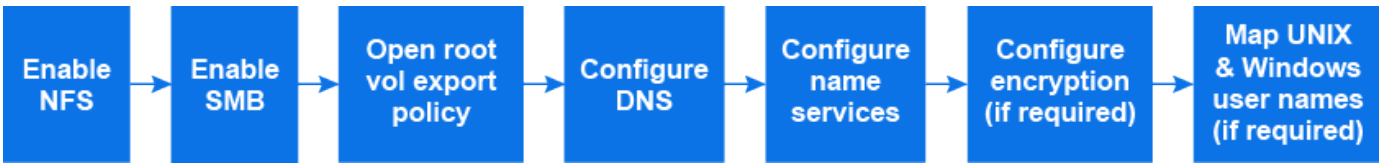
- 如果您使用的是NetBios別名、請建立別名標準名稱（CNAME資源記錄）查詢項目、將每個別名對應至SMB伺服器資料網路介面的IP位址。

4. 視需要設定名稱服務
   a. 按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * LDAP * 或 * NIS* 下的。
   b. 在名稱服務切換檔中加入任何變更：按一下 * 名稱服務切換 * 底下的。
5. 如有必要、請設定Kerberos：
   a. 按一下「儲存設備>儲存虛擬機器」、選取儲存虛擬機器、然後按一下「設定」。
   b. 按一下 * Kerberos * 下的、然後按一下 * 新增 * 。

透過 **ONTAP** 系統管理員使用 **NFS** 和 **SMB** 為 **Windows** 和 **Linux** 啟用 **NAS** 存儲

建立或修改儲存VM、以啟用NFS和SMB伺服器、將資料提供給Linux和Windows用戶端。

啟用新的或現有的儲存 VM 、以使用此程序同時提供 NFS 和 SMB 傳輸協定。



開始之前

請確定您已記下環境中所需的任何網路、驗證或安全服務的組態詳細資料。

步驟

1. 在儲存VM上啟用NFS和SMB。
   a. 對於新的儲存虛擬機器：按一下*儲存設備>儲存虛擬機器*、按一下*新增*、輸入儲存虛擬機器名稱、然後在* SMB/CIFS、NFS、S2*索引標籤中、選取*啟用SMB/CIFS/CIFS 和*啟用**NFS**。
   b. 輸入下列資訊：
      - 系統管理員名稱與密碼
      - 伺服器名稱
      - Active Directory網域
   c. 確認組織單位。
   d. 確認DNS值。
   e. 確認預設語言。
   f. 新增網路介面。
   g. 更新儲存VM管理員帳戶資訊（選用）。
   h. 對於現有的儲存虛擬機器：按一下*儲存設備>儲存虛擬機器*、選取儲存虛擬機器、然後按一下*設定*。如果尚未啟用NFS或SMB、請完成下列子步驟。
      - 按一下 **NFS** 下的。
      - 按一下「 **smb** 」下的。

2. 開啟儲存VM根磁碟區的匯出原則：
   a. 按一下「儲存設備>磁碟區」、選取儲存VM的根磁碟區（預設為_volume名稱_root_）、然後按一下「匯出原則」下顯示的原則。
   b. 按一下「新增」以新增規則。
      - 用戶端規格 = `0.0.0.0/0`
      - 存取傳輸協定= NFS
      - 存取詳細資料 = NFS 唯讀
3. 設定DNS進行主機名稱解析：
   a. 按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * DNS * 下的。
   b. DNS組態完成後、切換至DNS伺服器並對應SMB伺服器。
      - 建立轉送（A -位址記錄）和反轉（PTTR-指標記錄）查詢項目、將SMB伺服器名稱對應至資料網路介面的IP位址。
      - 如果您使用的是NetBios別名、請建立別名標準名稱（CNAME資源記錄）查詢項目、將每個別名對應至SMB伺服器資料網路介面的IP位址。
4. 視需要設定名稱服務：
   a. 按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 LDAP 或 NIS 。
   b. 在名稱服務切換檔中加入任何變更：按一下 * 名稱服務切換 * 底下的。
5. 如有必要、請設定Kerberos：
   a. 按一下「儲存設備>儲存虛擬機器」、選取儲存虛擬機器、然後按一下「設定」。
   b. 按一下 Kerberos 方塊、然後按一下 * 新增 * 。
6. 必要時對應 UNIX 和 Windows 使用者名稱：按一下 * 名稱對應 * 下的，然後按一下 * 新增 * 。

   只有當您的網站具有未隱含對應的 Windows 和 UNIX 使用者帳戶、亦即每個 Windows 使用者名稱的小寫版本與 UNIX 使用者名稱相符時、才應該這麼做。您可以使用 LDAP 、 NIS 或本機使用者來對應使用者名稱。如果您有兩組使用者不相符、則應設定名稱對應。

配置 NFS

使用 ONTAP CLI 瞭解 NFS 組態

您可以使用ONTAP Sf9 CLI命令來設定NFS用戶端對新磁碟區或qtree中新儲存虛擬機器（SVM）所含檔案的存取。

如果您想要以下列方式設定對磁碟區或qtree的存取權、請使用下列程序：

- 您想要使用ONTAP 目前由支援的任何NFS版本：NFSv3、NFSv3、NFSv3、NFSv3 4.1、NFSSv4.2或NFSv3 4.1 with pNFS。
- 您想要使用命令列介面（CLI）、而非System Manager或自動化指令碼工具。

  若要使用 System Manager 設定 NAS 多重傳輸協定存取"同時使用NFS和SMB為Windows和Linux配置NAS儲存設備"、請參閱。

- 您想要使用最佳實務做法、而非探索每個可用選項。

  如需命令語法的詳細"指令參考資料ONTAP"資訊，請參閱。

- UNIX檔案權限將用於保護新磁碟區。
- 您擁有叢集管理員權限、而非SVM管理員權限。

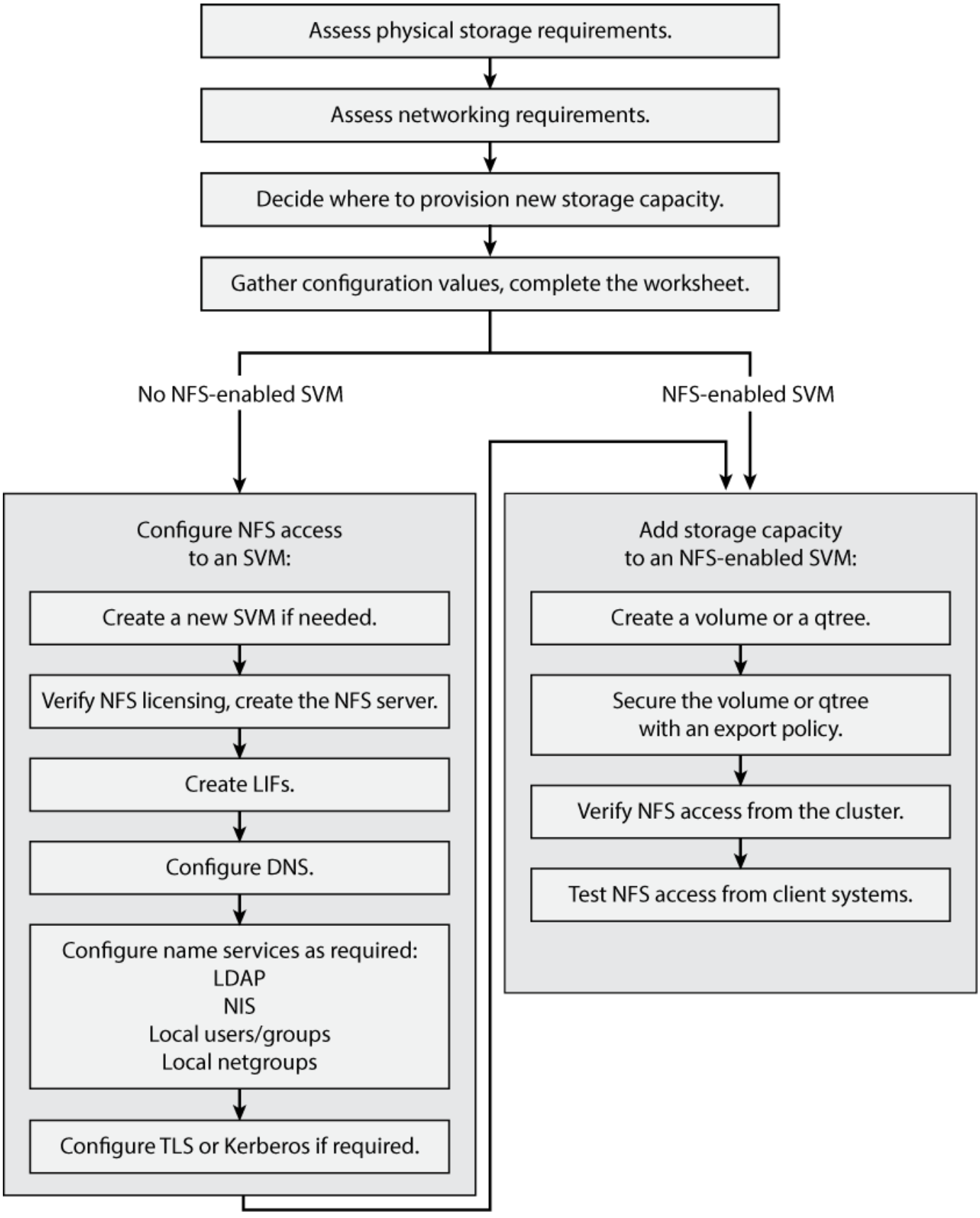
如需 ONTAP NFS 通訊協定功能範圍的詳細資訊，請參閱"了解 NFS 協定的 ONTAP 檔案訪問"。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作…	請參閱…
重新設計的System Manager（ONTAP 提供更新版本的更新版本）	"使用NFS為Linux伺服器配置NAS儲存設備"
System Manager Classic（ONTAP 適用於更新版本的更新版本	"NFS組態總覽"

了解 **ONTAP NFS** 設定工作流程

設定NFS需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、包括設定NFS存取新的或現有的SVM、或將Volume或qtree新增至已完全設定NFS存取的現有SVM。


Assess physical storage requirements.
Assess networking requirements.
Decide where to provision new storage capacity.
Gather configuration values, complete the worksheet.
No NFS-enabled SVM
NFS-enabled SVM
Configure NFS access
to an SVM:
Create a new SVM if needed.
Verify NFS licensing, create the NFS server.
Create LIFs.
Configure DNS.
Configure name services as required:
LDAP
NIS
Local users/groups
Local netgroups
Configure TLS or Kerberos if required.
Add storage capacity
to an NFS-enabled SVM:
Create a volume or a qtree.
Secure the volume or qtree
with an export policy.
Verify NFS access from the cluster.
Test NFS access from client systems.

準備

評估 **ONTAP NFS** 實體儲存需求

在為用戶端配置NFS儲存設備之前、您必須確保現有的集合體中有足夠的空間可容納新磁碟區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型的新Aggregate。

步驟

1. 顯示現有Aggregate中的可用空間：

   ```
   storage aggregate show
   ```

   如果集合體有足夠的空間、請在工作表中記錄其名稱。

   ```
   cluster::> storage aggregate show
   Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
   --------- -------- --------- ----- ------- ------ ------ -----------
   aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                             normal
   aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                             normal
   aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                             normal
   aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                             normal
   6 entries were displayed.
   ```

2. 如果沒有具有足夠空間的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

相關資訊

- "新增磁碟至本機層（Aggregate）"
- "存儲聚合添加磁碟"
- "儲存聚合創建"

評估 **ONTAP NFS** 網路配置需求

將NFS儲存設備提供給用戶端之前、您必須先確認網路設定正確、以符合NFS資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

步驟

1. 顯示可用的實體和虛擬連接埠：

   `network port show`

   - 如果可能、您應該使用資料網路速度最高的連接埠。
   - 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。
   - 如"指令參考資料ONTAP"需詳細 `network port show`資訊，請參閱。

2. 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、請確認該子網路存在且有足夠的可用位址：+

   `network subnet show`

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

   子網路包含屬於同一第3層子網路的IP位址集區。子網路是使用建立的 `network subnet create` 命令。

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

3. 顯示可用的IPspaces：

   `network ipspace show`

   您可以使用預設IPspace或自訂IPspace。

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

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6：

   `network options ipv6 show`

   如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

   深入瞭解 `network options ipv6 show`及 `network options ipv6 modify` "指令參考資料ONTAP"。

瞭解 ONTAP NFS 儲存容量配置

在建立新的NFS Volume或qtree之前、您必須先決定要將其放入新的或現有的SVM、以及SVM所需的組態量。此決定決定決定您的工作流程。

選擇

- 如果您想要在新的SVM上配置磁碟區或qtree、或是在已啟用NFS但尚未設定的現有SVM上配置、請完成「設定NFS存取SVM」和「將NFS儲存設備新增至啟用NFS的SVM」中的步驟。

  設定SVM的NFS存取

  將NFS儲存設備新增至啟用NFS的SVM

  如果符合下列任一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用NFS。
  - 您在不想啟用NFS支援的叢集中有現有的SVM。
  - 您在叢集中有一個或多個NFS型SVM、而您想要在隔離的命名空間中使用另一個NFS伺服器（多租戶案例）。
    您也應該選擇此選項、以便在已啟用NFS但尚未設定的現有SVM上配置儲存設備。如果您為SAN存取建立SVM、或是在建立SVM時未啟用任何傳輸協定、則可能會發生這種情況。

  在SVM上啟用NFS之後、請繼續配置磁碟區或qtree。

- 如果您想要在已完全設定為NFS存取的現有SVM上配置磁碟區或qtree、請完成「將NFS儲存設備新增至已啟用NFS的SVM」中的步驟。

  將NFS儲存設備新增至啟用NFS的SVM

ONTAP NFS 組態工作表

NFS組態工作表可讓您收集必要資訊、以便為用戶端設定NFS存取。

您應該根據您對儲存資源配置的決策、完成工作表的一或兩個區段：

如果您要設定SVM的NFS存取、請完成這兩個部分。

- 設定SVM的NFS存取
- 將儲存容量新增至啟用NFS的SVM

如果您要將儲存容量新增至啟用NFS的SVM、則只應完成下列步驟：

- 將儲存容量新增至啟用NFS的SVM

設定**SVM**的**NFS**存取

*用於建立SVM*的參數

您可以將這些值提供給 `vserver create` 命令、如果您要建立新的 SVM 。

欄位	說明	您的價值

`-vserver`	您為新SVM提供的名稱、可以是完整網域名稱（FQDN）、也可以遵循另一種在叢集內強制執行唯一SVM名稱的慣例。	
`-aggregate`	叢集中有足夠空間可容納新NFS儲存容量的集合體名稱。	
`-rootvolume`	您為SVM根磁碟區提供的唯一名稱。	
`-rootvolume-security-style`	使用SVM的UNIX安全樣式。	`unix`
`-language`	使用此工作流程中的預設語言設定。	`C.UTF-8`
`ipspace`	IPspaces是（儲存虛擬機器（SVM））所在的不同IP位址空間。	

建立**NFS**伺服器的參數

您可以將這些值提供給 `vserver nfs create` 命令：建立新的 NFS 伺服器並指定支援的 NFS 版本。

如果您要啟用NFSv4或更新版本、則應使用LDAP來改善安全性。

欄位	說明	您的價值
`-v3、 -v4.0、 -v4.1、 -v4.1 -pnfs`	視需要啟用NFS版本。 ONTAP 9.8 及更新版本也支援 V4.2 `v4.1` 已啟用。	
`-v4-id-domain`	ID對應網域名稱。	
`-v4-numeric-ids`	支援數字擁有者ID（啟用或停用）。	

*用於建立LIF*的參數

建立生命時，您可以使用命令來提供這些值 `network interface create`。如"指令參考資料ONTAP"需詳細`network interface create`資訊，請參閱。

如果您使用Kerberos、則應在多個LIF上啟用Kerberos。

欄位	說明	您的價值

`-lif`	您為新LIF提供的名稱。	
`-role`	在此工作流程中使用資料LIF角色。	`data`
`-data-protocol`	在此工作流程中僅使用NFS傳輸協定。	`nfs`
`-home-node`	LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。 如"指令參考資料ONTAP"需詳細 `network interface revert`資訊，請參閱。	
`-home-port`	LIF 在返回時傳回的連接埠或介面群組 `network interface revert` 命令會在LIF上執行。	
`-address`	叢集上的IPV4或IPv6位址、用於新LIF的資料存取。	
`-netmask`	LIF的網路遮罩和閘道。	
`-subnet`	IP位址集區。改用 `-address` 和 `-netmask` 自動指派位址和網路遮罩。	
`-firewall-policy`	在此工作流程中使用預設的資料防火牆原則。	`data`

- DNS主機名稱解析參數*

您可以將這些值提供給 `vserver services name-service dns create` 設定 DNS 時的命令。

欄位	說明	您的價值
`-domains`	最多五個DNS網域名稱。	
`-name-servers`	每個DNS名稱伺服器最多三個IP位址。	

名稱服務資訊

建立本機使用者的參數

如果您是使用建立本機使用者、請提供這些值 `vserver services name-service unix-user create`

命令。如果您是透過從統一資源識別元（URI）載入含有UNIX使用者的檔案來設定本機使用者、則不需要手動指定這些值。

	使用者名稱 (-user)	使用者ID (-id)	群組ID (-primary-gid)	全名 (-full-name)
範例	johnm	123.	100	John Miller
1.				
2.				
3.				
…				
n				

建立本機群組的參數

如果您是使用建立本機群組、請提供這些值 `vserver services name-service unix-group create` 命令。如果您是從URI載入含有UNIX群組的檔案來設定本機群組、則不需要手動指定這些值。

	群組名稱 (-name)	群組ID (-id)
範例	工程	100
1.		
2.		
3.		
…		
n		

- NIS的參數*

您可以將這些值提供給 `vserver services name-service nis-domain create` 命令。

這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

欄位	說明	您的價值

`-domain`	SVM將用於名稱查詢的NIS網域。	
`-active`	作用中的NIS網域伺服器。	`true` 或 `false`
`-nis-servers`	網域配置使用的 NIS 伺服器的 IP 位址和主機名稱的逗號分隔清單。	

- LDAP*的參數

您可以將這些值提供給 `vserver services name-service ldap client create` 命令。

您也需要自我簽署的根 CA 憑證 `.pem` 檔案：

欄位	說明	您的價值
`-vserver`	您要為其建立LDAP用戶端組態的SVM名稱。	
`-client-config`	您指派給新LDAP用戶端組態的名稱。	
`-ldap-servers`	以逗號分隔的 LDAP 伺服器 IP 位址和主機名稱清單。	
`-query-timeout`	使用預設值 `3` 此工作流程的秒數。	`3`
`-min-bind-level`	最小連結驗證層級。預設值為 `anonymous`。必須設定為 `sasl` 如果已設定簽署和密封。	
`-preferred-ad-servers`	在以逗號分隔的清單中、依IP位址列出一或多個慣用的Active Directory伺服器。	
`-ad-domain`	Active Directory網域。	
`-schema`	要使用的架構範本。您可以使用預設或自訂架構。	
`-port`	使用預設的 LDAP 伺服器連接埠 `389` 適用於此工作流程。	`389`
`-bind-dn`	「連結」使用者辨別名稱。	

欄位	說明	您的價值
-base-dn	基礎辨別名稱。預設值為 "" （根目錄）。	
-base-scope	使用預設的基礎搜尋範圍 subnet 適用於此工作流程。	subnet
-session-security	啟用LDAP簽署或簽署及密封。預設值為 none。	
-use-start-tls	啟用LDAP over TLS。預設值為 false。	

- Kerberos驗證的參數*

您可以將這些值提供給 vserver nfs kerberos realm create 命令。部分值會因您使用Microsoft Active Directory做為金鑰發佈中心（Kdc）伺服器、MIT或其他UNIX Kdc伺服器而有所不同。

欄位	說明	您的價值
-vserver	與Kdc通訊的SVM。	
-realm	Kerberos領域。	
-clock-skew	用戶端與伺服器之間允許的時鐘偏移。	
-kdc-ip	Kdc IP位址。	
-kdc-port	Kdc連接埠號碼。	
-adserver-name	僅限Microsoft Kdc：AD伺服器名稱。	
-adserver-ip	僅限Microsoft Kdc：AD伺服器IP位址。	
-adminserver-ip	僅UNIX Kdc：管理伺服器IP位址。	
-adminserver-port	僅UNIX Kdc：管理伺服器連接埠號碼。	
-passwordserver-ip	僅UNIX Kdc：密碼伺服器IP位址。	
-passwordserver-port	僅UNIX Kdc：密碼伺服器連接埠。	

-kdc-vendor	Kdc廠商：	{Microsoft
Other}	-comment	任何想要的意見。

您可以將這些值提供給 vserver nfs kerberos interface enable 命令。

欄位	說明	您的價值
-vserver	您要為其建立Kerberos組態的SVM名稱。	
-lif	您要啟用Kerberos的資料LIF。您可以在多個LIF上啟用Kerberos。	
-spn	服務原則名稱（SPN-）	
-permitted-enc-types	Kerberos over NFS 允許的加密類型； aes-256 建議使用、視用戶端功能而定。	
-admin-username	用於直接從Kdc擷取SPN機密金鑰的Kdc系統管理員認證。需要密碼	
-keytab-uri	如果您沒有Kdc系統管理員認證、則會從包含SPN-Key的Kdc取得Keytab檔案。	
-ou	當您使用領域為Microsoft Kdc啟用Kerberos時、會在組織單位（OU）下建立Microsoft Active Directory伺服器帳戶。	

將儲存容量新增至啟用**NFS**的**SVM**

用於建立匯出原則與規則的參數

您可以將這些值提供給 vserver export-policy create 命令。

欄位	說明	您的價值
-vserver	將裝載新磁碟區的SVM名稱。	
-policyname	您為新的匯出原則提供的名稱。	

您可以為每個規則提供這些值 vserver export-policy rule create 命令。

欄位	說明	您的價值
`-clientmatch`	用戶端符合規格。	
`-ruleindex`	匯出規則在規則清單中的位置。	
`-protocol`	在此工作流程中使用NFS。	`nfs`
`-rorule`	唯讀存取的驗證方法。	
`-rwrule`	讀寫存取的驗證方法。	
`-superuser`	超級使用者存取的驗證方法。	
`-anon`	匿名使用者對應的使用者ID。	

您必須為每個匯出原則建立一或多個規則。

`-ruleindex`	**`-clientmatch`**	**`-rorule`**	**`-rwrule`**	**`-superuser`**	**`-anon`**
範例	0.00.0.0/0、@rootaccess_netgroup	任何	KRB5	系統	65534
1.					
2.					
3.					
…					
n					

建立**Volume**的參數

您可以將這些值提供給 `volume create` 如果您要建立的是 Volume 而非 qtree 、則為命令。

欄位	說明	您的價值
`-vserver`	將裝載新磁碟區的新SVM或現有SVM名稱。	
`-volume`	您為新磁碟區提供的唯一描述性名稱。	

`-aggregate`	叢集中有足夠空間可容納新NFS磁碟區的集合體名稱。	
`-size`	您為新磁碟區大小所提供的整數。	
`-user`	設定為磁碟區根目錄擁有者的使用者名稱或ID。	
`-group`	設定為磁碟區根目錄擁有者的群組名稱或ID。	
`--security-style`	使用UNIX安全樣式來執行此工作流程。	`unix`
`-junction-path`	要掛載新磁碟區的根目錄（/）下的位置。	
`-export-policy`	如果您打算使用現有的匯出原則、則可以在建立Volume時輸入其名稱。	

用於建立**qtree**的參數

您可以將這些值提供給 `volume qtree create` 如果您要建立 qtree 而非 Volume 、請執行命令。

欄位	說明	您的價值
`-vserver`	包含qtree之磁碟區所在的SVM名稱。	
`-volume`	將包含新qtree的磁碟區名稱。	
`-qtree`	您為新qtree提供的唯一描述性名稱、64個字元或更少。	
`-qtree-path`	格式中的 qtree path 引數 */vol/volume_name/qtree_name\>* 可以指定、而非將 Volume 和 qtree 指定為個別的引數。	
`-unix-permissions`	選用：qtree的UNIX權限。	
`-export-policy`	如果您打算使用現有的匯出原則、可以在建立qtree時輸入其名稱。	

相關資訊

- "指令參考資料ONTAP"

設定SVM的NFS存取

建立 ONTAP SVM 以進行 NFS 資料訪問

如果叢集中沒有至少一個SVM來提供NFS用戶端的資料存取、則必須建立一個SVM。

開始之前

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

步驟

1. 建立SVM：

   ```
   vserver create -vserver vserver_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace
   ipspace_name
   ```

   - 使用的 UNIX 設定 `-rootvolume-security-style` 選項。
   - 使用預設的 C.UTF-8 `-language` 選項。
   - 。 `ipspace` 設定為選用項目。

2. 驗證新建立的SVM的組態和狀態：

   ```
   vserver show -vserver vserver_name
   ```

   。 `Allowed Protocols` 欄位必須包含 NFS 。您可以稍後再編輯此清單。

   。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會在IPspace ipspaceA中建立SVM以供資料存取：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style unix -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

驗證 **ONTAP SVM** 上 **NFS** 協定的啟用情況

在SVM上設定及使用NFS之前、您必須先確認已啟用該傳輸協定。

關於這項工作

這通常是在 SVM 設定期間完成、但如果您在設定期間未啟用傳輸協定、您可以稍後使用加以啟用 `vserver add-protocols` 命令。

一旦建立LIF、您就無法從其新增或移除通訊協定。

您也可以使用停用 SVM 上的通訊協定 `vserver remove-protocols` 命令。

步驟

1. 檢查SVM目前啟用和停用的傳輸協定：

```
vserver show -vserver vserver_name -protocols
```

您也可以使用 `vserver show-protocols` 用於檢視叢集中所有 SVM 上目前啟用的通訊協定的命令。

2. 如有必要、請啟用或停用傳輸協定：
   - 若要啟用 NFS 傳輸協定：

     ```
     vserver add-protocols -vserver vserver_name -protocols nfs
     ```

   - 若要停用通訊協定：

     ```
     vserver remove-protocols -vserver vserver_name -protocols protocol_name
     [,protocol_name,…]
     ```

3. 確認已啟用和停用的傳輸協定已正確更新：

```
vserver show -vserver vserver_name -protocols
```

範例

下列命令顯示名為VS1的SVM上目前啟用和停用（允許和不允許）的傳輸協定：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   nfs                       cifs, fcp, iscsi, ndmp
```

下列命令可新增以允許透過 NFS 存取 `nfs` 到名為 VS1 的 SVM 上已啟用的通訊協定清單：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols nfs
```

在 **ONTAP SVM** 上開啟 **NFS** 用戶端訪問

SVM根磁碟區的預設匯出原則必須包含允許所有用戶端透過NFS開啟存取的規則。如果沒有這樣的規則、所有NFS用戶端都會被拒絕存取SVM及其磁碟區。

關於這項工作

建立新的SVM時、會自動為SVM的根Volume建立預設匯出原則（稱為預設）。您必須先為預設匯出原則建立一或多個規則、用戶端才能存取SVM上的資料。

您應該確認預設匯出原則中的所有NFS用戶端都已開啟存取權、之後再建立個別磁碟區或qtree的自訂匯出原則、以限制個別磁碟區的存取權。

步驟

1. 如果您使用現有的SVM、請檢查預設的根Volume匯出原則：

```
vserver export-policy rule show
```

命令輸出應類似下列內容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol:  nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

如果存在允許開啟存取的規則、則此工作即告完成。如果沒有、請繼續下一步。

2. 建立SVM根磁碟區的匯出規則：

   `vserver export-policy rule create -vserver` *`vserver_name`* `-policyname default -ruleindex 1 -protocol nfs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`

   如果 SVM 只包含受 Kerberos 保護的磁碟區、您可以設定匯出規則選項 `-rorule`、`-rwrule`和 `-superuser` 將根磁碟區移至 `krb5` 或 `krb5i`。例如：

   `-rorule krb5i -rwrule krb5i -superuser krb5i`

3. 使用驗證規則建立 `vserver export-policy rule show` 命令。

結果

任何NFS用戶端現在都可以存取在SVM上建立的任何Volume或qtree。

建立 **ONTAP NFS** 伺服器

在驗證 NFS 是否已在叢集上取得授權之後、您可以使用 `vserver nfs create` 命令在 SVM 上建立 NFS 伺服器、並指定其支援的 NFS 版本。

關於這項工作

SVM可設定為支援一或多個NFS版本。如果您支援NFSv4或更新版本：

- NFSv4使用者ID對應網域名稱在NFSv4伺服器和目標用戶端上必須相同。

  只要NFSv4伺服器和用戶端使用相同名稱、就不一定需要與LDAP或NIS網域名稱相同。

- 目標用戶端必須支援NFSv4數值ID設定。

- 基於安全考量、您應該在NFSv4部署中使用LDAP作為名稱服務。

開始之前

SVM必須已設定為允許NFS傳輸協定。

步驟

1. 驗證叢集上的NFS是否已獲得授權：

   ```
   system license show -package nfs
   ```

   如果沒有、請聯絡您的銷售代表。

2. 建立NFS伺服器：

   ```
   vserver nfs create -vserver vserver_name -v3 {enabled|disabled} -v4.0
   {enabled|disabled} -v4-id-domain nfsv4_id_domain -v4-numeric-ids
   {enabled|disabled} -v4.1 {enabled|disabled} -v4.1-pnfs {enabled|disabled}
   ```

   您可以選擇啟用任何NFS版本組合。如果您想要支援 pNFS 、則必須同時啟用兩者 `-v4.1` 和 `-v4.1-pnfs` 選項：

   如果您啟用v4或更新版本、也應該確定下列選項設定正確：

   - `-v4-id-domain`

     此選用參數指定NFSv4傳輸協定所定義之使用者和群組名稱字串形式的網域部分。根據預設、ONTAP 如果已設定NIS網域、則會使用該NIS網域；如果未設定、則會使用DNS網域。您必須提供與目標用戶端所使用的網域名稱相符的值。

   - `-v4-numeric-ids`

     此選用參數可指定是否啟用NFSv4擁有者屬性中的數字字串識別碼支援。預設設定為已啟用、但您應該確認目標用戶端是否支援此設定。

   您可以稍後使用啟用其他 NFS 功能 `vserver nfs modify` 命令。

3. 確認NFS正在執行：

   ```
   vserver nfs status -vserver vserver_name
   ```

4. 確認NFS已設定為所需：

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

範例

下列命令會在名為VS1的SVM上建立NFS伺服器、並啟用NFSv3和NFSv4.0：

```
vs1::> vserver nfs create -vserver vs1 -v3 enabled -v4.0 enabled -v4-id
-domain my_domain.com
```

下列命令可驗證名為VS1的新NFS伺服器的狀態和組態值：

```
vs1::> vserver nfs status -vserver vs1
The NFS server is running on Vserver "vs1".

vs1::> vserver nfs show -vserver vs1

                                Vserver: vs1
                  General NFS Access: true
                               NFS v3: enabled
                             NFS v4.0: enabled
                          UDP Protocol: enabled
                          TCP Protocol: enabled
                 Default Windows User: -
                  NFSv4.0 ACL Support: disabled
    NFSv4.0 Read Delegation Support: disabled
   NFSv4.0 Write Delegation Support: disabled
             NFSv4 ID Mapping Domain: my_domain.com
...
```

建立 **ONTAP NFS** 生命

LIF是與實體或邏輯連接埠相關聯的IP位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

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

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果您使用Kerberos驗證、請在多個LIF上啟用Kerberos。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

  深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。

- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他LIF。ONTAP

從ONTAP 支援FFC-NVMe的支援功能到支援的功能表9.4開始。如果您要建立FC-NVMe LIF、應該注意下列事項：

- NVMe傳輸協定必須受到建立LIF的FC介面卡支援。
- FC-NVMe是資料生命中唯一的資料傳輸協定。
- 必須為每個支援SAN的儲存虛擬機器（SVM）設定一個LIF處理管理流量。
- NVMe LIF和命名空間必須裝載在同一個節點上。
- 每個SVM只能設定一個處理資料流量的NVMe LIF

步驟

1. 建立LIF：

   ```
   network interface create -vserver vserver_name -lif lif_name -role data -data
   -protocol nfs -home-node node_name -home-port port_name {-address IP_address
   -netmask IP_address | -subnet-name subnet_name} -firewall-policy data -auto
   -revert {true|false}
   ```

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

選項	說明
《》第9.5版及更早版本* ONTAP	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`
版本**9.6**及更新版本 ONTAP	`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol nfs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true	false}`

   - 。 `-role` 使用服務原則（從 ONTAP 9.6 開始）建立 LIF 時不需要參數。
   - 。 `-data-protocol` 必須在建立 LIF 時指定參數、而且必須在稍後修改、才能銷毀及重新建立資料 LIF 。
     - 。 `-data-protocol` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。
   - `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

     您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 `-auto-revert` 選項。

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

- `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
- 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料ONTAP"。
- 適用於 `-firewall-policy` 選項、請使用相同的預設值 `data` 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 `false`**但您可以將其設定為** `false` 視環境中的網路管理原則而定。

  a. 使用確認 LIF 已成功建立 `network interface show` 命令。

  b. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

  c. 如果您使用Kerberos、請重複步驟1到3以建立其他生命週期。

     Kerberos必須在每個生命區上分別啟用。

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol nfs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol nfs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

下列命令顯示如何建立指派給的 NAS 資料 LIF `default-data-files` 服務原則：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

相關資訊

- "網路ping"
- "網路介面"

為 ONTAP NFS SVM 主機名稱解析啟用 DNS

您可以使用 `vserver services name-service dns` 命令在 SVM 上啟用 DNS 、並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。。 `vserver services name-service dns create` 如果只輸入一個 DNS 伺服器名稱、命令會發出警告。

關於這項工作

深入瞭解 "在 SVM 上設定動態 DNS"。

步驟

1. 在SVM上啟用DNS：

   ```
   vserver services name-service dns create -vserver vserver_name -domains
   domain_name -name-servers ip_addresses -state enabled
   ```

   下列命令可啟用SVM VS1上的外部DNS伺服器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   > ℹ 。 `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用顯示 DNS 網域組態 `vserver services name-service dns show` 命令。

   下列命令會顯示叢集中所有SVM的DNS組態：

```
vserver services name-service dns show
                                                Name
Vserver           State     Domains              Servers
----------------- --------- ------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
---------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

設定名稱服務

了解 **ONTAP NFS** 名稱服務

根據儲存系統的組態、ONTAP 支援功能需要能夠查詢主機、使用者、群組或網路群組資訊、才能正確存取用戶端。您必須設定名稱服務、才能讓ONTAP 支援功能支援使用本機或外部名稱服務來取得此資訊。

您應該使用名稱服務（例如NIS或LDAP）、以便在用戶端驗證期間進行名稱查詢。最好盡可能使用LDAP來提高安全性、尤其是在部署NFSv4或更新版本時。如果外部名稱伺服器無法使用、您也應該設定本機使用者和群組。

名稱服務資訊必須在所有來源上保持同步。

配置 **ONTAP NFS** 名稱服務切換表

您必須正確設定名稱服務交換器表、才能讓ONTAP 支援功能支援使用者參考本機或外部名稱服務、以擷取主機、使用者、群組、網路群組或名稱對應資訊。

開始之前

您必須決定要用於主機、使用者、群組、netgroup或名稱對應的名稱服務、以符合您的環境需求。

如果您打算使用netGroups、則必須依照RFC 5952中的指定、縮短及壓縮netGroups中指定的所有IPv6位址。

關於這項工作

請勿包含未使用的資訊來源。例如、如果您的環境中未使用 NIS 、請勿指定 `-sources nis` 選項。

步驟

1. 將必要的項目新增至名稱服務交換器表：

   `vserver services name-service ns-switch create -vserver` *`vserver_name`* `-database` *`database_name`* `-sources` *`source_names`*

2. 驗證名稱服務交換器表格是否包含所需順序的預期項目：

   `vserver services name-service ns-switch show -vserver` *`vserver_name`*

   如果您想要進行任何修正、您必須使用 `vserver services name-service ns-switch modify` 或 `vserver services name-service ns-switch delete` 命令。

範例

下列範例會在名稱服務交換器表中建立新項目、讓SVM VS1使用本機netgroup檔案和外部NIS伺服器、以該順序查詢netgroup資訊：

```
cluster::> vserver services name-service ns-switch create -vserver vs1
-database netgroup -sources files,nis
```

完成後

- 您必須設定您為SVM指定的名稱服務、才能提供資料存取。
- 如果您刪除SVM的任何名稱服務、也必須將其從名稱服務交換器表格中移除。

  如果您無法從名稱服務交換器表格中刪除名稱服務、用戶端對儲存系統的存取可能無法如預期般運作。

設定本機**UNIX**使用者和群組

了解 **ONTAP NFS SVM** 的本機 **UNIX** 使用者和群組

您可以使用SVM上的本機UNIX使用者和群組進行驗證和名稱對應。您可以手動建立UNIX使用者和群組、也可以從統一資源識別元（URI）載入包含UNIX使用者或群組的檔案。

叢集中的本機UNIX使用者群組和群組成員、預設上限為32、768。叢集管理員可以修改此限制。

在 ONTAP NFS SVM 上建立本機 UNIX 用戶

您可以使用 `vserver services name-service unix-user create` 建立本機 UNIX 使用者的命令。本機UNIX使用者是您在SVM上建立的UNIX使用者、是UNIX名稱服務選項、用於處理名稱對應。

步驟

1. 建立本機UNIX使用者：

   `vserver services name-service unix-user create -vserver` *`vserver_name`* `-user` *`user_name`* `-id` *`integer`* `-primary-gid` *`integer`* `-full-name` *`full_name`*

   `-user` *`user_name`* 指定使用者名稱。使用者名稱長度必須少於64個字元。

   `-id` *`integer`* 指定您指派的使用者 ID 。

   `-primary-gid` *`integer`* 指定主要群組 ID 。這會將使用者新增至主要群組。建立使用者之後、您可以手動將使用者新增至任何想要的其他群組。

範例

下列命令會在名為VS1的SVM上建立名為johnm（全名「John Miller」）的本機UNIX使用者。使用者的 ID 為 123 、主要群組 ID 為 100 。

```
node::> vserver services name-service unix-user create -vserver vs1 -user
johnm -id 123
-primary-gid 100 -full-name "John Miller"
```

在 ONTAP NFS SVM 上載入本機 UNIX 使用者列表

除了在 SVM 中手動建立個別的本機 UNIX 使用者之外、您也可以從統一的資源識別元（ URI ）將本機 UNIX 使用者清單載入 SVM 、以簡化工作。（`vserver services name-service unix-user load-from-uri`）。

步驟

1. 建立包含您要載入之本機UNIX使用者清單的檔案。

   檔案必須包含 UNIX 中的使用者資訊 `/etc/passwd` 格式：

   `user_name: password: user_ID: group_ID: full_name`

   命令會捨棄的值 *`password`* 欄位和之後欄位的值 *`full_name`* 欄位 (*`home_directory`* 和 *`shell`*）。

   支援的檔案大小上限為2.5 MB。

2. 確認清單中沒有任何重複資訊。

   如果清單包含重複的項目、則載入清單時會失敗並顯示錯誤訊息。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX使用者清單的檔案載入SVM：

   ```
   vserver services name-service unix-user load-from-uri -vserver vserver_name
   -uri {ftp|http|ftps|https}://uri -overwrite {true|false}
   ```

   `-overwrite {true false}` 指定是否覆寫項目。預設值為 `false`。

範例

下列命令會從 URI 載入本機 UNIX 使用者清單 `ftp://ftp.example.com/passwd` 進入名為 VS1 的 SVM 。SVM上的現有使用者不會被URI的資訊覆寫。

```
node::> vserver services name-service unix-user load-from-uri -vserver vs1
-uri ftp://ftp.example.com/passwd -overwrite false
```

在 ONTAP NFS SVM 上建立本機 UNIX 群組

您可以使用 `vserver services name-service unix-group create` 建立 SVM 本機 UNIX 群組的命令。本機UNIX群組適用於本機UNIX使用者。

步驟

1. 建立本機UNIX群組：

   ```
   vserver services name-service unix-group create -vserver vserver_name -name
   group_name -id integer
   ```

   `-name group_name` 指定群組名稱。群組名稱長度必須少於64個字元。

   `-id integer` 指定您指派的群組 ID 。

範例

下列命令會在名為VS1的SVM上建立名為eng的本機群組。群組的ID為101。

```
vs1::> vserver services name-service unix-group create -vserver vs1 -name
eng -id 101
```

將使用者新增至 ONTAP NFS SVM 上的本機 UNIX 群組

您可以使用 `vserver services name-service unix-group adduser` 命令、將使

用者新增至 SVM 本機的輔助 UNIX 群組。

步驟

1. 新增使用者至本機UNIX群組：

`vserver services name-service unix-group adduser -vserver` *`vserver_name`* `-name` *`group_name`* `-username` *`user_name`*

`-name` *`group_name`* 指定要新增使用者的 UNIX 群組名稱、以及使用者的主要群組。

範例

下列命令會將名為max的使用者新增至名為VS1的SVM上名為eng的本機UNIX群組：

```
vs1::> vserver services name-service unix-group adduser -vserver vs1 -name
eng
-username max
```

從 **ONTAP NFS SVM** 上的 **URI** 載入本機 **UNIX** 群組

除了手動建立個別的本機 UNIX 群組之外、您也可以使用、從統一的資源識別元（ URI ）將本機 UNIX 群組清單載入 SVM `vserver services name-service unix-group load-from-uri` 命令。

步驟

1. 建立包含您要載入之本機UNIX群組清單的檔案。

   檔案必須包含 UNIX 中的群組資訊 `/etc/group` 格式：

   `group_name: password: group_ID: comma_separated_list_of_users`

   命令會捨棄的值 *`password`* 欄位。

   支援的檔案大小上限為 1 MB 。

   群組檔案中每一行的長度上限為32、768個字元。

2. 確認清單中沒有任何重複資訊。

   清單不得包含重複的項目、否則載入清單將會失敗。如果 SVM 中已有項目、您必須設定 `-overwrite` 參數至 `true` 以新檔案覆寫所有現有項目、或確保新檔案不包含任何重複現有項目的項目。

3. 將檔案複製到伺服器。

   儲存系統必須透過HTTP、HTTPS、FTP或FTPS連線至伺服器。

4. 判斷檔案的URI是什麼。

   URI是您提供給儲存系統的位址、用以指出檔案所在位置。

5. 從URI將包含本機UNIX群組清單的檔案載入SVM：

   `vserver services name-service unix-group load-from-uri -vserver` *vserver_name* `-uri {ftp|http|ftps|https}://`*uri* `-overwrite {true|false}`

   `-overwrite true false}` 指定是否覆寫項目。預設值為 `false`。如果您將此參數指定為 `true`， ONTAP 會將指定 SVM 的整個現有本機 UNIX 群組資料庫，取代為您所載入檔案的項目。

範例

下列命令會從 URI 載入本機 UNIX 群組清單 `ftp://ftp.example.com/group` 進入名為 VS1 的 SVM 。SVM上的現有群組不會被URI的資訊覆寫。

```
vs1::> vserver services name-service unix-group load-from-uri -vserver vs1
-uri ftp://ftp.example.com/group -overwrite false
```

使用**netGroups**

了解 **ONTAP NFS SVM** 上的網路群組

您可以使用netGroups進行使用者驗證、並在匯出原則規則中比對用戶端。您可以從外部名稱伺服器（ LDAP 或 NIS ）提供網路群組的存取權、也可以使用將網路群組從統一的資源識別碼（ URI ）載入 SVM `vserver services name-service netgroup load` 命令。

開始之前

在使用netGroups之前、您必須確保符合下列條件：

- 不論來源（NIS、LDAP或本機檔案）為何、網路群組中的所有主機都必須同時擁有轉送（A）和反向（PTr）DNS記錄、才能提供一致的轉送和反向DNS查詢。

  此外、如果用戶端的IP位址有多筆PTr記錄、則所有這些主機名稱都必須是netgroup的成員、並具有對應的A記錄。

- 不論來源（NIS、LDAP或本機檔案）為何、netGroups中所有主機的名稱都必須正確拼寫、並使用正確的大小寫。在netGroups中使用的主機名稱若不一致、可能會導致非預期的行為、例如匯出檢查失敗。
- 在netGroups中指定的所有IPv6位址都必須依照RFC 5952中的指定來縮短和壓縮。

  例如、2011：hu9：0：0：0：0：3：1必須縮短為2011：hu9：3：1。

關於這項工作

使用netGroups時、您可以執行下列作業：

- 您可以使用 `vserver export-policy netgroup check-membership` 用於確定客戶端 IP 是否是某個 netgroup 的成員的命令。
- 您可以使用 `vserver services name-service getxxbyyy netgrp` 用於檢查用戶端是否為 netgroup 的一部分的命令。

執行查詢的基礎服務是根據設定的名稱服務交換器順序來選取。

從 **ONTAP NFS SVM** 上的 **URI** 載入網路組

您可以在匯出原則規則中使用符合用戶端的方法之一、就是使用netGroups中列出的主機。您可以將網路群組從統一的資源識別碼（ URI ）載入 SVM 、以取代使用儲存在外部名稱伺服器中的網路群組 (`vserver services name-service netgroup load`) 。

開始之前

Netgroup檔案在載入SVM之前、必須符合下列要求：

- 檔案必須使用與NIS相同的適當netgroup文字檔格式。

  此功能可在載入netgroup文字檔格式之前檢查其內容。ONTAP如果檔案包含錯誤、則不會載入、並會顯示訊息、指出您必須在檔案中執行的修正。更正錯誤後、您可以將netgroup檔案重新載入指定的SVM。

- netgroup檔案中主機名稱中的任何字母字元都應為小寫。
- 支援的檔案大小上限為 5 MB 。
- 巢狀網路群組支援的最大層級為1000。
- 在netgroup檔案中定義主機名稱時、只能使用主要DNS主機名稱。

  為了避免匯出存取問題、不應使用DNS CNAME/或循環配置資源記錄來定義主機名稱。

- netgroup檔案中三個群組的使用者和網域部分應保持空白、因為ONTAP 無法支援它們。

  僅支援主機/IP部分。

關於這項工作

支援各主機的netgroup搜尋本機netgroup檔案。ONTAP載入netgroup檔案後ONTAP 、Syname會自動建立netgroup .byhost對應、以啟用逐主機的netgroup搜尋。這可大幅加速本機netgroup搜尋、以處理匯出原則規則來評估用戶端存取。

步驟

1. 從URI將網路群組載入SVM：

   ```
   vserver services name-service netgroup load -vserver vserver_name -source
   {ftp|http|ftps|https}://uri
   ```

   載入netgroup檔案並建置netgroup。byhost對應可能需要數分鐘的時間。

   如果要更新netgroup、您可以編輯該檔案、然後將更新的netgroup檔案載入SVM。

範例

下列命令會從 HTTP URL 將 netgroup 定義載入名為 VS1 的 SVM `http://intranet/downloads/corp-netgroup`：

```
vs1::> vserver services name-service netgroup load -vserver vs1
-source http://intranet/downloads/corp-netgroup
```

驗證 ONTAP NFS SVM 網路組定義

將網路群組載入 SVM 後、您可以使用 `vserver services name-service netgroup status` 用於驗證 netgroup 定義狀態的命令。這可讓您判斷支援SVM的所有節點上的netgroup定義是否一致。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 驗證netgroup定義的狀態：

   ```
   vserver services name-service netgroup status
   ```

   您可以在更詳細的檢視畫面中顯示其他資訊。

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

設定權限層級後、下列命令會顯示所有SVM的netgroup狀態：

```
vs1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when
         directed to do so by technical support.
Do you wish to continue? (y or n): y

vs1::*> vserver services name-service netgroup status
Virtual
Server    Node            Load Time           Hash Value
--------- --------------- -------------------
--------------------------------
vs1
          node1           9/20/2006 16:04:53
e6cb38ec1396a280c0d2b77e3a84eda2
          node2           9/20/2006 16:06:26
e6cb38ec1396a280c0d2b77e3a84eda2
          node3           9/20/2006 16:08:08
e6cb38ec1396a280c0d2b77e3a84eda2
          node4           9/20/2006 16:11:33
e6cb38ec1396a280c0d2b77e3a84eda2
```

為 ONTAP NFS SVM 建立 NIS 域配置

如果您的環境中使用網路資訊服務（ NIS ）來提供名稱服務、則必須使用為 SVM 建立 NIS 網域組態 `vserver services name-service nis-domain create` 命令。

開始之前

在SVM上設定NIS網域之前、所有已設定的NIS伺服器都必須可供使用且可連線。

如果您打算使用NIS進行目錄搜尋、則NIS伺服器中的對應每個項目不得超過1,024個字元。請勿指定不符合此限制的NIS伺服器。否則、用戶端存取相依於NIS項目可能會失敗。

關於這項工作

如果您的 NIS 資料庫包含 `netgroup.byhost` MAP 、 ONTAP 可以使用它來加快搜尋速度。。 `netgroup.byhost` 和 `netgroup` 目錄中的地圖必須隨時保持同步、以避免用戶端存取問題。從 ONTAP 9.7 開始、 NIS `netgroup.byhost` 您可以使用快取項目 `vserver services name-service nis-domain netgroup-database` 命令。

不支援使用 NIS 進行主機名稱解析。

步驟

1. 建立NIS網域組態：

   ```
   vserver services name-service nis-domain create -vserver vs1 -domain
   <domain_name> -nis-servers <IP_addresses>
   ```

您最多可以指定10部NIS伺服器。

> 這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

2. 確認網域已建立：

```
vserver services name-service nis-domain show
```

範例

下列命令會針對在 SVM 上以 IP 位址的 NIS 伺服器 `192.0.2.180`命名的 `vs1` NIS 網域建立 NIS 網域組態 `nisdomain`：

```
vs1::> vserver services name-service nis-domain create -vserver vs1
-domain nisdomain -nis-servers 192.0.2.180
```

使用**LDAP**

了解如何在 **ONTAP NFS SVM** 上使用 **LDAP** 名稱服務

如果您的環境中使用LDAP來提供名稱服務、您必須與LDAP管理員合作、以判斷需求和適當的儲存系統組態、然後將SVM啟用為LDAP用戶端。

從ONTAP 功能支援的版本為：從功能支援的版本為：LDAP通道繫結、依預設會同時支援Active Directory和名稱服務LDAP連線。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與名稱伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding` 參數 `ldap client modify` 命令。

如需詳細資訊、請參閱
"2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

- 在設定LDAP ONTAP 以供使用之前、您應確認您的站台部署符合LDAP伺服器和用戶端組態的最佳實務做法。尤其必須符合下列條件：
  - LDAP伺服器的網域名稱必須符合LDAP用戶端上的項目。
  - LDAP伺服器支援的LDAP使用者密碼雜湊類型必須包含ONTAP 下列項目：
    - 加密（所有類型）和SHA-1（SHa、SSHA）。
    - 從ONTAP 《Sf9.8》、《SHA-2雜湊》（SHA-256、SSH-384、SHA-512、SSHA-256、 也支援SSHA-384和SSHA-512）。
  - 如果LDAP伺服器需要工作階段安全性措施、您必須在LDAP用戶端中進行設定。

    下列工作階段安全性選項可供使用：
    - LDAP簽署（提供資料完整性檢查）及LDAP簽署與密封（提供資料完整性檢查與加密）
    - 啟動TLS
    - LDAPS（LDAP over TLS或SSL）

- 若要啟用已簽署和密封的LDAP查詢、必須設定下列服務：
  - LDAP伺服器必須支援GSPI（Kerberos）SASL機制。
  - LDAP伺服器必須在DNS伺服器上設定DNS A/AAAA記錄和PTr記錄。
  - Kerberos伺服器必須在DNS伺服器上存在SRV.記錄。
- 若要啟用Start TLS或LDAPS、應考慮下列事項。
  - 使用Start TLS而非LDAPS是NetApp最佳實務做法。
  - 如果使用LDAPS、則LDAP伺服器必須在ONTAP 支援TLS或支援SSL的情況下、於支援更新版本的支援更新版本中啟用。不支援SSL。ONTAP
  - 必須已在網域中設定憑證伺服器。
- 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：
  - 這兩個網域都應設定下列其中一個信任關係：
    - 雙向
    - 單向、主要信任參照網域
    - 父-子
  - DNS必須設定為解析所有參照的伺服器名稱。
  - 網域密碼在-bind-as CIFS伺服器設定為true時、應相同進行驗證。

> LDAP參照追蹤不支援下列組態。
>
> - 所有ONTAP 版本：
>   - 管理SVM上的LDAP用戶端
> - 適用於更新版本的支援功能（9.9.1及更新版本均支援）ONTAP ：
>   - LDAP 簽署與密封（ `-session-security` 選項）
>   - 加密 TLS 連線（ `-use-start-tls` 選項）
>   - 透過 LDAPS 連接埠 636 （ `-use-ldaps-for-ad-ldap` 選項）

- 在SVM上設定LDAP用戶端時、您必須輸入LDAP架構。

  在大多數情況下、預設ONTAP 的架構之一將是適當的。不過、如果您環境中的LDAP架構與這些架構不同、則必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端。請洽詢您的LDAP管理員、瞭解您環境的需求。

- 不支援使用LDAP進行主機名稱解析。

以取得更多資訊

- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"
- "在 ONTAP SMB SVM 上安裝自我簽署的根 CA 憑證"

為 **ONTAP NFS SVM** 建立新的 **LDAP** 用戶端模式

如果您環境中的LDAP架構不同於ONTAP 支援功能的預設值、您必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端組態。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU（Windows 2008、Windows 2012及更新版本的AD伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

如果您需要使用非預設LDAP架構、則必須先建立該架構、再建立LDAP用戶端組態。在建立新架構之前、請先諮詢您的LDAP管理員。

無法修改由功能提供的預設LDAP架構ONTAP 。若要建立新架構、請建立複本、然後據此修改複本。

步驟

1. 顯示現有的LDAP用戶端架構範本、以識別您要複製的範本：

   ```
   vserver services name-service ldap client schema show
   ```

2. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

3. 複製現有的LDAP用戶端架構：

   ```
   vserver services name-service ldap client schema copy -vserver vserver_name
   -schema existing_schema_name -new-schema-name new_schema_name
   ```

4. 修改新的架構並針對您的環境自訂：

   ```
   vserver services name-service ldap client schema modify
   ```

5. 返回管理權限層級：

   ```
   set -privilege admin
   ```

為 **ONTAP NFS** 存取建立 **LDAP** 用戶端配置

如果您想要 ONTAP 存取環境中的外部 LDAP 或 Active Directory 服務、則必須先在儲存系統上設定 LDAP 用戶端。

開始之前

Active Directory 網域解析清單中前三部伺服器之一必須為正常運作並提供資料。否則、此工作將會失敗。

有多部伺服器、其中有兩部以上的伺服器在任何時間點停機。

步驟

1. 請洽詢您的 LDAP 管理員、以決定的適當組態值 `vserver services name-service ldap client create` 命令：

   a. 指定與LDAP伺服器的網域型或位址型連線。

      ◦ `-ad-domain` 和 `-servers` 選項是互斥的。

      - 使用 `-ad-domain` 在 Active Directory 網域中啟用 LDAP 伺服器探索的選項。
        - 您可以使用 `-restrict-discovery-to-site` 將 LDAP 伺服器探索限制在指定網域的 CIFS 預設網站的選項。如果使用此選項、您也需要使用指定 CIFS 預設站台 `-default-site`。
      - 您可以使用 `-preferred-ad-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個偏好的 Active Directory 伺服器。建立用戶端之後、您可以使用修改此清單 `vserver services name-service ldap client modify` 命令。
      - 使用 `-servers` 選項可依以逗號分隔的清單中的 IP 位址來指定一或多個 LDAP 伺服器（ Active Directory 或 UNIX ）。

        已棄用。 `-ldap-servers`字段替換 `-servers`場地。此欄位可取得 LDAP 伺服器的主機名稱或 IP 位址。

   b. 指定預設或自訂LDAP架構。

      大多數LDAP伺服器都可以使用ONTAP 由功能介紹的預設唯讀架構。除非有其他需求、否則最好使用這些預設架構。如果是、您可以複製預設架構（它們是唯讀的）、然後修改複本、藉此建立自己的架構。

      預設架構：

      - MS-AD-BIS

        根據RFC-2307bis、這是大多數標準Windows 2012及更新版本LDAP部署的慣用LDAP架構。

      - `AD-IDMU`

        根據Active Directory Identity Management for UNIX、此架構適用於大多數Windows 2008、Windows 2012及更新的AD伺服器。

      - `AD-SFU`

        此架構以Active Directory Services for UNIX為基礎、適用於大多數Windows 2003和舊版AD伺服器。

      - `RFC-2307`

        根據RFC-2307（*an*方法使用*LDAP*做為網路資訊服務）、此架構適用於大多數UNIX AD伺服器。

   c. 選取「連結值」。

      - `-min-bind-level {anonymous|simple|sasl}` 指定最小繫結驗證層級。

預設值為 **anonymous**。

- `-bind-dn LDAP_DN` 指定綁定用戶。

  對於Active Directory伺服器、您必須在帳戶（網域\使用者）或主體（user@domain.com）表單中指定使用者。否則、您必須以辨別名稱（CN=user,DC=domain,DC=com）格式指定使用者。

- `-bind-password password` 指定綁定密碼。

d. 如有需要、請選取工作階段安全選項。

如果LDAP伺服器需要、您可以啟用LDAP簽署和密封、或透過TLS啟用LDAP。

- `--session-security {none|sign|seal}`

  您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal`或兩者皆非 `none`、無簽署或密封）。預設值為 `none`。

  您也應該設定 `-min-bind-level {sasl}` 除非您想讓繫結驗證回復為 **anonymous** 或 **simple** 如果簽署和密封綁定失敗。

- `-use-start-tls {true|false}`

  如果設為 **true** LDAP 伺服器也支援此功能、 LDAP 用戶端會使用加密的 TLS 連線連線至伺服器。預設值為 **false**。您必須安裝LDAP伺服器的自我簽署根CA憑證、才能使用此選項。

> 如果儲存 VM 已將 SMB 伺服器新增至網域、而 LDAP 伺服器是 SMB 伺服器主網域的其中一個網域控制器、則您可以修改 `-session-security-for-ad-ldap` 選項：使用 `vserver cifs security modify` 命令。

e. 選取連接埠、查詢和基礎值。

建議使用預設值、但您必須向LDAP管理員確認這些值是否適合您的環境。

- `-port port` 指定 LDAP 伺服器連接埠。

  預設值為 `389`。

如果您打算使用Start TLS來保護LDAP連線、則必須使用預設連接埠389。啟動TLS會以純文字連線的形式透過LDAP預設連接埠389開始、然後將該連線升級為TLS。如果您變更連接埠、啟動TLS就會失敗。

- `-query-timeout integer` 指定查詢逾時（以秒為單位）。

  允許的範圍為1到10秒。預設值為 `3` 秒。

- `-base-dn LDAP_DN` 指定基礎 DN 。

  如有需要、可輸入多個值（例如啟用LDAP參照追蹤）。預設值為 `""` （根目錄）。

- `-base-scope {base|onelevel|subtree}` 指定基本搜尋範圍。

  預設值為 `subtree`。

- `-referral-enabled {true|false}` 指定是否啟用 LDAP 參照追蹤。

  從ONTAP 功能介紹9.5開始、ONTAP 如果主要LDAP伺服器傳回LDAP參照回應、表示所需記錄存在於參照的LDAP伺服器上、即可讓功能介紹LDAP用戶端將查詢要求參照到其他LDAP伺服器。預設值為 **false**。

若要搜尋所參照LDAP伺服器中的記錄、必須將所參照記錄的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。

2. 在儲存 VM 上建立 LDAP 用戶端組態：

```
vserver services name-service ldap client create -vserver vserver_name -client
-config client_config_name {-servers LDAP_server_list | -ad-domain ad_domain}
-preferred-ad-servers preferred_ad_server_list -restrict-discovery-to-site
{true|false} -default-site CIFS_default_site -schema schema -port 389 -query
-timeout 3 -min-bind-level {anonymous|simple|sasl} -bind-dn LDAP_DN -bind
-password password -base-dn LDAP_DN -base-scope subtree -session-security
{none|sign|seal} [-referral-enabled {true|false}]
```

   建立 LDAP 用戶端組態時、您必須提供儲存 VM 名稱。

3. 確認LDAP用戶端組態已成功建立：

```
vserver services name-service ldap client show -client-config
client_config_name
```

範例

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與 Active Directory 伺服器 for LDAP 搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level simple -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要簽署和密封的 Active Directory 伺服器搭配使用、而 LDAP 伺服器探索則僅限於指定網域的特定站台：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -restrict
-discovery-to-site true -default-site cifsdefaultsite.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
DC=addomain,DC=example,DC=com -base-scope subtree -preferred-ad-servers
172.17.32.100 -session-security seal
```

下列命令會建立名為 ldap1 的新 LDAP 用戶端組態、讓儲存 VM VS1 與需要 LDAP 參照追蹤的 Active Directory

伺服器搭配使用：

```
cluster1::> vserver services name-service ldap client create -vserver vs1
-client-config ldapclient1 -ad-domain addomain.example.com -schema AD-SFU
-port 389 -query-timeout 3 -min-bind-level sasl -base-dn
"DC=adbasedomain,DC=example1,DC=com; DC=adrefdomain,DC=example2,DC=com"
-base-scope subtree -preferred-ad-servers 172.17.32.100 -referral-enabled
true
```

下列命令會指定基礎 DN 、以修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn CN=Users,DC=addomain,DC=example,DC=com
```

下列命令可啟用參照追蹤功能、修改儲存 VM VS1 的 LDAP 用戶端組態 ldap1 ：

```
cluster1::> vserver services name-service ldap client modify -vserver vs1
-client-config ldap1 -base-dn "DC=adbasedomain,DC=example1,DC=com;
DC=adrefdomain,DC=example2,DC=com"  -referral-enabled true
```

將 **LDAP** 用戶端配置與 **ONTAP NFS SVM** 關聯

若要在 SVM 上啟用 LDAP 、您必須使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

開始之前

- LDAP網域必須已存在於網路中、且SVM所在的叢集必須能夠存取。
- SVM上必須存在LDAP用戶端組態。

步驟

1. 在 SVM 上啟用 LDAP ：

   `vserver services name-service ldap create -vserver` *`vserver_name`* `-client-config` *`client_config_name`*

   > 這 `vserver services name-service ldap create`如果ONTAP無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

   下列命令可在「VS1」SVM上啟用LDAP、並將其設定為使用「LDAP1」LDAP用戶端組態：

   ```
   cluster1::> vserver services name-service ldap create -vserver vs1
   -client-config ldap1 -client-enabled true
   ```

2. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令可驗證SVM VS1上的LDAP伺服器。

```
cluster1::> vserver services name-service ldap check -vserver vs1

| Vserver: vs1                                                    |
| Client Configuration Name: c1                                   |
| LDAP Status: up                                                 |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                  |
```

驗證 **ONTAP NFS SVM** 的 **LDAP** 來源

您必須驗證SVM的名稱服務交換器表中是否正確列出名稱服務的LDAP來源。

步驟

1. 顯示目前名稱服務交換器表格內容：

   `vserver services name-service ns-switch show -vserver svm_name`

   下列命令顯示SVM My_SVM的結果：

```
ie3220-a::> vserver services name-service ns-switch show -vserver My_SVM
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
My_SVM          hosts            files,
                                 dns
My_SVM          group            files,ldap
My_SVM          passwd           files,ldap
My_SVM          netgroup         files
My_SVM          namemap          files
5 entries were displayed.
```

   `namemap` 指定要搜尋名稱對應資訊的來源、以及搜尋順序。在純UNIX環境中、不需要輸入此項目。只有在同時使用UNIX和Windows的混合環境中才需要名稱對應。

2. 更新 `ns-switch` 視情況輸入：

如果您想要更新下列項目的**ns**交換器項目...	輸入命令...
使用者資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database passwd -sources ldap,files`

如果您想要更新下列項目的**ns**交換器項目...	輸入命令...
群組資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database group -sources ldap,files`
網路群組資訊	`vserver services name-service ns-switch modify -vserver vserver_name -database netgroup -sources ldap,files`

使用**Kerberos**搭配**NFS**以獲得強大的安全性

了解如何將 **Kerberos** 與 **ONTAP NFS** 結合使用以進行安全性驗證

如果您的環境使用Kerberos進行強式驗證、您必須與Kerberos管理員合作、以判斷需求和適當的儲存系統組態、然後將SVM啟用為Kerberos用戶端。

您的環境應符合下列準則：

- 您的站台部署應遵循Kerberos伺服器和用戶端組態的最佳實務做法、才能設定Kerberos ONTAP 以供執行效能。
- 如果可能、請使用NFSv4或更新版本（如果需要Kerberos驗證）。

  NFSv3可與Kerberos搭配使用。不過、Kerberos的完整安全效益只能在ONTAP NFSv4或更新版本的部署中實現。

- 若要提升備援伺服器存取、應在叢集中多個節點上使用相同的SPN-啟用 多個資料LIF上的Kerberos。
- 在SVM上啟用Kerberos時、必須根據NFS用戶端組態、在Volume或qtree的匯出規則中指定下列其中一種安全性方法。
  - `krb5` （ Kerberos v5 通訊協定）
  - `krb5i` （使用 checksum 進行完整性檢查的 Kerberos v5 通訊協定）
  - `krb5p` （ Kerberos v5 通訊協定與隱私權服務）

除了Kerberos伺服器和用戶端之外、還必須設定下列外部服務ONTAP 以支援Kerberos：

- 目錄服務

  您應該在環境中使用安全目錄服務、例如Active Directory或OpenLDAP、這類服務設定為使用LDAP over SSL/TLS。請勿使用NIS、因為NIS的要求會以純文字傳送、因此不安全。

- NTP

  您必須有執行NTP的工作時間伺服器。這是防止Kerberos驗證因時間偏移而失敗的必要步驟。

- 網域名稱解析（DNS）

  每個UNIX用戶端和每個SVM LIF都必須在Kdc的正向和反向對應區域下註冊適當的服務記錄（SRF）。所有參與者都必須透過DNS正確解析。

Kerberos需要為SVM根磁碟區及本機使用者和群組設定特定的UNIX權限。

步驟

1. 顯示SVM根磁碟區的相關權限：

   `volume show -volume root_vol_name-fields user,group,unix-permissions`

   SVM的根Volume必須具有下列組態：

名稱...	正在設定...
UID	root或ID 0
Gid	root或ID 0
UNIX權限	755

   如果未顯示這些值、請使用 `volume modify` 命令進行更新。

2. 顯示本機UNIX使用者：

   `vserver services name-service unix-user show -vserver vserver_name`

   SVM必須設定下列UNIX使用者：

使用者名稱	使用者ID	主要群組ID	留言
NFS	500	0%	GSS初始化階段所需的項目。 NFS用戶端使用者的第一個使用者是使用者。 如果NFS用戶端使用者的SPN-UNIX名稱對應存在、則不需要NFS使用者。
根	0%	0%	安裝所需。

   如果未顯示這些值、您可以使用 `vserver services name-service unix-user modify` 命令進行更新。

3. 顯示本機UNIX群組：

   `vserver services name-service unix-group show -vserver vserver _name`

   SVM必須設定下列UNIX群組：

群組名稱	群組ID
精靈	1.
根	0%

如果未顯示這些值、您可以使用 `vserver services name-service unix-group modify` 命令進行更新。

在 **ONTAP SVM** 上建立 **NFS Kerberos** 領域配置

如果您想ONTAP 要讓靜態存取環境中的外部Kerberos伺服器、必須先設定SVM使用現有的Kerberos領域。若要這麼做、您需要收集 Kerberos KDC 伺服器的組態值、然後使用 `vserver nfs kerberos realm create` 在 SVM 上建立 Kerberos 領域組態的命令。

開始之前

叢集管理員應已在儲存系統、用戶端和Kdc伺服器上設定NTP、以避免驗證問題。用戶端與伺服器之間的時間差異（時鐘偏移）是驗證失敗的常見原因。

步驟

1. 請洽詢您的 Kerberos 系統管理員、以決定提供的適當組態值 `vserver nfs kerberos realm create` 命令。
2. 在SVM上建立Kerberos領域組態：

   ```
   vserver nfs kerberos realm create -vserver vserver_name -realm realm_name
   {AD_KDC_server_values |AD_KDC_server_values} -comment "text"
   ```

3. 確認已成功建立Kerberos領域組態：

   ```
   vserver nfs kerberos realm show
   ```

範例

下列命令會為SVM VS1建立NFS Kerberos領域組態、該組態使用Microsoft Active Directory伺服器做為Kdc伺服器。Kerberos領域是AUTH.EXAMPLE.COM。Active Directory伺服器的名稱為ad-1、其IP位址為10.10.8.14。允許的時鐘偏移為300秒（預設值）。Kdc伺服器的IP位址為10.10.8.14、其連接埠號碼為88（預設）。「Microsoft Kerberos組態」是註解。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
AUTH.EXAMPLE.COM -adserver-name ad-1
-adserver-ip 10.10.8.14 -clock-skew 300 -kdc-ip 10.10.8.14 -kdc-port 88
-kdc-vendor Microsoft
-comment "Microsoft Kerberos config"
```

下列命令會為使用MIT Kdc的SVM VS1建立NFS Kerberos領域組態。Kerberos領域是SECURITY.EXAMPLE.COM。允許的時鐘偏移為300秒。Kdc伺服器的IP位址為10.10.9.1、其連接埠號碼為88。其他的Kdc廠商則表示UNIX廠商。管理伺服器的IP位址為10.10.9.1、其連接埠號碼為749（預設）。密碼

伺服器的IP位址為10.10.9.1、其連接埠號碼為464（預設）。「UNIX Kerberos組態」是註解。

```
vs1::> vserver nfs kerberos realm create -vserver vs1 -realm
SECURITY.EXAMPLE.COM. -clock-skew 300
-kdc-ip 10.10.9.1 -kdc-port 88 -kdc-vendor Other -adminserver-ip 10.10.9.1
-adminserver-port 749
-passwordserver-ip 10.10.9.1 -passwordserver-port 464 -comment "UNIX
Kerberos config"
```

為 **ONTAP SVM** 配置 **NFS Kerberos** 允許的加密類型

根據預設ONTAP 、支援下列NFS Kerberos加密類型：DE、3DES、AES-128和AES-256。您可以使用設定每個 SVM 的允許加密類型、以符合特定環境的安全需求 `vserver nfs modify` 命令 `-permitted-enc-types` 參數。

關於這項工作

為了達到最大的用戶端相容性、ONTAP 根據預設、支援弱的Des和強式AES加密。例如、如果您想要提高安全性、而且環境支援、可以使用此程序來停用Des和3DES、並要求用戶端僅使用AES加密。

您應該使用目前最強大的加密功能。對於支援支援、也就是AES-256。ONTAP您應該向您的kdc管理員確認您的環境支援此加密層級。

- 在SVM上完全啟用或停用AES（AES-128和AES-256）會造成中斷、因為它會破壞原始的Des主體/索引標籤檔案、因此需要在SVM的所有生命體上停用Kerberos組態。

  在進行此變更之前、您應該確認NFS用戶端不依賴SVM上的AES加密。

- 啟用或停用Des或3DES不需要變更lifs上的Kerberos組態。

步驟

1. 啟用或停用所需的允許加密類型：

如果您要啟用或停用...	請遵循下列步驟...
DE或3DES	a. 設定 SVM 的 NFS Kerberos 允許加密類型： `vserver nfs modify -vserver` *`vserver_name`* `-permitted-enc-types` *`encryption_types`* 以逗號分隔多種加密類型。 b. 確認變更成功： `vserver nfs show -vserver` *`vserver_name`* `-fields permitted-enc-types`

如果您要啟用或停用...	請遵循下列步驟...

AES-128 或 AES-256	a. 識別啟用哪個 SVM 和 LIF Kerberos ：
	
	`vserver nfs kerberos interface show`
	
	b. 在要修改其 NFS Kerberos 允許加密類型的 SVM 上、停用所有生命負載上的 Kerberos ：
	
	`vserver nfs kerberos interface disable -lif lif_name`
	
	c. 設定 SVM 的 NFS Kerberos 允許加密類型：
	
	`vserver nfs modify -vserver vserver_name -permitted-enc-types encryption_types`
	
	以逗號分隔多種加密類型。
	
	d. 確認變更成功：
	
	`vserver nfs show -vserver vserver_name -fields permitted-enc-types`
	
	e. 在 SVM 上的所有生命上重新啟用 Kerberos ：
	
	`vserver nfs kerberos interface enable -lif lif_name -spn service_principal_name`
	
	f. 驗證是否已在所有生命中啓用 Kerberos ：
	
	`vserver nfs kerberos interface show`

在 **ONTAP LIF** 上啟用 **NFS Kerberos**

您可以使用 `vserver nfs kerberos interface enable` 在資料 LIF 上啟用 Kerberos 的命令。這可讓SVM使用Kerberos安全服務來執行NFS。

關於這項工作

如果您使用Active Directory Kdc、則所使用的任何SPN前15個字元在領域或網域內的SVM之間必須是唯一的。

步驟

1. 建立NFS Kerberos組態：

   ```
   vserver nfs kerberos interface enable -vserver vserver_name -lif
   logical_interface -spn service_principal_name
   ```

   支援Kerberos介面時、需要使用來自Kdc的SPN秘密金鑰。ONTAP

對於Microsoft KDC、會聯絡到KDC、並在CLI發出使用者名稱和密碼提示以取得秘密金鑰。如果您需要在Kerberos 領域的不同 OU 中建立 SPN 、您可以指定選用的 `-ou` 參數。

對於非Microsoft KDC、可使用下列兩種方法之一取得秘密金鑰：

如果您...	您也必須在命令中加入下列參數...
請讓Kdc系統管理員認證資料直接從Kdc擷取金鑰	`-admin-username` *kdc_admin_username*
不具有kdc系統管理員認證、但從包含金鑰的kdc取得Keytab檔案	`-keytab-uri` ｛FTP

2. 確認LIF上已啟用Kerberos：

   `vserver nfs kerberos-config show`

3. 重複步驟1和2、在多個LIF上啟用Kerberos。

範例

下列命令會在邏輯介面v03至D1上為名為VS1的SVM建立及驗證NFS Kerberos組態、並在OU lab2ou中使用SPn NFS/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM：

```
vs1::> vserver nfs kerberos interface enable -lif ves03-d1 -vserver vs2
-spn nfs/ves03-d1.lab.example.com@TEST.LAB.EXAMPLE.COM -ou "ou=lab2ou"

vs1::>vserver nfs kerberos-config show
        Logical
Vserver Interface Address       Kerberos  SPN
------- --------- -------       --------- ------------------------------
vs0     ves01-a1
                  10.10.10.30   disabled  -
vs2     ves01-d1
                  10.10.10.40   enabled   nfs/ves03-
d1.lab.example.com@TEST.LAB.EXAMPLE.COM
2 entries were displayed.
```

將儲存容量新增至啟用**NFS**的**SVM**

了解如何為啟用 **ONTAP NFS** 的 **SVM** 新增儲存容量

若要將儲存容量新增至啟用NFS的SVM、您必須建立一個Volume或qtree以提供儲存容器、並建立或修改該容器的匯出原則。然後、您可以從叢集驗證NFS用戶端存取、並測試用戶端系統的存取。

開始之前

- NFS必須在SVM上完全設定。

- SVM根磁碟區的預設匯出原則必須包含允許存取所有用戶端的規則。
- 您名稱服務組態的任何更新都必須完成。
- Kerberos組態的任何新增或修改都必須完成。

建立 **ONTAP NFS** 導出策略

在建立匯出規則之前、您必須先建立匯出原則以保留這些規則。您可以使用 `vserver export-policy create` 建立匯出原則的命令。

步驟

1. 建立匯出原則：

   ```
   vserver export-policy create -vserver vserver_name -policyname policy_name
   ```

   原則名稱最長可達256個字元。

2. 確認已建立匯出原則：

   ```
   vserver export-policy show -policyname policy_name
   ```

範例

下列命令會在名為VS1的SVM上建立並驗證名為exp1的匯出原則：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1

vs1::> vserver export-policy show -policyname exp1
Vserver          Policy Name
---------------  -------------------
vs1              exp1
```

在 **ONTAP NFS** 匯出策略中新增規則

如果沒有規則、匯出原則就無法讓用戶端存取資料。若要建立新的匯出規則、您必須識別用戶端並選取用戶端比對格式、選取存取和安全性類型、指定匿名使用者ID對應、選取規則索引編號、然後選取存取傳輸協定。然後您就可以使用 `vserver export-policy rule create` 命令將新規則新增至匯出原則。

開始之前

- 您要新增匯出規則的匯出原則必須已經存在。
- 必須在資料SVM上正確設定DNS、而且DNS伺服器必須為NFS用戶端設定正確的項目。

  這是因為ONTAP 針對某些用戶端比對格式、使用資料SVM的DNS組態執行DNS查詢、而匯出原則規則比對失敗則會妨礙用戶端資料存取。

- 如果您使用Kerberos進行驗證、則必須確定NFS用戶端使用下列哪些安全性方法：

- `krb5` （ Kerberos V5 傳輸協定）
- `krb5i` （使用 Checksum 進行完整性檢查的 Kerberos V5 傳輸協定）
- `krb5p` （具有隱私權服務的 Kerberos V5 傳輸協定）

關於這項工作

如果匯出原則中的現有規則涵蓋了用戶端的相符和存取需求、則不需要建立新規則。

如果您正在使用 Kerberos 進行驗證、而且 SVM 的所有磁碟區都是透過 Kerberos 存取、您可以設定匯出規則選項 `-rorule`、 `-rwrule`和 `-superuser` 將根磁碟區移至 `krb5`、 `krb5i`或 `krb5p`。

步驟

1. 識別新規則的用戶端和用戶端比對格式。

   。 `-clientmatch` 選項指定規則所套用的用戶端。可以指定單一或多個用戶端符合值；多個值的規格必須以逗號分隔。您可以指定下列任一格式的相符項目：

用戶端比對格式	範例
網域名稱前面加上「.」字元	`.example.com` 或 `.example.com,.example.net,...`
主機名稱	`host1` 或 `host1,host2, ...`
IPV4位址	`10.1.12.24` 或 `10.1.12.24,10.1.12.25, ...`
以多位元表示子網路遮罩的IPv4位址	`10.1.12.10/4` 或 `10.1.12.10/4,10.1.12.11/4,...`
具有網路遮罩的IPV4位址	`10.1.16.0/255.255.255.0` 或 `10.1.16.0/255.255.255.0,10.1.17.0/255.255.255.0,...`
以點分格式提供IPv6位址	`::1.2.3.4` 或 `::1.2.3.4,::1.2.3.5,...`
IPv6 位址、子網路遮罩以位元數表示	`ff::00/32` 或 `ff::00/32,ff::01/32,...`
以@字元開頭的netgroup名稱為單一netgroup	`@netgroup1` 或 `@netgroup1,@netgroup2,...`

   您也可以合併用戶端定義的類型、例如 `.example.com,@netgroup1`。

   指定IP位址時、請注意下列事項：

   - 不允許輸入IP位址範圍、例如10.12.10-10.12.70。

     此格式的項目會解譯為文字字串、並視為主機名稱。

- 在匯出規則中指定個別IP位址以精細管理用戶端存取時、請勿指定動態（例如DHCP）或暫時（例如IPv6）指派的IP位址。

  否則、當用戶端的IP位址變更時、就會失去存取權。

- 不允許使用網路遮罩輸入IPv6位址、例如ff:12/ff:00。

2. 選取用戶端相符項目的存取和安全性類型。

   您可以指定下列一或多種存取模式、以驗證具有指定安全性類型的用戶端：

   - `-rorule` （唯讀存取）
   - `-rwrule` （讀寫存取權）
   - `-superuser` （ root 存取權）

   > 如果匯出規則也允許該安全性類型的唯讀存取權、則用戶端只能取得特定安全性類型的讀寫存取權。如果安全性類型的唯讀參數比讀寫參數的限制更多、用戶端可能無法取得讀寫存取權。超級使用者存取也是如此。

   您可以為規則指定多種安全性類型的以逗號分隔的清單。如果您將安全性類型指定為 `any` 或 `never`，請勿指定任何其他安全類型。從下列有效的安全類型中選擇：

當安全性類型設定為...	相符的用戶端可以存取匯出的資料...
`any`	無論傳入的安全類型為何、
`none`	如果單獨列出、則會將具有任何安全類型的用戶端授予匿名存取權。如果列出其他安全性類型、則會授與具有指定安全性類型的用戶端存取權、而具有任何其他安全性類型的用戶端則會以匿名存取權。
`never`	永不、無論傳入的安全類型為何。
`krb5`	如果是由Kerberos 5驗證。 僅驗證：簽署每個要求和回應的標頭。
`krb5i`	如果通過Kerberos 5i驗證。 驗證與完整性：簽署每個要求與回應的標頭與實體。
`krb5p`	如果是由 Kerberos 5p 驗證。 驗證、完整性和隱私：簽署每個要求和回應的標頭和實體、並加密NFS資料有效負載。
`ntlm`	如果通過CIFS的NTLM驗證。
`sys`	如果是由NFS AUTH_SYS驗證的。

建議的安全類型為 `sys`或是使用 `Kerberos 、 `krb5、 krb5i`或 `krb5p。

如果將 Kerberos 與 NFSv3 搭配使用、則匯出原則規則必須允許 `-rorule` 和 `-rwrule` 存取 `sys` 此外 `krb5`。這是因為需要允許網路鎖定管理程式（NLM）存取匯出。

3. 指定匿名使用者ID對應。

。 `-anon` 選項會指定 UNIX 使用者 ID 或使用者名稱、該使用者 ID 會對應至以 0 （零）為使用者 ID 的用戶端要求、此 ID 通常與使用者名稱根目錄相關聯。預設值為 `65534`。NFS用戶端通常會將使用者ID 65534與使用者名稱nobody建立關聯（也稱為根系統衝突_）。在本功能中、此使用者ID與使用者pcuser相關聯。ONTAP若要停用使用者 ID 為 0 的任何用戶端存取、請指定值為 `65535`。

4. 選取規則索引順序。

。 `-ruleindex` 選項指定規則的索引編號。規則會根據索引編號清單中的順序來評估；索引編號較低的規則會先評估。例如、索引編號為1的規則會在索引編號為2的規則之前進行評估。

如果您要新增...	然後...
匯出原則的第一條規則	輸入 `1`。
匯出原則的其他規則	a. 在原則中顯示現有規則： `vserver export-policy rule show -instance -policyname` *`your_policy`* b. 根據新規則的評估順序、為新規則選取索引編號。

5. 選取適用的 NFS 存取值：{`nfs`|`nfs3`|`nfs4`}。

`nfs` 符合任何版本、 `nfs3` 和 `nfs4` 僅符合這些特定版本。

6. 建立匯出規則並將其新增至現有的匯出原則：

`vserver export-policy rule create -vserver` *`vserver_name`* `-policyname` *`policy_name`* `-ruleindex` *`integer`* `-protocol {nfs|nfs3|nfs4} -clientmatch { text |` *`"text,text,…"`* `} -rorule` *`security_type`* `-rwrule` *`security_type`* `-superuser` *`security_type`* `-anon` *`user_ID`*

7. 顯示匯出原則的規則、以驗證是否存在新規則：

`vserver export-policy rule show -policyname` *`policy_name`*

命令會顯示該匯出原則的摘要、包括套用至該原則的規則清單。此功能會為每個規則指派一個規則索引編號。ONTAP知道規則索引編號之後、您可以使用它來顯示指定匯出規則的詳細資訊。

8. 確認已正確設定套用至匯出原則的規則：

`vserver export-policy rule show -policyname` *`policy_name`* `-vserver` *`vserver_name`* `-ruleindex` *`integer`*

範例

下列命令會在名為RSR1的匯出原則中、在名為VS1的SVM上建立匯出規則、並驗證其建立。規則的索引編號為1。規則會比對網域eng.company.com和netgroup @netGroup1中的任何用戶端。此規則可啟用所有NFS存取。它可對驗證了AUTH_SYS的使用者啟用唯讀和讀寫存取權。除非透過Kerberos驗證、否則使用UNIX使用者ID 0（零）的用戶端會匿名。

```
vs1::> vserver export-policy rule create -vserver vs1 -policyname exp1
-ruleindex 1 -protocol nfs
-clientmatch .eng.company.com,@netgoup1 -rorule sys -rwrule sys -anon
65534 -superuser krb5

vs1::> vserver export-policy rule show -policyname nfs_policy
Virtual      Policy         Rule    Access    Client           RO
Server       Name           Index   Protocol  Match            Rule
------------ -------------- ------  --------  ---------------- ------
vs1          exp1           1       nfs       eng.company.com, sys
                                              @netgroup1

vs1::> vserver export-policy rule show -policyname exp1 -vserver vs1
-ruleindex 1

                                Vserver: vs1
                            Policy Name: exp1
                             Rule Index: 1
                           Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
eng.company.com,@netgroup1
                             RO Access Rule: sys
                             RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

下列命令會在名為expol2的匯出原則中、在名為VS2的SVM上建立匯出規則、並加以驗證。此規則的索引編號為21。此規則會將用戶端與netgroup dev_netgroup_main.此規則可啟用所有NFS存取。此功能可為使用AUTH_SYS驗證的使用者啟用唯讀存取、並需要Kerberos驗證才能進行讀寫和root存取。除非透過Kerberos進行驗證、否則使用UNIX使用者ID 0（零）的用戶端會被拒絕root存取。

```
vs2::> vserver export-policy rule create -vserver vs2 -policyname expol2
-ruleindex 21 -protocol nfs
-clientmatch @dev_netgroup_main -rorule sys -rwrule krb5 -anon 65535
-superuser krb5

vs2::> vserver export-policy rule show -policyname nfs_policy
Virtual  Policy       Rule    Access    Client                RO
Server   Name         Index   Protocol  Match                 Rule
-------- ------------ ------  --------  --------------------  ------
vs2      expol2       21       nfs      @dev_netgroup_main  sys

vs2::> vserver export-policy rule show -policyname expol2 -vserver vs1
-ruleindex 21

                                Vserver: vs2
                            Policy Name: expol2
                             Rule Index: 21
                          Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain:
                                         @dev_netgroup_main
                          RO Access Rule: sys
                          RW Access Rule: krb5
User ID To Which Anonymous Users Are Mapped: 65535
                  Superuser Security Types: krb5
              Honor SetUID Bits in SETATTR: true
                 Allow Creation of Devices: true
```

建立Volume或qtree儲存容器

建立 ONTAP NFS 卷

您可以使用建立 Volume 並指定其連接點和其他屬性 `volume create` 命令。

關於這項工作

磁碟區必須包含_交會路徑_、才能讓用戶端使用其資料。您可以在建立新磁碟區時指定交會路徑。如果您在建立磁碟區時未指定連接路徑、則必須使用 _ 掛載 _ SVM 命名空間中的磁碟區 `volume mount` 命令。

開始之前

- NFS 應設定並執行。
- SVM 安全樣式必須是 UNIX 。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

  若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume

create`資訊，請參閱。

步驟

1. 建立具有交會點的Volume：

   `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number -group group_name_or_number -junction-path junction_path [-policy export_policy_name]`

   的選擇 `-junction-path` 以下是：

   - 直接位於根目錄下、例如 */new_vol*

     您可以建立新磁碟區、並指定將其直接掛載到SVM根磁碟區。

   - 在現有目錄下、例如 */existing_dir/new_vol*

     您可以建立新磁碟區、並指定將其掛載至現有磁碟區（在現有階層架構中）、以目錄形式表示。

     如果您想在新目錄中建立磁碟區（在新磁碟區下的新階層中）、例如：*`/new_dir/new_vol`*接著、您必須先建立與 SVM 根 Volume 相關的新父 Volume 。接著、您會在新父Volume（新目錄）的交會路徑中建立新的子Volume。

     如果您打算使用現有的匯出原則、則可以在建立磁碟區時指定。您也可以稍後使用新增匯出原則 `volume modify` 命令。

2. 確認已使用所需的交會點建立磁碟區：

   `volume show -vserver svm_name -volume volume_name -junction`

範例

下列命令會在SVM vs1.example.com和Aggr1上建立名為user1的新磁碟區。新的 Volume 可在取得 `/users`。磁碟區大小為750 GB、磁碟區保證為磁碟區類型（預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver           Volume   Active   Junction Path   Path Source
----------------- ------- -------- --------------- -----------
vs1.example.com   users1   true     /users          RW_volume
```

下列命令會在SVM「vs1.example.com」和Aggr1上建立名為「home4」的新磁碟區。目錄 `/eng/` VS1 SVM 的命名空間已存在、新的 Volume 可從取得 `/eng/home`、成為的主目錄 `/eng/` 命名空間。磁碟區大小為 750 GB 、其磁碟區保證屬於類型 `volume` （預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4     true     /eng/home       RW_volume
```

建立 **ONTAP NFS qtree**

您可以建立 qtree 來包含資料、並使用來指定其內容 `volume qtree create` 命令。

開始之前

- SVM和將要包含新qtree的Volume必須已經存在。
- SVM的安全樣式必須是UNIX、NFS應設定並執行。

步驟

1. 建立qtree：

   ```
   volume qtree create -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path } -security-style unix [-policy
   export_policy_name]
   ```

   您可以將 Volume 和 qtree 指定為個別的引數、或以格式指定 qtree 路徑引數 `/vol/volume_name/_qtree_name`。

   根據預設、qtree會繼承其父Volume的匯出原則、但可以設定為使用自己的原則。如果您打算使用現有的匯出原則、則可以在建立qtree時加以指定。您也可以稍後使用新增匯出原則 `volume qtree modify` 命令。

2. 確認qtree是以所需的交會路徑建立：

   ```
   volume qtree show -vserver vserver_name { -volume volume_name -qtree
   qtree_name | -qtree-path qtree path }
   ```

範例

以下範例建立一個 qtree 、名稱為 qt01 、位於 SVM vs1.example.com 上、具有交會路徑 `/vol/data1`：

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style unix
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: unix
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

使用匯出原則保護**NFS**存取安全

了解如何使用匯出策略保護 **ONTAP NFS** 訪問

您可以使用匯出原則、將NFS存取磁碟區或qtree的權限限制在符合特定參數的用戶端。配置新儲存設備時、您可以使用現有的原則和規則、新增規則至現有原則、或建立新的原則和規則。您也可以檢查匯出原則的組態

> 從ONTAP 功能表支援的支援範例9.3開始、您可以啟用匯出原則組態檢查、做為背景工作、將任何違反規則的行為記錄在錯誤規則清單中。。 `vserver export-policy config-checker` 命令會叫用檢查程式並顯示結果、您可以使用這些結果來驗證組態、並從原則中刪除錯誤的規則。這些命令只會驗證主機名稱、網路群組和匿名使用者的匯出組態。

管理 **ONTAP NFS** 匯出規則的處理順序

您可以使用 `vserver export-policy rule setindex` 手動設定現有匯出規則索引編號的命令。這可讓您指定ONTAP 將匯出規則套用至用戶端要求的優先順序。

關於這項工作

如果新的索引編號已經在使用中、命令會在指定的點插入規則、並據此重新排序清單。

步驟

1. 修改指定匯出規則的索引編號：

   ```
   vserver export-policy rule setindex -vserver virtual_server_name -policyname
   policy_name -ruleindex integer -newruleindex integer
   ```

範例

下列命令會將索引編號3的匯出規則索引編號變更為SVM上名為VS1的匯出原則RSR1編號2：

```
vs1::> vserver export-policy rule setindex -vserver vs1
-policyname rs1 -ruleindex 3 -newruleindex 2
```

將 ONTAP NFS 導出策略指派給磁碟區

SVM中包含的每個磁碟區都必須與包含匯出規則的匯出原則相關聯、以便用戶端存取磁碟區中的資料。

關於這項工作

您可以在建立磁碟區時或建立磁碟區後的任何時間、將匯出原則與磁碟區建立關聯。您可以將一個匯出原則與磁碟區建立關聯、不過一個原則可以與許多磁碟區建立關聯。

步驟

1. 如果在建立磁碟區時未指定匯出原則、請將匯出原則指派給磁碟區：

   ```
   volume modify -vserver vserver_name -volume volume_name -policy
   export_policy_name
   ```

2. 確認原則已指派給磁碟區：

   ```
   volume show -volume volume_name -fields policy
   ```

範例

下列命令會將匯出原則nfs_policy指派給SVM VS1上的Volume vol1、並驗證指派：

```
cluster::> volume modify -v1server vs1 -volume vol1 -policy nfs_policy

cluster::>volume show -volume vol -fields policy
vserver volume       policy
------- ------------ ----------------
vs1     vol1         nfs_policy
```

將 ONTAP NFS 導出策略指派給 qtree

您也可以在磁碟區上匯出特定qtree、讓用戶端直接存取、而非匯出整個磁碟區。您可以將匯出原則指派給qtree來匯出qtree。您可以在建立新的qtree或修改現有的qtree時指派匯出原則。

開始之前

匯出原則必須存在。

關於這項工作

根據預設、如果在建立時未另外指定、qtree會繼承包含Volume的父匯出原則。

您可以在建立qtree時或在建立qtree之後的任何時間、將匯出原則與qtree建立關聯。您可以將一個匯出原則與qtree建立關聯、不過一個原則可以與許多qtree建立關聯。

步驟

1. 如果在建立qtree時未指定匯出原則、請將匯出原則指派給qtree：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy export_policy_name
   ```

2. 確認原則已指派給qtree：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

範例

下列命令會將匯出原則nfs_policy指派給SVM VS1上的qtree qt1、並驗證指派：

```
cluster::> volume modify -v1server vs1 -qtree-path /vol/vol1/qt1 -policy
nfs_policy

cluster::>volume qtree show -volume vol1 -fields export-policy
vserver volume qtree export-policy
------- ------ ----- -------------
vs1     data1  qt01  nfs_policy
```

驗證叢集中的 **ONTAP NFS** 用戶端存取

您可以在UNIX管理主機上設定UNIX檔案權限、讓選取的用戶端存取共用區。您可以使用檢查用戶端存取 `vserver export-policy check-access` 命令、視需要調整匯出規則。

步驟

1. 在叢集上、使用檢查用戶端對匯出的存取權 `vserver export-policy check-access` 命令。

   下列命令會檢查IP位址為1.2.3.4的NFSv3用戶端對Volume Home2的讀取/寫入存取。命令輸出顯示該Volume 使用匯出原則 `exp-home-dir` 這種存取被拒絕。

```
cluster1::> vserver export-policy check-access -vserver vs1 -client-ip
1.2.3.4 -volume home2 -authentication-method sys -protocol nfs3 -access
-type read-write
                                        Policy    Policy     Rule
Path                    Policy          Owner     Owner Type Index  Access
----------------------- --------------- --------- ---------- ------
----------
/                       default         vs1_root  volume          1 read
/eng                    default         vs1_root  volume          1 read
/eng/home2              exp-home-dir    home2     volume          1 denied

3 entries were displayed.
```

2. 檢查輸出、判斷匯出原則是否如預期運作、以及用戶端存取行為是否如預期。

   具體而言、您應該確認磁碟區或qtree使用的匯出原則、以及用戶端因此而擁有的存取類型。

3. 如有必要、請重新設定匯出原則規則。

從客戶端系統測試 **ONTAP NFS** 存取

驗證NFS對新儲存物件的存取之後、您應該登入NFS管理主機、從SVM讀取資料並將資料寫入SVM、以測試組態。接著、您應該在用戶端系統上以非root使用者的身分重複此程序。

開始之前

- 用戶端系統必須具有您先前指定的匯出規則所允許的IP位址。
- 您必須擁有root使用者的登入資訊。

步驟

1. 在叢集上、驗證裝載新磁碟區之LIF的IP位址：

   ```
   network interface show -vserver svm_name
   ```

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

2. 以root使用者身分登入管理主機用戶端系統。
3. 將目錄變更為掛載資料夾：

   ```
   cd /mnt/
   ```

4. 使用SVM的IP位址建立及掛載新資料夾：

   a. 建立新資料夾：

      ```
      mkdir /mnt/folder
      ```

b. 將新磁碟區掛載至此新目錄：

```
mount -t nfs -o hard IPAddress:/volume_name /mnt/folder
```

c. 將目錄變更為新資料夾：

```
cd folder
```

下列命令會建立名為test1的資料夾、將vol1磁碟區掛載到test1掛載資料夾的192.0.2.130 IP位址、然後變更為新的test1目錄：

```
host# mkdir /mnt/test1
host# mount -t nfs -o hard 192.0.2.130:/vol1 /mnt/test1
host# cd /mnt/test1
```

5. 建立新檔案、確認檔案是否存在、然後將文字寫入：

a. 建立測試檔案：

```
touch filename
```

b. 確認檔案存在：

```
ls -l filename
```

c. 輸入：

```
cat > filename
```

輸入一些文字、然後按下Ctrl+D將文字寫入測試檔案。

d. 顯示測試檔案的內容。

```
cat filename
```

e. 移除測試檔案：

```
rm filename
```

f. 返回父目錄：

```
cd ..
```

```
host# touch myfile1
host# ls -l myfile1
-rw-r--r-- 1 root root 0 Sep 18 15:58 myfile1
host# cat >myfile1
This text inside the first file
host# cat myfile1
This text inside the first file
host# rm -r myfile1
host# cd ..
```

6. 以root使用者的身份、在掛載的Volume上設定任何所需的UNIX擁有權和權限。
7. 在匯出規則中識別的UNIX用戶端系統上、以目前擁有新磁碟區存取權的授權使用者之一登入、然後重複步驟3到5中的程序、確認您可以掛載磁碟區並建立檔案。

在哪裡可以找到更多 **ONTAP NFS** 信息

成功測試NFS用戶端存取之後、您可以執行其他NFS組態或新增SAN存取。傳輸協定存取完成時、您應該保護儲存虛擬機器（SVM）的根磁碟區。

NFS 組態

您可以使用下列資訊和技術報告進一步設定NFS存取：

- "NFS管理"

  說明如何使用NFS設定及管理檔案存取。

- "NetApp技術報告4067：NFS最佳實務與實作指南"

  提供NFSv3和NFSv3作業指南、並概述ONTAP 以NFSv3為焦點的作業系統。

- "NetApp技術報告4073：安全統一化驗證"

  說明如何設定ONTAP 搭配UNIX型Kerberos第5版（krb5）伺服器使用的功能、以進行NFS儲存驗證、以及將Windows Server Active Directory（AD）設定為Kdc和輕量型目錄存取傳輸協定（LDAP）身分識別供應商。

- "NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"

  說明在掛接到執行ONTAP 此功能的系統上、在AIX、Linux或Solaris用戶端上實作NFSv4元件時應遵循的最佳實務做法。

網路組態

您可以使用下列資訊與技術報告、進一步設定網路功能與名稱服務：

- "NFS管理"

說明如何設定及管理ONTAP 靜態網路。

- "NetApp技術報告4182：乙太網路儲存設計考量與叢集Data ONTAP 式的最佳實務做法"

  說明ONTAP 實作的環節、並提供常見的網路部署情境和最佳實務建議。

- "NetApp技術報告4668：名稱服務最佳實務做法指南"

  說明如何設定LDAP、NIS、DNS及本機檔案組態以進行驗證。

SAN傳輸協定組態

如果您想要提供或修改SAN對新SVM的存取、可以使用FC或iSCSI組態資訊、此資訊適用於多個主機作業系統。

根**Volume**保護

在SVM上設定傳輸協定之後、您應確保其根Volume受到保護：

- "資料保護"

  說明如何建立負載共用鏡像來保護SVM根磁碟區、這是NetApp啟用NAS的SVM最佳實務做法。同時也說明如何從負載共用鏡像中提升SVM根磁碟區、以快速從磁碟區故障或損失中恢復。

此功能與**7-Mode**匯出有何不同**ONTAP**

此功能與**7-Mode**匯出有何不同**ONTAP**

如果您不熟悉 ONTAP 如何實作 NFS 匯出、您可以比較 7-Mode 和 ONTAP 匯出組態工具、以及 7-Mode 範例 `/etc/exports` 具有叢集式原則和規則的檔案。

在 ONTAP 中沒有 `/etc/exports` 檔案與否 `exportfs` 命令。而是必須定義匯出原則。匯出原則可讓您以與7-Mode相同的方式來控制用戶端存取、但提供額外的功能、例如針對多個磁碟區重複使用相同的匯出原則。

相關資訊

"NFS管理"

"NetApp技術報告4067：NFS最佳實務與實作指南"

了解 **7-**模式和 **ONTAP NFS** 導出的比較

以功能為基礎的匯出ONTAP 是以不同於7-Mode環境的方式定義和使用。

差異領域	7-Mode	ONTAP
如何定義匯出	匯出是在中定義的 `/etc/exports` 檔案：	匯出是透過在SVM中建立匯出原則來定義。SVM可包含多個匯出原則。

匯出範圍	• 匯出會套用至指定的檔案路徑或qtree。 • 您必須在中建立個別項目 `/etc/exports` 針對每個檔案路徑或 qtree 。 • 只有在中定義匯出時、匯出才會持續進行 `/etc/exports` 檔案：	• 匯出原則適用於整個Volume、包括Volume中包含的所有檔案路徑和qtree。 • 如果需要、匯出原則可套用至多個Volume。 • 所有匯出原則都會在系統重新啟動時持續執行。
隔離（指定特定用戶端對相同資源的不同存取）	若要為特定用戶端提供對單一匯出資源的不同存取權、您必須在中列出每個用戶端及其允許的存取權 `/etc/exports` 檔案：	匯出原則是由許多個別的匯出規則所組成。每個匯出規則都會定義資源的特定存取權限、並列出擁有這些權限的用戶端。若要為特定用戶端指定不同的存取權限、您必須為每組特定的存取權限建立匯出規則、列出具有這些權限的用戶端、然後將規則新增至匯出原則。
名稱別名	定義匯出時、您可以選擇讓匯出名稱與檔案路徑名稱不同。您應該使用 `-actual` 在中定義此類匯出時的參數 `/etc/exports` 檔案：	您可以選擇讓匯出的Volume名稱不同於實際的Volume名稱。若要這麼做、您必須在SVM命名空間內以自訂的交會路徑名稱來掛載磁碟區。 根據預設、磁碟區會以其Volume名稱掛載。若要自訂磁碟區的交會路徑名稱、您需要卸載、重新命名、然後重新掛載。

了解 **ONTAP NFS** 導出策略範例

您可以檢閱範例匯出原則、進一步瞭解匯出原則在ONTAP 功能方面的運作方式。

7-Mode匯出的實作範例ONTAP

下列範例顯示的 7-Mode 匯出與中所顯示的相同 `/etc/export` 檔案：

```
/vol/vol1 -sec=sys,ro=@readonly_netgroup,rw=@readwrite_netgroup1:
@readwrite_netgroup2:@rootaccess_netgroup,root=@rootaccess_netgroup
```

若要將此匯出重新產生為叢集匯出原則、您必須建立具有三個匯出規則的匯出原則、然後將匯出原則指派給Volume vol1。

規則	元素	價值
規則1.	-clientmatch （用戶端規格）	@readonly_netgroup
-ruleindex（出口規則在規則清單中的位置）	1	-protocol
nfs	-rorule（允許唯讀存取）	sys （使用驗證的用戶端）
-rwrule（允許讀寫存取）	never	-superuser（允許超級使用者存取）
none（根目錄 _ 分段 _ 至安納）	第2條	-clientmatch
@rootaccess_netgroup	-ruleindex	2
-protocol	nfs	-rorule
sys	-rwrule	sys
-superuser	sys	第 3 條
-clientmatch	@readwrite_netgroup1,@readwrite_netgroup2	-ruleindex
3	-protocol	nfs
-rorule	sys	-rwrule
sys	-superuser	none

1. 建立名為exp_vol1的匯出原則：

   ```
   vserver export-policy create -vserver NewSVM -policyname exp_vol1
   ```

2. 在base命令中建立三個具有下列參數的規則：
   - 基本命令：

     ```
     vserver export-policy rule create -vserver NewSVM -policyname exp_vol1
     ```

   - 規則參數：

     ```
     -clientmatch @readonly_netgroup -ruleindex 1 -protocol nfs -rorule sys
     -rwrule never -superuser none

     -clientmatch @rootaccess_netgroup -ruleindex 2 -protocol nfs -rorule sys
     ```

```
-rwrule sys -superuser sys

-clientmatch @readwrite_netgroup1,@readwrite_netgroup2 -ruleindex 3
-protocol nfs -rorule sys -rwrule sys -superuser none
```

3. 將原則指派給Volume vol1：

```
volume modify -vserver NewSVM -volume vol1 -policy exp_vol1
```

7-Mode匯出的整合範例

以下範例顯示 7-Mode `/etc/export` 每 10 個 qtree 包含一行的檔案：

```
/vol/vol1/q_1472 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1471 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1473 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1570 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_1571 -sec=sys,rw=host1519s,root=host1519s
/vol/vol1/q_2237 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2238 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2239 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2240 -sec=sys,rw=host2057s,root=host2057s
/vol/vol1/q_2241 -sec=sys,rw=host2057s,root=host2057s
```

在 ONTAP 中、每個 qtree 都需要兩個原則之一：一個原則包含規則 `-clientmatch host1519s`或具有規則的規則 `-clientmatch host2057s`。

1. 建立兩個匯出原則、稱為exp_vol1q1和exp_vol1q2：
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q1`
   - `vserver export-policy create -vserver NewSVM -policyname exp_vol1q2`
2. 為每個原則建立規則：
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q1 -clientmatch host1519s -rwrule sys -superuser sys`
   - `vserver export-policy rule create -vserver NewSVM -policyname exp_vol1q2 -clientmatch host1519s -rwrule sys -superuser sys`
3. 將原則套用至qtree：
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_1472 -export -policy exp_vol1q1`
   - [接下來的4個qtree …]
   - `volume qtree modify -vserver NewSVM -qtree-path /vol/vol1/q_2237 -export -policy exp_vol1q2`
   - [接下來的4個qtree …]

如果您稍後需要為這些主機新增其他qtree、則會使用相同的匯出原則。

管理 NFS

了解 NFS 協定的 ONTAP 檔案訪問

包含NFS傳輸協定可用的檔案存取功能。ONTAP您可以啟用NFS伺服器並匯出Volume或qtree。

您可在下列情況下執行這些程序：

- 您想要瞭解ONTAP 各種不同的NFS傳輸協定功能。
- 您想要執行較不常見的組態和維護工作、而非基本NFS組態。
- 您想要使用命令列介面（CLI）、而非System Manager或自動化指令碼工具。

瞭解NAS檔案存取

命名空間和交會點

了解 ONTAP NAS 命名空間和連接點

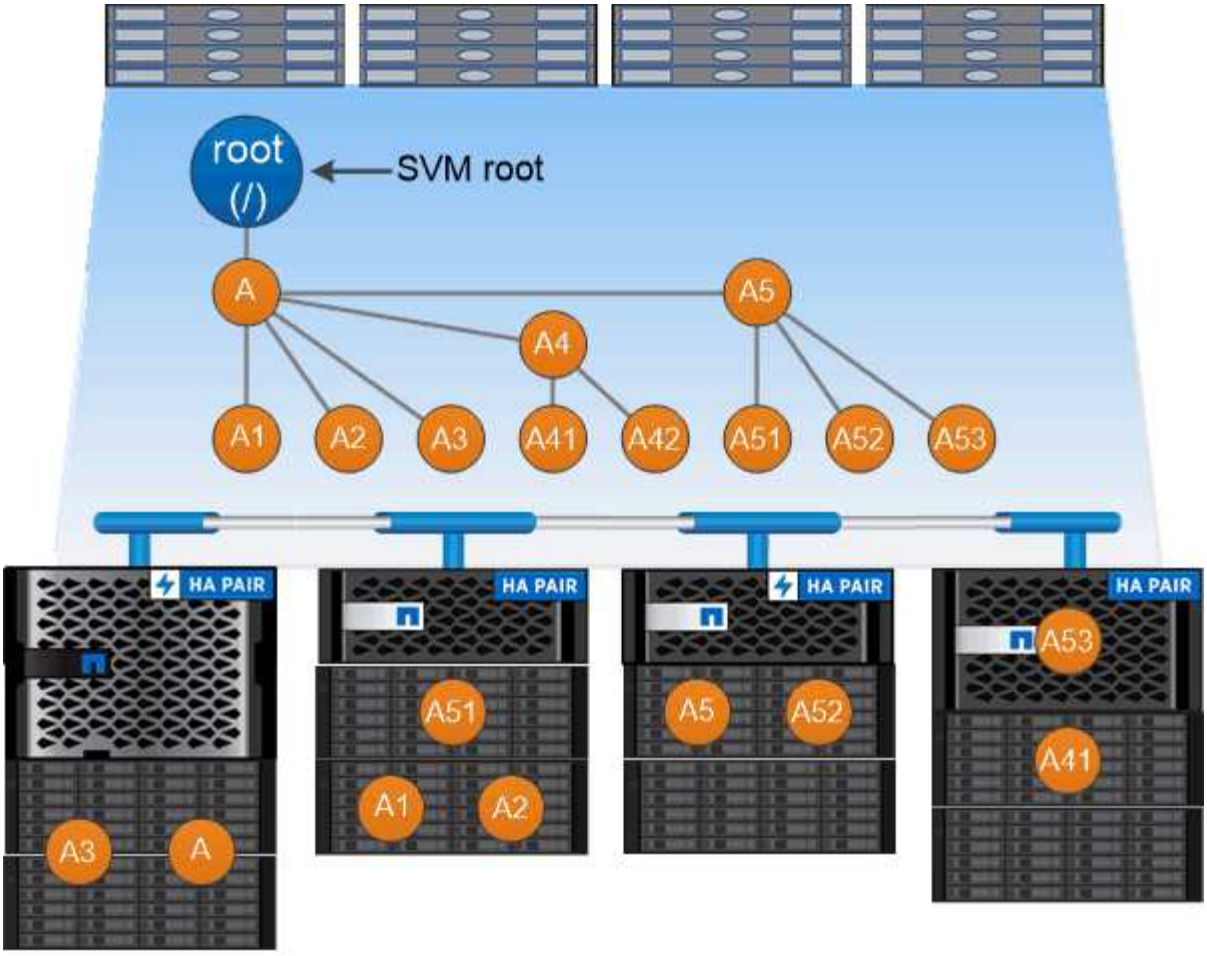
NAS *namespacity*_是一個邏輯群組、集合在_交會點、以建立單一檔案系統階層架構。具有足夠權限的用戶端可存取命名空間中的檔案、而無需指定檔案在儲存設備中的位置。未分段的磁碟區可位於叢集中的任何位置。

NAS用戶端不會掛載每個包含感興趣檔案的磁碟區、而是掛載NFS _EX出口_或存取SMB共享區。_匯出或共用區代表整個命名空間或命名空間內的中繼位置。用戶端只會存取裝載於其存取點下方的磁碟區。

您可以視需要將磁碟區新增至命名空間。您可以直接在父磁碟區交會下方或磁碟區內的目錄上建立交會點。名稱為「 'vol3' 」的 Volume 交會路徑可能是 `/vol1/vol2/vol3`或 `/vol1/dir2/vol3`或甚至 `/dir1/dir2/vol3`。路徑稱為_junction路徑。_

每個SVM都有一個獨特的命名空間。SVM根磁碟區是命名空間階層架構的起點。

> 為了確保資料在節點中斷或容錯移轉的情況下仍然可用、您應該為SVM根磁碟區建立_load-sharing mirror _複本。



A namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy.

範例

以下範例建立一個名為「 'home4' 」的 Volume 、該 Volume 位於 SVM VS1 上、且具有交會路徑 `/eng/home` ：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```

了解 **ONTAP NAS** 命名空間架構

您可以在建立SVM名稱空間時、使用幾種典型的NAS命名空間架構。您可以選擇符合業務和工作流程需求的命名空間架構。

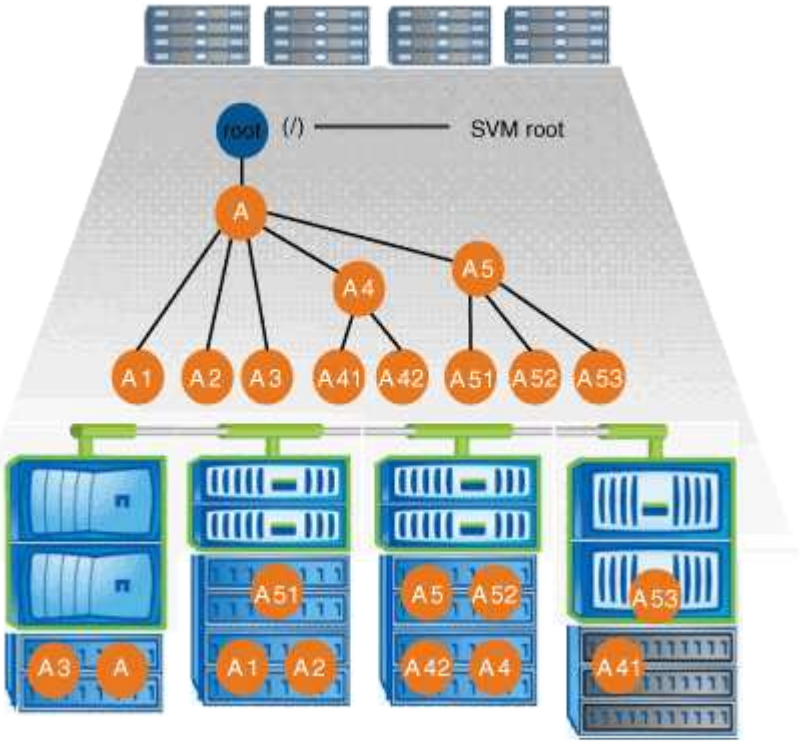
命名空間的頂端永遠是根磁碟區、以斜槓（/）表示。根目錄下的命名空間架構可分為三個基本類別：

- 單一分支樹狀結構、只有一個連接點可連接至命名空間的根
- 多個分支樹狀結構、並有多個交會點指向命名空間的根目錄

- 多個獨立磁碟區、每個磁碟區都有一個指向名稱空間根的獨立交會點

具有單一分支樹狀結構的命名空間

具有單一分支樹狀結構的架構具有單一插入點、可插入SVM命名空間的根目錄。單一插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在單一插入點下方的交會點（可以是磁碟區或目錄）。

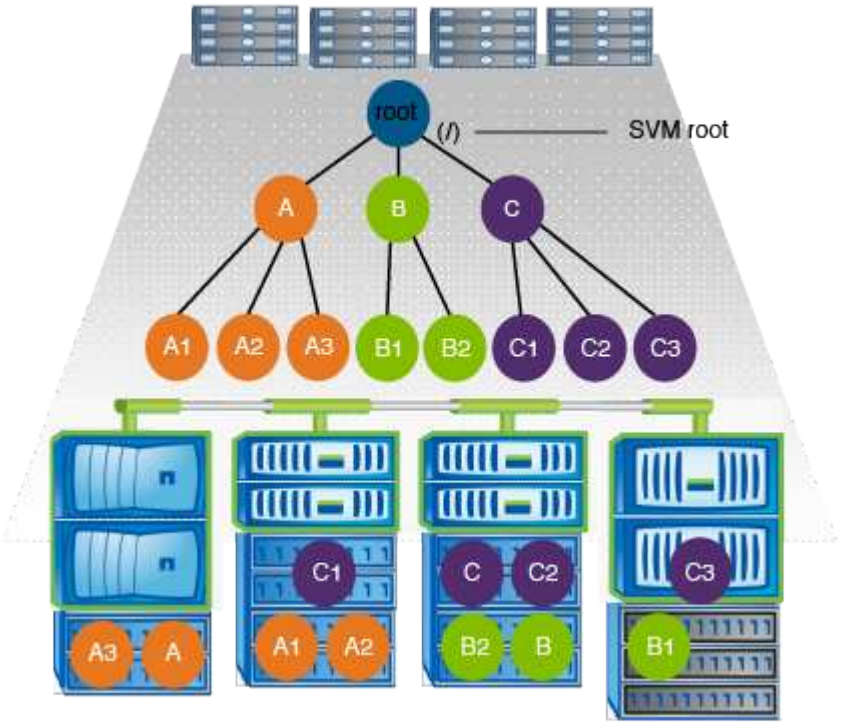


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中所有磁碟區都會連結到單一插入點下方、亦即名為「data'」的目錄：

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     corp1       true     /data/dir1/corp1         RW_volume
vs1     corp2       true     /data/dir1/corp2         RW_volume
vs1     data1       true     /data/data1              RW_volume
vs1     eng1        true     /data/data1/eng1         RW_volume
vs1     eng2        true     /data/data1/eng2         RW_volume
vs1     sales       true     /data/data1/sales        RW_volume
vs1     vol1        true     /data/vol1               RW_volume
vs1     vol2        true     /data/vol2               RW_volume
vs1     vol3        true     /data/vol3               RW_volume
vs1     vs1_root    -        /                        -
```

具有多個分支樹狀結構的命名空間

具有多個分支樹狀結構的架構具有多個插入點、可插入到SVM命名空間的根目錄。插入點可以是輔助磁碟區、也可以是根目錄下的目錄。所有其他磁碟區都會安裝在插入點下方的交會點（可以是磁碟區或目錄）。

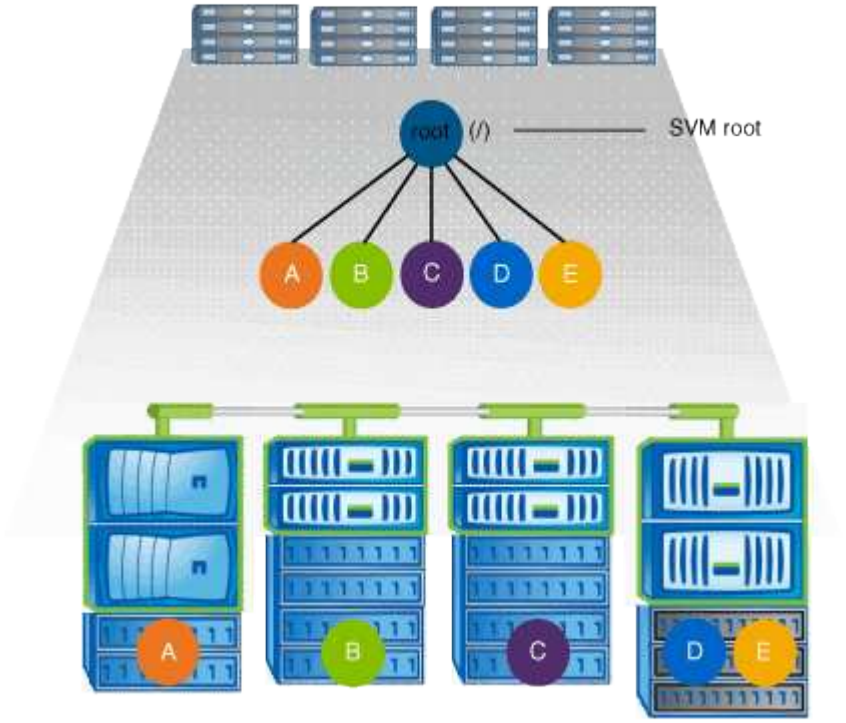


例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有三個插入點可插入SVM的根Volume。兩個插入點是名為「dATA」和「專案」的目錄。其中一個插入點是名為「稽核」的輔助磁碟區：

```
                 Junction                       Junction
Vserver Volume   Active   Junction Path         Path Source
------- -------- -------- -------------------   -----------
vs1     audit    true     /audit                RW_volume
vs1     audit_logs1  true     /audit/logs1          RW_volume
vs1     audit_logs2  true     /audit/logs2          RW_volume
vs1     audit_logs3  true     /audit/logs3          RW_volume
vs1     eng      true     /data/eng             RW_volume
vs1     mktg1    true     /data/mktg1           RW_volume
vs1     mktg2    true     /data/mktg2           RW_volume
vs1     project1 true     /projects/project1    RW_volume
vs1     project2 true     /projects/project2    RW_volume
vs1     vs1_root -        /                     -
```

具有多個獨立磁碟區的命名空間

在具有獨立磁碟區的架構中、每個磁碟區都有一個插入點、指向SVM命名空間的根目錄、但是該磁碟區並未與另一個磁碟區連結。每個磁碟區都有一個獨特的路徑、可以直接連接到根目錄下方、也可以連接到根目錄下方的目錄下。



例如、具有上述命名空間架構的典型Volume交會組態可能類似下列組態、其中有五個插入點指向SVM的根Volume、每個插入點代表一個Volume的路徑。

```
                    Junction                        Junction
Vserver Volume      Active   Junction Path          Path Source
------- ----------- -------- --------------------   -----------
vs1     eng         true     /eng                   RW_volume
vs1     mktg        true     /vol/mktg              RW_volume
vs1     project1    true     /project1              RW_volume
vs1     project2    true     /project2              RW_volume
vs1     sales       true     /sales                 RW_volume
vs1     vs1_root    -        /                      -
```

如何控制對檔案的存取**ONTAP**

了解 **ONTAP NAS** 檔案存取控制

根據您指定的驗證型和檔案型限制、支援對檔案的存取。ONTAP

當用戶端連線至儲存系統以存取檔案時ONTAP 、必須執行兩項工作：

- 驗證

  透過驗證信任來源的身分識別、即可驗證用戶端。ONTAP此外、用戶端的驗證類型是一種方法、可用來判斷用戶端在設定匯出原則時是否能存取資料（CIFS為選用）。

- 授權

透過比較使用者的認證資料與檔案或目錄上設定的權限、以及決定要提供的存取類型（如果有）、即可授權使用者。ONTAP

為了妥善管理檔案存取控制、ONTAP 必須與外部服務（例如NIS、LDAP和Active Directory伺服器）通訊。若要使用CIFS或NFS設定檔案存取的儲存系統、必須視ONTAP 您的環境而定、設定適當的服務。

了解 **ONTAP NAS SVM** 基於身份驗證的限制

有了驗證型限制、您可以指定哪些用戶端機器、以及哪些使用者可以連線至儲存虛擬機器（SVM）。

支援UNIX和Windows伺服器的Kerberos驗證。ONTAP

了解 **ONTAP NAS SVM** 的基於檔案的限制

此功能可評估三種安全層級、以判斷實體是否有權針對位於SVM上的檔案和目錄執行要求的動作。ONTAP存取權取決於評估三種安全層級後的有效權限。

任何儲存物件最多可包含三種類型的安全層：

- 匯出（NFS）和共用（SMB）安全性

  匯出及共用安全性適用於用戶端存取特定NFS匯出或SMB共用區。具有管理權限的使用者可以從SMB和NFS用戶端管理匯出和共用層級的安全性。

- 儲存層級的存取保護檔案和目錄安全性

  儲存層級的存取保護安全性適用於存取SVM磁碟區的SMB和NFS用戶端。僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

  > 如果您從NFS或SMB用戶端檢視檔案或目錄的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。

- NTFS、UNIX及NFSv4原生檔案層級安全性

  代表儲存物件的檔案或目錄中存在原生檔案層級安全性。您可以從用戶端設定檔案層級的安全性。無論使用SMB或NFS存取資料、檔案權限都有效。

ONTAP 如何處理 **NFS** 用戶端驗證

了解 **NAS** 用戶端的 **ONTAP** 驗證

NFS用戶端必須經過適當驗證、才能存取SVM上的資料。利用您所設定的名稱服務來檢查UNIX認證、藉此驗證用戶端。ONTAP

當NFS用戶端連線至SVM時、ONTAP 根據SVM的名稱服務組態、透過檢查不同的名稱服務來取得使用者的UNIX認證。可檢查本機UNIX帳戶、NIS網域及LDAP網域的認證資料。ONTAP至少必須設定其中一項、ONTAP 才能讓支援中心成功驗證使用者。您可以指定多個名稱服務及ONTAP 其搜尋順序。

在純NFS環境中使用UNIX Volume安全性樣式、此組態足以驗證並為從NFS用戶端連線的使用者提供適當的檔案存取。

如果您使用混合、NTFS或統一磁碟區安全樣式、ONTAP 則必須為UNIX使用者取得SMB使用者名稱、才能使用Windows網域控制器進行驗證。這可能是因為使用本機UNIX帳戶或LDAP網域來對應個別使用者、或改用預設的SMB使用者。您可以指定ONTAP 名稱服務以何種順序搜尋、或指定預設的SMB使用者。

了解 **ONTAP** 如何使用名稱服務

使用名稱服務取得使用者和用戶端的相關資訊。ONTAP使用此資訊驗證使用者存取或管理儲存系統上的資料、並在混合式環境中對應使用者認證資料。ONTAP

當您設定儲存系統時、必須指定ONTAP 要使用哪些名稱服務來取得使用者認證以進行驗證。支援下列名稱服務：ONTAP

- 本機使用者（檔案）
- 外部NIS網域（NIS）
- 外部 LDAP 網域（ LDAP ）

您可以使用 `vserver services name-service ns-switch` 命令系列可將 SVM 設定為使用來源來搜尋網路資訊、以及搜尋這些資訊的順序。這些命令可提供的等效功能 `/etc/nsswitch.conf` UNIX 系統上的檔案。

當NFS用戶端連線至SVM時、ONTAP 此功能會檢查指定的名稱服務、以取得使用者的UNIX認證資料。如果名稱服務設定正確、ONTAP 而且能夠取得UNIX認證資料、ONTAP 則無法成功驗證使用者。

在混合式安全型態的環境中ONTAP 、可能必須對應使用者認證資料。您必須針對環境適當設定名稱服務、以便ONTAP 讓支援功能能夠正確對應使用者認證資料。

此外、還會使用名稱服務來驗證SVM系統管理員帳戶。ONTAP在設定或修改名稱服務交換器時、您必須謹記此點、以免意外停用SVM系統管理員帳戶的驗證。如需SVM管理使用者的詳細資訊、請參閱 "系統管理員驗證與RBAC"。

授予從 **NFS** 用戶端存取 **ONTAP SMB** 檔案的權限

使用Windows NT檔案系統（NTFS）安全性語意、判斷UNIX使用者是否能在NFS用戶端上存取具有NTFS權限的檔案。ONTAP

為達成此目的、可將使用者的UNIX使用者ID（UID）轉換成SMB認證、然後使用SMB認證來驗證使用者是否擁有檔案的存取權限。ONTAPSMB認證包含主要安全性識別碼（SID）、通常是使用者的Windows使用者名稱、以及對應於使用者所屬Windows群組的一或多個群組SID。

將UNIX UID轉換為SMB認證所需的時間ONTAP 可從數十毫秒轉換為數百毫秒、因為此程序涉及連絡網域控制器。此功能可將UID對應至SMB認證、並在認證快取中輸入對應、以縮短轉換所造成的驗證時間。ONTAP

ONTAP NFS 憑證快取的工作原理

當NFS使用者要求存取儲存系統上的NFS匯出時、ONTAP 必須從外部名稱伺服器或從本機檔案擷取使用者認證資料、才能驗證使用者。然後將這些認證資料儲存在內部認證快取中、以供日後參考。ONTAP瞭解NFS認證快取的運作方式、可讓您處理潛在的效能和存取問題。

如果沒有認證快取、ONTAP 每當NFS使用者要求存取時、就必須查詢名稱服務。在許多使用者存取的忙碌儲存系統上、這很快就會導致嚴重的效能問題、造成不必要的延遲、甚至使NFS用戶端存取遭到拒絕。

利用認證快取功能、ONTAP 當NFS用戶端傳送另一個要求時、將會擷取使用者認證資料、然後儲存預先決定的時間量、以便快速輕鬆地存取。此方法具有下列優點：

- 它可處理較少的外部名稱伺服器（例如NIS或LDAP）要求、進而減輕儲存系統的負載。
- 它能減少傳送要求給外部名稱伺服器的次數、進而減輕其負載。
- 它可免除從外部來源取得認證的等待時間、以便驗證使用者、進而加速使用者存取。

支援將正面和負面的認證資料儲存在認證快取中。ONTAP正向認證表示使用者已通過驗證並獲得存取權。負面認證表示使用者未通過驗證、因此被拒絕存取。

根據預設、ONTAP 將正向認證資料儲存24小時；也就是ONTAP 在初始驗證使用者之後、將快取認證資料用於該使用者24小時內的任何存取要求。如果使用者在24小時後要求存取、週期就會開始：ONTAP 由下列項目開始：循環捨棄快取的認證資料、並從適當的名稱服務來源再次取得認證資料。如果在過去24小時內、名稱伺服器上的認證有所變更、ONTAP 則會快取更新的認證資料、以供未來24小時使用。

根據預設、ONTAP 功能不正常的情況下、將負面認證資料儲存兩小時；也就是ONTAP 在一開始拒絕使用者存取之後、該使用者在兩小時內仍拒絕任何存取要求。如果使用者在2小時後要求存取、則週期將從下列項目開始：ONTAP 再次從適當的名稱服務來源取得認證。如果在過去兩小時內、名稱伺服器上的認證資料有所變更、ONTAP 則會快取更新的認證資料、以供未來兩小時使用。

在NAS命名空間中建立及管理資料磁碟區

使用指定的連接點建立 **ONTAP NAS** 卷

您可以在建立資料Volume時指定交會點。結果Volume會自動掛載於交會點、並可立即設定以進行NAS存取。

開始之前

- 您要在其中建立磁碟區的集合體必須已經存在。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

  若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

> 下列字元無法用於連接路徑： `* # " > < | ? \`

此外、交會路徑長度不得超過255個字元。

步驟

1. 建立具有交會點的Volume：

```
volume create -vserver <vserver_name> -volume <volume_name> -aggregate
<aggregate_name> -size {integer[KB|MB|GB|TB|PB]} -security-style
{ntfs|unix|mixed} -junction-path <junction_path>
```

交會路徑必須以根（/）開頭、且可同時包含目錄和輔助磁碟區。交會路徑不需要包含磁碟區名稱。交會路徑與磁碟區名稱無關。

指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用至所建立資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

接合路徑不區分大小寫； `/ENG` 與相同 `/eng`。如果您建立CIFS共用區、Windows會將交會路徑視為區分大小寫。例如、如果交會是 `/ENG`， SMB 共享的路徑必須以開頭 `/ENG`、不是 `/eng`。

您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 確認已使用所需的交會點建立磁碟區：

```
volume show -vserver <vserver_name> -volume <volume_name> -junction
```

範例

以下範例建立一個名為 SVM VS1 的磁碟區，該磁碟區 `home4`具有連接路徑 `/eng/home`：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

建立沒有特定連接點的 **ONTAP NAS** 卷

您可以建立資料Volume而不指定交會點。結果Volume不會自動掛載、也無法設定NAS存取。您必須先掛載磁碟區、才能設定該磁碟區的SMB共用區或NFS匯出。

開始之前

- 您要在其中建立磁碟區的集合體必須已經存在。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

步驟

1. 使用下列命令建立沒有交會點的磁碟區：

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style
   {ntfs|unix|mixed}
   ```

   指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用到資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

   您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 驗證是否在沒有連接點的情況下建立磁碟區：

   ```
   volume show -vserver vserver_name -volume volume_name -junction
   ```

範例

下列範例建立名為「shes」的磁碟區、位於SVM VS1上、但未掛載於交會點：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      -        -               -
```

在 **NAS** 命名空間中掛載或卸載 **ONTAP NFS** 卷

磁碟區必須先掛載到NAS命名空間、才能設定NAS用戶端存取儲存虛擬機器（SVM）磁碟區中所含的資料。如果目前未掛載磁碟區、您可以將其掛載至交會點。您也可以卸載Volume。

關於這項工作

如果您卸載磁碟區並使其離線、則 NAS 用戶端無法存取連接點內的所有資料、包括位於未掛載磁碟區命名空間內具有連接點的磁碟區中的資料。

若要停止NAS用戶端對磁碟區的存取、只是卸載磁碟區是不夠的。您必須將磁碟區離線、或採取其他步驟、確保用戶端檔案處理快取無效。如需詳細資訊、請參閱下列知識庫文章：

"NFSv3用戶端在從ONTAP 靜態命名空間移除後、仍可存取Volume"

當您卸載磁碟區並離線時、磁碟區內的資料不會遺失。此外、在磁碟區或未掛載磁碟區內的目錄和交會點上建立的現有磁碟區匯出原則和SMB共用也會保留下來。如果您重新掛載未掛載的Volume、NAS用戶端可以使用現有的匯出原則和SMB共用來存取磁碟區內的資料。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
掛載Volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

卸載Volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 驗證磁碟區是否處於所需的掛載狀態：

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

範例

以下範例將位於 SVM 'VS1' 的名為 """""""s'" 的 Volume 裝入連接點 "'/sales" ：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下範例將卸載並離線位於 SVM 「'VS1 」上的名為「 dATA 」的磁碟區：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

顯示 **ONTAP NAS Volume** 裝載和交會點資訊

您可以顯示儲存虛擬機器（SVM）掛載磁碟區的相關資訊、以及掛載磁碟區的交會點。您也可以決定哪些磁碟區未掛載到交會點。您可以使用此資訊來瞭解及管理SVM命名空間。

步驟

1. 執行所需的動作：

如果您要顯示…	輸入命令…
SVM上掛載與卸載磁碟區的摘要資訊	`volume show -vserver vserver_name -junction`
SVM上掛載與卸載磁碟區的詳細資訊	`volume show -vserver vserver_name -volume volume_name -instance`

有關SVM上掛載和卸載磁碟區的特定資訊	a. 如有必要、您可以顯示的有效欄位 `-fields` 使用下列命令的參數：
	`volume show -fields ?`
	b. 使用顯示所需資訊 `-fields` 參數：
	`volume show -vserver vserver_name -fields fieldname,…`

範例

下列範例顯示SVM VS1上掛載與卸載磁碟區的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

下列範例顯示SVM VS2上磁碟區的指定欄位資訊：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

設定安全樣式

安全樣式如何影響資料存取

了解 **ONTAP NAS** 安全模式

共有四種不同的安全型態：UNIX、NTFS、混合式及統一化。每種安全樣式對資料權限的處理方式都有不同的影響。您必須瞭解不同的影響、以確保為您的目的選擇適當的安全型態。

請務必瞭解、安全樣式並未決定哪些用戶端類型可以或無法存取資料。安全樣式只會決定ONTAP 用來控制資料存取的權限類型、以及哪些用戶端類型可以修改這些權限。

例如、如果某個磁碟區使用UNIX安全型態、則SMB用戶端仍可存取資料（前提是他們必須正確驗證及授權）、因為ONTAP 此為多重傳輸協定的本質。不過ONTAP 、VMware使用UNIX權限、只有UNIX用戶端可以使用原生工具進行修改。

安全風格	可以修改權限的用戶端	用戶端可以使用的權限	打造出有效的安全風格	可存取檔案的用戶端
UNIX	NFS	NFSv3模式位元	UNIX	NFS與SMB
		NFSv4.x ACL		
NTFS	中小企業	NTFS ACL	NTFS	
混合	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.ACL		
		NTFS ACL	NTFS	
統一化（僅適用於 Infinite Volume 、 ONTAP 9.4 及更早版本。）	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

支援UNIX、NTFS和混合式安全型態的支援。FlexVol當安全性樣式混合或統一化時、有效權限取決於上次修改權限的用戶端類型、因為使用者是個別設定安全性樣式。如果上次修改權限的用戶端是NFSv3用戶端、則權限為UNIX NFSv3模式位元。如果最後一個用戶端是NFSv4用戶端、則權限為NFSv4 ACL。如果最後一個用戶端是SMB用戶端、則權限為Windows NTFS ACL。

統一化的安全風格僅適用於無限個Volume、ONTAP 而不再支援於更新版本的版本。如需詳細資訊、請參閱 介紹Volume管理總覽FlexGroup。

這 `show-effective-permissions`參數 `vserver security file-directory`命令可讓您顯示授予 Windows 或 UNIX 使用者在指定檔案或資料夾路徑上的有效權限。此外，選用參數 `-share-name`可讓您顯示有效共用權限。如"指令參考資料ONTAP"需詳細 `vserver security file-directory show-effective-permissions`資訊，請參閱。

> 最初設定部分預設檔案權限。ONTAP根據預設、UNIX、混合式及統一化安全樣式磁碟區中所有資料的有效安全樣式為UNIX、有效權限類型為UNIX模式位元（0755、除非另有說明）、直到用戶端依照預設安全性樣式所允許的方式進行設定為止。根據預設、NTFS安全型磁碟區中所有資料的有效安全樣式為NTFS、並具有ACL、可讓所有人完全掌控。

相關資訊

- "指令參考資料ONTAP"

了解 **ONTAP NFS FlexVol** 磁碟區的安全模式

安全樣式可在FlexVol 支援樹狀結構（根或資料磁碟區）和qtree上設定。安全樣式可在建立時手動設定、自動繼承或稍後變更。

確定在 **ONTAP NAS SVM** 上使用哪種安全模式

為了協助您決定要在磁碟區上使用哪種安全樣式、您應該考慮兩個因素。主要因素是管理檔案系統的系統管理員類型。次要因素是存取磁碟區上資料的使用者或服務類型。

在Volume上設定安全樣式時、您應該考慮環境的需求、以確保您選擇最佳的安全樣式、並避免管理權限時發生問題。下列考量事項可協助您決定：

安全風格	選擇是否…
UNIX	• 檔案系統由UNIX管理員管理。 • 大多數使用者是NFS用戶端。 • 存取資料的應用程式會使用UNIX使用者做為服務帳戶。
NTFS	• 檔案系統由Windows管理員管理。 • 大多數使用者是 SMB 用戶端。 • 存取資料的應用程式會使用Windows使用者做為服務帳戶。
混合	• 檔案系統由UNIX和Windows系統管理員管理、使用者同時由NFS和SMB用戶端組成。

瞭解 **ONTAP NFS** 安全風格的繼承

如果您在建立新FlexVol 的流通量或qtree時未指定安全樣式、它會以不同的方式繼承其安全風格。

安全樣式會以下列方式繼承：

- 此功能會繼承包含SVM的根磁碟區安全樣式。FlexVol
- qtree會繼承其包含FlexVol 的不穩定區的安全樣式。
- 檔案或目錄會繼承其包含FlexVol 的不穩定磁碟區或qtree的安全樣式。

了解 **ONTAP NFS UNIX** 權限保留

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

使用 **Windows** 安全性標籤管理 **ONTAP NFS SVM** 上的 **UNIX** 權限

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、

可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

  您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全性型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

  如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

  您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全性型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

  您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全性型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

  變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。

在 **ONTAP NFS SVM** 根磁碟區上設定安全模式

您可以設定儲存虛擬機器（SVM）根磁碟區安全樣式、以決定SVM根磁碟區上資料所使用的權限類型。

步驟

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 定義安全樣式的參數。

   根 Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

2. 顯示並驗證組態、包括您所建立SVM的根磁碟區安全樣式：

   ```
   vserver show -vserver vserver_name
   ```

在 **ONTAP NFS FlexVol** 磁碟區上設定安全樣式

您可以設定FlexVol 「靜態Volume」安全樣式、以判斷FlexVol 儲存虛擬機器（SVM）的各個版本上的資料所使用的權限類型。

步驟

1. 執行下列其中一項動作：

如果FlexVol 是這個問題…	使用命令…

尚不存在	`volume create` 並包含 `-security-style` 指定安全樣式的參數。
已存在	`volume modify` 並包含 `-security-style` 指定安全樣式的參數。

FlexVol Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果您在建立FlexVol 一個穩定區時未指定安全樣式、則此磁碟區會繼承根磁碟區的安全樣式。

如需更多關於的資訊、請參閱 `volume create` 或 `volume modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括FlexVol 您所建立的穩定功能、請輸入下列命令：

```
volume show -volume volume_name -instance
```

在 ONTAP NFS qtree 上設定安全模式

您可以設定qtree Volume安全樣式、以決定用於qtree上資料的權限類型。

步驟

1. 執行下列其中一項動作：

如果qtree …	使用命令…
尚未存在	`volume qtree create` 並包含 `-security-style` 指定安全樣式的參數。
已存在	`volume qtree modify` 並包含 `-security-style` 指定安全樣式的參數。

qtree 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果在建立 qtree 時未指定安全樣式、則預設的安全樣式為 `mixed`。

如需更多關於的資訊、請參閱 `volume qtree create` 或 `volume qtree modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括您建立的 qtree 安全樣式、請輸入下列命令： `volume qtree show -qtree` *`qtree_name`* `-instance`

使用 NFS 設定檔案存取

了解如何在 ONTAP SVM 上設定 NFS 檔案訪問

您必須完成許多步驟、才能讓用戶端使用NFS存取儲存虛擬機器（SVM）上的檔案。根據您環境的目前組態、還有一些額外的選用步驟。

若要讓用戶端能夠使用NFS存取SVM上的檔案、您必須完成下列工作：

1. 在SVM上啟用NFS傳輸協定。

   您必須設定SVM、以便透過NFS從用戶端存取資料。

2. 在SVM上建立NFS伺服器。

   NFS伺服器是SVM上的邏輯實體、可讓SVM透過NFS提供檔案服務。您必須建立NFS伺服器、並指定您要允許的NFS傳輸協定版本。

3. 在SVM上設定匯出原則。

   您必須設定匯出原則、讓用戶端可使用磁碟區和qtree。

4. 視網路和儲存環境而定、使用適當的安全性和其他設定來設定NFS伺服器。

   此步驟可能包括設定Kerberos、LDAP、NIS、名稱對應及本機使用者。

使用匯出原則保護**NFS**存取安全

導出策略如何控制用戶端對 **ONTAP NFS** 磁碟區或 **qtree** 的存取

匯出原則包含一或多個用以處理每個用戶端存取要求的_EXPORT規則_。此程序的結果決定了用戶端是被拒絕還是被授予存取權限、以及存取層級。儲存虛擬機器（SVM）上必須存在具有匯出規則的匯出原則、用戶端才能存取資料。

您只需將一個匯出原則與每個Volume或qtree建立關聯、即可設定用戶端對Volume或qtree的存取。SVM可包含多個匯出原則。這可讓您針對具有多個磁碟區或qtree的SVM執行下列作業：

- 為SVM的每個Volume或qtree指派不同的匯出原則、以便個別用戶端存取控制到SVM中的每個Volume或qtree。
- 將相同的匯出原則指派給SVM的多個磁碟區或qtree、以獲得相同的用戶端存取控制、而不需要為每個磁碟區或qtree建立新的匯出原則。

如果用戶端提出的存取要求不受適用的匯出原則允許、則要求會以拒絕權限的訊息失敗。如果用戶端不符合匯出原則中的任何規則、則會拒絕存取。如果匯出原則是空的、則所有存取都會隱含拒絕。

您可以在執行ONTAP 不正常運作的系統上動態修改匯出原則。

ONTAP NFS SVM 的預設導出策略

每個SVM都有一個預設匯出原則、不含任何規則。用戶端必須先存在具有規則的匯出原則、才能存取SVM上的資料。SVM中包含的每FlexVol 個SVM磁碟區都必須與匯出原則相關聯。

建立 SVM 時、儲存系統會自動建立名為的預設匯出原則 `default` 適用於 SVM 的根 Volume 。您必須先為預設匯出原則建立一或多個規則、用戶端才能存取SVM上的資料。或者、您也可以建立具有規則的自訂匯出原則。您可以修改及重新命名預設匯出原則、但無法刪除預設匯出原則。

當您在FlexVol 包含SVM的磁碟區中建立一個SVM時、儲存系統會建立該磁碟區、並將該磁碟區與SVM根磁碟區的預設匯出原則建立關聯。根據預設、在SVM中建立的每個Volume都會與根Volume的預設匯出原則相關聯。您可以針對SVM中包含的所有磁碟區使用預設匯出原則、也可以針對每個磁碟區建立唯一的匯出原則。您可以將

多個磁碟區與相同的匯出原則建立關聯。

ONTAP NFS 導出規則的工作原理

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、將用戶端存取要求與磁碟區相符、以決定如何處理用戶端存取要求。

匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而且不會再處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

您可以使用下列準則來設定匯出規則、以決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定、例如NFSv4或SMB。
- 用戶端識別碼、例如主機名稱或IP位址。

  的最大大小 `-clientmatch` 欄位為 4096 個字元。

- 用戶端用來驗證的安全性類型、例如Kerberos v5, NTL,或AUTH_SYS。

如果規則指定多個準則、用戶端必須符合所有準則、才能套用規則。

> 從ONTAP 功能表支援的支援範例9.3開始、您可以啟用匯出原則組態檢查、做為背景工作、將任何違反規則的行為記錄在錯誤規則清單中。。 `vserver export-policy config-checker` 命令會叫用檢查程式並顯示結果、您可以使用這些結果來驗證組態並從原則中刪除錯誤規則。
>
> 這些命令只會驗證主機名稱、網路群組和匿名使用者的匯出組態。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv3傳輸協定傳送、用戶端的IP位址為10.1.17.37。

即使用戶端存取傳輸協定相符、用戶端的IP位址仍位於與匯出規則中指定的子網路不同的子網路中。因此、用戶端比對失敗、此規則不適用於此用戶端。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`

- `-rwrule any`

用戶端存取要求是使用NFSv4傳輸協定傳送、用戶端的IP位址為10.1.16.54。

用戶端存取傳輸協定相符、用戶端的IP位址位於指定的子網路中。因此、用戶端配對成功、此規則適用於此用戶端。無論用戶端的安全類型為何、都能取得讀寫存取權。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。因此這兩個用戶端都能取得唯讀存取權。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

管理具有未列出的安全性類型的 **NFS** 用戶端的 **ONTAP SVM** 訪問

當用戶端呈現未列在匯出規則存取參數中的安全性類型時、您可以選擇拒絕用戶端存取、或改用選項將其對應至匿名使用者 ID `none` 在存取參數中。

用戶端可能會出現未列在存取參數中的安全性類型、因為它是以不同的安全性類型驗證、或根本未驗證（安全性類型AUTH_NONE）。根據預設、用戶端會自動拒絕存取該層級。不過、您可以新增選項 `none` 存取參數。因此、具有未列出安全性樣式的用戶端會對應至匿名使用者ID。。 `-anon` 參數決定指派給這些用戶端的使用者 ID 。為指定的使用者 ID `-anon` 參數必須是有效的使用者、且必須設定您認為適合匿名使用者的權限。

的有效值 `-anon` 參數範圍從 `0` 至 `65535`。

指派給的使用者 **ID** `-anon`	最終處理用戶端存取要求
`0 - 65533`	用戶端存取要求會對應至匿名使用者ID、並根據為此使用者設定的權限而取得存取權。
`65534`	用戶端存取要求會對應至使用者nobody、並根據為此使用者設定的權限而取得存取權。這是預設值。
`65535`	任何用戶端的存取要求都會在對應至此ID時遭到拒絕、而用戶端會顯示安全性類型AUTH_NONE。當用戶ID為0的用戶端對應至此ID時、會拒絕該用戶端的存取要求、而用戶端會顯示任何其他安全類型。

使用選項時 `none`請務必記住、唯讀參數會先處理。針對未列出的安全性類型用戶端設定匯出規則時、請考慮下列準則：

唯讀包含 none	讀寫包括 none	產生未列出安全性類型之用戶端的存取權
否	否	已拒絕
否	是的	因為先處理唯讀而遭拒
是的	否	唯讀為匿名
是的	是的	匿名讀寫

範例

以下範例展示了一個出口策略，該策略包含： `-rwrule any` 範圍：

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`
- `-rwrule any`
- `-anon 70`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

用戶端#3的IP位址為10.1.16.234、使用NFSv3傳輸協定傳送存取要求、但未驗證（亦即安全性類型AUTH_NONE）。

這三個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許以驗證為AUTH_SYS的自有使用者ID來唯讀存取用戶端。唯讀參數允許匿名使用者以使用者ID 70的身分存取使用任何其他安全性類型驗證的用戶端。讀寫參數允許對任何安全類型進行讀寫存取、但在這種情況下、僅適用於已由唯讀規則篩選的用戶端。

因此、用戶端#1和#3只能以使用者ID 70的匿名使用者身分取得讀寫存取權。用戶端#2使用自己的使用者ID取得讀寫存取權。

以下範例展示了一個出口策略，該策略包含： `-rwrule none` 範圍：

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule sys,none`

- `-rwrule none`
- `-anon 70`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

用戶端#3的IP位址為10.1.16.234、使用NFSv3傳輸協定傳送存取要求、但未驗證（亦即安全性類型AUTH_NONE）。

這三個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許以驗證為AUTH_SYS的自有使用者ID來唯讀存取用戶端。唯讀參數允許匿名使用者以使用者ID 70的身分存取使用任何其他安全性類型驗證的用戶端。讀寫參數只允許匿名使用者進行讀寫存取。

因此、用戶端#1和用戶端#3只能以使用者ID 70的匿名使用者身分取得讀寫存取權。用戶端#2使用自己的使用者ID取得唯讀存取權、但拒絕讀寫存取。

ONTAP 安全性類型如何決定 **NFS** 用戶端存取級別

用戶端驗證的安全性類型在匯出規則中扮演特殊角色。您必須瞭解安全性類型如何決定用戶端存取Volume或qtree的層級。

三種可能的存取層級如下：

1. 唯讀
2. 讀寫
3. 超級使用者（適用於使用者ID為0的用戶端）

由於依安全性類型評估存取層級的順序如下、因此在匯出規則中建構存取層級參數時、您必須遵守下列規則：

若要讓用戶端取得存取層級...	這些存取參數必須符合用戶端的安全類型...
一般使用者唯讀	唯讀 (`-rorule`)
一般使用者讀寫	唯讀 (`-rorule`) 和讀寫 (`-rwrule`)
超級使用者唯讀	唯讀 (`-rorule`) 和 `-superuser`
超級使用者讀寫	唯讀 (`-rorule`) 和讀寫 (`-rwrule`) 和 `-superuser`

以下是這三種存取參數的有效安全類型：

- `any`
- `none`
- `never`

  此安全性類型不適用於 `-superuser` 參數。

- krb5
- krb5i
- krb5p
- ntlm
- sys

將用戶端的安全類型與三個存取參數中的每個參數配對時、可能會產生三種結果：

如果用戶端的安全類型...	然後用戶端...
符合存取參數中指定的。	使用自己的使用者ID取得該層級的存取權。
與指定的不相符、但存取參數包含選項 none。	取得該層級的存取權、但以匿名使用者的身分、使用由指定的使用者 ID -anon 參數。
與指定的不相符、存取參數不包含選項 none。	無法取得該層級的任何存取權。這不適用於 -superuser 參數、因為它永遠包含在內 none 即使未指定、

範例

匯出原則包含具有下列參數的匯出規則：

- -protocol nfs3
- -clientmatch 10.1.16.0/255.255.255.0
- -rorule any
- -rwrule sys,krb5
- -superuser krb5

用戶端#1的IP位址為10.1.16.207、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

用戶端#3的IP位址為10.1.16.234、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、但未驗證（AUTH_NONE）。

用戶端存取傳輸協定和IP位址符合這三個用戶端。唯讀參數允許所有用戶端的唯讀存取權、無論安全類型為何。讀寫參數允許以驗證為AUTH_SYS或Kerberos v5的用戶ID讀寫用戶端存取。超級使用者參數可讓超級使用者存取使用Kerberos v5驗證的用戶ID 0用戶端。

因此、用戶端#1會取得超級使用者讀寫存取權、因為它會符合所有三個存取參數。用戶端#2可取得讀寫存取權、但不具備超級使用者存取權。用戶端#3可取得唯讀存取權、但無法取得超級使用者存取權。

了解如何管理 **ONTAP NFS** 超級使用者存取請求

設定匯出原則時、您必須考量儲存系統收到使用者ID為0的用戶端存取要求（表示以超級使

用者身分）時、會發生什麼情況、並據此設定匯出規則。

在UNIX世界中、使用者ID為0的使用者稱為超級使用者、通常稱為root、在系統上擁有無限存取權限。使用進階使用者權限可能會有危險、原因包括系統和資料安全性遭到破壞。

根據預設ONTAP 、功能表會將使用者ID為0的用戶端對應至匿名使用者。不過、您可以指定 - `superuser` 匯出規則中的參數、可決定如何處理使用者 ID 0 呈現的用戶端、視其安全性類型而定。下列是的有效選項 `-superuser` 參數：

- `any`
- `none`

  如果您未指定、這是預設設定 `-superuser` 參數。

- `krb5`
- `ntlm`
- `sys`

根據的不同、有兩種不同的方式來處理以使用者 ID 0 呈現的用戶端 `-superuser` 參數組態：

如果是 **`-superuser`** 參數和用戶端的安全類型 **...**	然後用戶端**...**
相符	以使用者ID 0取得超級使用者存取權。
不相符	以匿名使用者的身分取得存取權、並使用指定的使用者 ID `-anon` 參數及其指派的權限。無論唯讀或讀寫參數是否指定選項、都是如此 `none`。

如果用戶端提供使用者 ID 0 來存取具有 NTFS 安全性樣式的磁碟區、以及 `-superuser` 參數設定為 `none`，ONTAP 使用匿名使用者的名稱對應來取得適當的認證。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-anon 127`

用戶端 1 的 IP 位址為 10.16.207 、使用者 ID 746 、使用 NFSv3 傳輸協定傳送存取要求、並使用 Kerberos v5 進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。

用戶端#2無法取得超級使用者存取權。而是會對應至匿名、因為 `-superuser` 未指定參數。這表示預設為 `none` 並自動將使用者 ID 0 對應至匿名。用戶端#2也只會取得唯讀存取權、因為其安全性類型與讀寫參數不符。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`
- `-superuser krb5`
- `-anon 0`

用戶端#1的IP位址為10.1.16.207、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用者ID為0、使用NFSv3傳輸協定傳送存取要求、並以AUTH_SYS驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

匯出規則可讓使用者ID為0的用戶端擁有超級使用者存取權。用戶端 #1 獲得超級使用者存取權、因為它符合唯讀和的使用者 ID 和安全類型 `-superuser` 參數。用戶端 #2 無法取得讀寫或超級使用者存取權、因為其安全性類型與讀寫參數或不相符 `-superuser` 參數。而是將用戶端#2對應至匿名使用者、在此案例中、該使用者ID為0。

了解 **ONTAP NFS** 匯出策略緩存

為了提升系統效能、ONTAP 此功能使用本機快取來儲存主機名稱和網路群組等資訊。相較於從外部來源擷取資訊、這樣的功能可讓ONTAP 支援部門更快處理匯出原則規則。瞭解快取內容及其功能有助於疑難排解用戶端存取問題。

您可以設定匯出原則來控制用戶端對NFS匯出的存取。每個匯出原則都包含規則、而且每個規則都包含參數、可讓規則符合要求存取的用戶端。有些參數需要ONTAP 使用支援功能來聯絡外部來源、例如DNS或NIS伺服器、才能解析網域名稱、主機名稱或網路群組等物件。

這些與外部來源的通訊只需要很短的時間。為了提升效能ONTAP 、利用將資訊儲存在多個快取的每個節點上、藉此減少解析匯出原則規則物件所需的時間。

快取名稱	儲存的資訊類型
存取	用戶端對應至對應的匯出原則
名稱	UNIX使用者名稱對應至對應的UNIX使用者ID

快取名稱	儲存的資訊類型
ID	UNIX使用者ID對應至對應的UNIX使用者ID和延伸UNIX群組ID
主機	將主機名稱對應至對應的IP位址
網路群組	網路群組對應至成員對應的IP位址
showmount	從SVM命名空間匯出的目錄清單

如果在擷取並儲存於本機之後、變更環境中外部名稱伺服器的資訊ONTAP 、快取現在可能會包含過時的資訊。雖然在特定時間段後、會自動重新整理快取、但不同的快取會有不同的過期時間、重新整理時間和演算法。ONTAP

另一個快取包含過時資訊的可能原因是ONTAP 、當某些人嘗試重新整理快取的資訊、但嘗試與名稱伺服器通訊時卻遭遇失敗。如果發生這種情況、ONTAP 則會繼續使用目前儲存在本機快取中的資訊、以防止用戶端中斷運作。

因此、原本應該成功的用戶端存取要求可能會失敗、而原本應該失敗的用戶端存取要求可能會成功。疑難排解此類用戶端存取問題時、您可以檢視並手動清除部分匯出原則快取。

了解 **ONTAP NFS** 存取快取

使用存取快取來儲存匯出原則規則評估的結果、以便用戶端存取磁碟區或qtree的作業。ONTAP這會提高效能、因為每次用戶端傳送I/O要求時、從存取快取中擷取資訊的速度比執行匯出原則規則評估程序快得多。

每當NFS用戶端傳送I/O要求以存取磁碟區或qtree上的資料時、ONTAP 必須評估每個I/O要求、以判斷是否要授予或拒絕I/O要求。此評估包括檢查與Volume或qtree相關之匯出原則的每個匯出原則規則。如果通往Volume或qtree的路徑涉及跨越一或多個交會點、則可能需要對路徑上的多個匯出原則執行此檢查。

請注意、這項評估是針對從NFS用戶端傳送的每個I/O要求進行、例如讀取、寫入、清單、複製及其他作業；不只是針對初始掛載要求。

在確定適用的匯出原則規則並決定是否允許或拒絕該要求之後ONTAP 、即可在存取快取中建立一個項目來儲存此資訊。ONTAP

當NFS用戶端傳送I/O要求時、ONTAP 請注意用戶端的IP位址、SVM的ID、以及與目標Volume或qtree相關的匯出原則、然後先檢查存取快取是否有相符的項目。如果存取快取中存在相符的項目、ONTAP 則使用儲存的資訊來允許或拒絕I/O要求。如果不存在相符的項目、ONTAP 那麼就會依照上述說明、完成評估所有適用原則規則的正常程序。

未使用的存取快取項目不會重新整理。如此可減少使用外部名稱服務的不必要和浪費通訊。

從存取快取中擷取資訊的速度遠勝過針對每個I/O要求執行整個匯出原則規則評估程序。因此、使用存取快取可減少用戶端存取檢查的負荷、大幅提升效能。

了解 **ONTAP NFS** 存取快取參數

多個參數可控制存取快取中項目的重新整理期間。瞭解這些參數的運作方式、可讓您修改這些參數、以調整存取快取、並在效能與儲存資訊的最新程度之間取得平衡。

存取快取會儲存包含一或多個匯出規則的項目、這些規則適用於嘗試存取磁碟區或qtree的用戶端。這些項目會在重新整理之前儲存一段時間。重新整理時間取決於存取快取參數、並取決於存取快取項目的類型。

您可以指定個別SVM的存取快取參數。如此可讓參數根據SVM存取需求而有所不同。未使用的存取快取項目不會重新整理、如此可減少使用外部名稱服務的不必要和浪費通訊。

存取快取項目類型	說明	重新整理期間（以秒為單位）
正面項目	存取快取項目未導致用戶端存取遭拒。	最低：300 上限：86400 預設：3、600
負項目	存取快取項目導致拒絕用戶端存取。	最低： 60 上限：86400 預設：3、600

範例

NFS用戶端嘗試存取叢集上的磁碟區。將用戶端比對至匯出原則規則、並根據匯出原則規則組態來判斷用戶端是否可存取。ONTAP將匯出原則規則儲存在存取快取中、做為正面項目。ONTAP根據預設、ONTAP 功能表會在存取快取中保留正面項目一小時（3、600秒）、然後自動重新整理項目以保持資訊最新。

為了避免存取快取不必要地填滿、有一個額外的參數可以清除在特定時間段內尚未使用的現有存取快取項目、以決定用戶端存取。這 `-harvest-timeout` 參數的允許範圍為 60 到 2,592,000 秒、預設設定為 86,400 秒。

從 **ONTAP NFS qtree** 中刪除匯出策略

如果您決定不再想將特定的匯出原則指派給qtree、您可以修改qtree來移除匯出原則、改為繼承包含Volume的匯出原則。您可以使用來執行此作業 `volume qtree modify` 命令 `-export-policy` 參數和空白名稱字串（""）。

步驟

1. 若要從qtree移除匯出原則、請輸入下列命令：

   ```
   volume qtree modify -vserver vserver_name -qtree-path
   /vol/volume_name/qtree_name -export-policy ""
   ```

2. 驗證qtree是否已相應修改：

   ```
   volume qtree show -qtree qtree_name -fields export-policy
   ```

驗證 ONTAP NFS qtree ID 以執行 qtree 檔案操作

可選擇性地執行qtree ID的額外驗證。ONTAP此驗證可確保用戶端檔案作業要求使用有效的qtree ID、而且用戶端只能在同一個qtree內移動檔案。您可以修改來啟用或停用此驗證 `-validate-qtree-export` 參數。此參數預設為啟用。

關於這項工作

此參數僅在您已將匯出原則直接指派給儲存虛擬機器（SVM）上的一或多個qtree時有效。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要**qtree ID**驗證…	輸入下列命令…
已啟用	`vserver nfs modify -vserver vserver_name -validate-qtree-export enabled`
已停用	`vserver nfs modify -vserver vserver_name -validate-qtree-export disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

ONTAP NFS FlexVol 磁碟區的匯出策略限制和巢狀連接

如果您將匯出原則設定為在巢狀連接點上設定較少限制的原則、但在較高層連接點上設定較嚴格的原則、則對較低層連接點的存取可能會失敗。

您應確保較高層級的匯接器比較低層級的匯接器具有較少的匯出原則限制。

使用**Kerberos**搭配**NFS**以獲得強大的安全性

ONTAP NFS 對 Kerberos 的支持

Kerberos為用戶端/伺服器應用程式提供強大的安全驗證功能。驗證可驗證伺服器的使用者和處理程序身分。在支援VMware的環境中ONTAP 、Kerberos可在儲存虛擬機器（SVM）和NFS用戶端之間提供驗證。

在發揮作用的過程中、支援下列Kerberos功能：ONTAP

- Kerberos 5驗證搭配完整性檢查（krb5i）

Krb5i使用Checksum來驗證用戶端與伺服器之間傳輸的每個NFS訊息完整性。這項功能在安全性方面非常實用（例如、確保資料未遭竄改）、也有助於確保資料完整性（例如、在不可靠的網路上使用NFS時、可防止資料毀損）。

- Kerberos 5驗證搭配隱私權檢查（krb5p）

  Krb5p使用Checksum加密用戶端與伺服器之間的所有流量。這更安全、也會產生更多負載。

- 128位元和256位元AES加密

  進階加密標準（AES）是一種加密演算法、用於保護電子資料安全。ONTAP 支援採用 128 位元金鑰（ AES-128 ）的 AES 、以及採用 256 位元金鑰（ AES-256 ）加密的 AES 、以提供更強大的安全性。

- SVM層級Kerberos領域組態

  SVM系統管理員現在可以在SVM層級建立Kerberos領域組態。這表示SVM管理員不再需要仰賴叢集管理員來進行Kerberos領域組態、也能在多租戶環境中建立個別的Kerberos領域組態。

使用 **ONTAP NFS** 設定 **Kerberos** 的要求

在系統上使用NFS設定Kerberos之前、您必須先確認網路和儲存環境中的某些項目已正確設定。

> 設定環境的步驟取決於您所使用的用戶端作業系統、網域控制器、Kerberos、DNS等版本和類型。記錄所有這些變數不在此文件範圍之內。如需詳細資訊、請參閱各元件的相關文件。
>
> 如需ONTAP 如何在使用Windows Server 2008 R2 Active Directory和Linux主機的環境中使用NFSv3和NFSv3設定支援功能的支援功能和Kerberos 5的詳細範例、請參閱技術報告4073。

應先設定下列項目：

網路環境需求

- Kerberos

  您必須使用金鑰發佈中心（Kdc）進行有效的Kerberos設定、例如Windows Active Directory型Kerberos或MIT Kerberos。

  NFS 伺服器必須使用 `nfs` 作為其機器主體的主要元件。

- 目錄服務

  您必須在環境中使用安全目錄服務、例如Active Directory或OpenLDAP、這類服務設定為使用LDAP over SSL/TLS。

- NTP

  您必須有執行NTP的工作時間伺服器。這是防止Kerberos驗證因時間偏移而失敗的必要步驟。

- 網域名稱解析（DNS）

  每個UNIX用戶端和每個SVM LIF都必須在Kdc的正向和反向對應區域下註冊適當的服務記錄（SRF）。所有

參與者都必須透過DNS正確解析。

- 使用者帳戶

  每個用戶端都必須在Kerberos領域中擁有使用者帳戶。NFS伺服器必須使用「NFS」作為其機器主體的主要元件。

NFS 用戶端需求

- NFS

  每個用戶端都必須正確設定、才能使用NFSv3或NFSv4透過網路進行通訊。

  用戶端必須支援RFC1964和RFC2203。

- Kerberos

  每個用戶端都必須正確設定、才能使用Kerberos驗證、包括下列詳細資料：

  - 已啟用TGS通訊的加密。

    AES-256提供最強大的安全性。

  - 已啟用TGTT通訊最安全的加密類型。
  - Kerberos領域和網域已正確設定。
  - GSS 已啟用。

    使用機器認證時：

  - 請勿執行 `gssd` 使用 `-n` 參數。
  - 請勿執行 `kinit` 作為 root 使用者。

- 每個用戶端都必須使用最新且更新的作業系統版本。

  這可為使用Kerberos的AES加密提供最佳的相容性與可靠性。

- DNS

  每個用戶端都必須正確設定、才能使用DNS進行正確的名稱解析。

- NTP

  每個用戶端都必須與NTP伺服器同步。

- 主機與網域資訊

  每個用戶端 `/etc/hosts` 和 `/etc/resolv.conf` 檔案必須分別包含正確的主機名稱和 DNS 資訊。

- Keytab檔案

  每個用戶端都必須有來自於Kdc的Keytab檔案。領域必須以大寫字母顯示。加密類型必須為AES-256、才能獲得最強的安全性。

- 選用：為獲得最佳效能、用戶端可享有至少兩個網路介面：一個用於與區域網路通訊、另一個用於與儲存網路通訊。

儲存系統需求

- NFS授權

  儲存系統必須安裝有效的NFS授權。

- CIFS 授權

  CIFS授權為選用授權。只有在使用多重傳輸協定名稱對應時、才需要檢查Windows認證。在純UNIX的嚴格環境中、不需要這項功能。

- SVM

  您必須在系統上設定至少一個SVM。

- SVM上的DNS

  您必須在每個SVM上設定DNS。

- NFS 伺服器

  您必須在SVM上設定NFS。

- AES加密

  為了獲得最強大的安全性、您必須設定NFS伺服器、使其僅允許Kerberos使用AES-256加密。

- SMB 伺服器

  如果您執行的是多重傳輸協定環境、則必須在SVM上設定SMB。多重傳輸協定名稱對應需要SMB伺服器。

- 磁碟區

  您必須有根磁碟區和至少一個設定供SVM使用的資料磁碟區。

- 根Volume

  SVM的根Volume必須具有下列組態：

名稱	設定
安全風格	UNIX
UID	root或ID 0
Gid	root或ID 0
UNIX權限	7777

相較於根磁碟區、資料磁碟區可以有任一種安全樣式。

- UNIX 群組

  SVM必須設定下列UNIX群組：

群組名稱	群組**ID**
精靈	1.
根	0%
pcuser	65534（ONTAP 建立SVM時由SVM自動建立）

- UNIX 使用者

  SVM必須設定下列UNIX使用者：

使用者名稱	使用者**ID**	主要群組**ID**	留言
NFS	500	0%	GSS 初始化階段所需 NFS用戶端使用者的第一個使用者是使用者。
pcuser	65534	65534	NFS 和 CIFS 多重傳輸協定的使用需求 建立 SVM 時、由 ONTAP 自動建立並新增至 pcuser 群組。
根	0%	0%	安裝所需

  如果NFS用戶端使用者的SPN-UNIX名稱對應存在、則不需要NFS使用者。

- 匯出原則與規則

  您必須設定匯出原則、並針對根磁碟區、資料磁碟區和qtree設定必要的匯出規則。如果透過 Kerberos 存取 SVM 的所有磁碟區、您可以設定匯出規則選項 `-rorule`、 `-rwrule`和 `-superuser` 將根磁碟區移至 `krb5` 、 `krb5i`或 `krb5p`。

- Kerberos UNIX名稱對應

  如果您想讓NFS用戶端使用者的使用者具有root權限、您必須建立一個指向root的名稱對應。

相關資訊

"NetApp技術報告4073：安全統一化驗證"

"NetApp 互通性對照表工具"

"系統管理"

"邏輯儲存管理"

為 NFSv4 指定 ONTAP 使用者 ID 網域

若要指定使用者 ID 網域、您可以設定 `-v4-id-domain` 選項。

關於這項工作

根據預設ONTAP 、如果已設定NFSv4使用者ID對應、則使用NIS網域。如果未設定NIS網域、則會使用DNS網域。例如、如果您有多個使用者ID網域、則可能需要設定使用者ID網域。網域名稱必須符合網域控制器上的網域組態。NFSv3不需要此功能。

步驟

1. 輸入下列命令：

```
vserver nfs modify -vserver vserver_name -v4-id-domain NIS_domain_name
```

設定名稱服務

瞭解 ONTAP NFS 名稱服務交換器組態

ONTAP 會將名稱服務組態資訊儲存在相當於的表格中 `/etc/nsswitch.conf` UNIX 系統上的檔案。您必須瞭解表格的功能及ONTAP 其使用方式、以便根據環境適當設定。

這個名稱服務交換器表決定哪些名稱服務來源可以查詢、以便擷取特定類型名稱服務資訊的資訊。ONTAP ONTAP針對每個SVM維護個別的名稱服務交換器表。ONTAP

資料庫類型

此表格會針對下列每一種資料庫類型儲存個別的名稱服務清單：

資料庫類型	定義名稱服務來源：	有效來源為...
主機	將主機名稱轉換為IP位址	檔案、DNS
群組	查詢使用者群組資訊	檔案、NIS、LDAP
密碼	查詢使用者資訊	檔案、NIS、LDAP
網路群組	查詢netgroup資訊	檔案、NIS、LDAP
名稱	對應使用者名稱	檔案、LDAP

來源類型

這些來源會指定要用於擷取適當資訊的名稱服務來源。

指定來源類型...	若要查詢資訊...	由命令系列管理...

檔案	本機來源檔案	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在SVM的NIS網域組態中指定的外部NIS伺服器	`vserver services name-service nis-domain`
LDAP	在SVM的LDAP用戶端組態中指定的外部LDAP伺服器	`vserver services name-service ldap`
DNS	在SVM的DNS組態中指定的外部DNS伺服器	`vserver services name-service dns`

即使您計畫同時使用 NIS 或 LDAP 來進行資料存取和 SVM 管理驗證、您仍應納入 `files` 並將本機使用者設定為在 NIS 或 LDAP 驗證失敗時的後援。

用於存取外部來源的傳輸協定

若要存取伺服器的外部來源、ONTAP 可使用下列通訊協定：

外部名稱服務來源	用於存取的傳輸協定
NIS	UDP
DNS	UDP
LDAP	TCP

範例

下列範例顯示SVM SVM_1的名稱服務交換器組態：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

若要查詢主機的IP位址、ONTAP 請先查詢本機來源檔案。如果查詢未傳回任何結果、則會勾選DNS伺服器。

若要查詢使用者或群組資訊、ONTAP 僅查詢本機來源檔案。如果查詢未傳回任何結果、則查詢會失敗。

若要查詢netgroup資訊、ONTAP 請先諮詢外部NIS伺服器。如果查詢未傳回任何結果、則會勾選本機netgroup檔案。

SVM SVM_1的表格中沒有名稱對應的名稱服務項目。因此ONTAP 、根據預設、僅查詢本機來源檔案。

相關資訊

"NetApp技術報告4668：名稱服務最佳實務做法指南"

使用**LDAP**

了解適用於 **ONTAP NFS SVM** 的 **LDAP**

LDAP（輕量型目錄存取傳輸協定）伺服器可讓您集中維護使用者資訊。如果您將使用者資料庫儲存在環境中的LDAP伺服器上、您可以設定儲存系統、以便在現有的LDAP資料庫中查詢使用者資訊。

- 在設定LDAP ONTAP 以供使用之前、您應確認您的站台部署符合LDAP伺服器和用戶端組態的最佳實務做法。尤其必須符合下列條件：
  - LDAP伺服器的網域名稱必須符合LDAP用戶端上的項目。
  - LDAP伺服器支援的LDAP使用者密碼雜湊類型必須包含ONTAP 下列項目：
    - 加密（所有類型）和SHA-1（SHa、SSHA）。
    - 從ONTAP 《Sf9.8》、《SHA-2雜湊》（SHA-256、SSH-384、SHA-512、SSHA-256、 也支援SSHA-384和SSHA-512）。
  - 如果LDAP伺服器需要工作階段安全性措施、您必須在LDAP用戶端中進行設定。

    下列工作階段安全性選項可供使用：

    - LDAP簽署（提供資料完整性檢查）及LDAP簽署與密封（提供資料完整性檢查與加密）
    - 啟動TLS

- LDAPS（LDAP over TLS或SSL）

◦ 若要啟用已簽署和密封的LDAP查詢、必須設定下列服務：

- LDAP伺服器必須支援GSPI（Kerberos）SASL機制。
- LDAP伺服器必須在DNS伺服器上設定DNS A/AAAA記錄和PTr記錄。
- Kerberos伺服器必須在DNS伺服器上存在SRV.記錄。

◦ 若要啟用Start TLS或LDAPS、應考慮下列事項。

- 使用Start TLS而非LDAPS是NetApp最佳實務做法。
- 如果使用 LDAPS，則必須在ONTAP 9.5 及更高版本中為 TLS 或 SSL 啟用 LDAP 伺服器。 ONTAP 9.4 - 9.0 不支援 SSL。
- 必須已在網域中設定憑證伺服器。

◦ 若要啟用LDAP參照追蹤（ONTAP 在更新版本的版本中）、必須滿足下列條件：

- 這兩個網域都應設定下列其中一個信任關係：
  - 雙向
  - 單向、主要信任參照網域
  - 父-子
- DNS必須設定為解析所有參照的伺服器名稱。
- 網域密碼應相同、以在何時進行驗證 `--bind-as-cifs-server` 設為 true 。

> LDAP參照追蹤不支援下列組態。
>
> ◦ 所有ONTAP 版本：
> ◦ 管理SVM上的LDAP用戶端
> ◦ 適用於更新版本的支援功能（9.9.1及更新版本均支援）ONTAP ：
> ◦ LDAP 簽署與密封（ `-session-security` 選項）
> ◦ 加密 TLS 連線（ `-use-start-tls` 選項）
> ◦ 透過 LDAPS 連接埠 636 （ `-use-ldaps-for-ad-ldap` 選項）

- 從 ONTAP 9.11.1 開始，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證。"
- 在SVM上設定LDAP用戶端時、您必須輸入LDAP架構。

  在大多數情況下、預設ONTAP 的架構之一將是適當的。不過、如果您環境中的LDAP架構與這些架構不同、則必須先建立新的LDAP用戶端架構ONTAP 以供使用、才能建立LDAP用戶端。請洽詢您的LDAP管理員、瞭解您環境的需求。

- 不支援使用LDAP進行主機名稱解析。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

了解 **ONTAP NFS SVM** 的 **LDAP** 簽章和密封

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能

性管理功能。您必須在儲存虛擬機器（ SVM ）上設定 NFS 伺服器安全性設定、使其對應於 LDAP 伺服器上的設定。

簽署可確認LDAP有效負載資料使用秘密金鑰技術的完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。「*LDAP*安全性層級」選項會指出LDAP流量是否需要簽署、簽署及密封、或兩者皆不需要。預設值為 `none`。測試

在 SVM 上啟用 SMB 流量的 LDAP 簽署與密封功能 `-session-security-for-ad-ldap` 選項 `vserver cifs security modify` 命令。

了解適用於 **ONTAP NFS SVM** 的 **LDAPS**

您必須瞭ONTAP 解有關如何保護LDAP通訊的某些詞彙與概念。支援使用start TLS或LDAPS、在Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器之間設定驗證工作階段。ONTAP

術語

您應該瞭ONTAP 解某些詞彙、瞭解如何使用LDAPS來保護LDAP通訊安全。

- * LDAP *

  （輕量型目錄存取傳輸協定）一種用於存取和管理資訊目錄的傳輸協定。LDAP是用來儲存使用者、群組和網路群組等物件的資訊目錄。LDAP也提供目錄服務、可管理這些物件並滿足LDAP用戶端的LDAP要求。

- * SSL *

  （安全通訊端層）一種通訊協定、專為透過網際網路安全傳送資訊而開發。ONTAP 9 及更新版本支援 SSL 、但已不再採用 TLS 。

- * TLS *

  （傳輸層安全性）一種根據舊版SSL規格追蹤傳輸協定的IETF標準。這是SSL的後續版本。ONTAP 9.5 及更新版本支援 TLS 。

- * LDAPS（LDAP over SSL或TLS）*

  一種傳輸協定、使用TLS或SSL來保護LDAP用戶端與LDAP伺服器之間的通訊安全。術語 *LDAP over SSL* 和 *LDAP over TLS* 有時會互換使用。ONTAP 9.5 及更新版本支援 LDAPS 。

  - 在ONTAP 9.8-9.5 中，LDAPS 只能在連接埠 636 上啟用。為此，請使用 `-use-ldaps-for-ad-ldap`參數 `vserver cifs security modify`命令。
  - 從ONTAP 推出《支援支援支援支援服務的支援服務：支援服務器支援服務」、從功能支援服務的支援服務開始、您可以在任何連接埠上啟用LDAPS、但連接埠636仍為預設若要這麼做，請將參數設定 `-ldaps-enabled`為 `true`，並指定所需的 `-port`參數。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

  使用Start TLS而非LDAPS是NetApp最佳實務做法。

- 啟動**TLS**

（也稱為_start_tls_、_startTLs_和_StartTLS）一種機制、可透過TLS傳輸協定提供安全的通訊。

支援使用STARTTLS來保護LDAP通訊安全、並使用預設的LDAP連接埠（389）與LDAP伺服器通訊。ONTAPLDAP伺服器必須設定為允許透過LDAP連接埠389進行連線、否則SVM與LDAP伺服器之間的LDAP TLS連線將會失敗。

如何使用**LDAPS ONTAP**

支援TLS伺服器驗證、可讓SVM LDAP用戶端在連結作業期間確認LDAP伺服器的身分。ONTAP啟用TLS的LDAP用戶端可使用公開金鑰密碼編譯的標準技術、檢查伺服器的憑證和公開ID是否有效、以及是否已由用戶端信任CA清單中所列的憑證授權單位（CA）核發。

LDAP支援使用TLS加密通訊的ARTTLS。StartTLS會以純文字連線形式透過標準LDAP連接埠（389）開始、然後將該連線升級為TLS。

支援下列項目：ONTAP

- LDAPS用於Active Directory整合式LDAP伺服器與SVM之間的SMB相關流量
- LDAP流量的LDAPS、用於名稱對應和其他UNIX資訊

  Active Directory整合式LDAP伺服器或UNIX型LDAP伺服器均可用來儲存LDAP名稱對應和其他UNIX資訊的資訊、例如使用者、群組和網路群組。

- 自我簽署的根CA憑證

  使用Active Directory整合式LDAP時、會在網域中安裝Windows Server憑證服務時產生自我簽署的根憑證。使用UNIX LDAP伺服器進行LDAP名稱對應時、會使用適合該LDAP應用程式的方法、產生並儲存自我簽署的根憑證。

根據預設、LDAPS會停用。

為 **ONTAP NFS SVM** 啟用 **LDAP RFC2307bis** 支援

如果您想要使用LDAP並需要額外的功能來使用巢狀群組成員資格、您可以設定ONTAP 支援功能以啟用LDAP RFC2307bis。

開始之前

您必須已建立要使用的預設LDAP用戶端架構之一的複本。

關於這項工作

在LDAP用戶端架構中、群組物件使用memberUid屬性。此屬性可包含多個值、並列出屬於該群組的使用者名稱。在啟用RFC2307bis的LDAP用戶端架構中、群組物件會使用uniqueMember屬性。此屬性可包含LDAP目錄中其他物件的完整辨別名稱（DN）。這可讓您使用巢狀群組、因為群組可以有其他群組作為成員。

使用者不應是256個以上群組的成員、包括巢狀群組。不考慮超過256個群組限制的任何群組。ONTAP

根據預設、會停用RFC2307bis支援。

當ONTAP 使用MS -AD-BIS架構建立LDAP用戶端時、即可在功能上自動啟用RFC2307bis支援。

如需其他資訊、請參閱 "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 修改複製的RFC2307 LDAP用戶端架構、以啟用RFC2307bis支援：

   ```
   vserver services name-service ldap client schema modify -vserver vserver_name
   -schema schema-name -enable-rfc2307bis true
   ```

3. 修改架構以符合LDAP伺服器支援的物件類別：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -group-of-unique-names-object-class object_class
   ```

4. 修改架構以符合LDAP伺服器支援的屬性名稱：

   ```
   vserver services name-service ldap client schema modify -vserver vserver-name
   -schema schema_name -unique-member-attribute attribute_name
   ```

5. 返回管理權限層級：

   ```
   set -privilege admin
   ```

用於 **LDAP** 目錄搜尋的 **ONTAP NFS** 設定選項

您可以設定ONTAP 支援使用者、群組和netgroup資訊等方式、將LDAP用戶端設定為以最適合您環境的方式連線至LDAP伺服器、藉此最佳化LDAP目錄搜尋。您需要瞭解預設的LDAP基礎和範圍搜尋值何時足夠、以及指定自訂值何時更合適的參數。

使用者、群組和netgroup資訊的LDAP用戶端搜尋選項、有助於避免LDAP查詢失敗、進而避免用戶端無法存取儲存系統。它們也有助於確保搜尋作業盡可能有效率、以避免用戶端效能問題。

預設基礎和範圍搜尋值

LDAP基礎是LDAP用戶端用來執行LDAP查詢的預設基礎DN。所有搜尋、包括使用者、群組和網路群組搜尋、都是使用基礎DN來完成。當您的LDAP目錄相對較小、且所有相關項目都位於相同的DN中時、此選項是適當的。

如果未指定自訂基礎 DN 、則預設值為 `root`。這表示每個查詢都會搜尋整個目錄。雖然如此一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

LDAP基礎範圍是LDAP用戶端用來執行LDAP查詢的預設搜尋範圍。所有搜尋、包括使用者、群組和netgroup搜尋、都是使用基礎範圍來完成。它決定LDAP查詢只搜尋命名項目、DN下一層的項目、或DN下的整個子樹狀結構。

如果未指定自訂基礎範圍、則預設為 `subtree`。這表示每個查詢都會搜尋DN下方的整個子樹狀結構。雖然如此一來、LDAP查詢的成功機會就會最大化、但效率卻會降低、而且大型LDAP目錄的效能也會大幅降低。

自訂基礎和範圍搜尋值

您也可以為使用者、群組和netgroup搜尋指定個別的基礎和範圍值。以這種方式限制搜尋基礎和查詢範圍、可大幅提升效能、因為它會將搜尋範圍限制在LDAP目錄的較小子部分。

如果指定自訂基礎和範圍值、則會覆寫一般預設搜尋基礎和範圍、以供使用者、群組和netgroup搜尋。可在進階權限層級使用指定自訂基礎和範圍值的參數。

LDAP用戶端參數…	指定自訂…
`-base-dn`	所有 LDAP 搜尋的基準 DN。如果需要，可以輸入多個值（例如，如果在 ONTAP 9.5 及更高版本中啟用了 LDAP 引用追蹤）。
`-base-scope`	所有 LDAP 搜尋的基本範圍。
`-user-dn`	所有 LDAP 使用者搜尋的基本 DN。此參數也適用於使用者名稱映射搜尋。
`-user-scope`	所有 LDAP 使用者搜尋的基本範圍。此參數也適用於使用者名稱映射搜尋。
`-group-dn`	所有 LDAP 群組搜尋的基本 DN。
`-group-scope`	所有 LDAP 群組搜尋的基本範圍。
`-netgroup-dn`	所有 LDAP 網路群組搜尋的基本 DN。
`-netgroup-scope`	所有 LDAP 網路組搜尋的基本範圍。

多個自訂基礎**DN**值

如果您的LDAP目錄結構較為複雜、您可能需要指定多個基礎DNS、以搜尋LDAP目錄的多個部分以取得特定資訊。您可以為使用者、群組和netgroup DN參數指定多個DNS、方法是以分號（；）分隔這些DNS、並以雙引號（"）括住整個DN搜尋清單。如果DN包含分號、您必須在DN中的分號前面新增轉義字元（\）。

請注意、此範圍適用於為對應參數指定的整個DNS清單。例如、如果您為使用者範圍指定三個不同使用者DNS和子樹狀結構的清單、則LDAP使用者會搜尋三個指定DNS中的每個子樹狀結構。

從ONTAP 功能介紹9.5開始、您也可以指定LDAP _Referring Chasing _、以便ONTAP 在主要LDAP伺服器未傳回LDAP參照回應時、讓該支援功能可將查詢要求參照到其他LDAP伺服器。用戶端會使用該參照資料、從參照資料中所述的伺服器擷取目標物件。若要搜尋參照LDAP伺服器中的物件、可將參照物件的基礎DN新增至基礎DN、做為LDAP用戶端組態的一部分。不過、只有在啟用參照追蹤（使用 `-referral-enabled true` 選項）。

自訂 **LDAP** 搜尋篩選器

您可以使用 LDAP 組態選項參數來建立自訂搜尋篩選器。此 `-group-membership-filter`參數指定從 LDAP 伺服器查詢群組成員資格時所使用的搜尋篩選器。

有效篩選的範例包括：

```
(cn=*99), (cn=1*), (|(cn=*22)(cn=*33))
```

深入瞭解 "如何在 ONTAP 中設定 LDAP"。

提高 **ONTAP NFS SVM** 的 **LDAP** 目錄網路群組按主機搜尋的效能

如果您的LDAP環境已設定為允許依主機進行網路群組搜尋、您可以設定ONTAP 支援使用此功能的支援、並依主機執行網路群組搜尋。如此可大幅加快網路群組搜尋速度、並減少網路群組搜尋期間的延遲所導致的NFS用戶端存取問題。

開始之前

您的 LDAP 目錄必須包含 `netgroup.byhost` 地圖。

您的DNS伺服器應同時包含NFS用戶端的轉送（A）和反轉（PTr）查詢記錄。

當您在netGroups中指定IPv6位址時、必須一律縮短並壓縮RFC 5952中指定的每個位址。

關於這項工作

NIS 伺服器會將網路群組資訊儲存在三個不同的對應中、稱為 `netgroup`、 `netgroup.byuser`和 `netgroup.byhost`。的用途 `netgroup.byuser` 和 `netgroup.byhost` 地圖是為了加速網路群組搜尋。支援在NIS伺服器上執行各主機的網路群組搜尋、以縮短掛載回應時間。ONTAP

根據預設、 LDAP 目錄沒有這樣的 `netgroup.byhost` 對應 NIS 伺服器。不過、在協力廠商工具的協助下、可以匯入 NIS `netgroup.byhost` 映射到 LDAP 目錄以啓用逐主機快速 netgroup 搜索。如果您已將 LDAP 環境設定為允許逐主機網路群組搜尋、則可以使用來設定 ONTAP LDAP 用戶端 `netgroup.byhost` 對應名稱、 DN 和搜尋範圍、可更快速地逐主機搜尋 netgroup-by host 。

當ONTAP NFS用戶端要求存取匯出時、若能更快接收各主機的網路群組搜尋結果、則可讓支援者更快處理匯出規則。如此可降低網路群組搜尋延遲問題導致存取延遲的機率。

步驟

1. 取得確切完整的 NIS 辨別名稱 `netgroup.byhost` 將您匯入 LDAP 目錄的對應。

   對應DN可能會因您用於匯入的協力廠商工具而異。若要獲得最佳效能、您應該指定確切的對應DN。

2. 將權限層級設為進階： `set -privilege advanced`
3. 在儲存虛擬機器（ SVM ）的 LDAP 用戶端組態中、啟用逐主機網路群組搜尋： `vserver services name-service ldap client modify -vserver vserver_name -client-config config_name -is-netgroup-byhost-enabled true -netgroup-byhost-dn netgroup-by-host_map_distinguished_name -netgroup-byhost-scope netgroup-by-host_search_scope`

   `-is-netgroup-byhost-enabled {true false}` 啓用或禁用逐主機對 LDAP 目錄的 netgroup 搜索。預設值為 `false`。

   `-netgroup-byhost-dn netgroup-by-host_map_distinguished_name` 指定的辨別名稱 `netgroup.byhost` 在 LDAP 目錄中對應。它會覆寫基礎DN、以便依主機搜尋網路群組。如果您未指定此

參數、ONTAP 則使用基礎DN。

`-netgroup-byhost-scope {base|onelevel subtree}` 指定 netgroup-by host 搜尋的搜尋範圍。如果您未指定此參數、則預設值為 `subtree`。

如果 LDAP 用戶端組態尚不存在、您可以在使用建立新的 LDAP 用戶端組態時、指定這些參數來啟用逐主機網路群組搜尋 `vserver services name-service ldap client create` 命令。

> 這 `-ldap-servers`字段替換 `-servers`字段。您可以使用 `-ldap-servers`欄位指定 LDAP 伺服器的主機名稱或 IP 位址。

4. 返回管理權限層級： `set -privilege admin`

範例

下列命令會修改名為「 `LDAP_corp` 」的現有 LDAP 用戶端組態、以使用啟用逐主機網路群組搜尋 `netgroup.byhost` 名爲 "`nisMapName="netgroup.byhost" 、 DC=corp 、 DC=example 、 DC=com 的地圖和默認搜索範圍 `subtree`：

```
cluster1::*> vserver services name-service ldap client modify -vserver vs1
-client-config ldap_corp -is-netgroup-byhost-enabled true -netgroup-byhost
-dn nisMapName="netgroup.byhost",dc=corp,dc=example,dc=com
```

完成後

。 `netgroup.byhost` 和 `netgroup` 目錄中的地圖必須隨時保持同步、以避免用戶端存取問題。

相關資訊

"IETF RFC 5952：IPv6位址文字呈現的建議"

使用 **LDAP** 快速綁定對 **ONTAP NFS SVM** 進行 **nsswitch** 驗證

從SURF9.11.1開始ONTAP 、您可以利用LDAP _fast bind_Functionality（也稱為_並行 連結）、以更快、更簡單的用戶端驗證要求。若要使用此功能、LDAP伺服器必須支援快速連結功能。

關於這項工作

如果沒有快速連結、ONTAP 則使用LDAP Simple Bind來驗證LDAP伺服器的管理使用者。利用這種驗證方法、ONTAP 將使用者或群組名稱傳送至LDAP伺服器、接收儲存的雜湊密碼、並將伺服器雜湊代碼與本機使用者密碼產生的雜湊密碼進行比較。如果完全相同、ONTAP 則此功能會授予登入權限。

利用快速連結功能、ONTAP 透過安全連線、僅將使用者認證（使用者名稱和密碼）傳送至LDAP伺服器。然後LDAP伺服器會驗證這些認證資料、並指示ONTAP 資訊技術授予登入權限。

快速連結的優點之一是ONTAP 、不需要支援LDAP伺服器所支援的每一種新雜湊演算法、因為密碼雜湊是由LDAP伺服器執行。

"深入瞭解如何使用快速連結。"

您可以使用現有的LDAP用戶端組態進行LDAP快速連結。不過、強烈建議將LDAP用戶端設定為TLS或LDAPS、

否則密碼會以純文字透過線路傳送。

若要在ONTAP 整個環境中啟用LDAP快速連結、您必須滿足下列需求：

- 必須在支援快速連結的LDAP伺服器上設定支援使用者的支援。ONTAP
- 必須在名稱服務交換器（nsswitch）資料庫中設定LDAP的支援功能。ONTAP
- 必須使用FAST Bind設定NS交換 器驗證的使用者和群組帳戶。ONTAP

步驟

1. 請向LDAP管理員確認LDAP伺服器支援LDAP快速連結。
2. 確保ONTAP LDAP伺服器上已設定了這個使用者認證資料。
3. 確認已針對LDAP快速連結正確設定管理或資料SVM。

   a. 若要確認LDAP FAST Bind伺服器已列在LDAP用戶端組態中、請輸入：

      `vserver services name-service ldap client show`

      "瞭解LDAP用戶端組態。"

   b. 以確認 `ldap` 是 nsswitch 設定的來源之一 `passwd` 資料庫、輸入：

      `vserver services name-service ns-switch show`

   "深入瞭解nsswitch組態。"

4. 確保管理使用者正在使用nsswitch進行驗證、且其帳戶中已啟用LDAP快速連結驗證。

   ◦ 對於現有使用者、請輸入 `security login modify` 並驗證下列參數設定：

      `-authentication-method nsswitch`

      `-is-ldap-fastbind true`

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

   ◦ 對於新的管理員使用者，請參閱"啟用 LDAP 或 NIS ONTAP 帳戶存取"。

顯示 **ONTAP NFS SVM** 的 **LDAP** 統計資訊

您可以顯示儲存系統上的儲存虛擬機器 (SVM) 的 LDAP 統計訊息，以監控效能和診斷問題。

開始之前

- 您必須在SVM上設定LDAP用戶端。
- 您必須已識別可從中檢視資料的LDAP物件。

步驟

1. 檢視計數器物件的效能資料：

```
statistics show
```

範例

下列範例顯示計數器名稱為 **SMPL_1** 的範例統計資料： Avg_processor_busy 和 CPU_busy

```
cluster1::*> statistics start -object system -counter
avg_processor_busy|cpu_busy -sample-id smpl_1
Statistics collection is being started for Sample-id: smpl_1

cluster1::*> statistics stop -sample-id smpl_1
Statistics collection is being stopped for Sample-id: smpl_1

cluster1::*> statistics show -sample-id smpl_1
Object: system
Instance: cluster
Start-time: 8/2/2012 18:27:53
End-time: 8/2/2012 18:27:56
Cluster: cluster1
   Counter                                                     Value
   -------------------------------- --------------------------------
   avg_processor_busy                                             6%
   cpu_busy
```

相關資訊

- "統計數據顯示"
- "統計開始"
- "統計停止"

設定名稱對應

了解 **ONTAP NAS SVM** 的名稱對映配置

ONTAP 使用名稱對應將 SMB 身分識別對應至 UNIX 身分識別、將 Kerberos 身分識別對應至 UNIX 身分識別、以及將 UNIX 身分識別對應至 SMB 身分識別。無論是從 NFS 用戶端或 SMB 用戶端連線、 IT 都需要這些資訊來取得使用者認證、並提供適當的檔案存取。

您不需要使用名稱對應的情況有兩種例外：

- 您可以設定純 UNIX 環境、而不打算在磁碟區上使用 SMB 存取或 NTFS 安全樣式。
- 您可以設定要使用的預設使用者。

  在此案例中、不需要名稱對應、因為不會對應每個個別用戶端認證、而是將所有用戶端認證對應至相同的預設使用者。

請注意、您只能針對使用者使用名稱對應、而不能針對群組使用名稱對應。

不過、您可以將一組個別使用者對應至特定使用者。例如、您可以將開頭或結尾的所有AD使用者對應至特定UNIX使用者、以及使用者的UID。

了解 **ONTAP NAS SVM** 的名稱映射

當必須對應使用者的認證資料時、它會先檢查本機名稱對應資料庫和LDAP伺服器、以找出現有的對應。ONTAP無論是檢查一項或兩項、或是按SVM的名稱服務組態來決定順序。

- 適用於Windows至UNIX對應

  如果找不到對應、ONTAP 則此功能會檢查UNIX網域中的Windows使用者名稱是否為有效的使用者名稱。如果這不管用、它會使用預設的UNIX使用者、前提是已設定。如果未設定預設UNIX使用者、ONTAP 且無法以這種方式取得對應、則對應會失敗、並傳回錯誤。

- 適用於UNIX至Windows對應

  如果找不到對應、ONTAP 則嘗試尋找與SMB網域中UNIX名稱相符的Windows帳戶。如果這不管用、它會使用預設的SMB使用者、前提是已設定。如果預設的SMB使用者未設定、ONTAP 且無法以此方式取得對應、則對應會失敗、並傳回錯誤。

依預設、機器帳戶會對應至指定的預設UNIX使用者。如果未指定預設UNIX使用者、則機器帳戶對應會失敗。

- 從功能表9.5開始ONTAP 、您可以將機器帳戶對應至預設UNIX使用者以外的使用者。
- 在更新版本的版本中、您無法將機器帳戶對應到其他使用者。ONTAP

  即使已定義機器帳戶的名稱對應、也會忽略對應。

在 **ONTAP NAS SVM** 上進行多域搜尋以尋找 **UNIX** 到 **Windows** 使用者名稱映射

將UNIX使用者對應至Windows使用者時、支援多網域搜尋。ONTAP在傳回相符結果之前、會搜尋所有探索到的信任網域是否符合取代模式。或者、您也可以設定偏好的信任網域清單、以取代探索到的信任網域清單、並依序搜尋、直到傳回相符的結果為止。

網域信任如何影響**UNIX**使用者對**Windows**使用者名稱對應搜尋

若要瞭解多網域使用者名稱對應的運作方式、您必須瞭解網域信任如何搭配ONTAP 使用。Active Directory 與 SMB 伺服器主網域之間的信任關係可以是雙向信任、也可以是兩種單向信任類型之一、可以是傳入信任或傳出信任。主網域是 SVM 上 SMB 伺服器所屬的網域。

- 雙向信任

  透過雙向信任、這兩個網域彼此信任。如果 SMB 伺服器的主網域與其他網域具有雙向信任、則主網域可以驗證並授權屬於信任網域的使用者、反之亦然。

  UNIX使用者對Windows使用者名稱對應搜尋只能在主網域與其他網域之間具有雙向信任的網域上執行。

- 傳出信任_

  透過傳出信任、主網域信任其他網域。在此情況下、主網域可以驗證及授權屬於傳出信任網域的使用者。

執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域外傳信任的網域。

- 傳入信任_

  透過傳入信任、另一個網域會信任 SMB 伺服器的主網域。在此情況下、主網域無法驗證或授權屬於傳入信任網域的使用者。

  在執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域傳入信任的網域。

如何使用萬用字元（*）來設定多網域搜尋名稱對應

在Windows使用者名稱的網域區段中使用萬用字元、可協助進行多網域名稱對應搜尋。下表說明如何在名稱對應項目的網域部分使用萬用字元來啟用多網域搜尋：

模式	更換	結果
根	{星號} {反斜槓} {反斜槓} 管理員	UNIX使用者「root」會對應至名為「Administrator」的使用者。搜尋所有信任的網域、直到找到第一個相符的使用者「'Administrator」為止。
*	{星號} {反斜槓} {反斜槓} {星號}	有效的UNIX使用者會對應至對應的Windows使用者。會依序搜尋所有信任的網域、直到找到第一個與該名稱相符的使用者為止。 模式 {星號} {反斜槓} {反斜槓} {星號} 僅適用於從UNIX到Windows的名稱對應、而非其他方式。

執行多網域名稱搜尋的方式

您可以選擇兩種方法之一來決定用於多網域名稱搜尋的信任網域清單：

- 使用ONTAP 由資訊更新所編譯的自動探索雙向信任清單
- 使用您所編譯的慣用信任網域清單

如果UNIX使用者以萬用字元對應至使用者名稱的網域區段、則Windows使用者會在所有信任的網域中查詢、如下所示：

- 如果已設定慣用的信任網域清單、則對應的Windows使用者只會依序在搜尋清單中查詢。
- 如果未設定信任網域的慣用清單、則會在主網域的所有雙向信任網域中查詢Windows使用者。
- 如果主網域沒有雙向信任的網域、則會在主網域中查詢該使用者。

如果UNIX使用者對應至使用者名稱中沒有網域區段的Windows使用者、則會在主網域中查詢Windows使用者。

ONTAP NAS SVM 的名稱對映轉換規則

這個系統可為每個SVM保留一組轉換規則。ONTAP每個規則包含兩個部分：*Pattern_* 和*_replace*。轉換從適當清單的開頭開始、並根據第一個相符規則執行替代。模式是UNIX樣式的規則運算式。取代是包含轉義序列的字串、代表模式中的子運算式、如同 UNIX `sed` 方案。

為 ONTAP NAS SVM 建立名稱映射

您可以使用 `vserver name-mapping create` 建立名稱對應的命令。您可以使用名稱對應來讓Windows使用者存取UNIX安全樣式的磁碟區和相反的磁碟區。

關於這項工作

針對每個SVM、ONTAP 支援最多12、500個各個方向的名稱對應。

步驟

1. 建立名稱對應：

```
vserver name-mapping create -vserver vserver_name -direction {krb-unix|win-
unix|unix-win} -position integer -pattern text -replacement text
```

> ⓘ `-pattern`和 `-replacement`陳述式可做為規則運算式來表示。您也可以使用 `-replacement` null
> 置換字串（空格字元），使用陳述式明確拒絕對應至使用者 `" "`
> 。如link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["指令參考資料ONTAP"^]需詳細 `vserver name-mapping create`資訊，請參閱。

建立Windows對UNIX的對應時、ONTAP 在建立新對應時、任何與該系統有開放連線的SMB用戶端、都必須登出並重新登入、才能看到新的對應。

範例

下列命令會在名為VS1的SVM上建立名稱對應。對應是從UNIX到Windows的對應、位於優先順序清單中的位置1。對應會將UNIX使用者johnd對應至Windows使用者ENH\JohnDoe。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。對應是從Windows到UNIX的對應、位於優先順序清單中的位置1。這裏的模式和替換包括正則表達式。對應會將網域中的每個CIFS使用者對應到與SVM相關聯的LDAP網域中的使用者。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。在此模式中、Windows使用者名稱中的「$」元素必須轉義、對應會將Windows使用者ENH\ John$ops對應至UNIX使用者john_ops。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

為 **ONTAP NAS SVM** 配置預設用戶

您可以將預設使用者設定為在使用者的所有其他對應嘗試失敗時使用、或是不想在UNIX與Windows之間對應個別使用者時使用。或者、如果您想要驗證未對應的使用者失敗、則不應設定預設使用者。

關於這項工作

對於CIFS驗證、如果您不想將每個Windows使用者對應至個別的UNIX使用者、則可以改為指定預設的UNIX使用者。

對於NFS驗證、如果您不想將每個UNIX使用者對應至個別的Windows使用者、則可以改為指定預設的Windows使用者。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
設定預設UNIX使用者	`vserver cifs options modify -default-unix-user user_name`
設定預設的Windows使用者	`vserver nfs modify -default-win-user user_name`

用於管理 **NFS** 名稱對應的 **ONTAP** 命令

管理名稱對應時、會ONTAP 有特定的功能不全指令。

如果您想要...	使用此命令...
建立名稱對應	`vserver name-mapping create`
在特定位置插入名稱對應	`vserver name-mapping insert`

顯示名稱對應	`vserver name-mapping show`
交換兩個名稱對應的位置附註：當名稱對應設定為IP辨識符號項目時、不允許交換。	`vserver name-mapping swap`
修改名稱對應	`vserver name-mapping modify`
刪除名稱對應	`vserver name-mapping delete`
驗證正確的名稱對應	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

如"指令參考資料ONTAP"需詳細 `vserver name-mapping`資訊，請參閱。

為 **ONTAP SVM** 啟用 **Windows NFS** 用戶端的存取

支援從Windows NFSv3用戶端存取檔案。ONTAP這表示執行支援 NFSv3 之 Windows 作業系統的用戶端可以存取叢集上 NFSv3 匯出的檔案。若要成功使用此功能、您必須正確設定儲存虛擬機器（SVM）、並注意某些需求和限制。

關於這項工作

依照預設、Windows NFSv3用戶端支援會停用。

開始之前

必須在SVM上啟用NFSv3。

步驟

1. 啟用Windows NFSv3用戶端支援：

   ```
   vserver nfs modify -vserver svm_name -v3-ms-dos-client enabled -mount-rootonly disabled
   ```

2. 在所有支援 Windows NFSv3 用戶端的 SVM 上、停用 `-enable-ejukebox` 和 `-v3-connection-drop` 參數：

   ```
   vserver nfs modify -vserver vserver_name -enable-ejukebox false -v3-connection-drop disabled
   ```

   Windows NFSv3用戶端現在可以在儲存系統上掛載匯出。

3. 請指定、確保每個 Windows NFSv3 用戶端都使用硬掛載 `-o mtype=hard` 選項。

   這是確保可靠掛載的必要條件。

   ```
   mount -o mtype=hard \\10.53.33.10\vol\vol1 z:\
   ```

啟用 **ONTAP SVM** 的 **NFS** 用戶端上的匯出顯示

NFS 用戶端可以使用 `showmount -e` 命令以查看 ONTAP NFS 伺服器可用的匯出清單。這有助於使用者識別要掛載的檔案系統。

ONTAP預設允許 NFS 用戶端查看匯出清單。在舊版中， `showmount`**必須明確啟用命令選項** `vserver nfs modify`。若要檢視匯出清單、應在SVM上啟用NFSv3。

範例

下列命令顯示名為VS1的SVM上的showmount功能：

```
clusterl : : > vserver nfs show -vserver vs1 -fields showmount
vserver showmount
------- ---------
vs1     enabled
```

在NFS用戶端上執行的下列命令會顯示NFS伺服器上IP位址為10.63.21.9的匯出清單：

```
showmount -e 10.63.21.9
Export list for 10.63.21.9:
/unix         (everyone)
/unix/unixl   (everyone)
/unix/unix2   (everyone)
/             (everyone)
```

使用 **NFS** 管理檔案存取

為 **ONTAP SVM** 啟用或停用 **NFSv3**

您可以修改來啟用或停用 NFSv3 `-v3` 選項。這可讓使用 NFSv3 傳輸協定的用戶端存取檔案。依預設、NFSv3已啟用。

步驟

1. 執行下列其中一項動作：

如果您想要…	輸入命令…
啟用NFSv3	`vserver nfs modify -vserver vserver_name -v3 enabled`
停用 NFSv3	`vserver nfs modify -vserver vserver_name -v3 disabled`

為 **ONTAP SVM** 啟用或停用 **NFSv4.0**

您可以修改來啟用或停用 NFSv4.0 `-v4.0` 選項。這可讓使用NFSv4.0傳輸協定的用戶端存

取檔案。在更新版本中、NFSv4.0預設為啟用；在舊版中、預設為停用。ONTAP

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 enabled`
停用NFSv4.0	`vserver nfs modify -vserver vserver_name -v4.0 disabled`

為 **ONTAP SVM** 啟用或停用 **NFSv4.1**

您可以修改來啟用或停用 NFSv4.1 `-v4.1` 選項。這可讓使用 NFSv4.1 傳輸協定的用戶端存取檔案。在 ONTAP 9.9.1 中、預設會啟用 NFSv4.1 ；在舊版中、預設會停用 NFSv4.1 。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 enabled`
停用 NFSv4.1	`vserver nfs modify -vserver vserver_name -v4.1 disabled`

管理 **ONTAP NFSv4** 儲存池限制

從 ONTAP 9.13 開始、系統管理員可以讓 NFSv4 伺服器在達到每個用戶端儲存資源限制時、拒絕資源給 NFSv4 用戶端。當用戶端使用過多的 NFSv4 儲存工具資源時、這可能會導致其他 NFSv4 用戶端因為 NFSv4 儲存工具資源無法使用而遭到封鎖。

啟用此功能也可讓客戶檢視每個用戶端的作用中 storepool 資源使用量。如此一來、就能更輕鬆地識別耗盡系統資源的用戶端、並使每個用戶端的資源限制得以實施。

檢視已使用的 **storepool** 資源

。 `vserver nfs storepool show` 命令會顯示使用的 storepool 資源數量。storepool 是 NFSv4 用戶端所使用的資源集區。

步驟

1. 以系統管理員身分執行 `vserver nfs storepool show` 命令顯示 NFSv4 用戶端的 storepool 資訊。

範例

此範例顯示 NFSv4 用戶端的 storepool 資訊。

```
cluster1::*> vserver nfs storepool show

Node: node1

Vserver: vs1

Data-Ip: 10.0.1.1

Client-Ip Protocol IsTrunked OwnerCount OpenCount DelegCount LockCount

-------------- --------- --------- ---------- ---------- ----------
---------

10.0.2.1          nfs4.1     true    2 1 0 4

10.0.2.2          nfs4.2     true    2 1 0 4

2 entries were displayed.
```

啟用或停用 **storepool** 限制控制項

系統管理員可以使用下列命令來啟用或停用 storepool 限制控制項。

步驟

1. 身為管理員、請執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用 storepool 限制控制	`vserver nfs storepool config modify -limit-enforce enabled`
停用 storepool 限制控制項	`vserver nfs storepool config modify -limit-enforce disabled`

檢視封鎖的用戶端清單

如果已啟用 storepool 限制、則系統管理員可以查看哪些用戶端在達到其每個用戶端資源臨界值時遭到封鎖。系統管理員可以使用下列命令來查看哪些用戶端已標示為封鎖用戶端。

步驟

1. 使用 `vserver nfs storepool blocked-client show` 顯示 NFSv4 封鎖用戶端清單的命令。

達到其每個用戶端臨界值的用戶端將會中斷連線、並新增至區塊用戶端快取。系統管理員可以使用下列命令、從區塊用戶端快取中移除用戶端。這將允許用戶端連線至 ONTAP NFSv4 伺服器。

步驟

1. 使用 `vserver nfs storepool blocked-client flush -client-ip <ip address>` 用於清除 storepool 封鎖用戶端快取的命令。
2. 使用 `vserver nfs storepool blocked-client show` 用於驗證用戶端已從區塊用戶端快取移除的命令。

範例

此範例顯示封鎖的用戶端、其 IP 位址為 "10.2.1.1 " 、正在從所有節點中清除。

```
cluster1::*>vserver nfs storepool blocked-client flush -client-ip 10.2.1.1

cluster1::*>vserver nfs storepool blocked-client show

Node: node1

Client IP
----------
10.1.1.1

1 entries were displayed.
```

為 **ONTAP SVM** 啟用或停用 **pNFS**

pNFS可讓NFS用戶端直接並平行地在儲存裝置上執行讀寫作業、藉此改善效能、避免NFS伺服器成為潛在的瓶頸。若要啟用或停用 pNFS （平行 NFS ）、您可以修改 `-v4.1 -pnfs` 選項。

如果**ONTAP** 這個版本是...	**pNFS**預設為...
9.8 或更新版本	已停用
9.7 或更早版本	已啟用

開始之前

需要NFSv4.1支援才能使用pNFS。

如果您要啟用pNFS、必須先停用NFS參照。兩者無法同時啟用。

如果您在SVM上使用pNFS搭配Kerberos、則必須在SVM上的每個LIF上啟用Kerberos。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs enabled`
停用pNFS	`vserver nfs modify -vserver vserver_name -v4.1-pnfs disabled`

相關資訊

- NFS 主幹總覽

控制 ONTAP SVM 透過 TCP 和 UDP 進行的 NFS 訪問

您可以透過修改來啟用或停用透過 TCP 和 UDP 對儲存虛擬機器（ SVM ）的 NFS 存取 `-tcp` 和 `-udp` 參數。這可讓您控制NFS用戶端是否能在您的環境中透過TCP或UDP存取資料。

關於這項工作

這些參數僅適用於NFS。它們不會影響輔助通訊協定。例如、如果停用NFS over TCP、則透過TCP掛載作業仍會成功。若要完全封鎖TCP或UDP流量、您可以使用匯出原則規則。

> 在停用TCP for NFS之前、您必須先關閉SnapDiff RPC伺服器、以免發生命令故障的錯誤。您可以使用命令停用 TCP `vserver snapdiff-rpc-server off -vserver vserver name`。

步驟

1. 執行下列其中一項動作：

如果您想要NFS存取...	輸入命令...
透過TCP啟用	`vserver nfs modify -vserver vserver_name -tcp enabled`
已透過TCP停用	`vserver nfs modify -vserver vserver_name -tcp disabled`
已透過udp啟用	`vserver nfs modify -vserver vserver_name -udp enabled`
已透過udp停用	`vserver nfs modify -vserver vserver_name -udp disabled`

控制來自 ONTAP SVM 非保留埠的 NFS 請求

您可以啟用來拒絕來自非保留連接埠的 NFS 掛載要求 `-mount-rootonly` 選項。若要拒絕來自非保留連接埠的所有 NFS 要求、您可以啟用 `-nfs-rootonly` 選項。

關於這項工作

依預設、選項 `-mount-rootonly` 是 `enabled`。

依預設、選項 `-nfs-rootonly` 是 `disabled`。

這些選項不適用於空程序。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
允許來自非保留連接埠的NFS掛載要求	`vserver nfs modify -vserver vserver_name -mount -rootonly disabled`
拒絕來自非保留連接埠的NFS掛載要求	`vserver nfs modify -vserver vserver_name -mount -rootonly enabled`
允許來自非保留連接埠的所有NFS要求	`vserver nfs modify -vserver vserver_name -nfs -rootonly disabled`
拒絕來自非保留連接埠的所有NFS要求	`vserver nfs modify -vserver vserver_name -nfs -rootonly enabled`

處理未知 **UNIX** 使用者對 **ONTAP NTFS** 磁碟區或 **qtree** 的 **NFS** 訪問

如果ONTAP 無法識別嘗試連線至NTFS安全樣式之磁碟區或qtree的UNIX使用者、就無法將使用者明確對應至Windows使用者。您可以設定ONTAP 支援不允許存取此類使用者以獲得更嚴格的安全性、或將其對應至預設的Windows使用者、以確保所有使用者都能享有最低的存取層級。

開始之前

若要啟用此選項、必須設定預設的Windows使用者。

關於這項工作

如果UNIX使用者嘗試存取NTFS安全樣式的磁碟區或qtree、則必須先將UNIX使用者對應至Windows使用者、ONTAP 才能讓支援者正確評估NTFS權限。但是ONTAP 、如果無法在已設定的使用者資訊名稱服務來源中查詢UNIX使用者的名稱、就無法明確地將UNIX使用者對應至特定的Windows使用者。您可以決定如何以下列方式處理這類未知的UNIX使用者：

- 拒絕未知UNIX使用者的存取。

  如此一來、所有UNIX使用者都需要明確對應、才能存取NTFS磁碟區或qtree、進而加強更嚴格的安全性。

- 將未知的UNIX使用者對應至預設的Windows使用者。

  如此可確保所有使用者透過預設的Windows使用者、獲得對NTFS磁碟區或qtree的最低存取層級、進而降低安全性、但更為便利。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想讓未知UNIX使用者使用預設的Windows使用者…	輸入命令…
已啟用	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user enabled`
已停用	`vserver nfs modify -vserver vserver_name -map -unknown-uid-to-default-windows-user disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

在非保留連接埠上掛載 **ONTAP NFS** 匯出的用戶端的注意事項

。 `-mount-rootonly` 必須在必須支援用戶端的儲存系統上停用此選項、即使使用者以 root 登入、也能使用非保留連接埠來掛載 NFS 匯出。這類用戶端包括HummingBird用戶端和Solaris NFS/IPv6用戶端。

如果是 `-mount-rootonly` 此選項已啟用、 ONTAP 不允許使用非保留連接埠的 NFS 用戶端（亦即數字大於 1,023 的連接埠）掛載 NFS 匯出。

透過驗證 **ONTAP NFS SVM** 的網域來對網路群組執行更嚴格的存取檢查

根據預設、ONTAP 在評估網路群組的用戶端存取時、會執行額外的驗證。額外檢查可確保用戶端的網域符合儲存虛擬機器（SVM）的網域組態。否則ONTAP 、不允許用戶端存取。

關於這項工作

當針對用戶端存取評估匯出原則規則、且匯出原則規則包含netgroup時ONTAP 、必須判斷用戶端的IP位址是否屬於netgroup。ONTAP為此目的、ONTAP 將用戶端的IP位址轉換成使用DNS的主機名稱、並取得完整網域名稱（FQDN）。

如果netgroup檔案只列出主機的簡短名稱、而且主機的簡短名稱存在於多個網域中、則不同網域的用戶端可以在不進行此檢查的情況下取得存取權。

為了避免這種情況ONTAP 、此功能會將從DNS傳回的主機網域、與針對SVM設定的DNS網域名稱清單進行比較。如果符合、則允許存取。如果不相符、則會拒絕存取。

此驗證預設為啟用。您可以修改來管理 `-netgroup-dns-domain-search` 參數、可在進階權限層級使用。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 執行所需的動作：

如果您希望網路群組的網域驗證...	輸入...
已啟用	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search enabled`
已停用	`vserver nfs modify -vserver vserver_name -netgroup-dns-domain -search disabled`

3. 將權限等級設為admin：

```
set -privilege admin
```

修改 **ONTAP SVM** 的 **NFSv3** 服務所使用的連接埠

儲存系統上的NFS伺服器會使用掛載精靈和網路鎖定管理程式等服務、透過特定的預設網路連接埠與NFS用戶端進行通訊。在大多數NFS環境中、預設連接埠都能正常運作、不需要修改、但如果您想在NFSv3環境中使用不同的NFS網路連接埠、您可以這麼做。

開始之前

變更儲存系統上的NFS連接埠需要所有NFS用戶端重新連線至系統、因此您應該在變更前先將此資訊傳達給使用者。

關於這項工作

您可以為每個儲存虛擬機器（SVM）設定NFS掛載精靈、網路鎖定管理程式、網路狀態監視器和NFS配額精靈服務所使用的連接埠。連接埠號碼變更會影響透過TCP和udp存取資料的NFS用戶端。

NFSv4和NFSv4.1的連接埠無法變更。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 停用NFS存取：

```
vserver nfs modify -vserver vserver_name -access false
```

3. 設定特定NFS服務的NFS連接埠：

```
vserver nfs modify -vserver vserver_namenfs_port_parameterport_number
```

NFS連接埠參數	說明	預設連接埠
`-mountd-port`	NFS掛載精靈	635
`-nlm-port`	網路鎖定管理程式	4045
`-nsm-port`	網路狀態監視器	4046
`-rquotad-port`	NFS配額精靈	4049

除了預設連接埠之外、允許的連接埠號碼範圍為1024到65535.每個NFS服務都必須使用唯一的連接埠。

4. 啟用NFS存取：

   ```
   vserver nfs modify -vserver vserver_name -access true
   ```

5. 使用 `network connections listening show` 用於驗證連接埠號碼變更的命令。

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

6. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

下列命令會將SVM上名為VS1的NFS掛載Daemon連接埠設為1113：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -access false

vs1::*> vserver nfs modify -vserver vs1 -mountd-port 1113

vs1::*> vserver nfs modify -vserver vs1 -access true

vs1::*> network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: cluster1-01
Cluster          cluster1-01_clus_1:7700          TCP/ctlopcp
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:1113                       TCP/mount
vs1              data1:1113                       UDP/mount
...
vs1::*> set -privilege admin
```

用於管理 **NFS** 伺服器的 **ONTAP** 命令

管理ONTAP NFS伺服器時、會有特定的功能不一的指令。

如果您想要...	使用此命令...
建立NFS伺服器	`vserver nfs create`
顯示NFS伺服器	`vserver nfs show`
修改NFS伺服器	`vserver nfs modify`
刪除NFS伺服器	`vserver nfs delete`

隱藏 `.snapshot` NFSv3 掛載點下的目錄列表 明確存取 `.snapshot` 即使已啟用此選項、仍會允許目錄。	`vserver nfs` 的命令 `-v3-hide-snapshot` 選項已啟用

如"指令參考資料ONTAP"需詳細 `vserver nfs`資訊，請參閱。

解決 **ONTAP NAS SVM** 的名稱服務問題

當用戶端因為名稱服務問題而發生存取失敗時、您可以使用 `vserver services name-service getxxbyyy` 命令系列可手動執行各種名稱服務查詢、並檢查查詢的詳細資料和結果、以協助進行疑難排解。

關於這項工作

- 您可以針對每個命令指定下列項目：
  - 執行查詢的節點或儲存虛擬機器（SVM）名稱。

    這可讓您測試特定節點或SVM的名稱服務查詢、以縮小搜尋名稱服務組態問題的範圍。

  - 是否顯示用於查詢的來源。

    這可讓您檢查是否使用了正確的來源。

- 根據設定的名稱服務交換器訂單、選擇執行查詢的服務。ONTAP
- 這些命令可在進階權限層級使用。

步驟

1. 執行下列其中一項動作：

若要擷取...	使用命令...
主機名稱的IP位址	`vserver services name-service getxxbyyy getaddrinfo vserver services name-service getxxbyyy gethostbyname` （僅限IPv4 位址）
依群組ID的群組成員	`vserver services name-service getxxbyyy getgrbygid`
群組成員（依群組名稱）	`vserver services name-service getxxbyyy getgrbyname`
使用者所屬的群組清單	`vserver services name-service getxxbyyy getgrlist`

IP位址的主機名稱	`vserver services name-service getxxbyyy getnameinfo vserver services name-service getxxbyyy gethostbyaddr` （僅限IPv4 位址）
使用者名稱的使用者資訊	`vserver services name-service getxxbyyy getpwbyname` 您可以指定來測試 RBAC 使用者的名稱解析 `-use-rbac` 參數為 `true`。
使用者ID的使用者資訊	`vserver services name-service getxxbyyy getpwbyuid` 您可以指定來測試 RBAC 使用者的名稱解析 `-use-rbac` 參數為 `true`。
用戶端的網路群組成員資格	`vserver services name-service getxxbyyy netgrp`
使用netgroup by host搜尋的用戶端網路群組成員資格	`vserver services name-service getxxbyyy netgrpbyhost`

下列範例顯示SVM VS1的DNS查詢測試、嘗試取得主機acast1.eng.example.com的IP位址：

```
cluster1::*> vserver services name-service getxxbyyy getaddrinfo -vserver
vs1 -hostname acast1.eng.example.com -address-family all -show-source true
Source used for lookup: DNS
Host name: acast1.eng.example.com
Canonical Name: acast1.eng.example.com
IPv4: 10.72.8.29
```

下列範例顯示SVM VS1的NIS查詢測試、嘗試擷取使用者的UID 501768使用者資訊：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyuid -vserver
vs1 -userID 501768 -show-source true
Source used for lookup: NIS
pw_name: jsmith
pw_passwd: $1$y8rA4XX7$/DDOXAvc2PC/IsNFozfIN0
pw_uid: 501768
pw_gid: 501768
pw_gecos:
pw_dir: /home/jsmith
pw_shell: /bin/bash
```

下列範例顯示SVM VS1的LDAP查詢測試、嘗試擷取名稱為LDAP1之使用者的使用者資訊：

```
cluster1::*> vserver services name-service getxxbyyy getpwbyname -vserver
vs1 -username ldap1 -use-rbac false -show-source true
Source used for lookup: LDAP
pw_name: ldap1
pw_passwd: {crypt}JSPM6yc/ilIX6
pw_uid: 10001
pw_gid: 3333
pw_gecos: ldap1 user
pw_dir: /u/ldap1
pw_shell: /bin/csh
```

下列範例顯示SVM VS1的網路群組查詢測試、嘗試找出用戶端dnshost0是否為netgroup lnetgroup 136的成員：

```
cluster1::*> vserver services name-service getxxbyyy netgrp -vserver vs1
-netgroup lnetgroup136 -client dnshost0 -show-source true
Source used for lookup: LDAP
dnshost0 is a member of lnetgroup136
```

1. 分析您執行的測試結果、並採取必要行動。

如果...	請查看...
主機名稱或IP位址查詢失敗或產生不正確的結果	DNS 組態
查詢查詢的來源不正確	名稱服務交換器組態
使用者或群組查詢失敗或產生不正確的結果	• 名稱服務交換器組態 • 來源組態（本機檔案、 NIS 網域、 LDAP 用戶端） • 網路組態（例如、LIF和Routes）
主機名稱查詢失敗或逾時、而且DNS伺服器不會解析DNS短名稱（例如host1）	頂層網域（頂級域）查詢的DNS組態。您可以使用停用 TLD 查詢 `-is-tld-query-enabled false` 選項 `vserver services name-service dns modify` 命令。

相關資訊

"NetApp技術報告4668：名稱服務最佳實務做法指南"

驗證 **ONTAP NAS SVM** 的名稱服務連接

您可以檢查 DNS 和輕量級目錄存取協定 (LDAP) 名稱伺服器以驗證它們是否已連接到ONTAP。這些命令可在管理權限層級使用。

關於這項工作

您可以使用名稱服務組態檢查程式、視需要檢查有效的DNS或LDAP名稱服務組態。此驗證檢查可在命令列或系統管理員中啟動。

對於DNS組態、所有伺服器均已經過測試、需要進行設定才能視為有效。對於LDAP組態、只要任何伺服器都已啟動、組態就會生效。名稱服務命令會套用組態檢查程式、除非是 `skip-config-validation` 欄位為 true （預設為 false ）。

步驟

1. 使用適當的命令來檢查名稱服務組態。UI會顯示已設定伺服器的狀態。

若要檢查…	使用此命令…
DNS組態狀態	`vserver services name-service dns check`
LDAP 組態狀態	`vserver services name-service ldap check`

```
cluster1::> vserver services name-service dns check -vserver vs0

Vserver         Name Server     Status  Status Details
--------------  --------------- ------- -------------------------
 vs0            10.11.12.13     up      Response time (msec): 55
 vs0            10.11.12.14     up      Response time (msec): 70
 vs0            10.11.12.15     down    Connection refused.
+-------------------------------------------------------------+
```

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                |
| Client Configuration Name: c1                               |
| LDAP Status: up                                             |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                              |
```

如果至少有一部已設定的伺服器（名稱伺服器/ LDAP伺服器）可連線並提供服務、則組態驗證會成功。如果部分伺服器無法連線、則會顯示警告。

用於管理 **NAS** 名稱服務交換器條目的 **ONTAP** 命令

您可以透過建立、顯示、修改及刪除名稱服務交換器項目來管理這些項目。

如果您想要…	使用此命令…

建立名稱服務交換器項目	`vserver services name-service ns-switch create`
顯示名稱服務交換器項目	`vserver services name-service ns-switch show`
修改名稱服務交換器項目	`vserver services name-service ns-switch modify`
刪除名稱服務交換器項目	`vserver services name-service ns-switch delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch`資訊，請參閱。

相關資訊

"NetApp技術報告4668：名稱服務最佳實務做法指南"

用於管理 **NAS** 名稱服務快取的 **ONTAP** 命令

您可以修改存留時間（TTL）值來管理名稱服務快取。TTL值決定名稱服務資訊在快取中持續存在的時間長度。

如果您要修改下列項目的TTL值：	使用此命令...
UNIX使用者	`vserver services name-service cache unix-user settings`
UNIX群組	`vserver services name-service cache unix-group settings`
UNIX網路群組	`vserver services name-service cache netgroups settings`
主機	`vserver services name-service cache hosts settings`
群組成員資格	`vserver services name-service cache group-membership settings`

相關資訊

"指令參考資料ONTAP"

用於管理 **NFS** 名稱對應的 **ONTAP** 命令

管理名稱對應時、會ONTAP 有特定的功能不全指令。

如果您想要...	使用此命令...
建立名稱對應	`vserver name-mapping create`

在特定位置插入名稱對應	`vserver name-mapping insert`
顯示名稱對應	`vserver name-mapping show`
交換兩個名稱對應的位置附註：當名稱對應設定為IP辨識符號項目時、不允許交換。	`vserver name-mapping swap`
修改名稱對應	`vserver name-mapping modify`
刪除名稱對應	`vserver name-mapping delete`
驗證正確的名稱對應	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

如"指令參考資料ONTAP"需詳細 `vserver name-mapping`資訊，請參閱。

用於管理 **NAS** 本機 **UNIX** 使用者的 **ONTAP** 指令

有特定ONTAP 的功能可用來管理本機UNIX使用者。

如果您想要...	使用此命令...
建立本機UNIX使用者	`vserver services name-service unix-user create`
從URI載入本機UNIX使用者	`vserver services name-service unix-user load-from-uri`
顯示本機UNIX使用者	`vserver services name-service unix-user show`
修改本機UNIX使用者	`vserver services name-service unix-user modify`
刪除本機UNIX使用者	`vserver services name-service unix-user delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-user`資訊，請參閱。

用於管理 **NAS** 本機 **UNIX** 群組的 **ONTAP** 指令

管理本機UNIX群組時、會ONTAP 有特定的指令檔。

如果您想要...	使用此命令...
建立本機UNIX群組	`vserver services name-service unix-group create`

新增使用者至本機UNIX群組	`vserver services name-service unix-group adduser`
從URI載入本機UNIX群組	`vserver services name-service unix-group load-from-uri`
顯示本機UNIX群組	`vserver services name-service unix-group show`
修改本機UNIX群組	`vserver services name-service unix-group modify`
從本機UNIX群組刪除使用者	`vserver services name-service unix-group deluser`
刪除本機UNIX群組	`vserver services name-service unix-group delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service unix-group`資訊，請參閱。

ONTAP NFS SVM 的本機 **UNIX** 使用者、群組和群組成員限制

介紹叢集中UNIX使用者和群組的最大數量限制、以及管理這些限制的命令。ONTAP這些限制可防止系統管理員在叢集中建立過多的本機UNIX使用者和群組、有助於避免效能問題。

本機UNIX使用者群組和群組成員的總數有限制。本機UNIX使用者有不同的限制。限制是整個叢集的。每個新限制都會設定為預設值、您最多可以修改為預先指派的硬限制。

資料庫	預設限制	硬限制
本機UNIX使用者	32、768	65,536
本機UNIX群組和群組成員	32、768	65,536

管理 **ONTAP NFS SVM** 的本機 **UNIX** 使用者和群組的限制

我們提供特定ONTAP 的指令來管理本機UNIX使用者和群組的限制。叢集管理員可以使用這些命令來疑難排解叢集內的效能問題、這些問題被認為與大量的本機UNIX使用者和群組有關。

關於這項工作

叢集管理員可在進階權限層級使用這些命令。

步驟

1. 執行下列其中一項動作：

如果您想要...	使用命令...
顯示本機UNIX使用者限制的相關資訊	`vserver services unix-user max-limit show`
顯示本機UNIX群組限制的相關資訊	`vserver services unix-group max-limit show`
修改本機UNIX使用者限制	`vserver services unix-user max-limit modify`
修改本機UNIX群組限制	`vserver services unix-group max-limit modify`

如"指令參考資料ONTAP"需詳細 `vserver services unix`資訊，請參閱。

用於管理 **NFS** 本機網路群組的 **ONTAP** 命令

您可以從URI載入本機網路群組、驗證節點的狀態、顯示及刪除它們、藉此管理本機網路群組。

如果您想要...	使用命令...
從URI載入網路群組	`vserver services name-service netgroup load`
驗證各節點的網路群組狀態	`vserver services name-service netgroup status` 可在進階權限層級或更高層級使用。
顯示本機網路群組	`vserver services name-service netgroup file show`
刪除本機網路群組	`vserver services name-service netgroup file delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service netgroup file`資訊，請參閱。

用於管理 **NFS NIS** 網域配置的 **ONTAP** 命令

管理ONTAP NIS網域組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
建立NIS網域組態	`vserver services name-service nis-domain create`
顯示 NIS 網域組態	`vserver services name-service nis-domain show`

顯示NIS網域組態的繫結狀態	`vserver services name-service nis-domain show-bound`
顯示 NIS 統計資料	`vserver services name-service nis-domain show-statistics` 可在進階權限層級或更高層級使用。
清除NIS統計資料	`vserver services name-service nis-domain clear-statistics` 可在進階權限層級或更高層級使用。
修改NIS網域組態	`vserver services name-service nis-domain modify`
刪除NIS網域組態	`vserver services name-service nis-domain delete`
啟用網路群組各主機搜尋的快取	`vserver services name-service nis-domain netgroup-database config modify` 可在進階權限層級或更高層級使用。

如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain`資訊，請參閱。

用於管理 **NFS LDAP** 用戶端設定的 **ONTAP** 命令

有特定ONTAP 的功能可用來管理LDAP用戶端組態。

SVM管理員無法修改或刪除由叢集管理員所建立的LDAP用戶端組態。

如果您想要…	使用此命令…
建立LDAP用戶端組態	`vserver services name-service ldap client create`
顯示LDAP用戶端組態	`vserver services name-service ldap client show`
修改LDAP用戶端組態	`vserver services name-service ldap client modify`
變更LDAP用戶端的BIND密碼	`vserver services name-service ldap client modify-bind-password`
刪除LDAP用戶端組態	`vserver services name-service ldap client delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client`資訊，請參閱。

用於管理 **NFS LDAP** 配置的 **ONTAP** 命令

有特定ONTAP 的功能可用來管理LDAP組態。

如果您想要…	使用此命令…

建立LDAP組態	`vserver services name-service ldap create`
顯示LDAP組態	`vserver services name-service ldap show`
修改LDAP組態	`vserver services name-service ldap modify`
刪除LDAP組態	`vserver services name-service ldap delete`

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap`資訊，請參閱。

用於管理 **NFS LDAP** 用戶端架構模板的 **ONTAP** 命令

管理ONTAP LDAP用戶端架構範本時、會有特定的支援功能指令。

SVM管理員無法修改或刪除由叢集管理員所建立的LDAP用戶端架構。

如果您想要...	使用此命令...
複製現有的LDAP架構範本	`vserver services name-service ldap client schema copy` 可在進階權限層級或更高層級使用。
顯示LDAP架構範本	`vserver services name-service ldap client schema show`
修改LDAP架構範本	`vserver services name-service ldap client schema modify` 可在進階權限層級或更高層級使用。
刪除LDAP架構範本	`vserver services name-service ldap client schema delete` 可在進階權限層級或更高層級使用。

如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client schema`資訊，請參閱。

用於管理 **NFS Kerberos** 介面設定的 **ONTAP** 命令

管理ONTAP NFS Kerberos介面組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
在LIF上啟用NFS Kerberos	`vserver nfs kerberos interface enable`
顯示NFS Kerberos介面組態	`vserver nfs kerberos interface show`
修改NFS Kerberos介面組態	`vserver nfs kerberos interface modify`

停用LIF上的NFS Kerberos	`vserver nfs kerberos interface disable`

如"指令參考資料ONTAP"需詳細 `vserver nfs kerberos interface`資訊，請參閱。

用於管理 **NFS Kerberos** 領域配置的 **ONTAP** 命令

管理ONTAP NFS Kerberos領域組態時、會有特定的功能不完整的指令。

如果您想要...	使用此命令...
建立NFS Kerberos領域組態	`vserver nfs kerberos realm create`
顯示NFS Kerberos領域組態	`vserver nfs kerberos realm show`
修改NFS Kerberos領域組態	`vserver nfs kerberos realm modify`
刪除NFS Kerberos領域組態	`vserver nfs kerberos realm delete`

如"指令參考資料ONTAP"需詳細 `vserver nfs kerberos realm`資訊，請參閱。

用於管理匯出策略的 **ONTAP** 命令

管理匯出原則時、會ONTAP 有特定的指令。

如果您想要...	使用此命令...
顯示匯出原則的相關資訊	`vserver export-policy show`
重新命名匯出原則	`vserver export-policy rename`
複製匯出原則	`vserver export-policy copy`
刪除匯出原則	`vserver export-policy delete`

如"指令參考資料ONTAP"需詳細 `vserver export-policy`資訊，請參閱。

用於管理匯出規則的 **ONTAP** 命令

管理匯出規則時、會ONTAP 有一些特定的指令。

如果您想要...	使用此命令...
建立匯出規則	`vserver export-policy rule create`

顯示匯出規則的相關資訊	`vserver export-policy rule show`
修改匯出規則	`vserver export-policy rule modify`
刪除匯出規則	`vserver export-policy rule delete`

如果您已設定多個符合不同用戶端的相同匯出規則、請務必在管理匯出規則時保持同步。

如"指令參考資料ONTAP"需詳細 `vserver export-policy`資訊，請參閱。

設定**NFS**認證快取

修改 **ONTAP SVM** 的 **NFS** 憑證快取生存時間的原因

使用認證快取來儲存NFS匯出存取使用者驗證所需的資訊、以加快存取速度並改善效能。ONTAP您可以設定資訊儲存在認證快取中的時間長度、以便針對您的環境進行自訂。

修改NFS認證快取存留時間（TTL）有幾種情況可協助解決問題。您應該瞭解這些情境、以及進行這些修改的後果。

理由

在下列情況下、請考慮變更預設TTL：

問題	補救行動
您環境中的名稱伺服器因為ONTAP 來自VMware的大量要求而效能降低。	增加快取的正向和負向認證的TTL、以減少ONTAP 從功能驗證到名稱伺服器的要求數量。
名稱伺服器管理員進行變更、以允許存取先前遭拒的NFS使用者。	減少快取負面認證的TTL、以縮短NFS使用者等待ONTAP 來自外部名稱伺服器的更新認證要求、以便存取的時間。
名稱伺服器管理員進行變更、以拒絕先前允許的NFS使用者存取。	減少快取正向認證資料的TTL、縮短ONTAP 從外部名稱伺服器要求新認證資料的時間、讓NFS使用者現在無法存取。

後果

您可以個別修改快取正面和負面認證的時間長度。不過、您應該瞭解這樣做的優點和缺點。

如果您...	優勢在於...	缺點是...
增加正向認證快取時間	不常將認證要求傳送至名稱伺服器、減少名稱伺服器的負載。ONTAP	拒絕存取先前允許存取但不再允許的NFS使用者所需的時間較長。

如果您...	優勢在於...	缺點是...
縮短正向認證快取時間	拒絕存取先前允許存取但不再允許的NFS使用者所需的時間較短。	利用此功能、將認證要求更頻繁地傳送至名稱伺服器、增加名稱伺服器的負載。ONTAP
增加負面認證快取時間	不常將認證要求傳送至名稱伺服器、減少名稱伺服器的負載。ONTAP	將存取權限授予先前不允許存取但現在不允許存取的NFS使用者所需的時間較長。
減少負面認證快取時間	將存取權限授予先前不允許存取但現在不允許存取的NFS使用者所需的時間較短。	利用此功能、將認證要求更頻繁地傳送至名稱伺服器、增加名稱伺服器的負載。ONTAP

為 **ONTAP SVM** 配置快取 **NFS** 使用者憑證的生存時間

您可以ONTAP 修改儲存虛擬機器（SVM）的NFS伺服器、設定將NFS使用者認證儲存在內部快取（生存時間或TTL）的時間長度。這可讓您減輕與名稱伺服器負載過高或認證變更影響NFS使用者存取有關的某些問題。

關於這項工作

這些參數可在進階權限層級使用。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行所需的動作：

如果您要修改快取的TTL ...	使用命令...
正面認證	`vserver nfs modify -vserver vserver_name -cached -cred-positive-ttl time_to_live` TTL的測量單位為毫秒。從 ONTAP 9.10.1 及更新版本開始，預設值為 1 小時（ 3,600,000 毫秒）。在 ONTAP 9.9.1 及更早版本中、預設值為 24 小時（ 86,400,000 毫秒）。此值允許的範圍為1分鐘（60000毫秒）到7天（604,800,000毫秒）。
負面認證	`vserver nfs modify -vserver vserver_name -cached -cred-negative-ttl time_to_live` TTL的測量單位為毫秒。預設值為2小時（7、200、000毫秒）。此值允許的範圍為1分鐘（60000毫秒）到7天（604,800,000毫秒）。

3. 返回管理權限層級：

```
set -privilege admin
```

管理匯出原則快取

刷新 **ONTAP NAS SVM** 的匯出策略快取

使用多個匯出原則快取來儲存匯出原則相關資訊、以加快存取速度。ONTAP手動排清匯出原則快取 (`vserver export-policy cache flush`）移除可能過期的資訊、並強制 ONTAP 從適當的外部資源擷取目前資訊。這有助於解決與用戶端存取NFS匯出相關的各種問題。

關於這項工作

匯出原則快取資訊可能因為下列原因而過期：

- 最近對匯出原則規則所做的變更
- 最近變更名稱伺服器中的主機名稱記錄
- 最近在名稱伺服器中變更netgroup項目
- 從網路中斷中恢復、避免網路群組完全載入

步驟

1. 如果您未啟用名稱服務快取、請在預先權限模式中執行下列其中一項動作：

如果您想要清除...	輸入命令...
所有匯出原則快取（showmount除外）	`vserver export-policy cache flush -vserver vserver_name`
匯出原則規則存取快取	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以加入選用的 `-node` 用於指定要清除存取快取的節點的參數。
主機名稱快取	`vserver export-policy cache flush -vserver vserver_name -cache host`
netgroup快取	`vserver export-policy cache flush -vserver vserver_name -cache netgroup` 網路群組的處理需要大量資源。如果您嘗試解決由舊網路群組所造成的用戶端存取問題、則只能清除網路群組快取。
showmount快取	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

2. 如果已啟用名稱服務快取、請執行下列其中一項動作：

如果您想要清除...	輸入命令...
匯出原則規則存取快取	`vserver export-policy cache flush -vserver vserver_name -cache access` 您可以加入選用的 `-node` 用於指定要清除存取快取的節點的參數。
主機名稱快取	`vserver services name-service cache hosts forward-lookup delete-all`
netgroup快取	`vserver services name-service cache netgroups ip-to-netgroup delete-all` `vserver services name-service cache netgroups members delete-all` 網路群組的處理需要大量資源。如果您嘗試解決由舊網路群組所造成的用戶端存取問題、則只能清除網路群組快取。
showmount快取	`vserver export-policy cache flush -vserver vserver_name -cache showmount`

顯示 ONTAP NFS SVM 的匯出策略網路群組佇列和快取

在匯入及解析網路群組時、使用netgroup佇列、並使用netgroup快取來儲存產生的資訊。ONTAP疑難排解匯出原則網路群組相關問題時、您可以使用 `vserver export-policy netgroup queue show` 和 `vserver export-policy netgroup cache show` 用於顯示 netgroup 隊列狀態和 netgroup 高速緩存內容的命令。

步驟

1. 執行下列其中一項動作：

若要顯示匯出原則netgroup …	輸入命令…
佇列	`vserver export-policy netgroup queue show`
快取	`vserver export-policy netgroup cache show -vserver vserver_name`

如"指令參考資料ONTAP"需詳細 `vserver export-policy netgroup`資訊，請參閱。

檢查客戶端 IP 位址是否為 ONTAP NFS 網路群組的成員

疑難排解與網路群組相關的 NFS 用戶端存取問題時、您可以使用 `vserver export-policy netgroup check-membership` 用於確定客戶端 IP 是否是某個 netgroup 的成員的命令。

關於這項工作

檢查netgroup成員資格可讓您判斷ONTAP 是否知道客戶端是或不是netgroup的成員。它也能讓您知道ONTAP 、在重新整理netgroup資訊的同時、該功能是否處於暫時性狀態。此資訊可協助您瞭解為何用戶端可能會被意外授予或拒絕存取。

步驟

1. 檢查用戶端 IP 位址的 netgroup 成員資格： `vserver export-policy netgroup check-membership -vserver vserver_name -netgroup netgroup_name -client-ip client_ip`

   命令可傳回下列結果：

   - 用戶端是netgroup的成員。

     這是透過反向查詢掃描或逐主機搜尋網路群組來確認的。

   - 用戶端是netgroup的成員。

     這是ONTAP 在foundnetgroup快取中找到的。

   - 用戶端不是netgroup的成員。
   - 由於目前正在重新整理網路群組快取、所以無法判斷用戶端的成員資格ONTAP 。

     除非如此、否則無法明確排除成員資格。使用 `vserver export-policy netgroup queue show` 命令來監控 netgroup 的載入、並在完成後重試檢查。

範例

下列範例會檢查IP位址為172.17.16.72的用戶端是否為SVM VS1上的netgroup水銀成員：

```
 cluster1::> vserver export-policy netgroup check-membership -vserver vs1
-netgroup  mercury -client-ip 172.17.16.72
```

優化 **ONTAP NFS SVM** 的存取快取效能

您可以設定數個參數來最佳化存取快取、並在效能與儲存在存取快取中的資訊目前狀態之間找到適當的平衡點。

關於這項工作

當您設定存取快取重新整理期間時、請謹記下列事項：

- 較高的值表示項目在存取快取中的時間較長。

  優勢在於效能更佳、ONTAP 因為用較少資源來重新整理存取快取項目。缺點是、如果匯出原則規則發生變更、而存取快取項目因而變得過時、則更新這些規則所需的時間會較長。因此、應該存取的用戶端可能會遭到拒絕、而應該遭到拒絕的用戶端可能會取得存取權。

- 較低的值代表ONTAP 更常更新存取快取項目。

  優點是項目較新、用戶端較可能被正確授予或拒絕存取。缺點是效能降低、因為ONTAP 用更多資源重新整

理存取快取項目。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行所需的動作：

若要修改...	輸入...
正項目的重新整理期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-positive timeout_value`
否定項目的重新整理期間	`vserver export-policy access-cache config modify-all-vservers -refresh -period-negative timeout_value`
舊項目的逾時期間	`vserver export-policy access-cache config modify-all-vservers -harvest -timeout timeout_value`

3. 驗證新的參數設定：

   ```
   vserver export-policy access-cache config show-all-vservers
   ```

4. 返回管理權限層級：

   ```
   set -privilege admin
   ```

管理檔案鎖定

了解 **ONTAP NFS SVM** 協定之間的檔案鎖定

檔案鎖定是用戶端應用程式用來防止使用者存取先前由其他使用者開啟的檔案的方法。如何鎖定檔案取決於用戶端的傳輸協定。ONTAP

如果用戶端是NFS用戶端、則鎖定為建議事項；如果用戶端是SMB用戶端、則鎖定為必要項目。

由於NFS與SMB檔案鎖定之間的差異、NFS用戶端可能無法存取先前由SMB應用程式開啟的檔案。

當NFS用戶端嘗試存取SMB應用程式鎖定的檔案時、會發生下列情況：

- 在混合或 NTFS 磁碟區中、檔案處理作業、例如 `rm`、 `rmdir`和 `mv` 可能導致 NFS 應用程式失敗。
- SMB拒絕讀取和拒絕寫入開啟模式會分別拒絕NFS讀取和寫入作業。
- 當檔案的寫入範圍遭專屬SMB bytelock鎖定時、NFS寫入作業會失敗。

在UNIX安全型磁碟區中、NFS取消連結和重新命名作業會忽略SMB鎖定狀態、並允許存取檔案。UNIX安全型磁碟區上的所有其他NFS作業都會遵守SMB鎖定狀態。

了解 **ONTAP NFS SVM** 的唯讀位

唯讀位元是逐一檔案設定、以反映檔案是可寫入（停用）或唯讀（啟用）。

使用Windows的SMB用戶端可以設定每個檔案的唯讀位元。NFS用戶端不會設定每個檔案的唯讀位元、因為NFS用戶端沒有任何使用每個檔案唯讀位元的傳輸協定作業。

當使用Windows的SMB用戶端建立檔案時、可以在檔案上設定唯讀位元。ONTAP在NFS用戶端和SMB用戶端之間共用檔案時、也可以設定唯讀位元。ONTAP有些軟體在NFS用戶端和SMB用戶端使用時、需要啟用唯讀位元。

為了在NFS用戶端和SMB用戶端之間共用的檔案上保留適當的讀取和寫入權限、它會根據下列規則來處理唯讀位元：ONTAP

- NFS會將任何啟用唯讀位元的檔案視為未啟用寫入權限位元。
- 如果NFS用戶端停用所有寫入權限位元、且至少有一個位元先前已啟用、ONTAP 則會啟用該檔案的唯讀位元。
- 如果NFS用戶端啟用任何寫入權限位元、ONTAP 則無法使用該檔案的唯讀位元。
- 如果已啟用檔案的唯讀位元、且NFS用戶端嘗試探索檔案的權限、則檔案的權限位元不會傳送至NFS用戶端；ONTAP 而是將權限位元傳送至NFS用戶端、並遮罩寫入權限位元。
- 如果已啟用檔案的唯讀位元、且SMB用戶端停用唯讀位元、ONTAP 則會啟用檔案的擁有者寫入權限位元。
- 啟用唯讀位元的檔案只能由root寫入。

唯讀位元以下列方式與 ACL 和 Unix 模式位元互動：

當檔案設定了唯讀位元：

- 該文件的 ACL 不會發生任何變更。 NFS用戶端將看到與設定唯讀位元之前相同的 ACL。
- 任何允許對檔案進行寫入存取的 Unix 模式位元都會被忽略。
- NFS 和 SMB 用戶端都可以讀取該文件，但不能修改它。
- ACL 和 UNIX 模式位元將被忽略，取而代之的是唯讀位元。這意味著，即使 ACL 允許寫入訪問，只讀位元也會阻止修改。

當檔案未設定唯讀位元：

- ONTAP根據 ACL 和 UNIX 模式位元決定存取權限。
  - 如果 ACL 或 UNIX 模式位元拒絕寫入訪問，則 NFS 和 SMB 用戶端無法修改該檔案。
  - 如果 ACL 和 UNIX 模式位元均不拒絕寫入訪問，則 NFS 和 SMB 用戶端可以修改該檔案。

檔案權限的變更會立即在SMB用戶端上生效、但如果NFS用戶端啟用屬性快取、則可能不會立即在NFS用戶端上生效。

了解 **ONTAP NFS** 和 **Windows** 在處理共用路徑元件鎖定方面有何不同

不像Windows、ONTAP 在檔案開啟時、不會鎖定開啟檔案路徑的每個元件。此行為也會影響SMB共用路徑。

由於無法鎖定路徑的每個元件、因此可以重新命名開啟檔案或共用區上方的路徑元件、這可能會對某些應用程式造成問題、也可能導致SMB組態中的共用路徑無效。ONTAP這可能導致無法存取共用區。

為了避免重新命名路徑元件所造成的問題、您可以套用Windows存取控制清單（ACL）安全性設定、防止使用者或應用程式重新命名重要目錄。

深入瞭解 "如何防止在用戶端存取目錄時重新命名目錄"。

顯示有關 **ONTAP NFS SVM** 的鎖定訊息

您可以顯示目前檔案鎖定的相關資訊、包括鎖定的類型、鎖定狀態、位元組範圍鎖定、共用鎖定模式、委派鎖定及投機鎖定的詳細資料、以及鎖定是以耐久或持續的控點開啟。

關於這項工作

無法針對透過NFSv4或NFSv4.1建立的鎖定顯示用戶端IP位址。

依預設、命令會顯示所有鎖定的相關資訊。您可以使用命令參數來顯示特定儲存虛擬機器（SVM）的鎖定資訊、或是根據其他條件篩選命令的輸出。

。 `vserver locks show` 命令會顯示四種鎖定類型的相關資訊：

- 位元組範圍鎖定、僅鎖定部分檔案。
- 共用鎖定、可鎖定開啟的檔案。
- 投機鎖定、可控制SMB上的用戶端快取。
- 委派：透過NFSv4.x控制用戶端快取

藉由指定選用參數、您可以決定每種鎖定類型的重要資訊。如"指令參考資料ONTAP"需詳細 `vserver locks show`資訊，請參閱。

步驟

1. 使用顯示鎖定的相關資訊 `vserver locks show` 命令。

範例

以下範例顯示具有路徑之檔案上 NFSv4 鎖定的摘要資訊 `/vol1/file1`。共享鎖定存取模式為WRITE拒絕_nONE、且鎖定是以寫入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
              Sharelock Mode: write-deny_none
                                                        delegation  -
              Delegation Type: write
```

以下範例顯示有關 SMB 鎖定的詳細 oplock 和共享鎖定資訊、這些資訊位於具有路徑的檔案上 `/data2/data2_2/intro.pptx`。對於IP位址為10.3.1.3的用戶端、檔案上會以寫入拒絕的共用鎖定存取模式授予可持久使用的控制代碼。批次oplock層級的租賃oplock已授予：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
```

```
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
    Node Holding Lock State: node3
                 Lock State: granted
   Bytelock Starting Offset: -
     Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
    Shared Lock Access Mode: -
        Shared Lock is Soft: -
            Delegation Type: -
             Client Address: 10.3.1.3
               SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

打破 **ONTAP NFS SVM** 的檔案鎖

當檔案鎖定阻礙用戶端存取檔案時、您可以顯示目前保留的鎖定資訊、然後中斷特定鎖定。您可能需要中斷鎖定的案例包括偵錯應用程式。

關於這項工作

此 `vserver locks break`命令僅適用於進階權限層級及更高層級。如"指令參考資料ONTAP"需詳細 `vserver locks break`資訊，請參閱。

步驟

1. 若要尋找打破鎖定所需的資訊、請使用 `vserver locks show` 命令。

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

2. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

3. 執行下列其中一項動作：

如果您要指定…來中斷鎖定	輸入命令…

SVM名稱、Volume名稱、LIF名稱及檔案路徑	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
鎖定ID	`vserver locks break -lockid UUID`

4. 返回管理權限層級：

   ```
   set -privilege admin
   ```

了解 **ONTAP FPolicy** 首次讀取和首次寫入過濾器如何與 **NFS** 配合使用

當使用外部FPolicy伺服器啟用FPolicy、並將讀寫作業設為監控事件時、NFS用戶端在讀寫要求的高流量期間會經歷較長的回應時間。對於NFS用戶端、在FPolicy中使用第一讀取和第一寫入篩選器可減少FPolicy通知的數量、並改善效能。

在NFS中、用戶端會擷取檔案的控制代碼來執行I/O作業。在重新啟動伺服器和用戶端之後、此處理程序可能仍有效。因此、用戶端可自由快取處理代碼並傳送要求、而無需再次擷取處理代碼。在一般工作階段中、會將許多讀取/寫入要求傳送至檔案伺服器。如果針對所有這些要求產生通知、可能會導致下列問題：

- 由於額外的通知處理和更高的回應時間、所以負載較大。
- 即使伺服器不受所有通知影響、仍有大量通知會傳送至FPolicy伺服器。

從用戶端收到特定檔案的第一次讀取/寫入要求後、就會建立快取項目、而且讀取/寫入計數也會遞增。此要求會標示為第一次讀取/寫入作業、並產生FPolicy事件。在規劃及建立NFS用戶端的FPolicy篩選器之前、您應該先瞭解FPolicy篩選器的基本運作方式。

- 第一讀取：篩選用戶端的第一讀取要求。

  當此篩選器用於NFS事件時 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 設定決定處理 FPolicy 的第一讀取要求。

- 第一寫入：篩選用戶端的第一寫入要求。

  當此篩選器用於NFS事件時 `-file-session-io-grouping-count` 和 `-file-session-io-grouping-duration` 設定決定 FPolicy 處理的第一次寫入要求。

NFS伺服器資料庫中會新增下列選項。

```
file-session-io-grouping-count: Number of I/O Ops on a File to Be Clubbed
and Considered as One Session
for Event Generation
file-session-io-grouping-duration: Duration for Which I/O Ops on a File to
Be Clubbed and Considered as
One Session for Event Generation
```

修改 ONTAP SVM 的 NFSv4.1 伺服器實作 ID

NFSv4.1傳輸協定包含一個伺服器實作ID、其中記錄伺服器網域、名稱和日期。您可以修改伺服器實作ID預設值。變更預設值很有用、例如收集使用量統計資料或疑難排解互通性問題時。如需詳細資訊、請參閱RFC 5661。

關於這項工作

這三個選項的預設值如下：

選項	選項名稱	預設值
NFSv4.1實作ID網域	`-v4.1-implementation-domain`	netapp.com
NFSv4.1實作ID名稱	`-v4.1-implementation-name`	叢集版本名稱
NFSv4.1實作ID日期	`-v4.1-implementation-date`	叢集版本日期

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要修改**NFSv4.1**實作識別碼...	輸入命令...
網域	`vserver nfs modify -v4.1 -implementation-domain domain`
名稱	`vserver nfs modify -v4.1 -implementation-name name`
日期	`vserver nfs modify -v4.1 -implementation-date date`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

管理NFSv4 ACL

了解為 ONTAP SVM 啟用 NFSv4 ACL 的好處

啟用NFSv4 ACL有許多好處。

啟用NFSv4 ACL的好處包括：

- 更精細地控制使用者對檔案和目錄的存取
- 更好的NFS安全性
- 改善與CIFS的互通性
- 移除每位使用者16個群組的NFS限制

了解 **ONTAP SVM** 的 **NFSv4 ACL**

使用NFSv4 ACL的用戶端可以設定及檢視系統上檔案和目錄的ACL。在具有 ACL 的目錄中建立新檔案或子目錄時、新檔案或子目錄會繼承 ACL 中所有已標記適當繼承旗標的存取控制項目（ ACE ）。

當檔案或目錄是因NFSv4要求而建立時、產生的檔案或目錄上的ACL取決於檔案建立要求是否包含ACL或僅包含標準UNIX檔案存取權限、以及父目錄是否具有ACL：

- 如果要求包含ACL、則會使用該ACL。
- 如果要求僅包含標準UNIX檔案存取權限、但父目錄具有ACL、則只要將ACE標記為適當的繼承旗標、父目錄ACL中的ACE就會由新檔案或目錄繼承。

  即使是、父 ACL 也會繼承 `-v4.0-acl` 設為 `off`。

- 如果要求僅包含標準UNIX檔案存取權限、且父目錄沒有ACL、則會使用用戶端檔案模式來設定標準UNIX檔案存取權限。
- 如果要求僅包含標準UNIX檔案存取權限、且父目錄具有不可繼承的ACL、則只會以模式位元建立新物件。

如果參數已設為 `restricted`或 `vserver export-policy rule`系列中的命令 `vserver nfs`，則`-chown-mode`即使使用 NFSv4 ACL 設定的磁碟上權限允許非 root 使用者變更檔案擁有權，進階使用者也只能變更檔案擁有權。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

為 **ONTAP SVM** 啟用或停用 **NFSv4 ACL** 修改

當 ONTAP 收到 `chmod` 具有 ACL 之檔案或目錄的命令、依預設會保留及修改 ACL 、以反映模式位元變更。您可以停用 `-v4-acl-preserve` 如果您想要刪除 ACL 、請使用此參數來變更行為。

關於這項工作

使用統一化安全性樣式時、此參數也會指定當用戶端傳送檔案或目錄的chmod、chgroup或chown命令時、是否保留或捨棄NTFS檔案權限。

此參數的預設值為啟用。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要…	輸入下列命令…
啟用現有NFSv4 ACL的保留與修改（預設）	`vserver nfs modify -vserver vserver_name -v4-acl -preserve enabled`
變更模式位元時、請停用保留和丟棄NFSv4 ACL	`vserver nfs modify -vserver vserver_name -v4-acl -preserve disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

了解 **ONTAP** 如何使用 **NFSv4 ACL** 來決定是否可以刪除文件

為了判斷是否能刪除檔案、ONTAP 它使用檔案的刪除位元組合、以及包含目錄的刪除子位元。如需詳細資訊、請參閱NFS 4.1 RFC 5661。

為 **ONTAP SVM** 啟用或停用 **NFSv4 ACL**

若要啟用或停用 NFSv4 ACL 、您可以修改 `-v4.0-acl` 和 `-v4.1-acl` 選項：這些選項預設為停用。

關於這項工作

。 `-v4.0-acl` 或 `-v4.1-acl` 選項可控制 NFSv4 ACL 的設定和檢視、但無法控制這些 ACL 的存取檢查強制執行。

步驟

1. 執行下列其中一項動作：

如果您想要…	然後…
啟用NFSv4.0 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0-acl enabled`
停用NFSv4.0 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0-acl disabled`
啟用 NFSv4.1 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-acl enabled`

停用 NFSv4.1 ACL	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-acl disabled`

修改 **ONTAP SVM** 的 **NFSv4 ACL** 的最大 **ACE** 限制

您可以修改參數、以修改每個 NFSv4 ACL 允許的 ACE 數量上限 `-v4-acl-max-aces`。根據預設、每個ACL的限制設為400個ACE。增加此限制有助於確保資料成功移轉、ACL中包含超過400個ACE、以移轉至執行ONTAP 效益測試的儲存系統。

關於這項工作

增加此限制可能會影響使用NFSv4 ACL存取檔案的用戶端效能。

步驟

1. 將權限層級設為進階：

   `set -privilege advanced`

2. 修改NFSv4 ACL的最大ACE限制：

   `vserver nfs modify -v4-acl-max-aces max_ace_limit`

   的有效範圍

   `max_ace_limit` 是 `192` 至 `1024`.

3. 返回管理權限層級：

   `set -privilege admin`

管理**NFSv4**檔案委派

為 **ONTAP SVM** 啟用或停用 **NFSv4** 讀取檔案委派

若要啟用或停用 NFSv4 讀取檔案委派、您可以修改 `-v4.0-read-delegation`或 選項。啟用讀取檔案委派、您就能免除開啟和關閉檔案所產生的大部分訊息負荷。

關於這項工作

預設會停用讀取檔案委派。

啟用讀取檔案委派的缺點是、伺服器及其用戶端必須在伺服器重新開機或重新啟動、用戶端重新開機或重新啟動、或發生網路分割區之後、才能恢復委派。

步驟

1. 執行下列其中一項動作：

如果您想要...	然後...
啟用NFSv4讀取檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation enabled`
啟用 NFSv4.1 讀取檔案委派	輸入下列命令： + `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation enabled`
停用NFSv4讀取檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0 -read-delegation disabled`
停用 NFSv4.1 讀取檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1 -read-delegation disabled`

結果

檔案委派選項會在變更後立即生效。不需要重新開機或重新啟動NFS。

為 **ONTAP SVM** 啟用或停用 **NFSv4** 寫入檔案委派

若要啟用或停用寫入檔案委派、您可以修改 `-v4.0-write-delegation`或 選項。啟用寫入檔案委派之後、除了開啟和關閉檔案之外、您還可以免除與檔案和記錄鎖定相關的大部分訊息負荷。

關於這項工作

預設會停用寫入檔案委派。

啟用寫入檔案委派的缺點是、伺服器及其用戶端必須在伺服器重新開機或重新啟動、用戶端重新開機或重新啟動、或發生網路分割之後、執行其他工作來恢復委派。

步驟

1. 執行下列其中一項動作：

如果您想要...	然後...
啟用NFSv4寫入檔案委派	輸入下列命令：`vserver nfs modify -vserver vserver_name -v4.0-write -delegation enabled`

如果您想要...	然後...
啟用 NFSv4.1 寫入檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-write-delegation enabled`
停用NFSv4寫入檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.0-write-delegation disabled`
停用 NFSv4.1 寫入檔案委派	輸入下列命令： `vserver nfs modify -vserver vserver_name -v4.1-write-delegation disabled`

結果

檔案委派選項會在變更後立即生效。不需要重新開機或重新啟動NFS。

設定NFSv4檔案和記錄鎖定

了解 ONTAP SVM 的 NFSv4 檔案和記錄鎖定

對於NFSv4用戶端、ONTAP 支援NFSv4檔案鎖定機制、在租賃型模式下維持所有檔案鎖定的狀態。

"NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"

指定 ONTAP SVM 的 NFSv4 鎖定租賃期

若要指定 NFSv4 鎖定租用期間（也就是 ONTAP 不可撤銷地授予用戶端鎖定的期間）、您可以修改 `-v4-lease-seconds` 選項。較短的租用期間可加速伺服器恢復、而較長的租用期間則有利於處理大量用戶端的伺服器。

關於這項工作

根據預設、此選項設為 `30`。此選項的最小值為 `10`。此選項的最大值是鎖定寬限期、您可以使用設定 `locking.lease_seconds` 選項。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令：

   ```
   vserver nfs modify -vserver vserver_name -v4-lease-seconds number_of_seconds
   ```

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

為 ONTAP SVM 指定 NFSv4 鎖定寬限期

若要指定 NFSv4 鎖定寬限期（也就是用戶端在伺服器恢復期間嘗試從 ONTAP 重新取得鎖定狀態的時間週期）、您可以修改 `-v4-grace-seconds` 選項。

關於這項工作

根據預設、此選項設為 `45`。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令：

   ```
   vserver nfs modify -vserver vserver_name -v4-grace-seconds number_of_seconds
   ```

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

了解 ONTAP SVM 的 NFSv4 引用

啟用NFSv4轉介時ONTAP 、支援將「IN-SVM」轉介給NFSv4用戶端。SVM內部參照是指接收NFSv4要求的叢集節點將NFSv4用戶端參照至儲存虛擬機器（SVM）上的另一個邏輯介面（LIF）。

NFSv4用戶端應該從該點開始存取目標LIF接收參照的路徑。當原始叢集節點判斷SVM中存在存留在資料磁碟區所在叢集節點上的LIF時、會提供此類參照、進而讓用戶端能夠更快存取資料、並避免額外的叢集通訊。

啟用或停用 ONTAP SVM 的 NFSv4 引用

您可以啟用選項、在儲存虛擬機器（ SVM ）上啟用 NFSv4 參照 `-v4-fsid-change` 和 `-v4.0-referrals`或。啟用NFSv4參照可讓支援此功能的NFSv4用戶端更快存取資料。

開始之前

如果您想要啟用NFS參照、必須先停用平行NFS。您無法同時啟用兩者。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要…	輸入命令…

啟用NFSv4參照	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.0-referrals enabled`
停用NFSv4參照	`vserver nfs modify -vserver vserver_name -v4.0 -referrals disabled`
啟用 NFSv4.1 參照	`vserver nfs modify -vserver vserver_name -v4-fsid -change enabled vserver nfs modify -vserver vserver_name -v4.1-referrals enabled`
停用 NFSv4.1 參照	`vserver nfs modify -vserver vserver_name -v4.1 -referrals disabled`

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

顯示 **ONTAP NFS SVM** 的統計訊息

您可以在儲存系統上顯示儲存虛擬機器（SVM）的NFS統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料之 NFS 物件的命令。

   ```
   statistics catalog object show -object nfs*
   ```

2. 使用 `statistics start` 和選用 `statistics stop` 從一或多個物件收集資料範例的命令。
3. 使用 `statistics show` 命令以檢視範例資料。

範例：監控**NFSv3**效能

下列範例顯示NFSv3傳輸協定的效能資料。

下列命令會啟動新範例的資料收集：

```
vs1::> statistics start -object nfsv3 -sample-id nfs_sample
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示成功讀取和寫入要求的數目、以及讀取和寫入要求的總數：

```
vs1::> statistics show -sample-id nfs_sample -counter
read_total|write_total|read_success|write_success

Object: nfsv3
Instance: vs1
Start-time: 2/11/2013 15:38:29
End-time: 2/11/2013 15:38:41
Cluster: cluster1

    Counter                                     Value
    --------------------------- ----------------------------
    read_success                                40042
    read_total                                  40042
    write_success                              1492052
    write_total                                1492052
```

相關資訊

- "效能監控設定"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

顯示 **ONTAP NFS SVM** 的 **DNS** 統計訊息

您可以顯示儲存系統上儲存虛擬機器（ SVM ）的 DNS 統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料的 DNS 物件的命令。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 從一或多個物件收集資料範例的命令。
3. 使用 `statistics show` 命令以檢視範例資料。

監控 **DNS** 統計資料

下列範例顯示DNS查詢的效能資料。下列命令會開始收集新範例的資料：

```
vs1::*> statistics start -object external_service_op -sample-id
dns_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
dns_sample2
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示所傳送的DNS查詢數、以及所接收、失敗或逾時的DNS查詢數：

```
vs1::*> statistics show -sample-id dns_sample1 -counter
num_requests_sent|num_responses_received|num_successful_responses|num_time
outs|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:DNS:Query:10.72.219.109
Start-time: 3/8/2016 11:15:21
End-time: 3/8/2016 11:16:52
Elapsed-time: 91s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           0
    num_requests_sent                                              1
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

下列命令會指定計數器顯示特定伺服器上DNS查詢收到特定錯誤的次數、以顯示範例中的資料：

```
vs1::*> statistics show -sample-id dns_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:DNS:Query:NXDOMAIN:10.72.219.109
Start-time: 3/8/2016 11:23:21
End-time: 3/8/2016 11:24:25
Elapsed-time: 64s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                             NXDOMAIN
    server_ip_address                                   10.72.219.109
3 entries were displayed.
```

相關資訊

- "效能監控設定"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

顯示 ONTAP NFS SVM 的 NIS 統計資訊

您可以顯示儲存系統上儲存虛擬機器（ SVM ）的 NIS 統計資料、以監控效能並診斷問題。

步驟

1. 使用 `statistics catalog object show` 用於識別可從中檢視資料的 NIS 物件的命令。

   ```
   statistics catalog object show -object external_service_op*
   ```

2. 使用 `statistics start` 和 `statistics stop` 從一或多個物件收集資料範例的命令。
3. 使用 `statistics show` 命令以檢視範例資料。

監控NIS統計資料

下列範例顯示NIS查詢的效能資料。下列命令會開始收集新範例的資料：

```
vs1::*> statistics start -object external_service_op -sample-id
nis_sample1
vs1::*> statistics start -object external_service_op_error -sample-id
nis_sample2
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示已傳送的NIS查詢數、以及已接收、失敗或逾時的NIS查詢數：

```
vs1::*> statistics show -sample-id nis_sample1 -counter
instance|num_requests_sent|num_responses_received|num_successful_responses
|num_timeouts|num_request_failures|num_not_found_responses

Object: external_service_op
Instance: vs1:NIS:Query:10.227.13.221
Start-time: 3/8/2016 11:27:39
End-time: 3/8/2016 11:27:56
Elapsed-time: 17s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    num_not_found_responses                                        0
    num_request_failures                                           1
    num_requests_sent                                              2
    num_responses_received                                         1
    num_successful_responses                                       1
    num_timeouts                                                   0
6 entries were displayed.
```

下列命令會指定計數器來顯示範例中的資料、這些計數器會顯示特定伺服器上的NIS查詢收到特定錯誤的次數：

```
vs1::*> statistics show -sample-id nis_sample2 -counter
server_ip_address|error_string|count

Object: external_service_op_error
Instance: vs1:NIS:Query:YP_NOTFOUND:10.227.13.221
Start-time: 3/8/2016 11:33:05
End-time: 3/8/2016 11:33:10
Elapsed-time: 5s
Scope: vs1

    Counter                                                     Value
    -------------------------------- --------------------------------
    count                                                           1
    error_string                                           YP_NOTFOUND
    server_ip_address                                   10.227.13.221
3 entries were displayed.
```

相關資訊

- "效能監控設定"
- "統計目錄物件顯示"
- "統計數據顯示"
- "統計開始"
- "統計停止"

了解對 **VMware vStorage over ONTAP NFS** 的支持

支援某些VMware vStorage API、以利在NFS環境中整合陣列（VAAI）功能。ONTAP

支援的功能

支援下列功能：

- 複本卸載

  可讓ESXi主機直接在來源與目的地資料儲存區位置之間複製虛擬機器或虛擬機器磁碟（VMDK）、而不需涉及主機。這可節省ESXi主機CPU週期和網路頻寬。如果來源磁碟區很少、複本卸載可保留空間效率。

- 保留空間

  保留空間以保證VMDK檔案的儲存空間。

限制

VMware vStorage over NFS具有下列限制：

- 複本卸載作業可能會在下列情況下失敗：
  - 在來源或目的地Volume上執行wafliron時、因為它會暫時將Volume離線
  - 同時移動來源或目的地Volume
  - 同時移動來源或目的地LIF
  - 執行接管或恢復作業時
  - 執行切換或切換作業時
- 伺服器端複製可能會因為下列案例中的檔案處理格式差異而失敗：

  您嘗試從目前或先前已將qtree匯出至從未匯出qtree的SVM複製資料。若要解決此限制、您可以在目的地SVM上匯出至少一個qtree。

相關資訊

"哪些VAAI卸載作業受Data ONTAP 支援？"

啟用或停用基於 **ONTAP NFS** 的 **VMware vStorage**

您可以使用來啟用或停用儲存虛擬機器（ SVM ）上透過 NFS 對 VMware vStorage 的支援 `vserver nfs modify` 命令。

關於這項工作

預設會停用透過NFS支援VMware vStorage。

步驟

1. 顯示SVM目前的vStorage支援狀態：

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

2. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
啟用VMware vStorage支援	`vserver nfs modify -vserver vserver_name -vstorage enabled`
停用VMware vStorage支援	`vserver nfs modify -vserver vserver_name -vstorage disabled`

完成後

您必須先安裝適用於VMware VAAI的NFS外掛程式、才能使用此功能。如需詳細資訊、請參閱_安裝適用於VMware VAA__的NetApp NFS外掛程式。

相關資訊

"NetApp文件：適用於VMware VAAI的NetApp NFS外掛程式"

在 ONTAP NFS SVM 上啟用或停用 rquota 支持

遠端配額傳輸協定（ rquota ）可讓 NFS 用戶端從遠端機器取得使用者的配額資訊。rquota 版本的支援會因您的 ONTAP 版本而異。

- ONTAP 9 及更新版本支援 rquota v1 。
- ONTAP 9.12.1 及更新版本支援 rquota v2 。

  如果您從 rquota v1 升級到 rquota v2，您可能會注意到用戶配額限制發生了意外變化。此變化是由於 rquota v1 和 rquota v2 之間的配額計算方式不同所造成的。欲了解更多信息，請參閱"NetApp知識庫：用戶配額限制為何意外變化"。

關於這項工作

預設會停用rquota。

步驟

1. 啟用或停用 rquota ：

如果您想要...	輸入下列命令...
啟用SVM的rquota支援	`vserver nfs modify -vserver vserver_name -rquota enable`
停用SVM的rquota支援	`vserver nfs modify -vserver vserver_name -rquota disable`

如需配額的詳細資訊、請參閱 "邏輯儲存管理"。

了解 NFSv3 和 NFSv4 效能改進以及 ONTAP SVM 的 TCP 傳輸大小

您可以修改TCP最大傳輸大小、藉此改善透過高延遲網路連線至儲存系統的NFSv3和NFSv4用戶端效能。

當用戶端透過延遲時間超過10毫秒的廣域網路（WAN）或城域網路（MAN）存取儲存系統時、您可能可以修改TCP最大傳輸大小來改善連線效能。在低延遲網路（例如區域網路（LAN））中存取儲存系統的用戶端、可能無法從修改這些參數中獲益。如果處理量改善並不超過延遲影響、則不應使用這些參數。

若要判斷您的儲存環境是否能從修改這些參數中獲益、您應該先對效能不佳的NFS用戶端進行全面的效能評估。檢閱低效能是否是因為用戶端的往返延遲過大和要求較少。在這些情況下、用戶端和伺服器無法完全使用可用頻寬、因為他們大部分的工作週期都在等待透過連線傳輸的小要求和回應。

藉由增加NFSv3和NFSv4要求大小、用戶端和伺服器可以更有效地使用可用頻寬、以每單位時間移動更多資料、進而提高連線的整體效率。

請記住、儲存系統與用戶端之間的組態可能有所不同。儲存系統和用戶端支援最大1 MB的傳輸作業大小。不

過、如果您將儲存系統設定為支援1 MB的最大傳輸大小、但用戶端僅支援64 KB、則掛載傳輸大小限制為64 KB或更小。

在修改這些參數之前、您必須注意、這會在組裝和傳輸大量回應所需的一段時間內、在儲存系統上產生額外的記憶體使用量。與儲存系統的高延遲連線越多、額外的記憶體使用量就越高。高記憶體容量的儲存系統可能因為這項變更而幾乎沒有任何影響。記憶體容量過低的儲存系統可能會發生明顯的效能降低。

成功使用這些參數取決於從叢集的多個節點擷取資料的能力。叢集網路固有的延遲可能會增加回應的整體延遲。使用這些參數時、整體延遲通常會增加。因此、對延遲敏感的工作負載可能會產生負面影響。

修改 **ONTAP SVM** 的 **NFSv3** 和 **NFSv4 TCP** 最大傳輸大小

您可以修改 `-tcp-max-xfer-size` 使用 NFSv3 和 NFSv4.x 通訊協定、為所有 TCP 連線設定最大傳輸大小的選項。

關於這項工作

您可以針對每個儲存虛擬機器（SVM）個別修改這些選項。

從 ONTAP 9 開始 `v3-tcp-max-read-size` 和 `v3-tcp-max-write-size` 選項已過時。您必須使用 `-tcp-max-xfer-size` 選項。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要...	輸入命令...
修改NFSv3或NFSv4 TCP最大傳輸大小	`vserver nfs modify -vserver vserver_name -tcp-max-xfer-size integer_max_xfer_size`

選項	範圍	預設
`-tcp-max-xfer-size`	8192至1048576位元組	65536 位元組

> 您輸入的最大傳輸大小必須是4 KB（4096位元組）的倍數。未適當調整的要求會對效能造成負面影響。

3. 使用 `vserver nfs show -fields tcp-max-xfer-size` 用於驗證變更的命令。
4. 如果有任何用戶端使用靜態掛載、請卸載並重新掛載新的參數大小以使其生效。

範例

下列命令會將SVM上的NFSv3和NFSv4.x TCP最大傳輸大小設為1048576位元組、名稱為VS1：

```
vs1::> vserver nfs modify -vserver vs1 -tcp-max-xfer-size 1048576
```

配置 ONTAP SVM 的 NFS 使用者允許的群組 ID 數量

根據預設、ONTAP 使用Kerberos（RPCSEC_GSS）驗證處理NFS使用者認證時、支援最多32個群組ID。使用AUTH_SYS驗證時、預設的群組ID最大數量為16、如RFC 5531所定義。如果您的使用者成員超過預設群組數、則最多可增加1,024個。

關於這項工作

如果使用者的認證中有超過預設的群組ID數目、則其餘的群組ID會被刪減、而且使用者在嘗試從儲存系統存取檔案時可能會收到錯誤訊息。您應該將每個SVM的最大群組數設定為代表環境中最大群組數的數字。

了解啟用擴充組的 AUTH_SYS 驗證先決條件(`-auth-sys-extended-groups`) 使用超出預設最大 16 個群組 ID，請參閱"NetApp知識庫：啟用 auth-sys-extended-groups 的先決條件是什麼？"

下表顯示的兩個參數 `vserver nfs modify` 決定三個範例組態中群組 ID 最大數目的命令：

參數	設定	產生的群組ID限制

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`32`
	
	`disabled`
	
	這些是預設設定。
		RPCSEC_GSS：32
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`256`
	
	`disabled`
		RPCSEC_GSS ： 256
		
		AUTH_SYS：16

`-extended-groups-limit`
 	
`-auth-sys-extended-groups`
	`512`
	
	`enabled`
		RPCSEC_GSS ： 512
		
		驗證系統： 512

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行所需的動作：

如果您要設定允許的輔助群組數目上限…	輸入命令…

僅適用於RPCSEC_GSS、並將AUTH_SYS設為預設值16	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups disabled`
適用於RPCSEC_GSS和AUTH_SYS	`vserver nfs modify -vserver vserver_name -extended-groups-limit {32-1024} -auth-sys-extended-groups enabled`

3. 驗證 `-extended-groups-limit` 並驗證 AUTH_SYS 是否使用延伸群組： `vserver nfs show -vserver vserver_name -fields auth-sys-extended-groups,extended-groups-limit`
4. 返回管理權限層級：

   `set -privilege admin`

範例

下列範例可啟用AUTH_SYS驗證的延伸群組、並將AUTH_SYS和RPCSEC_GSS驗證的延伸群組數目上限設為512。這些變更僅適用於存取名為VS1的SVM的用戶端：

```
vs1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use
         them only when directed to do so by NetApp personnel.
Do you want to continue? {y|n}: y

vs1::*> vserver nfs modify -vserver vs1 -auth-sys-extended-groups enabled
-extended-groups-limit 512

vs1::*> vserver nfs show -vserver vs1 -fields auth-sys-extended-
groups,extended-groups-limit
vserver auth-sys-extended-groups extended-groups-limit
------- ----------------------- --------------------
vs1     enabled                 512

vs1::*> set -privilege admin
```

相關資訊

- "NetApp知識庫：針對ONTAP 9 的 NFS 驗證的 AUTH_SYS 擴充組更改"

控制根用戶對 **ONTAP SVM** 的 **NTFS** 安全模式資料的存取

您可以設定ONTAP 讓NFS用戶端存取NTFS安全型資料和NTFS用戶端、以存取NFS安全型資料。在NFS資料儲存區上使用NTFS安全樣式時、您必須決定如何處理root使用者的存取、並據此設定儲存虛擬機器（SVM）。

關於這項工作

當root使用者存取NTFS安全型資料時、您有兩種選擇：

- 將root使用者對應至Windows使用者、就像任何其他NFS使用者一樣、並根據NTFS ACL來管理存取。
- 忽略NTFS ACL並提供root的完整存取權。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行所需的動作：

如果您希望root使用者…	輸入命令…
對應至Windows使用者	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root disabled`
略過NT ACL檢查	`vserver nfs modify -vserver vserver_name -ignore -nt-acl-for-root enabled`

   預設會停用此參數。

   如果啟用此參數、但root使用者沒有名稱對應、ONTAP 則使用預設的SMB系統管理員認證來進行稽核。

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

支援的**NFS**版本和用戶端

了解支援的 **ONTAP NFS** 版本和用戶端

在網路中使用NFS之前、您必須先知道哪些NFS版本和用戶端ONTAP 支援哪些NFS。

下表指出ONTAP 、在預設情況下、當支援主要和次要NFS傳輸協定版本時、依預設、支援並不表示這是ONTAP 支援該NFS傳輸協定的最早版本。

版本	支援	引進
NFSv3.	是的	所有 ONTAP 版本
NFSv4.0	是的	版本8 ONTAP
NFSv4.1	是的	版本8.1 ONTAP
NFSv4.2	是的	部分9.8 ONTAP

版本	支援	引進
pNFS	是的	版本8.1 ONTAP

如需NFS用戶端ONTAP 所支援的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

了解 **ONTAP** 對 **NFSv4.0** 功能的支持

除了SPKM3和LIPKEYY安全機制、支援NFSv4.0中的所有必要功能。ONTAP

支援下列NFSv4功能：

- 複合

  允許用戶端在單一遠端程序呼叫（RPC）要求中要求多個檔案作業。

- 檔案委派

  可讓伺服器將檔案控制權委派給某些類型的用戶端、以進行讀取和寫入存取。

- 虛擬**FS**

  由NFSv4伺服器用來判斷儲存系統上的掛載點。NFSv4中沒有掛載傳輸協定。

- 鎖定

  租賃型。NFSv4中沒有個別的網路鎖定管理程式（NLM）或網路狀態監視器（NSM）傳輸協定。

如需NFSv4.0傳輸協定的詳細資訊、請參閱RFC 3530。

了解 **ONTAP** 對 **NFSv4** 的支援限制

您應該瞭ONTAP 解NFSv4支援的若干項功能限制。

- 委派功能不受每種用戶端類型支援。
- 在更新版本的版本中、除了UTF8磁碟區之外、其他磁碟區上的非Ascii字元名稱會被儲存系統拒絕。ONTAP

  在更新版本的發行版中、使用utf8mb4語言設定建立並使用NFS v4掛載的Volume不再受此限制。ONTAP

- 所有檔案處理常式；伺服器不會提供揮發性檔案處理常式。
- 不支援移轉與複寫。
- NFSv4用戶端不支援唯讀負載共用鏡像。

  將NFSv4用戶端路由至負載共用鏡射的來源、以進行直接讀取和寫入存取。ONTAP

- 不支援命名屬性。

- 支援所有建議的屬性、但下列項目除外：
  - `archive`
  - `hidden`
  - `homogeneous`
  - `mimetype`
  - `quota_avail_hard`
  - `quota_avail_soft`
  - `quota_used`
  - `system`
  - `time_backup`

> 雖然它不支援 `quota*` 屬性、 ONTAP 確實透過 RQUOTA 側頻傳輸協定支援使用者和群組配額。

了解 **ONTAP** 對 **NFSv4.1** 的支持

從功能不支援的問題9.8開始ONTAP 、NFSv4.1啟用時、預設會提供nconnect功能。

較早的NFS用戶端實作只使用單一TCP連線與掛載。在鏈接功能中、單一TCP連線可能會成為瓶頸、導致IOPS增加。ONTAP

nconnect 透過允許單一掛載點建立多個 TCP 連線（最多 16 個），提高了 NFS 用戶端的效能，有助於克服隨著 IOPS 增加，單一 TCP 連線可能出現的效能瓶頸。

NFSv4.1預設會在ONTAP 更新版本的版本中啟用。在舊版中、您可以透過指定來啟用 `-v4.1` 選項並將其設定為 `enabled` 在儲存虛擬機器（ SVM ）上建立 NFS 伺服器時。

不支援NFSv4.1目錄和檔案層級委派。ONTAP

相關資訊

"了解 nconnect 如何提升 NFS 效能"。

了解 **ONTAP** 對 **NFSv4.2** 的支持

從 ONTAP 9.8 開始、 ONTAP 支援 NFSv4.2 傳輸協定、以允許啟用 NFSv4.2 的用戶端存取。

ONTAP 9.9.1 及更高版本預設為啟用 NFSv4.2。在ONTAP 9.8 中，需要透過指定以下參數手動啟用 v4.2： `-v4.2`選項並將其設為 `enabled`在儲存虛擬機器 (SVM) 上建立 NFS 伺服器時。啟用 NFSv4.1 也允許客戶端在掛載為 v4.2 時使用 NFSv4.1 的功能。

後續的 ONTAP 版本擴大支援 NFSv4.2 選用功能。

開始於...	**NFSv4.2** 選用功能包括 ...
ONTAP 9.12.1	• NFS擴充屬性 • 稀疏檔案 • 空間保留
部分9.9.1 ONTAP	標示為NFS的強制存取控制（MAC）

NFS v4.2 安全性標籤

從ONTAP 推出支援NFS9.9.1的功能開始、就能啟用NFS安全標籤。依預設會停用。

使用NFS v4.2安全性標籤時、ONTAP 即可識別出需求性的NFS伺服器存取控制（MAC）、儲存及擷取用戶端傳送的sec_label屬性。

如需詳細資訊、請參閱 "RFC 7240"。

從ONTAP S廳9.12.1開始、支援NDMP傾印作業的NFS v4.2安全標籤。如果在舊版的檔案或目錄上遇到安全性標籤、傾印就會失敗。

步驟

1. 將權限設定變更為進階：

```
set -privilege advanced
```

2. 啟用安全性標籤：

```
vserver nfs modify -vserver <svm_name> -v4.2-seclabel enabled
```

NFS擴充屬性

從S廳9.12.1開始ONTAP 、預設會啟用NFS擴充屬性（xattro）。

延伸屬性是定義的標準NFS屬性 "RFC 8276" 並在現代化的NFS用戶端中啟用。它們可用於將使用者定義的中繼資料附加至檔案系統物件、而且對進階安全性部署非常感興趣。

NDMP傾印作業目前不支援NFS擴充屬性。如果在檔案或目錄上遇到延伸屬性、傾印會繼續進行、但不會備份這些檔案或目錄上的延伸屬性。

如果您需要停用延伸屬性、請使用 `vserver nfs modify -v4.2-xattrs disabled` 命令。

了解 **nconnect** 如何提升 **NFS** 效能

從ONTAP 9.8 開始，啟用 NFSv4.1 時，nconnect 功能預設可用。 nconnect 透過允許單一掛載點建立多個 TCP 連線來提升 NFS 用戶端效能。

nconnect 的工作原理

較早的NFS用戶端實作只使用單一TCP連線與掛載。在鏈接功能中、單一TCP連線可能會成為瓶頸、導致IOPS增加。ONTAP

啟用 nconnect 的用戶端可以為單一 NFS 掛載點建立多個 TCP 連線（最多 16 個）。 nconnect 僅使用一個 IP 位址，並透過該 IP 位址建立多個 TCP 連線來掛載 NFS 匯出。NFS 用戶端以輪詢方式將檔案操作指派到多個 TCP 連線上，從而從可用的網路頻寬中獲得更高的吞吐量。

支援的 NFS 版本

- 建議將 nconnect 用於 NFSv3、NFSv4.2 和 NFSv4.1 掛載。
- 不建議將 nconnect 用於 NFSv4.0 掛載。

> 為了獲得最佳效能， NetApp建議使用 nconnect 搭配 NFSv4.1，而不是 NFSv4.0。雖然 NFSv4.0 支援多個連接，但 NFSv4.1 與 nconnect 結合使用可提供更好的負載分配和更高的吞吐量。

客戶支援

請參閱NFS用戶端文件、確認您的用戶端版本是否支援nconnect。

相關資訊

- "了解 ONTAP 對 NFSv4.1 的支持"
- "了解 ONTAP 對 NFSv4.2 的支持"

了解 ONTAP 對平行 NFS 的支持

支援平行NFS（pNFS）ONTAP 。pNFS傳輸協定可讓用戶端直接存取分散在叢集多個節點上的一組檔案資料、藉此提升效能。它可協助用戶端找到磁碟區的最佳路徑。

了解 ONTAP NFS 硬掛載

疑難排解掛載問題時、您必須確定使用正確的掛載類型。NFS支援兩種掛載類型：軟掛載和硬掛載。基於可靠性考量、您只能使用硬體掛載。

您不應該使用軟掛載、尤其是在NFS逾時頻繁的情況下。競爭情況可能是因為這些逾時而發生、可能導致資料毀損。

並行 NFS

簡介

了解ONTAP中的平行 NFS (pNFS)

並行 NFS 於 2010 年 1 月作為 RFC 標準 RFC-5661 推出，旨在透過分離元資料和資料路徑，允許客戶端直接存取 NFSv4.1 伺服器上的檔案資料。這種直接存取方式透過資料本地化、CPU效率和操作並行化帶來效能優勢。2018 年編寫了後續的 RFC，涵蓋 pNFS 佈局

類型（RFC-8434），其中定義了文件、區塊和物件佈局的標準。ONTAP利用 pNFS 操作的檔案佈局類型。

> 從 2024 年 7 月開始，先前以 PDF 形式發布的技術報告內容已與ONTAP產品文件整合。ONTAP NFS 儲存管理文件現在包含了來自 *TR-4063： NetApp ONTAP* 中的平行網路檔案系統 *(pNFS)* 的內容。

多年來，NFSv3 一直是 NFS 協定的標準版本，幾乎適用於所有用例。然而，該協定存在一些局限性，例如缺乏狀態性、權限模型簡陋以及基本的鎖定功能。NFSv4.0 (RFC 7530) 在 NFSv3 的基礎上進行了一系列改進，隨後的 NFSv4.1 (RFC 5661) 和 NFSv4.2 (RFC 7862) 版本進一步改進了這些改進，增加了並行 NFS (pNFS) 等功能。

NFSv4.x 的優勢

NFSv4.x 相較於 NFSv3 有下列優勢：

- 由於 NFSv4 僅使用單一連接埠（2049）進行操作，因此對防火牆友善。
- 進階且積極的快取管理，例如 NFSv4.x 中的委託機制
- 採用密碼學的強大 RPC 安全選項
- 字元國際化
- 複合操作
- 僅支援 TCP
- 有狀態協定（不像NFSv3那樣是無狀態的）
- 全面整合 Kerberos，實現高效率的身份驗證機制
- NFS轉診
- 支援與 UNIX 和 Windows 相容的存取控制
- 基於字串的使用者和群組標識符
- pNFS（NFSv4.1）
- 擴展屬性（NFSv4.2）
- 安全標籤（NFSv4.2）
- 稀疏檔案操作（FALLOCATE）（NFSv4.2）

有關 NFSv4.x 的更多信息，包括最佳實踐和功能詳情，請參閱 "NetApp技術報告4067：NFS最佳實務與實作指南"。

相關資訊

- "NFS組態總覽"
- "NFS 管理概述"
- "資料區管理FlexGroup"
- "NFS 主幹總覽"
- https://www.netapp.com/pdf.html?item=/media/19370-tr-4523.pdf

- "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"

了解**ONTAP**中的 **pNFS** 架構

pNFS 架構由三個主要元件組成：支援 pNFS 的 NFS 用戶端、為元資料操作提供專用路徑的元資料伺服器以及提供檔案本地化路徑的資料伺服器。

用戶端存取 pNFS 需要與 NFS 伺服器上的資料和元資料路徑建立網路連線。如果 NFS 伺服器包含用戶端無法存取的網路接口，則伺服器可能會向客戶端通告無法存取的資料路徑，從而導致服務中斷。

元資料伺服器

當用戶端使用 NFSv4.1 或更高版本發起掛載，且 NFS 伺服器上啟用了 pNFS 時，pNFS 中的元資料伺服器就會建立。完成此操作後，所有元資料流量都將透過此連接發送，並在掛載期間保持在此連接上，即使介面遷移到另一個節點。

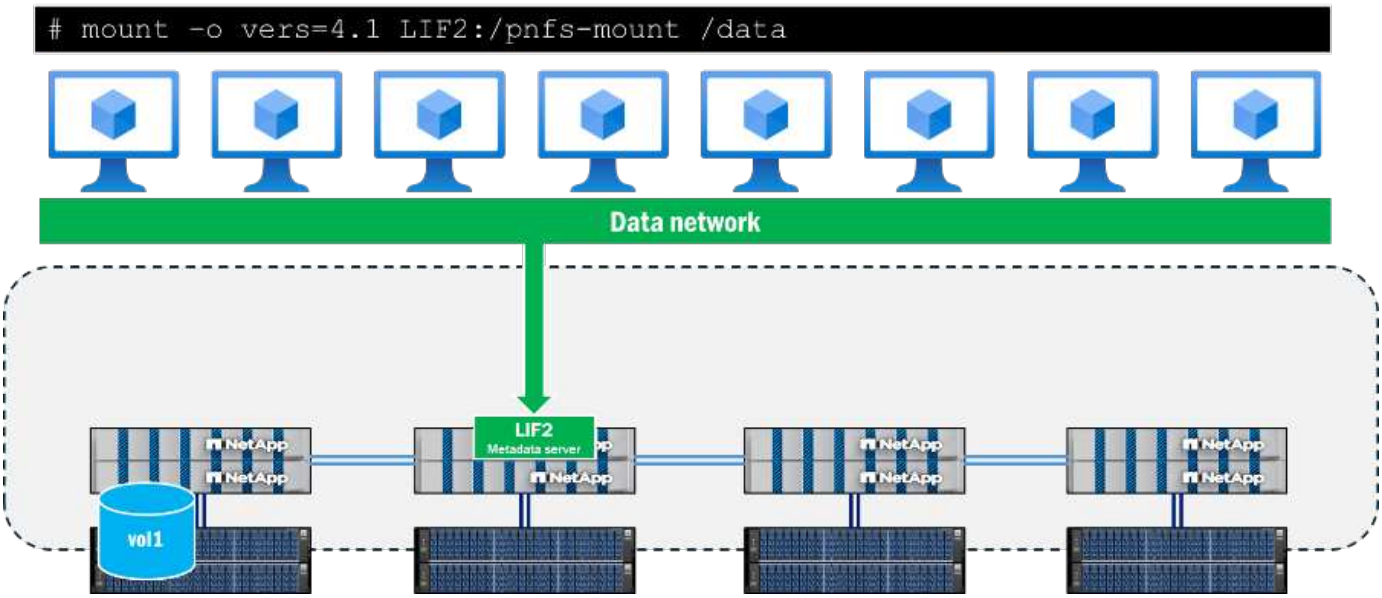


圖 **1.** 在**ONTAP**的 **pNFS** 中建立元資料伺服器

pNFS 支援是在掛載呼叫期間確定的，具體是在 EXCHANGE_ID 呼叫中確定的。在 NFS 操作下方的封包擷取中可以看到這個標誌。當 pNFS 標誌 `EXCHGID4_FLAG_USE_PNFS_DS` 和 `EXCHGID4_FLAG_USE_PNFS_MDS` 如果設定為 1，則該介面符合 pNFS 中的資料和元資料操作條件。

```
Operations (count: 1)
  Opcode: EXCHANGE_ID (42)
      Status: NFS4_OK (0)
      clientid: 0x004050a97100001c
      seqid: 0x00000001
    flags: 0x00060100, EXCHGID4_FLAG_USE_PNFS_DS, EXCHGID4_FLAG_USE_PNFS_MDS, EXCHGID4_FLAG_BIND_PRINC
        0... .... .... .... .... .... .... .... = EXCHGID4_FLAG_CONFIRMED_R: Not set
        .0.. .... .... .... .... .... .... .... = EXCHGID4_FLAG_UPD_CONFIRMED_REC_A: Not set
        .... .... .... .1.. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_DS: Set
        .... .... .... ..1. .... .... .... .... = EXCHGID4_FLAG_USE_PNFS_MDS: Set
        .... .... .... ...0 .... .... .... .... = EXCHGID4_FLAG_USE_NON_PNFS: Not set
        .... .... .... .... .... ...1 .... .... = EXCHGID4_FLAG_BIND_PRINC_STATEID: Set
        .... .... .... .... .... .... .... ..0. = EXCHGID4_FLAG_SUPP_MOVED_MIGR: Not set
        .... .... .... .... .... .... .... ...0 = EXCHGID4_FLAG_SUPP_MOVED_REFER: Not set
```

圖 **2. pNFS**掛載的資料包捕獲

NFS 中的元資料通常包括檔案和資料夾屬性，例如檔案句柄、權限、存取和修改時間以及所有權資訊。元資料還可以包括建立和刪除呼叫、連結和取消連結呼叫以及重新命名。

在 pNFS 中，還有一部分元資料呼叫是 pNFS 特性特有的，這些呼叫將在後續章節中進行更詳細的介紹。 "RFC 5661"。這些呼叫用於協助確定 pNFS 合格設備、設備到資料集的映射以及其他所需資訊。下表列出了 pNFS 特有的元資料操作。

營運	說明
佈局獲取	從元資料伺服器取得資料伺服器對應。
佈局委員會	伺服器提交佈局並更新元資料映射。
佈局返回	返回佈局；如果資料被修改，則傳回新佈局。
取得設備資訊	客戶端取得儲存叢集中資料伺服器的最新資訊。
取得設備列表	客戶端請求提供參與儲存叢集的所有資料伺服器的清單。
CB_LAYOUTRECALL	如果偵測到衝突，伺服器會從客戶端呼叫資料佈局。
CB_RECALL_ANY	將所有佈局傳回給元資料伺服器。
CB_NOTIFY_DEVICEID	設備 ID 發生任何變更時發出通知。

資料路徑資訊

元資料伺服器建立並開始資料操作後， ONTAP開始追蹤符合 pNFS 讀取和寫入操作條件的設備 ID，以及將叢集中的磁碟區與本機網路介面關聯起來的設備對應。當對掛載點執行讀取或寫入操作時，就會發生此程序。元資料調用，例如 `GETATTR`**不會觸發這些設備映射。因此，運行一個** `ls` 掛載點內的命令不會更新映射。

可以使用ONTAP CLI 的高階權限查看設備和映射，如下所示。

```
::*> pnfs devices show -vserver DEMO
  (vserver nfs pnfs devices show)
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
DEMO             16              2157024470      available       1

::*> pnfs devices mappings show -vserver SVM
  (vserver nfs pnfs devices mappings show)
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
DEMO            16              2488            10.193.67.211
```

這些指令中沒有磁碟區名稱。相反，將使用與這些磁碟區關聯的數字 ID：主集 ID (MSID) 和資料集 ID (DSID)。若要尋找與映射相關的體積，您可以使用 `volume show -dsid [dsid_numeric]` 或者 `volume show -msid [msid_numeric]` 具備ONTAP CLI 的高階權限。

當客戶端嘗試讀取或寫入位於遠離元資料伺服器連接的節點上的檔案時，pNFS 將協商適當的存取路徑，以確保這些操作的資料本地性，並且客戶端將重定向到已發布的 pNFS 設備，而不是嘗試穿越叢集網路來存取該檔案。這有助於降低CPU佔用率和網路延遲。

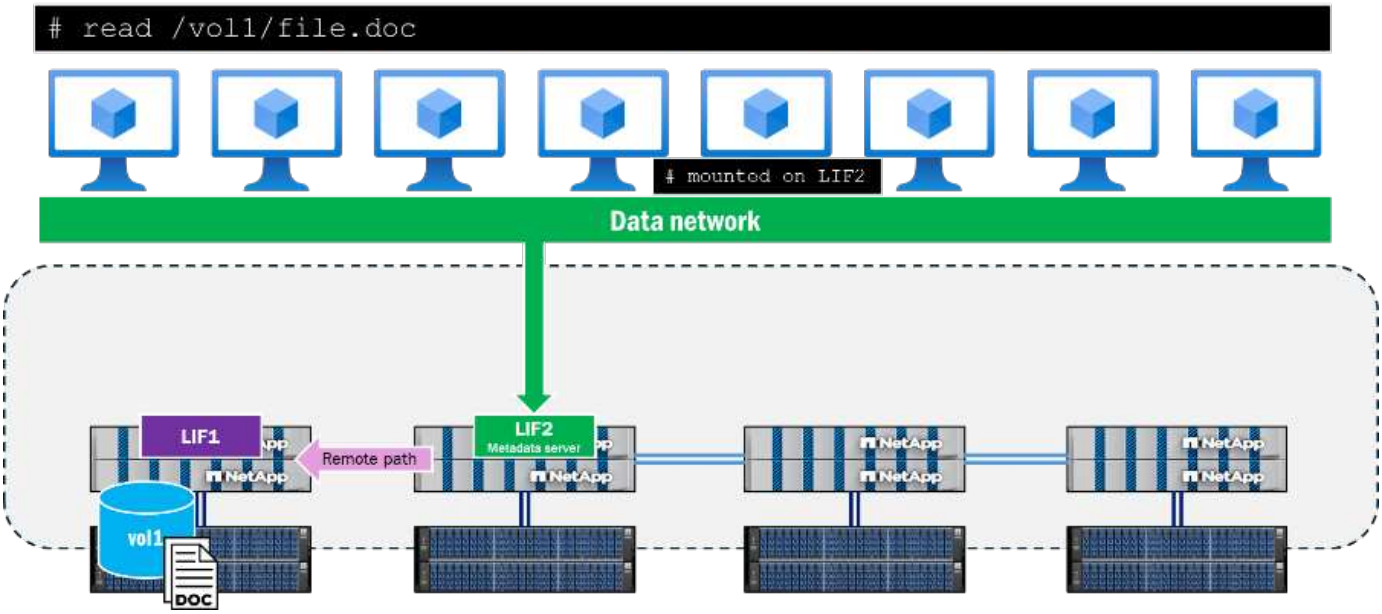


圖 3. 使用 **NFSv4.1** 的遠端讀取路徑，無需 **pNFS**

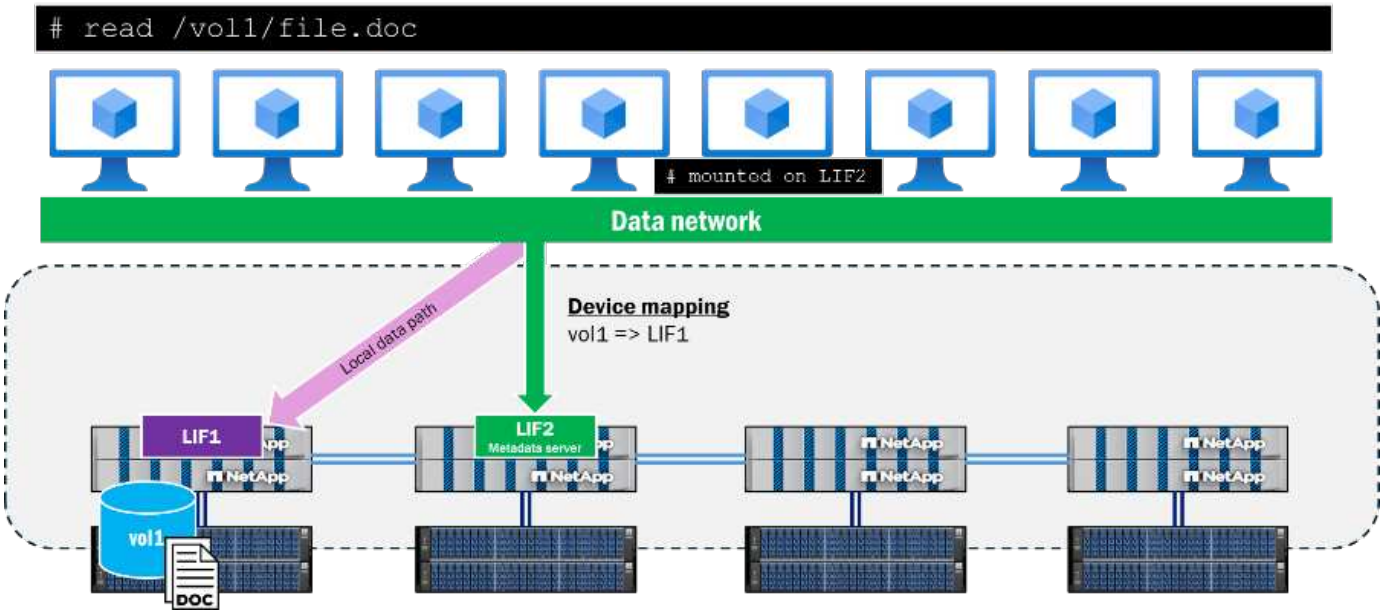


圖 **4.** 使用 **pNFS** 的本地化讀取路徑

pNFS 控制路徑

除了 pNFS 的元資料和資料部分之外，還有一個 pNFS 控制路徑。控制路徑由 NFS 伺服器用於同步檔案系統資訊。在ONTAP集群中，後端集群網路會定期複製，以確保所有 pNFS 設備和設備映射保持同步。

pNFS 設備群組工作流程

以下描述了客戶端請求讀取或寫入磁碟區中的檔案後，pNFS 設備如何在ONTAP中填入。

1. 客戶端請求讀取或寫入；執行 OPEN 操作並檢索檔案句柄。
2. 執行 OPEN 操作後，用戶端透過元資料伺服器連接，以 LAYOUTGET 呼叫的方式將檔案句柄傳送至儲存裝置。
3. LAYOUTGET 向客戶端傳回有關文件佈局的信息，例如狀態 ID、條帶大小、文件段和裝置 ID。
4. 然後客戶端取得裝置 ID，並向伺服器發送 GETDEVINFO 呼叫以檢索與該裝置關聯的 IP 位址。
5. 儲存裝置會傳送回覆，其中包含用於本機存取該裝置的關聯 IP 位址清單。
6. 用戶端透過儲存設備傳回的本機 IP 位址繼續進行 NFS 通訊。

pNFS與**FlexGroup**體積的交互

ONTAP中的FlexGroup磁碟區將儲存呈現為跨越叢集中多個節點的FlexVol volume組成部分，從而允許工作負載利用多個硬體資源，同時保持單一掛載點。由於多個具有多個網路介面的節點與工作負載交互，因此在ONTAP中看到遠端流量穿越後端叢集網路是很自然的結果。

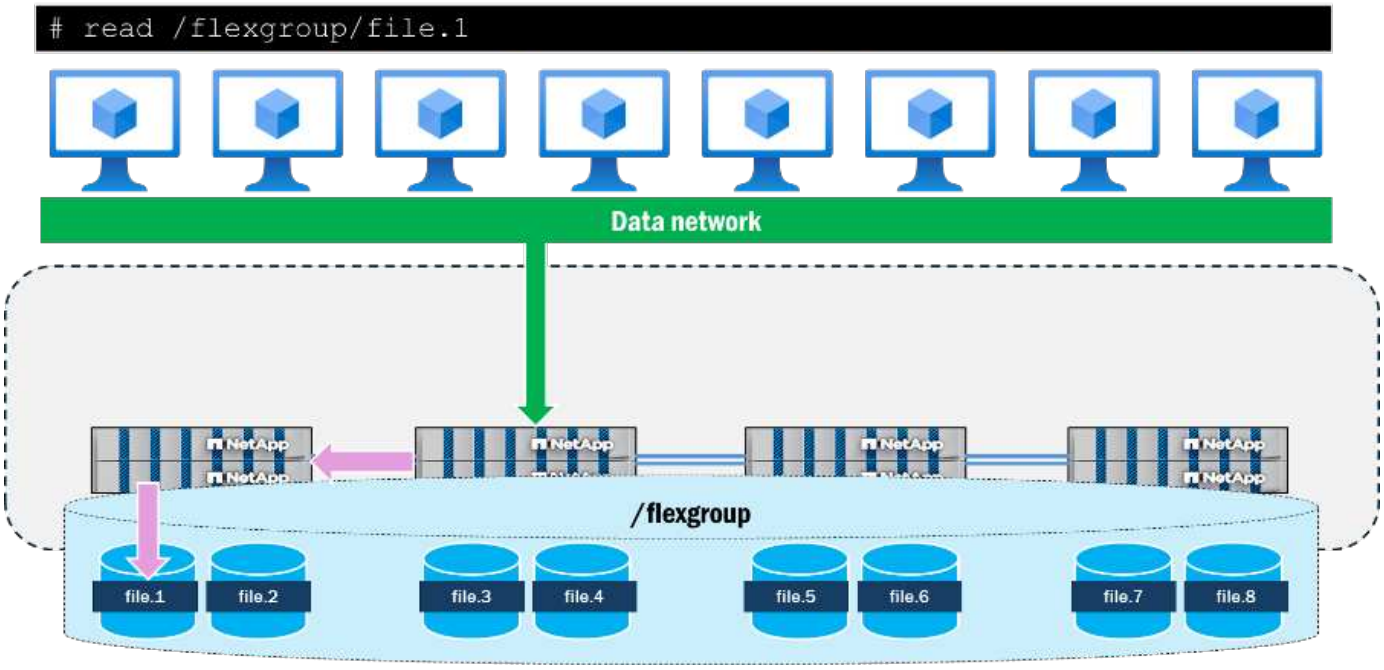


圖 **5.** 在不使用 **pNFS** 的情況下，透過**FlexGroup**磁碟區存取單一文件

使用 pNFS 時， ONTAP會追蹤FlexGroup磁碟區的檔案和磁碟區佈局，並將它們對應到叢集中的本機資料介面。例如，如果包含正在存取的檔案的組成磁碟區位於節點 1 上，則ONTAP將通知用戶端將資料流量重新導向至節點 1 上的資料介面。

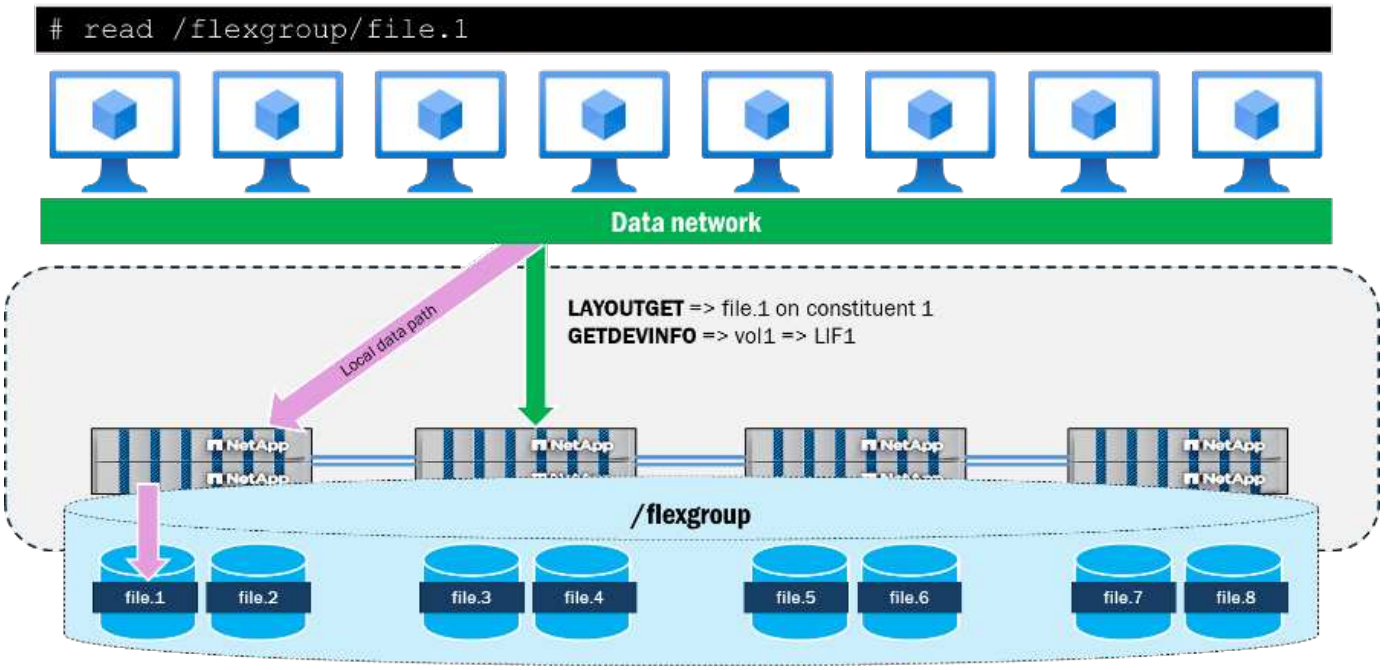


圖 **6.** 在**FlexGroup**區中使用 **pNFS** 進行單一檔案存取

pNFS 也提供了從單一客戶端呈現平行網路路徑到檔案的功能，而沒有 pNFS 的 NFSv4.1 則不具備此功能。例如，如果用戶端想要使用 NFSv4.1（不使用 pNFS）從相同掛載點同時存取四個文件，則所有文件都將使用相同的網路路徑， ONTAP叢集將改為向這些文件發送遠端請求。掛載路徑可能會成為操作的瓶頸，因為它們都遵循一條路徑到達同一個節點，並且還要處理元資料操作以及資料操作。

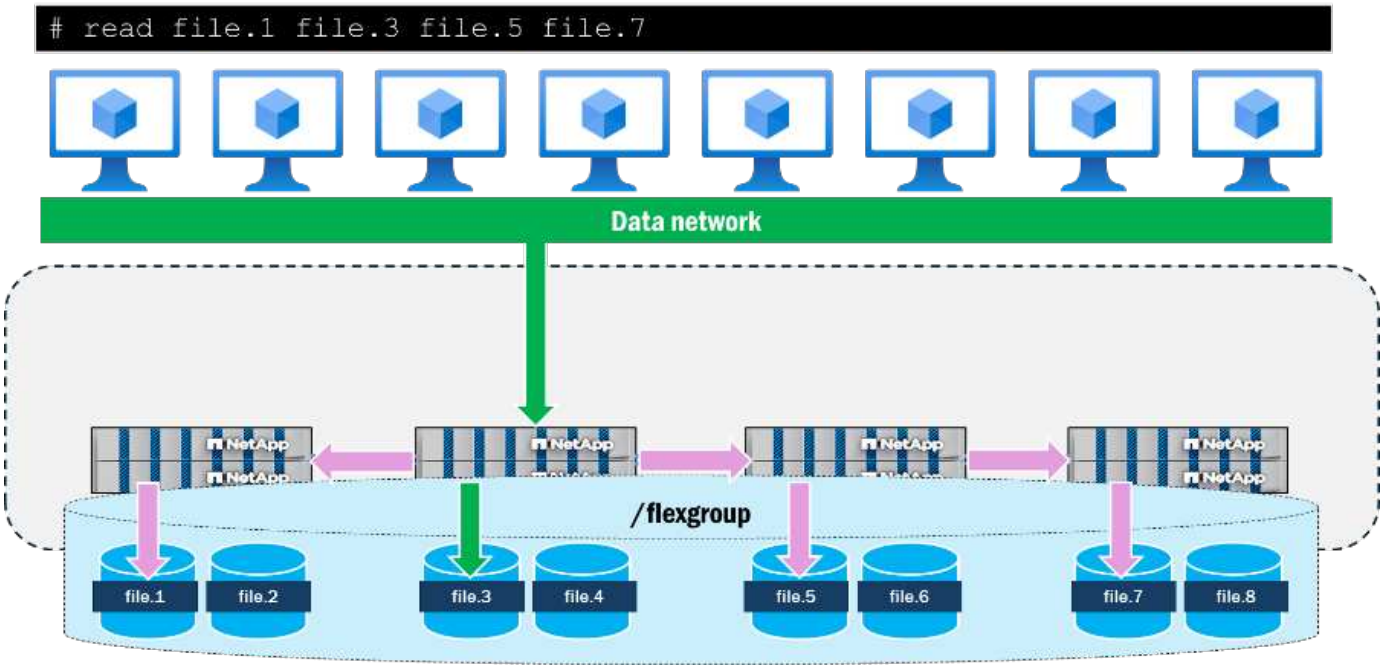


圖 **7.** 在不使用 **pNFS** 的情況下， **FlexGroup**磁碟區中可同時存取多個檔案。

當使用 pNFS 從單一客戶端同時存取相同的四個檔案時，用戶端和伺服器會協商每個節點上的檔案本機路徑，並使用多個 TCP 連線進行資料操作，而掛載路徑則作為所有元資料操作的位置。這樣既可以利用本地檔案路徑來降低延遲，也可以透過使用多個網路介面來提高吞吐量，前提是客戶端可以發送足夠的資料來使網路飽和。

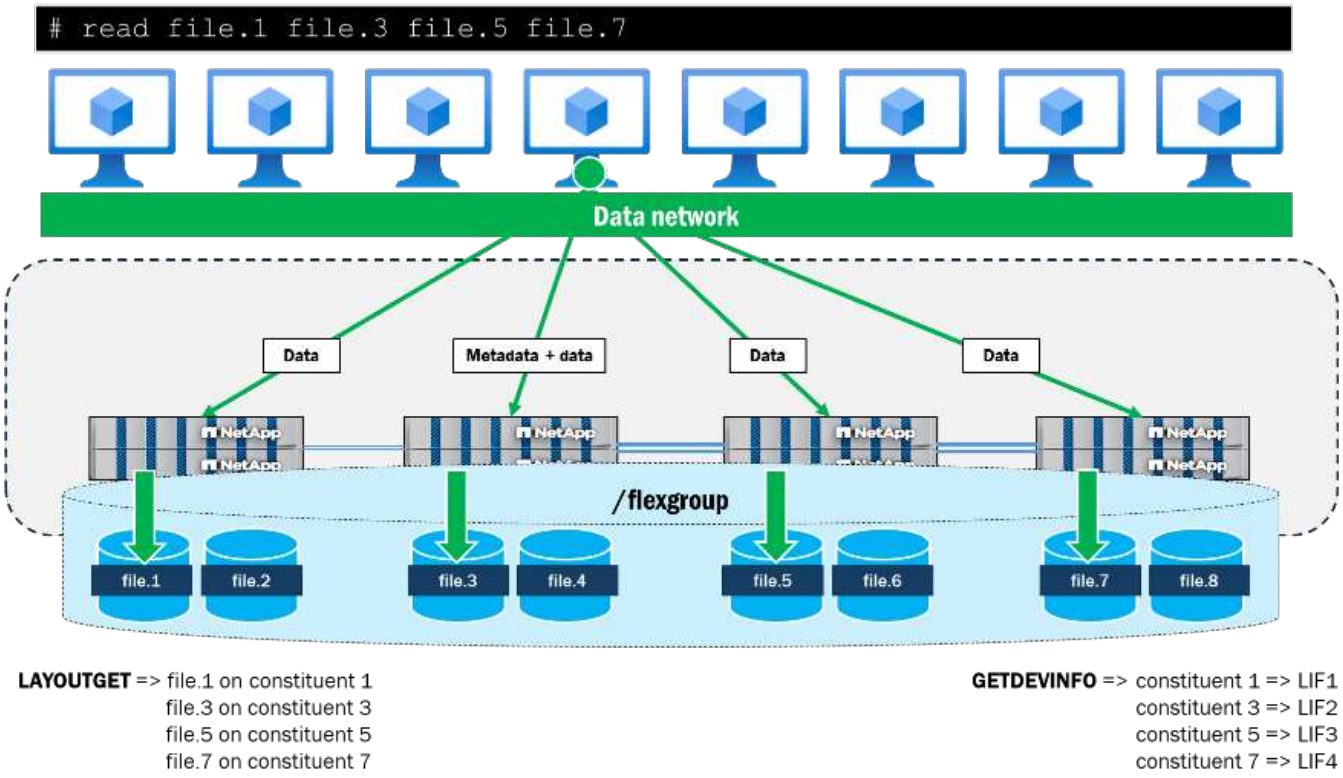


圖 **8.** 在**FlexGroup**卷中使用 **pNFS** 實現多個文件同時訪問

以下顯示的是在單一 RHEL 9.5 用戶端上進行簡單測試運行的結果，其中使用 dd 並行讀取四個 10GB 檔案（全部位於兩個ONTAP叢集節點的不同組成磁碟區上）。使用 pNFS 時，每個檔案的整體吞吐量和完成時間都提高了。當不使用 pNFS 而使用 NFSv4.1 時，掛載點本機檔案和遠端檔案之間的效能差異比使用 pNFS 時更大。

測試	每個檔案的吞吐量（**MB/s**）	每個文件的完成時間
NFSv4.1：無 pNFS	• 文件 1–228（本地） • 文件.2–227（本地） • 文件.3–192（遠端） • 文件.4–192（遠端）	• 文件 1–46（本地） • 文件.2–46.1（本地） • 文件.3–54.5（遠端） • 文件.4–54.5（遠端）
NFSv4.1：與 pNFS	• 文件 1–248（本地） • 文件.2–246（本地） • 文件.3–244（本地透過pNFS） • 文件.4–244（本地透過pNFS）	• 文件.1–42.3（本地） • 文件.2–42.6（本地） • 文件.3–43（本地透過pNFS） • 文件 4–43（本地透過 pNFS）

相關資訊

- "資料區管理FlexGroup"
- "NetApp技術報告 4571： FlexGroup最佳實踐"

ONTAP中的 **pNFS** 用例

pNFS 可以與ONTAP 的各種功能一起使用，以提高效能並為 NFS 工作負載提供更大的靈活性。

使用 **nconnect** 的 **pNFS**

NFS 為一些較新的客戶端和伺服器引入了一種新的掛載選項，該選項提供了一種在掛載單一 IP 位址的同時提供多個 TCP 連線的方法。這提供了一種機制，可以更好地並行化操作，繞過 NFS 伺服器和客戶端的限制，並有可能為某些工作負載提供更高的整體效能。 ONTAP 9.8 及更高版本支援 nconnect，前提是用戶端支援 nconnect。

當使用 nconnect 連接 pNFS 時，將使用 nconnect 選項並行連接 NFS 伺服器通告的每個 pNFS 裝置。例如，如果 nconnect 設置為 4，並且有 4 個符合 pNFS 條件的接口，則每個掛載點創建的連接總數最多為 16 個（4 個 nconnect x 4 個 IP 位址）。

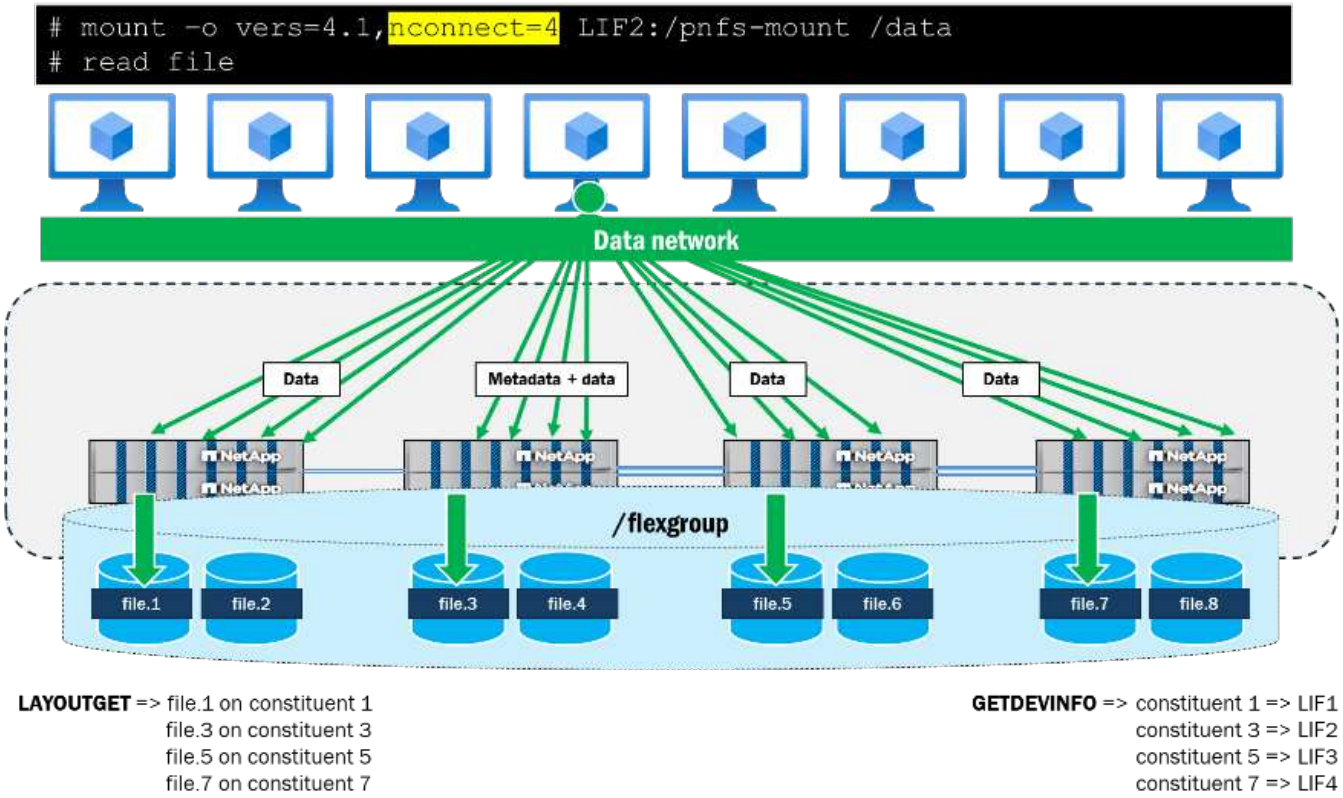


圖 **9. pNFS** 的 **nconnect** 設定為 **4**

"了解更多關於ONTAP對 NFSv4.1 的支持"

pNFS 與 **NFSv4.1** 會話中繼

NFSv4.1 會話中繼 ("RFC 5661，第 2.10.5 節") 是指在客戶端和伺服器之間使用多個 TCP 連線來提高資料傳輸速度。ONTAP 9.14.1 新增了對 NFSv4.1 會話中繼的支持，必須與也支援會話中繼的用戶端一起使用。

在ONTAP中，會話中繼可以跨叢集中的多個節點使用，以提供額外的吞吐量和連接冗餘。

會話中繼可以透過多種方式建立：

- 透過掛載選項自動發現： 大多數現代 NFS 用戶端可以透過掛載選項建立會話中繼（請查看您的作業系統供應商的文件），該選項會向 NFS 伺服器發出訊號，以便將有關會話中繼的資訊傳送回用戶端。此資訊以 NFS 資料包的形式出現。 `fs_location4` 稱呼。

  所使用的掛載選項取決於客戶端的作業系統版本。例如，Ubuntu Linux 的各種版本通常使用 `max_connect=n` 表示要使用會話中繼。在 RHEL Linux 發行版中， `trunkdiscovery` 使用了掛載選項。

  Ubuntu 範例

  ```
  mount -o vers=4.1,max_connect=8 10.10.10.10:/pNFS /mnt/pNFS
  ```

  RHEL 範例

  ```
  mount -o vers=4.1,trunkdiscovery 10.10.10.10:/pNFS /mnt/pNFS
  ```

如果您嘗試使用 `max_connect` 在 RHEL 發行版上，它將被視為 nconnect，會話中繼將無法如預期般運作。

- 手動建立： 您可以透過將每個單獨的 IP 位址掛載到相同的匯出路徑和掛載點來手動建立會話中繼。例如，如果同一個節點上有兩個 IP 位址（10.10.10.10 和 10.10.10.11），用於匯出路徑，`/pNFS`你需要運行兩次 mount 指令：

```
mount -o vers=4.1 10.10.10.10:/pNFS /mnt/pNFS
mount -o vers=4.1 10.10.10.11:/pNFS /mnt/pNFS
```

對所有要參與主幹的介面重複此程序。

每個節點都有自己的會話主幹。主幹不經過節點。

使用 pNFS 時，僅使用會話中繼_或_ nconnect。同時使用兩者會導致不良行為，例如只有元資料伺服器連線才能獲得 nconnect 的好處，而資料伺服器只能使用單一連線。

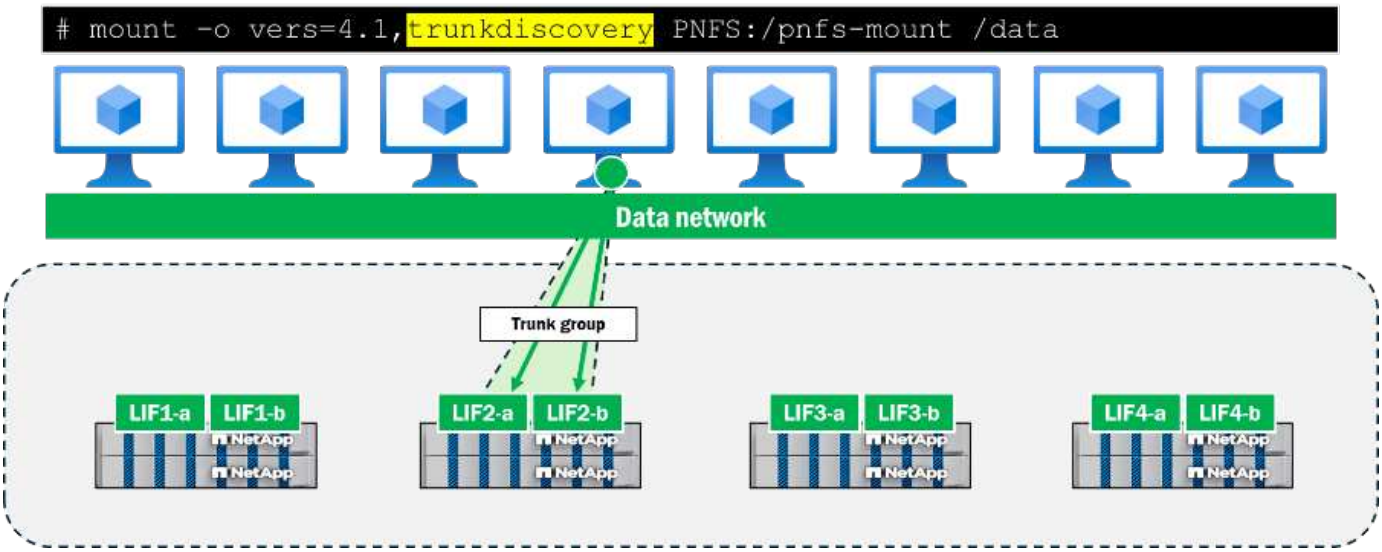
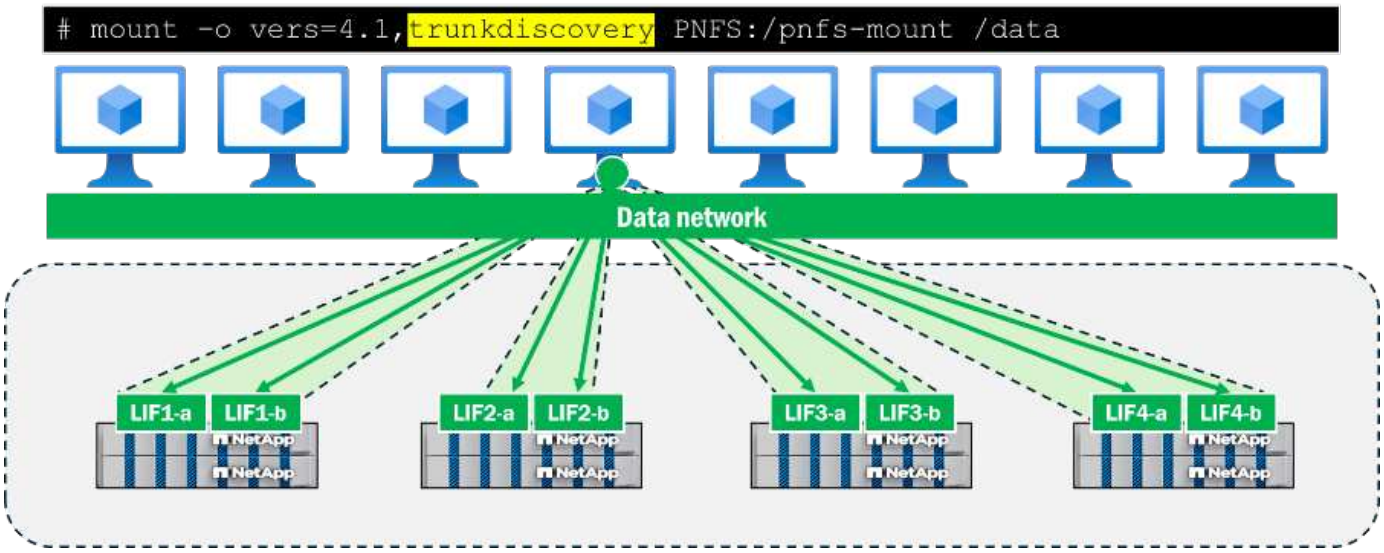


圖 **10. ONTAP**中的 **NFSv4.1** 會話中繼

pNFS 可以為叢集中的每個參與節點提供本機路徑，並且當與會話中繼一起使用時，pNFS 可以利用每個節點的會話中繼來最大限度地提高整個叢集的吞吐量。



什麼時候 `trunkdiscovery` 如果使用，則會利用附加的 GETATTR 呼叫 (FS_Locations) 來取得 NFS 伺服器節點上所列的會話中繼接口，該節點是掛載介面所在的位置。一旦這些位址返回，後續的掛載點就會指向返回的位址。這可以從掛載過程中的資料包擷取中看出。

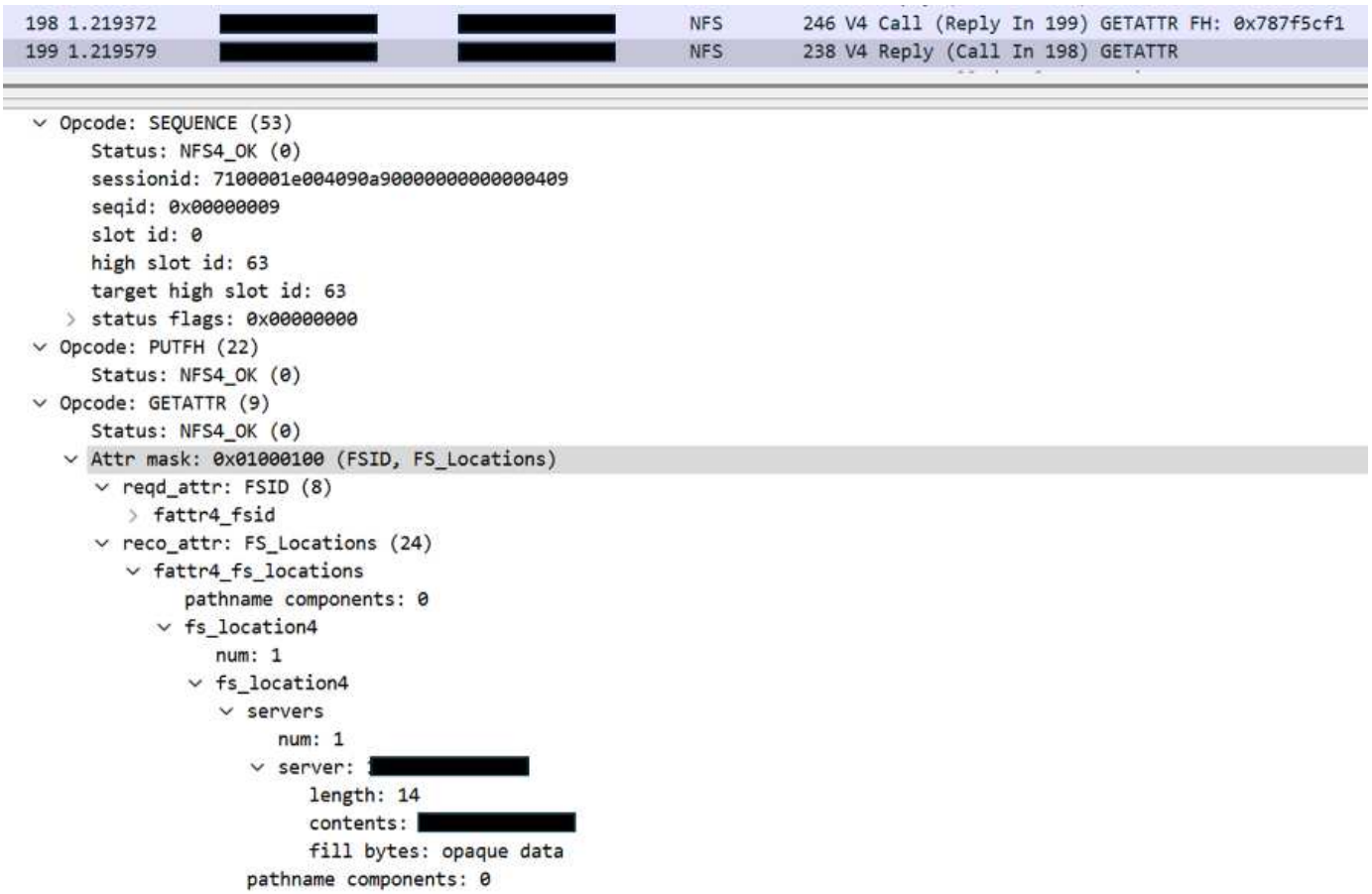


圖 **11.** 掛載期間的 **NFS** 會話主幹發現：資料包捕獲

"了解更多關於NFS中繼的信息"

pNFS 與 **NFSv4.1** 轉診

NFSv4.1 參考提供了一種初始掛載路徑重新導向模式，該模式會在發出掛載請求時將用戶端引導至磁碟區的位

置。NFSv4.1 轉介功能在單一 SVM 內運作。此功能嘗試將 NFS 掛載點定位到與資料磁碟區位於相同節點上的網路介面。如果該介面或磁碟區在掛載到客戶端時移動到另一個節點，則資料路徑將不再本地化，直到建立新的掛載點為止。

pNFS 不會嘗試定位掛載路徑。相反，它會使用掛載路徑建立一個元資料伺服器，然後根據需要動態地本地化資料路徑。

NFSv4.1 引用可以與 pNFS 一起使用，但此功能沒有必要。啟用 pNFS 的轉診功能不會產生明顯效果。

"啟用或停用 NFSv4 引用"

pNFS與高階容量平衡的交互

"進階容量平衡" ONTAP會將檔案資料的一部分寫入FlexGroup磁碟區的各個組成磁碟區（單一FlexVol磁碟區不支援此功能）。隨著檔案的成長， ONTAP決定開始將資料寫入不同的組成磁碟區上的新的多部分 inode，該組成磁碟區可能位於同一節點上，也可能位於不同的節點上。對這些多 inode 檔案進行的寫入、讀取和元資料操作對客戶端是透明的，不會造成乾擾。先進的容量平衡技術改善了FlexGroup各組成磁碟區之間的空間管理，從而提供了更穩定的效能。

pNFS 可以根據 NFS 伺服器中儲存的檔案佈局訊息，將資料 I/O 重新導向到本機網路路徑。當一個大檔案被分成多個部分，分佈在多個組成磁碟區中，而這些磁碟區可能跨越叢集中的多個節點時， ONTAP中的 pNFS 仍然可以為每個檔案部分提供本機流量，因為ONTAP也維護了所有檔案部分的檔案佈局資訊。讀取檔案時，資料路徑的局部性會根據需要而改變。

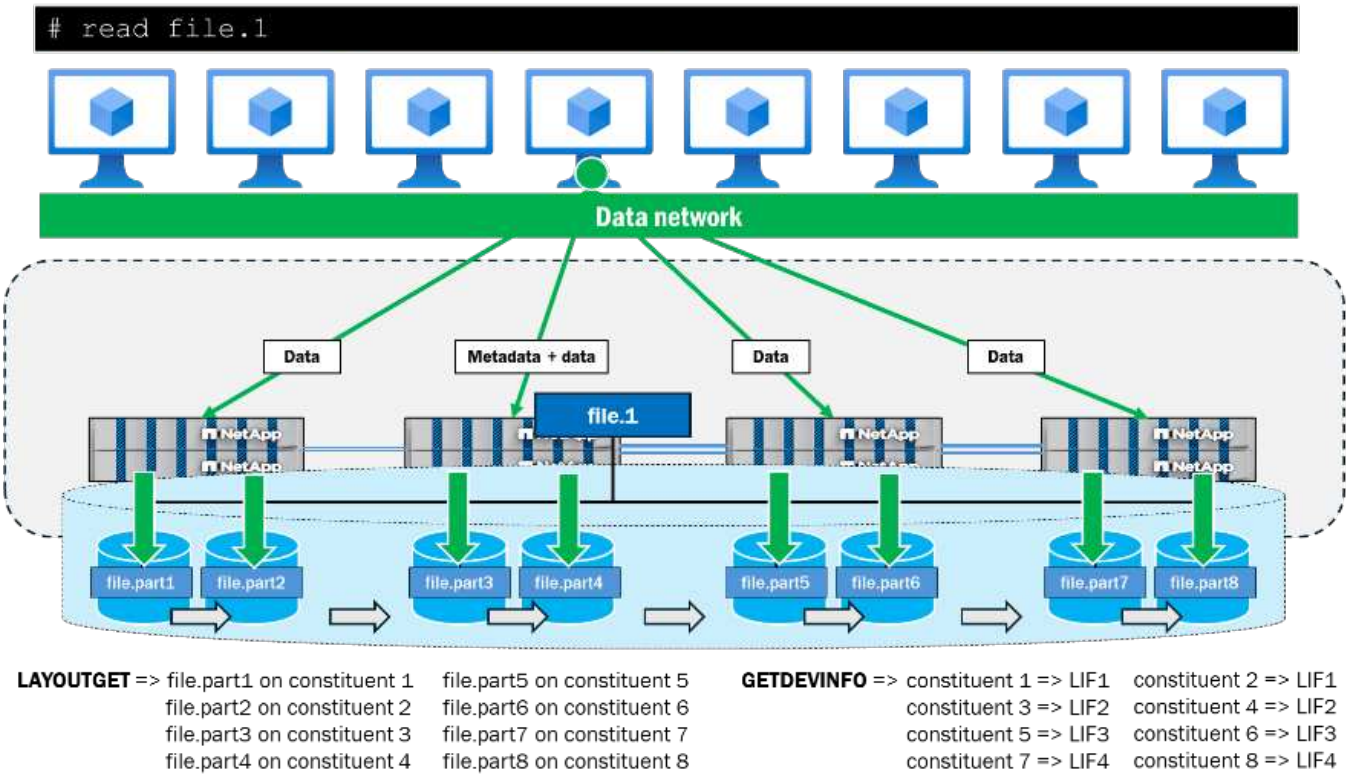


圖 **12.** 基於 **pNFS** 的高階容量平衡

相關資訊

- "FlexGroup卷配置"

pNFS 的引入是為了改進傳統的 NFS，它分離元資料和資料路徑，提供資料本地化，並支援平行操作。

傳統NFS的挑戰與pNFS的優勢

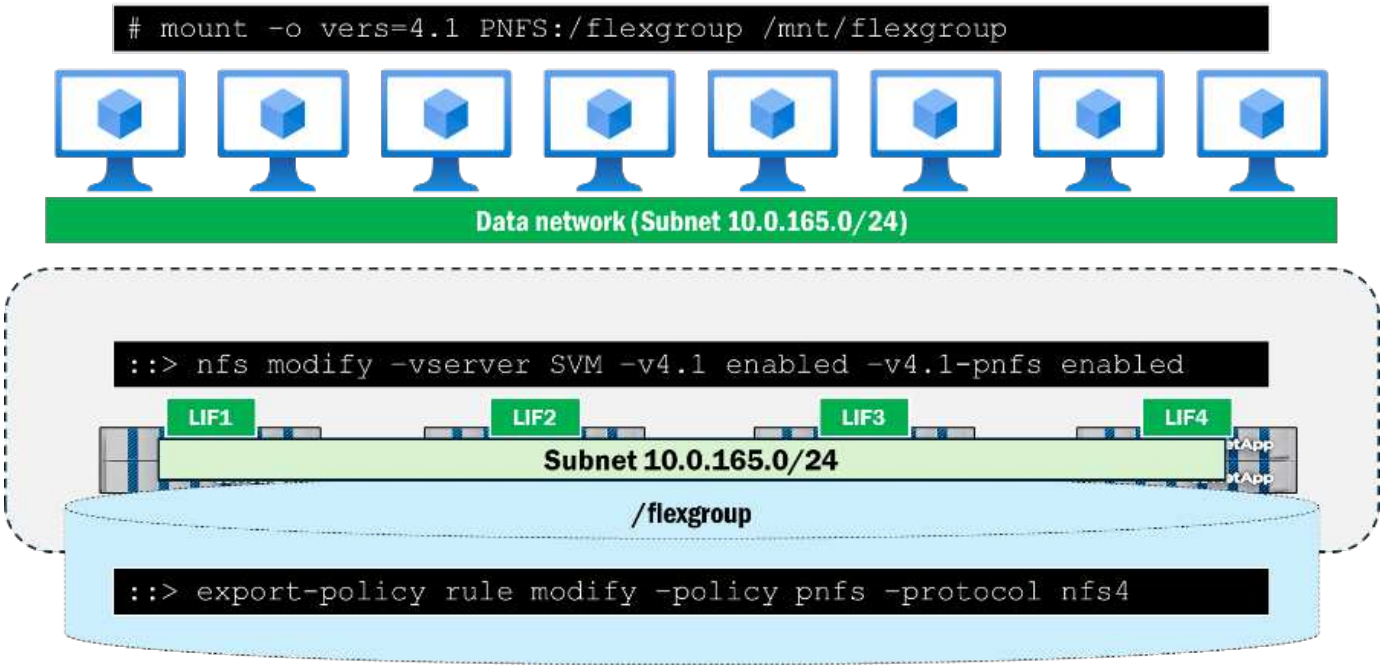
下表列出了傳統 NFS 面臨的挑戰，並解釋了ONTAP中的 pNFS 如何解決這些挑戰。

挑戰	pNFS 獲益
元資料和資料走同一條路徑 在傳統的 NFS 中，元資料和資料走同一條路徑，這可能會導致網路和 CPU 飽和，因為一條路徑會連接到叢集中的單一硬體節點。當許多用戶嘗試存取同一個 NFS 匯出時，這種情況會更加嚴重。	元資料和資料路徑分離，資料路徑並行化 透過分離 NFS 流量的元資料和資料路徑，並為資料路徑提供多條網路路徑， ONTAP叢集中的 CPU 和網路資源得到最大化利用，從而提高了工作負載的擴展性。
工作負載分配挑戰 在ONTAP NAS 叢集中，最多可以有 24 個節點，每個節點都可以有自己的一組資料捲和網路介面。每個磁碟區都可以承載自己的工作負載，或是工作負載的子集；而使用FlexGroup卷，為了簡化操作，工作負載可以存在於存取單一命名空間的多個節點上。當客戶端掛載 NFS 匯出時，網路流量將在單一節點上建立。當被存取的資料位於叢集中的單獨節點上時，就會發生遠端流量，這會增加工作負載的延遲和管理的複雜性。	本地並行資料結構路徑 由於 pNFS 將資料路徑與元資料分離，並根據磁碟區在叢集中的位置提供多個並行資料路徑，因此可以透過減少叢集中網路流量的距離以及利用叢集中的多個硬體資源來降低延遲。此外，由於ONTAP中的 pNFS 會自動重新導向資料流量，管理員無需管理多個匯出路徑和位置。
NFS 掛載點遷移 掛載點建立後，卸載並重新掛載磁碟區會造成乾擾。ONTAP提供了在節點之間遷移網路介面的功能，但這會增加管理開銷，並且會對使用 NFSv4.x 的有狀態 NFS 連線造成乾擾。重新定位掛載點的部分原因與資料本地性挑戰有關。	自動路徑重定位 使用 pNFS 時，NFS 伺服器會維護一個網路介面和磁碟區位置的表。當客戶端透過 pNFS 中的元資料路徑請求資料結構時，伺服器將向客戶端提供最佳化的網路路徑，然後客戶端將使用該路徑進行資料操作。這大大降低了工作負載的管理開銷，並且在某些情況下可以提高效能。

配置要求

在NetApp ONTAP中設定 pNFS 需要以下步驟：

- 支援 pNFS 且掛載於 NFSv4.1 或更高版本的 NFS 用戶端
- ONTAP中的 NFS 伺服器已啟用 NFSv4.1 (`nfs modify -v4.1 enabled`（預設為關閉）
- ONTAP中的 NFS 伺服器已啟用 pNFS (`nfs modify -v4.1-pnfs enabled`（預設為禁用）
- 每個節點至少需要一個可路由至 NFS 用戶端的網路介面。
- SVM 中具有允許 NFSv4 導出策略和規則的資料卷



滿足上述配置要求後，pNFS 即可自行運作。

相關資訊

- "NFS 組態"
- "ONTAP對 NFSv4.1 的支持"
- "pNFS 的網路介面連接"

規劃

pNFS部署計劃

在您的環境中部署 pNFS 之前，請確保滿足先決條件，並了解互通性要求和配置限制。

先決條件

在ONTAP中啟用和使用 pNFS 之前，請確保符合以下要求：

- NFS伺服器上已啟用NFSv4.1或更高版本
- 至少一個 "每個節點都存在資料 LIF。" 在託管 NFS 伺服器的 SVM 叢集中
- 全部 "SVM 中的資料 LIF 是可路由的" 致 NFS 用戶端
- NFS 用戶端支援 pNFS（2014 年及以後的大多數現代 Linux 發行版均支援）。
- 客戶端與SVM中所有資料LIF之間的網路連線正常
- 所有資料 LIF 的 DNS 解析（如果使用主機名稱）均已正確配置。
- "資料量FlexGroup" 已配置（建議使用以獲得最佳效果）
- "NFSv4.x ID 域匹配" 客戶與ONTAP之間
- "NFS Kerberos" （如果使用）在 SVM 中的所有資料 LIF 上啟用。

最佳實務總結

在您的環境中部署 pNFS 時，請遵循以下最佳實務：

- 使用 "資料量FlexGroup" 為了獲得最佳性能和容量擴展性
- 確保所有 "SVM中的網路介面是可路由的。" 致客戶
- "停用NFSv4.0" 確保客戶端使用 NFSv4.1 或更高版本
- 分散掛載點到多個網路介面和節點
- 使用輪詢 DNS "負載平衡元資料伺服器"
- 核實 "NFSv4.x ID 域匹配" 在客戶端和伺服器上
- 執行 "網路介面遷移" 和 "儲存故障轉移" 維護窗口期
- 使能夠 "NFS Kerberos" 如果使用 Kerberos 安全機制，則所有資料 LIF 都會受到影響。
- 避免使用 "NFSv4.1 轉介" 使用 pNFS 時
- 測試 "nconnect 設定" 謹慎操作，避免超出 TCP 連線限制
- 考慮 "會話中繼" 作為替代方案 "n 連接" （請勿同時使用兩者）
- 核實 "客戶端作業系統供應商支持" 部署前先對 pNFS 進行處理

互通性

ONTAP中的 pNFS 設計用於與符合 RFC 標準的 NFS 用戶端搭配使用。以下幾點要考慮：

- 最現代 "2014 年及以後的 Linux 發行版" 支援 pNFS（RHEL 6.4、Fedora 17 及更高版本）
- 請向您的用戶端作業系統供應商確認是否支援 pNFS。
- pNFS 可與FlexVol和 "資料量FlexGroup"
- pNFS 支援 NFSv4.1 和 "NFSv4.2"
- pNFS 可以與…一起使用 "NFS Kerberos" （krb5、krb5i、krb5p），但性能可能會受到影響
- pNFS 可以與…一起使用 "n 連接" 或者 "會話中繼" （但不能同時進行）
- pNFS 無法在 "NFSv4.0"

限制

以下限制適用於ONTAP中的 pNFS：

- "TCP 連線限制" 每個節點的具體限制因平台而異（請查看NetAppHardware Universe以了解特定限制）。
- 最大檔案大小：取決於磁碟區類型和ONTAP版本
- 最大文件數：最多 2000 億個文件 "資料量FlexGroup"
- 最大容量：高達 60 PB "資料量FlexGroup"
- "網路介面數量"每個節點至少需要一個資料 LIF；負載平衡可能需要更多。

使用時 "nconnect 與 pNFS"請注意，TCP 連線數會迅速成長：

- 每個使用 nconnect 的客戶端掛載都會為每個資料 LIF 建立多個 TCP 連線。
- 由於許多客戶使用了較高的 nconnect 值， "TCP 連線限制" 可以超過
- TCP連線數超過限制會阻止建立新連接，直到現有連線被釋放為止。

相關資訊

- "pNFS 的網路介面連接"
- "啟用或停用 NFSv4.1"
- "ONTAP對 NFSv4.1 的支持"
- "ONTAP對 NFSv4.2 的支持"
- "NetApp Hardware Universe"

pNFS調優與效能最佳實踐

在ONTAP中使用 pNFS 時，請遵循以下注意事項和最佳實踐，以獲得最佳結果。

容量類型推薦

ONTAP中的 pNFS 可以與FlexVol捲和FlexGroup磁碟區一起使用，但為了獲得最佳的整體效果，請使用FlexGroup磁碟區。

FlexGroup卷提供：

- 單一掛載點可以跨越叢集中的多個硬體資源，同時允許 pNFS 本地化資料流量。
- 海量儲存容量（高達 60 PB）和高檔案數量（高達 2000 億個檔案）
- 支援多部分文件以實現容量平衡和潛在的性能優勢
- 支援對單一工作負載的捲和硬體進行並行訪問

"了解FlexGroup磁碟區管理"

客戶推薦

並非所有 NFS 用戶端都支援 pNFS，但大多數現代客戶端都支援。 RHEL 6.4 和 Fedora 17 是最早支援 pNFS 的用戶端（大約在 2014 年），因此可以合理地假設過去幾年發布的客戶端版本都完全支援此功能。ONTAP 對 NFS 的支援立場是「如果用戶端支援該功能且符合 RFC 標準，而我們也支援該功能，那麼這種組合就是受支援的」。但是，最佳實踐是確保客戶端作業系統供應商支援 pNFS。

成交量變動

ONTAP能夠以非中斷的方式在同一叢集中的節點或聚合之間移動捲，從而提供容量和效能平衡的靈活性。當ONTAP中發生磁碟區移動時，pNFS 設備對應會自動更新，以便在必要時通知客戶端使用新的捲到介面關係。

"了解如何移動卷"

網路介面遷移

ONTAP能夠將網路介面遷移到同一叢集中的不同節點，從而實現效能平衡和維護靈活性。與磁碟區遷移類似，

當ONTAP中發生網路介面遷移時，pNFS 設備對應會自動更新，以便在必要時通知用戶端使用新的捲到介面關係。

然而，由於 NFSv4.1 是有狀態協議，網路介面遷移可能會對正在積極使用 NFS 掛載的客戶端造成乾擾。最佳實踐是在維護視窗期間進行網路介面遷移，並通知客戶可能出現的網路中斷。

儲存故障轉移/恢復

pNFS 遵循與 NFSv4.1 相同的儲存故障轉移考量。這些內容在下文有詳細介紹。 "NetApp技術報告4067：NFS最佳實務與實作指南"一般來說，任何涉及 pNFS 的儲存故障轉移/復原都應該在維護視窗內進行，由於協定的狀態性，可能會出現儲存中斷。

元資料工作負載

元資料操作的規模很小，但數量可能很大，具體取決於工作負載（您是否正在建立大量檔案？）您是否正在執行“查找”命令？ ）以及文件總數。因此，元資料呼叫量高的工作負載會佔用 NFS 伺服器大量的 CPU 資源，並可能導致單一連線瓶頸。 pNFS（以及一般的 NFSv4.x）並不適合對效能要求較高的元資料工作負載，因為該協定版本的狀態性、鎖定機制以及某些安全特性會對 CPU 使用率和延遲產生負面影響。這些工作負載類型（例如高 GETATTR 或 SETATTR）通常在 NFSv3 中表現較好。

元資料伺服器

pNFS 中的元資料伺服器是在 NFS 匯出首次掛載時建立的。安裝點一旦建立，就會一直保持原位，直到重新安裝或移動資料介面為止。因此，最佳實務是確保多個客戶端存取同一磁碟區時掛載到 SVM 的不同節點和資料介面。這種方法可以實現跨節點和 CPU 資源的元資料伺服器負載平衡，同時最大限度地利用叢集中的網路介面。實現此目的的一種方法是建立輪詢 DNS 設置，這在下文中有所介紹。 "NetApp技術報告 4523： ONTAP中的 DNS 負載平衡"。

NFSv4.x ID 域

NFSv4.x 透過多種方式提供安全功能（詳見下文）。 "NetApp技術報告4067：NFS最佳實務與實作指南" ）。NFSv4.x ID 網域是實作 NFS 匯出時客戶端和伺服器必須就 ID 網域進行驗證的方法之一。ID 網域不匹配的副作用之一是，使用者或群組會顯示為匿名使用者（本質上是被壓制），以防止未經授權的存取。對於 NFSv4.x（以及 pNFS），最佳實踐是確保客戶端和伺服器上的 NFSv4.x ID 網域匹配。

n 連接

如前所述， ONTAP中的 nconnect 可以幫助提高某些工作負載的效能。對於 pNFS，需要了解的是，雖然 nconnect 可以透過大幅增加與儲存系統的 TCP 連線總數來提高效能，但當許多客戶端利用掛載選項時，它也可能透過使儲存上的 TCP 連接過載而造成問題。NetAppHardware Universe涵蓋了每個節點的 TCP 連線限制。

當節點的 TCP 連線數超過限制時，在現有連線釋放之前，不允許建立新的 TCP 連線。這可能會為可能遭遇暴風雪的地區帶來複雜情況。

下表顯示了使用 nconnect 的 pNFS 如何可能超出 TCP 連線限制：

客戶數量	**nconnect** 值	每個掛載點每個節點的潛在 **TCP** 連線總數
1.	4.	4.
100	4.	400
1000	8.	8000

客戶數量	**nconnect** 值	每個掛載點每個節點的潛在 **TCP** 連線總數
10000.	8.	80000
10000.	16.	160000 [1]

[1] 超出大多數ONTAP單節點 TCP 連線限制

NFSv4.1 工作階段主幹

ONTAP中的會話中繼可用於提高 NFSv4.x 掛載的吞吐量和路徑彈性。與 pNFS 一起使用時，叢集中的每個節點都可以建立會話中繼。但是，會話中繼需要每個節點至少兩個接口，而 pNFS 需要每個節點至少有一個接口才能按預期工作。此外，SVM 中的所有介面都必須能夠路由到 NFS 用戶端。同時使用 nconnect 時，會話中繼和 pNFS 無法正常運作。將 nconnect 和會話中繼視為互斥的功能。

"了解NFS中繼"

網路介面連接

pNFS 需要叢集中每個節點都具有可路由的網路介面才能正常運作。如果與託管 pNFS 的 NFS 伺服器位於同一 SVM 中，且存在其他無法路由到 NFS 用戶端的網路接口，則ONTAP仍會在設備映射中向客戶端通告這些接口。當 NFS 用戶端嘗試透過不同子網路中的介面存取資料時，將無法連接，導致服務中斷。最佳實踐是，在使用 pNFS 時，只允許 SVM 中的網路介面可供客戶端存取。

> ⓘ 預設情況下，pNFS 要求 SVM 中的任何資料 LIF 都可路由到 NFS 用戶端上的接口，因為 pNFS 設備清單將填入 SVM 中的任何資料 LIF。因此，可能會選擇不可路由的資料 LIF，這可能會造成中斷情況。最佳實踐是，僅在使用 pNFS 時配置可路由資料 LIF。
>
> 從ONTAP 9.18.1 RC1 及更高版本開始，您可以按子網路指定哪些介面符合 pNFS 流量的條件，從而允許混合使用可路由介面和不可路由介面。請聯絡NetApp支援部門以取得有關指令的資訊。

NFSv4.0

NFSv4.0 是ONTAP NFS 伺服器中可以與 NFSv4.1 一起啟用的選項。但是，pNFS 不能在 NFSv4.0 上運作。如果 NFS 伺服器啟用了 NFSv4.0，則用戶端可能會在不知情的情況下掛載該協定版本，並且無法利用 pNFS。因此，在使用 pNFS 時，最佳實踐是明確停用 NFSv4.0。NFSv4.1 仍需啟用，並且可以獨立於 NFSv4.0 運作。

NFSv4.1 轉介

NFSv4.1 引用會將客戶端的掛載路徑本地化到擁有該磁碟區的節點上的網路介面。 pNFS 在地化資料路徑，而掛載路徑則成為元資料伺服器。

雖然這兩個功能可以實際一起使用，但將 NFSv4.1 引用與 pNFS 一起使用可能會導致在同一節點上堆疊多個元資料伺服器，從而降低將元資料伺服器分散到多個叢集節點的能力，這種效果並不理想。在使用 pNFS 時，如果元資料伺服器沒有均勻分佈在叢集中，那麼單一節點的 CPU 可能會被元資料請求淹沒，從而造成效能瓶頸。

因此，在使用 pNFS 時，最好避免使用 NFSv4.1 引用。相反，應將掛載點分散到叢集中的多個網路介面和節點上。

"了解如何啟用或停用 NFSv4 轉儲"

NFS Kerberos

使用 NFS Kerberos，可以對 krb5 進行身份驗證加密，並進一步對封包進行 krb5i 和 krb5p 加密。在SVM中，此功能是基於每個網路介面啟用的，詳情請參見[此處]。 "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"。

由於 pNFS 可以將資料流量重定向到 SVM 中的節點和網路接口，因此 SVM 中的每個網路介面都必須啟用 NFS Kerberos 並使其正常運作。如果 SVM 中的任何網路介面未啟用 Kerberos，則 pNFS 在嘗試存取這些介面上的資料磁碟區時將無法正常運作。

例如，當在具有兩個網路介面（只有一個啟用了 Kerberos）的 pNFS 支援的 SVM 上使用並行 dd 運行讀取測試時，位於啟用了 Kerberos 的介面上的檔案效能良好，而位於未啟用 Kerberos 的介面上的節點上的檔案始終無法完成讀取。當兩個介面都啟用 Kerberos 時，所有檔案都能如預期運作。

只要在 SVM 的所有網路介面上啟用了 NFS Kerberos，NFS Kerberos 就可以與 pNFS 一起使用。請記住，由於封包的加密/解密，NFS Kerberos 可能會造成效能損失，因此最佳實踐是使用工作負載徹底測試 pNFS 與 NFS Kerberos，以確保任何效能損失都不會對工作負載造成過大的影響。

下面是一個在 RHEL 9.5 用戶端上使用 pNFS 並結合 krb5（身份驗證）和 krb5p（端對端加密）時的平行讀取效能範例。Krb5p 在這項測試中表現下降了 70%。

克爾貝羅斯口味	**MB**/秒	完成時間
KRB5	• File1-243 • File2-243 • File3-238 • File4-238	• File1-43 • File2-43.1 • File3-44 • File4-44.1
krb5p	• File1-72.9 • File2-72.8 • File3-71.4 • File4-71.2	• File1-143.9 • File2-144.1 • File3-146.9 • File4-147.3

"了解 NFS 中的 Kerberos，以實現強大的安全性"

NFSv4.2

NFSv4.2 已加入ONTAP 9.8 中，是目前可用的最新 NFSv4.x 版本 (RFC-7862)。NFSv4.2 沒有明確的選項來啟用/停用它。相反，它是與 NFSv4.1 一起啟用/停用的。（`-4.1 enabled`）。如果用戶端支援 NFSv4.2，則在掛載命令期間，除非另有指定，否則它將協商支援的最高 NFS 版本。 `minorversion=2` 安裝選項。

ONTAP中的 NFSv4.2 支援以下功能：

- 安全標籤（MAC標籤）
- 延伸屬性
- 稀疏文件操作（FALLOCATE）

pNFS 隨 NFSv4.1 引入，但也受 NFSv4.2 及其相關功能的支援。

"了解 ONTAP 對 NFSv4.2 的支持"

pNFS 指令、統計資料和事件日誌

這些ONTAP CLI 指令專門用於 pNFS。您可以使用它們進行配置、故障排除和收集統計資料。

啟用 **NFSv4.1**

```
nfs modify -vserver SVM -v4.1 enabled
```

啟用**pNFS**

```
nfs modify -vserver SVM -v4.1-pnfs enabled
```

顯示 **pNFS** 設備（進階權限）

```
pnfs devices show -vserver SVM
```

```
Vserver Name     Mapping ID      Volume MSID     Mapping Status
Generation
---------------  --------------- --------------- ---------------
-------------
SVM              17              2157024470      notavailable    2
SVM              18              2157024463      notavailable    2
SVM              19              2157024469      available       3
SVM              20              2157024465      available       4
SVM              21              2157024467      available       3
SVM              22              2157024462      available       1
```

顯示 **pNFS** 裝置對映（高階權限）

```
pnfs devices mappings show -vserver SVM
```

```
Vserver Name    Mapping ID      Dsid            LIF IP
--------------  --------------- --------------- --------------------
SVM             19              2449            10.x.x.x
SVM             20              2512            10.x.x.y
SVM             21              2447            10.x.x.x
SVM             22              2442            10.x.x.y
```

擷取 **pNFS** 特有的效能計數器（進階權限）

```
statistics start -object nfsv4_1 -vserver SVM -sample-id [optional-name]
```

查看 **pNFS** 特有的效能計數器（進階權限）

```
statistics show -object nfsv4_1 -vserver SVM
```

查看 **pNFS** 特有計數器清單（進階權限）

```
statistics catalog counter show -object nfsv4_1 -counter *layout*|*device*
```

```
Object: nfsv4_1

Counter                     Description
--------------------------- ----------------------------------------------
getdeviceinfo_avg_latency   Average latency of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_error         The number of failed NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_percent       Percentage of NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_success       The number of successful NFSv4.1 GETDEVICEINFO
operations.
getdeviceinfo_total         Total number of NFSv4.1 GETDEVICEINFO
operations.
getdevicelist_avg_latency   Average latency of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_error         The number of failed NFSv4.1 GETDEVICELIST
operations.
getdevicelist_percent       Percentage of NFSv4.1 GETDEVICELIST
operations.
getdevicelist_success       The number of successful NFSv4.1 GETDEVICELIST
operations.
getdevicelist_total         Total number of NFSv4.1 GETDEVICELIST
operations.
layoutcommit_avg_latency    Average latency of NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_error          The number of failed NFSv4.1 LAYOUTCOMMIT
operations.
layoutcommit_percent        Percentage of NFSv4.1 LAYOUTCOMMIT operations.
layoutcommit_success        The number of successful NFSv4.1 LAYOUTCOMMIT
```

```
operations.
layoutcommit_total          Total number of NFSv4.1 LAYOUTCOMMIT
operations.
layoutget_avg_latency       Average latency of NFSv4.1 LAYOUTGET
operations.
layoutget_error             The number of failed NFSv4.1 LAYOUTGET
operations.
layoutget_percent           Percentage of NFSv4.1 LAYOUTGET operations.
layoutget_success           The number of successful NFSv4.1 LAYOUTGET
operations.
layoutget_total             Total number of NFSv4.1 LAYOUTGET operations.
layoutreturn_avg_latency    Average latency of NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_error          The number of failed NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_percent        Percentage of NFSv4.1 LAYOUTRETURN operations.
layoutreturn_success        The number of successful NFSv4.1 LAYOUTRETURN
operations.
layoutreturn_total          Total number of NFSv4.1 LAYOUTRETURN
operations.
```

查看 **NFS** 的活動網路連接

您可以使用以下命令驗證是否與 SVM 建立了多個 TCP 連線： `network connections active show` 命令。

例如，如果要查看 NFS 會話中繼，請尋找來自相同客戶端在每個節點的不同介面上的連線：

```
cluster::*> network connections active show -node cluster-0* -vserver PNFS
              Vserver   Interface         Remote
      CID Ctx Name      Name:Local Port   Host:Port
Protocol/Service
--------- --- --------- ----------------- --------------------
----------------
Node: node-01
2304333128 14 PNFS      data1:2049        ubuntu22-224:740     TCP/nfs
2304333144 10 PNFS      data3:2049        ubuntu22-224:864     TCP/nfs
2304333151  5 PNFS      data1:2049        ubuntu22-226:848     TCP/nfs
2304333167 15 PNFS      data3:2049        ubuntu22-226:684     TCP/nfs
Node: node-02
2497668321 12 PNFS      data2:2049        ubuntu22-224:963     TCP/nfs
2497668337 18 PNFS      data4:2049        ubuntu22-224:859     TCP/nfs
2497668344 14 PNFS      data2:2049        ubuntu22-226:675     TCP/nfs
2497668360  7 PNFS      data4:2049        ubuntu22-226:903     TCP/nfs
```

查看已連接客戶端的 **NFS** 版本信息

您也可以使用以下方式查看 NFS 連線： `nfs connected-clients show` 命令。請注意，此處顯示的客戶名單是過去 48 小時內有活躍 NFS 流量的客戶。空閒的 NFS 用戶端（即使仍然掛載）可能要等到存取掛載點時才會顯示出來。您可以透過指定以下參數來篩選這些客戶端，使其僅顯示最近造訪過的用戶端： `-idle-time` 特徵。

例如，要查看過去 10 分鐘內 pNFS SVM 中有活動的客戶：

```
cluster::*> nfs connected-clients show -vserver PNFS -idle-time <10m>

 Node: node-01

Vserver: PNFS Data-Ip: 10.x.x.x Local Remote Client-Ip Protocol Volume
Policy Idle-Time Reqs Reqs Trunking

10.x.x.a nfs4.2 PNFS_root default 9m 10s 0 149 false 10.x.x.a nfs4.2
FG_0001 default 9m 10s 135847 0 false 10.x.x.b nfs4.2 PNFS_root default 8m
12s 0 157 false 10.x.x.b nfs4.2 FG_0001 default 8m 12s 52111 0 false
```

相關資訊

- "了解ONTAP中的平行 NFS (pNFS)"

NFS和SMB檔案及目錄命名相依性

了解 **ONTAP NFS** 和 **SMB** 檔案和目錄命名依賴關係

檔案和目錄命名慣例取決於網路用戶端的作業系統和檔案共用傳輸協定、以及ONTAP 在叢集和用戶端上的語言設定。

作業系統和檔案共用傳輸協定決定下列事項：

- 檔案名稱可使用的字元
- 檔案名稱的大小寫敏感度

根據發行版的資訊、支援檔案、目錄和qtree名稱中的多位元組字元。ONTAP ONTAP

了解 **ONTAP NFS SVM** 在不同作業系統中的有效字符

如果您從具有不同作業系統的用戶端存取檔案或目錄、則應使用兩個作業系統中有效的字元。

例如、如果您使用UNIX建立檔案或目錄、請勿在名稱中使用分號（：）、因為在MS－DOS檔案或目錄名稱中不允許使用分號。由於有效字元的限制因作業系統而異、請參閱用戶端作業系統的說明文件、以取得有關禁止字元的詳細資訊。

了解 **ONTAP NFS** 多協定環境中檔案和目錄名稱的大小寫敏感性

檔案和目錄名稱對NFS用戶端區分大小寫、對SMB用戶端則不區分大小寫、但大小寫保留。您必須瞭解多重傳輸協定環境的影響、以及在建立SMB共用區時指定路徑以及存取共用區內資料時、可能需要採取的行動。

如果 SMB 用戶端建立名為的目錄 `testdir`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `testdir`。不過、如果 SMB 使用者稍後嘗試建立目錄名稱 `TESTDIR`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的目錄 `TESTDIR`NFS 和 SMB 用戶端會以不同方式顯示目錄名稱、如下所示：

- 例如、在 NFS 用戶端上、您會看到兩個目錄名稱都是建立的 `testdir` 和 `TESTDIR`，因爲目錄名稱區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個目錄。一個目錄有基礎檔案名稱。其他目錄會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `testdir` 和 `TESTDI~1`。
  - ONTAP 會建立 `TESTDI~1` 用於區分兩個目錄的目錄名稱。

    在這種情況下、您必須在建立或修改儲存虛擬機器（SVM）上的共用區時、使用8.3名稱來指定共用路徑。

同樣地、如果 SMB 用戶端建立檔案 `test.txt`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `text.txt`。不過、如果 SMB 使用者稍後嘗試建立 `Test.txt`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的檔案 `Test.txt`NFS 和 SMB 用戶端會以不同方式顯示檔案名稱、如下所示：

- 在 NFS 用戶端上、您會看到兩個檔案名稱都是建立的、 `test.txt` 和 `Test.txt`，因爲文件名區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個檔案。一個檔案有基礎檔案名稱。其他檔案會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP 會建立 `TEST~1.TXT` 檔案名稱可區分這兩個檔案。

> ⓘ 如果使用 vserver CIFS 字元對應命令建立字元對應、通常不區分大小寫的 Windows 查詢可能會變成區分大小寫的查詢。這表示只有在建立字元對應且檔案名稱使用該字元對應時、檔案名稱查詢才會區分大小寫。

了解如何建立 **ONTAP NFS** 檔案和目錄名稱

在任何可從SMB用戶端存取的目錄中、利用此程式建立並維護兩個檔案或目錄名稱：原始的長名稱和8.3格式的名稱。ONTAP

若檔案或目錄名稱超過八個字元名稱或三個字元副檔名限制（檔案）、ONTAP 則會產生8.3格式的名稱、如下所示：

- 如果名稱超過六個字元、則會將原始檔案或目錄名稱刪減為六個字元。
- 它會在檔案或目錄名稱中附加一個或多個數字（從一到五）、這些名稱在被截短後不再是唯一的。

  如果因為有五個以上的相似名稱而導致號碼不足、就會建立一個與原始名稱無關的唯一名稱。

- 如果是檔案、則會將副檔名縮短為三個字元。

例如、如果 NFS 用戶端建立名為的檔案 `specifications.html`，由 ONTAP 建立的 8.3 格式檔案名稱為 `specif~1.htm`。如果此名稱已經存在、ONTAP 則在檔案名稱結尾處使用不同的編號。例如、如果 NFS 用戶端接著建立另一個名為的檔案 `specifications_new.html`的 8.3 格式 `specifications_new.html` 是 `specif~2.htm`。

了解 **ONTAP NFS** 對多位元組檔案、目錄和 **qtree** 名稱的處理

從支援4位元組的UTF-8編碼名稱開始、即可建立及顯示包含基本多語言平面（BMP）以外之統一碼輔助字元的檔案、目錄和樹狀名稱。ONTAP在早期版本中、這些補充字元無法在多重傳輸協定環境中正確顯示。

若要啟用 4 位元組 UTF-8 編碼名稱的支援、可使用新的 *utf8mb4* 語言代碼 `vserver` 和 `volume` 命令系列。

- 您必須以下列其中一種方式建立新的Volume：
- 設定音量 `-language` 選項明確：

```
volume create -language utf8mb4 {…}
```

- 繼承 Volume `-language` SVM 中的選項、此選項已針對選項建立或修改：

```
vserver [create|modify] -language utf8mb4 {…}``volume create {…}
```

- 如果您使用的是 ONTAP 9.6 及更早版本、則無法修改現有的 Volume 以獲得 utf8mb4 支援；您必須建立新的 utf8mb4 就緒 Volume 、然後使用用戶端型複本工具移轉資料。

  如果您使用的是 ONTAP 9.7P1 或更新版本、您可以透過支援要求修改 utf8mb4 的現有磁碟區。如需詳細資訊、請參閱 "是否可以在 ONTAP 中建立後變更 Volume 語言？"。

  您可以更新SVM以取得utf8mb4支援、但現有磁碟區仍保留其原始語言代碼。

  目前不支援使用4位元組utf-8字元的LUN名稱。

- 在Windows檔案系統應用程式中、通常會使用16位元的統一碼轉換格式（UTF-16）來表示統一碼字元資料、在使用8位元的統一碼轉換格式（UTF-8）的NFS檔案系統中則代表統一碼字元資料。

  在發行版不含更新版本的版本中、Windows用戶端所建立的名稱（包括UTF-16輔助字元）會正確顯示給其他Windows用戶端、但不會正確轉譯為適用於NFS用戶端的UTF-8。ONTAP同樣地、已建立NFS用戶端的名稱若含有UTF-8補充字元、則無法正確轉譯為適用於Windows用戶端的UTF-16。

- 當您在執行ONTAP 包含有效或無效補充字元的系統上建立檔案名稱時ONTAP 、不接受檔案名稱、並傳回無效的檔案名稱錯誤。

  若要避免此問題、請在檔案名稱中僅使用BMP字元、避免使用補充字元、或升級ONTAP 至版本號（或更新版本）。

qtree名稱中允許使用統一碼字元。

- 您可以使用 `volume qtree` 命令系列或系統管理程式來設定或修改 qtree 名稱。

- qtree名稱可以包含多位元組的統一碼格式字元、例如日文和中文字元。
- 在版本不含支援的版本中、僅支援使用BMP字元（也就是可以以3個位元組表示的字元）ONTAP 。

> 在發行版之前的版本中、qtree父磁碟區的交會路徑可以包含qtree和含有統一碼字元的目錄名稱。ONTAP。 `volume show` 當父磁碟區具有 UTF-8 語言設定時、命令會正確顯示這些名稱。不過、如果父Volume語言不是UTF-8語言設定之一、則會使用數值NFS替代名稱來顯示交會路徑的某些部分。

- 在9.5及更新版本中、如果qtree位於啟用utf8mb4的Volume中、則qtree名稱中支援4位元組字元。

在 **ONTAP NFS** 磁碟區上配置 **SMB** 檔案名稱轉換的字元映射

NFS用戶端可以建立檔案名稱、其中包含對SMB用戶端和某些Windows應用程式無效的字元。您可以設定磁碟區上檔案名稱轉譯的字元對應、讓SMB用戶端能夠存取NFS名稱、否則將無效。

關於這項工作

當SMB用戶端存取NFS用戶端所建立的檔案時、ONTAP 即可查看檔案名稱。如果名稱不是有效的SMB檔案名稱（例如、如果名稱有內嵌的結腸「」字元）、ONTAP 則無法返回每個檔案所保留的8.3檔名。不過、這會對將重要資訊編碼成長檔名的應用程式造成問題。

因此、如果您要在不同作業系統上的用戶端之間共用檔案、則應該在兩個作業系統中都有效的檔案名稱中使用字元。

不過、如果您有NFS用戶端建立的檔案名稱包含SMB用戶端無效檔案名稱的字元、您可以定義將無效NFS字元轉換成SMB和某些Windows應用程式所接受的統一碼字元的對應。例如、此功能支援CATIA MCAD和Mathatica應用程式、以及其他有此需求的應用程式。

您可以依Volume設定字元對應。

在磁碟區上設定字元對應時、必須謹記下列事項：

- 字元對應不會套用至交叉點。

  您必須明確設定每個交會Volume的字元對應。

- 您必須確定用於表示無效或非法字元的unicode字元是通常不會出現在檔案名稱中的字元、否則會產生不必要的對應。

  例如、如果您嘗試將一個分號（：）對應至連字號（-）、但檔案名稱中正確使用連字號（-）、則嘗試存取名為「a-b」的檔案的Windows用戶端會將其要求對應至NFS名稱「a:b」（而非所需結果）。

- 套用字元對應之後、如果對應仍包含無效的Windows字元、ONTAP 則將還原為Windows 8.3檔名。
- 在FPolicy通知、NAS稽核記錄和安全追蹤訊息中、會顯示對應的檔案名稱。
- 建立DP類型的SnapMirror關係時、來源磁碟區的字元對應不會複寫到目的地DP磁碟區。
- 區分大小寫：由於對應的Windows名稱會變成NFS名稱、因此名稱的查詢會遵循NFS語義。這包括NFS查詢區分大小寫。這表示存取對應共用的應用程式不得仰賴Windows不區分大小寫的行為。但是8.3名稱是可用的、而且不區分大小寫。
- 部分或無效對應：在將名稱對應至執行目錄列舉（「dir」）的用戶端之後、會檢查所產生的UNICODE名稱

是否為Windows有效性。如果該名稱中仍有無效字元、或Windows的名稱無效（例如結尾為「.」或空白）、則會傳回8.3名稱而非無效名稱。

步驟

1. 設定字元對應：

```
vserver cifs character-mapping create -vserver vserver_name -volume
volume_name -mapping mapping_text, ...
```

對應包含以「」分隔的來源目標字元配對清單。這些字元是以十六進位數字輸入的統一碼字元。例如：3c：E03C。

每個值的第一個值 `mapping_text` 以冒號分隔的配對是您要轉譯之 NFS 字元的十六進位值、第二個值是 SMB 使用的 Unicode 值。對應配對必須是唯一的（一對一對應應該存在）。

- 來源對應

  下表顯示來源對應的允許UNICODE字元集：

統一碼字元	列印字元	說明
01-0x19	不適用	非列印控制字元
0x5C	\	反斜槓
x3A.	：	結腸
0X2A	*	星號
x3F	？	問號
x22	"	引號
x3C	<	小於
x3E	>	大於
x7C		
垂直線	0xB1	±

- 目標對應

  您可以在下列範圍內指定「Private Use Area」（私有使用區域）中的目標字元：u+E0000…U+F8FF。

範例

下列命令會在儲存虛擬機器（SVM）VS1上、針對名為「dATA」的磁碟區建立字元對應：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  -----------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

用於管理 **SMB** 檔案名稱轉換的字元對映的 **ONTAP NFS** 命令

您可以建立、修改、顯示有關資訊、或刪除FlexVol 在支援使用於支援SMB檔案名稱轉譯的檔案字元對應、來管理字元對應。

如果您想要…	使用此命令…
建立新的檔案字元對應	`vserver cifs character-mapping create`
顯示檔案字元對應的相關資訊	`vserver cifs character-mapping show`
修改現有的檔案字元對應	`vserver cifs character-mapping modify`
刪除檔案字元對應	`vserver cifs character-mapping delete`

如"指令參考資料ONTAP"需詳細 `vserver cifs character-mapping`資訊，請參閱。

管理 NFS 主幹

瞭解 ONTAP NFS 主幹

從 ONTAP 9.14.1 開始、 NFSv4.1 用戶端可以利用工作階段主幹功能、在 NFS 伺服器上開啟多個不同生命週期的連線、藉此提高資料傳輸速度、並透過多重路徑提供恢復能力。

Trunking 對於將 FlexVol 磁碟區匯出至具備主幹功能的用戶端（尤其是 VMware 和 Linux 用戶端）、或透過 RDMA 、 TCP 或 pNFS 匯出至 NFS 而言非常有利。

在 ONTAP 9.14.1 中、主幹僅限於單一節點上的生命負載、主幹無法跨越多個節點的生命負載。

FlexGroup 磁碟區支援主幹。雖然這可以提供更好的效能、但只能在單一節點上設定 FlexGroup Volume 的多重路徑存取。

本版本僅支援多重路徑的工作階段主幹。

如何使用主幹

若要善用主幹所提供的多重路徑優點、您需要一組生命（稱為 *truning group* ）、這些生命體與包含啟用主幹的

NFS 伺服器的 SVM 相關聯。主幹群組中的生命體必須在叢集的同一個節點上有主連接埠、而且它們必須位於這些主連接埠上。最佳做法是主幹群組中的所有生命都是同一個容錯移轉群組的成員。

ONTAP 可從指定的用戶端、每個節點最多支援 16 個中繼連線。

當用戶端從啟用主幹連線的伺服器掛載匯出時、會在主幹群組中指定多個用於生命的 IP 位址。用戶端連線至第一個 LIF 後、只會將額外的生命體新增至 NFSv4.1 工作階段、並在符合主幹群組需求的情況下用於主幹。然後用戶端會根據自己的演算法（例如循環配置資源）、透過多個連線來散佈 NFS 作業。

為了獲得最佳效能、您應該在專用於提供多重路徑匯出的 SVM 中設定主幹連線、而非單一路徑匯出。也就是說、您只應在 SVM 中的 NFS 伺服器上啟用主幹、該伺服器的匯出僅提供給啟用主幹的用戶端。

支援的用戶端

ONTAP NFSv4.1 伺服器支援主幹連線、可與任何能夠進行 NFSv4.1 工作階段主幹的用戶端連線。

下列用戶端已通過 ONTAP 9.14.1 測試：

- VMware - ESXi 7.0U3F 及更新版本
- Linux - Red Hat Enterprise Linux （ RHEL ） 8.8 和 9.3

如果在容錯移轉事件（例如控制器容錯移轉）中將主幹的生命體移轉至另一個節點， RHEL NFS 用戶端將不會重新建立主幹。當將生命體移轉至另一個節點時，它們會從主幹群組中移除。如果主幹群組中的所有生命體都已移轉， NFS 用戶端將只會使用第一個 LIF 來繼續 I/O

在 NFS 伺服器上啟用主幹時、在不支援主幹的 NFS 用戶端上存取匯出共用的使用者可能會看到效能下降。這是因為 SVM 資料生命期的多個掛載只會使用單一 TCP 連線。

NFS 主幹與 **nconnect** 之間的差異

從功能不支援的問題9.8開始ONTAP 、NFSv4.1啟用時、預設會提供nconnect功能。在具有 nconnect 功能的用戶端上、單一 NFS 裝載可透過單一 LIF 進行多個 TCP 連線（最多 16 個）。

相反地、主幹是 _ 多重路徑 _ 功能、可在多個生命體上提供多個 TCP 連線。如果您能夠在環境中使用額外的 NIC 、則主幹可提供比 nconnect 更高的平行度和效能。

深入瞭解 "n 連接"。

設定新的 **NFS** 伺服器並匯出以進行主幹連線

在 **ONTAP SVM** 上建立啟用主幹的 **NFS** 伺服器

從 ONTAP 9.14.1 開始、可在 NFS 伺服器上啟用主幹。在建立 NFS 伺服器時、預設會啟用 NFSv4.1 。

開始之前

建立啟用主幹的 NFS 伺服器需要 SVM 。SVM 必須：

- 有足夠的儲存設備作為後盾、可滿足用戶端資料需求。

- 已啟用 NFS 。

您可以使用現有的 SVM ；但是啟用主幹必須重新掛載所有 NFSv4.x 用戶端、這可能會造成中斷。如果無法重新掛載、請為 NFS 伺服器建立新的 SVM 。

步驟

1. 如果不存在合適的 SVM 、請建立一個：

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. 驗證新建立的SVM的組態和狀態：

   ```
   vserver show -vserver svm_name
   ```

   深入瞭解 "建立 SVM"。

3. 建立 NFS 伺服器：

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. 確認NFS正在執行：

   ```
   vserver nfs status -vserver svm_name
   ```

5. 確認NFS已設定為所需：

   ```
   vserver nfs show -vserver svm_name
   ```

   深入瞭解 "NFS 伺服器組態。"

完成後

視需要設定下列服務：

- "DNS"
- "LDAP"
- "Kerberos"

為 **ONTAP NFS** 主幹準備網路

若要善用 NFSv4.1 主幹、主幹群組中的生命體必須位於同一個節點上、且同一個節點上必須有主連接埠。應在同一個節點上的容錯移轉群組中設定生命體。

關於這項工作

一對一的生命與 NIC 對應可產生最大的效能增益、但不需要啟用主幹連線。至少安裝兩個 NIC 可提供效能優勢、但並非必要。

主幹群組中的所有生命體應屬於同一個容錯移轉群組。請注意，當在同一個節點的容錯移轉群組中設定生命體時，該節點上的控制器容錯移轉可能會導致生命體離線。如果在同一個節點上的容錯移轉群組中未設定生命體，並

容錯移轉至另一個節點，則主幹將無法再運作。

您應該隨時調整主幹容錯移轉群組、以便從容錯移轉群組新增或移除連線（及基礎 NIC ）。

開始之前

- 您必須知道與 NIC 相關聯的連接埠名稱、才能建立容錯移轉群組。
- 連接埠必須全部位於同一個節點上。

步驟

1. 確認您打算使用的網路連接埠名稱和狀態：

```
network port show
```

2. 建立容錯移轉群組：

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

   這並不需要容錯移轉群組、但強烈建議您使用。

   - `<svm_name>`是包含 NFS 伺服器的 SVM 名稱。
   - `<ports_list>`是要新增至容錯移轉群組的連接埠清單。

     端口以格式添加 `<node_name>:<port_number>`，例如 `node1:e0c`：。

     下列命令會為 SVM VS1 建立容錯移轉群組 fg3 、並新增三個連接埠：

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

     深入瞭解 "容錯移轉群組。"

   如"指令參考資料ONTAP"需詳細 `network interface failover-groups create`資訊，請參閱。

3. 如有需要、請為主幹群組的成員建立生命體：

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

   - `-home-node` - 在 LIF 上執行網路介面還原命令時、 LIF 會傳回的節點。

     您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 `-auto-revert` 選項。

   - `-home-port` 是在 LIF 上執行網路介面還原命令時 LIF 傳回的實體或邏輯連接埠。
   - 您可以使用指定 IP 位址 `-address` 和 `-netmask` 選項、而非 `-subnet` 選項。
   - 當您指派 IP 位址時、如果不同 IP 子網路上有用戶端或網域控制站、則可能需要設定通往閘道的預設路

由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料ONTAP"。

- `-service-policy` - LIF 的服務原則。如果未指定原則、則會自動指派預設原則。使用 `network interface service-policy show` 命令以檢閱可用的服務原則。
- `-auto-revert` - 指定在啟動、管理資料庫狀態變更或建立網路連線等情況下、資料 LIF 是否會自動還原至其主節點。預設設定為 false 、但您可以根據環境中的網路管理原則將其設為 true 。

針對主幹群組中的每個 LIF 重複此步驟。

下列命令會建立 `lif-A` 適用於 SVM `vs1`、連接埠 `e0c` 節點的 `cluster1_01`：

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

深入瞭解 "LIF 建立："

4. 確認已建立生命：

```
network interface show
```

5. 驗證設定的 IP 位址是否可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

相關資訊

- "網路ping"
- "網路介面"
- "網路連接埠顯示"

建立 **ONTAP Volume** 匯出原則

若要讓用戶端存取資料共用、您必須建立一個或多個磁碟區、而且該磁碟區必須具有至少一個規則的匯出原則。

用戶端匯出需求：

- Linux 用戶端必須為每個主幹連線（亦即每個 LIF ）分別安裝一個裝載點和一個裝載點。
- VMware 用戶端只需要單一裝載點即可匯出磁碟區、並指定多個生命量。

  VMware 用戶端需要在匯出原則中具有 root 存取權。

步驟

1. 建立匯出原則：

```
vserver export-policy create -vserver svm_name -policyname policy_name
```

原則名稱最長可達256個字元。

2. 確認已建立匯出原則：

```
vserver export-policy show -policyname policy_name
```

範例
下列命令會在名為VS1的SVM上建立並驗證名為exp1的匯出原則：

```
vs1::> vserver export-policy create -vserver vs1 -policyname exp1
```

3. 建立匯出規則並將其新增至現有的匯出原則：

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

。 `-clientmatch` 參數應識別可用於主幹的 Linux 或 VMware 用戶端、以裝載匯出。

深入瞭解 "建立匯出規則。"

4. 建立具有交會點的Volume：

```
volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
-size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
-group group_name_or_number -junction-path junction_path -policy
export_policy_name
```

深入瞭解 "正在建立 Volume 。"

5. 確認已使用所需的交會點建立磁碟區：

```
volume show -vserver svm_name -volume volume_name -junction-path
```

掛載 **ONTAP Volume** 或資料共用以進行 **NFS** 主幹連線

支援主幹的 Linux 和 VMware 用戶端可以從啟用主幹的 ONTAP NFSv4.1 伺服器掛載磁碟區或資料共用。

深入瞭解 "支援的用戶端"。

Linux 用戶端需求

如果您使用 ONTAP 9.16.1 或更新版本，以及 Red Hat Enterprise Linux 8.7 或更新版本（適用於 RHEL 8 ）或 9.2 或更新版本（適用於 RHEL 9 ）作為 Linux 用戶端，則主幹群組只需要一個掛載點。使用以下選項，使用此命令裝載匯出的磁碟區 `trunkdiscovery`：

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

否則，主幹群組中的每個連線都需要個別的掛載點。使用類似下列命令的選項掛載匯出的 Volume `max_connect` ：

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

版本 (`vers`）值應為 `4.1` 或更新版本。

。 `max_connect` 值對應於主幹群組中的連線數目。

VMware 用戶端需求

需要掛載陳述式、其中包含主幹群組中每個連線的 IP 位址。

使用類似下列的命令掛載匯出的資料存放區：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值對應於主幹群組中的連線。

調整現有的 **NFS** 匯出以進行主幹連線

調整 **ONTAP NFS** 主幹的單一路徑匯出

您可以調整現有的單一路徑（非主幹） NFSv4.1 匯出以使用主幹。只要伺服器和用戶端的必要條件已滿足、只要在伺服器上啟用主幹功能、具有 Trunking 功能的用戶端就能立即發揮更好的效能。

針對主幹調整單一路徑匯出、可讓您在現有的磁碟區和 SVM 中維護匯出的資料集。若要這麼做、您必須在 NFS 伺服器上啟用主幹、更新網路和匯出組態、然後在用戶端上重新掛載匯出的共用。

啟用主幹會影響重新啟動伺服器。然後 VMware 用戶端必須重新掛載匯出的資料存放區； Linux 用戶端必須使用重新掛載匯出的磁碟區 `max_connect` 選項。

在 **ONTAP NFS** 伺服器上啟用主幹連線

必須在 NFS 伺服器上明確啟用 Trunking 。在建立 NFS 伺服器時、預設會啟用 NFSv4.1 。

啟用主幹連線後、請確認已視需要設定下列服務。

- "DNS"
- "LDAP"
- "Kerberos"

步驟

1. 啟用主幹連線、並確保已啟用 NFSv4.1 ：

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. 確認NFS正在執行：
   `vserver nfs status -vserver svm_name`
3. 確認NFS已設定為所需：

   ```
   vserver nfs show -vserver svm_name
   ```

   深入瞭解 "NFS 伺服器組態。"
   …如果您是從此 SVM 服務至 Windows 用戶端、請移動共用區、然後刪除伺服器。
   `vserver cifs show -vserver svm_name`

   +
   `vserver cifs delete -vserver svm_name`

更新您的網路以進行 **ONTAP NFS** 主幹連線

若要善用 NFSv4.1 主幹、主幹群組中的生命體必須位於同一個節點上、且同一個節點上必須有主連接埠。應在同一個節點上的容錯移轉群組中設定生命體。

關於這項工作

一對一的生命與 NIC 對應可產生最大的效能增益、但不需要啟用主幹連線。至少安裝兩個 NIC 可提供效能優勢、但並非必要。

主幹群組中的所有生命體應屬於同一個容錯移轉群組。請注意，當在同一個節點的容錯移轉群組中設定生命體時，該節點上的控制器容錯移轉可能會導致生命體離線。如果在同一個節點上的容錯移轉群組中未設定生命體，並容錯移轉至另一個節點，則主幹將無法再運作。

您應該隨時調整主幹容錯移轉群組、以便從容錯移轉群組新增或移除連線（及基礎 NIC ）。

開始之前

- 您必須知道與 NIC 相關聯的連接埠名稱、才能建立容錯移轉群組。
- 連接埠必須全部位於同一個節點上。

步驟

1. 確認您打算使用的網路連接埠名稱和狀態：

   ```
   network port show
   ```

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

2. 建立主幹容錯移轉群組或修改現有的群組以進行主幹連線：

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   ```
   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   這並不需要容錯移轉群組、但強烈建議您使用。

   - `<svm_name>`是包含 NFS 伺服器的 SVM 名稱。
   - `<ports_list>`是要新增至容錯移轉群組的連接埠清單。

     端口以格式（例如 `node1:e0c`）添加 `<node_name>:<port_number>`。

     下列命令會建立容錯移轉群組 `fg3` 對於 SVM VS1 、並新增三個連接埠：

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   深入瞭解 "容錯移轉群組。"

3. 視需要為主幹群組的成員建立額外的生命體：

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` - 在 LIF 上執行網路介面還原命令時、 LIF 會傳回的節點。

     您可以指定 LIF 是否應使用自動還原至主節點和主連接埠 `-auto-revert` 選項。

   - `-home-port` 是在 LIF 上執行網路介面還原命令時 LIF 傳回的實體或邏輯連接埠。
   - 您可以使用指定 IP 位址 `-address` 和 `-netmask` 選項：
   - 當您手動指派 IP 位址（不使用子網路）時、如果不同 IP 子網路上有用戶端或網域控制站、您可能需要設定通往閘道的預設路由。 `network route create`命令頁面包含在 SVM 中建立靜態路由的相關資訊。如"指令參考資料ONTAP"需詳細 `network route create`資訊，請參閱。
   - `-service-policy` - LIF 的服務原則。如果未指定原則、則會自動指派預設原則。使用 `network interface service-policy show` 命令以檢閱可用的服務原則。

     如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。

   - `-auto-revert` - 指定在啟動、管理資料庫狀態變更或建立網路連線等情況下、資料 LIF 是否會自動還

原至其主節點。* 預設設定為 FALSE* 、但您可以根據環境中的網路管理原則將其設為 true 。

針對主幹群組中所需的每個額外 LIF 重複此步驟。

下列命令會建立 `lif-A` 適用於 SVM `vs1`、連接埠 `e0c` 節點的 `cluster1_01`：

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

深入瞭解 "LIF 建立："

4. 確認已建立生命：

```
network interface show
```

5. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

相關資訊

- "網路ping"
- "網路介面"

修改 **ONTAP Volume** 匯出原則

若要讓用戶端能夠利用主幹功能來進行現有的資料共用、您可能必須修改匯出原則和規則、以及它們所附加的磁碟區。Linux 用戶端和 VMware 資料存放區有不同的匯出需求。

用戶端匯出需求：

- Linux 用戶端必須為每個主幹連線（亦即每個 LIF ）分別安裝一個裝載點和一個裝載點。

  如果您要升級至 ONTAP 9.14.1 、且已匯出 Volume 、則可以繼續在主幹群組中使用該 Volume 。

- VMware 用戶端只需要單一裝載點即可匯出磁碟區、並指定多個生命量。

  VMware 用戶端需要在匯出原則中具有 root 存取權。

步驟

1. 確認現有的匯出原則已就緒：

```
vserver export-policy show
```

2. 確認現有的匯出原則規則適用於主幹組態：

```
vserver export-policy rule show -policyname policy_name
```

請特別確認 `-clientmatch` 參數可正確識別要掛載匯出的具有主幹功能的 Linux 或 VMware 用戶端。

如果需要調整、請使用修改規則 `vserver export-policy rule modify` 命令或建立新規則：

```
vserver export-policy rule create -vserver svm_name -policyname policy_name
-ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
-rorule security_type -rwrule security_type -superuser security_type -anon
user_ID
```

深入瞭解 "建立匯出規則。"

3. 驗證現有匯出的磁碟區是否在線上：

```
volume show -vserver svm_name
```

重新掛載 **ONTAP** 磁碟區或 **NFS** 主幹的資料共用

若要將非主幹用戶端連線轉換為主幹連線、必須使用有關生命體的資訊、卸載及重新掛載 Linux 和 VMware 用戶端上的現有掛載。

深入瞭解 "支援的用戶端"。

卸載 VMware 用戶端會中斷資料存放區上的任何 VM 。另一種方法是建立啟用主幹的新資料存放區、並使用 * Storage VMotion* 將 VM 從舊資料存放區移至新資料存放區。如需詳細資訊、請參閱 VMware 文件。

Linux 用戶端需求

如果您使用 ONTAP 9.16.1 或更新版本，以及 Red Hat Enterprise Linux 8.7 或更新版本（適用於 RHEL 8 ）或 9.2 或更新版本（適用於 RHEL 9 ）作為 Linux 用戶端，則主幹群組只需要一個掛載點。使用以下選項，使用此命令裝載匯出的磁碟區 `trunkdiscovery`：

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

否則，主幹群組中的每個連線都需要個別的掛載點。使用類似下列命令的選項掛載匯出的磁碟區 `max_connect`：

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

版本 (`vers`）值應為 `4.1` 或更新版本。

。 `max_connect` 值對應於主幹群組中的連線數目。

VMware 用戶端需求

需要掛載陳述式、其中包含主幹群組中每個連線的 IP 位址。

使用類似下列的命令掛載匯出的資料存放區：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值應對應於主幹群組中的連線。

透過RDMA管理NFS

瞭解 ONTAP 中的 NFS over RDMA

NFS over RDMA 使用支援 RDMA 的網路介面卡，可在儲存系統記憶體和主機系統記憶體之間直接複製資料，避免 CPU 中斷和額外負荷。

NFS over RDMA組態是專為具有延遲敏感或高頻寬工作負載（例如機器學習和分析）的客戶所設計。ONTAP NFS over RDMA 可用於任何 NFS 型工作負載。此外， NVIDIA 已透過 RDMA 擴充 NFS ，以啟用 GPU 直接儲存（ GDS ）。GDS會繞過CPU和主記憶體、使用RDMA直接在儲存系統和GPU記憶體之間傳輸資料、進一步加速啟用GPU的工作負載。

從 ONTAP 9.10.1 開始， NFSv4.0 傳輸協定支援 NFS over RDMA 組態。後續的 ONTAP 版本推出了對其他 NFS 版本的支援。

需求

- 請確定您執行的 ONTAP 版本正確、適用於您要使用的 NFS 版本。

NFS版本	支援**ONTAP**
NFSv4.0	更新版本ONTAP
NFSv4.1	ONTAP 9.14.1 及更新版本
NFSv3.	ONTAP 9.15.1 及更新版本

  - 您可以使用System Manager從ONTAP 版本S59.12.1開始、透過RDMA設定NFS。在《S209.10.1》和《9.11.1》中ONTAP 、您需要使用CLI透過RDMA來設定NFS。

- 高可用度（ HA ）配對中的兩個節點都必須是相同版本。
- 儲存系統控制器必須支援 RDMA ：

從**ONTAP** 無到無…開始	下列控制器支援 **RDMI…**
9.10.1 及更新版本	• 解答400 AFF • AFF A700 • 解答800 AFF
ONTAP 9.14.1 及更新版本	• AFF C 系列 • 解答900 AFF
ONTAP 9.15.1 及更新版本	• AFF A1K • AFF A90 • AFF A70
ONTAP 9.16.1 及更新版本	• AFF A50 • AFF A30 • AFF A20

- 資料生命期必須設定為支援RDMA。
- 有關目標 RNIC 支持的信息，請參閱 "NetApp Hardware Universe"。
- 如需有關支援的 Client 作業系統 for NFS over RDMA 的資訊，請參閱 "NetApp互通性對照表IMT （僅限部分）"。如需 Roce v2 支援的 RNIC ，請參閱各自的 RNIC 廠商文件。

透過RDMA的NFS不支援介面群組。

後續步驟

- 透過RDMA設定NFS的NIC
- 透過RDMA設定NFS的LIF
- NFS over RDMA的NFS設定

相關資訊

- "RDMA"
- NFS 主幹總覽
- "RFC 7530：NFS版本4傳輸協定"
- "RFC 8166：遠端程序呼叫版本1的遠端直接記憶體存取傳輸"
- "RFC 8167：雙向遠端程序呼叫RFC-over RDMA傳輸"
- "RFC 8267：NFS上層繫結至RPC-over RDMA版本1"

透過RDMA設定NFS的NIC

NFS over RDMA需要用戶端系統和儲存平台的NIC組態。

儲存平台組態

有關目標 RNIC 支持的信息，請參閱 "NetApp Hardware Universe"。

如果您使用高可用度（ HA ）組態，兩個節點都必須使用相同的 RNIC 來支援 RDMA 容錯移轉。NIC 必須具備 ROCE 功能。

- 從 ONTAP 9.10.1 開始、您可以使用命令檢視 RDMA 卸載通訊協定清單：

```
network port show -rdma-protocols roce
```

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

- 從 ONTAP 9.16.1 開始，建議使用優先流量控制（ PFC ）。使用命令設定 PFC `network port modify` ：

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
pfc -pfc-queues-admin 3
```

- 在 ONTAP 9.16.1 之前，建議您使用預設的全域流程控制（ GFC ）。如果流程控制設定已變更，請使用命令來設定 GFC `network port modify` ：

```
network port modify -node <nodename> -port <portname> -flowcontrol-admin
full
```

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

用戶端系統組態

如需有關支援的 Client 作業系統 for NFS over RDMA 的資訊，請參閱 "NetApp互通性對照表IMT （僅限部分）"。如需 Roce v2 支援的 RNIC ，請參閱各自的 RNIC 廠商文件。

雖然用戶端和伺服器可以直接連線，但建議使用交換器來改善容錯移轉效能。

必須使用巨型框架來設定用戶端，伺服器，任何交換器和交換器上的所有連接埠。用戶端和交換器上的流程控制組態應符合 ONTAP 的流程控制組態。從 ONTAP 9.16.1 開始，最佳做法是在 ONTAP ，交換器和用戶端上啟用和設定優先順序流程控制。在 ONTAP 9.16.1 之前，建議使用全域流程控制。

確認此組態之後，您可以使用 RDMA 掛載 NFS 匯出。

系統管理員

您必須使用ONTAP S廳9.12.1或更新版本、才能使用System Manager透過RDMA設定網路介面與NFS。

步驟

1. 檢查是否支援RDMA。瀏覽至*「網路」>「乙太網路連接埠」、然後在群組檢視中選取適當的節點。展開節點時、請查看指定連接埠的 * **RDMA** 傳輸協定 * 欄位：值 * **roce** 表示支援 RDMA ；破折號（ * - * ）表示不支援。
2. 若要新增VLAN、請選取*+ VLAN*。選取適當的節點。在 **Port** 下拉式功能表中、如果可用連接埠支援 RDMA 、則會顯示文字 * roce Enabled* 。如果不支援 RDMA 、則不會顯示任何文字。
3. 遵循中的工作流程 使用NFS為Linux伺服器啟用NAS儲存設備 設定新的NFS伺服器。

   新增網路介面時、您可以選擇*使用roce連接埠*。對於任何想要透過RDMA使用NFS的網路介面、請選取此選項。

CLI

1. 使用下列命令檢查NFS伺服器上是否已啟用RDMA存取：

   ```
   vserver nfs show-vserver <SVM_name>
   ```

   根據預設、 `-rdma` 應啟用。如果不是、請在NFS伺服器上啟用RDMA存取：

   ```
   vserver nfs modify -vserver <SVM_name> -rdma enabled
   ```

2. 透過NFSv4.0透過RDMA掛載用戶端：
   a. proto參數的輸入取決於伺服器IP傳輸協定版本。如果是IPV4、請使用 `proto=rdma`。如果是IPv6、請使用 `proto=rdma6`。
   b. 將NFS目標連接埠指定為 `port=20049` 而非標準連接埠2049：

      ```
      mount -o vers=4,minorversion=0,proto=rdma,port=20049
      <Server_IP_address>:/<volume_path> <mount_point>
      ```

3. * 選用 * ：如果您需要卸載用戶端，請執行命令 `unmount <mount_path>`

更多資訊

- 建立 ONTAP NFS 伺服器
- 使用NFS為Linux伺服器啟用NAS儲存設備

透過**RDMA**設定**NFS**的**LIF**

若要透過 RDMA 使用 NFS ，您必須將您的生命（網路介面）設定為與 RDMA 相容。LIF 及其容錯移轉配對都必須能夠支援RDMA。

建立新的**LIF**

系統管理員

您必須執行ONTAP 支援功能更新版本的S廳9.12.1、才能使用System Manager透過RDMA建立NFS的網路介面。

步驟

1. 選擇*網路>總覽>網路介面*。
2. 選取 + Add 。
3. 當您選取 **NFS** 、 **SMB/CIFS** 、 **S2** 時、您可以選擇 * 使用 roce 連接埠 * 。選取「使用**roce**連接埠」核取方塊。
4. 選取儲存VM和主節點。指派一個 名稱 、 **IP** 位址 和 子網路遮罩 。
5. 輸入 IP 位址和子網路遮罩後、 System Manager 會將廣播網域清單篩選為具有具備 ROCE 功能連接埠的網域。選取廣播網域。您可以選擇性地新增閘道。
6. 選擇*保存*。

CLI

步驟

1. 建立LIF：

```
network interface create -vserver SVM_name -lif lif_name -service-policy
service_policy_name -home-node node_name -home-port port_name {-address
IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
-policy policy_name -auto-revert {true|false} -rdma-protocols roce
```

   - 服務原則必須是預設資料檔案或包含資料NFS網路介面服務的自訂原則。
   - 。 `-rdma-protocols` 參數接受預設為空白的清單。何時 `roce` 新增的值是 LIF 只能在支援 roce 卸載的連接埠上設定、影響 bot LIF 移轉和容錯移轉。

修改**LIF**

系統管理員

您必須執行ONTAP 支援功能更新版本的S廳9.12.1、才能使用System Manager透過RDMA建立NFS的網路介面。

步驟

1. 選擇*網路>總覽>網路介面*。
2. 在您要變更的網路介面旁選取 ⋮ * > 編輯 * 。
3. 選中*使用roce Ports*以通過RDMA啓用NFS或取消選中此框以禁用NFS。如果網路介面位於具備RoCE功能的連接埠、您會看到*使用roce連接埠*旁邊的核取方塊。
4. 視需要修改其他設定。
5. 選取*「Save（儲存）」*以確認您的變更。

CLI

1. 您可以使用檢查您的生命狀態 `network interface show` 命令。服務原則必須包含資料NFS網路介面服務。。 `-rdma-protocols` 清單應包含在內 `roce`。如果上述任一條件不正確、請修改LIF。

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

2. 若要修改LIF、請執行：

   ```
   network interface modify vserver SVM_name -lif lif_name -service-policy
   service_policy_name -home-node node_name -home-port port_name {-address
   IP_address -netmask netmask_value | -subnet-name subnet_name} -firewall
   -policy policy_name -auto-revert {true|false} -rdma-protocols roce
   ```

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

ⓘ 如果將LIF修改為需要特定卸載傳輸協定、但目前未將LIF指派給支援該傳輸協定的連接埠、將會產生錯誤。

移轉**LIF**

ONTAP 也可讓您移轉網路介面（ Lifs ），以透過 RDMA 使用 NFS 。執行此移轉時、您必須確保目的地連接埠具備RoCE功能。從《支援資料》9.12.1開始ONTAP 、您可以在System Manager中完成此程序。選取網路介面的目的地連接埠時、System Manager會指定連接埠是否具備RoCE功能。

只有在下列情況下、才能透過RDMA組態將LIF移轉至NFS：

- 它是NFS RDMA網路介面（LIF）、裝載於具備RoCE功能的連接埠上。
- 它是 NFS TCP 網路介面（ LIF ）、主控於具備 ROCE 功能的連接埠上。
- 它是NFS TCP網路介面（LIF）、裝載於不具備資源處理能力的連接埠上。

如需移轉網路介面的詳細資訊、請參閱 移轉LIF。

相關資訊

- 建立LIF
- 建立LIF
- 修改LIF
- 移轉LIF

修改NFS組態

在大多數情況下、您不需要透過 RDMA 修改 NFS 儲存 VM for NFS 的組態。

不過、如果您正在處理與Mellanox晶片和LIF移轉相關的問題、您應該延長NFSv4鎖定寬限期。依預設、寬限期設為45秒。從ONTAP 零點9.10.1開始、寬限期的最大值為180（秒）。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 輸入下列命令：

   ```
   vserver nfs modify -vserver SVM_name -v4-grace-seconds number_of_seconds
   ```

如需此工作的詳細資訊，請參閱為 ONTAP SVM 指定 NFSv4 鎖定寬限期。

使用 CLI 設定 SMB

使用 ONTAP CLI 瞭解 SMB 組態

您可以使用ONTAP 支援功能支援功能支援支援功能、以設定SMB用戶端存取新磁碟區或新SVM或現有SVM中qtree中所含的檔案。

> *SMB*（伺服器訊息區塊）是指通用網際網路檔案系統（CIFS）傳輸協定的現代語言。您仍會在ONTAP VMware的指令行介面（CLI）和OnCommand VMware的管理工具中看到_CIFS_。

如果您想要以下列方式設定SMB對磁碟區或qtree的存取權、請使用下列程序：

- 您想要使用SMB第2版或更新版本。
- 您只想為SMB用戶端服務、而非NFS用戶端（而非多重傳輸協定組態）。
- NTFS 檔案權限將用於保護新磁碟區的安全。
- 您擁有叢集管理員權限、而非SVM管理員權限。

  建立SVM和LIF需要叢集管理員權限。SVM管理員權限足以執行其他SMB組態工作。

- 您想要使用CLI、而非System Manager或自動化指令碼工具。

  若要使用 System Manager 設定 NAS 多重傳輸協定存取"同時使用NFS和SMB為Windows和Linux配置NAS儲存設備"、請參閱。

- 您想要使用最佳實務做法、而非探索每個可用選項。

  如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

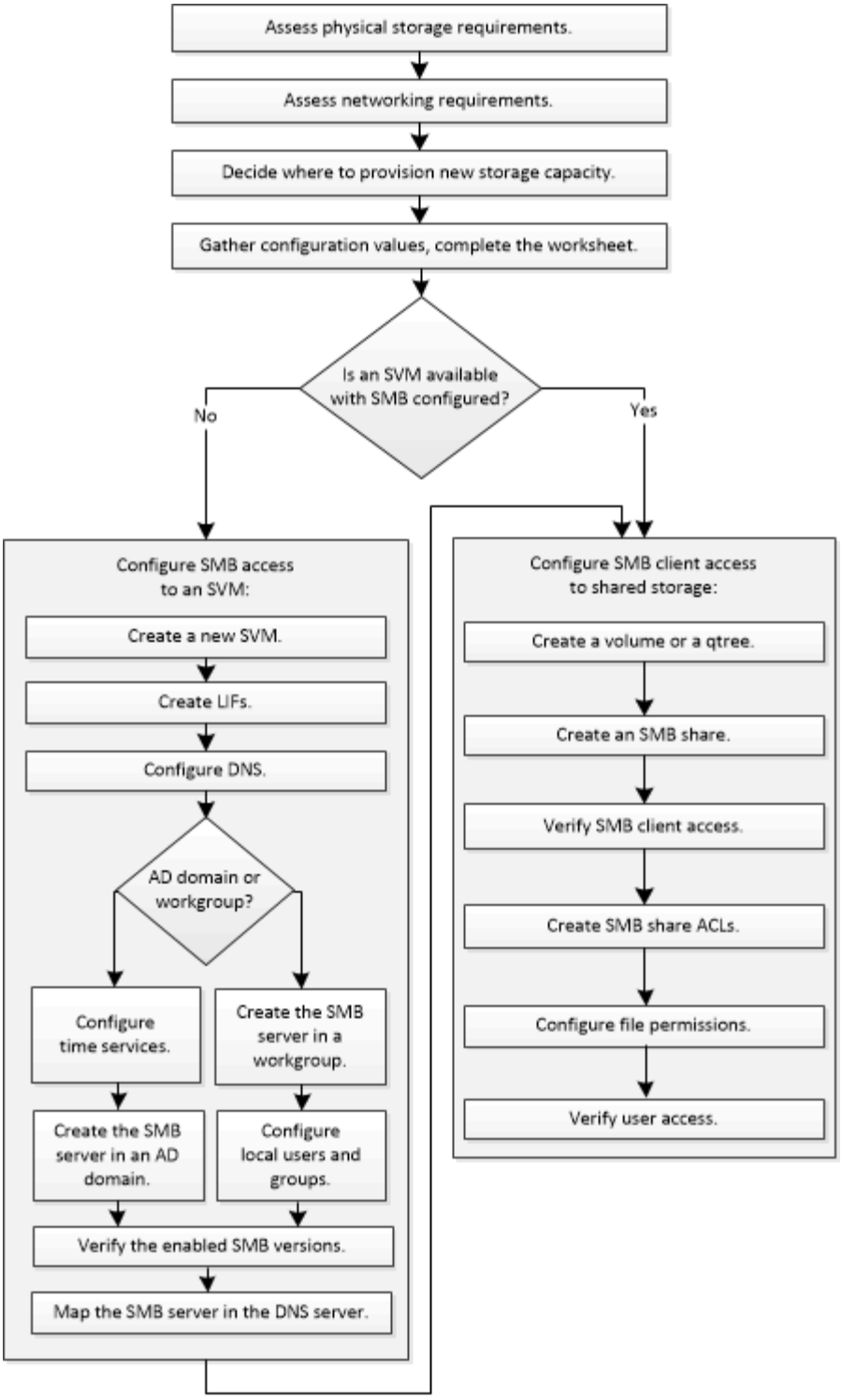
如果您想要瞭解ONTAP 有關各項功能的詳細資訊、請參閱 "SMB參考總覽"。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作…	請參閱…
重新設計的System Manager（ONTAP 提供更新版本的更新版本）	"使用SMB為Windows伺服器配置NAS儲存設備"
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"SMB 組態概觀"

ONTAP SMB 組態工作流程

設定SMB需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、設定SMB存取新的或現有的SVM、或將Volume或qtree新增至已完全設定為SMB存取的現有SVM。



準備

評估 **ONTAP SMB** 實體儲存需求

在為用戶端配置SMB儲存設備之前、您必須確保現有的集合體中有足夠的空間可容納新的磁碟區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型的新Aggregate。

步驟

1. 顯示現有Aggregate中的可用空間： `storage aggregate show`

   如果集合體有足夠的空間、請在工作表中記錄其名稱。

```
cluster::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 如果沒有具有足夠空間的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

相關資訊

- "存儲聚合添加磁碟"
- "儲存聚合創建"

評估 **ONTAP SMB** 網路需求

向用戶端提供SMB儲存設備之前、您必須確認網路設定正確、以符合SMB資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

步驟

1. 顯示可用的實體和虛擬連接埠： `network port show`

- 如果可能、您應該使用資料網路速度最高的連接埠。
- 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。

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

2. 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、請確認該子網路存在且有足夠的可用位址：`network subnet show`

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

   子網路包含屬於同一第3層子網路的IP位址集區。子網路是使用建立的 `network subnet create` 命令。

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

3. 顯示可用的IPspaces： `network ipspace show`

   您可以使用預設IPspace或自訂IPspace。

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

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6： `network options ipv6 show`

   如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

   深入瞭解 `network options ipv6 show`及 `network options ipv6 modify` "指令參考資料ONTAP"。

瞭解 **ONTAP SMB** 儲存容量配置

在建立新的 SMB Volume 或 qtree 之前、您必須先決定要將它放在新的或現有的 SVM 中、以及 SVM 需要多少組態。此決定決定決定您的工作流程。

選擇

- 如果您想要在新的SVM上配置磁碟區或qtree、或是在已啟用SMB但尚未設定的現有SVM上配置、請完成「設定SMB存取SVM」和「將儲存容量新增至啟用SMB的SVM」中的步驟。

  設定SMB存取SVM

  設定SMB用戶端存取共享儲存設備

  如果符合下列任一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用 SMB 。
  - 您在不想啟用 SMB 支援的叢集中有現有的 SVM 。
  - 叢集中有一個或多個啟用SMB的SVM、您需要下列其中一個連線：
    - 至不同的Active Directory樹系或工作群組。
    - 至隔離命名空間中的SMB伺服器（多租戶案例）。
      您也應該選擇此選項、在已啟用 SMB 但尚未設定 SMB 的現有 SVM 上佈建儲存設備。如果您為SAN存取建立SVM、或是在建立SVM時未啟用任何傳輸協定、則可能會發生這種情況。

在 SVM 上啟用 SMB 之後、請繼續配置 Volume 或 qtree 。

- 如果您想要在完全設定為SMB存取的現有SVM上配置磁碟區或qtree、請完成「將儲存容量新增至啟用SMB的SVM」中的步驟。

  設定SMB用戶端存取共享儲存設備

ONTAP SMB 組態工作表

SMB 組態工作表可讓您收集設定用戶端 SMB 存取所需的資訊。

您應該完成工作表的一或兩個區段、視您對儲存資源配置的決策而定：

- 如果您要設定SMB存取SVM、請完成這兩個部分。

  設定SMB存取SVM

  設定SMB用戶端存取共享儲存設備

- 如果您要將儲存容量新增至啟用 SMB 的 SVM 、則只需完成第二節。

  設定SMB用戶端存取共享儲存設備

深入瞭解中的參數"指令參考資料ONTAP"。

設定**SMB**存取**SVM**

*用於建立SVM*的參數

如果您要建立新的 SVM ，請使用命令提供這些值 `vserver create`。如"指令參考資料ONTAP"需詳細`vserver create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	您為新SVM提供的名稱、可以是完整網域名稱（FQDN）、也可以遵循另一種在叢集內強制執行唯一SVM名稱的慣例。	
`-aggregate`	叢集中有足夠空間容納新SMB儲存容量的集合體名稱。	
`-rootvolume`	您為SVM根磁碟區提供的唯一名稱。	
`-rootvolume-security-style`	使用 SVM 的 NTFS 安全樣式。	`ntfs`
`-language`	使用此工作流程中的預設語言設定。	`C.UTF-8`

欄位	說明	您的價值
ipspace	選用：IPspaces是SVM所在的不同IP位址空間。	

*用於建立LIF*的參數

建立生命時，您可以使用命令來提供這些值 `network interface create`。如"指令參考資料ONTAP"需詳細`network interface create`資訊，請參閱。

欄位	說明	您的價值
-lif	您為新LIF提供的名稱。	
-role	在此工作流程中使用資料LIF角色。	data
-data-protocol	在此工作流程中、請僅使用 SMB 傳輸協定。	cifs
-home-node	LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。 如"指令參考資料ONTAP"需詳細`network interface revert`資訊，請參閱。	
-home-port	LIF 在返回時傳回的連接埠或介面群組 `network interface revert` 命令會在LIF上執行。	
-address	叢集上的IPV4或IPv6位址、用於新LIF的資料存取。	
-netmask	LIF的網路遮罩和閘道。	
-subnet	IP位址集區。改用 `-address` 和 `-netmask` 自動指派位址和網路遮罩。	
-firewall-policy	在此工作流程中使用預設的資料防火牆原則。	data
-auto-revert	選用：指定資料LIF在啟動時或其他情況下是否自動還原至主節點。預設設定為 `false`。	

- DNS主機名稱解析參數*

當您設定 DNS 時，您可以使用命令來提供這些值 `vserver services name-service dns create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service dns create`資訊，請參閱。

欄位	說明	您的價值
`-domains`	最多五個DNS網域名稱。	
`-name-servers`	每個DNS名稱伺服器最多三個IP位址。	

在**Active Directory**網域中設定**SMB**伺服器

時間服務組態的參數

您可以在設定時間服務時，使用命令提供這些值 `cluster time-service ntp server create`。如"指令參考資料ONTAP"需詳細 `cluster time-service ntp server create`資訊，請參閱。

欄位	說明	您的價值
`-server`	Active Directory網域的NTP伺服器主機名稱或IP位址。	

在**Active Directory**網域中建立**SMB**伺服器的參數

當您建立新的 SMB 伺服器並指定網域資訊時，可以使用命令提供這些值 `vserver cifs create`。如"指令參考資料ONTAP"需詳細 `vserver cifs create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB伺服器的SVM名稱。	
`-cifs-server`	SMB伺服器名稱（最多15個字元）。	
`-domain`	要與SMB伺服器建立關聯的Active Directory網域完整網域名稱（FQDN）。	
`-ou`	選用：Active Directory網域中與SMB伺服器相關聯的組織單位。依預設、此參數設為「CN=電腦」。	
`-netbios-aliases`	選用：NetBios別名清單、是SMB伺服器名稱的替代名稱。	

欄位	說明	您的價值
`-comment`	選用：伺服器的文字註解。瀏覽網路上的伺服器時、Windows用戶端可以看到此SMB伺服器說明。	

在工作群組中設定**SMB**伺服器

在工作群組中建立**SMB**伺服器的參數

當您建立新的 SMB 伺服器並指定支援的 SMB 版本時，可以使用命令提供這些值 `vserver cifs create`。如"指令參考資料ONTAP"需詳細 `vserver cifs create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB伺服器的SVM名稱。	
`-cifs-server`	SMB伺服器名稱（最多15個字元）。	
`-workgroup`	工作群組名稱（最多15個字元）。	
`-comment`	選用：伺服器的文字註解。瀏覽網路上的伺服器時、Windows用戶端可以看到此SMB伺服器說明。	

建立本機使用者的參數

您可以在使用命令建立本機使用者時提供這些值 `vserver cifs users-and-groups local-user create`。工作群組中的SMB伺服器和AD網域中的選用伺服器都需要這些伺服器。如"指令參考資料ONTAP"需詳細 `vserver cifs users-and-groups local-user create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立本機使用者的SVM名稱。	
`-user-name`	本機使用者名稱（最多20個字元）。	
`-full-name`	選用：使用者的全名。如果全名包含空格、請將全名括在雙引號內。	
`-description`	選用：本機使用者的說明。如果說明包含空格、請將參數括在引號中。	

欄位	說明	您的價值
-is-account-disabled	選用：指定使用者帳戶是啟用還是停用。如果未指定此參數、則預設為啟用使用者帳戶。	

建立本機群組的參數

您可以在使用命令建立本機群組時提供這些值 `vserver cifs users-and-groups local-group create`。對於AD網域和工作群組中的SMB伺服器而言、它們是選用的。如"指令參考資料ONTAP"需詳細 `vserver cifs users-and-groups local-group create`資訊，請參閱。

欄位	說明	您的價值
-vserver	要在其中建立本機群組的SVM名稱。	
-group-name	本機群組名稱（最多256個字元）。	
-description	選用：本機群組的說明。如果說明包含空格、請將參數括在引號中。	

將儲存容量新增至啟用 **SMB** 的 **SVM**

建立**Volume**的參數

如果您要建立的是 Volume 而非 qtree ，則可以使用命令來提供這些值 `volume create`。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

欄位	說明	您的價值
-vserver	將裝載新磁碟區的新SVM或現有SVM名稱。	
-volume	您為新磁碟區提供的唯一描述性名稱。	
-aggregate	叢集中有足夠空間可容納新SMB Volume的集合體名稱。	
-size	您為新磁碟區大小所提供的整數。	
-security-style	此工作流程使用NTFS安全樣式。	ntfs
-junction-path	要掛載新磁碟區的根目錄（/）下的位置。	

用於建立**qtree**的參數

如果您要建立 qtree 而非 Volume ，請使用命令提供這些值 `volume qtree create`。如"指令參考資料ONTAP"需詳細 `volume qtree create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	包含qtree之磁碟區所在的SVM名稱。	
`-volume`	將包含新qtree的磁碟區名稱。	
`-qtree`	您為新qtree提供的唯一描述性名稱、64個字元或更少。	
`-qtree-path`	格式中的 qtree path 引數 `/vol/volume_name/qtree_name\>` 可以指定、而非將 Volume 和 qtree 指定為個別的引數。	

建立**SMB**共用的參數

您可以使用命令提供這些值 `vserver cifs share create`。如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB共用區的SVM名稱。	
`-share-name`	您要建立的SMB共用區名稱（最多256個字元）。	
`-path`	SMB共用區路徑名稱（最多256個字元）。此路徑必須存在於磁碟區中、才能建立共用區。	
`-share-properties`	選用：共用內容清單。預設設定為 `oplocks`、`browsable`、`changenotify`和 `show-previous-versions`。	
`-comment`	選用：伺服器的文字註解（最多256個字元）。在網路上瀏覽時、Windows用戶端可以看到此SMB共用說明。	

建立**SMB**共用存取控制清單（**ACL**）的參數

您可以使用命令提供這些值 `vserver cifs share access-control create`。如"指令參考資料ONTAP"

需詳細 `vserver cifs share access-control create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立SMB ACL的SVM名稱。	
`-share`	要在其中建立的SMB共用區名稱。	
`-user-group-type`	要新增至共用ACL的使用者或群組類型。預設類型為 `windows`	`windows`
`-user-or-group`	要新增至共用ACL的使用者或群組。如果您指定使用者名稱、則必須使用「domain\userName」格式來包含使用者的網域。	
`-permission`	指定使用者或群組的權限。	`[No_access
Read	Change	Full_Control]`

設定SMB存取SVM

設定 SMB 存取 ONTAP SVM

如果您尚未設定SVM進行SMB用戶端存取、則必須建立並設定新的SVM、或是設定現有的SVM。設定SMB需要開啟SVM根磁碟區存取、建立SMB伺服器、建立LIF、啟用主機名稱解析、設定名稱服務、以及視需要進行、 啟用Kerberos安全性。

建立 ONTAP SVM 以提供 SMB 資料存取

如果叢集中尚未至少有一個 SVM 可提供 SMB 用戶端的資料存取、則必須建立一個 SVM 。

開始之前

- 從 ONTAP 9.13.1 開始，您可以設定儲存 VM 的最大容量。您也可以在 SVM 接近臨界值容量層級時設定警示。如需更多資訊、請參閱 管理 SVM 容量。

步驟

1. 建立SVM： `vserver create -vserver svm_name -rootvolume root_volume_name -aggregate aggregate_name -rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspace_name`
   - 使用的 NTFS 設定 `-rootvolume-security-style` 選項。
   - 使用預設的 C.UTF-8 `-language` 選項。
   - 。 `ipspace` 設定為選用項目。
2. 驗證新建立的SVM的組態和狀態： `vserver show -vserver vserver_name`

- Allowed Protocols 欄位必須包含 CIFS 。您可以稍後再編輯此清單。

- Vserver Operational State 欄位必須顯示 running 州/省。如果顯示 initializing 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會建立 SVM 、以便在 IPspace 中存取資料 ipspaceA：

```
cluster1::> vserver create -vserver vs1.example.com -rootvolume root_vs1
-aggregate aggr1
-rootvolume-security-style ntfs -language C.UTF-8 -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 running 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。

```
cluster1::> vserver show -vserver vs1.example.com
                                    Vserver: vs1.example.com
                                Vserver Type: data
                             Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_vs1
                                  Aggregate: aggr1
                                 NIS Domain: -
                  Root Volume Security Style: ntfs
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                     Comment:
                                Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                        Vserver Admin State: running
                  Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                           Allowed Protocols: nfs, cifs, fcp, iscsi, ndmp
                        Disallowed Protocols: -
                            QoS Policy Group: -
                                 Config Lock: false
                                IPspace Name: ipspaceA
```

從 ONTAP 9.13.1 開始，您可以設定調適性 QoS 原則群組範本，將處理量下限套用至 SVM 中的磁碟區。您只能在建立 SVM 之後套用此原則。若要深入瞭解此程序，請參閱設定調適性原則群組範本。

確認 **ONTAP SVM** 上已啟用 **SMB** 傳輸協定

在 SVM 上設定和使用 SMB 之前、您必須先確認已啟用傳輸協定。

關於這項工作

這通常是在 SVM 設定期間完成、但如果您在設定期間未啟用傳輸協定、您可以稍後使用加以啟用 `vserver add-protocols` 命令。

一旦建立LIF、您就無法從其新增或移除通訊協定。

您也可以使用停用 SVM 上的通訊協定 `vserver remove-protocols` 命令。

步驟

1. 檢查SVM目前啟用和停用的傳輸協定： `vserver show -vserver vserver_name -protocols`

   您也可以使用 `vserver show-protocols` 用於檢視叢集中所有 SVM 上目前啟用的通訊協定的命令。

2. 如有必要、請啟用或停用傳輸協定：
   - 若要啟用 SMB 傳輸協定： `vserver add-protocols -vserver vserver_name -protocols cifs`
   - 若要停用通訊協定： `vserver remove-protocols -vserver vserver_name -protocols protocol_name[,protocol_name,...]`
3. 確認已啟用和停用的傳輸協定已正確更新： `vserver show -vserver vserver_name -protocols`

範例

下列命令顯示名為VS1的SVM上目前啟用和停用（允許和不允許）的傳輸協定：

```
vs1::> vserver show -vserver vs1.example.com -protocols
Vserver           Allowed Protocols         Disallowed Protocols
-----------       ----------------------    ------------------------
vs1.example.com   cifs                       nfs, fcp, iscsi, ndmp
```

下列命令可透過新增來存取 SMB `cifs` 到名為 VS1 的 SVM 上已啟用的通訊協定清單：

```
vs1::> vserver add-protocols -vserver vs1.example.com -protocols cifs
```

開啟 **ONTAP SVM** 根 **Volume** 的 **SMB** 匯出原則

SVM 根 Volume 的預設匯出原則必須包含一條規則、以允許所有用戶端透過 SMB 開啟存取。如果沒有這種規則、所有 SMB 用戶端都會被拒絕存取 SVM 及其磁碟區。

關於這項工作

建立新的SVM時、會自動為SVM的根Volume建立預設匯出原則（稱為預設）。您必須先為預設匯出原則建立一或多個規則、用戶端才能存取SVM上的資料。

您應該確認所有SMB存取都是在預設匯出原則中開啟、之後再建立個別磁碟區或qtree的自訂匯出原則、以限制個別磁碟區的存取。

步驟

1. 如果您使用現有的SVM、請檢查預設的根Volume匯出原則： `vserver export-policy rule show`

   命令輸出應類似下列內容：

```
cluster::> vserver export-policy rule show -vserver vs1.example.com
-policyname default -instance

                                    Vserver: vs1.example.com
                                Policy Name: default
                                 Rule Index: 1
                            Access Protocol: cifs
Client Match Hostname, IP Address, Netgroup, or Domain: 0.0.0.0/0
                             RO Access Rule: any
                             RW Access Rule: any
User ID To Which Anonymous Users Are Mapped: 65534
                   Superuser Security Types: any
               Honor SetUID Bits in SETATTR: true
                  Allow Creation of Devices: true
```

   如果存在允許開啟存取的規則、則此工作即告完成。如果沒有、請繼續下一步。

2. 建立SVM根磁碟區的匯出規則： `vserver export-policy rule create -vserver vserver_name -policyname default -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule any -rwrule any -superuser any`
3. 使用驗證規則建立 `vserver export-policy rule show` 命令。

結果

任何 SMB 用戶端現在都可以存取 SVM 上建立的任何 Volume 或 qtree 。

建立 **ONTAP SMB** 生命

LIF是與實體或邏輯連接埠相關聯的IP位址。如果元件發生故障、LIF可能會容錯移轉至不同的實體連接埠、或移轉至不同的實體連接埠、進而繼續與網路通訊。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

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

- 指定LIF處理之流量類型的機制已變更。對於僅適用於更新版本的版本、LIF會使用角色來指定其處理的流量類型。ONTAP從ONTAP Sf6開始、I生命 就會使用服務原則來指定處理的流量類型。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

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

- 從ONTAP NetApp 9.7開始、如果相同子網路中的SVM已存在其他LIF、您就不需要指定LIF的主連接埠。在相同的廣播網域中、系統會自動在指定的主節點上選擇隨機連接埠、如同在同一個子網路中設定的其他LIF。ONTAP

步驟

1. 建立LIF：

   `network interface create -vserver` *`vserver_name`* `-lif` *`lif_name`* `-role data -data -protocol cifs -home-node` *`node_name`* `-home-port` *`port_name`* `{-address` *`IP_address`* `-netmask IP_address | -subnet-name` *`subnet_name`*`} -firewall-policy data -auto -revert {true|false}`

《》第9.5版及更早版本* ONTAP
`network interface create -vserver *vserver_name* -lif *lif_name* -role data -data-protocol cifs -home-node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

版本**9.6**及更新版本 ONTAP
`network interface create -vserver *vserver_name* -lif *lif_name* -service-policy *service_policy_name* -home -node *node_name* -home-port *port_name* {-address *IP_address* -netmask *IP_address*`
-subnet-name *subnet_name*} -firewall-policy data -auto-revert {true
false}`

   - 。 `-role` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。
   - 。 `-data-protocol` 使用服務原則建立 LIF 時不需要參數（從 ONTAP 9.6 開始）。使用 ONTAP 9.5 或更早版本時 `-data-protocol` 必須在建立 LIF 時指定參數、而且必須在稍後修改、才能銷毀及重新建立資料 LIF 。
   - `-home-node` 是 LIF 在返回時返回的節點 `network interface revert` 命令會在LIF上執行。

您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 `-auto-revert` 選項。

- `-home-port` 是 LIF 在時傳回的實體或邏輯連接埠 `network interface revert` 命令會在LIF上執行。
- 您可以使用指定 IP 位址 `-address` 和 `-netmask` 或是您可以使用從子網路進行分配 `-subnet_name` 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料ONTAP"。
- 適用於 `-firewall-policy` 選項、請使用相同的預設值 `data` 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- `-auto-revert` 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 `false`**但您可以將其設定為** `false` 視環境中的網路管理原則而定。

2. 確認LIF已成功建立：

   ```
   network interface show
   ```

3. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	`network ping`
IPv6位址	`network ping6`

範例

下列命令會建立 LIF 並使用指定 IP 位址和網路遮罩值 `-address` 和 `-netmask` 參數：

```
network interface create -vserver vs1.example.com -lif datalif1 -role data
-data-protocol cifs -home-node node-4 -home-port e1c -address 192.0.2.145
-netmask 255.255.255.0 -firewall-policy data -auto-revert true
```

下列命令會建立LIF、並從指定的子網路（名為client1_sub）指派IP位址和網路遮罩值：

```
network interface create -vserver vs3.example.com -lif datalif3 -role data
-data-protocol cifs -home-node node-3 -home-port e1c -subnet-name
client1_sub -firewall-policy data -auto-revert true
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

下列命令顯示如何建立指派給的 NAS 資料 LIF `default-data-files` 服務原則：

```
network interface create -vserver vs1 -lif lif2 -home-node node2 -homeport
e0d -service-policy default-data-files -subnet-name ipspace1
```

相關資訊

- "網路ping"
- "網路介面回復"

啟用 **DNS** 以進行 **ONTAP SMB** 主機名稱解析

您可以使用 `vserver services name-service dns`命令在 SVM 上啟用 DNS ，並將其設定為使用 DNS 進行主機名稱解析。使用外部DNS伺服器解析主機名稱。如"指令參考資料ONTAP"需詳細 `vserver services name-service dns`資訊，請參閱。

開始之前

站台範圍的DNS伺服器必須可供主機名稱查詢。

您應該設定多個DNS伺服器、以避免單點故障。如果您只輸入一個 DNS 伺服器名稱，則命令會 `vserver services name-service dns create`發出警告。如"指令參考資料ONTAP"需詳細 `vserver services name-service dns create`資訊，請參閱。

關於這項工作

深入瞭解 "在 SVM 上設定動態 DNS"。

步驟

1. 在SVM上啟用DNS： `vserver services name-service dns create -vserver vserver_name -domains domain_name -name-servers ip_addresses -state enabled`

   下列命令可啟用SVM VS1上的外部DNS伺服器：

   ```
   vserver services name-service dns create -vserver vs1.example.com
   -domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
   enabled
   ```

   ⓘ ◦ `vserver services name-service dns create` 如果 ONTAP 無法連絡名稱伺服器、命令會執行自動組態驗證、並回報錯誤訊息。

2. 使用顯示 DNS 網域組態 `vserver services name-service dns show` 命令。

   下列命令會顯示叢集中所有SVM的DNS組態：

```
vserver services name-service dns show
                                                 Name
Vserver           State     Domains              Servers
----------------- --------- -------------------- -------------
cluster1          enabled   example.com          192.0.2.201,
                                                 192.0.2.202
vs1.example.com   enabled   example.com          192.0.2.201,
                                                 192.0.2.202
```

下列命令會顯示SVM VS1的詳細DNS組態資訊：

```
vserver services name-service dns show -vserver vs1.example.com
               Vserver: vs1.example.com
               Domains: example.com
         Name Servers: 192.0.2.201, 192.0.2.202
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

3. 使用驗證名稱伺服器的狀態 `vserver services name-service dns check` 命令。

```
vserver services name-service dns check -vserver vs1.example.com

Vserver           Name Server     Status       Status Details
----------------  -------------   ----------
---------------------------
vs1.example.com   10.0.0.50         up         Response time (msec): 2
vs1.example.com   10.0.0.51         up         Response time (msec): 2
```

在**Active Directory**網域中設定**SMB**伺服器

為 **SMB** 伺服器設定 **ONTAP** 時間服務

在Active Domain控制器中建立SMB伺服器之前、您必須確保SMB伺服器所屬網域的網域控制器上的叢集時間和時間、在五分鐘內相符。

關於這項工作

您應該設定叢集 NTP 服務以使用與 Active Directory 網域相同的 NTP 伺服器進行同步。

從功能完善的9.5開始ONTAP 、您可以使用對稱驗證來設定NTP伺服器。

步驟

1. 使用設定時間服務 `cluster time-service ntp server create` 命令。

- 若要在不使用對稱驗證的情況下設定時間服務、請輸入下列命令： `cluster time-service ntp server create -server server_ip_address`
- 若要使用對稱驗證來設定時間服務、請輸入下列命令： `cluster time-service ntp server create -server server_ip_address -key-id key_id`
  `cluster time-service ntp server create -server 10.10.10.1 cluster time-service ntp server create -server 10.10.10.2`

2. 使用確認時間服務已正確設定 `cluster time-service ntp server show` 命令。

```
cluster time-service ntp server show
```

```
Server                          Version
------------------------------- -------
10.10.10.1                      auto
10.10.10.2                      auto
```

相關資訊

- "叢集時間服務 NTP"

用於管理 **NTP** 伺服器上對稱驗證的 **ONTAP** 命令

從推出支援的版本號為《支援網路時間傳輸協定》（NTP）第3版。ONTAPNTPv3包含使用SHA-1金鑰的對稱驗證、可提高網路安全性。

若要這麼做...	使用此命令...
設定NTP伺服器而不進行對稱驗證	`cluster time-service ntp server create -server server_name`
設定採用對稱驗證的NTP伺服器	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
啟用現有NTP伺服器的對稱驗證您可以修改現有NTP伺服器、藉由新增所需的金鑰ID來啟用驗證。	`cluster time-service ntp server modify -server server_name -key-id key_id`
設定共用的NTP金鑰	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` 共用金鑰是由ID所指。節點和NTP伺服器上的ID、其類型和值必須相同
使用未知的金鑰ID設定NTP伺服器	`cluster time-service ntp server create -server server_name -key-id key_id`

若要這麼做...	使用此命令...
在NTP伺服器上設定未設定金鑰ID的伺服器。	`cluster time-service ntp server create -server server_name -key-id key_id` 金鑰ID、類型和值必須與NTP伺服器上設定的金鑰ID、類型和值相同。
停用對稱驗證	`cluster time-service ntp server modify -server server_name -authentication disabled`

相關資訊

- "叢集時間服務 NTP"

在 **ONTAP Active Directory** 網域中建立 **SMB** 伺服器

您可以使用 `vserver cifs create` 命令在 SVM 上建立 SMB 伺服器、並指定其所屬的 Active Directory （ AD ）網域。

開始之前

您用來提供資料的SVM和LIF必須設定為允許SMB傳輸協定。生命期必須能夠連線到SVM上設定的DNS伺服器、以及要加入SMB伺服器之網域的AD網域控制器。

任何有權在您要加入SMB伺服器的AD網域中建立機器帳戶的使用者、都可以在SVM上建立SMB伺服器。這可能包括來自其他網域的使用者。

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

關於這項工作

在活動目錄網域中建立SMB伺服器時：

- 指定網域時、您必須使用完整網域名稱（FQDN）。
- 預設設定是將SMB伺服器機器帳戶新增至Active Directory CN=電腦物件。
- 您可以選擇使用將 SMB 伺服器新增至不同的組織單位（ OU ） `-ou` 選項。
- 您可以選擇性地為SMB伺服器新增一個或多個NetBios別名（最多200個）的以逗號分隔的清單。

  當您將其他檔案伺服器的資料整合到SMB伺服器、並希望SMB伺服器回應原始伺服器的名稱時、設定SMB伺服器的NetBios別名很有用。

如需更多"指令參考資料ONTAP"資訊，以及選用參數和命名需求的詳細 `vserver cifs`資訊，請參閱。

從ONTAP 功能表9.8開始、您可以指定要加密網域控制器的連線。ONTAP 需要加密網域控制站通訊 `-encryption-required-for-dc-connection` 選項設定為 `true`；預設值為 `false`。設定此選項時、只有SMb3傳輸協定會用於ONTAP-DC連線、因為只有SMb3才支援加密。。

"中小企業管理" 包含SMB伺服器組態選項的詳細資訊。

步驟

1. 驗證叢集上是否已授權 SMB ： `system license show -package cifs`

   SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

   如果SMB伺服器僅用於驗證、則不需要CIFS授權。

2. 在 AD 網域中建立 SMB 伺服器： `vserver cifs create -vserver vserver_name -cifs-server smb_server_name -domain FQDN [-ou organizational_unit][-netbios-aliases NetBIOS_name, ...][-keytab-uri {(ftp|http)://hostname|IP_address}][-comment text]`

   加入網域時、此命令可能需要幾分鐘的時間才能完成。

   下列命令會在網域「example.com`":」中建立SMB伺服器「'shMB_server01」

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   smb_server01 -domain example.com
   ```

   下列命令會在「mydomain.com`"」網域中建立SMB伺服器「'shMB_server02」、並使用ONTAP Keytab檔案驗證該管理員：

   ```
   cluster1::> vserver cifs create -vserver vs1.mydomain.com -cifs-server
   smb_server02 -domain mydomain.com -keytab-uri
   http://admin.mydomain.com/ontap1.keytab
   ```

3. 使用驗證 SMB 伺服器組態 `vserver cifs show` 命令。

   在此範例中、命令輸出顯示在SVM vs1.example.com上建立名為「smb_server01」的SMB伺服器、並加入「example.com`"網域」。

   ```
   cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
   Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: -
   ```

4. 如有需要、請啟用與網域控制器（ ONTAP 9.8 及更新版本）的加密通訊： `vserver cifs security modify -vserver svm_name -encryption-required-for-dc-connection true`

範例

下列命令會在「example.com`"網域」的SVM vs2.example.com上建立名為「shmb_server02」的SMB伺服器。機器帳戶是在「'ou=eng,ou=corp,d=exam,dc=exam,d=com'」容器中建立。SMB伺服器會被指派一個NetBios別名。

```
cluster1::> vserver cifs create -vserver vs2.example.com –cifs-server
smb_server02 -domain example.com –ou OU=eng,OU=corp -netbios-aliases
old_cifs_server01

cluster1::> vserver cifs show -vserver vs1
                                          Vserver: vs2.example.com
                        CIFS Server NetBIOS Name: SMB_SERVER02
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description: -
                          List of NetBIOS Aliases: OLD_CIFS_SERVER01
```

下列命令可讓來自不同網域的使用者（在此情況下為信任網域的系統管理員）在SVM vs3.example.com上建立名為「sMB _server03」的SMB伺服器。。 `-domain` 選項指定您要在其中建立 SMB 伺服器的主網域名稱（在 DNS 組態中指定）。。 `username` 選項指定信任網域的系統管理員。

- 主網域：example.com
- 信任的網域：trust.lab.com
- 信任網域的使用者名稱：Administrator 1

```
cluster1::> vserver cifs create -vserver vs3.example.com -cifs-server
smb_server03 -domain example.com

Username: Administrator1@trust.lab.com
Password: . . .
```

為 **ONTAP SMB** 驗證建立 **Keytab** 檔案

從支援SVM 9.7開始ONTAP 、ONTAP 使用Keytab檔案、透過Active Directory（AD）伺服器支援SVM驗證。AD 系統管理員會產生 Keytab 檔案、並將其提供給 ONTAP 系統管理員、做為統一的資源識別元（ URI ） `vserver cifs` 命令需要使用 AD 網域進行 Kerberos 驗證。

AD 管理員可以使用標準 Windows Server 建立 Keytab 檔案 `ktpass` 命令。命令應在需要驗證的主要網域上執

行。。 `ktpass` 命令僅可用於為主要網域使用者產生 Keytab 檔案；不支援使用信任網域使用者所產生的金鑰。

Keytab檔案是針對特定ONTAP 的資訊管理員使用者所產生。只要管理員使用者的密碼未變更、針對特定加密類型和網域所產生的金鑰就不會變更。因此、每當管理員使用者的密碼變更時、都需要新的Keytab檔案。

支援下列加密類型：

- AES256-SHA1
- 德斯CBC-MD5

> 不支援DES-CBC-CRC加密類型。ONTAP

- RC4-HMAC

ES256是最高的加密類型、如果在ONTAP 支援的系統上啟用、就應該使用。

您可以指定管理密碼或使用隨機產生的密碼來產生Keytab檔案。不過、在任何指定時間、只能使用一個密碼選項、因為AD伺服器需要專屬的管理使用者私密金鑰、才能解密Keytab檔案中的金鑰。對特定管理員的私密金鑰進行任何變更、都會使Keytab檔案失效。

在工作群組中設定**SMB**伺服器

瞭解 **ONTAP** 工作群組中的 **SMB** 伺服器組態

將SMB伺服器設定為工作群組的成員包括建立SMB伺服器、然後建立本機使用者和群組。

當Microsoft Active Directory網域基礎架構無法使用時、您可以在工作群組中設定SMB伺服器。

工作群組模式中的SMB伺服器僅支援NTLM驗證、不支援Kerberos驗證。

在具有指定工作群組的 **ONTAP SVM** 上建立 **SMB** 伺服器

您可以使用 `vserver cifs create` 命令在 SVM 上建立 SMB 伺服器、並指定其所屬的工作群組。

開始之前

您用來提供資料的SVM和LIF必須設定為允許SMB傳輸協定。生命期必須能夠連線到SVM上設定的DNS伺服器。

關於這項工作

工作群組模式的SMB伺服器不支援下列SMB功能：

- SMB3見證傳輸協定
- SMB3 CA共用
- SQL over SMB
- 資料夾重新導向
- 漫遊設定檔
- 群組原則物件（GPO）

- Volume Snapshot服務（VSS）

如需更多 `vserver cifs`"指令參考資料ONTAP"資訊，以及選用的組態參數和命名需求，請參閱。

步驟

1. 驗證叢集上是否已授權 SMB ： `system license show -package cifs`

   SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

   如果SMB伺服器僅用於驗證、則不需要CIFS授權。

2. 在工作群組中建立 SMB 伺服器： `vserver cifs create -vserver vserver_name -cifs -server cifs_server_name -workgroup workgroup_name [-comment text]`

   下列命令會在工作群組「workgroup 01」中建立SMB伺服器「'shMB_server01」：

   ```
   cluster1::> vserver cifs create -vserver vs1.example.com -cifs-server
   SMB_SERVER01 -workgroup workgroup01
   ```

3. 使用驗證 SMB 伺服器組態 `vserver cifs show` 命令。

   在下列範例中、命令輸出顯示在工作群組「workgroup 01」的SVM vs1.example.com上建立了名為「shmb_server01」的SMB伺服器：

   ```
   cluster1::> vserver cifs show -vserver vs0

                                           Vserver: vs1.example.com
                         CIFS Server NetBIOS Name: SMB_SERVER01
                     NetBIOS Domain/Workgroup Name: workgroup01
                       Fully Qualified Domain Name: -
                               Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                     Workgroup Name: workgroup01
                                Authentication Style: workgroup
                  CIFS Server Administrative Status: up
                            CIFS Server Description:
                            List of NetBIOS Aliases: -
   ```

完成後

對於工作群組中的CIFS伺服器、您必須在SVM上建立本機使用者及選擇性的本機群組。

相關資訊

"中小企業管理"

您可以建立本機使用者帳戶、以便透過SMB連線授權存取SVM中所含的資料。您也可以在建立SMB工作階段時、使用本機使用者帳戶進行驗證。

關於這項工作

建立SVM時、預設會啟用本機使用者功能。

建立本機使用者帳戶時、您必須指定使用者名稱、並指定要與帳戶建立關聯的SVM。

如需更多"指令參考資料ONTAP"資訊，以及選用參數和命名需求的詳細 `vserver cifs users-and-groups local-user`資訊，請參閱。

步驟

1. 建立本機使用者： `vserver cifs users-and-groups local-user create -vserver` *`vserver_name`* `-user-name` *`user_name optional_parameters`*

   下列選用參數可能很有用：

   - `-full-name`

     使用者的全名。

   - `-description`

     本機使用者的說明。

   - `-is-account-disabled {true|false}`

     指定使用者帳戶是啟用還是停用。如果未指定此參數、則預設為啟用使用者帳戶。

   命令會提示輸入本機使用者的密碼。

2. 輸入本機使用者的密碼、然後確認密碼。
3. 確認已成功建立使用者： `vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

範例

以下範例建立一個本機使用者「'Smb_server01\sue」、全名為「'Shue Chang'」、與SVM vs1.example.com相關聯：

```
cluster1::> vserver cifs users-and-groups local-user create -vserver
vs1.example.com -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:

cluster1::> vserver cifs users-and-groups local-user show
Vserver  User Name                   Full Name  Description
-------- --------------------------- ---------- -------------
vs1      SMB_SERVER01\Administrator             Built-in administrator
account
vs1      SMB_SERVER01\sue             Sue Chang
```

建立本機 **ONTAP SMB** 群組

您可以建立本機群組、以便透過SMB連線授權存取與SVM相關的資料。您也可以指派權限來定義群組成員擁有的使用者權限或功能。

關於這項工作

建立SVM時、預設會啟用本機群組功能。

當您建立本機群組時、必須為群組指定名稱、而且必須指定要與群組建立關聯的SVM。您可以使用或不使用本機網域名稱來指定群組名稱、也可以選擇性地指定本機群組的說明。您無法將本機群組新增至其他本機群組。

如需更多"指令參考資料ONTAP"資訊，以及選用參數和命名需求的詳細 `vserver cifs users-and-groups local-group`資訊，請參閱。

步驟

1. 建立本機群組： `vserver cifs users-and-groups local-group create -vserver vserver_name -group-name group_name`

   下列選用參數可能很有用：

   - `-description`

     本機群組的說明。

2. 確認已成功建立群組： `vserver cifs users-and-groups local-group show -vserver vserver_name`

範例

下列範例建立與SVM VS1相關的本機群組「'Smb_server01\Engineering」：

```
cluster1::> vserver cifs users-and-groups local-group create -vserver
vs1.example.com -group-name SMB_SERVER01\engineering

cluster1::> vserver cifs users-and-groups local-group show -vserver
vs1.example.com
Vserver          Group Name                    Description
---------------- ----------------------------- ----------------------------
vs1.example.com  BUILTIN\Administrators        Built-in Administrators
group
vs1.example.com  BUILTIN\Backup Operators      Backup Operators group
vs1.example.com  BUILTIN\Power Users           Restricted administrative
privileges
vs1.example.com  BUILTIN\Users                 All users
vs1.example.com  SMB_SERVER01\engineering
vs1.example.com  SMB_SERVER01\sales
```

完成後

您必須將成員新增至新群組。

管理本機 **ONTAP SMB** 群組成員資格

您可以新增及移除本機或網域使用者、或新增及移除網域群組、來管理本機群組成員資格。如果您想要根據群組中的存取控制來控制資料存取、或是想要使用者擁有與該群組相關的權限、這很有用。

關於這項工作

如果您不再希望本機使用者、網域使用者或網域群組擁有根據群組成員資格而設定的存取權限或權限、您可以從群組中移除成員。

將成員新增至本機群組時、必須謹記下列事項：

- 您無法將使用者新增至特殊的_Everyon__群組。
- 您無法將本機群組新增至其他本機群組。
- 若要將網域使用者或群組新增至本機群組、ONTAP 則必須能夠將名稱解析為SID。

從本機群組中移除成員時、必須謹記下列事項：

- 您無法從特殊的_Everyon__群組中移除成員。
- 若要從本機群組中移除成員、ONTAP 則必須能夠將成員的名稱解析為一個SID。

步驟

1. 新增成員至群組或從群組中移除成員。
   - 新增成員：`vserver cifs users-and-groups local-group add-members -vserver vserver_name -group-name group_name -member-names name[,...]`

您可以指定要新增至指定本機群組的本機使用者、網域使用者或網域群組的以逗號分隔的清單。

- 移除成員： `vserver cifs users-and-groups local-group remove-members -vserver vserver_name -group-name group_name -member-names name[,...]`

  您可以指定要從指定本機群組中移除的本機使用者、網域使用者或網域群組的以逗號分隔的清單。

範例

以下範例將本機使用者「'Smb_server01\sue」新增至SVM vs1.example.com上的本機群組「'Smb_server01\Engineering」：

```
cluster1::> vserver cifs users-and-groups local-group add-members -vserver
vs1.example.com -group-name SMB_SERVER01\engineering -member-names
SMB_SERVER01\sue
```

以下範例將本機使用者「'MB_server01\sue」和「'MB_server01\James」從SVM vs1.example.com上的本機群組「'MB_server01\Engineering」中移除：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1.example.com -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

驗證啟用的 **ONTAP SMB** 版本

您的版本支援的版本取決於預設啟用哪些SMB版本、以便與用戶端和網域控制器連線。ONTAP您應該確認SMB伺服器是否支援您環境中所需的用戶端和功能。

關於這項工作

若要與用戶端和網域控制器連線、您應該盡可能啟用SMB 2.0和更新版本。基於安全考量、您應該避免使用SMB 1.0、如果您已確認環境中不需要SMB 1.0、則應該停用SMB 1.0。

從功能更新9.3開始ONTAP 、它在新的SVM上預設為停用。

> 如果 `-smb1-enabled-for-dc-connections` 設為 `false` 而 `-smb1-enabled` 設為 `true`，ONTAP 拒絕 SMB 1.0 連線做為用戶端，但會繼續接受傳入 SMB 1.0 連線做為伺服器。

"中小企業管理" 包含支援的SMB版本和功能的詳細資料。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 確認啟用哪些 SMB 版本：

```
vserver cifs options show
```

您可以向下捲動清單、檢視啟用用戶端連線的SMB版本、如果您要在AD網域中設定SMB伺服器、以進行AD網域連線。

3. 視需要啟用或停用用戶端連線的SMB傳輸協定：
   - 若要啟用 SMB 版本：

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     true
     ```

     的可能值 `smb_version`：

     - `-smb1-enabled`
     - `-smb2-enabled`
     - `-smb3-enabled`
     - `-smb31-enabled`

       下列命令可在 SVM vs1.example.com 上啟用 SMB 3.1 ：
       `cluster1::*> vserver cifs options modify -vserver vs1.example.com -smb31 -enabled true`

   - 若要停用 SMB 版本：

     ```
     vserver cifs options modify -vserver <vserver_name> -<smb_version>
     false
     ```

4. 如果SMB伺服器位於Active Directory網域中、請視需要啟用或停用SMB傳輸協定以進行DC連線：
   - 若要啟用 SMB 版本：

     ```
     vserver cifs security modify -vserver <vserver_name> -smb2-enabled
     -for-dc-connections true
     ```

   - 若要停用 SMB 版本：

     ```
     vserver cifs security modify -vserver <vserver_name> -smb2-enabled
     -for-dc-connections false
     ```

5. 返回管理權限層級：

```
set -privilege admin
```

對應 **DNS** 伺服器上的 **ONTAP SMB** 伺服器

您站台的DNS伺服器必須有一個項目、將SMB伺服器名稱和任何NetBios別名指向資料LIF的IP位址、以便Windows使用者將磁碟機對應至SMB伺服器名稱。

開始之前

您必須擁有站台DNS伺服器的管理存取權。如果您沒有管理存取權、則必須要求DNS管理員執行此工作。

關於這項工作

如果您使用SMB伺服器名稱的NetBios別名、最好為每個別名建立DNS伺服器進入點。

步驟

1. 登入DNS伺服器。
2. 建立轉送（A -位址記錄）和反轉（PTL -指標記錄）查詢項目、將SMB伺服器名稱對應至資料LIF的IP位址。
3. 如果您使用的是NetBios別名、請建立別名標準名稱（CNAME資源記錄）查詢項目、將每個別名對應至SMB伺服器資料LIF的IP位址。

結果

在整個網路傳播對應之後、Windows使用者可以將磁碟機對應到SMB伺服器名稱或其NetBios別名。

設定**SMB**用戶端存取共享儲存設備

設定 **SMB** 用戶端存取共用 **ONTAP** 儲存設備

若要讓SMB用戶端存取SVM上的共享儲存設備、您必須建立一個Volume或qtree以提供儲存容器、然後建立或修改該容器的共用區。然後您可以設定共用和檔案權限、並測試用戶端系統的存取。

開始之前

- 必須在 SVM 上完全設定 SMB 。
- 您名稱服務組態的任何更新都必須完成。
- 對Active Directory網域或工作群組組組態的任何新增或修改都必須完成。

建立**Volume**或**qtree**儲存容器

建立 **ONTAP SMB Volume**

您可以使用建立 Volume 並指定其連接點和其他屬性 `volume create` 命令。

關於這項工作

磁碟區必須包含_交會路徑_、才能讓用戶端使用其資料。您可以在建立新磁碟區時指定交會路徑。如果您在建立磁碟區時未指定連接路徑、則必須使用 _ 掛載 _ SVM 命名空間中的磁碟區 `volume mount` 命令。

開始之前

- 應設定並執行 SMB 。
- SVM 安全樣式必須是 NTFS 。
- 從 ONTAP 9.13.1 開始，您可以使用容量分析和活動追蹤功能來建立 Volume 。若要啟用容量或活動追蹤，請使用或 `-activity-tracking-state`設定為 `on`發出 `volume create`命令 `-analytics-state`。

  若要深入瞭解容量分析和活動追蹤、請參閱 "啟用檔案系統分析"。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

步驟

1. 建立具有交會點的Volume： `volume create -vserver svm_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style ntfs -junction-path junction_path]`

   的選擇 `-junction-path` 以下是：

   - 直接位於根目錄下、例如 `/new_vol`

     您可以建立新磁碟區、並指定將其直接掛載到SVM根磁碟區。

   - 在現有目錄下、例如 `/existing_dir/new_vol`

     您可以建立新磁碟區、並指定將其掛載至現有磁碟區（在現有階層架構中）、以目錄形式表示。

   如果您想在新目錄中建立磁碟區（在新磁碟區下的新階層中）、例如： `/new_dir/new_vol`接著、您必須先建立與 SVM 根 Volume 相關的新父 Volume 。接著、您會在新父Volume（新目錄）的交會路徑中建立新的子Volume。

2. 確認已使用所需的交會點建立磁碟區： `volume show -vserver svm_name -volume volume_name -junction`

範例

下列命令會在SVM vs1.example.com和Aggr1上建立名為user1的新磁碟區。新的 Volume 可在取得 `/users`。磁碟區大小為750 GB、磁碟區保證為磁碟區類型（預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume users
-aggregate aggr1 -size 750g -junction-path /users
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume users -junction
                           Junction                 Junction
Vserver          Volume    Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  users1  true     /users          RW_volume
```

下列命令會在SVM上建立一個名為「'home4'」的新磁碟區：vs1.example.com`"和Aggr1'集合體。目錄 `/eng/`

VS1 SVM 的命名空間已存在、新的 Volume 可從取得 `/eng/home`、成為的主目錄 `/eng/` 命名空間。磁碟區大小為 750 GB 、其磁碟區保證屬於類型 `volume` （預設）。

```
cluster1::> volume create -vserver vs1.example.com -volume home4
-aggregate aggr1 -size 750g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1.example.com -volume home4 -junction
                           Junction                 Junction
Vserver          Volume  Active   Junction Path   Path Source
---------------- ------- -------- --------------- -----------
vs1.example.com  home4   true     /eng/home       RW_volume
```

建立 **ONTAP SMB qtree**

您可以建立 qtree 來包含資料、並使用來指定其內容 `volume qtree create` 命令。

開始之前

- SVM和將要包含新qtree的Volume必須已經存在。
- SVM安全樣式必須為NTFS、且SMB必須設定並執行。

步驟

1. 建立qtree： `volume qtree create -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path } -security-style ntfs`

   您可以將 Volume 和 qtree 指定為個別的引數、或以格式指定 qtree 路徑引數 `/vol/volume_name/_qtree_name`。

2. 確認qtree是以所需的交會路徑建立： `volume qtree show -vserver vserver_name { -volume volume_name -qtree qtree_name | -qtree-path qtree path }`

範例

以下範例建立一個 qtree 、名稱為 qt01 、位於 SVM vs1.example.com 上、具有交會路徑 `/vol/data1`：

```
cluster1::> volume qtree create -vserver vs1.example.com -qtree-path
/vol/data1/qt01 -security-style ntfs
[Job 1642] Job succeeded: Successful

cluster1::> volume qtree show -vserver vs1.example.com -qtree-path
/vol/data1/qt01

                      Vserver Name: vs1.example.com
                       Volume Name: data1
                        Qtree Name: qt01
  Actual (Non-Junction) Qtree Path: /vol/data1/qt01
                    Security Style: ntfs
                       Oplock Mode: enable
                  Unix Permissions: ---rwxr-xr-x
                          Qtree Id: 2
                      Qtree Status: normal
                     Export Policy: default
        Is Export Policy Inherited: true
```

建立 **ONTAP SMB** 共用時的需求與考量

在建立SMB共用區之前、您必須先瞭解共用路徑和共用內容的需求、尤其是對於主目錄。

建立 SMB 共用需要指定目錄路徑結構（使用 `-path` 中的選項 `vserver cifs share create` 命令）。目錄路徑會對應到您在SVM命名空間中建立之磁碟區或qtree的交會路徑。建立共用區之前、目錄路徑和對應的交會路徑必須存在。

共用路徑有下列需求：

- 目錄路徑名稱最長可達255個字元。
- 如果路徑名稱中有空格、則必須將整個字串放在引號中（例如、 `"/new volume/mount here"`）。
- 如果是 UNC 路徑 (`\\servername\sharename\filepath`）共享區包含超過 256 個字元（不包括 UNC 路徑中的初始「」）、則 Windows 內容方塊中的 * 安全性 * 索引標籤無法使用。

  這是Windows用戶端問題、而非ONTAP 功能不均的問題。為避免此問題、請勿使用超過256個字元的UNC路徑建立共用。

共用內容預設值可以變更：

- 所有共用的預設初始屬性為 `oplocks`、 `browsable`、 `changenotify`和 `show-previous-versions`。
- 您可以在建立共用時指定共用內容。

  不過、如果您在建立共用時確實指定共用內容、則不會使用預設值。如果您使用 `-share-properties` 參數建立共用時、您必須使用逗號分隔的清單、指定要套用至共用的所有共用屬性。

- 若要指定主目錄共用、請使用 `homedirectory` 屬性。

  此功能可讓您根據連線的使用者及一組變數、設定對應至不同目錄的共用區。您不需要為每個使用者建立個別的共用區、而是使用幾個主目錄參數來設定單一共用區、以定義使用者在入口點（共用區）及其主目錄（SVM上的目錄）之間的關係。

  您無法在建立共用之後新增或移除此內容。

主目錄共用具有下列需求：

- 在建立 SMB 主目錄之前、您必須使用新增至少一個主目錄搜尋路徑 `vserver cifs home-directory search-path add` 命令。
- 主目錄共用、由的值指定 `homedirectory` 在上 `-share-properties` 參數必須包含 `%w` （ Windows 使用者名稱）共用名稱中的動態變數。

  共用名稱也可以包含 `%d` （網域名稱）動態變數（例如、 `%d/%w`）或共享區名稱中的靜態部分（例如、 `home1_%w`） 。

- 如果系統管理員或使用者使用共用來連線至其他使用者的主目錄（使用的選項） `vserver cifs home-directory modify` 命令）、動態共用名稱模式必須在開頭加上代字符號 (~) 。

如"指令參考資料ONTAP"需詳細 `vserver cifs share`資訊，請參閱。

相關資訊

- "中小企業管理"

建立 ONTAP SMB 共享區

您必須先建立SMB共用區、才能與SMB用戶端共用SMB伺服器的資料。建立共用時、您可以設定共用內容、例如將共用區指定為主目錄。您也可以設定選用的設定來自訂共用區。

開始之前

在建立共用之前、磁碟區或qtree的目錄路徑必須存在於SVM命名空間中。

關於這項工作

建立共用時、預設的共用 ACL （預設共用權限）為 `Everyone / Full Control`。在測試共用區的存取之後、您應該移除預設的共用ACL、並改用更安全的替代方法。

步驟

1. 如有必要、請建立共用的目錄路徑結構。

   。 `vserver cifs share create` 命令會檢查中指定的路徑 `-path` 共享區建立期間的選項。如果指定的路徑不存在、則命令會失敗。

2. 建立與指定SVM相關的SMB共用區： `vserver cifs share create -vserver vserver_name -share-name share_name -path path [-share-properties share_properties,...] [other_attributes] [-comment text]`
3. 確認共用區已建立：`vserver cifs share show -share-name share_name`

範例

下列命令會在 SVM 上建立名為「 HARE1 」的 SMB 共用區 `vs1.example.com`。其目錄路徑為 `/users`，然後使用預設內容建立。

```
cluster1::> vserver cifs share create -vserver vs1.example.com -share-name
SHARE1 -path /users

cluster1::> vserver cifs share show -share-name SHARE1

Vserver          Share    Path     Properties Comment  ACL
---------------  -------- -------- ---------- -------- -----------
vs1.example.com  SHARE1   /users   oplocks    -        Everyone / Full
Control
                                   browsable
                                   changenotify
                                   show-previous-versions
```

驗證 **ONTAP SMB** 用戶端存取

您應該存取並寫入資料至共用區、以確認SMB設定正確。您應該使用SMB伺服器名稱和任何NetBios別名來測試存取。

步驟

1. 登入Windows用戶端。
2. 使用SMB伺服器名稱進行測試存取：

   a. 在 Windows 檔案總管中、以下列格式將磁碟機對應至共用區： `\\\SMB_Server_Name\Share_Name`

      如果對應不成功、則DNS對應可能尚未傳播到整個網路。您必須在稍後使用SMB伺服器名稱來測試存取。

      如果 SMB 伺服器名稱為 vs1.example.com 、且共用名稱為 share1 、則應輸入下列內容： `\\vs0.example.com\SHARE1`

   b. 在新建立的磁碟機上、建立測試檔案、然後刪除該檔案。

   您已使用SMB伺服器名稱驗證共用的寫入存取權。

3. 對任何NetBios別名重複步驟2。

建立 **ONTAP SMB** 共用存取控制清單

建立SMB共用區的存取控制清單（ACL）來設定共用權限、可讓您控制使用者和群組對共用區的存取層級。

開始之前

您必須決定要授予哪些使用者或群組存取該共用區的權限。

關於這項工作

您可以使用本機或網域Windows使用者或群組名稱來設定共用層級ACL。

建立新 ACL 之前、您應該先刪除預設的共用 ACL `Everyone / Full Control`，這會帶來安全風險。

在工作群組模式中、本機網域名稱是SMB伺服器名稱。

步驟

1. 刪除預設的共用 ACL ：`vserver cifs share access-control delete -vserver` *`vserver_name`* `-share` *`share_name`* `-user-or-group everyone`
2. 設定新ACL：

如果您想要使用...來設定**ACL**	輸入命令...
Windows使用者	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_domain_name`*`\\`*`user_name`* `-permission access_right`
Windows群組	`vserver cifs share access-control create -vserver` *`vserver_name`* `-share` *`share_name`* `-user-group-type windows -user-or-group` *`Windows_group_name`* `-permission access_right`

3. 使用驗證套用至共用的 ACL 是否正確 `vserver cifs share access-control show` 命令。

範例

下列命令提供 `Change` 「銷售團隊」 Windows 群組在「 vs1.example.com`"SVM: 」上的「銷售」共用區的權限

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "Sales Team" -permission
Change

cluster1::> vserver cifs share access-control show
                 Share       User/Group              User/Group  Access
Vserver          Name        Name                    Type
Permission
---------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\"Sales Team"     windows     Change
```

下列命令會提供 `Change` 允許本機Windows群組名為「老虎團隊」和 `Full_Control` 本機 Windows 使用者在「 'VS1' SVM 」上的「 datavol5 」共用區的「 Shue Chang 」權限：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    DOMAIN\"Tiger Team"         windows     Change
vs1            datavol5    DOMAIN\"Sue Chang"          windows
Full_Control
```

在 **ONTAP SMB** 共用中設定 **NTFS** 檔案權限

若要讓具有共用存取權的使用者或群組能夠存取檔案、您必須從Windows用戶端設定該共用區中檔案和目錄的NTFS檔案權限。

開始之前

執行此工作的系統管理員必須擁有足夠的NTFS權限、才能變更所選物件的權限。

關於這項工作

"中小企業管理" 而您的Windows文件則包含如何設定標準和進階NTFS權限的相關資訊。

步驟

1. 以系統管理員身分登入Windows用戶端。
2. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
3. 填寫*對應網路磁碟機*方塊：
   a. 選取*磁碟機*字母。
   b. 在 * 資料夾 * 方塊中、輸入 SMB 伺服器名稱、其中包含您要套用權限的資料、以及共用名稱。

      如果您的 SMB 伺服器名稱為 smb_server01 、而您的共用名稱為「 'SPARE1' 」、則您必須輸入 `\\SMB_SERVER01\SHARE1`。

您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

c. 單擊*完成*。

您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

4. 選取您要設定NTFS檔案權限的檔案或目錄。
5. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
6. 選取*安全性*索引標籤。

「安全性」索引標籤會顯示已設定NTFS權限的使用者和群組清單。「物件的權限」方塊會顯示所選使用者或群組有效的「允許」和「拒絕」權限清單。

7. 按一下 * 編輯 * 。

「物件的權限」方塊隨即開啟。

8. 執行所需的動作：

如果你想...	請執行下列動作...
設定新使用者或群組的標準NTFS權限	a. 按一下「 * 新增 * 」。 「選取使用者、電腦、服務帳戶或群組」視窗即會開啟。 b. 在「輸入要選取的物件名稱」方塊中、輸入您要新增NTFS權限的使用者或群組名稱。 c. 按一下「確定」。
變更或移除使用者或群組的標準NTFS權限	在*群組或使用者名稱*方塊中、選取您要變更或移除的使用者或群組。

9. 執行所需的動作：

如果您想要...	請執行下列動作
為新的或現有的使用者或群組設定標準NTFS權限	在「物件權限>」方塊中、針對您要允許或不允許選取的使用者或群組存取的類型、選取*允許*或*拒絕*方塊。
移除使用者或群組	按一下「移除」。

如果部分或全部的標準權限方塊無法選取、這是因為權限是從父物件繼承而來。*特殊權限*方塊無法選取。如果選取此選項、表示已為選取的使用者或群組設定一或多個精細的進階權限。

10. 在您完成新增、移除或編輯該物件的NTFS權限之後、請按一下「確定」。

驗證 ONTAP SMB 使用者共用存取權

您應該測試您設定的使用者是否可以存取SMB共用區及其所包含的檔案。

步驟

1. 在Windows用戶端上、以目前擁有共用存取權的其中一位使用者身分登入。
2. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
3. 填寫*對應網路磁碟機*方塊：

   a. 選取*磁碟機*字母。

   b. 在*資料夾*方塊中、輸入您要提供給使用者的共用名稱。

      如果您的 SMB 伺服器名稱為 smb_server01 、而您的共用名稱為「 'SPARE1' 」、則您必須輸入 `\\SMB_SERVER01\share1`。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

4. 建立測試檔案、確認其存在、將文字寫入其中、然後移除測試檔案。

使用 CLI 管理 SMB

瞭解 ONTAP SMB

SMB傳輸協定可使用的支援資料檔存取功能。ONTAP您可以啟用CIFS伺服器、建立共用及啟用Microsoft服務。

> *SMB*（伺服器訊息區塊）是指通用網際網路檔案系統（CIFS）傳輸協定的現代語言。您仍會在ONTAP VMware的指令行介面（CLI）和OnCommand VMware的管理工具中看到_CIFS_。

SMB伺服器支援

瞭解 ONTAP SMB 伺服器支援

您可以在儲存虛擬機器（SVM）上啟用和設定SMB伺服器、讓SMB用戶端存取叢集上的檔案。

- 叢集中的每個資料SVM只能繫結到一個Active Directory網域。
- 資料SVM不需要繫結至同一個網域。
- 多個SVM可以綁定到同一個網域。

您必須先設定用來提供資料的SVM和LIF、才能建立SMB伺服器。如果您的資料網路不平坦、您可能還需要設定IPspace、廣播網域和子網路。

相關資訊

"網路管理"

修改伺服器

"系統管理"

支援的 **ONTAP SMB** 版本與功能

伺服器訊息區（SMB）是Microsoft Windows用戶端和伺服器所使用的遠端檔案共用傳輸協定。支援所有 SMB 版本。您應該確認ONTAP 支援您環境中所需的用戶端和功能的功能。

有關哪些SMB用戶端和網域控制器ONTAP 支援的最新資訊、請參閱「互通性對照表工具」。

ONTAP SMB 伺服器預設會啟用 SMB 2.0 及更新版本，並可視需要啟用或停用。SMB 1.0 可視需要啟用或停用。

SMB 1.0和2.0連線至網域控制器的預設設定也取決於ONTAP 版本。如"指令參考資料ONTAP"需詳細 `vserver cifs security modify`資訊，請參閱。對於現有CIFS伺服器執行SMB 1.0的環境、您應該盡快移轉至較新的SMB版本、以準備增強安全性與法規遵循。如需詳細資訊、請聯絡您的NetApp代表。

下表顯示每個SMB版本支援哪些SMB功能。部分SMB功能預設為啟用、有些則需要額外的組態。

此功能：	需要啟用：	*支援上述**SMB**版本*的支援功能**ONTAP**	
		3.0	3.1.1
舊版SMB 1.0功能		x	x
耐用的握把		x	x
複雜作業		x	x
非同步作業		x	x
增加讀寫緩衝區大小		x	x
提升擴充性		x	x
SMB簽署	x	x	x
替代資料串流（ADS）檔案格式	x	x	x
大型MTU（預設為ONTAP以支援功能更新為開頭）	x	x	x
租賃oplocks		x	x

此功能：	需要啟用：	*支援上述**SMB**版本*的支援功能**ONTAP**	
持續可用的共用	x	x	x
持續處理		x	x
見證人		x	x
SMB加密：AES-128與CCM	x	x	x
橫向擴充（CA共用區要求）		x	x
透明的容錯移轉		x	x
SMB多通道（從ONTAP NetApp 9.4開始）	x	x	x
預先驗證完整性			x
叢集用戶端容錯移轉v.2（CCFv2）			x
SMB 加密： AES-128/GCM	x		x

相關資訊

了解如何使用 ONTAP 簽章來增強網路安全

設定伺服器最低身份驗證安全級別

在SMB伺服器上設定必要的SMB加密、以便透過SMB傳輸資料

"NetApp互通性"

ONTAP SMB 中不支援的 **Windows** 功能

在您的網路中使用CIFS之前、您必須注意ONTAP 到某些不支援的Windows功能。

不支援下列Windows功能：ONTAP

- 加密檔案系統（EFS）
- 在變更日誌中記錄NT檔案系統（NTFS）事件
- Microsoft檔案複寫服務（FRS）
- Microsoft Windows索引服務

- 透過階層式儲存管理（HSM）進行遠端儲存
- 從Windows用戶端進行配額管理
- Windows配額語義
- LMHOSTS.檔案
- NTFS原生壓縮

在 **ONTAP SMB VM** 上設定 **NIS** 或 **LDAP** 名稱服務

透過SMB存取、即使存取NTFS安全型磁碟區中的資料、也會一律執行與UNIX使用者的使用者對應。如果您將Windows使用者對應至儲存在NIS或LDAP目錄存放區中的對應UNIX使用者、或是使用LDAP進行名稱對應、則應該在SMB設定期間設定這些名稱服務。

開始之前

您必須自訂名稱服務資料庫組態、以符合您的名稱服務基礎架構。

關於這項工作

SVM會使用名稱服務ns-交換器資料庫來決定查詢指定名稱服務資料庫來源的順序。ns 交換器來源可以是、 `nis`或 `ldap`的任意組合 `files`。針對Groups資料庫、ONTAP Ses庫 會嘗試從所有已設定的來源取得群組成員資格、然後使用整合的群組成員資格資訊進行存取檢查。如果其中一個來源在取得UNIX群組資訊時無法使用、ONTAP 則無法取得完整的UNIX認證、後續的存取檢查可能會失敗。因此、您必須一律在ns交換器設定中、檢查是否已針對群組資料庫設定所有的ns交換器來源。

預設是讓 SMB 伺服器將所有 Windows 使用者對應至儲存在本機中的預設 UNIX 使用者 `passwd` 資料庫。如果您想要使用預設組態、則可選擇設定NIS或LDAP UNIX使用者與群組名稱服務或LDAP使用者對應、以供SMB存取。

步驟

1. 如果UNIX使用者、群組及netgroup資訊是由NIS名稱服務管理、請設定NIS名稱服務：

   a. 使用判斷名稱服務的目前順序 `vserver services name-service ns-switch show` 命令。

      在此範例中、這三個資料庫 (`group`、 `passwd`和 `netgroup`） `nis` 因為名稱服務來源僅在使用中 `files` 做為來源。

      ```
      vserver services name-service ns-switch show -vserver vs1
      ```

      ```
                                                   Source
      Vserver         Database       Enabled       Order
      --------------- ------------   ---------     ---------
      vs1             hosts          true          dns,
                                                   files
      vs1             group          true          files
      vs1             passwd         true          files
      vs1             netgroup       true          files
      vs1             namemap        true          files
      ```

您必須新增 `nis` 的來源 `group` 和 `passwd` 資料庫、或是選擇性的 `netgroup` 資料庫。

b. 使用調整名稱服務 nS-switch 資料庫的順序 `vserver services name-service ns-switch modify` 命令。

為獲得最佳效能、除非您計畫在SVM上設定名稱服務、否則不應將名稱服務新增至名稱服務資料庫。

如果您修改多個名稱服務資料庫的組態、則必須針對每個要修改的名稱服務資料庫分別執行命令。

在此範例中、 `nis` 和 `files` 設定為的來源 `group` 和 `passwd` 資料庫、依此順序。其餘的名稱服務資料庫則維持不變。

```
vserver services name-service ns-switch modify -vserver vs1 -database group
-sources nis,files vserver services name-service ns-switch modify -vserver
vs1 -database passwd -sources nis,files
```

c. 使用確認名稱服務的順序正確無誤 `vserver services name-service ns-switch show` 命令。

```
vserver services name-service ns-switch show -vserver vs1
```

```
                                                Source
Vserver         Database       Enabled          Order
--------------- ------------   ---------        ---------
vs1             hosts          true             dns,
                                                files
vs1             group          true             nis,
                                                files
vs1             passwd         true             nis,
                                                files
vs1             netgroup       true             files
vs1             namemap        true             files
```

d. 建立 NIS 名稱服務組態：
`vserver services name-service nis-domain create -vserver <vserver_name> -domain <NIS_domain_name> -servers <NIS_server_IPaddress>,…`

```
vserver services name-service nis-domain create -vserver vs1 -domain
example.com -servers 10.0.0.60
```

> 領域 `-nis-servers`取代了領域 `-servers` 。此欄位可以採用 NIS 伺服器的主機名稱或 IP 位址。

e. 確認 NIS 名稱服務已正確設定： `vserver services name-service nis-domain show vserver <vserver_name>`

```
vserver services name-service nis-domain show vserver vs1
```

```
Vserver         Domain                Server
--------------- --------------------- ---------------
vs1             example.com           10.0.0.60
```

2. 如果UNIX使用者、群組及netgroup資訊或名稱對應是由LDAP名稱服務管理、請使用所在的資訊來設定LDAP名稱服務 "NFS管理"。

瞭解 **ONTAP SMB** 名稱服務交換器組態

ONTAP 會將名稱服務組態資訊儲存在相當於的表格中 `/etc/nsswitch.conf` UNIX 系統上的檔案。您必須瞭解表格的功能及ONTAP 其使用方式、以便根據環境適當設定。

這個名稱服務交換器表決定哪些名稱服務來源可以查詢、以便擷取特定類型名稱服務資訊的資訊。ONTAP ONTAP針對每個SVM維護個別的名稱服務交換器表。ONTAP

資料庫類型

此表格會針對下列每一種資料庫類型儲存個別的名稱服務清單：

資料庫類型	定義名稱服務來源：	有效來源為...
主機	將主機名稱轉換為IP位址	檔案、DNS
群組	查詢使用者群組資訊	檔案、NIS、LDAP
密碼	查詢使用者資訊	檔案、NIS、LDAP
網路群組	查詢netgroup資訊	檔案、NIS、LDAP
名稱	對應使用者名稱	檔案、LDAP

來源類型

這些來源會指定要用於擷取適當資訊的名稱服務來源。

指定來源類型...	若要查詢資訊...	由命令系列管理...

檔案	本機來源檔案	`vserver services name-service unix-user` `vserver services name-service unix-group`
		
		`vserver services name-service netgroup`
		
		`vserver services name-service dns hosts`

NIS	在SVM的NIS網域組態中指定的外部NIS伺服器	`vserver services name-service nis-domain`
LDAP	在SVM的LDAP用戶端組態中指定的外部LDAP伺服器	`vserver services name-service ldap`
DNS	在SVM的DNS組態中指定的外部DNS伺服器	`vserver services name-service dns`

即使您計畫同時使用 NIS 或 LDAP 來進行資料存取和 SVM 管理驗證、您仍應納入 `files` 並將本機使用者設定為在 NIS 或 LDAP 驗證失敗時的後援。

用於存取外部來源的傳輸協定

若要存取伺服器的外部來源、ONTAP 可使用下列通訊協定：

外部名稱服務來源	用於存取的傳輸協定
NIS	UDP
DNS	UDP
LDAP	TCP

範例

以下範例顯示 SVM 的名稱服務交換器組態 `svm_1`：

```
cluster1::*> vserver services name-service ns-switch show -vserver svm_1
                                 Source
Vserver         Database         Order
--------------- ------------     ---------
svm_1           hosts            files,
                                 dns
svm_1           group            files
svm_1           passwd           files
svm_1           netgroup         nis,
                                 files
```

若要查詢使用者或群組資訊、ONTAP 僅查詢本機來源檔案。如果查詢未傳回任何結果、則查詢會失敗。

若要查詢netgroup資訊、ONTAP 請先諮詢外部NIS伺服器。如果查詢未傳回任何結果、則會勾選本機netgroup檔案。

SVM SVM_1的表格中沒有名稱對應的名稱服務項目。因此ONTAP 、根據預設、僅查詢本機來源檔案。

管理SMB伺服器

修改 ONTAP SMB 伺服器

您可以使用將 SMB 伺服器從工作群組移至 Active Directory 網域、從工作群組移至其他工作群組、或從 Active Directory 網域移至工作群組 `vserver cifs modify` 命令。

關於這項工作

您也可以修改SMB伺服器的其他屬性、例如SMB伺服器名稱和管理狀態。如"指令參考資料ONTAP"需詳細`vserver cifs modify`資訊，請參閱。

選擇

- 將SMB伺服器從工作群組移至Active Directory網域：

  a. 將 SMB 伺服器的管理狀態設為 `down`。

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
  ```

  b. 將SMB伺服器從工作群組移至Active Directory網域： `vsserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`*

  ```
  Cluster1::>vserver cifs modify -vserver vs1 -domain example.com
  ```

  若要為 SMB 伺服器建立 Active Directory 機器帳戶、您必須提供具有足夠權限的 Windows 帳戶名稱和密碼、以便將電腦新增至 `ou=`*`example`* `ou` 中的容器 *`example`*.com 網域。

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

- 將SMB伺服器從工作群組移至其他工作群組：
  a. 將 SMB 伺服器的管理狀態設為 `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. 修改 SMB 伺服器的工作群組： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`new_workgroup_name`*

```
Cluster1::>vserver cifs modify -vserver vs1 -workgroup workgroup2
```

- 將SMB伺服器從Active Directory網域移至工作群組：
  a. 將 SMB 伺服器的管理狀態設為 `down`。

```
Cluster1::>vserver cifs modify -vserver vs1 -status-admin down
```

  b. 將 SMB 伺服器從 Active Directory 網域移至工作群組： `vserver cifs modify -vserver` *`vserver_name`* `-workgroup` *`workgroup_name`*

```
cluster1::> vserver cifs modify -vserver vs1 -workgroup workgroup1
```

> 若要進入工作群組模式、系統必須停用所有網域型功能、並自動移除其組態、包括持續可用的共用、陰影複製及AES。不過、網域設定的共用ACL（例
> 如「EXAMPLE.COM\userName"」）無法正常運作、ONTAP 但無法由支援部門移除。命令完成後、請使用外部工具儘快移除這些共用ACL。如果啟用AES、系統可能會要求您提供具有足夠權限的Windows帳戶名稱和密碼、以便在「example.com」網域中停用該帳戶。

  - 使用的適當參數修改其他屬性 `vserver cifs modify` 命令。

使用選項自訂**SMB**伺服器

可用的 **ONTAP SMB** 伺服器選項

在考量如何自訂SMB伺服器時、瞭解可用的選項很有用。雖然有些選項適用於SMB伺服器的一般用途、但有幾個選項可用來啟用和設定特定的SMB功能。SMB 伺服器選項由控制 `vserver cifs options modify` 選項。

下列清單指定可在管理權限層級使用的SMB伺服器選項：

- 設定**SMB**工作階段逾時值

設定此選項可讓您指定SMB工作階段中斷連線之前的閒置時間秒數。閒置工作階段是指使用者在用戶端上沒有開啟任何檔案或目錄的工作階段。預設值為 900 秒。

- 設定預設的**UNIX**使用者

  設定此選項可讓您指定SMB伺服器使用的預設UNIX使用者。自動建立名為「'pcuser'」的預設使用者（UID為65534）、建立名為「'pcuser'」的群組（gid為65534）、並將預設使用者新增至「'pcuser'」群組。ONTAP當您建立SMB伺服器時ONTAP 、支援將「'pcuser'」自動設定為預設UNIX使用者。

- 設定來賓**UNIX**使用者

  設定此選項可讓您指定從不受信任網域登入的使用者所對應的UNIX使用者名稱、如此可讓來自不受信任網域的使用者連線至SMB伺服器。根據預設、此選項並未設定（沒有預設值）；因此、預設值是不允許來自不受信任網域的使用者連線至SMB伺服器。

- *啟用或停用模式位元*的讀取授與執行

  啟用或停用此選項可讓您指定是否允許SMB用戶端以UNIX模式位元執行可執行檔、即使未設定UNIX執行檔位元、也能存取這些位元。此選項預設為停用。

- 啟用或停用從**NFS**用戶端刪除唯讀檔案的功能

  啟用或停用此選項可決定是否允許NFS用戶端刪除具有唯讀屬性集的檔案或資料夾。NTFS刪除語義不允許在設定唯讀屬性時刪除檔案或資料夾。UNIX刪除語義會忽略唯讀位元、改用父目錄權限來判斷是否可以刪除檔案或資料夾。預設設定為 `disabled`，從而產生 NTFS 刪除義。

- 設定**Windows**網際網路名稱服務伺服器位址

  設定此選項可讓您將Windows網際網路名稱服務（WINS）伺服器位址清單指定為以逗號分隔的清單。您必須指定IPV4位址。不支援IPv6位址。沒有預設值。

下列清單指定可在進階權限層級使用的SMB伺服器選項：

- 授予**CIFS**使用者**UNIX**群組權限

  設定此選項可決定是否可以將不是檔案擁有者的傳入CIFS使用者授予群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `true`，則會授予該檔案的群組權限。如果 CIFS 使用者不是 UNIX 安全樣式檔案的擁有者、則此參數會設為 `false`，然後，正常的 UNIX 規則適用於授予檔案權限。此參數適用於權限設為的 UNIX 安全性樣式檔案 `mode bits` 且不適用於 NTFS 或 NFSv4 安全模式的檔案。預設設定為 `false`。

- 啟用或停用**SMB 1.0**

  SMB 1.0在SVM上預設為停用、而SVM是在ONTAP SVM上建立SMB伺服器、以供使用。

  > 從功能9.3開始ONTAP 、ONTAP 根據預設、針對以功能9.3建立的新SMB伺服器、會停用SMB 1.0。您應該盡快移轉至較新的SMB版本、以準備增強安全性和法規遵循。如需詳細資訊、請聯絡您的NetApp代表。

- *啟用或停用SMB 2.x *

  SMB 2.0是支援LIF容錯移轉的最小SMB版本。如果停用SMB 2.x、ONTAP 則無法使用支援功能的功能也會

自動停用SMB 3.x

SMB 2.0僅在SVM上受支援。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.0*

  SMB 3.0是支援持續可用共用的最小SMB版本。Windows Server 2012和Windows 8是支援SMB 3.0的最低Windows版本。

  SMB 3.0 僅支援 SVM 。此選項在SVM上預設為啟用

- * 啟用或停用 SMB 3.1*

  Windows 10是唯一支援SMB 3.1的Windows版本。

  SMB 3.1 僅支援 SVM 。此選項在SVM上預設為啟用

- 啟用或停用**ODX**複本卸載

  支援ODX複本卸載的Windows用戶端會自動使用ODX複本卸載。此選項預設為啟用。

- 啟用或停用**ODX**複本卸載的直接複製機制

  當Windows用戶端嘗試以一種模式開啟複本的來源檔案時、直接複製機制可提高複本卸載作業的效能、避免在複本進行期間變更檔案。根據預設、直接複製機制會啟用。

- 啟用或停用自動節點參照

  使用自動節點參照時、SMB伺服器會自動將用戶端參照到本機資料LIF、並將其指向裝載透過所要求共用區存取資料的節點。

- *啟用或停用SMB*的匯出原則

  此選項預設為停用。

- 啟用或停用使用連接點做為重新分析點

  如果啟用此選項、SMB伺服器會將連接點公開給SMB用戶端做為重新分析點。此選項僅適用於SMB 2.x或SMB 3.0連線。此選項預設為啟用。

  此選項僅在SVM上受支援。此選項在SVM上預設為啟用

- 設定每個**TCP**連線同時執行的最大作業數

  預設值為 255 。

- 啟用或停用本機**Windows**使用者和群組功能

  此選項預設為啟用。

- 啟用或停用本機**Windows**使用者驗證

  此選項預設為啟用。

- 啟用或停用**VSS**陰影複製功能

  利用陰影複製功能、對使用Hyper-V over SMB解決方案儲存的資料執行遠端備份。ONTAP

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 設定陰影複製目錄深度

  設定此選項可讓您定義在使用陰影複製功能時建立陰影複製的目錄深度上限。

  此選項僅在SVM上受支援、僅在Hyper-V over SMB組態上受支援。此選項在SVM上預設為啟用

- 啟用或停用名稱對應的多網域搜尋功能

  如果啟用、當UNIX使用者透過在Windows使用者名稱的網域部分（例如*\Joe）中使用萬用字元（*）對應至Windows網域使用者時ONTAP 、將會在所有具有雙向信任的網域中搜尋指定使用者。主網域是包含SMB伺服器電腦帳戶的網域。

  除了搜尋雙向信任的所有網域之外、您也可以設定偏好的信任網域清單。如果啟用此選項且已設定偏好的清單、則會使用偏好的清單來執行多網域名稱對應搜尋。

  預設為啟用多網域名稱對應搜尋。

- 設定檔案系統區段大小

  設定此選項可讓您設定以位元組為單位的檔案系統區段大小、ONTAP 以便向SMB用戶端回報。此選項有兩個有效值： `4096` 和 `512`。預設值為 `4096`。您可能需要將此值設為 `512` 如果 Windows 應用程式僅支援 512 位元組的扇區大小。

- 啟用或停用動態存取控制

  啟用此選項可讓您使用動態存取控制（DAC）來保護SMB伺服器上的物件、包括使用稽核來登入中央存取原則、以及使用群組原則物件來實作中央存取原則。此選項預設為停用。

  此選項僅在SVM上受支援。

- 設定未驗證工作階段的存取限制（限制匿名）

  設定此選項可決定未驗證工作階段的存取限制。這些限制適用於匿名使用者。根據預設、匿名使用者沒有存取限制。

- 在具有**UNIX**有效安全性的磁碟區上啟用或停用**NTFS ACL**的呈現（**UNIX**安全型磁碟區或具有**UNIX**有效安全性的混合式安全型磁碟區）

  啟用或停用此選項可決定如何向SMB用戶端呈現具有UNIX安全性之檔案和資料夾的檔案安全性。如果啟用ONTAP 此功能、則使用NTFS ACL將具有UNIX安全性的磁碟區中的檔案和資料夾、顯示為具有NTFS檔案安全性。如果停用ONTAP 、則在不提供檔案安全性的情況下、將UNIX安全性的磁碟區顯示為FAT磁碟區。根據預設、磁碟區會以NTFS ACL的NTFS檔案安全性呈現。

- 啟用或停用**SMB**假開放功能

  啟用此功能可最佳化ONTAP 當查詢檔案和目錄的屬性資訊時、如何執行開放和關閉要求、進而改善SMB 2.x和SMB 3.0的效能。依預設、SMB假開放功能已啟用。此選項僅適用於使用SMB 2.x或更新版本的連線。

- 啟用或停用**UNIX**擴充功能

  啟用此選項可在SMB伺服器上啟用UNIX擴充功能。UNIX擴充功能可透過SMB傳輸協定顯示POSIX / UNIX類型的安全性。此選項預設為停用。

  如果您的環境中有UNIX型SMB用戶端（例如Mac OSX用戶端）、則應該啟用UNIX擴充功能。啟用UNIX擴充功能可讓SMB伺服器透過SMB將Posix / UNIX安全資訊傳輸到UNIX用戶端、然後將安全資訊轉譯為POSIX / UNIX安全性。

- 啟用或停用對簡短名稱搜尋的支援

  啟用此選項可讓SMB伺服器針對簡短名稱執行搜尋。啟用此選項的搜尋查詢會嘗試比對8.3檔名和長檔名。此參數的預設值為 `false`。

- *啟用或停用對自動通告DFS*功能的支援

  啟用或停用此選項可決定SMB伺服器是否自動向連線至共用的SMB 2.x和SMB 3.0用戶端通告DFS功能。在實作SMB存取的符號連結時、使用DFS轉介。ONTAP如果啟用、則無論是否啟用符號連結存取、SMB伺服器一律會通告DFS功能。如果停用、SMB伺服器只會在用戶端連線至啟用符號連結存取的共用時、才會通告「DFS功能」。

- 設定**SMB**點數上限

  從 ONTAP 9.4 開始、設定 `-max-credits` 選項可讓您在用戶端和伺服器執行 SMB 版本 2 或更新版本時、限制 SMB 連線上要授予的點數數量。預設值為 128 。

- *啟用或停用SMB多通道*支援

  啟用 `-is-multichannel-enabled` ONTAP 9.4 及更新版本中的選項可讓 SMB 伺服器在叢集及其用戶端上部署適當的 NIC 時、為單一 SMB 工作階段建立多個連線。這樣做可改善處理量和容錯能力。此參數的預設值為 `false`。

  啟用SMB多通道時、您也可以指定下列參數：

  - 每個多通道工作階段允許的最大連線數。此參數的預設值為 32 。
  - 每個多通道工作階段所通告的網路介面數量上限。此參數的預設值為 256 。

設定 **ONTAP SMB** 伺服器選項

您可以在儲存虛擬機器（SVM）上建立SMB伺服器之後、隨時設定SMB伺服器選項。

步驟

1. 執行所需的動作：

如果您要設定**SMB**伺服器選項…	輸入命令…
管理員權限等級	`vserver cifs options modify -vserver` *`vserver_name options`*

如果您要設定SMB伺服器選項...	輸入命令...
進階權限層級	a. `set -privilege advanced` b. `vserver cifs options modify -vserver vserver_name options` c. `set -privilege admin`

如"指令參考資料ONTAP"需瞭解及設定 SMB 伺服器選項的詳細 `vserver cifs options modify`資訊，請參閱。

設定 **ONTAP SMB** 使用者的「授與 **UNIX** 群組」權限

即使傳入的SMB使用者不是檔案的擁有者、您也可以設定此選項、以授予群組存取檔案或目錄的權限。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 視需要設定授予UNIX群組權限：

如果您想要	輸入命令
即使使用者不是檔案的擁有者、也能存取檔案或目錄、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others true`
即使使用者不是檔案的擁有者、也請停用檔案或目錄的存取權、以取得群組權限	`vserver cifs options modify -grant-unix-group-perms-to-others false`

3. 確認選項設定為所需的值： `vserver cifs options show -fields grant-unix-group-perms-to-others`
4. 返回管理權限層級： `set -privilege admin`

為匿名使用者設定 **ONTAP SMB** 存取限制

根據預設、匿名、未驗證的使用者（也稱為_null使用者_）可以存取網路上的特定資訊。您可以使用SMB伺服器選項來設定匿名使用者的存取限制。

關於這項工作

。 `-restrict-anonymous` SMB 伺服器選項對應於 `RestrictAnonymous` Windows 中的登錄項目。

匿名使用者可以從網路上的Windows主機列出或列舉特定類型的系統資訊、包括使用者名稱和詳細資料、帳戶原則和共用名稱。您可以指定下列三種存取限制設定之一來控制匿名使用者的存取：

價值	說明
`no-restriction` （預設）	不指定匿名使用者的存取限制。

價值	說明
`no-enumeration`	指定僅限匿名使用者進行列舉。
`no-access`	指定匿名使用者的存取受到限制。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定限制匿名設定： `vserver cifs options modify -vserver vserver_name -restrict -anonymous {no-restriction|no-enumeration|no-access}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver vserver_name`
4. 返回管理權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

管理如何向**SMB**用戶端提供**UNIX**安全型資料的檔案安全性

瞭解如何將 **ONTAP** 檔案安全性呈現給 **SMB** 用戶端，以取得 **UNIX** 安全性型資料

您可以啟用或停用將NTFS ACL呈現給SMB用戶端的功能、來選擇如何向SMB用戶端展示UNIX安全型資料的檔案安全性。每項設定都有優點、您應該瞭解如何選擇最適合您業務需求的設定。

根據預設、ONTAP 將UNIX安全型磁碟區上的UNIX權限以NTFS ACL形式呈現給SMB用戶端。有些情況需要這樣做、包括：

- 您想要使用「Windows內容」方塊中的「安全性」索引標籤來檢視及編輯UNIX權限。

  如果UNIX系統不允許此作業、您就無法從Windows用戶端修改權限。例如、您無法變更您不擁有的檔案所有權、因為UNIX系統不允許此作業。此限制可防止SMB用戶端略過在檔案和資料夾上設定的UNIX權限。

- 使用者使用某些Windows應用程式（例如Microsoft Office）來編輯及儲存UNIX安全型磁碟區上的檔案、ONTAP 而在這些應用程式中、當執行儲存作業時、必須保留UNIX權限。
- 您環境中有些Windows應用程式預期會讀取其所使用檔案的NTFS ACL。

在某些情況下、您可能會想要停用將UNIX權限呈現為NTFS ACL的功能。如果停用此功能、ONTAP 則將UNIX安全型磁碟區顯示為SMB用戶端的FAT磁碟區。您可能會想要將UNIX安全型磁碟區以FAT磁碟區的形式呈現給SMB用戶端的具體理由如下：

- 您只能在UNIX用戶端上使用掛載來變更UNIX權限。

  當SMB用戶端上對應UNIX安全型磁碟區時、「安全性」索引標籤將無法使用。對應的磁碟機似乎是以不具檔案權限的檔案系統格式化。

- 您正在使用SMB上的應用程式、在存取的檔案和資料夾上設定NTFS ACL、如果資料位於UNIX安全型磁碟區、則這些應用程式可能會失敗。

如果ONTAP 將磁碟區報告為「FAT」、應用程式就不會嘗試變更ACL。

相關資訊

- 在FlexVol 功能區上設定安全樣式
- 在qtree上設定安全性樣式

設定 **NTFS ACL** 呈現給 **ONTAP SMB** 用戶端以取得 **UNIX** 安全性型資料

您可以針對UNIX安全型資料（UNIX安全型磁碟區和混合式安全型磁碟區、以及UNIX有效安全性）、啟用或停用將NTFS ACL呈現給SMB用戶端的功能。

關於這項工作

如果啟用此選項、ONTAP 則將具有有效UNIX安全樣式的磁碟區上的檔案和資料夾、呈現給SMB用戶端、如同使用NTFS ACL。如果停用此選項、磁碟區會以FAT磁碟區的形式呈現給SMB用戶端。預設為向SMB用戶端顯示NTFS ACL。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 設定 UNIX NTFS ACL 選項設定： `vserver cifs options modify -vserver vserver_name -is-unix-nt-acl-enabled {true|false}`
3. 確認選項設定為所需的值： `vserver cifs options show -vserver vserver_name`
4. 返回管理權限層級： `set -privilege admin`

瞭解如何保留 **ONTAP SMB FlexVol** 磁碟區的 **UNIX** 權限

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

瞭解如何使用適用於 **ONTAP SMB** 伺服器的 **Windows** 安全性索引標籤來管理 **UNIX** 權限

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

  您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全性型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

  您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全性型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

  您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全性型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

  變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。

管理**SMB**伺服器安全性設定

瞭解如何處理 **ONTAP SMB** 用戶端驗證

使用者必須先由SMB伺服器所屬的網域驗證、才能建立SMB連線來存取SVM上所含的資料。SMB伺服器支援兩種驗證方法：Kerberos和NTLM（位在NTLMv1或NTLMv2之間）。Kerberos是用於驗證網域使用者的預設方法。

Kerberos驗證

建立驗證的SMB工作階段時、支援Kerberos驗證。ONTAP

Kerberos是Active Directory的主要驗證服務。Kerberos伺服器或Kerberos金鑰發佈中心（Kdc）服務會在Active Directory中儲存及擷取安全性原則的相關資訊。與NTLM模式不同的是、Active Directory用戶端若想要與另一部電腦（例如SMB伺服器）建立工作階段、請直接聯絡Kdc以取得其工作階段認證。

NTLM 驗證

以密碼為基礎、根據使用者專屬密碼的共享知識、使用挑戰回應傳輸協定來完成NTLM用戶端驗證。

如果使用者使用本機 Windows 使用者帳戶建立 SMB 連線、則驗證作業會由 SMB 伺服器使用 NTLMv2 在本機完成。

瞭解 **ONTAP SVM** 災難恢復組態的 **SMB** 伺服器安全性設定

建立 SVM 之前、請先將其設定為災難恢復目的地、但不會保留身分識別（ `-identity-preserve` 選項設定為 `false` 在 SnapMirror 組態中）、您應該知道如何在目的地 SVM 上管理 SMB 伺服器安全性設定。

- 非預設的SMB伺服器安全性設定不會複寫到目的地。

  當您在目的地SVM上建立SMB伺服器時、所有SMB伺服器安全性設定都會設為預設值。當SVM災難恢復目的地初始化、更新或重新同步時、來源上的SMB伺服器安全性設定不會複寫到目的地。

- 您必須手動設定非預設的SMB伺服器安全性設定。

如果您在來源SVM上設定了非預設的SMB伺服器安全性設定、則必須在目的地SVM變成讀寫（SnapMirror關係中斷之後）之後、在目的地上手動設定這些相同的設定。

顯示 **ONTAP SMB** 伺服器安全性設定的相關資訊

您可以在儲存虛擬機器（SVM）上顯示SMB伺服器安全性設定的相關資訊。您可以使用此資訊來驗證安全性設定是否正確。

關於這項工作

顯示的安全性設定可以是該物件的預設值、也可以是透過ONTAP 使用列舉CLI或使用Active Directory群組原則物件（GPO）設定的非預設值。

請勿使用 `vserver cifs security show` 工作群組模式中 SMB 伺服器的命令、因為某些選項無效。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
指定SVM上的所有安全性設定	`vserver cifs security show -vserver` *`vserver_name`*
SVM上的特定安全性設定或設定	`vserver cifs security show -vserver _vserver_name_ -fields [fieldname,...]` 您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

範例

下列範例顯示SVM VS1的所有安全性設定：

```
cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                           Kerberos Clock Skew:        5 minutes
                           Kerberos Ticket Age:        10 hours
                          Kerberos Renewal Age:        7 days
                          Kerberos KDC Timeout:        3 seconds
                           Is Signing Required:        false
                Is Password Complexity Required:        true
          Use start_tls For AD LDAP connection:        false
                      Is AES Encryption Enabled:        false
                         LM Compatibility Level:        lm-ntlm-ntlmv2-krb
                     Is SMB Encryption Required:        false
                        Client Session Security:        none
               SMB1 Enabled for DC Connections:        false
               SMB2 Enabled for DC Connections:        system-default
LDAP Referral Enabled For AD LDAP connections:        false
              Use LDAPS for AD LDAP connection:        false
    Encryption is required for DC Connections:        false
 AES session key enabled for NetLogon channel:        false
  Try Channel Binding For AD LDAP Connections:        false
```

請注意、顯示的設定取決於執行ONTAP 中的版本。

以下範例顯示SVM VS1的Kerberos時鐘偏移：

```
cluster1::> vserver cifs security show -vserver vs1 -fields kerberos-
clock-skew

            vserver kerberos-clock-skew
            ------- -------------------
            vs1     5
```

相關資訊

顯示有關GPO組態的資訊

為本機 SMB 使用者設定 ONTAP 密碼複雜度

所需的密碼複雜度可為儲存虛擬機器（SVM）上的本機SMB使用者提供更高的安全性。預設會啟用所需的密碼複雜度功能。您可以隨時停用並重新啟用。

開始之前

必須在CIFS伺服器上啟用本機使用者、本機群組和本機使用者驗證。

關於這項工作

請勿在工作群組模式中使用 `vserver cifs security modify` CIFS 伺服器的命令，因為某些選項無效。

步驟

1. 執行下列其中一項動作：

如果您想讓本機SMB使用者的密碼複雜度達到所需...	輸入命令...
已啟用	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required true`
已停用	`vserver cifs security modify -vserver vserver_name -is-password-complexity -required false`

2. 驗證所需密碼複雜度的安全性設定： `vserver cifs security show -vserver vserver_name`

範例

以下範例顯示、SVM VS1的本機SMB使用者已啟用必要的密碼複雜度：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-password
-complexity-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-password-
complexity-required
vserver is-password-complexity-required
------- -------------------------------
vs1     true
```

相關資訊

- 顯示有關伺服器安全設定的信息
- 了解本地用戶和群組
- 本機使用者密碼需求
- 變更本機使用者帳戶密碼

修改 **ONTAP SMB** 伺服器 **Kerberos** 安全性設定

您可以修改某些CIFS伺服器Kerberos安全性設定、包括允許的Kerberos時鐘偏移時間上限、Kerberos票證壽命、以及票證續約天數上限。

關於這項工作

使用修改 CIFS 伺服器 Kerberos 設定 `vserver cifs security modify` 命令只會修改您使用指定的單一儲存虛擬機器（ SVM ）上的設定 `-vserver` 參數。您可以使用Active Directory群組原則物件（GPO）、集中管理屬於同一個Active Directory網域之叢集上所有SVM的Kerberos安全性設定。

步驟

1. 執行下列一或多項動作：

如果您想要…	輸入…
指定允許的 Kerberos 時鐘偏差時間上限（以分鐘為單位（ 9.13.1 及更新版本）或秒（ 9.12.1 或更新版本）。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-clock-skew` *`integer_in_minutes`* 預設設定為5分鐘。
以小時為單位指定Kerberos票證壽命。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-ticket-age integer_in_hours` 預設設定為10小時。
指定通知單續約天數上限。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-renew-age` *`integer_in_days`* 預設設定為7天。
指定KDC上的通訊端逾時、之後所有KDC都會標示為無法連線。	`vserver cifs security modify -vserver` *`vserver_name`* `-kerberos-kdc-timeout` *`integer_in_seconds`* 預設設定為3秒。

2. 驗證Kerberos安全性設定：

   `vserver cifs security show -vserver` *`vserver_name`*

範例

下列範例對Kerberos安全性進行下列變更：「Kerberos時鐘偏移」設為3分鐘、而SVM VS1的「Kerberos票證時間」設為8小時：

```
cluster1::> vserver cifs security modify -vserver vs1 -kerberos-clock-skew
3 -kerberos-ticket-age 8

cluster1::> vserver cifs security show -vserver vs1

Vserver: vs1

                    Kerberos Clock Skew:                    3 minutes
                    Kerberos Ticket Age:                    8 hours
                  Kerberos Renewal Age:                     7 days
                  Kerberos KDC Timeout:                     3 seconds
                    Is Signing Required:                false
        Is Password Complexity Required:                 true
   Use start_tls For AD LDAP connection:                false
              Is AES Encryption Enabled:                false
                 LM Compatibility Level:  lm-ntlm-ntlmv2-krb
             Is SMB Encryption Required:                false
```

相關資訊

"顯示有關伺服器安全設定的信息"

"支援的GPO"

"將群組原則物件套用至CIFS伺服器"

設定 **ONTAP SMB** 伺服器的最低驗證安全層級

您可以在SMB伺服器上設定SMB伺服器的最低安全性層級（也稱為_LMCompatibilityLevel）、以符合SMB用戶端存取的企業安全性需求。最低安全層級是SMB伺服器從SMB用戶端接受的安全性權杖最低層級。

關於這項工作

- 工作群組模式中的SMB伺服器僅支援NTLM驗證。不支援Kerberos驗證。
- LMCompatibilityLevel僅適用於SMB用戶端驗證、不適用於管理驗證。

您可以將最低驗證安全性層級設為四種支援的安全性層級之一。

價值	說明
`lm-ntlm-ntlmv2-krb` （預設）	儲存虛擬機器（SVM）接受LM、NTLM、NTLMv2及Kerberos驗證安全性。
`ntlm-ntlmv2-krb`	SVM接受NTLM、NTLMv2及Kerberos驗證安全性。SVM拒絕LM驗證。

價值	說明
`ntlmv2-krb`	SVM接受NTLMv2和Kerberos驗證安全性。SVM拒絕LM和NTLM驗證。
`krb`	SVM僅接受Kerberos驗證安全性。SVM會拒絕LM、NTLM及NTLMv2驗證。

步驟

1. 設定最低驗證安全層級： `vserver cifs security modify -vserver vserver_name -lm -compatibility-level {lm-ntlm-ntlmv2-krb|ntlm-ntlmv2-krb|ntlmv2-krb|krb}`
2. 驗證驗證安全性層級是否設為所需層級： `vserver cifs security show -vserver vserver_name`

相關資訊

為基於 Kerberos 的通訊配置 AES 加密

使用 **AES** 加密，為 **Kerberos** 型通訊設定強大的 **ONTAP SMB** 安全性

為了以Kerberos為基礎的通訊提供最強大的安全性、您可以在SMB伺服器上啟用AES-256和AES-128加密。根據預設、當您在SVM上建立SMB伺服器時、會停用進階加密標準（AES）加密。您必須讓IT能夠充分利用AES加密所提供的強大安全性。

SMB的Kerberos相關通訊是在SVM上建立SMB伺服器期間、以及SMB工作階段設定階段期間使用。SMB伺服器支援下列Kerberos通訊加密類型：

- AES 256
- AES 128
- 第
- RC4-HMAC

如果您想要使用最高的安全性加密類型進行Kerberos通訊、您應該在SVM上啟用AES加密來進行Kerberos通訊。

建立SMB伺服器時、網域控制器會在Active Directory中建立電腦帳戶。此時、Kdc會得知特定機器帳戶的加密功能。之後、會選取特定的加密類型來加密用戶端在驗證期間向伺服器顯示的服務票證。

從ONTAP 《支援資料》9.12.1開始、您可以指定要向Active Directory（AD）kdc通告的加密類型。您可以使用`-advertised-enc-types`選項來啟用建議的加密類型，也可以使用它來停用較弱的加密類型。瞭解如何"為基於 Kerberos 的通訊配置 AES 加密"。

SMB 3.0提供Intel AES新指令（Intel AES NI）、可改善AES演算法、並以支援的處理器系列產品加速資料加密。從SMB 3.3.1開始、AES-120-GCM取代AES-120-CCMs做為SMB加密所使用的雜湊演算法。

相關資訊

修改伺服器安全設定

若要利用以 Kerberos 為基礎的通訊所提供的最強大安全性、您應該在 SMB 伺服器上使用 AES-256 和 AES-128 加密。從 ONTAP 9.13.1 開始、預設會啟用 AES 加密。 如果您不希望SMB伺服器選取AES加密類型、以便與Active Directory（AD）kdc進行Kerberos型通訊、您可以停用AES加密。

是否預設啟用 AES 加密、以及您是否可以選擇指定加密類型、取決於您的 ONTAP 版本。

版本**ONTAP**	**AES** 加密已啟用 **...**	您可以指定加密類型嗎？
9.13.1 及更新版本	依預設	是的
9.12.1	手動	是的
9.11.1 及更早版本	手動	否

從ONTAP 功能支援的9.12.1開始、AES加密會使用啟用和停用 `-advertised-enc-types` 選項、可讓您指定通告給AD Kdc的加密類型。預設設定為 `rc4` 和 `des`，但當指定AES類型時，將會啟用AES加密。您也可以使用選項來明確停用較弱的RC4和DES加密類型。在 ONTAP 9.11.1 及更早版本中、您必須使用 `-is-aes-encryption-enabled` 啟用和停用AES加密的選項、無法指定加密類型。

為了增強安全性、儲存虛擬機器（SVM）會在每次修改AES安全性選項時、變更AD中的機器帳戶密碼。變更密碼可能需要包含機器帳戶的組織單位（OU）的系統管理AD認證。

如果 SVM 設定為災難恢復目的地、而該目的地不會保留身分識別（ `-identity-preserve` 選項設定為 `false` 在 SnapMirror 組態中）、非預設 SMB 伺服器安全性設定不會複寫到目的地。如果您已在來源 SVM 上啟用 AES 加密、則必須手動啟用。

範例 **13.** 步驟

更新版本**ONTAP**

1. 執行下列其中一項動作：

如果您希望**Kerberos**通訊的**AES**加密類型…	輸入命令…
已啟用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types aes-128,aes-256`
已停用	`vserver cifs security modify -vserver vserver_name -advertised -enc-types des,rc4`

附註： The `-is-aes-encryption-enabled` 選項在ONTAP 更新版本中已過時、可能會在更新版本中移除。

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields advertised-enc-types`

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
cluster1::> vserver cifs security modify -vserver vs1 -advertised-enc
-types aes-128,aes-256

cluster1::> vserver cifs security show -vserver vs1 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs1      aes-128,aes-256
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
cluster1::> vserver cifs security modify -vserver vs2 -advertised-enc
-types aes-128,aes-256

Info: In order to enable SMB AES encryption, the password for the SMB
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields advertised-
enc-types

vserver  advertised-enc-types
-------- --------------------
vs2      aes-128,aes-256
```

更新版本**ONTAP**

1. 執行下列其中一項動作：

如果您希望**Kerberos**通訊的**AES**加密類型...	輸入命令...
已啟用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled true`
已停用	`vserver cifs security modify -vserver vserver_name -is-aes -encryption-enabled false`

2. 確認已視需要啟用或停用AES加密： `vserver cifs security show -vserver vserver_name -fields is-aes-encryption-enabled`

   ◦ `is-aes-encryption-enabled` 欄位隨即顯示 `true` 如果已啟用 AES 加密、且 `false` 如果已停用。

範例

以下範例可為 SVM VS1 上的 SMB 伺服器啟用 AES 加密類型：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-aes
-encryption-enabled true

cluster1::> vserver cifs security show -vserver vs1 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs1      true
```

下列範例可為SVM VS2上的SMB伺服器啟用AES加密類型。系統會提示系統管理員輸入包含SMB伺服器之OU的管理AD認證。

```
cluster1::> vserver cifs security modify -vserver vs2 -is-aes
-encryption-enabled true

Info: In order to enable SMB AES encryption, the password for the CIFS
server
machine account must be reset. Enter the username and password for the
SMB domain "EXAMPLE.COM".

Enter your user ID: administrator

Enter your password:

cluster1::> vserver cifs security show -vserver vs2 -fields is-aes-
encryption-enabled

vserver  is-aes-encryption-enabled
-------- -------------------------
vs2      true
```

相關資訊

"網域使用者無法使用網域通道登入叢集"

使用**SMB**簽署來強化網路安全性

瞭解如何使用 **ONTAP SMB** 簽署來增強網路安全性

SMB簽章有助於確保SMB伺服器與用戶端之間的網路流量不會受到影響、並可防止重播攻擊。根據預設ONTAP 、若用戶端要求、支援SMB簽署。或者、儲存管理員可以將SMB伺服器設定為需要SMB簽署。

除了CIFS伺服器SMB簽署安全性設定之外、Windows用戶端上的兩個SMB簽署原則也會控制用戶端與CIFS伺服器之間的通訊數位簽署。您可以設定符合業務需求的設定。

用戶端SMB原則是透過Windows本機安全性原則設定來控制、這些設定是使用Microsoft管理主控台（MMC）或Active Directory GPO來設定。如需用戶端SMB簽署與安全性問題的詳細資訊、請參閱Microsoft Windows文件。

以下是Microsoft用戶端上兩種SMB簽署原則的說明：

- `Microsoft network client: Digitally sign communications (if server agrees)`

  此設定可控制是否啟用用戶端的SMB簽署功能。預設為啟用。當用戶端停用此設定時、與CIFS伺服器的用戶端通訊取決於CIFS伺服器上的SMB簽署設定。

- `Microsoft network client: Digitally sign communications (always)`

  此設定可控制用戶端是否需要SMB簽署才能與伺服器通訊。預設為停用。當用戶端上停用此設定時、 SMB簽署行為會根據的原則設定而定 `Microsoft network client: Digitally sign communications (if server agrees)` 以及 CIFS 伺服器上的設定。

> ⓘ 如果您的環境包含設定為需要SMB簽署的Windows用戶端、則必須在CIFS伺服器上啟用SMB簽署。如果您沒有、CIFS伺服器就無法將資料提供給這些系統。

用戶端和CIFS伺服器SMB簽署設定的有效結果取決於SMB工作階段是使用SMB 1.0或SMB 2.x或更新版本。

下表摘要說明當工作階段使用SMB 1.0時的有效SMB簽署行為：

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
簽署已停用且不需要	未簽署	已簽署
簽署已啟用且不需要	未簽署	已簽署
簽署已停用且必要	已簽署	已簽署
簽署已啟用且必要	已簽署	已簽署

> ⓘ 舊版Windows SMB 1用戶端和部分非Windows SMB 1用戶端若在用戶端上停用簽署、但CIFS伺服器上需要簽署、則可能無法連線。

下表摘要說明當工作階段使用SMB 2.x或SMB 3.0時的有效SMB簽署行為：

> ⓘ 對於SMB 2.x和SMB 3.0用戶端、一律會啟用SMB簽署。無法停用。

用戶端	**ONTAP** -不需要簽署	**ONTAP** -需要簽署
不需要簽署	未簽署	已簽署
需要簽署	已簽署	已簽署

下表摘要說明預設的Microsoft用戶端和伺服器SMB簽署行為：

傳輸協定	雜湊演算法	可啟用/停用	可能需要/不需要	用戶端預設值	伺服器預設值	**DC**預設值
SMB 1.0	md5	是的	是的	已啟用（非必要）	已停用（非必要）	必要
SMB 2.x	HMAC SHA-256	否	是的	不需要	不需要	必要
SMB 3.0	AES-CMAC：	否	是的	不需要	不需要	必要

Microsoft 不再建議使用 `Digitally sign communications (if client agrees)` 或 `Digitally sign communications (if server agrees)` 群組原則設定。Microsoft 也不再建議使用 `EnableSecuritySignature` 登錄設定。這些選項只會影響 SMB 1 行為、可由取代 `Digitally sign communications (always)` 群組原則設定或 `RequireSecuritySignature` 登錄設定。您也可以從 Microsoft 部落格取得更多資訊。 The SMB 簽署基礎知識（涵蓋 SMB1 和 SMB2 ）

瞭解 **ONTAP SMB** 簽署對效能的影響

當SMB工作階段使用SMB簽署時、所有往返Windows用戶端的SMB通訊都會受到效能影響、這會影響用戶端和伺服器（亦即、叢集上執行SVM的節點包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 簽署的SMB流量中提供更好的效能。啟用SMB簽署時、預設會啟用SMB簽署卸載。

增強的SMB簽署效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB簽署的效能影響可能會有很大差異；您只能在網路環境中進行測試來驗證。

如果伺服器上已啟用SMB簽署、則大部分的Windows用戶端會依預設協調SMB簽署。如果您的部分Windows用戶端需要SMB保護、而且SMB簽章造成效能問題、您可以在任何不需要保護以防止重播攻擊的Windows用戶端上停用SMB簽署。如需在Windows用戶端上停用SMB簽署的相關資訊、請參閱Microsoft Windows文件。

ONTAP SMB 簽署組態建議

您可以設定SMB用戶端與CIFS伺服器之間的SMB簽署行為、以符合您的安全需求。您在CIFS伺服器上設定SMB簽署時所選擇的設定、取決於您的安全需求。

您可以在用戶端或CIFS伺服器上設定SMB簽署。設定SMB簽署時、請考慮下列建議：

如果...	建議...
您想要提高用戶端與伺服器之間通訊的安全性	啟用、讓用戶端需要 SMB 簽署 `Require Option (Sign always)` 用戶端上的安全性設定。
您希望所有SMB流量都簽署到特定的儲存虛擬機器（SVM）	設定安全性設定以要求SMB簽署、使CIFS伺服器上的SMB簽署成為必要項目。

如需設定Windows用戶端安全性設定的詳細資訊、請參閱Microsoft文件。

瞭解多重資料生命的 **ONTAP SMB** 簽署組態

如果您在SMB伺服器上啟用或停用必要的SMB簽署、您應該瞭解SVM多重資料生命量組態的準則。

設定SMB伺服器時、可能會設定多個資料生命量。如果是、則 DNS 伺服器包含多個 `A` 記錄 CIFS 伺服器的項目、所有項目都使用相同的 SMB 伺服器主機名稱、但每個項目都有唯一的 IP 位址。例如、已設定兩個資料生命期的 SMB 伺服器可能具有下列 DNS `A` 記錄項目：

```
10.1.1.128 A VS1.IEPUB.LOCAL VS1
10.1.1.129 A VS1.IEPUB.LOCAL VS1
```

正常情況是、變更必要的SMB簽署設定後、只有來自用戶端的新連線會受到SMB簽署設定的變更影響。不過、這種行為有例外。在某種情況下、用戶端與共用有現有的連線、而用戶端會在變更設定之後、建立新的連線至同一個共用區、同時維持原始連線。在這種情況下、新的和現有的SMB連線都會採用新的SMB簽署要求。

請考慮下列範例：

1. Client1 連接到共享區、而不需要使用路徑簽署 SMB `O:\`。
2. 儲存管理員會修改SMB伺服器組態、以要求SMB簽署。
3. Client1 會使用路徑連線到具有必要 SMB 簽署的同一個共用區 `S:\` （同時使用路徑維持連線 `O:\`）。
4. 結果是在存取兩者的資料時、會使用 SMB 簽署 `O:\` 和 `S:\` 磁碟機。

為傳入的 **SMB** 流量設定 **ONTAP** 簽署

您可以啟用必要的SMB簽署、強制要求用戶端簽署SMB訊息。如果啟用ONTAP 、僅當SMB訊息具有有效的簽名時、才會接受該訊息。如果您想要允許SMB簽署、但不需要SMB簽署、可以停用必要的SMB簽署。

關於這項工作

預設會停用必要的SMB簽署。您可以隨時啟用或停用所需的SMB簽署。

在下列情況下、預設不會停用SMB簽署：

1. 啟用必要的SMB簽署、叢集將還原為ONTAP 不支援SMB簽署的版本。
2. 叢集隨後會升級至ONTAP 支援SMB簽署的版本的支援。

   在這種情況下、原本設定在支援版本ONTAP 的支援版本上的SMB簽署組態會透過還原及後續升級來保留。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 簽署安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 簽署安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用必要的SMB簽署、則必須在目的地SVM上手動啟用必要的SMB簽署。

步驟

1. 執行下列其中一項動作：

如果您想要**SMB**簽署...	輸入命令...
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required true`
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-signing-required false`

2. 判斷中的值是否已啟用或停用必要的 SMB 簽署 `Is Signing Required` 下列命令輸出中的欄位設定為所需的值： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-signing-required`

範例

下列範例可為SVM VS1啟用必要的SMB簽署：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-signing-required
true

cluster1::> vserver cifs security show -vserver vs1 -fields is-signing-
required
vserver  is-signing-required
-------- --------------------
vs1      true
```

對加密設定的變更會對新連線生效。現有連線不受影響。

相關資訊

- "SnapMirror建立"

判斷 **ONTAP SMB** 工作階段是否已簽署

您可以在CIFS伺服器上顯示連線SMB工作階段的相關資訊。您可以使用此資訊來判斷SMB工作階段是否已簽署。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
指定儲存虛擬機器（SVM）上的所有簽署工作階段	`vserver cifs session show -vserver` *`vserver_name`* `-is-session-signed true`
在SVM上具有特定工作階段ID的已簽署工作階段詳細資料	`vserver cifs session show -vserver` *`vserver_name`* `-session-id integer -instance`

範例

下列命令會顯示SVM VS1上已簽署工作階段的相關工作階段資訊。預設的摘要輸出不會顯示「Is Session Signed」（已簽署的工作階段）輸出欄位：

```
cluster1::> vserver cifs session show -vserver vs1 -is-session-signed true
Node:    node1
Vserver: vs1
Connection Session                                      Open          Idle
ID         ID      Workstation      Windows User     Files         Time
---------- ------- ---------------- ------------- ------- ------------
3151272279 1       10.1.1.1         DOMAIN\joe           2          23s
```

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括工作階段是否已簽署：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                          Node: node1
                       Vserver: vs1
                    Session ID: 2
                 Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                   Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

相關資訊

監控SMB簽署的工作階段統計資料

監控 **ONTAP SMB** 簽署的工作階段統計資料

您可以監控SMB工作階段統計資料、並判斷哪些已建立的工作階段已簽署、哪些尚未簽署。

關於這項工作

。 `statistics` 進階權限層級的命令提供 `signed_sessions` 可用來監控已簽署 SMB 工作階段數量的計數器。。 `signed_sessions` 下列統計資料物件可使用計數器：

- `cifs` 可讓您監控所有 SMB 工作階段的 SMB 簽署。
- `smb1` 可讓您監控 SMB 1.0 工作階段的 SMB 簽署。
- `smb2` 可讓您監控 SMB 2.x 和 SMB 3.0 工作階段的 SMB 簽署。

  的輸出中包含 SMB 3.0 統計資料 `smb2` 物件：

如果您想要比較已簽署工作階段的數目與工作階段總數、您可以比較的輸出 `signed_sessions` 以的輸出進行計數 `established_sessions` 計數器。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+
   `statistics start -object {cifs|smb1|smb2} -instance instance -sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

   如"指令參考資料ONTAP"需詳細 `statistics start`資訊，請參閱。
3. 使用 `statistics stop` 停止收集樣本資料的命令。

   詳細了解 `statistics stop`在"指令參考資料ONTAP" 。
4. 檢視SMB簽署統計資料：

如果您要檢視下列項目的資訊...	輸入...
已簽署的工作階段	`show -sample-id sample_ID -counter signed_sessions
node_name [-node *node_name*]`	已簽署的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter signed_sessions	established_sessions

   如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

   如"指令參考資料ONTAP"需詳細 `statistics show`資訊，請參閱。
5. 返回管理權限層級：
   `set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 2.x和SMB 3.0簽署統計資料。

下列命令會移至進階權限層級：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

下列命令會啟動新範例的資料收集：

```
cluster1::*> statistics start -object smb2 -sample-id smbsigning_sample
-vserver vs1
Statistics collection is being started for Sample-id: smbsigning_sample
```

下列命令會停止範例的資料收集：

```
cluster1::*> statistics stop -sample-id smbsigning_sample
Statistics collection is being stopped for Sample-id: smbsigning_sample
```

下列命令會顯示已簽署的SMB工作階段、以及範例中各節點所建立的SMB工作階段：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|established_sessions|node_name

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:03:04
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    established_sessions                                         0
    node_name                                                node1
    signed_sessions                                              0
    established_sessions                                         1
    node_name                                                node2
    signed_sessions                                              1
    established_sessions                                         0
    node_name                                                node3
    signed_sessions                                              0
    established_sessions                                         0
    node_name                                                node4
    signed_sessions                                              0
```

以下命令顯示節點2的簽署SMB工作階段：

```
cluster1::*> statistics show -sample-id smbsigning_sample -counter
signed_sessions|node_name -node node2

Object: smb2
Instance: vs1
Start-time: 2/6/2013 01:00:00
End-time: 2/6/2013 01:22:43
Cluster: cluster1

    Counter                                                  Value
    -------------------------------- ------------------------
    node_name                                                node2
    signed_sessions                                              1
```

下列命令會移回管理權限層級：

```
cluster1::*> set -privilege admin
```

相關資訊

- 判斷SMB工作階段是否已簽署
- "效能監控與管理總覽"

在**SMB**伺服器上設定必要的**SMB**加密、以便透過**SMB**傳輸資料

瞭解 **ONTAP SMB** 加密

SMB加密可在SMB伺服器上啟用或停用SMB資料傳輸功能、是一項安全性增強功能。您也可以透過共用內容設定、逐一設定所需的SMB加密設定。

根據預設、當您在儲存虛擬機器（ SVM ）上建立 SMB 伺服器時、 SMB 加密會停用。您必須讓IT能夠充分利用SMB加密所提供的增強安全性。

若要建立加密的SMB工作階段、SMB用戶端必須支援SMB加密。從Windows Server 2012和Windows 8開始的Windows用戶端支援SMB加密。

SVM上的SMB加密可透過兩種設定加以控制：

- SMB 伺服器安全選項、可在 SVM 上啟用功能
- SMB 共用屬性，可依每個共用區設定 SMB 加密設定

您可以決定是否需要加密才能存取SVM上的所有資料、或是需要SMB加密才能存取所選共用區中的資料。SVM層級的設定會取代共用層級的設定。

有效的SMB加密組態取決於兩項設定的組合、如下表所述：

啟用**SMB**伺服器**SMB**加密	共用加密資料設定已啟用	伺服器端加密行為
是的	錯	SVM中的所有共用都啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
是的	是的	無論共用層級加密為何、SVM中的所有共用都會啟用伺服器層級加密。有了這項組態、整個SMB工作階段就會進行加密。
錯	是的	特定共用區已啟用共用層級加密。使用此組態、即可從樹狀結構連線進行加密。
錯	錯	未啟用加密。

不支援加密的 SMB 用戶端無法連線至需要加密的 SMB 伺服器或共用區。

對加密設定的變更會對新連線生效。現有連線不受影響。

瞭解 **ONTAP SMB** 加密對效能的影響

當SMB工作階段使用SMB加密時、所有往返Windows用戶端的SMB通訊都會受到效能影響、影響用戶端和伺服器（亦即叢集上執行SVM的節點、其中包含SMB伺服器）。

效能影響顯示用戶端和伺服器的CPU使用量增加、不過網路流量並未改變。

效能影響的程度取決於ONTAP 您所執行的版本的VMware®。從推出全新的加密卸載演算法、即可在ONTAP 加密的SMB流量中提供更好的效能。啟用SMB加密時、預設會啟用SMB加密卸載。

增強的SMB加密效能需要AES-NI卸載功能。請參閱Hardware Universe 《支援資料》（HWU）、確認您的平台是否支援AES-NI卸載。

如果您能夠使用支援速度更快的 GCM 演算法的 SMB 版本 3.11 、也可以進一步改善效能。

視您的網路ONTAP 、支援的版本為VMware、SMB版本及SVM實作而定、SMB加密的效能影響可能會有很大差異、您只能在網路環境中進行測試來驗證。

SMB加密在SMB伺服器上預設為停用。您只能在需要加密的SMB共用區或SMB伺服器上啟用SMB加密。藉由SMB加密、ONTAP 支援進一步處理解密要求、並加密每個要求的回應。因此、只有在必要時才應啟用SMB加密。

啟用或停用傳入流量的 **ONTAP SMB** 加密

如果您想為傳入的SMB流量要求SMB加密、可以在CIFS伺服器或共用層級啟用SMB加密。根據預設、不需要SMB加密。

關於這項工作

您可以在CIFS伺服器上啟用SMB加密、此功能適用於CIFS伺服器上的所有共用。如果您不希望CIFS伺服器上的所有共用都需要SMB加密、或是想要針對每個共用區的傳入SMB流量啟用必要的SMB加密、可以停用CIFS伺服器上所需的SMB加密。

當您設定儲存虛擬機器（ SVM ）災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、 SMB 加密安全性設定會複寫到目的地。

如果您設定 `-identity-preserve` 選項 `false` （非 ID-preserve ）、 SMB 加密安全性設定不會複寫到目的地。在此情況下、目的地上的CIFS伺服器安全性設定會設為預設值。如果您已在來源SVM上啟用SMB加密、則必須在目的地上手動啟用CIFS伺服器SMB加密。

步驟

1. 執行下列其中一項動作：

如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能**...**	輸入命令**...**
已啟用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required true`

如果您想要**CIFS**伺服器上傳入**SMB**流量的**SMB**加密功能...	輸入命令...
已停用	`vserver cifs security modify -vserver` *`vserver_name`* `-is-smb-encryption -required false`

2. 確認 CIFS 伺服器上所需的 SMB 加密已視需要啟用或停用： `vserver cifs security show -vserver` *`vserver_name`* `-fields is-smb-encryption-required`

   。 `is-smb-encryption-required` 欄位隨即顯示 `true` 如果需要、會在 CIFS 伺服器和上啟用 SMB 加密 `false` 如果已停用。

範例

下列範例為SVM VS1上的CIFS伺服器啟用必要的SMB加密功能：

```
cluster1::> vserver cifs security modify -vserver vs1 -is-smb-encryption
-required true

cluster1::> vserver cifs security show -vserver vs1 -fields is-smb-
encryption-required
vserver  is-smb-encryption-required
-------- --------------------------
vs1      true
```

相關資訊

- "SnapMirror建立"

判斷用戶端是否使用加密的 **ONTAP SMB** 工作階段連線

您可以顯示連線SMB工作階段的相關資訊、以判斷用戶端是否使用加密的SMB連線。這有助於判斷SMB用戶端工作階段是否與所需的安全性設定連線。

關於這項工作

SMB用戶端工作階段可以有三種加密層級之一：

- `unencrypted`

  SMB工作階段未加密。未設定儲存虛擬機器（SVM）層級或共用層級的加密。

- `partially-encrypted`

  當樹狀結構連線發生時、會啟動加密。已設定共用層級加密。未啟用SVM層級的加密。

- `encrypted`

  SMB工作階段已完全加密。已啟用SVM層級的加密。共用層級加密可能已啟用、也可能未啟用。SVM層級

的加密設定會取代共用層級的加密設定。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
針對指定SVM上的工作階段、具有指定加密設定的工作階段	`vserver cifs session show -vserver *vserver_name* {unencrypted
partially-encrypted	encrypted} -instance`
指定SVM上特定工作階段ID的加密設定	`vserver cifs session show -vserver *vserver_name* -session-id *integer* -instance`

範例

下列命令會在工作階段ID為2的SMB工作階段上顯示詳細的工作階段資訊、包括加密設定：

```
cluster1::> vserver cifs session show -vserver vs1 -session-id 2 -instance
                          Node: node1
                       Vserver: vs1
                    Session ID: 2
                 Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
                   Workstation: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\joe
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: true
       User Authenticated as: domain-user
                NetBIOS Name: CIFS_ALIAS1
       SMB Encryption Status: Unencrypted
```

監控 **ONTAP SMB** 加密統計資料

您可以監控SMB加密統計資料、並判斷哪些已建立的工作階段和共用連線已加密、哪些尚未加密。

關於這項工作

。 `statistics` 進階權限層級的命令會提供下列計數器、您可以使用這些計數器來監控加密的 SMB 工作階段數目及共用連線：

計數器名稱	說明
`encrypted_sessions`	提供加密的SMB 3.0工作階段數量
`encrypted_share_connections`	提供樹狀結構連線所在的加密共用數
`rejected_unencrypted_sessions`	提供因缺乏用戶端加密功能而遭拒的工作階段設定數
`rejected_unencrypted_shares`	提供因缺乏用戶端加密功能而遭拒的共用對應數目

這些計數器可與下列統計資料物件一起使用：

- `cifs` 可讓您監控所有 SMB 3.0 工作階段的 SMB 加密。

  的輸出中包含 SMB 3.0 統計資料 `cifs` 物件： 如果您想要比較加密工作階段的數目與工作階段總數、可以比較的輸出 `encrypted_sessions` 以的輸出進行計數 `established_sessions` 計數器。

  如果您要比較加密共用連線的數目與共用連線的總數、可以比較的輸出 `encrypted_share_connections` 以的輸出進行計數 `connected_shares` 計數器。

- `rejected_unencrypted_sessions` 提供嘗試建立 SMB 工作階段的次數、該工作階段需要從不支援 SMB 加密的用戶端進行加密。
- `rejected_unencrypted_shares` 提供嘗試連線至 SMB 共用的次數、該共用需要來自不支援 SMB 加密的用戶端進行加密。

您必須先開始收集統計資料樣本、才能檢視結果資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別趨勢。

步驟

1. 將權限等級設為進階：
   `set -privilege advanced`
2. 開始資料收集：+
   `statistics start -object {cifs|smb1|smb2} -instance` *`instance`* `-sample-id` *`sample_ID`* `[-node` *`node_name`*`]`

   如果您未指定 `-sample-id` 參數、命令會為您產生範例識別碼、並將此範例定義為 CLI 工作階段的預設範例。的價值 `-sample-id` 為文字字串。如果您在相同的CLI工作階段中執行此命令、但未指定 `-sample-id` 參數時、命令會覆寫先前的預設範例。

   您可以選擇性地指定要收集統計資料的節點。如果您未指定節點、範例會收集叢集中所有節點的統計資料。

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

3. 使用 `statistics stop` 停止收集樣本資料的命令。

   詳細了解 `statistics stop`在"指令參考資料ONTAP" 。

4. 檢視SMB加密統計資料：

如果您要檢視下列項目的資訊...	輸入...
加密工作階段	`show -sample-id *sample_ID* -counter encrypted_sessions
node_name [-node *node_name*]`	加密的工作階段和已建立的工作階段
`show -sample-id *sample_ID* -counter encrypted_sessions	established_sessions
node_name [-node *node_name*]`	加密的共用連線
`show -sample-id *sample_ID* -counter encrypted_share_connections	*node_name* [-node *node_name*]`
加密的共用連線和連線共用	`show -sample-id *sample_ID* -counter encrypted_share_connections
connected_shares	*node_name* [-node *node_name*]`
拒絕未加密的工作階段	`show -sample-id *sample_ID* -counter rejected_unencrypted_sessions
node_name [-node *node_name*]`	拒絕未加密的共用連線
`show -sample-id *sample_ID* -counter rejected_unencrypted_share	*node_name* [-node *node_name*]`

   如果您只想顯示單一節點的資訊、請指定選用項目 `-node` 參數。

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

5. 返回管理權限層級：
   `set -privilege admin`

範例

以下範例說明如何監控儲存虛擬機器（SVM）VS1上的SMB 3.0加密統計資料。

下列命令會移至進階權限層級：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by support personnel.
Do you want to continue? {y|n}: y
```

下列命令會啟動新範例的資料收集：

```
cluster1::*> statistics start -object cifs -sample-id
smbencryption_sample -vserver vs1
Statistics collection is being started for Sample-id:
smbencryption_sample
```

下列命令會停止該範例的資料收集：

```
cluster1::*> statistics stop -sample-id smbencryption_sample
Statistics collection is being stopped for Sample-id:
smbencryption_sample
```

下列命令顯示節點從範例中所建立的加密SMB工作階段和已建立的SMB工作階段：

```
cluster2::*> statistics show -object cifs -counter
established_sessions|encrypted_sessions|node_name -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:45
Scope: vsim2

    Counter                                 Value
    ----------------------------  ----------------------
    established_sessions                       1
    encrypted_sessions                         1

2 entries were displayed
```

下列命令顯示節點從範例中拒絕的未加密SMB工作階段數目：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_sessions –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 11:17:45
End-time: 4/12/2016 11:21:51
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    rejected_unencrypted_sessions                 1

1 entry was displayed.
```

下列命令顯示範例中節點所連線的SMB共用數和加密的SMB共用數：

```
clus-2::*> statistics show -object cifs -counter
connected_shares|encrypted_share_connections|node_name –node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:41:43
Scope: vsim2

    Counter                                     Value
    ----------------------------    ----------------------
    connected_shares                              2
    encrypted_share_connections                   1

2 entries were displayed.
```

下列命令顯示節點從範例中拒絕的未加密SMB共用連線數目：

```
clus-2::*> statistics show -object cifs -counter
rejected_unencrypted_shares -node node_name

Object: cifs
Instance: [proto_ctx:003]
Start-time: 4/12/2016 10:41:38
End-time: 4/12/2016 10:42:06
Scope: vsim2

    Counter                                     Value
    --------------------------------    ----------------------
    rejected_unencrypted_shares                   1

1 entry was displayed.
```

相關資訊

- 確定伺服器上可用的統計資料、物件和計數器
- "效能監控與管理總覽"

安全的**LDAP**工作階段通訊

瞭解 **ONTAP SMB LDAP** 簽署與封裝

從ONTAP 功能支援功能支援功能支援功能支援功能、從功能支援功能支援功能升級至功能性管理功能。您必須在儲存虛擬機器（SVM）上設定CIFS伺服器安全性設定、以對應於LDAP伺服器上的設定。

簽署可確認LDAP有效負載資料使用秘密金鑰技術的完整性。「密封」會加密LDAP有效負載資料、以避免以純文字傳輸敏感資訊。「*LDAP*安全性層級」選項會指出LDAP流量是否需要簽署、簽署及密封、或兩者皆不需要。預設值為 `none`。

在 SVM 上啟用 CIFS 流量的 LDAP 簽署與密封功能 `-session-security-for-ad-ldap` 選項 `vserver cifs security modify` 命令。

在 **ONTAP SMB** 伺服器上啟用 **LDAP** 簽署和密封

CIFS伺服器必須先修改CIFS伺服器安全性設定、才能使用簽署和密封功能與Active Directory LDAP伺服器進行安全通訊。

開始之前

您必須洽詢AD伺服器管理員、以判斷適當的安全性組態值。

步驟

1. 設定 CIFS 伺服器安全性設定、以啟用 Active Directory LDAP 伺服器的簽署和密封流量： `vserver cifs security modify -vserver` *`vserver_name`* `-session-security-for-ad-ldap`

`{none|sign|seal}`

您可以啟用簽署 (`sign`、資料完整性）、簽署及密封 (`seal`**或兩者皆非** `none`、無簽署或密封）。預設值為 `none`。

2. 確認 LDAP 簽署與密封安全設定已正確設定： `vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊、例如使用者、群組和網路群組、則必須使用啟用對應的設定 `-session-security` 的選項 `vserver services name-service ldap client modify` 命令。

設定**LDAP over TLS**

匯出 **ONTAP SMB SVM** 的自我簽署根 **CA** 憑證

若要使用LDAP over SSL/TLS來保護Active Directory通訊安全、您必須先將Active Directory憑證服務的自我簽署根CA憑證複本匯出至憑證檔案、然後將其轉換成Ascii文字檔。這個文字檔是ONTAP 由SITALL用來在儲存虛擬機器（SVM）上安裝憑證。

開始之前

Active Directory憑證服務必須已針對CIFS伺服器所屬的網域進行安裝和設定。如需安裝及設定Active Director憑證服務的相關資訊、請參閱Microsoft TechNet程式庫。

"Microsoft TechNet程式庫：technet.microsoft.com"

步驟

1. 取得中網域控制站的根 CA 憑證 `.pem` 文字格式。

   "Microsoft TechNet程式庫：technet.microsoft.com"

完成後

在SVM上安裝憑證。

相關資訊

"Microsoft TechNet程式庫"

在 **ONTAP SMB SVM** 上安裝自我簽署的根 **CA** 憑證

如果在連結至LDAP伺服器時需要使用TLS進行LDAP驗證、您必須先在SVM上安裝自我簽署的根CA憑證。

關於這項工作

ONTAP 中所有使用 TLS 通訊的應用程式，都可以使用線上憑證狀態傳輸協定（ OCSP ）來檢查數位憑證狀態。如果在TLS上為LDAP啟用OCSP、則撤銷的憑證會遭到拒絕、連線也會失敗。

步驟

1. 安裝自我簽署的根CA憑證：
   a. 開始安裝憑證： `security certificate install -vserver vserver_name -type server-ca`

      主控台輸出會顯示下列訊息： `Please enter Certificate: Press <Enter> when done`

   b. 開啟憑證 `.pem` 使用文字編輯器檔案、複製憑證、包括開頭的行 `-----BEGIN CERTIFICATE-----` 並以結束 `-----END CERTIFICATE-----`，然後在命令提示字元之後貼上憑證。
   c. 確認已正確顯示憑證。
   d. 按Enter完成安裝。
2. 確認已安裝憑證： `security certificate show -vserver vserver_name`

相關資訊

- "安全性憑證安裝"
- "安全證書展示"

在 ONTAP SMB 伺服器上啟用 LDAP over TLS

您的SMB伺服器必須先修改SMB伺服器安全性設定、才能使用TLS與Active Directory LDAP伺服器進行安全通訊。

從ONTAP 《支援範圍》9.10.1開始、Active Directory（AD）和名稱服務LDAP連線預設都支援LDAP通道繫結。僅當啟用Start-TLS或LDAPS並將工作階段安全性設定為簽署或密封時、才能嘗試透過LDAP連線進行通道繫結。ONTAP若要停用或重新啟用與 AD 伺服器的 LDAP 通道繫結、請使用 `-try-channel-binding-for-ad-ldap` 參數 `vserver cifs security modify` 命令。

若要深入瞭解、請參閱：

- "了解適用於 ONTAP NFS SVM 的 LDAP"
- "2020 LDAP通道繫結和LDAP簽署要求、適用於Windows"。

步驟

1. 設定 SMB 伺服器安全性設定、以允許與 Active Directory LDAP 伺服器進行安全的 LDAP 通訊： `vserver cifs security modify -vserver vserver_name -use-start-tls-for-ad-ldap true`
2. 確認 LDAP over TLS 安全性設定已設定為 `true`： `vserver cifs security show -vserver vserver_name`

> 如果 SVM 使用相同的 LDAP 伺服器來查詢名稱對應或其他 UNIX 資訊（例如使用者、群組和網路群組）、則您也必須修改 `-use-start-tls` 選項：使用 `vserver services name-service ldap client modify` 命令。

設定 ONTAP SMB 多通道以獲得效能和備援

從支援支援支援的9.4開始ONTAP 、您可以設定SMB多通道、ONTAP 在單一SMB工作階段中、在支援的情況下提供多個連接功能。這樣做可改善處理量和容錯能力。

開始之前

只有當用戶端在SMB 3.0或更新版本上進行交涉時、才能使用SMB多通道功能。根據預設、SMB 3.0及更新版本會在ONTAP 支援SMB的伺服器上啟用。

關於這項工作

如果ONTAP 在故障叢集上識別出適當的組態、SMB用戶端會自動偵測並使用多個網路連線。

SMB工作階段中的同時連線數目取決於您已部署的NIC：

- *用戶端和ONTAP 叢集上的1G NIC *

  用戶端每個NIC建立一個連線、並將工作階段連結至所有連線。

- *用戶端與ONTAP 支援叢集*上的10G與更大容量NIC

  用戶端每個NIC最多可建立四個連線、並將工作階段連結至所有連線。用戶端可在多個10G和更大容量的NIC上建立連線。

您也可以修改下列參數（進階權限）：

- `-max-connections-per-session`

  每個多通道工作階段允許的最大連線數。預設為32個連線。

  如果您想要啟用比預設值更多的連線、則必須對用戶端組態進行類似的調整、也就是預設的32個連線。

- `-max-lifs-per-session`

  每個多通道工作階段所通告的網路介面數量上限。預設為256個網路介面。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 在SMB伺服器上啟用SMB多通道：

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. 驗證ONTAP 此功能是否回報SMB多通道工作階段：

```
vserver cifs session show
```

4. 返回管理權限層級：

```
set -privilege admin
```

範例

下列範例顯示所有SMB工作階段的相關資訊、顯示單一工作階段的多個連線：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

下列範例顯示使用工作階段ID 1之SMB工作階段的詳細資訊：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
                Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
        Continuously Available: No
             Is Session Signed: false
                  NetBIOS Name: -
```

在SMB伺服器上設定預設的Windows使用者對UNIX使用者對應

設定預設的 ONTAP SMB UNIX 使用者

您可以將預設UNIX使用者設定為在使用者的所有其他對應嘗試失敗時使用、或是不想在UNIX和Windows之間對應個別使用者時使用。或者、如果您想要驗證未對應的使用者失敗、則不應設定預設的UNIX使用者。

關於這項工作

根據預設、預設UNIX使用者的名稱為「'pcuser'」、這表示預設會啟用使用者對應至預設UNIX使用者的功能。您可以指定其他名稱作為預設UNIX使用者。您指定的名稱必須存在於為儲存虛擬機器（SVM）設定的名稱服務資料庫中。如果此選項設為null字串、則無人能以UNIX預設使用者的身分存取CIFS伺服器。也就是、每位使用者必須在密碼資料庫中擁有帳戶、才能存取CIFS伺服器。

使用者若要使用預設UNIX使用者帳戶連線至CIFS伺服器、必須符合下列先決條件：

- 使用者已通過驗證。
- 使用者位於CIFS伺服器的本機Windows使用者資料庫、CIFS伺服器的主網域或信任的網域（如果CIFS伺服器上已啟用多網域名稱對應搜尋）中。
- 使用者名稱未明確對應至null字串。

步驟

1. 設定預設UNIX使用者：

如果您想...	輸入...
使用預設的UNIX使用者「'pcuser'」	`vserver cifs options modify -default -unix-user pcuser`
使用另一個UNIX使用者帳戶做為預設使用者	`vserver cifs options modify -default -unix-user user_name`
停用預設UNIX使用者	`vserver cifs options modify -default -unix-user ""`

```
vserver cifs options modify -default-unix-user pcuser
```

2. 確認預設UNIX使用者已正確設定：`vserver cifs options show -vserver vserver_name`

   在下列範例中、SVM VS1上的預設UNIX使用者和來賓UNIX使用者均設定為使用UNIX使用者「'pcuser'」：

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

設定來賓 **ONTAP SMB UNIX** 使用者

設定來賓UNIX使用者選項表示從不受信任網域登入的使用者會對應到來賓UNIX使用者、並可連線到CIFS伺服器。或者、如果您想要驗證來自不受信任網域的使用者、則不應該設定來賓UNIX使用者。預設值是不允許來自不受信任網域的使用者連線至CIFS伺服器（未設定來賓UNIX帳戶）。

關於這項工作

設定來賓UNIX帳戶時、請謹記下列事項：

- 如果CIFS伺服器無法針對主網域或信任的網域或本機資料庫的網域控制器驗證使用者、且已啟用此選項、則CIFS伺服器會將使用者視為來賓使用者、並將使用者對應至指定的UNIX使用者。
- 如果此選項設為null字串、則停用來賓UNIX使用者。
- 您必須建立UNIX使用者、才能在其中一個儲存虛擬機器（SVM）名稱服務資料庫中做為來賓UNIX使用者。

- 以訪客使用者身分登入的使用者會自動成為CIFS伺服器上BUILTIN\訪 客群組的成員。
- 「homdirs-public」選項僅適用於已驗證的使用者。以來賓使用者身分登入的使用者沒有主目錄、因此無法存取其他使用者的主目錄。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入...
設定來賓UNIX使用者	`vserver cifs options modify -guest -unix-user` *`unix_name`*
停用來賓UNIX使用者	`vserver cifs options modify -guest -unix-user ""`

```
vserver cifs options modify -guest-unix-user pcuser
```

2. 確認來賓 UNIX 使用者已正確設定： `vserver cifs options show -vserver` *`vserver_name`*

   在下列範例中、SVM VS1上的預設UNIX使用者和來賓UNIX使用者均設定為使用UNIX使用者「'pcuser'」：

   ```
   vserver cifs options show -vserver vs1
   ```

   ```
   Vserver: vs1

     Client Session Timeout : 900
     Default Unix Group     : -
     Default Unix User      : pcuser
     Guest Unix User        : pcuser
     Read Grants Exec       : disabled
     Read Only Delete       : disabled
     WINS Servers           : -
   ```

將系統管理員群組對應至 **ONTAP SMB** 根目錄

如果您的環境中只有CIFS用戶端、且儲存虛擬機器（SVM）設定為多重傳輸協定儲存系統、則您必須擁有至少一個具有root權限的Windows帳戶、才能存取SVM上的檔案； 否則、您將無法管理SVM、因為您沒有足夠的使用者權限。

關於這項工作

如果您的儲存系統設定為僅 NTFS ， `/etc`則目錄會有檔案層級的 ACL ，讓系統管理員群組能夠存取 ONTAP 組態檔案。

步驟

1. 將權限層級設為進階： `set -privilege advanced`

2. 設定CIFS伺服器選項、將系統管理員群組適當對應至root：

如果您想要...	然後...
將系統管理員群組成員對應至root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled true` 即使您沒有、系統管理員群組中的所有帳戶都會視為 root `/etc/usermap.cfg` 將帳戶對應至根目錄的項目。如果您使用屬於系統管理員群組的帳戶來建立檔案、則當您從UNIX用戶端檢視檔案時、檔案將由root擁有。
停用將系統管理員群組成員對應至root	`vserver cifs options modify -vserver` *`vserver_name`* `-is-admin-users-mapped-to-root-enabled false` 系統管理員群組中的帳戶不再對應至根目錄。您只能明確地將單一使用者對應至root。

3. 確認選項設定為所需的值： `vserver cifs options show -vserver` *`vserver_name`*
4. 返回管理權限層級： `set -privilege admin`

顯示透過 **ONTAP SMB** 工作階段連線的使用者類型資訊

您可以顯示透過SMB工作階段連線的使用者類型資訊。這有助於確保只有適當類型的使用者透過儲存虛擬機器（SVM）上的SMB工作階段進行連線。

關於這項工作

下列類型的使用者可透過SMB工作階段連線：

- `local-user`

  已驗證為本機CIFS使用者

- `domain-user`

  驗證為網域使用者（可從CIFS伺服器的主網域或信任的網域）

- `guest-user`

  驗證為來賓使用者

- `anonymous-user`

  驗證為匿名或null使用者

步驟

1. 判斷透過 SMB 工作階段連線的使用者類型： `vserver cifs session show -vserver` *`vserver_name`* `-windows-user` *`windows_user_name`* `-fields windows-user,address,lif-address,user-type`

如果您要顯示已建立工作階段的使用者類型資訊...	輸入下列命令...
適用於具有指定使用者類型的所有工作階段	`vserver cifs session show -vserver *vserver_name* -user-type {local-user
domain-user	guest-user
anonymous-user}`	適用於特定使用者

範例

下列命令會顯示使用者「eubs\user1'」在SVM VS1上建立之工作階段的使用者類型工作階段資訊：

```
cluster1::> vserver cifs session show -vserver pub1 -windows-user
iepubs\user1 -fields windows-user,address,lif-address,user-type
node      vserver session-id connection-id lif-address  address
windows-user         user-type
--------- ------- ---------- ------------- ------------ -------------
-------------------- -----------
pub1node1 pub1    1          3439441860    10.0.0.1     10.1.1.1
IEPUBS\user1         domain-user
```

ONTAP 命令選項可限制過度的 **Windows** 用戶端資源使用量

的選項 `vserver cifs options modify` 命令可讓您控制 Windows 用戶端的資源使用量。如果有任何用戶端超出資源使用量的正常範圍、例如開啟的檔案數量異常多、開啟的工作階段或變更通知要求、則這項功能會很有幫助。

的下列選項 `vserver cifs options modify` 已新增命令以控制 Windows 用戶端資源使用量。如果超過這些選項的最大值、則會拒絕要求、並傳送EMS訊息。當達到這些選項設定上限的80%時、也會傳送EMS警告訊息。

- `-max-opens-same-file-per-tree`

  每個CIFS樹狀結構在同一個檔案上開啟的最大數目

- `-max-same-user-sessions-per-connection`

  每個連線的相同使用者所開啟的工作階段數目上限

- `-max-same-tree-connect-per-session`

  每個工作階段在相同共用區上連線的樹狀結構數目上限

- `-max-watches-set-per-tree`

  每個樹狀結構建立的監視數目上限（也稱為「變更通知」）

如"指令參考資料ONTAP"需詳細 `vserver cifs options modify`資訊，請參閱。

從ONTAP Sf9.4開始、執行SMB第2版或更新版本的伺服器可以限制用戶端在SMB連線上傳送至伺服器的未處理要求數（*SMB*點數）。SMB信用管理是由用戶端啟動、由伺服器控制。

可在 SMB 連線上授予的未處理要求數目上限是由控制 `-max-credits` 選項。此選項的預設值為128。

利用傳統和租賃**oplock**來提升用戶端效能

瞭解如何利用傳統和租賃資源來改善 **ONTAP SMB** 用戶端效能

傳統oplocks（投機鎖定）和租用oplock可在某些檔案共用案例中、讓SMB用戶端執行預先讀取、回寫及鎖定資訊的用戶端快取。然後用戶端可以讀取或寫入檔案、而不會定期提醒伺服器需要存取相關檔案。如此可減少網路流量、進而提升效能。

租賃oplock是SMB 2.1傳輸協定及更新版本所提供的一種強化型oplock形式。租賃oplock可讓用戶端在自有的多個SMB之間取得及保留用戶端快取狀態。

oplocks有兩種控制方式：

- 透過共用屬性、使用 `vserver cifs share create` 建立共用時的命令、或 `vserver share properties` 建立後的命令。
- 使用 qtree 屬性 `volume qtree create` qtree 建立時的命令、或 `volume qtree oplock` 建立後的命令。

瞭解在使用 **oplocks** 時寫入 **ONTAP SMB** 快取資料遺失考量

在某些情況下、如果某個處理程序在檔案上有獨家oplock、而第二個處理程序嘗試開啟該檔案、則第一個處理程序必須使快取的資料失效、並清除寫入和鎖定。然後用戶端必須放棄oplock並存取檔案。如果在此排清期間發生網路故障、快取的寫入資料可能會遺失。

- 資料遺失的可能性

  任何具有寫入快取資料的應用程式、都可能在下列情況下遺失該資料：

  - 連線是使用SMB 1.0進行。
  - 檔案上有獨家oplock。
  - 系統會要求中斷oplock或關閉檔案。
  - 在清空寫入快取的過程中、網路或目標系統會產生錯誤。
- 錯誤處理和寫入完成

  快取本身沒有任何錯誤處理、應用程式也有。當應用程式寫入快取時、寫入作業一律會完成。如果快取反過來又透過網路寫入目標系統、則必須假設寫入作業已完成、因為如果寫入作業未完成、資料就會遺失。

建立 **ONTAP SMB** 共用時，請啟用或停用 **oplocks**

oplocks可讓用戶端在本機上鎖定檔案和快取內容、進而提升檔案作業的效能。在儲存虛擬機器（SVM）上的SMB共用上啟用oplocks。在某些情況下、您可能會想要停用oplocks。

您可以逐一啟用或停用oplocks。

關於這項工作

如果在包含共用區的磁碟區上啟用oplock、但該共用區的oplock共用內容已停用、則該共用區的oplocks會停用。停用共用上的oplocks優先於Volume oplock設定。停用共用區上的oplocks會停用投機和租用oplock。

除了使用以逗號分隔的清單來指定oplock共用屬性之外、您也可以指定其他共用屬性。您也可以指定其他共用參數。

步驟

1. 執行適用的行動：

如果您想要...	然後...
在共用建立期間、在共用區上啟用oplocks	輸入下列命令： `vserver cifs share create -vserver _vserver_name_ -share-name share_name -path path_to_share -share -properties [oplocks,...]` 如果您希望共用只有預設的共用內容、即 `oplocks`、`browsable`和 `changenotify` 啟用時、您不需要指定 `-share-properties` 建立 SMB 共用時的參數。如果您想要使用預設以外的任何共用內容組合、則必須指定 `-share-properties` 參數、以及用於該共用的共用內容清單。
在共用建立期間停用共用區上的oplocks	輸入下列命令： `vserver cifs share create -vserver _vserver_name_ -share-name _share_name_ -path _path_to_share_ -share-properties [other_share_property,...]` 停用 oplocks 時、您必須在建立共用時指定共用內容清單、但不應指定 `oplocks` 屬性。

相關資訊

啟用或停用現有SMB共用區上的oplocks

監控oplock狀態

ONTAP 命令，用於在 **SMB** 磁碟區和 **qtree** 上啟用或停用 **oplocks**

oplocks可讓用戶端在本機上鎖定檔案和快取內容、進而提升檔案作業的效能。您需要知道在磁碟區或qtree上啟用或停用oplocks的命令。您也必須知道何時可以在磁碟區和qtree上

啟用或停用oplocks。

- 預設會在磁碟區上啟用oplocks。
- 您無法在建立Volume時停用oplocks。
- 您可以隨時在現有磁碟區上為SVM啟用或停用oplock。
- 您可以在qtree上為SVM啟用oplocks。

  oplock模式設定是qtree ID 0的屬性、即所有磁碟區的預設qtree。如果您在建立qtree時未指定oplock設定、qtree會繼承父Volume的oplock設定、此設定預設為啟用。不過、如果您在新qtree上指定oplock設定、則其優先於Volume上的oplock設定。

如果您想要...	使用此命令...
在磁碟區或qtree上啟用oplocks	`volume qtree oplocks` 使用 `-oplock-mode` 參數設為 `enable`
停用磁碟區或qtree上的oplocks	`volume qtree oplocks` 使用 `-oplock-mode` 參數設為 `disable`

相關資訊

監控oplock狀態

啟用或停用現有 **ONTAP SMB** 共用上的 **oplocks**

預設會在儲存虛擬機器（SVM）上的SMB共用上啟用oplocks。在某些情況下、您可能想要停用oplocks；或者、如果您先前已停用共用區上的oplocks、則可能需要重新啟用oplocks。

關於這項工作

如果在包含共用區的磁碟區上啟用oplock、但該共用區的oplock共用內容已停用、則該共用區的oplocks會停用。停用共用區上的oplocks優先於在磁碟區上啟用oplocks。停用共用區上的oplocks、停用機會和租用oplock。您可以隨時在現有共用區上啟用或停用oplocks。

步驟

1. 執行適用的行動：

如果您想要...	然後...
修改現有的共用區、在共用區上啟用oplocks	輸入下列命令：`vserver cifs share properties add -vserver vserver_name -share-name share_name -share -properties oplocks` 您可以使用以逗號分隔的清單來指定要新增的其他共用屬性。 新增的內容會附加到現有的共用內容清單中。您先前指定的任何共用內容都會維持有效。
透過修改現有的共用區來停用共用區上的oplocks	輸入下列命令：`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties oplocks` 您可以使用以逗號分隔的清單來指定要移除的其他共用屬性。 您移除的共用內容會從現有的共用內容清單中刪除、不過您先前設定的共用內容若未移除、則仍會維持有效。

範例

下列命令可在儲存虛擬機器（SVM、先前稱為Vserver）VS1上、針對名為「Engineering」的共用區啟用oplocks：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      oplocks
                                  browsable
                                  changenotify
                                  showsnapshot
```

下列命令會停用SVM VS1上名為「Engineering」的共用區oplocks：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
Engineering -share-properties oplocks

cluster1::> vserver cifs share properties show
Vserver          Share            Properties
---------------- ---------------- -----------------
vs1              Engineering      browsable
                                  changenotify
                                  showsnapshot
```

相關資訊

- 建立SMB共用時啟用或停用oplocks
- 監控oplock狀態
- 新增或刪除現有共享的共享屬性

監控 **ONTAP SMB oplock** 狀態

您可以監控及顯示oplock狀態的相關資訊。您可以使用此資訊來判斷哪些檔案有oplock、oplock層級和oplock狀態層級、以及是否使用oplock租賃。您也可以決定手動中斷鎖定的相關資訊。

關於這項工作

您可以在摘要表單或詳細清單表單中顯示所有oplock的相關資訊。您也可以使用選用參數來顯示現有鎖定的較小子集相關資訊。例如、您可以指定輸出只傳回指定用戶端IP位址或指定路徑的鎖定。

您可以顯示下列關於傳統和租賃oplock的資訊：

- 建立oplock的SVM、節點、Volume和LIF
- 鎖定UUID
- 使用oplock的用戶端IP位址
- 建立oplock的路徑
- 鎖定傳輸協定（SMB）和類型（oplock）
- 鎖定狀態
- oplock層級
- 連線狀態和SMB到期時間
- 開放群組ID（如果已授予租賃oplock）

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

步驟

1. 使用顯示 oplock 狀態 `vserver locks show` 命令。

範例

下列命令會顯示所有鎖定的預設資訊。所顯示檔案上的 oplock 會授予 `read-batch` Oplock 層級：

```
cluster1::> vserver locks show

Vserver: vs0
Volume   Object Path        LIF         Protocol  Lock Type   Client
-------- ------------------ ----------- --------- ----------- ----------
vol1     /vol1/notes.txt    node1_data1
                                        cifs      share-level 192.168.1.5
         Sharelock Mode: read_write-deny_delete
                                                  op-lock     192.168.1.5
         Oplock Level: read-batch
```

下列範例顯示有關鎖定路徑檔案的詳細資訊 `/data2/data2_2/intro.pptx`。在檔案上授予租用 oplock `batch` Oplock 層級至 IP 位址為的用戶端 `10.3.1.3`：

> 顯示詳細資訊時、命令會針對oplock和共享鎖定資訊提供個別輸出。此範例僅顯示oplock區段的輸出。

```
cluster1::> vserver lock show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: ff1cbf29-bfef-4d91-ae06-062bf69212c3
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
      Bytelock is Mandatory: -
      Bytelock is Exclusive: -
      Bytelock is Superlock: -
           Bytelock is Soft: -
               Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: -
          SMB Connect State: connected
SMB Expiration Time (Secs): -
          SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

相關資訊

建立SMB共用時啟用或停用oplocks

啟用或停用現有SMB共用區上的oplocks

用於在 SMB 捲和 qtree 上啟用或停用 oplock 的命令

將群組原則物件套用至**SMB**伺服器

瞭解如何將群組原則物件套用至 **ONTAP SMB** 伺服器

您的SMB伺服器支援群組原則物件（GPO）、這是一套稱為「群組原則屬性」的規則、適用於Active Directory環境中的電腦。您可以使用GPO集中管理屬於同一個Active Directory網域之叢集上所有儲存虛擬機器（SVM）的設定。

在SMB伺ONTAP 服器上啟用GPO時、將LDAP查詢傳送至Active Directory伺服器、要求取得GPO資訊。如果您的SMB伺服器適用GPO定義、Active Directory伺服器會傳回下列GPO資訊：

- GPO 名稱
- 目前的GPO版本
- GPO定義的位置
- GPO原則集的UUID清單（通用唯一識別碼）

相關資訊

- 了解伺服器的檔案存取安全性
- "SMB與NFS稽核與安全性追蹤"

瞭解支援的 **ONTAP SMB GPO**

雖然並非所有的群組原則物件（GPO）都適用於CIFS型儲存虛擬機器（SVM）、但SVM可以辨識及處理相關的GPO集。

SVM目前支援下列GPO：

- 進階稽核原則組態設定：

  物件存取：集中存取原則接移

  指定要稽核中央存取原則（CAP）接移的事件類型、包括下列設定：

  - 請勿稽核
  - 僅稽核成功事件
  - 僅稽核失敗事件
  - 稽核成功與失敗事件

  > 如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

  使用設定 `Audit Central Access Policy Staging` 的設定 `Advanced Audit Policy Configuration/Audit Policies/Object Access` GPO ：

  > 若要使用進階稽核原則組態GPO設定、您必須在要套用這些設定的CIFS型SVM上設定稽核。如果未在SVM上設定稽核、則不會套用及捨棄GPO設定。

- 登錄設定：

  - 啟用CIFS的SVM的群組原則重新整理時間間隔

    使用設定 `Registry` GPO ：

  - 群組原則重新整理隨機偏移

    使用設定 `Registry` GPO ：

  - BranchCache的雜湊發佈

BranchCache GPO的雜湊發佈會對應到BranchCache作業模式。支援下列三種操作模式：

- 每個共用區
- All共享區
- 已停用
  使用設定 `Registry` GPO ：

◦ 支援BranchCache的雜湊版本

支援下列三種雜湊版本設定：

- BranchCache第1版
- BranchCache 版本 2
- BranchCache 第 1 版和第 2 版
  使用設定 `Registry` GPO ：

> 若要使用BranchCache GPO設定、必須在您要套用這些設定的CIFS型SVM上設定BranchCache。如果未在SVM上設定BranchCache、則不會套用GPO設定、也會捨棄。

- 安全性設定
  - 稽核原則與事件記錄
    - 稽核登入事件

      指定要稽核的登入事件類型、包括下列設定：

      - 請勿稽核
      - 僅稽核成功事件
      - 稽核失敗事件
      - 稽核成功與失敗事件
        使用設定 `Audit logon events` 的設定 `Local Policies/Audit Policy` GPO ：

        > 如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

    - 稽核物件存取

      指定要稽核的物件存取類型、包括下列設定：

      - 請勿稽核
      - 僅稽核成功事件
      - 稽核失敗事件
      - 稽核成功與失敗事件
        使用設定 `Audit object access` 的設定 `Local Policies/Audit Policy` GPO ：

如果三個稽核選項中有任何一個已設定（僅稽核成功事件、僅稽核失敗事件、同時稽核成功和失敗事件）ONTAP 、則會同時稽核成功和失敗事件。

- 記錄保留方法

  指定稽核記錄保留方法、包括下列設定：

  - 當記錄檔大小超過最大記錄檔大小時、請覆寫事件記錄
  - 不要覆寫事件記錄（手動清除記錄）
    使用設定 `Retention method for security log` 的設定 `Event Log` GPO ：

- 最大記錄大小

  指定稽核記錄的最大大小。

  使用設定 `Maximum security log size` 的設定 `Event Log` GPO ：

若要使用稽核原則和事件記錄GPO設定、您必須在要套用這些設定的CIFS型SVM上設定稽核。如果未在SVM上設定稽核、則不會套用及捨棄GPO設定。

- 檔案系統安全性

  指定透過GPO套用檔案安全性的檔案或目錄清單。

  使用設定 `File System` GPO ：

設定檔案系統安全性GPO的磁碟區路徑必須存在於SVM中。

- Kerberos原則

  - 最大時鐘偏移

    指定電腦時鐘同步的最大容許值（以分鐘為單位）。

    使用設定 `Maximum tolerance for computer clock synchronization` 的設定 `Account Policies/Kerberos Policy` GPO ：

  - 票證最長使用期限

    指定使用者票證的最長壽命（以小時為單位）。

    使用設定 `Maximum lifetime for user ticket` 的設定 `Account Policies/Kerberos Policy` GPO ：

  - 票證續約期限上限

    指定使用者票證續約的最長壽命（以天為單位）。

  使用設定 `Maximum lifetime for user ticket renewal` 的設定 `Account Policies/Kerberos Policy` GPO ：

- 使用者權限指派（權限）
  - 取得擁有權

    指定有權取得任何安全物件所有權的使用者和群組清單。

    使用設定 `Take ownership of files or other objects` 的設定 `Local Policies/User Rights Assignment` GPO ：

  - 安全性權限

    指定使用者和群組清單、這些使用者和群組可指定個別資源（例如檔案、資料夾和Active Directory物件）物件存取的稽核選項。

    使用設定 `Manage auditing and security log` 的設定 `Local Policies/User Rights Assignment` GPO ：

  - 變更通知權限（略過周遊檢查）

    指定可遍歷目錄樹狀結構的使用者和群組清單、即使使用者和群組對周遊目錄可能沒有權限。

  使用者必須擁有相同的權限、才能接收檔案和目錄變更通知。使用設定 `Bypass traverse checking` 的設定 `Local Policies/User Rights Assignment` GPO ：

- 登錄值
  - 需要簽署設定

    指定是否啟用或停用必要的SMB簽署。

  使用設定 `Microsoft network server: Digitally sign communications (always)` 的設定 `Security Options` GPO ：

- 限制匿名

  指定匿名使用者的限制、並包含下列三項GPO設定：

  - 無列舉安全性客戶經理（SAM）帳戶：

    此安全性設定可決定授與哪些其他權限給電腦的匿名連線。此選項會顯示為 `no-enumeration` 在 ONTAP 中（如果已啓用）。

    使用設定 `Network access: Do not allow anonymous enumeration of SAM accounts` 的設定 `Local Policies/Security Options` GPO ：

  - 未列舉SAM帳戶和共用

    此安全性設定可決定是否允許SAM帳戶和共用的匿名列舉。此選項會顯示為 `no-enumeration` 在 ONTAP 中（如果已啓用）。

    使用設定 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 的設定 `Local Policies/Security Options` GPO ：

- 限制匿名存取共用和具名管道

  此安全性設定會限制匿名存取共用和管道。此選項會顯示為 `no-access` 在 ONTAP 中（如果已啓用）。

  使用設定 `Network access: Restrict anonymous access to Named Pipes and Shares` 的設定 `Local Policies/Security Options` GPO ：

  顯示已定義和已套用群組原則的相關資訊時、會顯示 `Resultant restriction for anonymous user` 「輸出」欄位提供三個限制匿名 GPO 設定的結果限制相關資訊。可能的結果限制如下：

  - `no-access`

    匿名使用者無法存取指定的共用和具名管道、也無法使用SAM帳戶和共用的列舉。如果出現這種情況、就會出現這種限制 `Network access: Restrict anonymous access to Named Pipes and Shares` 已啟用 GPO 。

  - `no-enumeration`

    匿名使用者可以存取指定的共用和具名管道、但無法使用SAM帳戶和共用的列舉。如果符合下列兩項條件、就會看到這項限制：

    - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPO 已停用。
    - 或是 `Network access: Do not allow anonymous enumeration of SAM accounts` 或 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` 已啟用 GPO 。

  - `no-restriction`

    匿名使用者擁有完整存取權、可以使用列舉功能。如果符合下列兩項條件、就會看到這項限制：

    - 。 `Network access: Restrict anonymous access to Named Pipes and Shares` GPO 已停用。
    - 兩者皆是 `Network access: Do not allow anonymous enumeration of SAM accounts` 和 `Network access: Do not allow anonymous enumeration of SAM accounts and shares` GPO 已停用。

      - 受限群組

        您可以設定受限群組、集中管理內建或使用者定義群組的成員資格。透過群組原則套用受限群組時、CIFS伺服器本機群組的成員資格會自動設定為符合套用群組原則中定義的成員資格清單設定。

  使用設定 `Restricted Groups` GPO ：

- 集中存取原則設定

  指定集中存取原則清單。集中存取原則及相關的集中存取原則規則、決定SVM上多個檔案的存取權限。

相關資訊

- 在伺服器上啟用或停用 GPO 支援
- 了解伺服器的檔案存取安全性
- "SMB與NFS稽核與安全性追蹤"
- 修改伺服器安全設定
- 了解如何使用 BranchCache 在分公司快取共享內容
- 了解如何使用 ONTAP 簽章來增強網路安全
- 了解如何配置繞過遍歷檢查
- 設定匿名使用者的存取限制

ONTAP SMB 伺服器對 GPO 的需求

若要在SMB伺服器上使用群組原則物件（GPO）、您的系統必須符合多項需求。

- SMB必須在叢集上獲得授權。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。
- SMB伺服器必須設定並加入Windows Active Directory網域。
- SMB伺服器管理狀態必須為開啟。
- 必須設定GPO並套用至包含SMB伺服器電腦物件的Windows Active Directory組織單位（OU）。
- 必須在SMB伺服器上啟用GPO支援。

在 ONTAP SMB 伺服器上啟用或停用 GPO 支援

您可以在CIFS伺服器上啟用或停用群組原則物件（GPO）支援。如果您在CIFS伺服器上啟用GPO支援、則會將群組原則上定義的適用GPO（套用至包含CIFS伺服器電腦物件之組織單位（OU）的原則）套用至CIFS伺服器。

關於這項工作

無法在CIFS伺服器上以工作群組模式啟用GPO。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
啟用GPO	`vserver cifs group-policy modify -vserver vserver_name -status enabled`
停用GPO	`vserver cifs group-policy modify -vserver vserver_name -status disabled`

2. 確認 GPO 支援處於所需的狀態：`vserver cifs group-policy show -vserver +vserver_name_`

工作群組模式中CIFS伺服器的群組原則狀態顯示為「停用」。

範例

下列範例可在儲存虛擬機器（SVM）VS1上啟用GPO支援：

```
cluster1::> vserver cifs group-policy modify -vserver vs1 -status enabled

cluster1::> vserver cifs group-policy show -vserver vs1

            Vserver: vs1
Group Policy Status: enabled
```

相關資訊

了解受支援的 GPO

GPO 的伺服器要求

了解如何在 SMB 伺服器上更新 GPO

手動更新 SMB 伺服器上的 GPO 設定

顯示有關GPO組態的資訊

如何在 SMB 伺服器上更新 GPO

瞭解如何更新 ONTAP SMB 伺服器上的 GPO

根據預設ONTAP 、每90分鐘擷取並套用群組原則物件（GPO）變更一次。安全性設定每16小時重新整理一次。如果您想在ONTAP 更新GPO之前先套用新的GPO原則設定、然後再自動更新、您可以在CIFS伺服器上使用ONTAP flexto命令觸發手動更新。

- 根據預設、所有的GPO都會視需要每90分鐘進行一次驗證和更新。

  此時間間隔可設定、並可使用設定 `Refresh interval` 和 `Random offset` GPO 設定。

  可查詢Active Directory以取得變更GPO的資訊。ONTAP如果Active Directory中記錄的GPO版本號碼高於CIFS伺服器、ONTAP 則會擷取並套用新的GPO。如果版本號碼相同、則CIFS伺服器上的GPO不會更新。

- 安全性設定GPO每16小時重新整理一次。

  無論這些GPO是否已變更、均可每16小時擷取並套用安全性設定GPO。ONTAP

  目前ONTAP 版本的16小時預設值無法變更。這是Windows用戶端的預設設定。

- 所有的GPO都可以使用ONTAP flexflexfcommand手動更新。

  此命令模擬 Windows `gpupdate.exe`/force 命令。

相關資訊

手動更新 SMB 伺服器上的 GPO 設定

手動更新 **ONTAP SMB** 伺服器上的 **GPO** 設定

如果您想要立即更新CIFS伺服器上的群組原則物件（GPO）設定、您可以手動更新這些設定。您只能更新變更的設定、或是強制更新所有設定、包括先前套用但尚未變更的設定。

步驟

1. 執行適當的行動：

如果您想要更新...	輸入命令...
變更GPO設定	`vserver cifs group-policy update -vserver` *`vserver_name`*
所有GPO設定	`vserver cifs group-policy update -vserver` *`vserver_name`* `-force-reapply -all-settings true`

相關資訊

了解如何在 SMB 伺服器上更新 GPO

顯示 **ONTAP SMB GPO** 組態的相關資訊

您可以顯示Active Directory中定義的群組原則物件（GPO）組態資訊、以及應用於CIFS伺服器的GPO組態資訊。

關於這項工作

您可以顯示CIFS伺服器所屬網域Active Directory中定義的所有GPO組態資訊、或只顯示套用至CIFS伺服器之GPO組態的相關資訊。

步驟

1. 執行下列其中一項動作、以顯示有關GPO組態的資訊：

如果您要顯示所有群組原則組態的相關資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy show-defined -vserver vserver_name`
套用至CIFS型儲存虛擬機器（SVM）	`vserver cifs group-policy show-applied -vserver vserver_name`

範例

下列範例顯示在Active Directory中定義的GPO組態、其中CIFS啟用的SVM名稱為VS1屬於：

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
------------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache : version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

```
    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
```

下列範例顯示套用至CIFS型SVM VS1的GPO組態：

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1
```

```
Vserver: vs1
-----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: all-versions
  Security Settings:
      Event Audit and Event Log:
          Audit Logon Events: none
          Audit Object Access: success
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2

    GPO Name: Resultant Set of Policy
       Level: RSOP
```

```
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2
```

相關資訊

在伺服器上啟用或停用 GPO 支援

顯示 **ONTAP SMB** 受限群組 **GPO** 的相關資訊

您可以顯示Active Directory中定義為群組原則物件（GPO）且套用至CIFS伺服器的受限群組詳細資訊。

關於這項工作

依預設、會顯示下列資訊：

- 群組原則名稱
- 群組原則版本
- 連結

  指定群組原則的設定層級。可能的輸出值包括：

  - `Local` 在 ONTAP 中設定群組原則時
  - `Site` 在網域控制站的站台層級設定群組原則時
  - `Domain` 當群組原則是在網域控制站的網域層級設定時
  - `OrganizationalUnit` 當群組原則在網域控制站的組織單位（ OU ）層級上設定時
  - `RSOP` 針對衍生自各個層級所定義之所有群組原則的結果原則集
- 受限群組名稱
- 屬於受限群組且不屬於受限群組的使用者和群組
- 新增受限群組的群組清單

  群組可以是此處所列群組以外的群組成員。

步驟

1. 執行下列其中一項動作、顯示所有受限群組GPO的相關資訊：

如果您要顯示所有受限群組**GPO**的相關資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy restricted-group show-defined -vserver vserver_name`
套用至CIFS伺服器	`vserver cifs group-policy restricted-group show-applied -vserver vserver_name`

範例

下列範例顯示在Active Directory網域中定義的受限群組GPO相關資訊、其中CIFS啟用的SVM名稱為VS1屬於該網域：

```
cluster1::> vserver cifs group-policy restricted-group show-defined
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

下列範例顯示套用至CIFS型SVM VS1之受限群組GPO的相關資訊：

```
cluster1::> vserver cifs group-policy restricted-group show-applied
-vserver vs1

Vserver: vs1
-------------

     Group Policy Name: gpo1
               Version: 16
                  Link: OrganizationalUnit
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9

     Group Policy Name: Resultant Set of Policy
               Version: 0
                  Link: RSOP
           Group Name: group1
              Members: user1
            MemberOf: EXAMPLE\group9
```

相關資訊

顯示有關GPO組態的資訊

您可以顯示Active Directory中定義的中央存取原則詳細資訊。您也可以顯示透過群組原則物件（GPO）套用至CIFS伺服器的中央存取原則相關資訊。

關於這項工作

依預設、會顯示下列資訊：

- SVM名稱
- 中央存取原則的名稱
- SID
- 說明
- 建立時間
- 修改時間
- 成員規則

工作群組模式中的CIFS伺服器不會顯示、因為它們不支援GPO。

步驟

1. 執行下列其中一項動作、以顯示有關中央存取原則的資訊：

如果您想要顯示所有集中存取原則的相關資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy central-access-policy show-defined -vserver` *`vserver_name`*
套用至CIFS伺服器	`vserver cifs group-policy central-access-policy show-applied -vserver` *`vserver_name`*

範例

下列範例顯示Active Directory中定義的所有集中存取原則資訊：

```
cluster1::> vserver cifs group-policy central-access-policy show-defined

Vserver  Name                 SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

下列範例顯示套用至叢集上儲存虛擬機器（SVM）的所有集中存取原則資訊：

```
cluster1::> vserver cifs group-policy central-access-policy show-applied

Vserver    Name                   SID
-------- --------------------
-----------------------------------------------
vs1      p1                   S-1-17-3386172923-1132988875-3044489393-
3993546205
       Description: policy #1
     Creation Time: Tue Oct 22 09:34:13 2013
 Modification Time: Wed Oct 23 08:59:15 2013
      Member Rules: r1

vs1      p2                   S-1-17-1885229282-1100162114-134354072-
822349040
       Description: policy #2
     Creation Time: Tue Oct 22 10:28:20 2013
 Modification Time: Thu Oct 31 10:25:32 2013
      Member Rules: r1
                    r2
```

相關資訊

- 了解伺服器的檔案存取安全性

- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則規則的資訊

顯示 **ONTAP SMB** 中央存取原則規則的相關資訊

您可以顯示與Active Directory中定義的中央存取原則相關聯的中央存取原則規則詳細資訊。您也可以透過集中存取原則GPO（群組原則物件）、顯示套用至CIFS伺服器的中央存取原則規則相關資訊。

關於這項工作

您可以顯示已定義及已套用之集中存取原則規則的詳細資訊。依預設、會顯示下列資訊：

- Vserver名稱
- 中央存取規則的名稱
- 說明
- 建立時間
- 修改時間
- 目前權限
- 建議的權限
- 目標資源

如果您要顯示與集中存取原則相關的所有集中存取原則規則資訊...	輸入命令...
在Active Directory中定義	`vserver cifs group-policy central-access-rule show-defined -vserver vserver_name`
套用至CIFS伺服器	`vserver cifs group-policy central-access-rule show-applied -vserver vserver_name`

範例

下列範例顯示Active Directory中定義之中央存取原則相關的所有中央存取原則規則資訊：

```
cluster1::> vserver cifs group-policy central-access-rule show-defined

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

下列範例顯示與套用至叢集上儲存虛擬機器（SVM）的集中存取原則相關的所有集中存取原則規則資訊：

```
cluster1::> vserver cifs group-policy central-access-rule show-applied

Vserver     Name
----------- --------------------
vs1         r1
              Description: rule #1
            Creation Time: Tue Oct 22 09:33:48 2013
        Modification Time: Tue Oct 22 09:33:48 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)

vs1         r2
              Description: rule #2
            Creation Time: Tue Oct 22 10:27:57 2013
        Modification Time: Tue Oct 22 10:27:57 2013
       Current Permissions: O:SYG:SYD:AR(A;;FA;;;WD)
      Proposed Permissions: O:SYG:SYD:(A;;FA;;;OW)(A;;FA;;;BA)(A;;FA;;;SY)
```

相關資訊

- 了解伺服器的檔案存取安全性
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊

用於管理 **SMB** 伺服器電腦帳戶密碼的 **ONTAP** 命令

您需要知道變更、重設及停用密碼、以及設定自動更新排程的命令。您也可以在 SMB 伺服器上設定排程、以自動更新排程。

如果您想要...	使用此命令...
當 ONTAP 與 AD 服務同步時，請變更網域帳戶密碼	`vserver cifs domain password change`
當 ONTAP 未與 AD 服務同步時，請重設網域帳戶密碼	`vserver cifs domain password reset`
設定SMB伺服器以自動變更電腦帳戶密碼	`vserver cifs domain password schedule modify -vserver vserver_name -is -schedule-enabled true`
停用SMB伺服器上的自動電腦帳戶密碼變更	`vserver cifs domain password schedule modify -vserver vs1 -is-schedule -enabled false`

如"指令參考資料ONTAP"需詳細 `vserver cifs domain password`資訊，請參閱。

管理網域控制器連線

顯示 **ONTAP SMB** 探索伺服器的相關資訊

您可以顯示CIFS伺服器上探索到的LDAP伺服器和網域控制器相關資訊。

步驟

1. 若要顯示與探索到的伺服器相關的資訊、請輸入下列命令： `vserver cifs domain discovered-servers show`

範例

下列範例顯示SVM VS1探索到的伺服器：

```
cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

相關資訊

- 重設並重新探索伺服器
- 停止或啟動伺服器

重設及重新探索 **ONTAP SMB** 伺服器

重設及重新探索CIFS伺服器上的伺服器、可讓CIFS伺服器捨棄有關LDAP伺服器和網域控制器的儲存資訊。在捨棄伺服器資訊之後、CIFS伺服器會重新取得這些外部伺服器的目前資訊。當連線的伺服器沒有適當回應時、此功能很有用。

步驟

1. 輸入下列命令： `vserver cifs domain discovered-servers reset-servers -vserver` *`vserver_name`*
2. 顯示新重新探索到的伺服器相關資訊： `vserver cifs domain discovered-servers show -vserver` *`vserver_name`*

範例

下列範例可重設及重新探索儲存虛擬機器（SVM、先前稱為Vserver）VS1的伺服器：

```
cluster1::> vserver cifs domain discovered-servers reset-servers -vserver
vs1

cluster1::> vserver cifs domain discovered-servers show

Node: node1
Vserver: vs1

Domain Name     Type     Preference DC-Name     DC-Address     Status
--------------- -------- ---------- ----------- -------------- -------
example.com     MS-LDAP  adequate   DC-1        1.1.3.4        OK
example.com     MS-LDAP  adequate   DC-2        1.1.3.5        OK
example.com     MS-DC    adequate   DC-1        1.1.3.4        OK
example.com     MS-DC    adequate   DC-2        1.1.3.5        OK
```

相關資訊

- 顯示探索到的伺服器相關資訊
- 停止或啟動伺服器

管理 **ONTAP SMB** 網域控制站探索

從ONTAP 功能更新9.3開始、您可以修改探索網域控制器（DC）的預設程序。如此一來、您就能將探索範圍限制在網站或偏好的DC資源池中、進而提升效能、端視環境而定。

關於這項工作

根據預設、動態探索程序會探索所有可用的DC、包括任何慣用的DC、本機站台中的所有DC、以及所有遠端

DC。此組態可能會導致驗證延遲、以及在特定環境中存取共用區。如果您已經決定要使用的DC資源池、或是遠端DC不足或無法存取、您可以變更探索方法。

在 ONTAP 9.3 及更新版本中 `discovery-mode` 的參數 `cifs domain discovered-servers` 命令可讓您選取下列其中一個探索選項：

- 探索網域中的所有DC。
- 只會探索本機站台中的DC。
  - `default-site` SMB 伺服器的參數可定義為使用此模式搭配未指派給站台和服務中站台的生命。
- 未執行伺服器探索、SMB伺服器組態僅取決於偏好的DC。

  若要使用此模式、您必須先定義SMB伺服器的慣用DC。

開始之前

您必須處於進階權限層級。

步驟

1. 指定所需的探索選項： `vserver cifs domain discovered-servers discovery-mode modify -vserver` *`vserver_name`* `-mode {all|site|none}`

   的選項 `mode` 參數：

   - `all`

     探索所有可用的DC（預設）。

   - `site`

     將DC探索限制在您的站台上。

   - `none`

     僅使用偏好的DC、而不執行探索。

新增偏好的 **ONTAP SMB** 網域控制站

透過DNS自動探索網域控制器。ONTAP或者、您可以將一個或多個網域控制器新增至特定網域的慣用網域控制器清單。

關於這項工作

如果指定網域的慣用網域控制器清單已經存在、則新清單會與現有清單合併。

步驟

1. 若要新增至偏好的網域控制站清單、請輸入下列命令：
   `vserver cifs domain preferred-dc add -vserver` *`vserver_name`* `-domain` *`domain_name`* `-preferred-dc IP_address, …+`

`-vserver vserver_name` 指定儲存虛擬機器（ SVM ）名稱。

`-domain domain_name` 指定指定網域控制站所屬之網域的完整 Active Directory 名稱。

`-preferred-dc IP_address`、 ... 依喜好設定順序，指定慣用網域控制站的一或多個 IP 位址，以逗號分隔的清單形式顯示。

範例

下列命令會將網域控制器172.17.102.25和172.17.102.24新增至SVM VS1上的SMB伺服器用來管理cifs.lab.example.com網域外部存取的慣用網域控制器清單。

```
cluster1::> vserver cifs domain preferred-dc add -vserver vs1 -domain
cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

相關資訊

管理慣用網域控制器的命令

用於管理偏好的 **SMB** 網域控制站的 **ONTAP** 命令

您需要知道用於新增、顯示及移除慣用網域控制器的命令。

如果您想要...	使用此命令...
新增慣用的網域控制器	`vserver cifs domain preferred-dc add`
顯示慣用的網域控制器	`vserver cifs domain preferred-dc show`
移除慣用的網域控制器	`vserver cifs domain preferred-dc remove`

如"指令參考資料ONTAP"需詳細 `vserver cifs domain preferred-dc`資訊，請參閱。

相關資訊

新增慣用的網域控制器

啟用與 **ONTAP SMB** 網域控制站的加密連線

從ONTAP 功能表9.8開始、您可以指定要加密網域控制器的連線。

關於這項工作

ONTAP 需要加密網域控制站（ DC ）通訊 `-encryption-required-for-dc-connection` 選項設定為 `true`；預設值為 `false`。設定此選項時、只有SMb3傳輸協定會用於ONTAP-DC連線、因為只有SMb3才支援加密。

當需要加密的 DC 通訊時、 `-smb2-enabled-for-dc-connections` 選項會被忽略、因為 ONTAP 只會交涉 SMB3 連線。如果DC不支援SMB3和加密、ONTAP 則無法與之連線。

步驟

1. 啟用與 DC 的加密通訊： `vserver cifs security modify -vserver *svm_name* -encryption -required-for-dc-connection true`

使用**null**工作階段來存取非**Kerberos**環境中的儲存設備

使用 **ONTAP SMB null** 工作階段來存取非 **Kerberos** 環境中的儲存設備

null工作階段存取可提供網路資源（例如儲存系統資料）的權限、以及在本機系統下執行的用戶端型服務的權限。當用戶端程序使用「系統」帳戶存取網路資源時、就會發生null工作階段。null工作階段組態是專為非Kerberos驗證而設計。

瞭解 **ONTAP SMB** 儲存系統如何提供 **Null** 工作階段存取

由於null工作階段共用不需要驗證、因此需要null工作階段存取的用戶端必須在儲存系統上對應其IP位址。

根據預設、未對應的null工作階段用戶端可以存取某些ONTAP 功能不全的系統服務、例如共用列舉、但它們受到限制、無法存取任何儲存系統資料。

> ONTAP 支援使用選項的 Windows RestrictAnonymous 登錄設定值 `-restrict-anonymous`。這可讓您控制未對應的null使用者檢視或存取系統資源的程度。例如、您可以停用共用列舉並存取IPC$共用區（隱藏的命名管道共用區）。深入瞭解 `vserver cifs options modify`及 `vserver cifs options show `–restrict-anonymous`中的選項"指令參考資料ONTAP"。

除非另有設定、否則執行本機處理程序的用戶端透過null工作階段要求存取儲存系統、只是不受限制群組的成員、例如「'ee任何人'」。若要限制對所選儲存系統資源的null工作階段存取、您可能需要建立一個所有null工作階段用戶端所屬的群組；建立此群組可讓您限制儲存系統存取、並設定專屬於null工作階段用戶端的儲存系統資源權限。

ONTAP 在中提供對應語法 `vserver name-mapping` 命令集可指定允許使用 null 使用者工作階段存取儲存系統資源的用戶端 IP 位址。為null使用者建立群組之後、您可以針對僅適用於null工作階段的儲存系統資源和資源權限、指定存取限制。null使用者被識別為匿名登入。null使用者無法存取任何主目錄。

從對應IP位址存取儲存系統的任何null使用者、都會被授予對應的使用者權限。請考量適當的預防措施、以防止未獲授權存取與null使用者對應的儲存系統。為獲得最大保護、請將儲存系統和所有需要null使用者儲存系統存取的用戶端放在獨立的網路上、以避免IP位址「欺詐」的可能性。

相關資訊

設定匿名使用者的存取限制

授予 **null** 使用者存取 **ONTAP SMB** 檔案系統共用的權限

您可以指派一個群組供null工作階段用戶端使用、並記錄null工作階段用戶端的IP位址、以便新增至儲存系統允許使用null工作階段存取資料的用戶端清單、藉此允許null工作階段用戶端存取儲存系統資源。

步驟

1. 使用 `vserver name-mapping create` 命令，將 null 使用者對應至任何有效的 Windows 使用者，並提供 IP 辨識符號。

下列命令會將null使用者對應至具有有效主機名稱google.com的user1：

```
vserver name-mapping create -direction win-unix  -position 1 -pattern
"ANONYMOUS LOGON" -replacement user1 - hostname google.com
```

下列命令會將null使用者對應至具有有效IP位址10.238.2.54/32的user1：

```
vserver name-mapping create -direction win-unix  -position 2 -pattern
"ANONYMOUS LOGON" -replacement user1 -address 10.238.2.54/32
```

2. 使用 `vserver name-mapping show` 確認名稱對應的命令。

```
vserver name-mapping show

Vserver:   vs1
Direction: win-unix
Position Hostname         IP Address/Mask
-------- --------         ----------------
1       -                 10.72.40.83/32      Pattern: anonymous logon
                                          Replacement: user1
```

3. 使用 `vserver cifs options modify –win-name-for-null-user` 命令將 Windows 成員資格指派給 null 使用者。

此選項僅適用於具有null使用者有效名稱對應的情況。

```
vserver cifs options modify -win-name-for-null-user user1
```

4. 使用 `vserver cifs options show` 用於確認 null 使用者與 Windows 使用者或群組之間對應的命令。

```
vserver cifs options show

Vserver :vs1

Map Null User to Windows User of Group: user1
```

管理**SMB**伺服器的**NetBios**別名

瞭解如何管理 **ONTAP SMB** 伺服器的 **NetBios** 別名

NetBios別名是SMB伺服器的替代名稱、SMB用戶端可在連線至SMB伺服器時使用。當您

將其他檔案伺服器的資料整合到SMB伺服器、並希望SMB伺服器回應原始檔案伺服器的名稱時、設定SMB伺服器的NetBios別名很有用。

您可以在建立SMB伺服器時或建立SMB伺服器之後的任何時間、指定一個NetBios別名清單。您可以隨時從清單中新增或移除NetBios別名。您可以使用NetBios別名清單中的任何名稱連線至SMB伺服器。

相關資訊

顯示有關TCP連線上的NetBios資訊

將 NetBios 別名清單新增至 ONTAP SMB 伺服器

如果您希望SMB用戶端使用別名連線到SMB伺服器、您可以建立一份NetBios別名清單、或是將NetBios別名新增到現有的NetBios別名清單。

關於這項工作

- NetBios別名長度最多可為15個字元。
- 您最多可以在SMB伺服器上設定200個NetBios別名。
- 不允許使用下列字元：

  @ # * （） = + [ ] | ； ： " 、 < > \ / ？

步驟

1. 新增 NetBIOS 別名：
   `vserver cifs add-netbios-aliases -vserver vserver_name -netbios-aliases NetBIOS_alias,…`

   ```
   vserver cifs add-netbios-aliases -vserver vs1 -netbios-aliases
   alias_1,alias_2,alias_3
   ```

   - 您可以使用以逗號分隔的清單來指定一或多個NetBios別名。
   - 指定的NetBios別名會新增至現有清單。
   - 如果清單目前空白、則會建立新的NetBios別名清單。
2. 確認已正確新增 NetBIOS 別名：`vserver cifs show -vserver vserver_name -display -netbios-aliases`

   ```
   vserver cifs show -vserver vs1 -display-netbios-aliases
   ```

   ```
   Vserver: vs1

            Server Name: CIFS_SERVER
            NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
   ```

相關資訊

- 從 SMB 伺服器清單中刪除 NetBIOS 別名

- 顯示 SMB 伺服器的 NetBIOS 別名列表

從 **ONTAP SMB** 伺服器清單中移除 **NetBIOS** 別名

如果您不需要CIFS伺服器的特定NetBios別名、可以從清單中移除這些NetBios別名。您也可以從清單中移除所有的NetBios別名。

關於這項工作

您可以使用以逗號分隔的清單來移除多個NetBios別名。您可以透過指定來移除 CIFS 伺服器上的所有 NetBIOS 別名 – 做為的值 `-netbios-aliases` 參數。

步驟

1. 執行下列其中一項動作：

如果您要移除...	輸入...
清單中的特定NetBios別名	`vserver cifs remove-netbios-aliases -vserver _vserver_name_ -netbios -aliases _NetBIOS_alias_,...`
清單中的所有NetBios別名	`vserver cifs remove-netbios-aliases -vserver vserver_name -netbios-aliases -`

```
vserver cifs remove-netbios-aliases -vserver vs1 -netbios-aliases alias_1
```

2. 確認已移除指定的 NetBIOS 別名：`vserver cifs show -vserver vserver_name -display -netbios-aliases`

```
vserver cifs show -vserver vs1 -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_2, ALIAS_3
```

顯示 **ONTAP SMB** 伺服器的 **NetBios** 別名清單

您可以顯示NetBios別名清單。當您想要判斷SMB用戶端可連線至CIFS伺服器的名稱清單時、這項功能很實用。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入...
CIFS伺服器的NetBios別名	`vserver cifs show -display-netbios -aliases`
詳細CIFS伺服器資訊的一部分是NetBios別名清單	`vserver cifs show -instance`

下列範例顯示CIFS伺服器的NetBios別名相關資訊：

```
vserver cifs show -display-netbios-aliases
```

```
Vserver: vs1

         Server Name: CIFS_SERVER
         NetBIOS Aliases: ALIAS_1, ALIAS_2, ALIAS_3
```

下列範例顯示詳細CIFS伺服器資訊的一部分是NetBios別名清單：

```
vserver cifs show -instance
```

```
                                        Vserver: vs1
                      CIFS Server NetBIOS Name: CIFS_SERVER
                  NetBIOS Domain/Workgroup Name: EXAMPLE
                    Fully Qualified Domain Name: EXAMPLE.COM
Default Site Used by LIFs Without Site Membership:
                         Authentication Style: domain
              CIFS Server Administrative Status: up
                        CIFS Server Description:
                        List of NetBIOS Aliases: ALIAS_1, ALIAS_2,
ALIAS_3
```

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

相關資訊

- 向伺服器新增 NetBIOS 別名列表
- 管理伺服器的命令

判斷 **ONTAP SMB** 用戶端是否使用 **NetBIOS** 別名連線

您可以判斷SMB用戶端是否使用NetBios別名進行連線、如果是、則會使用哪個NetBios別名進行連線。這在疑難排解連線問題時很有用。

關於這項工作

您必須使用 `-instance` 顯示與 SMB 連線相關聯的 NetBIOS 別名（如果有）的參數。如果使用 CIFS 伺服器名

稱或 IP 位址建立 SMB 連線、則會輸出 `NetBIOS Name` 欄位為 - （連字號）。

步驟

1. 執行所需的動作：

如果您要顯示下列項目的**NetBios**資訊...	輸入...
SMB 連線	`vserver cifs session show -instance`
使用指定的NetBios別名的連線：	`vserver cifs session show -instance -netbios-name` *`netbios_name`*

下列範例顯示使用工作階段ID 1建立SMB連線所用的NetBios別名資訊：

```
vserver cifs session show -session-id 1 -instance
```

```
                          Node: node1
                       Vserver: vs1
                    Session ID: 1
                 Connection ID: 127834
 Incoming Data LIF IP Address: 10.1.1.25
                   Workstation: 10.2.2.50
     Authentication Mechanism: NTLMv2
                 Windows User: EXAMPLE\user1
                    UNIX User: user1
                  Open Shares: 2
                   Open Files: 2
                   Open Other: 0
                Connected Time: 1d 1h 10m 5s
                     Idle Time: 22s
            Protocol Version: SMB3
       Continuously Available: No
            Is Session Signed: true
        User Authenticated as: domain-user
                  NetBIOS Name: ALIAS1
        SMB Encryption Status: Unencrypted
```

管理各種**SMB**伺服器工作

停止或啟動 **ONTAP SMB** 伺服器

您可以停止SVM上的CIFS伺服器、這在使用者無法透過SMB共用存取資料時、在執行工作時很有用。您可以啟動CIFS伺服器來重新啟動SMB存取。停止CIFS伺服器之後、您也可以修改儲存虛擬機器（SVM）上允許的傳輸協定。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
停止CIFS伺服器	`vserver cifs stop -vserver *vserver_name* [-foreground {true
false}]`	啟動CIFS伺服器
`vserver cifs start -vserver *vserver_name* [-foreground {true	false}]`

`-foreground` 指定命令應在前景或背景執行。如果您未輸入此參數、則會將其設為 `true`，命令將在前臺執行。

2. 使用驗證 CIFS 伺服器管理狀態是否正確 `vserver cifs show` 命令。

範例

下列命令會在SVM VS1上啟動CIFS伺服器：

```
cluster1::> vserver cifs start -vserver vs1

cluster1::> vserver cifs show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: VS1
                    NetBIOS Domain/Workgroup Name: DOMAIN
                      Fully Qualified Domain Name: DOMAIN.LOCAL
Default Site Used by LIFs Without Site Membership:
                             Authentication Style: domain
                CIFS Server Administrative Status: up
```

相關資訊

- 顯示探索到的伺服器相關資訊
- 重設並重新探索伺服器

將 **ONTAP SMB** 伺服器移至不同的 **OU**

除非您指定不同的OU、否則CIFS伺服器建立程序會在設定期間使用預設的組織單位（OU）CN=電腦。您可以在設定後將CIFS伺服器移至不同的OU。

步驟

1. 在Windows伺服器上、開啟「* Active Directory使用者與電腦*」樹狀結構。
2. 找出儲存虛擬機器（SVM）的Active Directory物件。

3. 在物件上按一下滑鼠右鍵、然後選取*移動*。
4. 選取您要與SVM建立關聯的OU

結果

SVM物件會放置在選取的OU中。

在移動 **ONTAP SMB** 伺服器之前，請先修改動態 **DNS** 網域

如果您想要Active Directory整合式DNS伺服器在將SMB伺服器移至其他網域時、在DNS中動態登錄SMB伺服器的DNS記錄、則必須先修改儲存虛擬機器（SVM）上的動態DNS（DDNS）、才能移動SMB伺服器。

開始之前

必須在SVM上修改DNS名稱服務、才能使用DNS網域、其中包含將包含SMB伺服器電腦帳戶之新網域的服務位置記錄。如果您使用的是安全的DDNS、則必須使用Active Directory整合的DNS名稱伺服器。

關於這項工作

雖然DDNS（如果在SVM上設定）會自動將資料LIF的DNS記錄新增至新網域、但原始網域的DNS記錄不會自動從原始DNS伺服器刪除。您必須手動刪除。

若要在移動SMB伺服器之前完成DDNS修改、請參閱下列主題：

"設定動態DNS服務"

將 **ONTAP SMB SVM** 加入 **Active Directory** 網域

您可以使用修改網域、將儲存虛擬機器（ SVM ）加入 Active Directory 網域、而無需刪除現有的 SMB 伺服器 `vserver cifs modify` 命令。您可以重新加入目前的網域、或加入新的網域。

開始之前

- SVM必須已有DNS組態。
- SVM的DNS組態必須能夠為目標網域提供服務。

  DNS伺服器必須包含網域LDAP和網域控制器伺服器的服務位置記錄（SRV),

關於這項工作

- CIFS 伺服器的管理狀態必須設為 `down`，才能繼續 Active Directory 網域修改。
- 如果命令成功完成，管理狀態會自動設定為 `up`。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 加入網域時、此命令可能需要幾分鐘的時間才能完成。

步驟

1. 將 SVM 加入 CIFS 伺服器網域： `vserver cifs modify -vserver` *`vserver_name`* `-domain` *`domain_name`* `-status-admin down`

   如"指令參考資料ONTAP"需詳細 `vserver cifs modify`資訊，請參閱。如果您需要重新設定新網域的 DNS ，請在中深入瞭解 `vserver dns modify`"指令參考資料ONTAP"。

若要為 SMB 伺服器建立 Active Directory 機器帳戶、您必須提供具有足夠權限的 Windows 帳戶名稱和密碼、以便將電腦新增至 `ou= example ou` 中的容器 *example*.com 網域。

從ONTAP 功能更新9.7開始、AD管理員可以提供Keytab檔案的URI、作為提供權限Windows帳戶名稱和密碼的替代方案。當您收到 URI 時、請將其加入 `-keytab-uri` 參數 `vserver cifs` 命令。

2. 確認 CIFS 伺服器位於所需的 Active Directory 網域： `vserver cifs show`

範例

在下列範例中、SVM VS1上的SMB伺服器「'CIFSSERVER1'」會使用Keytab驗證加入example.com網域：

```
cluster1::> vserver cifs modify -vserver vs1 -domain example.com -status
-admin down -keytab-uri http://admin.example.com/ontap1.keytab

cluster1::> vserver cifs show

          Server       Status       Domain/Workgroup  Authentication
Vserver   Name         Admin        Name              Style
--------- -----------  ---------    ----------------  --------------
vs1       CIFSSERVER1  up           EXAMPLE          domain
```

顯示 **ONTAP SMB NetBios over TCP** 連線的相關資訊

您可以顯示有關TCP上的NetBios（NBT）連線的資訊。這在疑難排解與NetBios相關的問題時很有用。

步驟

1. 使用 `vserver cifs nbtstat` 顯示關於 TCP 連線上的 NetBIOS 資訊的命令。

不支援透過IPv6提供的NetBios名稱服務（NBNS）。

範例

以下範例顯示「'cluster1'」的NetBios名稱服務資訊：

```
cluster1::> vserver cifs nbtstat

          Vserver: vs1
          Node:    cluster1-01
          Interfaces:
                   10.10.10.32
                   10.10.10.33
         Servers:
                   17.17.1.2  (active  )
         NBT Scope:
                  [ ]
         NBT Mode:
                  [h]
         NBT Name    NetBIOS Suffix   State   Time Left   Type
         ----------- ---------------  ------- ---------   -----
         CLUSTER_1   00               wins    57
         CLUSTER_1   20               wins    57

         Vserver: vs1
         Node:    cluster1-02
         Interfaces:
                 10.10.10.35
         Servers:
                 17.17.1.2  (active  )
         CLUSTER_1          00               wins          58
         CLUSTER_1          20               wins          58
         4 entries were displayed.
```

用於管理 **SMB** 伺服器的 **ONTAP** 命令

您需要知道建立、顯示、修改、停止、啟動、 和刪除SMB伺服器。也有命令可重設和重新探索伺服器、變更或重設機器帳戶密碼、排程機器帳戶密碼變更、以及新增或移除NetBios別名。

如果您想要...	使用此命令...
建立 SMB 伺服器	`vserver cifs create`
顯示SMB伺服器的相關資訊	`vserver cifs show`
修改 SMB 伺服器	`vserver cifs modify`
將SMB伺服器移至其他網域	`vserver cifs modify`

停止SMB伺服器	`vserver cifs stop`
啟動SMB伺服器	`vserver cifs start`
刪除 SMB 伺服器	`vserver cifs delete`
重設並重新探索SMB伺服器的伺服器	`vserver cifs domain discovered-servers reset-servers`
變更SMB伺服器的機器帳戶密碼	`vserver cifs domain password change`
重設SMB伺服器的機器帳戶密碼	`vserver cifs domain password change`
排程SMB伺服器機器帳戶的自動密碼變更	`vserver cifs domain password schedule modify`
新增SMB伺服器的NetBios別名	`vserver cifs add-netbios-aliases`
移除SMB伺服器的NetBios別名	`vserver cifs remove-netbios-aliases`

如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

相關資訊

"刪除 SMB 伺服器時、本機使用者和群組會發生什麼情況"

啟用 **ONTAP SMB NetBios** 名稱服務

從ONTAP 功能更新開始、預設會停用NetBios名稱服務（NBNS、有時稱為Windows網際網路名稱服務或WINS）。先前、不論網路上是否啟用了WINS、均會傳送名稱登錄廣播給啟用CIFS的儲存虛擬機器（SVM）。若要將此類廣播限制在需要NBNS的組態、您必須針對新的CIFS伺服器明確啟用NBNS。

開始之前

- 如果您已經使用NBNS並升級ONTAP 至版本S9、則不需要完成此工作。NBNS將繼續如以往一樣運作。
- 透過udp（連接埠137）啟用NBNS。
- 不支援透過IPv6的NBNS。

步驟

1. 將權限層級設為進階。

```
set -privilege advanced
```

2. 在CIFS伺服器上啟用NBNS。

```
vserver cifs options  modify -vserver <vserver name> -is-nbns-enabled
true
```

3. 返回管理權限層級。

```
set -privilege admin
```

使用IPv6進行SMB存取和SMB服務

瞭解 ONTAP 的 IPv6 SMB 需求

在SMB伺ONTAP 服器上使用IPv6之前、您必須先知道哪些版本的支援哪些版本的支援、以及授權需求為何。

不含授權需求ONTAP

取得SMB授權時、IPv6不需要特殊授權。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

SMB傳輸協定版本需求

- 對於SVM、ONTAP 支援所有SMB傳輸協定版本上的IPv6。

不支援透過IPv6提供的NetBios名稱服務（NBNS）。

瞭解支援 ONTAP SMB 存取和 CIFS 服務的 IPv6

如果您想要在CIFS伺服器上使用IPv6、您必須瞭解ONTAP 如何支援使用IPv6進行SMB存取、以及使用網路通訊來進行CIFS服務。

Windows用戶端與伺服器支援

支援支援IPv6的Windows伺服器和用戶端。ONTAP以下說明Microsoft Windows用戶端和伺服器IPv6支援：

- Windows 7、Windows 8、Windows Server 2008、Windows Server 2012及更新版本均支援IPv6用於SMB檔案共用及Active Directory服務、包括DNS、LDAP、CLDAP及Kerberos服務。

  如果設定IPv6位址、Windows 7和Windows Server 2008及更新版本預設會使用IPv6來執行Active Directory服務。支援透過IPv6連線進行的NTLM和Kerberos驗證。

  支援的所有Windows用戶端ONTAP 都可以使用IPv6位址連線至SMB共用區。

如需 Windows 用戶端 ONTAP 支援的最新資訊、請參閱 "互通性對照表"。

IPv6不支援NT網域。

額外的**CIFS**服務支援

除了IPv6支援SMB檔案共用和Active Directory服務之外、ONTAP 支援下列項目的功能還包括：

- 用戶端服務、包括離線資料夾、漫遊設定檔、資料夾重新導向及舊版
- 伺服器端服務、包括動態主目錄（主目錄功能）、symlink和Widgelinks、BranchCache、ODX複本卸載、自動節點參照、 和舊版
- 檔案存取管理服務、包括使用Windows本機使用者和群組進行存取控制和權限管理、使用CLI設定檔案權限和稽核原則、安全追蹤、檔案鎖定管理、以及監控SMB活動
- NAS多重傳輸協定稽核
- FPolicy
- 持續可用的共享區、見證傳輸協定及遠端VSS（搭配SMB上的Hyper-V組態使用）

名稱服務與驗證服務支援

IPv6支援與下列名稱服務的通訊：

- 網域控制器
- DNS伺服器
- LDAP 伺服器
- Kdc伺服器
- NIS 伺服器

瞭解 **ONTAP SMB** 伺服器如何使用 **IPv6** 連線至外部伺服器

若要建立符合需求的組態、您必須瞭解CIFS伺服器在連線至外部伺服器時如何使用IPv6。

- 來源位址選擇

  如果嘗試連線至外部伺服器、則選取的來源位址必須與目的地位址的類型相同。例如、如果連線至IPv6位址、則託管CIFS伺服器的儲存虛擬機器（SVM）必須具有IPv6位址的資料LIF或管理LIF、才能作為來源位址。同樣地、如果連線至IPV4位址、SVM必須具有資料LIF或管理LIF、且該資料具有可作為來源位址的IPV4位址。

- 對於使用DNS動態探索的伺服器、伺服器探索的執行方式如下：
  - 如果叢集上停用IPv6、則只會探索到IPv6伺服器位址。
  - 如果叢集上已啟用IPv6、則會同時探索IPv4和IPv6伺服器位址。視位址所屬伺服器的適用性、以及IPv6或IPv4資料或管理生命期的可用度而定、可能會使用這兩種類型。
    動態伺服器探索可用於探索網域控制器及其相關服務、例如LSA、NETLOGON、Kerberos及LDAP。
- DNS伺服器連線能力

  SVM在連線至DNS伺服器時是否使用IPv6、取決於DNS名稱服務組態。如果DNS服務設定為使用IPv6位址、則會使用IPv6建立連線。如果需要、DNS名稱服務組態可以使用IPV4位址、讓DNS伺服器的連線繼續使用IPV4位址。設定DNS名稱服務時、可以指定同時使用的IPv6位址和IPv6位址。

- LDAP 伺服器連線

SVM在連線至LDAP伺服器時是否使用IPv6、取決於LDAP用戶端組態。如果LDAP用戶端設定為使用IPv6位址、則會使用IPv6建立連線。如果需要、LDAP用戶端組態可以使用IPv4位址、以便連線至LDAP伺服器、繼續使用IPv4位址。設定LDAP用戶端組態時、可指定IPv6位址的組合。

LDAP用戶端組態用於設定LDAP以供UNIX使用者、群組及netgroup名稱服務使用。

- NIS 伺服器連線

  SVM 連線至 NIS 伺服器時是否使用 IPv6 、取決於 NIS 名稱服務組態。如果 NIS 服務設定為使用 IPv6 位址、則會使用 IPv6 進行連線。如果需要、NIS名稱服務組態可以使用IPv4位址、以便連線至NIS伺服器時、繼續使用IPv4位址。設定NIS名稱服務時、可指定IPv6位址的組合。

  NIS名稱服務用於儲存及管理UNIX使用者、群組、netgroup及主機名稱物件。

相關資訊

- 為伺服器啟用 IPv6
- 監控並顯示有關 IPv6 會話的信息

啟用 **ONTAP SMB** 伺服器的 **IPv6**

在叢集設定期間、不會啟用IPv6網路。叢集管理員必須在完成叢集設定之後啟用IPv6、才能將IPv6用於SMB。當叢集管理員啟用IPv6時、會為整個叢集啟用IPv6。

步驟

1. 啟用 IPv6 ： `network options ipv6 modify -enabled true`

   IPv6已啟用。可設定用於SMB存取的IPv6資料生命量。

相關資訊

- 監控並顯示有關 IPv6 會話的信息
- "使用 System Manager 視覺化網路"
- "在叢集上啟用 IPv6"
- "網路選項IPv6修改"

瞭解如何停用 **ONTAP SMB** 伺服器的 **IPv6**

即使使用網路選項在叢集上啟用IPv6、您仍無法使用相同的命令來停用SMB的IPv6。而ONTAP 當叢集管理員停用叢集上最後啟用IPv6的介面時、則會停用IPv6。您應該與叢集管理員溝通、瞭解如何管理啟用IPv6的介面。

相關資訊

- "使用系統管理員視覺化 ONTAP 網路"

監控及顯示 **IPv6 ONTAP SMB** 工作階段的相關資訊

您可以監控及顯示使用IPv6網路連線的SMB工作階段相關資訊。此資訊可用於判斷哪些用

戶端使用IPv6連線、以及其他有關IPv6 SMB工作階段的實用資訊。

步驟

1. 執行所需的動作：

如果您想要判斷...	輸入命令...
儲存虛擬機器（SVM）的SMB工作階段會使用IPv6連線	`vserver cifs session show -vserver vserver_name -instance`
IPv6用於透過指定LIF位址進行SMB工作階段	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address -instance` *LIF_IP_address* 為資料 LIF 的 IPv6 位址。

使用**SMB**設定檔案存取

設定安全樣式

安全樣式如何影響資料存取

瞭解 **ONTAP SMB** 安全風格及其影響

共有四種不同的安全型態：UNIX、NTFS、混合式及統一化。每種安全樣式對資料權限的處理方式都有不同的影響。您必須瞭解不同的影響、以確保為您的目的選擇適當的安全型態。

請務必瞭解、安全樣式並未決定哪些用戶端類型可以或無法存取資料。安全樣式只會決定ONTAP 用來控制資料存取的權限類型、以及哪些用戶端類型可以修改這些權限。

例如、如果某個磁碟區使用UNIX安全型態、則SMB用戶端仍可存取資料（前提是他們必須正確驗證及授權）、因為ONTAP 此為多重傳輸協定的本質。不過ONTAP 、VMware使用UNIX權限、只有UNIX用戶端可以使用原生工具進行修改。

安全風格	可以修改權限的用戶端	用戶端可以使用的權限	打造出有效的安全風格	可存取檔案的用戶端
UNIX	NFS	NFSv3模式位元	UNIX	NFS與SMB
		NFSv4.x ACL		
NTFS	中小企業	NTFS ACL	NTFS	
混合	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.ACL		
		NTFS ACL	NTFS	
統一化（僅適用於 Infinite Volume 、 ONTAP 9.4 及更早版本。）	NFS或SMB	NFSv3模式位元	UNIX	
		NFSv4.1 ACL		
		NTFS ACL	NTFS	

支援UNIX、NTFS和混合式安全型態的支援。FlexVol當安全性樣式混合或統一化時、有效權限取決於上次修改權限的用戶端類型、因為使用者是個別設定安全性樣式。如果上次修改權限的用戶端是NFSv3用戶端、則權限為UNIX NFSv3模式位元。如果最後一個用戶端是NFSv4用戶端、則權限為NFSv4 ACL。如果最後一個用戶端是SMB用戶端、則權限為Windows NTFS ACL。

統一化的安全風格僅適用於無限個Volume、ONTAP 而不再支援於更新版本的版本。如需詳細資訊、請參閱 介紹Volume管理總覽FlexGroup。

這 `show-effective-permissions`參數 `vserver security file-directory`命令可讓您顯示授予 Windows 或 UNIX 使用者在指定檔案或資料夾路徑上的有效權限。此外，選用參數 `-share-name`可讓您顯示有效共用權限。如"指令參考資料ONTAP"需詳細 `vserver security file-directory show-effective-permissions`資訊，請參閱。

> 最初設定部分預設檔案權限。ONTAP根據預設、UNIX、混合式及統一化安全樣式磁碟區中所有資料的有效安全樣式為UNIX、有效權限類型為UNIX模式位元（0755、除非另有說明）、直到用戶端依照預設安全性樣式所允許的方式進行設定為止。根據預設、NTFS安全型磁碟區中所有資料的有效安全樣式為NTFS、並具有ACL、可讓所有人完全掌控。

相關資訊

- "指令參考資料ONTAP"

瞭解設定 **ONTAP SMB** 安全風格的地點和時機

安全樣式可在FlexVol 支援樹狀結構（根或資料磁碟區）和qtree上設定。安全樣式可在建立時手動設定、自動繼承或稍後變更。

決定在 **ONTAP VM** 上使用哪些 **SMB** 安全樣式

為了協助您決定要在磁碟區上使用哪種安全樣式、您應該考慮兩個因素。主要因素是管理檔案系統的系統管理員類型。次要因素是存取磁碟區上資料的使用者或服務類型。

在Volume上設定安全樣式時、您應該考慮環境的需求、以確保您選擇最佳的安全樣式、並避免管理權限時發生問題。下列考量事項可協助您決定：

安全風格	選擇是否...
UNIX	• 檔案系統由UNIX管理員管理。 • 大多數使用者是NFS用戶端。 • 存取資料的應用程式會使用UNIX使用者做為服務帳戶。
NTFS	• 檔案系統由Windows管理員管理。 • 大多數使用者是 SMB 用戶端。 • 存取資料的應用程式會使用Windows使用者做為服務帳戶。
混合	檔案系統由UNIX和Windows系統管理員管理、使用者同時由NFS和SMB用戶端組成。

瞭解 **ONTAP SMB** 安全風格的繼承

如果您在建立新FlexVol 的流通量或qtree時未指定安全樣式、它會以不同的方式繼承其安全風格。

安全樣式會以下列方式繼承：

- 此功能會繼承包含SVM的根磁碟區安全樣式。FlexVol
- qtree會繼承其包含FlexVol 的不穩定區的安全樣式。
- 檔案或目錄會繼承其包含FlexVol 的不穩定磁碟區或qtree的安全樣式。

瞭解如何保留 **ONTAP SMB FlexVol** 磁碟區的 **UNIX** 權限

當Windows應用程式編輯並儲存目前具有UNIX權限的FlexVol 檔案時ONTAP 、即可保留UNIX權限。

當Windows用戶端上的應用程式編輯及儲存檔案時、他們會讀取檔案的安全性內容、建立新的暫存檔、將這些內容套用至暫存檔、然後為暫存檔提供原始檔案名稱。

當Windows用戶端執行安全性內容查詢時、會收到完全代表UNIX權限的建構ACL。此建構ACL的唯一目的是在Windows應用程式更新檔案時、保留檔案的UNIX權限、以確保產生的檔案具有相同的UNIX權限。不使用建構的ACL來設定任何NTFS ACL。ONTAP

瞭解如何使用適用於 **ONTAP SMB** 伺服器的 **Windows** 安全性索引標籤來管理 **UNIX** 權限

如果您想要在混合式安全型磁碟區或SVM上的qtree中、處理檔案或資料夾的UNIX權限、可以使用Windows用戶端上的「安全性」索引標籤。或者、您也可以使用可查詢及設定Windows ACL的應用程式。

- 修改UNIX權限

您可以使用「Windows安全性」索引標籤來檢視及變更混合式安全性型磁碟區或qtree的UNIX權限。如果您使用Windows安全性主索引標籤來變更UNIX權限、則必須先移除您要編輯的現有ACE（這會將模式位元設為0）、才能進行變更。或者、您也可以使用進階編輯器來變更權限。

如果使用模式權限、您可以直接變更所列的UID、GID和其他（電腦上有帳戶的其他人）的模式權限。例如、如果顯示的UID具有r-x權限、您可以將UID權限變更為rwx。

- 將UNIX權限變更為NTFS權限

  您可以使用「Windows安全性」索引標籤、將UNIX安全性物件取代為混合式安全性型磁碟區或qtree上的Windows安全性物件、其中檔案和資料夾具有UNIX有效的安全性樣式。

  您必須先移除所有列出的UNIX權限項目、才能將其取代為所需的Windows使用者和群組物件。然後您可以在Windows使用者和群組物件上設定NTFS型ACL。只要移除所有UNIX安全性物件、並將Windows使用者和群組新增至混合式安全性型磁碟區或qtree中的檔案或資料夾、即可將檔案或資料夾上的有效安全性樣式從UNIX變更為NTFS。

  變更資料夾的權限時、預設的Windows行為是將這些變更傳播到所有子資料夾和檔案。因此、如果您不想將安全性樣式的變更傳播到所有子資料夾、子資料夾和檔案、則必須將傳播選項變更為所需的設定。

在 **ONTAP SVM** 根磁碟區上設定 **SMB** 安全樣式

您可以設定儲存虛擬機器（SVM）根磁碟區安全樣式、以決定SVM根磁碟區上資料所使用的權限類型。

步驟

1. 使用 `vserver create` 命令 `-rootvolume-security-style` 定義安全樣式的參數。

   根 Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

2. 顯示並驗證組態、包括您所建立SVM的根磁碟區安全樣式： `vserver show -vserver` *`vserver_name`*

在 **ONTAP FlexVol** 磁碟區上設定 **SMB** 安全樣式

您可以設定FlexVol 「靜態Volume」安全樣式、以判斷FlexVol 儲存虛擬機器（SVM）的各個版本上的資料所使用的權限類型。

步驟

1. 執行下列其中一項動作：

如果FlexVol 是這個問題…	使用命令…
尚不存在	`volume create` 並包含 `-security-style` 指定安全樣式的參數。
已存在	`volume modify` 並包含 `-security-style` 指定安全樣式的參數。

   FlexVol Volume 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果您在建立FlexVol 一個穩定區時未指定安全樣式、則此磁碟區會繼承根磁碟區的安全樣式。

如需更多關於的資訊、請參閱 `volume create` 或 `volume modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括FlexVol 您所建立的穩定功能、請輸入下列命令：

```
volume show -volume volume_name -instance
```

在 ONTAP qtree 上設定 SMB 安全樣式

您可以設定qtree Volume安全樣式、以決定用於qtree上資料的權限類型。

步驟

1. 執行下列其中一項動作：

如果**qtree ...**	使用命令**...**
尚未存在	`volume qtree create` 並包含 `-security -style` 指定安全樣式的參數。
已存在	`volume qtree modify` 並包含 `-security -style` 指定安全樣式的參數。

qtree 安全樣式的可能選項為 `unix`、 `ntfs`或 `mixed`。

如果在建立 qtree 時未指定安全樣式、則預設的安全樣式為 `mixed`。

如需更多關於的資訊、請參閱 `volume qtree create` 或 `volume qtree modify` 命令、請參閱 "邏輯儲存管理"。

2. 若要顯示組態、包括您建立的 qtree 安全樣式、請輸入下列命令： `volume qtree show -qtree qtree_name -instance`

在**NAS**命名空間中建立及管理資料磁碟區

瞭解如何在 NAS 命名空間中建立及管理 ONTAP SMB 資料磁碟區

若要管理NAS環境中的檔案存取、您必須管理儲存虛擬機器（SVM）上的資料磁碟區和交會點。這包括規劃命名空間架構、建立具有或不含交會點的磁碟區、掛載或卸載磁碟區、以及顯示資料磁碟區和NFS伺服器或CIFS伺服器命名空間的相關資訊。

使用指定的交會點建立 ONTAP SMB 資料磁碟區

您可以在建立資料Volume時指定交會點。結果Volume會自動掛載於交會點、並可立即設定以進行NAS存取。

開始之前

您要在其中建立磁碟區的集合體必須已經存在。

下列字元無法用於交會路徑：*#"><|？\

此外、交會路徑長度不得超過255個字元。

步驟

1. 建立具有交會點的Volume： `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed} -junction-path junction_path`

   交會路徑必須以根（/）開頭、且可同時包含目錄和輔助磁碟區。交會路徑不需要包含磁碟區名稱。交會路徑與磁碟區名稱無關。

   指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用至所建立資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

   接合路徑不區分大小寫； `/ENG` 與相同 `/eng`。如果您建立CIFS共用區、Windows會將交會路徑視為區分大小寫。例如、如果交會是 `/ENG`、 CIFS 共用路徑必須以開頭 `/ENG`、不是 `/eng`。

   您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 確認已使用所需的交會點建立磁碟區： `volume show -vserver vserver_name -volume volume_name -junction`

範例

以下範例建立一個名為「 'home4' 」的 Volume 、該 Volume 位於 SVM VS1 上、且具有交會路徑 `/eng/home` ：

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1
-size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -volume home4 -junction
                  Junction                 Junction
Vserver   Volume  Active   Junction Path   Path Source
--------- ------- -------- --------------- -----------
vs1       home4   true     /eng/home       RW_volume
```

建立 **ONTAP SMB** 資料磁碟區而不指定交會點

您可以建立資料Volume而不指定交會點。結果Volume不會自動掛載、也無法設定NAS存取。您必須先掛載磁碟區、才能設定該磁碟區的SMB共用區或NFS匯出。

開始之前

您要在其中建立磁碟區的集合體必須已經存在。

步驟

1. 使用下列命令建立沒有交會點的磁碟區： `volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size {integer[KB|MB|GB|TB|PB]} -security-style {ntfs|unix|mixed}`

   指定Volume安全樣式為選用項目。如果您未指定安全樣式、ONTAP 則會以套用至儲存虛擬機器（SVM）根磁碟區的相同安全樣式來建立磁碟區。不過、根磁碟區的安全樣式可能不是您要套用到資料磁碟區的安全樣式。建議您在建立磁碟區時指定安全樣式、以將難以疑難排解的檔案存取問題降至最低。

   您可以使用許多選用參數來自訂資料Volume。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

2. 驗證是否在沒有連接點的情況下建立磁碟區： `volume show -vserver vserver_name -volume volume_name -junction`

範例

下列範例建立名為「shes」的磁碟區、位於SVM VS1上、但未掛載於交會點：

```
cluster1::> volume create -vserver vs1 -volume sales -aggregate aggr3
-size 20GB
[Job 3406] Job succeeded: Successful

cluster1::> volume show -vserver vs1 -junction
                    Junction                 Junction
Vserver   Volume    Active   Junction Path   Path Source
--------- --------- -------- --------------- -----------
vs1       data      true     /data           RW_volume
vs1       home4     true     /eng/home       RW_volume
vs1       vs1_root  -        /               -
vs1       sales     -        -               -
```

在 **NAS** 命名空間中掛載或卸載現有的 **ONTAP SMB** 磁碟區

磁碟區必須先掛載到NAS命名空間、才能設定NAS用戶端存取儲存虛擬機器（SVM）磁碟區中所含的資料。如果目前未掛載磁碟區、您可以將其掛載至交會點。您也可以卸載Volume。

關於這項工作

如果您卸載磁碟區並使其離線、則 NAS 用戶端無法存取連接點內的所有資料、包括位於未掛載磁碟區命名空間內具有連接點的磁碟區中的資料。

若要停止NAS用戶端對磁碟區的存取、只是卸載磁碟區是不夠的。您必須將磁碟區離線、或採取其他步驟、確保用戶端檔案處理快取無效。如需詳細資訊、請參閱下列知識庫文章： "NFSv3用戶端在從ONTAP 靜態命名空間移除後、仍可存取Volume"

當您卸載磁碟區時、磁碟區內的資料不會遺失。此外、在磁碟區或未掛載磁碟區內的目錄和交會點上建立的現有磁碟區匯出原則和SMB共用也會保留下來。如果您重新掛載未掛載的Volume、NAS用戶端可以使用現有的匯出原則和SMB共用來存取磁碟區內的資料。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
掛載Volume	`volume mount -vserver svm_name -volume volume_name -junction-path junction_path`

卸載Volume	`volume unmount -vserver svm_name -volume volume_name`
	
	`volume offline -vserver svm_name -volume volume_name`

2. 驗證磁碟區是否處於所需的掛載狀態：

   `volume show -vserver svm_name -volume volume_name -fields state,junction-path,junction-active`

範例

以下範例將位於 SVM 'VS1' 的名為 """""""s'" 的 Volume 裝入連接點 "'/sales" ：

```
cluster1::> volume mount -vserver vs1 -volume sales -junction-path /sales

cluster1::> volume show -vserver vs1 state,junction-path,junction-active

vserver   volume     state     junction-path   junction-active
--------- ---------- -------- --------------- ----------------
vs1       data       online    /data           true
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

以下範例將卸載並離線位於 SVM 「 'VS1 」上的名為「 dATA 」的磁碟區：

```
cluster1::> volume unmount -vserver vs1 -volume data
cluster1::> volume offline -vserver vs1 -volume data

cluster1::> volume show -vserver vs1 -fields state,junction-path,junction-
active

vserver   volume     state     junction-path   junction-active
--------- ---------- --------- --------------- ---------------
vs1       data       offline   -               -
vs1       home4      online    /eng/home       true
vs1       sales      online    /sales          true
```

顯示 **ONTAP SMB Volume** 裝載和交會點資訊

您可以顯示儲存虛擬機器（SVM）掛載磁碟區的相關資訊、以及掛載磁碟區的交會點。您也可以決定哪些磁碟區未掛載到交會點。您可以使用此資訊來瞭解及管理SVM命名空間。

步驟

1. 執行所需的動作：

如果您要顯示...	輸入命令...
SVM上掛載與卸載磁碟區的摘要資訊	`volume show -vserver vserver_name -junction`
SVM上掛載與卸載磁碟區的詳細資訊	`volume show -vserver vserver_name -volume volume_name -instance`
有關SVM上掛載和卸載磁碟區的特定資訊	a. 如有必要、您可以顯示的有效欄位 `-fields` 使用下列命令的參數： `volume show -fields ?` b. 使用顯示所需資訊 `-fields` 參數： Volume show -vserver vserver_name -fieldname 、 …

範例

下列範例顯示SVM VS1上掛載與卸載磁碟區的摘要：

```
cluster1::> volume show -vserver vs1 -junction
                     Junction                 Junction
Vserver   Volume     Active   Junction Path   Path Source
--------- ---------- -------- --------------- -----------
vs1       data       true     /data           RW_volume
vs1       home4      true     /eng/home       RW_volume
vs1       vs1_root   -        /               -
vs1       sales      true     /sales          RW_volume
```

下列範例顯示SVM VS2上磁碟區的指定欄位資訊：

```
cluster1::> volume show -vserver vs2 -fields
vserver,volume,aggregate,size,state,type,security-style,junction-
path,junction-parent,node
vserver volume   aggregate size state  type security-style junction-path
junction-parent node
------- ------   --------- ---- ------ ---- -------------- -------------
--------------- -----
vs2     data1    aggr3     2GB  online RW   unix           -             -
node3
vs2     data2    aggr3     1GB  online RW   ntfs           /data2
vs2_root        node3
vs2     data2_1  aggr3     8GB  online RW   ntfs           /data2/d2_1
data2           node3
vs2     data2_2  aggr3     8GB  online RW   ntfs           /data2/d2_2
data2           node3
vs2     pubs     aggr1     1GB  online RW   unix           /publications
vs2_root        node1
vs2     images   aggr3     2TB  online RW   ntfs           /images
vs2_root        node3
vs2     logs     aggr1     1GB  online RW   unix           /logs
vs2_root        node1
vs2     vs2_root aggr3     1GB  online RW   ntfs           /             -
node3
```

設定名稱對應

瞭解 ONTAP SMB 名稱對應組態

利用名稱對應功能、將CIFS身分識別對應至UNIX身分識別、將Kerberos身分識別對應至UNIX身分識別、並將UNIX身分識別對應至CIFS身分識別。ONTAP無論是從NFS用戶端或CIFS用戶端連線、IT都需要這些資訊來取得使用者認證並提供適當的檔案存取。

您不需要使用名稱對應的情況有兩種例外：

- 您可以設定純UNIX環境、但不打算在磁碟區上使用CIFS存取或NTFS安全樣式。
- 您可以設定要使用的預設使用者。

  在此案例中、不需要名稱對應、因為不會對應每個個別用戶端認證、而是將所有用戶端認證對應至相同的預設使用者。

請注意、您只能針對使用者使用名稱對應、而不能針對群組使用名稱對應。

不過、您可以將一組個別使用者對應至特定使用者。例如、您可以將開頭或結尾的所有AD使用者對應至特定UNIX使用者、以及使用者的UID。

瞭解 **ONTAP SMB** 名稱對應

當必須對應使用者的認證資料時、它會先檢查本機名稱對應資料庫和LDAP伺服器、以找出現有的對應。ONTAP無論是檢查一項或兩項、或是按SVM的名稱服務組態來決定順序。

- 適用於Windows至UNIX對應

  如果找不到對應、ONTAP 則此功能會檢查UNIX網域中的Windows使用者名稱是否為有效的使用者名稱。如果這不管用、它會使用預設的UNIX使用者、前提是已設定。如果未設定預設UNIX使用者、ONTAP 且無法以這種方式取得對應、則對應會失敗、並傳回錯誤。

- 適用於UNIX至Windows對應

  如果找不到對應、ONTAP 則嘗試尋找與SMB網域中UNIX名稱相符的Windows帳戶。如果這不管用、它會使用預設的SMB使用者、前提是已設定。如果未設定預設的 CIFS 使用者、且 ONTAP 也無法以這種方式取得對應、則對應會失敗、並傳回錯誤。

依預設、機器帳戶會對應至指定的預設UNIX使用者。如果未指定預設UNIX使用者、則機器帳戶對應會失敗。

- 從功能表9.5開始ONTAP 、您可以將機器帳戶對應至預設UNIX使用者以外的使用者。
- 在更新版本的版本中、您無法將機器帳戶對應到其他使用者。ONTAP

  即使已定義機器帳戶的名稱對應、也會忽略對應。

瞭解 **ONTAP SMB** 多網域搜尋 **UNIX** 使用者至 **Windows** 使用者名稱對應

將UNIX使用者對應至Windows使用者時、支援多網域搜尋。ONTAP在傳回相符結果之前、會搜尋所有探索到的信任網域是否符合取代模式。或者、您也可以設定偏好的信任網域清單、以取代探索到的信任網域清單、並依序搜尋、直到傳回相符的結果為止。

網域信任如何影響**UNIX**使用者對**Windows**使用者名稱對應搜尋

若要瞭解多網域使用者名稱對應的運作方式、您必須瞭解網域信任如何搭配ONTAP 使用。Active Directory與CIFS伺服器主網域的信任關係可以是雙向信任關係、也可以是兩種單向信任關係之一、即傳入信任關係或傳出信任關係。主網域是SVM上CIFS伺服器所屬的網域。

- 雙向信任

透過雙向信任、這兩個網域彼此信任。如果CIFS伺服器的主網域與另一個網域具有雙向信任、主網域可以驗證及授權屬於信任網域的使用者、反之亦然。

UNIX使用者對Windows使用者名稱對應搜尋只能在主網域與其他網域之間具有雙向信任的網域上執行。

- 傳出信任_

  透過傳出信任、主網域信任其他網域。在此情況下、主網域可以驗證及授權屬於傳出信任網域的使用者。

  執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域外傳信任的網域。

- 傳入信任_

  在傳入信任的情況下、其他網域會信任CIFS伺服器的主網域。在此情況下、主網域無法驗證或授權屬於傳入信任網域的使用者。

  在執行UNIX使用者對Windows使用者名稱對應搜尋時、會搜尋具有主網域傳入信任的網域。

如何使用萬用字元（*）來設定多網域搜尋名稱對應

在Windows使用者名稱的網域區段中使用萬用字元、可協助進行多網域名稱對應搜尋。下表說明如何在名稱對應項目的網域部分使用萬用字元來啟用多網域搜尋：

模式	更換	結果
根	*\系統管理員	UNIX使用者「root」會對應至名為「Administrator」的使用者。搜尋所有信任的網域、直到找到第一個相符的使用者「'Administrator」為止。
*	**	有效的UNIX使用者會對應至對應的Windows使用者。會依序搜尋所有信任的網域、直到找到第一個與該名稱相符的使用者為止。 模式「*」僅適用於從UNIX到Windows的名稱對應、而非其他方式。

執行多網域名稱搜尋的方式

您可以選擇兩種方法之一來決定用於多網域名稱搜尋的信任網域清單：

- 使用ONTAP 由資訊更新所編譯的自動探索雙向信任清單
- 使用您所編譯的慣用信任網域清單

如果UNIX使用者以萬用字元對應至使用者名稱的網域區段、則Windows使用者會在所有信任的網域中查詢、如下所示：

- 如果已設定慣用的信任網域清單、則對應的Windows使用者只會依序在搜尋清單中查詢。
- 如果未設定信任網域的慣用清單、則會在主網域的所有雙向信任網域中查詢Windows使用者。
- 如果主網域沒有雙向信任的網域、則會在主網域中查詢該使用者。

如果UNIX使用者對應至使用者名稱中沒有網域區段的Windows使用者、則會在主網域中查詢Windows使用者。

瞭解 ONTAP SMB 名稱對應轉換規則

這個系統可為每個SVM保留一組轉換規則。ONTAP每個規則包含兩個部分：*Pattern_* 和*_replace*。轉換從適當清單的開頭開始、並根據第一個相符規則執行替代。模式是UNIX樣式的規則運算式。取代是包含轉義序列的字串、代表模式中的子運算式、如同 UNIX `sed` 方案。

建立 ONTAP SMB 名稱對應

您可以使用 `vserver name-mapping create` 建立名稱對應的命令。您可以使用名稱對應來讓Windows使用者存取UNIX安全樣式的磁碟區和相反的磁碟區。

關於這項工作

針對每個SVM、ONTAP 支援最多12、500個各個方向的名稱對應。

步驟

1. 建立名稱對應： `vserver name-mapping create -vserver *vserver_name* -direction {krb-unix|win-unix|unix-win} -position *integer* -pattern text -replacement *text*`

> ⓘ `-pattern`和 `-replacement`陳述式可做為規則運算式來表示。您也可以使用 `-replacement` null
> 置換字串（空格字元），使用陳述式明確拒絕對應至使用者 `" "`
> 。如link:https://docs.netapp.com/us-en/ontap-cli/vserver-name-mapping-create.html["指令參考資料ONTAP"^]需詳細 `vserver name-mapping create`資訊，請參閱。

建立Windows對UNIX的對應時、ONTAP 在建立新對應時、任何與該系統有開放連線的SMB用戶端、都必須登出並重新登入、才能看到新的對應。

範例

下列命令會在名為VS1的SVM上建立名稱對應。對應是從UNIX到Windows的對應、位於優先順序清單中的位置1。對應會將UNIX使用者johnd對應至Windows使用者ENH\JohnDoe。

```
vs1::> vserver name-mapping create -vserver vs1 -direction unix-win
-position 1 -pattern johnd
-replacement "ENG\\JohnDoe"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。對應是從Windows到UNIX的對應、位於優先順序清單中

的位置1。這裏的模式和替換包括正則表達式。對應會將網域中的每個CIFS使用者對應到與SVM相關聯的LDAP網域中的使用者。

```
vs1::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 1 -pattern "ENG\\(.+)"
-replacement "\1"
```

下列命令會在名為VS1的SVM上建立另一個名稱對應。在此模式中、Windows使用者名稱中的「$」元素必須轉義、對應會將Windows使用者ENH\ John$ops對應至UNIX使用者john_ops。

```
vs1::> vserver name-mapping create -direction win-unix -position 1
-pattern ENG\\john\$ops
-replacement john_ops
```

設定預設的 **ONTAP SMB** 使用者

您可以將預設使用者設定為在使用者的所有其他對應嘗試失敗時使用、或是不想在UNIX與Windows之間對應個別使用者時使用。或者、如果您想要驗證未對應的使用者失敗、則不應設定預設使用者。

關於這項工作

對於CIFS驗證、如果您不想將每個Windows使用者對應至個別的UNIX使用者、則可以改為指定預設的UNIX使用者。

對於NFS驗證、如果您不想將每個UNIX使用者對應至個別的Windows使用者、則可以改為指定預設的Windows使用者。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入下列命令...
設定預設UNIX使用者	`vserver cifs options modify -default -unix-user` *`user_name`*
設定預設的Windows使用者	`vserver nfs modify -default-win-user` *`user_name`*

用於管理 **SMB** 名稱對應的 **ONTAP** 命令

管理名稱對應時、會ONTAP 有特定的功能不全指令。

如果您想要...	使用此命令...
建立名稱對應	`vserver name-mapping create`

在特定位置插入名稱對應	`vserver name-mapping insert`
顯示名稱對應	`vserver name-mapping show`
交換兩個名稱對應的位置附註：當名稱對應設定為IP辨識符號項目時、不允許交換。	`vserver name-mapping swap`
修改名稱對應	`vserver name-mapping modify`
刪除名稱對應	`vserver name-mapping delete`
驗證正確的名稱對應	`vserver security file-directory show-effective-permissions -vserver vs1 -win-user-name user1 -path / -share-name sh1`

如"指令參考資料ONTAP"需詳細 `vserver name-mapping`資訊，請參閱。

設定多網域名稱對應搜尋

啟用或停用 **ONTAP SMB** 多網域名稱對應搜尋

透過多網域名稱對應搜尋、您可以在設定UNIX使用者至Windows使用者名稱對應時、在Windows名稱的網域部分使用萬用字元（*）。在名稱的網域部分使用萬用字元（*）、ONTAP 可讓Sylsin搜尋所有與包含CIFS伺服器電腦帳戶之網域具有雙向信任的網域。

關於這項工作

除了搜尋雙向信任的所有網域之外、您也可以設定偏好的信任網域清單。設定偏好的信任網域清單時ONTAP 、將使用偏好的信任網域清單、而非雙向探索的信任網域、來執行多網域名稱對應搜尋。

- 預設會啟用多網域名稱對應搜尋。
- 此選項適用於進階權限層級。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您想要多網域名稱對應搜尋...	輸入命令...
已啟用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-trusted-domain-enum -search-enabled true`

如果您想要多網域名稱對應搜尋...	輸入命令...
已停用	`vserver cifs options modify -vserver vserver_name -is-trusted-domain-enum -search-enabled false`

3. 返回管理權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

重設並重新探索信任的 **ONTAP SMB** 網域

您可以強制重新探索所有信任的網域。當受信任的網域伺服器沒有適當回應或信任關係變更時、此功能就很有用。只會探索主網域具有雙向信任的網域、亦即包含CIFS伺服器電腦帳戶的網域。

步驟

1. 使用重設及重新探索信任的網域 `vserver cifs domain trusts rediscover` 命令。

```
vserver cifs domain trusts rediscover -vserver vs1
```

相關資訊

顯示探索到的信任網域相關資訊

顯示探索到的受信任 **ONTAP SMB** 網域相關資訊

您可以顯示CIFS伺服器主網域（包含CIFS伺服器電腦帳戶的網域）的已探索信任網域資訊。當您想要知道要探索哪些信任網域、以及如何在探索到的信任網域清單中排序時、這項功能就很有用。

關於這項工作

只會探索具有主網域雙向信任的網域。由於主網域的網域控制器（DC）會依照DC決定的順序傳回信任網域清單、因此無法預測清單中網域的順序。藉由顯示信任網域的清單、您可以決定多網域名稱對應搜尋的搜尋順序。

顯示的信任網域資訊會依節點和儲存虛擬機器（SVM）分組。

步驟

1. 使用顯示探索到的信任網域相關資訊 `vserver cifs domain trusts show` 命令。

```
vserver cifs domain trusts show -vserver vs1
```

```
   Node: node1
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM

   Node: node2
Vserver: vs1

Home Domain             Trusted Domain
---------------------   ----------------------------------
EXAMPLE.COM             CIFS1.EXAMPLE.COM,
                        CIFS2.EXAMPLE.COM
                        EXAMPLE.COM
```

相關資訊

重設並重新探索信任的網域

在偏好的清單中新增，移除或取代信任的 **ONTAP SMB** 網域

您可以從SMB伺服器的慣用信任網域清單中新增或移除信任的網域、也可以修改目前的清單。如果您設定慣用的信任網域清單、則執行多網域名稱對應搜尋時、會使用此清單而非探索到的雙向信任網域。

關於這項工作

- 如果您要將信任的網域新增至現有清單、新清單會與現有清單合併、新項目會放在最後系統會依照信任網域清單中顯示的順序來搜尋信任的網域。
- 如果您要從現有清單中移除信任的網域、但未指定清單、則會移除指定儲存虛擬機器（SVM）的整個信任網域清單。
- 如果您修改現有的信任網域清單、新清單會覆寫現有清單。

> 您應該只在慣用的信任網域清單中輸入雙向信任的網域。即使您可以將傳出或傳入的信任網域輸入偏好的網域清單、但在執行多網域名稱對應搜尋時仍不會使用這些網域。跳過單向網域的項目、然後移至清單中的下一個雙向信任網域。ONTAP

步驟

1. 執行下列其中一項動作：

如果您要使用偏好的信任網域清單執行下列動作...	使用命令...
將信任的網域新增至清單	`vserver cifs domain name-mapping-search add -vserver _vserver_name_ -trusted-domains FQDN, ...`
從清單中移除信任的網域	`vserver cifs domain name-mapping-search remove -vserver _vserver_name_ [-trusted-domains FQDN, ...]`
修改現有清單	`vserver cifs domain name-mapping-search modify -vserver _vserver_name_ -trusted-domains FQDN, ...`

範例

下列命令會將兩個信任的網域（cifs1.example.com和cifs2.example.com）新增至SVM VS1所使用的慣用信任網域清單：

```
cluster1::> vserver cifs domain name-mapping-search add -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

下列命令會從SVM VS1使用的清單中移除兩個信任的網域：

```
cluster1::> vserver cifs domain name-mapping-search remove -vserver vs1
-trusted-domains cifs1.example.com, cifs2.example.com
```

下列命令會修改SVM VS1所使用的信任網域清單。新清單會取代原始清單：

```
cluster1::> vserver cifs domain name-mapping-search modify -vserver vs1
-trusted-domains cifs3.example.com
```

相關資訊

顯示偏好信任網域清單的相關資訊

顯示偏好的受信任 **ONTAP SMB** 網域清單的相關資訊

您可以顯示偏好的信任網域清單中的信任網域資訊、以及啟用多網域名稱對應搜尋時的搜尋順序。您可以將偏好的信任網域清單設定為使用自動探索的信任網域清單的替代方法。

步驟

1. 執行下列其中一項動作：

如果您要顯示下列項目的相關資訊...	使用命令...
叢集中依儲存虛擬機器（SVM）分組的所有慣用信任網域	`vserver cifs domain name-mapping-search show`
指定SVM的所有慣用信任網域	`vserver cifs domain name-mapping-search show -vserver` *vserver_name*

下列命令會顯示叢集上所有慣用信任網域的相關資訊：

```
cluster1::> vserver cifs domain name-mapping-search show
Vserver          Trusted Domains
--------------   ---------------------------------
vs1              CIFS1.EXAMPLE.COM
```

相關資訊

在首選清單中新增、刪除或取代受信任網域

建立及設定SMB共用區

瞭解如何建立及設定 ONTAP SMB 共用

在使用者和應用程式能夠透過SMB存取CIFS伺服器上的資料之前、您必須先建立和設定SMB共用、這是磁碟區中的命名存取點。您可以指定共用參數及共用屬性來自訂共用區。您可以隨時修改現有的共用區。

當您建立SMB共用時ONTAP 、利用「完全控制」權限、針對每個人建立共用區的預設ACL。

SMB共用會繫結至儲存虛擬機器（SVM）上的CIFS伺服器。如果刪除SVM、或從SVM中刪除與其相關聯的CIFS伺服器、則會刪除SMB共用。如果您在SVM上重新建立CIFS伺服器、則必須重新建立SMB共用。

相關資訊

- 了解本地用戶和群組
- "Microsoft Hyper-V和SQL Server的SMB組態"
- 配置卷上的檔案名稱轉換的字元映射

瞭解預設的管理 ONTAP SMB 共用

當您在儲存虛擬機器（SVM）上建立CIFS伺服器時、系統會自動建立預設的管理共用區。您應該瞭解這些預設共用是什麼、以及它們的使用方式。

建立CIFS伺服器時、會建立下列預設管理共用：ONTAP

> 從功能支援的9.8開始ONTAP 、系統將不再預設建立admin$共用區。

- IPC$
- admin$（ONTAP 僅限用作更新版本的版本）
- C$

因為以$字元結尾的共用是隱藏共用、所以「我的電腦」不會顯示預設的管理共用、但您可以使用「共用資料夾」來檢視這些共用。

如何使用**IPC$**和**admin$**預設共用

IPC$和admin$共用是ONTAP 由Windows管理員使用、無法用來存取位於SVM上的資料。

- IPC$共用

  IPC$共用資源可共用具名管道、這些管道對於程式之間的通訊非常重要。IPC$共用區用於遠端管理電腦、以及檢視電腦的共用資源。您無法變更IPC$共用區的共用設定、共用內容或ACL。您也無法重新命名或刪除IPC$共用區。

- admin$共享區（ONTAP 僅限用作更新版本的版本）

  > 從功能支援的9.8開始ONTAP 、系統將不再預設建立admin$共用區。

  admin$共用區是在遠端管理SVM期間使用。此資源的路徑永遠是SVM根目錄的路徑。您無法變更admin$共用區的共用設定、共用內容或ACL。您也無法重新命名或刪除admin$共用區。

使用**c$**預設共用的方式

c$共用區是叢集或SVM管理員可用來存取及管理SVM根磁碟區的管理共用區。

以下是c$共用區的特性：

- 此共用區的路徑永遠是SVM根磁碟區的路徑、無法修改。
- c$共用區的預設ACL為「管理員/完全控制」。

  此使用者為BUILTIN\Administrator。根據預設、BUILTIN\Administrator可以對應至共用區、並在對應的根目錄中檢視、建立、修改或刪除檔案和資料夾。管理此目錄中的檔案和資料夾時、請務必謹慎。

- 您可以變更c$共用區的ACL。
- 您可以變更c$共用設定及共用內容。
- 您無法刪除c$共用區。
- SVM系統管理員可以跨越命名空間連接點、從對應的c$共用區存取SVM命名空間的其餘部分。
- 您可以使用Microsoft管理主控台存取c$共用區。

相關資訊

使用 Windows 安全性標籤設定進階檔案權限

瞭解 **ONTAP SMB** 共享命名要求

在SMB伺服器ONTAP 上建立SMB共用時、請務必記住「不共享區」的命名要求。

共享的名稱命名慣例ONTAP 與Windows相同、並包含下列需求：

- SMB伺服器的每個共用區名稱必須是唯一的。
- 共用名稱不區分大小寫。
- 共享區名稱長度上限為80個字元。
- 支援統一碼共用名稱。
- 以$字元結尾的共用名稱為隱藏共用。
- 對於更新版本的版本、系統會自動在每部CIFS伺服器上建立管理共用區管理$、IPC$和c$、並保留共用名稱ONTAP 。從零件9.8開始ONTAP 、系統不再自動建立admin$共用區。
- 建立共用時、您無法使用共用名稱ONTAP_admin$。
- 支援含有空格的共用名稱：
  - 您不能使用空格作為共用名稱的第一個字元或最後一個字元。
  - 您必須以引號括住包含空格的共用名稱。

  單引號被視為共享區名稱的一部分、無法用來取代引號。
- 當您命名SMB共用時、支援下列特殊字元：

```
! @ # $ % & ' _ - . ~ ( ) { }
```

- 當您命名SMB共用時、不支援下列特殊字元：

```
** [ ] " / \ : ; | < > , ? * =
```

瞭解在多重傳輸協定環境中建立共用時， **ONTAP SMB** 目錄區分大小寫的需求

如果您在SVM中建立共用區、使用8.3命名配置來區分只有不同名稱大小寫的目錄名稱、則必須在共用路徑中使用8.3名稱、以確保用戶端連線至所需的目錄路徑。

在下列範例中、Linux用戶端上建立了兩個名為「'testdir'」和「'TESTDIR'」的目錄。包含目錄的磁碟區的交會路徑為 `/home`。第一個輸出來自Linux用戶端、第二個輸出來自SMB用戶端。

```
 ls -l
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:23 testdir
drwxrwxr-x 2 user1 group1   4096 Apr 17 11:24 TESTDIR
```

```
dir

 Directory of Z:\

04/17/2015  11:23 AM    <DIR>          testdir
04/17/2015  11:24 AM    <DIR>          TESTDI~1
```

建立第二個目錄的共用時、您必須在共用路徑中使用8.3名稱。在此範例中、第一個目錄的共用路徑為 `/home/testdir` 而第二個目錄的共用路徑則是 `/home/TESTDI~1`。

使用SMB共用內容

瞭解如何使用 **ONTAP SMB** 共用內容

您可以自訂SMB共用的內容。

可用的共用內容如下：

共用內容	說明
`oplocks`	此內容會指定共用區使用投機性鎖定、也稱為用戶端快取。
`browsable`	此內容可讓Windows用戶端瀏覽共用區。
`showsnapshot`	此內容指定用戶端可以檢視及周遊快照。
`changenotify`	此內容指定共用區支援變更通知要求。對於SVM上的共用、這是預設的初始屬性。
`attributecache`	此屬性可讓SMB共用區上的檔案屬性快取、以提供更快速的屬性存取。預設為停用屬性快取。只有當用戶端透過SMB 1.0連線至共用時、才應啟用此屬性。如果用戶端透過SMB 2.x或SMB 3.0連線至共用區、則此共用內容不適用。
`continuously-available`	此內容可讓支援此功能的SMB用戶端持續開啟檔案。以這種方式開啟的檔案可避免發生中斷事件、例如容錯移轉和還原。
`branchcache`	此內容指定共用區可讓用戶端要求此共用區內檔案的BranchCache雜湊。只有在CIFS BranchCache組態中指定「每個共用區」作為作業模式時、此選項才有用。

共用內容	說明
`access-based-enumeration`	此內容指定在此共用區上啟用_Access Based Enumeration_（ABE）。根據個別使用者的存取權限、使用者可以看到經過Abe篩選的共用資料夾、因此無法顯示使用者無權存取的資料夾或其他共用資源。
`namespace-caching`	此內容指定連線至此共用區的SMB用戶端可快取CIFS伺服器傳回的目錄列舉結果、以提供更好的效能。根據預設、SMB 1用戶端不會快取目錄列舉結果。由於SMB 2和SMB 3用戶端預設會快取目錄列舉結果、因此指定此共用內容只能為SMB 1用戶端連線提供效能優勢。
`encrypt-data`	此內容指定存取此共用時必須使用SMB加密。存取SMB資料時不支援加密的SMB用戶端將無法存取此共用區。

新增或移除現有 **ONTAP SMB** 共用上的共用內容

您可以新增或移除共用內容、來自訂現有的SMB共用區。如果您想要變更共用組態以符合環境中不斷變化的需求、這項功能就很有用。

開始之前

您要修改其內容的共用區必須存在。

關於這項工作

新增共用內容的準則：

- 您可以使用以逗號分隔的清單來新增一或多個共用屬性。
- 您先前指定的任何共用內容都會維持有效。

  新增的內容會附加到現有的共用內容清單中。
- 如果您為已套用至共用區的共用屬性指定新值、則新指定的值會取代原始值。
- 您無法使用移除共用內容 `vserver cifs share properties add` 命令。

  您可以使用 `vserver cifs share properties remove` 移除共用內容的命令。

移除共用內容的準則：

- 您可以使用以逗號分隔的清單來移除一或多個共用屬性。
- 您先前已指定但未移除的任何共用內容都會維持有效。

步驟

1. 輸入適當的命令：

如果您想要...	輸入命令...
新增共用內容	`vserver cifs share properties add -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`
移除共用內容	`vserver cifs share properties remove -vserver _vserver_name_ -share-name _share_name_ -share-properties _properties_,...`

2. 確認共用內容設定： `vserver cifs share show -vserver vserver_name -share-name share_name`

範例

下列命令會新增 `showsnapshot` 在 SVM VS1 上、將屬性共用至名為「 shahre1 」的共享區：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties showsnapshot

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share1  /share1   oplocks      -          Everyone / Full
Control
                             browsable
                             changenotify
                             showsnapshot
```

下列命令會移除 `browsable` 在 SVM VS1 上共享名爲 "shahre2" 的共享區的屬性：

```
cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share2 -share-properties browsable

cluster1::> vserver cifs share show -vserver vs1
Vserver    Share   Path      Properties   Comment    ACL
---------  ------  --------  ----------   --------   -----------
vs1        share2  /share2   oplocks      -          Everyone / Full
Control
                             changenotify
```

相關資訊

管理共享的命令

當您以ONTAP UNIX有效的安全性從Sflexity命令列建立共用區到資料時、可以指定該共用區中SMB使用者所建立的所有檔案都屬於同一個群組（稱為_force-group）、該群組必須是UNIX群組資料庫中預先定義的群組。使用強制群組可讓屬於不同群組的SMB使用者更容易存取檔案。

只有當共用位於UNIX或混合qtree中時、才需要指定強制群組。不需要為NTFS磁碟區或qtree中的共用設定強制群組、因為這些共用中的檔案存取權是由Windows權限而非UNIX GID決定。

如果已為共用區指定強制群組、則下列項目將成為該共用區的真實情況：

- 存取此共用區的強制群組中的SMB使用者會暫時變更為強制群組的GID。

  此項GID可讓他們存取此共用區中的檔案、這些檔案無法以主要的GID或UID正常存取。

- 無論檔案擁有者的主要Gid為何、SMB使用者在此共用區中建立的所有檔案都屬於同一個強制群組。

當SMB使用者嘗試存取NFS所建立的檔案時、SMB使用者的主要GID會決定存取權限。

強制群組不會影響NFS使用者存取此共用區中檔案的方式。NFS所建立的檔案會從檔案擁有者處取得Gid。存取權限的判斷取決於嘗試存取檔案的NFS使用者的UID和主要GID。

使用強制群組可讓屬於不同群組的SMB使用者更容易存取檔案。例如、如果您想要建立共用區來儲存公司的網頁、並將寫入權限授予工程與行銷部門的使用者、您可以建立共用區、並授予名為「webGroup1」的群組寫入權限。由於使用強制群組、因此此共用區中SMB使用者所建立的所有檔案均歸「webgroup 1」群組所有。此外、使用者在存取共用時、也會自動指派「webgroup 1」群組的GID。因此、所有使用者都可以寫入此共用區、而不需要管理工程與行銷部門使用者的存取權限。

相關資訊

使用強制群組共享設定建立共享

如果您想讓SMB使用者存取具有UNIX檔案安全性的磁碟區或qtree上的資料、ONTAP 將其視為屬於同一個UNIX群組、您可以使用強制群組共用設定來建立SMB共用區。

步驟

1. 建立 SMB 共用區： `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path path -force-group-for-create` *`UNIX_group_name`*

   如果是 UNC 路徑 (`\\servername\sharename\filepath`）共享區中包含超過 256 個字元（不包括初始「`\\`」）、「 Windows 內容」方塊中的「 * 安全性 * 」標籤將無法使用。這是Windows用戶端問題、而非ONTAP 功能不均的問題。為避免此問題、請勿使用超過256個字元的UNC路徑建立共用。

   如果您想要在建立共用之後移除強制群組、可以隨時修改共用區、並指定空字串（ "" ）作為的值 `-force-group-for-create` 參數。如果您透過修改共用區來移除強制群組、則此共用區的所有現有連線仍會將先前設定的強制群組設為主要的Gid。

範例

下列命令會建立「網頁」共用、可在中的網路上存取 `/corp/companyinfo` SMB 使用者建立的所有檔案都指派給 webgroup1 群組的目錄：

```
vserver cifs share create -vserver vs1 -share-name webpages -path
/corp/companyinfo -force-group-for-create webgroup1
```

相關資訊

使用強制群組共享設定優化用戶訪問

使用 **MMC** 檢視 **ONTAP SMB** 共用的相關資訊

您可以檢視SVM上SMB共用的相關資訊、並使用Microsoft管理主控台（MMC）執行部分管理工作。您必須先將MMC連線至SVM、才能檢視共用區。

關於這項工作

您可以使用MMC在SVM內的共用上執行下列工作：

- 檢視共享區
- 檢視作用中工作階段
- 檢視開啟的檔案
- 列舉系統中的工作階段、檔案和樹狀結構連線清單
- 關閉系統中開啟的檔案
- 關閉開啟的工作階段
- 建立/管理共用

> ⓘ 上述功能所顯示的檢視是節點專屬的、而非叢集專屬的。因此、當您使用MMC連線至SMB伺服器主機名稱（即cifs01.domain.local）時、系統會根據您設定DNS的方式、將您路由至叢集內的單一LIF。

MMC ONTAP 不支援下列功能以利執行下列功能：

- 建立新的本機使用者/群組
- 管理/檢視現有的本機使用者/群組
- 檢視事件或效能記錄
- 儲存設備
- 服務與應用程式

在不支援該作業的情況下、您可能會遇到問題 `remote procedure call failed` 錯誤。

"常見問題集：搭配ONTAP 使用Windows MMC搭配使用"

步驟

1. 若要在任何Windows伺服器上開啟「電腦管理」MMC、請在*「控制台」中選取「系統管理工具」*「電腦管理」。
2. 選取*「行動*」>*「連線到另一台電腦*」。

「選取電腦」對話方塊隨即出現。

3. 鍵入儲存系統的名稱、或按一下*瀏覽*以找出儲存系統。
4. 按一下「確定」。

   MMC會連線至SVM。

5. 在導覽窗格中、按一下*「共享資料夾」>「共享資料夾」*。

   SVM上的共用清單會顯示在右顯示窗格中。

6. 若要顯示共用區的共用內容、請按兩下該共用區、以開啟「內容」對話方塊。
7. 如果無法使用MMC連線至儲存系統、您可以在儲存系統上使用下列其中一個命令、將使用者新增至BUILTIN\Administrators群組或BUILTIN\Power Users群組：

```
cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name BUILTIN\Administrators -member-names <domainuser>

cifs users-and-groups local-groups add-members -vserver <vserver_name>
-group-name "BUILTIN\Power Users" -member-names <domainuser>
```

用於管理 **SMB** 共用的 **ONTAP** 命令

您可以使用 `vserver cifs share` 和 `vserver cifs share properties` 管理 SMB 共用的命令。

如果您想要...	使用此命令...
建立SMB共用區	`vserver cifs share create`
顯示SMB共用區	`vserver cifs share show`
修改SMB共用區	`vserver cifs share modify`
刪除SMB共用區	`vserver cifs share delete`
新增共用內容至現有的共用區	`vserver cifs share properties add`
從現有共用區移除共用內容	`vserver cifs share properties remove`
顯示共用內容的相關資訊	`vserver cifs share properties show`

如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

使用SMB共用ACL來保護檔案存取安全

瞭解如何管理 ONTAP SMB 共用層級 ACL

您可以變更共用層級的ACL、讓使用者擁有更多或更少的共用存取權限。您可以使用Windows使用者和群組或UNIX使用者和群組來設定共用層級ACL。

根據預設，共用層級 ACL 可完全控制名為 Everyone 的標準群組。ACL 中的完全控制權表示網域和所有信任網域中的所有使用者都能完整存取共用區。您可以使用 Windows 用戶端上的 Microsoft 管理主控台 (MMC) 或 ONTAP 命令列來控制共用級 ACL 的存取等級。"建立共用存取控制列表"。

當您使用MMC時、適用下列準則：

- 指定的使用者和群組名稱必須是Windows名稱。
- 您只能指定Windows權限。

當您使用ONTAP flexfuse命令列時、適用下列準則：

- 指定的使用者和群組名稱可以是Windows名稱或UNIX名稱。

  如果在建立或修改ACL時未指定使用者和群組類型、則預設類型為Windows使用者和群組。

- 您只能指定Windows權限。

建立 ONTAP SMB 共用存取控制清單

建立SMB共用區的存取控制清單（ACL）來設定共用權限、可讓您控制使用者和群組對共用區的存取層級。

關於這項工作

您可以使用本機或網域Windows使用者或群組名稱、或UNIX使用者或群組名稱來設定共用層級ACL。

建立新 ACL 之前、您應該先刪除預設的共用 ACL `Everyone / Full Control`，這會帶來安全風險。

在工作群組模式中、本機網域名稱是SMB伺服器名稱。

步驟

1. 刪除預設的共用 ACL:`vserver CIFS 共用存取控制刪除 -vserver <vserver_name> -share <share_name> -user-or -group Everyone
2. 設定新ACL：

如果您想要使用...來設定ACL	輸入命令...
Windows使用者	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\user_name> -permission <access_right>`

如果您想要使用...來設定**ACL**	輸入命令...
Windows群組	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type windows -user-or-group <Windows_domain_name\group_name> -permission <access_right>`
UNIX使用者	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-user> -user-or-group <UNIX_user_name> -permission <access_right>`
UNIX群組	`vserver cifs share access-control create -vserver <vserver_name> -share <share_name> -user-group-type <unix-group> -user-or-group <UNIX_group_name> -permission <access_right>`

3. 使用驗證套用至共用的 ACL 是否正確 `vserver cifs share access-control show` 命令。

範例

下列命令提供 `Change` 在「vs1.example.com」「SVM：

```
cluster1::> vserver cifs share access-control create -vserver
vs1.example.com -share sales -user-or-group "DOMAIN\Sales Team"
-permission Change

cluster1::> vserver cifs share access-control show -vserver
vs1.example.com
                Share       User/Group              User/Group  Access
Vserver         Name        Name                    Type
Permission
--------------- ----------- --------------------    ---------
-----------
vs1.example.com  c$          BUILTIN\Administrators  windows
Full_Control
vs1.example.com  sales       DOMAIN\Sales Team     windows     Change
```

下列命令會授予 `Read`「工程」 UNIX 群組在「 vs2.example.com 」 SVM 上「 eng 」共用區的權限：

```
cluster1::> vserver cifs share access-control create -vserver
vs2.example.com -share eng -user-group-type unix-group -user-or-group
engineering -permission Read

cluster1::> vserver cifs share access-control show -vserver
vs2.example.com
                Share       User/Group               User/Group  Access
Vserver         Name        Name                     Type
Permission
--------------- ----------- -------------------      -----------
-----------
vs2.example.com  c$          BUILTIN\Administrators   windows
Full_Control
vs2.example.com  eng         engineering              unix-group  Read
```

下列命令會授予 `Change`本機 Windows 群組「 Tiger Team 」的權限、並授予 `Full_Control`本機 Windows 使用者「 Sue Chang 」在「 VS1 」 SVM 上的「 datavol5 」共用區的權限：

```
cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Tiger Team" -permission
Change

cluster1::> vserver cifs share access-control create -vserver vs1 -share
datavol5 -user-group-type windows -user-or-group "Sue Chang" -permission
Full_Control

cluster1::> vserver cifs share access-control show -vserver vs1
               Share       User/Group                  User/Group  Access
Vserver        Name        Name                        Type
Permission
-------------- ----------- --------------------------- -----------
-----------
vs1            c$          BUILTIN\Administrators      windows
Full_Control
vs1            datavol5    Tiger Team         windows     Change
vs1            datavol5    Sue Chang          windows     Full_Control
```

用於管理 **SMB** 共用存取控制清單的 **ONTAP** 命令

您需要知道管理SMB存取控制清單（ACL）的命令、包括建立、顯示、修改及刪除這些清單。

如果您想要...	使用此命令...
建立新的 ACL	`vserver cifs share access-control create`
顯示ACL	`vserver cifs share access-control show`
修改ACL	`vserver cifs share access-control modify`
刪除ACL	`vserver cifs share access-control delete`

使用檔案權限來保護檔案存取安全

使用 **ONTAP SMB SVM** 的 **Windows** 安全性標籤配置進階 **NTFS** 檔案權限

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、設定檔案和資料夾的標準NTFS檔案權限。

開始之前

執行此工作的系統管理員必須擁有足夠的NTFS權限、才能變更所選物件的權限。

關於這項工作

在Windows主機上設定NTFS檔案權限的方法是將項目新增至NTFS安全性描述元相關聯的NTFS判別存取控制清單（DACL）。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 完成*對應網路磁碟機*對話方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入CIFS伺服器名稱、其中包含您要套用權限的資料及共用名稱。

      如果您的 CIFS 伺服器名稱為「 CIFS 伺服器」、且您的共用名稱為「 shahre1 」、則應輸入 `\\CIFS_SERVER\share1`。

      您可以指定CIFS伺服器的資料介面IP位址、而非CIFS伺服器名稱。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要設定NTFS檔案權限的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
5. 選取*安全性*索引標籤。

「安全性」標籤會顯示已設定NTFS權限的使用者和群組清單。「權限」方塊會針對每個選取的使用者或群組、顯示有效的「允許」和「拒絕」權限清單。

6. 按一下*進階*。

   「Windows內容」視窗會顯示指派給使用者和群組之現有檔案權限的相關資訊。

7. 按一下*變更權限*。

   「權限」視窗隨即開啟。

8. 執行所需的動作：

如果您想要...	請執行下列動作...
設定新使用者或群組的進階NTFS權限	a. 按一下「 * 新增 * 」。 b. 在*輸入要選取的物件名稱*方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。
變更使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要變更其進階權限的使用者或群組。 b. 按一下 * 編輯 * 。
移除使用者或群組的進階NTFS權限	a. 在「權限項目：」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 跳至步驟13。

   如果您要在新使用者或群組上新增進階NTFS權限、或是變更現有使用者或群組的NTFS進階權限、就會開啟「<Object>的權限項目」方塊。

9. 在「套用至」方塊中、選取您要套用此NTFS檔案權限項目的方式。

   如果您要在單一檔案上設定NTFS檔案權限、則「套用至」方塊不會作用。「套用至」設定預設為*僅此物件*。

10. 在「權限」方塊中、針對您要在此物件上設定的進階權限、選取「允許」或「拒絕」方塊。

    - 若要允許指定的存取權、請選取*允許*方塊。
    - 若要不允許指定的存取、請選取* Deny（拒絕）*方塊。
      您可以設定下列進階權限的權限：
    - 完全控制

      如果您選擇此進階權限、則會自動選擇所有其他進階權限（允許或拒絕權限）。

    - 周遊資料夾/執行檔案

- 列出資料夾/讀取資料
- 讀取屬性
- 讀取延伸屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入延伸屬性
- 刪除子資料夾與檔案
- 刪除
- 讀取權限
- 變更權限
- 取得所有權

如果任何進階權限方塊無法選取、這是因為權限是從父物件繼承而來。

11. 如果您希望此物件的子資料夾和檔案繼承這些權限、請選取「僅將這些權限套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「確定」。
13. 完成新增、移除或編輯NTFS權限之後、請指定此物件的繼承設定：
    - 選取「包含此物件父項的可繼承權限」方塊。

      這是預設值。

    - 選取「使用此物件的可繼承權限來取代所有子物件權限」方塊。

      如果您要在單一檔案上設定NTFS檔案權限、則此設定不會出現在「權限」方塊中。

      選取此設定時請務必謹慎。此設定會移除所有子物件上的所有現有權限、並以此物件的權限設定取代這些權限。您可能不小心移除不想移除的權限。在混合式安全型磁碟區或qtree中設定權限時尤其重要。如果子物件具有UNIX有效的安全樣式、將NTFS權限傳播到這些子物件會ONTAP 導致將這些物件從UNIX安全樣式變更為NTFS安全樣式、而這些子物件上的所有UNIX權限都會以NTFS權限取代。

    - 選取兩個方塊。
    - 請選取兩個方塊。
14. 按一下「確定」以關閉「權限」方塊。
15. 按一下「確定」以關閉「進階安全性設定**<Object>**」方塊。

如需如何設定進階NTFS權限的詳細資訊、請參閱Windows文件。

相關資訊

- 在伺服器上建立 NTFS 安全描述符

- 顯示NTFS安全型磁碟區上的檔案安全資訊
- 顯示混合式安全型磁碟區的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

用於 **SMB NTFS** 檔案權限的 **ONTAP** 命令

您可以使用ONTAP CLI在檔案和目錄上設定NTFS檔案權限。這可讓您設定NTFS檔案權限、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以將項目新增至與NTFS安全性描述元相關聯的NTFS判別存取控制清單（DACL）、以設定NTFS檔案權限。然後將安全性描述元套用至NTFS檔案和目錄。

您只能使用命令列設定NTFS檔案權限。您無法使用CLI來設定NFSv4 ACL。

步驟

1. 建立NTFS安全性描述元。

   ```
   vserver security file-directory ntfs create -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -owner owner_name -group primary_group_name
   -control-flags-raw raw_control_flags
   ```

2. 將DACL新增至NTFS安全性描述元。

   ```
   vserver security file-directory ntfs dacl add -vserver svm_name -ntfs-sd
   ntfs_security_descriptor_name -access-type {deny|allow} -account account_name
   -rights {no-access|full-control|modify|read-and-execute|read|write} -apply-to
   {this-folder|sub-folders|files}
   ```

3. 建立檔案/目錄安全性原則。

   ```
   vserver security file-directory policy create -vserver svm_name -policy-name
   policy_name
   ```

了解透過 **ONTAP SMB** 伺服器存取檔案時提供存取控制的 **UNIX** 檔案權限

一個包含以下三種類型的安全型態之一：NTFS、UNIX或混合式。FlexVol無論安全風格為何、您都可以透過SMB存取資料、不過需要適當的UNIX檔案權限、才能以UNIX有效的安全性存取資料。

當透過SMB存取資料時、在判斷使用者是否有權執行要求的動作時、會使用數種存取控制：

- 匯出權限

  設定SMB存取的匯出權限為選用項目。

- 共用權限
- 檔案權限

  下列類型的檔案權限可能會套用至使用者想要執行動作的資料：

- NTFS
- UNIX NFSv4 ACL
- UNIX模式位元

對於已設定NFSv4 ACL或UNIX模式位元的資料、會使用UNIX樣式權限來決定資料的檔案存取權限。SVM管理員需要設定適當的檔案權限、以確保使用者擁有執行所需動作的權限。

混合式安全型磁碟區中的資料可能具有NTFS或UNIX有效的安全風格。如果資料具有UNIX有效的安全樣式、則在決定資料的檔案存取權限時、會使用NFSv4權限或UNIX模式位元。

使用動態存取控制（**DAC**）保護檔案存取

了解 **ONTAP SMB** 伺服器的 **DAC** 檔案存取安全性

您可以使用動態存取控制、並在Active Directory中建立集中存取原則、並透過套用的群組原則物件（GPO）將其套用至SVM上的檔案和資料夾、以確保存取安全。您可以將稽核設定為使用集中式存取原則暫存事件、以便在套用變更之前查看中央存取原則的影響。

CIFS認證新增功能

在動態存取控制之前、CIFS認證會包含安全主體（使用者）的身分識別和Windows群組成員資格。有了動態存取控制、憑證中還會新增三種類型的資訊：裝置身分識別、裝置宣告及使用者宣告：

- 裝置識別

  使用者身分識別資訊的類比、但使用者登入裝置的身分識別和群組成員資格除外。

- 裝置聲明

  關於裝置安全主體的說法。例如、裝置宣告可能是特定OU的成員。

- 使用者聲明

  關於使用者安全性主體的說法。例如、使用者聲稱其AD帳戶可能是特定OU的成員。

集中存取原則

檔案的集中存取原則可讓組織集中部署及管理授權原則、這些原則包括使用者群組、使用者宣告、裝置宣告及資源內容的條件式運算式。

例如、若要存取高商業影響資料、使用者必須是全職員工、而且只能從受管理裝置存取資料。集中存取原則是在Active Directory中定義、並透過GPO機制散佈到檔案伺服器。

使用進階稽核進行集中式存取原則登臺

中央存取原則可以是「年齡」、在這種情況下、會在檔案存取檢查期間以「假設」的方式進行評估。原則生效時會發生的結果、以及與目前設定的不同之處、會記錄為稽核事件。如此一來、系統管理員就能在實際執行原則之前、先使用稽核事件記錄來研究存取原則變更的影響。評估存取原則變更的影響之後、即可透過GPO將原則部署至所需的SVM。

相關資訊

- 了解受支援的 GPO
- 了解如何將群組原則物件套用至 SMB 伺服器
- 在伺服器上啟用或停用 GPO 支援
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊
- 配置中央存取策略以保護伺服器上的數據
- 顯示有關伺服器安全的信息
- "SMB與NFS稽核與安全性追蹤"

ONTAP SMB 伺服器支援的 **DAC** 功能

如果您想要在CIFS伺服器上使用動態存取控制（DAC）、您需要瞭解ONTAP 如何在Active Directory環境中支援動態存取控制功能。

支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、支援下列功能：ONTAP

功能	註解
宣告進入檔案系統	聲稱是簡單的名稱和值配對、說明使用者的一些真實情況。使用者認證包含宣告資訊、檔案上的安全性描述元可以執行包含宣告檢查的存取檢查。如此可讓系統管理員更精細地控制哪些人可以存取檔案。
檔案存取檢查的條件式運算式	修改檔案的安全性參數時、使用者可以將任意複雜的條件運算式新增至檔案的安全性描述元。條件運算式可以包含宣告檢查。
透過集中存取原則集中控制檔案存取	集中存取原則是一種儲存在Active Directory中的ACL、可標記為檔案。只有在磁碟上的安全性描述元和標記的集中存取原則都允許存取時、才會授予檔案存取權。這可讓系統管理員控制從中央位置（AD）存取檔案的權限、而不需要修改磁碟上的安全性描述元。
集中存取原則接移	藉由「老舊」變更中央存取原則、並在稽核報告中看到變更的影響、來增加在不影響實際檔案存取的情況下嘗試安全性變更的能力。
支援使用ONTAP CLI顯示有關中央存取原則安全性的資訊	延伸 `vserver security file-directory show` 顯示已套用集中存取原則的相關資訊。

功能	註解
包括集中存取原則的安全性追蹤	延伸 `vserver security trace` 命令系列可顯示包含已套用集中存取原則相關資訊的結果。

不支援動態存取控制

在CIFS伺服器上啟用動態存取控制時、不支援下列功能：ONTAP

功能	註解
NTFS檔案系統物件的自動分類	這是ONTAP Windows檔案分類基礎架構的副檔名、不受支援。
進階稽核、不包括集中存取原則接移	進階稽核僅支援集中存取原則移位。

了解如何將 **DAC** 和中央存取原則與 **ONTAP SMB** 伺服器結合使用

使用動態存取控制（DAC）和集中存取原則來保護CIFS伺服器上的檔案和資料夾安全時、必須謹記某些考量事項。

如果原則規則套用至網域\系統管理員使用者、則**NFS**存取權限可能會被拒絕

在某些情況下、如果將集中存取原則安全性套用至root使用者嘗試存取的資料、則可能會拒絕NFS存取root。當集中存取原則包含套用至網域\系統管理員的規則、且根帳戶對應至網域\系統管理員帳戶時、就會發生此問題。

您應該將規則套用至具有管理權限的群組、例如網域\系統管理員群組、而非套用規則至網域\系統管理員使用者。如此一來、您就可以將root對應到網域\系統管理員帳戶、而不受root影響。

在**Active Directory**中找不到所套用的集中存取原則時、**CIFS**伺服器的**BUILTIN\Administrator**群組可存取資源

CIFS伺服器中包含的資源可能會套用集中存取原則、但如果CIFS伺服器使用集中存取原則的SID嘗試從Active Directory擷取資訊、則該SID與Active Directory中任何現有的集中存取原則SID都不相符。在此情況下、CIFS伺服器會套用該資源的本機預設還原原則。

本機預設還原原則可讓CIFS伺服器的BUILTIN\Administrator群組存取該資源。

為 **ONTAP SMB** 伺服器啟用或停用 **DAC**

預設會停用可讓您使用動態存取控制（DAC）來保護CIFS伺服器上物件的選項。如果您想要在CIFS伺服器上使用動態存取控制、則必須啟用此選項。如果您稍後決定不想使用動態存取控制來保護儲存在CIFS伺服器上的物件、可以停用此選項。

您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定動態存取控制的資訊。

"Microsoft TechNet：動態存取控制案例總覽"

關於這項工作

啟用動態存取控制後、檔案系統就能包含具有動態存取控制相關項目的ACL。如果停用動態存取控制、則會忽略

目前的動態存取控制項目、不允許新的項目。

此選項僅適用於進階權限層級。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

| 如果您想要動態存取控制... | 輸入命令...

- 您必須對Active Directory網域控制器擁有足夠的存取權限、才能建立集中存取原則、以及建立GPO並套用至包含CIFS伺服器的容器。
- 您必須對儲存虛擬機器（SVM）擁有足夠的管理存取權限、才能執行必要的命令。

關於這項工作

集中存取原則會定義並套用至Active Directory上的群組原則物件（GPO）。您可以在 Microsoft TechNet Library 中找到有關如何在 Active Directory 上設定集中存取原則的資訊。

"Microsoft TechNet：集中存取原則案例"

步驟

1. 如果 SVM 尚未使用啟用動態存取控制、請在 SVM 上啟用動態存取控制 `vserver cifs options modify` 命令。

   ```
   vserver cifs options modify -vserver vs1 -is-dac-enabled true
   ```

2. 如果尚未使用啟用群組原則物件（ GPO ）、請在 CIFS 伺服器上啟用這些物件 `vserver cifs group-policy modify` 命令。

   ```
   vserver cifs group-policy modify -vserver vs1 -status enabled
   ```

3. 在Active Directory上建立集中存取規則和集中存取原則。
4. 建立群組原則物件（GPO）、在Active Directory上部署集中存取原則。
5. 將GPO套用至CIFS伺服器電腦帳戶所在的容器。
6. 使用手動更新套用至 CIFS 伺服器的 GPO `vserver cifs group-policy update` 命令。

   ```
   vserver cifs group-policy update -vserver vs1
   ```

7. 使用確認 GPO 中央存取原則已套用至 CIFS 伺服器上的資源 `vserver cifs group-policy show-applied` 命令。

   下列範例顯示預設網域原則有兩個套用至CIFS伺服器的集中存取原則：

   ```
   vserver cifs group-policy show-applied
   ```

   ```
   Vserver: vs1
   ----------------------------
       GPO Name: Default Domain Policy
          Level: Domain
         Status: enabled
     Advanced Audit Settings:
         Object Access:
             Central Access Policy Staging: failure
     Registry Settings:
         Refresh Time Interval: 22
         Refresh Random Offset: 8
         Hash Publication Mode for BranchCache: per-share
   ```

```
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
        Log Retention Method: overwrite-as-needed
        Max Log Size: 16384
    File Security:
        /vol1/home
        /vol1/dir1
    Kerberos:
        Max Clock Skew: 5
        Max Ticket Age: 10
        Max Renew Age:  7
    Privilege Rights:
        Take Ownership: usr1, usr2
        Security Privilege: usr1, usr2
        Change Notify: usr1, usr2
    Registry Values:
        Signing Required: false
    Restrict Anonymous:
        No enumeration of SAM accounts: true
        No enumeration of SAM accounts and shares: false
        Restrict anonymous access to shares and named pipes: true
        Combined restriction for anonymous user: no-access
    Restricted Groups:
        gpr1
        gpr2
Central Access Policy Settings:
    Policies: cap1
              cap2

  GPO Name: Resultant Set of Policy
     Level: RSOP
Advanced Audit Settings:
    Object Access:
        Central Access Policy Staging: failure
Registry Settings:
    Refresh Time Interval: 22
    Refresh Random Offset: 8
    Hash Publication Mode for BranchCache: per-share
    Hash Version Support for BranchCache: all-versions
Security Settings:
    Event Audit and Event Log:
        Audit Logon Events: none
        Audit Object Access: success
```

```
          Log Retention Method: overwrite-as-needed
          Max Log Size: 16384
      File Security:
          /vol1/home
          /vol1/dir1
      Kerberos:
          Max Clock Skew: 5
          Max Ticket Age: 10
          Max Renew Age:  7
      Privilege Rights:
          Take Ownership: usr1, usr2
          Security Privilege: usr1, usr2
          Change Notify: usr1, usr2
      Registry Values:
          Signing Required: false
      Restrict Anonymous:
          No enumeration of SAM accounts: true
          No enumeration of SAM accounts and shares: false
          Restrict anonymous access to shares and named pipes: true
          Combined restriction for anonymous user: no-access
      Restricted Groups:
          gpr1
          gpr2
  Central Access Policy Settings:
      Policies: cap1
                cap2
2 entries were displayed.
```

相關資訊

- 了解如何將群組原則物件套用至 SMB 伺服器
- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊
- 啟用或停用伺服器的 DAC

顯示有關 **ONTAP SMB** 伺服器的 **DAC** 安全性的信息

您可以顯示NTFS磁碟區上的動態存取控制（DAC）安全性資訊、以及在混合式安全型磁碟區上具有NTFS有效安全性的資料。這包括有關條件式ACE、資源ACE和集中存取原則ACE的資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及您要顯示其檔案或資料夾安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`
其中輸出會顯示群組和使用者的SID	`vserver security file-directory show -vserver vserver_name -path path -lookup-names false`
關於將十六進位位元遮罩轉譯為文字格式之檔案和目錄的檔案和目錄安全性	`vserver security file-directory show -vserver vserver_name -path path -textual-mask true`

範例

下列範例顯示有關路徑的動態存取控制安全性資訊 `/vol1` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /vol1
                           Vserver: vs1
                         File Path: /vol1
                File Inode Number: 112
                   Security Style: mixed
                  Effective Style: ntfs
                   DOS Attributes: 10
           DOS Attributes in Text: ----D---
           Expanded Dos Attribute: -
                     Unix User Id: 0
                    Unix Group Id: 1
                   Unix Mode Bits: 777
           Unix Mode Bits in Text: rwxrwxrwx
                             ACLs: NTFS Security Descriptor
                                   Control:0xbf14
                                   Owner:CIFS1\Administrator
                                   Group:CIFS1\Domain Admins
                                   SACL - ACEs
                                      ALL-Everyone-0xf01ff-OI|CI|SA|FA
                                      RESOURCE ATTRIBUTE-Everyone-0x0

("Department_MS",TS,0x10020,"Finance")
                                      POLICY ID-All resources - No Write-
0x0-OI|CI
                                   DACL - ACEs
                                      ALLOW-CIFS1\Administrator-0x1f01ff-
OI|CI
                                      ALLOW-Everyone-0x1f01ff-OI|CI
                                      ALLOW CALLBACK-DAC\user1-0x1200a9-
OI|CI

((@User.department==@Resource.Department_MS&&@Resource.Impact_MS>1000)&&@D
evice.department==@Resource.Department_MS)
```

相關資訊

- 顯示有關GPO組態的資訊
- 顯示有關集中存取原則的資訊
- 顯示有關集中存取原則規則的資訊

ONTAP SMB 伺服器上 **DAC** 的復原註意事項

您應該瞭解還原ONTAP 至不支援動態存取控制（DAC）的版本時會發生什麼事、以及還原之前和之後必須執行的動作。

如果您想要將叢集還原成ONTAP 不支援動態存取控制的版本、且已在一或多個儲存虛擬機器（SVM）上啟用動

態存取控制、則必須先執行下列動作、才能還原：

- 您必須停用叢集上所有已啟用動態存取控制的SVM。
- 您必須修改包含的叢集上的任何稽核組態 `cap-staging` 僅使用的事件類型 `file-op` 事件類型。

您必須瞭解動態存取控制ACE的檔案和資料夾、並採取行動：

- 如果叢集還原、則不會移除現有的動態存取控制ACE；不過、檔案存取檢查會忽略這些ACE。
- 由於還原後會忽略動態存取控制ACE、因此使用動態存取控制ACE的檔案存取權會有所變更。

  這可能會允許使用者存取先前無法存取的檔案、或無法存取先前可能存取的檔案。

- 您應該將非動態存取控制ACE套用至受影響的檔案、以還原其先前的安全層級。

  這可以在還原之前或還原完成後立即完成。

> 由於還原後會忽略動態存取控制ACE、因此在將非動態存取控制ACE套用至受影響的檔案時、不需要將其移除。不過、如果需要、您可以手動移除。

使用匯出原則保護 **SMB** 存取安全

了解如何將匯出策略與 **ONTAP SMB** 存取權結合使用

如果SMB伺服器上已啟用SMB存取的匯出原則、則會在控制SMB用戶端對SVM磁碟區的存取時使用匯出原則。若要存取資料、您可以建立允許SMB存取的匯出原則、然後將原則與包含SMB共用的磁碟區建立關聯。

匯出原則會套用一或多個規則、指定允許哪些用戶端存取資料、以及哪些驗證傳輸協定支援唯讀和讀寫存取。您可以設定匯出原則、允許透過SMB存取所有用戶端、用戶端子網路或特定用戶端、並在決定資料的唯讀和讀寫存取時、允許使用Kerberos驗證、NTLM驗證或Kerberos和NTLM驗證進行驗證。

在處理所有套用至匯出原則的匯出規則之後ONTAP 、即可判斷用戶端是否已獲授予存取權限、以及授予何種存取層級。匯出規則適用於用戶端機器、而非Windows使用者和群組。匯出規則不會取代Windows使用者和群組型驗證與授權。匯出規則除了提供共用和檔案存取權限之外、還提供另一層存取安全性。

您只需將一個匯出原則與每個磁碟區建立關聯、即可設定用戶端對磁碟區的存取。每個SVM可包含多個匯出原則。這可讓您針對具有多個磁碟區的SVM執行下列作業：

- 為SVM的每個Volume指派不同的匯出原則、以便個別用戶端存取控制到SVM中的每個Volume。
- 將相同的匯出原則指派給SVM的多個磁碟區、以獲得相同的用戶端存取控制權、而無需為每個磁碟區建立新的匯出原則。

每個SVM至少有一個稱為「預設」的匯出原則、不含任何規則。您無法刪除此匯出原則、但可以重新命名或修改它。SVM上的每個Volume預設都與預設匯出原則相關聯。如果在SVM上停用SMB存取的匯出原則、「預設」匯出原則對SMB存取沒有影響。

您可以設定規則來提供NFS和SMB主機的存取權、並將該規則與匯出原則建立關聯、然後再與包含NFS和SMB主機所需存取之資料的磁碟區建立關聯。或者、如果有些磁碟區只有SMB用戶端需要存取、您可以設定匯出原則、其中的規則僅允許使用SMB傳輸協定存取、而且只使用Kerberos或NTLM（或兩者）進行唯讀和寫入存取驗證。然後、匯出原則會與僅需要SMB存取的磁碟區建立關聯。

如果啟用SMB的匯出原則、且用戶端提出的存取要求不受適用的匯出原則允許、則要求會以拒絕權限的訊息失敗。如果用戶端不符合磁碟區匯出原則中的任何規則、則會拒絕存取。如果匯出原則是空的、則所有存取都會隱含拒絕。即使共用和檔案權限不允許存取、也會發生這種情況。這表示您必須將匯出原則設定為在包含SMB共用的磁碟區上、至少允許下列項目：

- 允許存取所有用戶端或適當的用戶端子集
- 允許透過SMB存取
- 使用Kerberos或NTLM驗證（或兩者）、允許適當的唯讀和寫入存取

深入瞭解 "設定及管理匯出原則"。

了解 **ONTAP SMB** 匯出規則

匯出規則是匯出原則的功能要素。匯出規則會根據您設定的特定參數、將用戶端存取要求與磁碟區相符、以決定如何處理用戶端存取要求。

匯出原則必須包含至少一個匯出規則、才能允許存取用戶端。如果匯出原則包含多個規則、則會依照規則在匯出原則中的顯示順序來處理這些規則。規則順序由規則索引編號決定。如果規則符合用戶端、則會使用該規則的權限、而且不會再處理其他規則。如果沒有符合的規則、用戶端就會被拒絕存取。

您可以使用下列準則來設定匯出規則、以決定用戶端存取權限：

- 傳送要求的用戶端所使用的檔案存取傳輸協定、例如NFSv4或SMB。
- 用戶端識別碼、例如主機名稱或IP位址。

  的最大大小 `-clientmatch` 欄位為 4096 個字元。

- 用戶端用來驗證的安全性類型、例如Kerberos v5, NTL,或AUTH_SYS。

如果規則指定多個準則、用戶端必須符合所有準則、才能套用規則。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv3傳輸協定傳送、用戶端的IP位址為10.1.17.37。

即使用戶端存取傳輸協定相符、用戶端的IP位址仍位於與匯出規則中指定的子網路不同的子網路中。因此、用戶端比對失敗、此規則不適用於此用戶端。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs`

- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule any`

用戶端存取要求是使用NFSv4傳輸協定傳送、用戶端的IP位址為10.1.16.54。

用戶端存取傳輸協定相符、用戶端的IP位址位於指定的子網路中。因此、用戶端配對成功、此規則適用於此用戶端。無論用戶端的安全類型為何、都能取得讀寫存取權。

範例

匯出原則包含具有下列參數的匯出規則：

- `-protocol nfs3`
- `-clientmatch 10.1.16.0/255.255.255.0`
- `-rorule any`
- `-rwrule krb5,ntlm`

用戶端#1的IP位址為10.1.16.207、使用NFSv3傳輸協定傳送存取要求、並使用Kerberos v5進行驗證。

用戶端#2的IP位址為10.1.16.211、使用NFSv3傳輸協定傳送存取要求、並透過AUTH_SYS進行驗證。

兩個用戶端的用戶端存取傳輸協定和IP位址都相符。唯讀參數允許所有用戶端的唯讀存取權、無論其驗證的安全類型為何。因此這兩個用戶端都能取得唯讀存取權。但是、只有用戶端#1會取得讀寫存取權、因為它使用核准的安全性類型Kerberos v5.x進行驗證。用戶端#2無法取得讀寫存取權。

限製或允許透過 **SMB** 進行存取的 **ONTAP** 導出策略規則範例

這些範例說明如何在啟用SMB存取匯出原則的SVM上、建立限制或允許存取SMB的匯出原則規則。

SMB存取的匯出原則預設為停用。只有在啟用SMB存取的匯出原則時、才需要設定限制或允許透過SMB存取的匯出原則規則。

僅適用於**SMB**存取的匯出規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：if1
- 索引編號：1.
- 用戶端比對：僅比對網路192.168.1.0/24上的用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：使用NTLM或Kerberos驗證的用戶端
- 讀寫存取：使用Kerberos驗證的用戶端

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifs1 -ruleindex 1 -protocol cifs -clientmatch 192.168.1.0/255.255.255.0
-rorule krb5,ntlm -rwrule krb5
```

SMB與NFS存取的匯出規則

下列命令會在SVM上建立具有下列組態的「」VS1「匯出規則：

- 原則名稱：ifsnfs1
- 索引編號： 2.
- 用戶端配對：符合所有用戶端
- 傳輸協定：SMB與NFS存取
- 唯讀存取：存取所有用戶端
- 讀寫存取：使用Kerberos（NFS和SMB）或NTLM驗證（SMB）的用戶端
- UNIX使用者ID 0對應（零）：對應至使用者ID 65534（通常對應至使用者名稱nobnobody）
- SUID和SGID存取：允許

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
cifsnfs1 -ruleindex 2 -protocol cifs,nfs -clientmatch 0.0.0.0/0 -rorule
any -rwrule krb5,ntlm -anon 65534 -allow-suid true
```

僅使用**NTLM**匯出**SMB**存取規則

下列命令會在名為「'VS1'」的SVM上建立具有下列組態的匯出規則：

- 原則名稱：ntlm1
- 索引編號：1.
- 用戶端配對：符合所有用戶端
- 傳輸協定：僅啟用SMB存取
- 唯讀存取：僅限使用NTLM的用戶端
- 讀寫存取：僅限使用NTLM的用戶端

如果您將唯讀選項或讀寫選項設定為僅限NTL-存取、則必須在用戶端比對選項中使用IP位址型項目。否則、您就會收到 `access denied` 錯誤。這是因為ONTAP 使用主機名稱檢查用戶端存取權限時、使用Kerberos服務主要名稱（SPN-）。NTLM驗證不支援SPN-Name。

```
cluster1::> vserver export-policy rule create -vserver vs1 -policyname
ntlm1 -ruleindex 1 -protocol cifs -clientmatch 0.0.0.0/0 -rorule ntlm
-rwrule ntlm
```

您可以在儲存虛擬機器（SVM）上啟用或停用SMB存取的匯出原則。您可以選擇使用匯出原則來控制SMB對資源的存取。

開始之前

以下是啟用SMB匯出原則的需求：

- 在您為該用戶端建立匯出規則之前，用戶端必須在 DNS 中有「 PTR 」記錄。
- 如果 SVM 提供對 NFS 用戶端的存取，而您要用於 NFS 存取的主機名稱與 CIFS 伺服器名稱不同，則需要額外的一組主機名稱「 A 」和「 PTR 」記錄。

關於這項工作

在SVM上設定新的CIFS伺服器時、預設會停用SMB存取的匯出原則。如果您想要根據驗證傳輸協定或用戶端IP位址或主機名稱來控制存取、可以啟用SMB存取的匯出原則。您可以隨時啟用或停用SMB存取的匯出原則。

> 在啟用 NFS 的 SVM 中啟用 CIFS/SMB 的匯出原則，可讓 Linux 用戶端使用 `showmount -e` SVM 上的命令，檢視所有 SMB 磁碟區的交會路徑及相關的匯出原則規則。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 啟用或停用匯出原則：
   - 啟用匯出原則： `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled true`
   - 停用匯出原則： `vserver cifs options modify -vserver vserver_name -is -exportpolicy-enabled false`
3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可讓您使用匯出原則來控制SMB用戶端對SVM VS1上資源的存取：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-exportpolicy
-enabled true

cluster1::*> set -privilege admin
```

使用儲存層級存取保護來保護檔案存取安全

除了使用原生檔案層級來保護存取安全、以及匯出及共用安全性、您也可以設定儲存層級的存取保護、ONTAP 這是由流通量層級的第三層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取套用到儲存物件的存取。

僅支援NTFS存取權限。為了對UNIX使用者執行安全性檢查、以存取已套用Storage Level Access Guard的磁碟區上的資料、UNIX使用者必須對應至擁有該磁碟區的SVM上的Windows使用者。ONTAP

儲存層級存取保護行為

- 儲存層級的存取保護適用於儲存物件中的所有檔案或目錄。

  由於某個Volume中的所有檔案或目錄都受限於儲存層級的存取保護設定、因此不需要透過傳播進行繼承。

- 您可以設定儲存層級的存取保護、使其僅套用至檔案、僅套用至目錄、或同時套用至磁碟區內的檔案和目錄。
  - 檔案與目錄安全性

    適用於儲存物件內的每個目錄和檔案。這是預設設定。

  - 檔案安全性

    適用於儲存物件內的每個檔案。套用此安全性不會影響目錄的存取或稽核。

  - 目錄安全性

    適用於儲存物件內的每個目錄。套用此安全性不會影響檔案的存取或稽核。

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

- 如果您從NFS或SMB用戶端檢視檔案或目錄的安全性設定、就不會看到儲存層級的存取保護安全性。

  它會套用至儲存物件層級、並儲存在用於判斷有效權限的中繼資料中。

- 即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的安全性。

  它的設計僅供儲存管理員修改。

- 您可以將儲存層級的存取保護套用至NTFS或混合式安全型態的磁碟區。
- 只要包含該磁碟區的SVM已設定CIFS伺服器、您就可以將儲存層級的存取保護套用至具有UNIX安全樣式的磁碟區。
- 當磁碟區掛載於磁碟區交會路徑下、且該路徑上有儲存層級存取保護、則不會將其傳播至其下掛載的磁碟區。
- 儲存層級的存取保護安全性描述元會透過SnapMirror資料複寫和SVM複寫來複寫。
- 病毒掃描程式有特殊的分配。

  即使儲存層級的存取保護拒絕存取物件、這些伺服器仍可享有特殊存取權限來篩選檔案和目錄。

- 如果因為儲存層級存取保護而拒絕存取、則不會傳送FPolicy通知。

存取檢查順序

檔案或目錄的存取權取決於匯出或共用權限、在磁碟區上設定的儲存層級存取保護權限、以及套用至檔案和/或目錄的原生檔案權限的組合效應。評估所有層級的安全性、以判斷檔案或目錄具有哪些有效權限。安全性存取檢查的執行順序如下：

1. SMB共用區或NFS匯出層級權限
2. 儲存層級存取保護
3. NTFS檔案/資料夾存取控制清單（ACL）、NFSv4 ACL或UNIX模式位元

使用儲存層級存取保護的使用案例

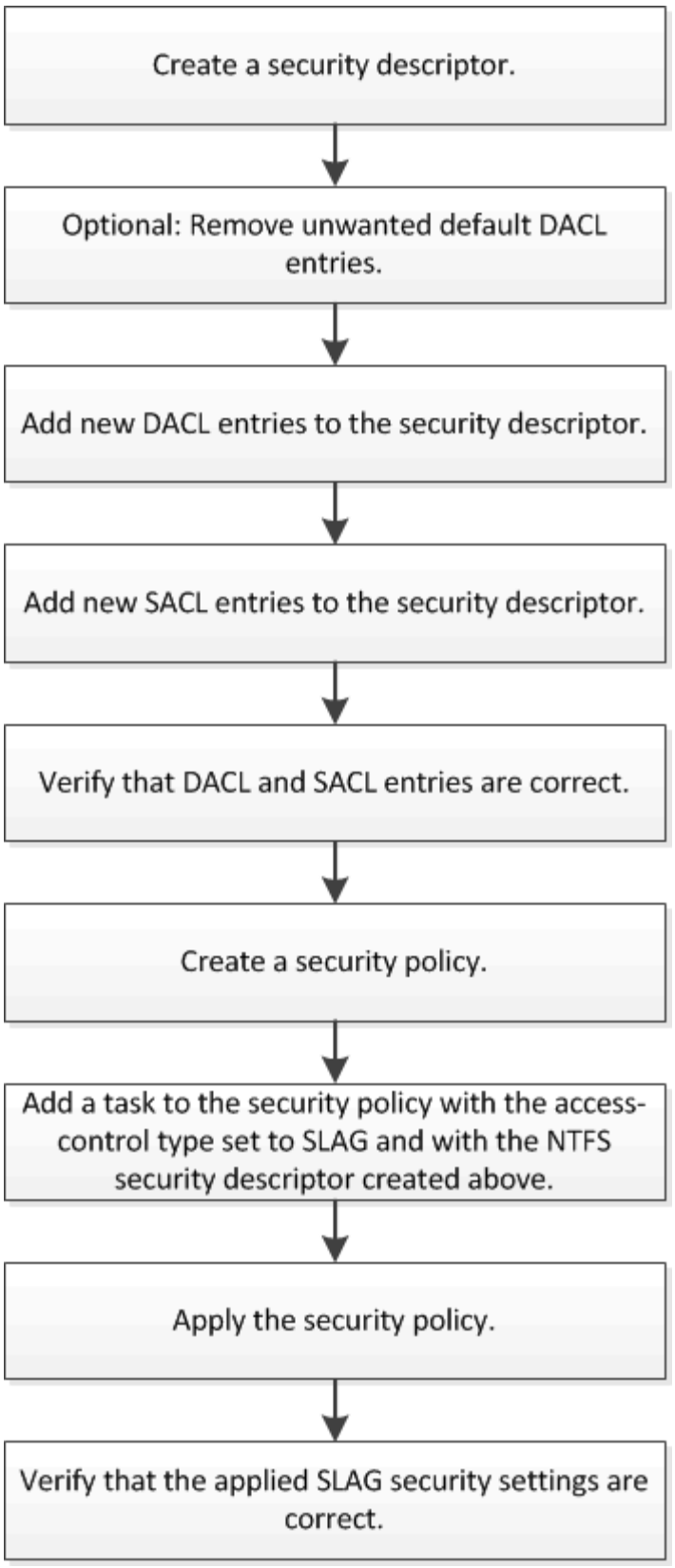
儲存層級的存取保護功能可在儲存層級提供額外的安全性、從用戶端看不到；因此、任何使用者或系統管理員都無法從其桌面撤銷。在某些使用案例中、在儲存層級控制存取的能力是有益的。

此功能的一般使用案例包括下列案例：

- 透過稽核及控制所有使用者在儲存層級的存取、來保護智慧財產
- 金融服務公司（包括銀行和交易集團）的儲存設備
- 為個別部門提供具有獨立檔案儲存設備的政府服務
- 大學保護所有學生檔案

ONTAP SMB 伺服器上儲存層級存取防護的設定工作流程

設定儲存層級存取保護（slag）的工作流程使用相同ONTAP 的CLI命令來設定NTFS檔案權限和稽核原則。您可以在指定的儲存虛擬機器（SVM）磁碟區上設定slag、而非在指定的目標上設定檔案和目錄存取。



相關資訊

在伺服器上配置儲存級別存取防護

在Volume或qtree上設定儲存層級存取保護時、您需要遵循許多步驟。儲存層級的存取保護可提供在儲存層級設定的存取安全性層級。它提供的安全性適用於從所有NAS傳輸協定到套用它的儲存物件的所有存取。

步驟

1. 使用建立安全性描述元 `vserver security file-directory ntfs create` 命令。

   `vserver security file-directory ntfs create -vserver vs1 -ntfs-sd sd1 vserver security file-directory ntfs show -vserver vs1`

```
Vserver: vs1

   NTFS Security    Owner Name
   Descriptor Name
   ------------     --------------
   sd1              -
```

   安全性描述元會以下列四個預設DACL存取控制項目（ACE）建立：

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    BUILTIN\Administrators
                     allow    full-control   this-folder, sub-folders,
files
    BUILTIN\Users    allow    full-control   this-folder, sub-folders,
files
    CREATOR OWNER    allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

   如果您不想在設定儲存層級存取保護時使用預設項目、可以在建立及新增自己的ACE至安全性描述元之前將其移除。

2. 從安全性描述元中移除任何您不想設定儲存層級存取保護安全性的預設DACL ACE：

   a. 使用移除任何不想要的 DACL ACE `vserver security file-directory ntfs dacl remove` 命令。

在此範例中、安全性描述元中會移除三個預設的DACL ACE：BUILTIN\Administrator、BUILTIN\Users和Creator Owners。

```
vserver security file-directory ntfs dacl remove -vserver vs1 -ntfs-sd sd1
-access-type allow -account builtin\users vserver security file-directory
ntfs dacl remove -vserver vs1 -ntfs-sd sd1 -access-type allow -account
builtin\administrators vserver security file-directory ntfs dacl remove
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "creator owner"
```

b. 請使用確認您不想用於儲存層級存取保護安全性的 DACL ACE 已從安全性描述元中移除 `vserver security file-directory ntfs dacl show` 命令。

在此範例中、命令的輸出會驗證安全性描述元中是否已移除三個預設的DACL ACE、只留下NT AUTORITY\SYSTEM預設的DACL ACE項目：

```
vserver security file-directory ntfs dacl show -vserver vs1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

3. 使用將一或多個 DACL 項目新增至安全性描述元 `vserver security file-directory ntfs dacl add` 命令。

在此範例中、安全性描述元中會新增兩個DACL ACE：

```
vserver security file-directory ntfs dacl add -vserver vs1 -ntfs-sd sd1
-access-type allow -account example\engineering -rights full-control -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs dacl add
-vserver vs1 -ntfs-sd sd1 -access-type allow -account "example\Domain Users"
-rights read -apply-to this-folder,sub-folders,files
```

4. 使用將一或多個 SACL 項目新增至安全性描述元 `vserver security file-directory ntfs sacl add` 命令。

在此範例中、兩個 SACL ACE 會新增至安全性描述元：

```
vserver security file-directory ntfs sacl add -vserver vs1 -ntfs-sd sd1
-access-type failure -account "example\Domain Users" -rights read -apply-to
this-folder,sub-folders,files vserver security file-directory ntfs sacl add
-vserver vs1 -ntfs-sd sd1 -access-type success -account example\engineering
-rights full-control -apply-to this-folder,sub-folders,files
```

5. 使用確認 DACL 和 SACL ACE 已正確設定 `vserver security file-directory ntfs dacl show`

和 `vserver security file-directory ntfs sacl show` 命令。

在此範例中、下列命令會顯示安全性描述元「'shd1」的DACL項目資訊：

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     allow    read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     allow    full-control   this-folder, sub-folders,
files
    NT AUTHORITY\SYSTEM
                     allow    full-control   this-folder, sub-folders,
files
```

在此範例中、下列命令會顯示安全性描述元「'shd1'」的SACL項目相關資訊：

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
```

```
Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access          Apply To
                     Type     Rights
    --------------   -------  -------         -----------
    EXAMPLE\Domain Users
                     failure  read           this-folder, sub-folders,
files
    EXAMPLE\engineering
                     success  full-control   this-folder, sub-folders,
files
```

6. 使用建立安全性原則 `vserver security file-directory policy create` 命令。

以下範例建立名為「policy1'」的原則：

```
vserver security file-directory policy create -vserver vs1 -policy-name
policy1
```

7. 使用確認原則已正確設定 `vserver security file-directory policy show` 命令。

   `vserver security file-directory policy show`

   ```
   Vserver          Policy Name
   ------------     --------------
   vs1              policy1
   ```

8. 使用將具有相關安全性描述元的工作新增至安全性原則 `vserver security file-directory policy task add` 命令 `-access-control` 參數設為 `slag`。

   即使原則可以包含多個儲存層級的存取保護工作、您也無法將原則設定為同時包含檔案目錄和儲存層級的存取保護工作。原則必須包含所有儲存層級的存取保護工作或所有檔案目錄工作。

   在此範例中、工作會新增至名為「policy1」的原則、該原則會指派給安全性描述元「shD1」。它會指派給 `/datavol1` 存取控制類型設為「 lag 」的路徑。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name
   policy1 -path /datavol1 -access-control slag -security-type ntfs -ntfs-mode
   propagate -ntfs-sd sd1
   ```

9. 使用確認工作已正確設定 `vserver security file-directory policy task show` 命令。

   ```
   vserver security file-directory policy task show -vserver vs1 -policy-name
   policy1
   ```

   ```
    Vserver: vs1
     Policy: policy1

      Index  File/Folder  Access           Security  NTFS       NTFS
   Security
             Path         Control          Type      Mode       Descriptor
   Name
      -----  -----------  ---------------  --------  ----------
   ---------------
      1      /datavol1    slag             ntfs      propagate  sd1
   ```

10. 使用套用儲存層級存取保護安全性原則 `vserver security file-directory apply` 命令。

    ```
    vserver security file-directory apply -vserver vs1 -policy-name policy1
    ```

    已排程要套用安全性原則的工作。

11. 使用驗證套用的儲存層級存取保護安全性設定是否正確 `vserver security file-directory show` 命令。

    在此範例中、命令的輸出顯示儲存層級存取保護安全性已套用至 NTFS 磁碟區 `/datavol1`。即使預設

的DACL允許「所有人」完全控制、儲存層級的存取保護安全性仍會限制（及稽核）存取儲存層級存取保護設定中定義的群組。

```
vserver security file-directory show -vserver vs1 -path /datavol1
```

```
                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

相關資訊

- 用於管理 NTFS 檔案安全、NTFS 審核原則和儲存層級存取防護的命令
- 伺服器上儲存層級存取防護的設定工作流程

- 顯示有關伺服器上儲存層級存取防護的信息
- 刪除伺服器上的儲存層級存取保護

ONTAP SMB 伺服器上的有效 **SLAG** 矩陣

您可以在磁碟區或qtree或兩者上設定slag。根據slog對照表、您可以定義哪些Volume或qtree是適用的slog組態、以符合表格中所列的各種情境。

	在美國的主動轉向系統中使用大量的	快照中的 **Volume slag**	在美國的美國美國美國戰地服務團（**AFF S**）中使用**qtree**	在快照中使用 **qtree slig**
存取檔案系統（AFs）中的Volume存取	是的	否	不適用	不適用
快照中的 Volume 存取	是的	否	不適用	不適用
在主動轉向服務器中存取qtree（當qtree中有slog時）	否	否	是的	否
在主動轉向服務器中存取qtree（當qtree中不存在slog時）	是的	否	否	否
在快照中存取 qtree（當 qtree AFS 中存在 slag 時）	否	否	是的	否
qtree 存取快照（當 qtree AFS 中不存在 slag 時）	是的	否	否	否

顯示有關 **ONTAP SMB** 伺服器上的儲存層級存取防護的信息

儲存層級的存取保護是套用在磁碟區或qtree上的第三層安全保護。無法使用Windows內容視窗檢視儲存層級的存取保護設定。您必須使用ONTAP VMware CLI來檢視儲存層級存取保護安全性的相關資訊、以便用來驗證組態或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其儲存層級存取保護安全性資訊的磁碟區或qtree路徑。您可以以摘要形式或詳細清單來顯示輸出。

步驟

1. 顯示儲存層級的存取保護安全設定、並提供所需的詳細資料：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

以下範例顯示 NTFS 安全性樣式磁碟區的儲存層級存取保護安全性資訊及路徑 `/datavol1` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

以下範例顯示儲存層級存取保護在路徑上的混合式安全樣式磁碟區相關資訊 `/datavol5` 在 SVM VS1 中。此磁碟區的最上層具有UNIX有效的安全性。Volume具有儲存層級的存取保護安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

刪除 **ONTAP SMB** 伺服器上的儲存層級存取保護

如果您不想再在儲存層級設定存取安全性、可以移除磁碟區或qtree上的儲存層級存取保護。移除儲存層級的存取保護不會修改或移除一般NTFS檔案和目錄安全性。

步驟

1. 使用確認磁碟區或 qtree 已設定儲存層級存取保護 `vserver security file-directory show` 命令。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI

                         Storage-Level Access Guard security
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

2. 使用移除儲存層級存取保護 `vserver security file-directory remove-slag` 命令。

   ```
   vserver security file-directory remove-slag -vserver vs1 -path /datavol2
   ```

3. 使用確認儲存層級存取保護已從 Volume 或 qtree 移除 `vserver security file-directory show` 命令。

   ```
   vserver security file-directory show -vserver vs1 -path /datavol2
   ```

```
                Vserver: vs1
              File Path: /datavol2
      File Inode Number: 99
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xbf14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\Domain Users-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\Domain Users-0x1301bf-OI|CI
```

使用SMB管理檔案存取

使用本機使用者和群組進行驗證和授權

如何使用本機使用者和群組ONTAP

了解本機 ONTAP SMB 使用者和群組

您應該先知道哪些是本機使用者和群組、以及這些使用者和群組的一些基本資訊、然後再決定是否要在環境中設定及使用本機使用者和群組。

- 本機使用者

  具有唯一安全性識別碼（SID）的使用者帳戶、只有在建立該帳戶的儲存虛擬機器（SVM）上才具有可見度。本機使用者帳戶具有一組屬性、包括使用者名稱和SID。本機使用者帳戶會使用NTLM驗證、在CIFS伺服器上進行本機驗證。

  使用者帳戶有多種用途：

  - 用於授予_使用者權限管理_權限給使用者。
  - 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機群組

具有唯一SID的群組只能在建立該群組的SVM上看到。群組包含一組成員。成員可以是本機使用者、網域使用者、網域群組和網域機器帳戶。可以建立、修改或刪除群組。

群組有多種用途：

- 用於授予_使用者權限管理_權限給其成員。
- 用於控制SVM擁有之檔案和資料夾資源的共用層級和檔案層級存取。

- 本機網域

  具有本機範圍的網域、受SVM限制。本機網域名稱為CIFS伺服器名稱。本機使用者和群組包含在本機網域內。

- 安全性識別碼（**SID**）

  SID是可識別Windows型安全性主體的可變長度數值。例如、一般的SID格式如下：s-1-5-21-3136354847-3130905135-2517279418-123456。

- * NTLM驗證*

  一種Microsoft Windows安全性方法、用於驗證CIFS伺服器上的使用者。

- 叢集複寫資料庫（**RDB**）

  叢集中每個節點上都有執行個體的複寫資料庫。本機使用者和群組物件會儲存在RDB中。

建立本機 **ONTAP SMB** 使用者和本機群組的原因

在您的儲存虛擬機器（SVM）上建立本機使用者和本機群組的理由有好幾種。例如、如果網域控制器（DC）無法使用、您可能想要使用本機群組來指派權限、或SMB伺服器位於工作群組中、您可以使用本機使用者帳戶來存取SMB伺服器。

您可以基於下列理由建立一或多個本機使用者帳戶：

- 您的SMB伺服器位於工作群組中、網域使用者無法使用。

  工作群組組組態需要本機使用者。

- 如果網域控制器無法使用、您希望能夠驗證並登入SMB伺服器。

  本機使用者可以在網域控制器當機或網路問題使SMB伺服器無法連絡網域控制器時、使用NTLM驗證來驗證SMB伺服器。

- 您想要指派_使用者權限管理_權限給本機使用者。

  _使用者權限管理_是SMB伺服器管理員控制使用者和群組在SVM上擁有哪些權限的能力。您可以將權限指派給使用者帳戶、或是將使用者設為具有這些權限的本機群組成員、藉此指派權限給使用者。

您可以基於下列理由建立一或多個本機群組：

- 您的SMB伺服器位於工作群組中、而且網域群組無法使用。

工作群組組組態不需要本機群組、但這些群組對於管理本機工作群組使用者的存取權限非常有用。

- 您想要使用本機群組來控制檔案和資料夾資源的存取、以進行共用和檔案存取控制。
- 您想要使用自訂的_使用者權限管理_權限來建立本機群組。

  某些內建使用者群組具有預先定義的權限。若要指派一組自訂的權限、您可以建立本機群組、並將必要的權限指派給該群組。然後您可以將本機使用者、網域使用者和網域群組新增至本機群組。

相關資訊

- 了解本地用戶身份驗證
- 支援的權限清單

了解本機 **ONTAP SMB** 使用者身份驗證

本機使用者必須先建立已驗證的工作階段、才能存取CIFS伺服器上的資料。

由於SMB是以工作階段為基礎、因此在第一次設定工作階段時、只要確定一次使用者身分即可。CIFS伺服器在驗證本機使用者時、會使用以NTLM為基礎的驗證。支援「位在位在位在位在位」的「位在位

在三種使用案例下使用本機驗證。ONTAP每個使用案例取決於使用者名稱的網域部分（使用網域\使用者格式）是否符合CIFS伺服器的本機網域名稱（CIFS伺服器名稱）：

- 網域部分相符

  在要求存取資料時提供本機使用者認證的使用者、會在CIFS伺服器本機驗證。

- 網域部分不符

  嘗試在CIFS伺服器所屬網域中的網域控制器上使用NTLM驗證。ONTAP如果驗證成功、登入即告完成。如果驗證失敗、接下來的情況取決於驗證失敗的原因。

  例如、如果使用者存在於Active Directory中、但密碼無效或過期、ONTAP 則無法嘗試在CIFS伺服器上使用對應的本機使用者帳戶。而是驗證失敗。有些情況ONTAP 下、即使有CIFS伺服器上的對應本機帳戶存在、也會使用該帳戶進行驗證、即使這些NetBios網域名稱不相符。例如、如果存在相符的網域帳戶、但該帳戶已停用、ONTAP 則會使用CIFS伺服器上對應的本機帳戶進行驗證。

- 未指定網域部分

  以本機使用者身分先嘗試驗證。ONTAP如果本機使用者驗證失敗、ONTAP 則由CIFS伺服器所屬網域中的網域控制器來驗證使用者。

成功完成本機或網域使用者驗證後ONTAP 、將會建構完整的使用者存取權杖、並將本機群組成員資格和權限納入考量。

如需本機使用者的NTLM驗證詳細資訊、請參閱Microsoft Windows文件。

相關資訊

在伺服器上啟用或停用本機使用者身份驗證

了解 **ONTAP SMB** 使用者存取權令牌

當使用者對應共用時、會建立已驗證的SMB工作階段、並建構使用者存取權杖、其中包含使用者、使用者群組成員資格和累積權限、以及對應的UNIX使用者的相關資訊。

除非停用此功能、否則本機使用者和群組資訊也會新增至使用者存取權杖。存取權杖的建構方式取決於登入是針對本機使用者還是Active Directory網域使用者：

- 本機使用者登入

  雖然本機使用者可以是不同本機群組的成員、但本機群組不能是其他本機群組的成員。本機使用者存取權杖是由指派給特定本機使用者所屬群組的所有權限聯合所組成。

- 網域使用者登入

  當網域使用者登入時ONTAP 、即可取得使用者存取權杖、其中包含使用者所屬之所有網域群組的使用者ID和SID。使用網域使用者存取權杖的聯合、搭配使用者網域群組的本機成員資格（若有）所提供的存取權杖、以及指派給網域使用者或其任何網域群組成員資格的任何直接權限。ONTAP

對於本機和網域使用者登入、也會針對使用者存取權杖設定主要群組RID。預設 RID 為 `Domain Users` （ RID 513 ）。您無法變更預設值。

Windows對UNIX和UNIX對Windows名稱對應程序、對本機和網域帳戶都遵循相同的規則。

> 從UNIX使用者到本機帳戶並無暗示的自動對應。如果需要、則必須使用現有的名稱對應命令來指定明確的對應規則。

了解如何在包含本機群組的 **ONTAP SMB SVM** 上使用 **SnapMirror**

在包含本機群組的SVM所擁有的磁碟區上設定SnapMirror時、您應該瞭解相關準則。

您無法使用應用到SnapMirror複寫到另一個SVM之檔案、目錄或共用的ACE中的本機群組。如果您使用SnapMirror功能在另一個SVM上建立磁碟區的DR鏡像、而該磁碟區有一個用於本機群組的ACE、則該ACE在鏡射上無效。如果將資料複寫到不同的SVM、資料就會有效地跨入不同的本機網域。授予本機使用者和群組的權限僅在最初建立的SVM範圍內有效。

了解刪除 **ONTAP SMB** 伺服器對使用者和群組的影響

預設的本機使用者和群組集是在建立CIFS伺服器時建立、並與託管CIFS伺服器的儲存虛擬機器（SVM）建立關聯。SVM管理員可以隨時建立本機使用者和群組。刪除CIFS伺服器時、您必須瞭解本機使用者和群組的情況。

本機使用者和群組與SVM相關聯、因此在刪除CIFS伺服器時、不會因為安全考量而刪除它們。雖然在刪除CIFS伺服器時不會刪除本機使用者和群組、但它們會隱藏起來。在SVM上重新建立CIFS伺服器之前、您無法檢視或管理本機使用者和群組。

> CIFS伺服器管理狀態不會影響本機使用者或群組的可見度。

了解如何將 **Microsoft** 管理主控台與本機 **ONTAP SMB** 使用者和群組結合使用

您可以從Microsoft管理主控台檢視本機使用者和群組的相關資訊。有了這個版本ONTAP的功能、您就無法從Microsoft管理主控台為本機使用者和群組執行其他管理工作。

了解如何恢復 **ONTAP SMB** 叢集

如果您計畫將叢集還原至ONTAP 不支援本機使用者和群組的支援版本、以及本機使用者和群組用於管理檔案存取或使用者權限、則必須注意某些考量。

- 基於安全考量、當ONTAP 將設定的本機使用者、群組和權限資訊還原至不支援本機使用者和群組功能的版本時、不會刪除這些資訊。
- 還原至ONTAP 舊版的主要版本時ONTAP 、在驗證和認證建立期間、不使用本地使用者和群組。
- 本機使用者和群組不會從檔案和資料夾ACL中移除。
- 由於授予本機使用者或群組權限、因此會拒絕視存取權限而定的檔案存取要求。

  若要允許存取、您必須重新設定檔案權限、以根據網域物件而非本機使用者和群組物件來允許存取。

什麼是本機權限

受支援的 **ONTAP SMB** 權限列表

支援的權限已預先定義。ONTAP某些預先定義的本機群組預設會新增其中一些權限。您也可以從預先定義的群組新增或移除權限、或建立新的本機使用者或群組、並新增權限至您所建立的群組、或新增至現有的網域使用者和群組。

下表列出儲存虛擬機器（SVM）上支援的權限、並提供具有指派權限的BUILTIN群組清單：

權限名稱	預設安全性設定	說明
`SeTcbPrivilege`	無	做為作業系統的一部分
`SeBackupPrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	備份檔案和目錄、覆寫任何ACL
`SeRestorePrivilege`	`BUILTIN\Administrators`、`BUILTIN\Backup Operators`	還原檔案和目錄、覆寫任何ACL、將任何有效的使用者或群組SID設為檔案擁有者
`SeTakeOwnershipPrivilege`	`BUILTIN\Administrators`	取得檔案或其他物件的擁有權
`SeSecurityPrivilege`	`BUILTIN\Administrators`	管理稽核 這包括檢視、卸載及清除安全性記錄。

權限名稱	預設安全性設定	說明
SeChangeNotifyPrivilege	BUILTIN\Administrators、BUILTIN\Backup Operators、BUILTIN\Power Users、BUILTIN\Users、Everyone	略過周遊檢查 具有此權限的使用者不需要具有周遊（x）權限、即可周遊資料夾、符號連結或交叉路口。

相關資訊

- 了解如何分配權限
- 了解如何配置繞過遍歷檢查

了解如何指派 **ONTAP SMB** 權限

您可以直接將權限指派給本機使用者或網域使用者。或者、您也可以將使用者指派給本機群組、其指派的權限與您希望這些使用者擁有的功能相符。

- 您可以將一組權限指派給所建立的群組。

  接著、您可以將擁有該使用者所擁有權限的使用者新增至群組。

- 您也可以將本機使用者和網域使用者指派給預先定義的群組、這些群組的預設權限與您要授予這些使用者的權限相符。

相關資訊

- 新增權限給本機或網域使用者或群組
- 移除本機或網域使用者或群組的權限
- 重設本機或網域使用者和群組的權限
- 了解如何配置繞過遍歷檢查

了解 **ONTAP SMB** 伺服器上的 **BUILTIN** 群組和本機管理員帳戶

當您使用BUILTIN群組和本機系統管理員帳戶時、請謹記以下幾項準則。例如、您可以重新命名本機系統管理員帳戶、但無法刪除此帳戶。

- 系統管理員帳戶可以重新命名、但無法刪除。
- 系統管理員帳戶無法從BUILTIN\Administrator群組中移除。
- 可以重新命名內建群組、但無法刪除。

  在重新命名BUILTIN群組之後、可以使用已知名稱建立另一個本機物件、但會指派新的RID給該物件。

- 沒有本機來賓帳戶。

相關資訊

預先定義的BUILTIN群組和預設權限

本地 **ONTAP SMB** 使用者密碼要求

根據預設、本機使用者密碼必須符合複雜度要求。密碼複雜度需求與Microsoft Windows本地安全策略_中定義的要求類似。

密碼必須符合下列條件：

- 長度必須至少六個字元
- 不得包含使用者帳戶名稱
- 必須包含下列四種類別中至少三種的字元：
  - 英文大寫字元（A到Z）
  - 英文小寫字元（a到z）
  - 基礎10位數（0到9）
  - 特殊字元：

```
~ ! @ # $ % {caret} & * _ - + = ` \ | ( ) [ ] : ; " ' < > , . ? /
```

相關資訊

- 設定本地用戶的密碼複雜度
- 顯示有關伺服器安全設定的信息
- 變更本機使用者帳戶密碼

預先定義的 **BUILTIN** 群組和預設 **ONTAP SMB** 權限

您可以將本機使用者或網域使用者的成員資格指派給ONTAP 由供應的一組預先定義的BUILTIN群組。預先定義的群組已指派預先定義的權限。

下表說明預先定義的群組：

預先定義的**BUILTIN**群組	預設權限
`BUILTIN\Administrators`RID 544 第一次建立時、即為本機 `Administrator` 帳戶（ RID 為 500 ）會自動成為此群組的成員。當儲存虛擬機器（ SVM ）加入網域時 `domain\Domain Admins` 群組即會新增至群組。如果 SVM 離開網域、則為 `domain\Domain Admins` 群組即會從群組中移除。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeSecurityPrivilege` • `SeTakeOwnershipPrivilege` • `SeChangeNotifyPrivilege`

預先定義的**BUILTIN**群組	預設權限
`BUILTIN\Power Users`RID 547 第一次建立時、此群組沒有任何成員。此群組成員具有下列特性： • 可建立及管理本機使用者和群組。 • 無法將自己或任何其他物件新增至 `BUILTIN\Administrators` 群組：	`SeChangeNotifyPrivilege`
`BUILTIN\Backup Operators`RID 551. 第一次建立時、此群組沒有任何成員。如果是以備份目的開啟檔案或資料夾、則此群組的成員可以覆寫其讀取和寫入權限。	• `SeBackupPrivilege` • `SeRestorePrivilege` • `SeChangeNotifyPrivilege`
`BUILTIN\Users`RID 545 第一次建立時、此群組沒有任何成員（隱含的除外）`Authenticated Users` 特殊群組）。當 SVM 加入網域時 `domain\Domain Users` 群組隨即新增至此群組。如果 SVM 離開網域、則為 `domain\Domain Users` 群組已從此群組中移除。	`SeChangeNotifyPrivilege`
`Everyone`SID S-1-1-0 此群組包括所有使用者、包括來賓（但非匿名使用者）。這是暗示的群組、具有暗示的成員資格。	`SeChangeNotifyPrivilege`

相關資訊

- 了解伺服器上的 BUILTIN 群組和本機管理員帳戶
- 支援的權限清單
- 了解如何配置繞過遍歷檢查

啟用或停用本機使用者和群組功能

了解本機 **ONTAP SMB** 使用者和群組功能

您必須先啟用本機使用者和群組功能、才能使用本機使用者和群組來存取NTFS安全型資料。此外、如果您想要使用本機使用者進行SMB驗證、則必須啟用本機使用者驗證功能。

預設會啟用本機使用者和群組功能和本機使用者驗證。如果未啟用這些功能、您必須先啟用這些功能、才能設定及使用本機使用者和群組。您可以隨時停用本機使用者和群組功能。

除了明確停用本機使用者和群組功能之外、ONTAP 如果叢集中的任何節點還原ONTAP 為不支援此功能的版本、則無法使用本地使用者和群組功能。本機使用者和群組功能只有在叢集中的所有節點都執行ONTAP 支援的版本支援之前、才會啟用。

相關資訊

- 修改本機使用者帳戶
- 修改本機群組
- 新增權限給本機或網域使用者或群組

在 ONTAP SMB 伺服器上啟用或停用本機使用者和群組

您可以在儲存虛擬機器（SVM）上啟用或停用本機使用者和群組進行SMB存取。預設會啟用本機使用者和群組功能。

關於這項工作

您可以在設定SMB共用區和NTFS檔案權限時使用本機使用者和群組、也可以在建立SMB連線時選用本機使用者進行驗證。若要使用本機使用者進行驗證、您也必須啟用本機使用者和群組驗證選項。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您希望本機使用者和群組...	輸入命令...
已啟用	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -is-local-users-and -groups-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者和群組功能：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-users-and
-groups-enabled true

cluster1::*> set -privilege admin
```

相關資訊

- 在伺服器上啟用或停用本機使用者身份驗證
- 啟用或停用本機使用者帳戶

在 **ONTAP SMB** 伺服器上啟用或停用本機使用者身份驗證

您可以在儲存虛擬機器（SVM）上啟用或停用SMB存取的本機使用者驗證。預設為允許本機使用者驗證、這在SVM無法連絡網域控制器或您選擇不使用網域層級存取控制時非常有用。

開始之前

必須在CIFS伺服器上啟用本機使用者和群組功能。

關於這項工作

您可以隨時啟用或停用本機使用者驗證。如果您想要在建立SMB連線時使用本機使用者進行驗證、也必須啟用CIFS伺服器的本機使用者和群組選項。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您希望本機驗證...	輸入命令...
已啟用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled true`
已停用	`vserver cifs options modify -vserver` *`vserver_name`* `-is-local-auth-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用本機使用者驗證：

```
cluster1::>set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -is-local-auth
-enabled true

cluster1::*> set -privilege admin
```

相關資訊

- 了解本地用戶身份驗證
- 啟用或停用伺服器上的本機使用者和群組

管理本機使用者帳戶

修改本機 **ONTAP SMB** 使用者帳戶

如果您想要變更現有使用者的完整名稱或說明、以及要啟用或停用使用者帳戶、您可以修改本機使用者帳戶。如果使用者名稱遭入侵、或是為了管理目的而需要變更名稱、您也可以重新命名本機使用者帳戶。

如果您想要...	輸入命令...
修改本機使用者的全名	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-full-name text` 如果全名包含空格、則必須以雙引號括住。
修改本機使用者的說明	`vserver cifs users-and-groups local-user modify -vserver` *`vserver_name`* `-user-name` *`user_name`* `-description text` 如果描述包含空格、則必須以雙引號括住。
啟用或停用本機使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver` *vserver_name* -user-name *user_name* -is-account-disabled {true
false}`	重新命名本機使用者帳戶

範例

下列範例將儲存虛擬機器（SVM、先前稱為Vserver）VS1上的本機使用者「'CIFs_Server\sue」重新命名為「'CIFS伺服器\ sue新'」：

```
cluster1::> vserver cifs users-and-groups local-user rename -user-name
CIFS_SERVER\sue -new-user-name CIFS_SERVER\sue_new -vserver vs1
```

啟用或停用本機 **ONTAP SMB** 使用者帳戶

如果您希望使用者能夠透過SMB連線存取儲存虛擬機器（SVM）中所含的資料、請啟用本機使用者帳戶。如果您不想讓本機使用者帳戶透過SMB存取SVM資料、也可以停用該使用者帳戶。

關於這項工作

您可以修改使用者帳戶來啟用本機使用者。

步驟

1. 執行適當的行動：

如果您想要...	輸入命令...
啟用使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled false`
停用使用者帳戶	`vserver cifs users-and-groups local-user modify -vserver vserver_name -user-name user_name -is-account -disabled true`

變更本機 **ONTAP SMB** 使用者帳戶密碼

您可以變更本機使用者的帳戶密碼。如果使用者的密碼遭入侵或使用者忘記密碼、這項功能就很有用。

步驟

1. 請執行適當的動作來變更密碼： `vserver cifs users-and-groups local-user set-password -vserver vserver_name -user-name user_name`

範例

下列範例設定與儲存虛擬機器（SVM、先前稱為Vserver）VS1相關之本機使用者「'CIFS/Server\sue」的密碼：

```
cluster1::> vserver cifs users-and-groups local-user set-password -user
-name CIFS_SERVER\sue -vserver vs1

Enter the new password:
Confirm the new password:
```

相關資訊

設定本地用戶的密碼複雜度

顯示有關伺服器安全設定的信息

顯示有關 **ONTAP SMB** 本地用戶的信息

您可以在摘要表單中顯示所有本機使用者的清單。如果您想要判斷特定使用者的帳戶設定、可以顯示該使用者的詳細帳戶資訊、以及多位使用者的帳戶資訊。此資訊可協助您判斷是否需要修改使用者的設定、以及疑難排解驗證或檔案存取問題。

關於這項工作

永遠不會顯示使用者密碼的相關資訊。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
顯示儲存虛擬機器（SVM）上所有使用者的相關資訊	`vserver cifs users-and-groups local-user show -vserver vserver_name`
顯示使用者的詳細帳戶資訊	`vserver cifs users-and-groups local-user show -instance -vserver vserver_name -user-name user_name`

您可以在執行命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

範例

下列範例顯示SVM VS1上所有本機使用者的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name     Description
-------- ---------------------------- ------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith   Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones
```

顯示有關本機使用者的 **ONTAP SMB** 群組成員身分的信息

您可以顯示本機使用者所屬的本機群組資訊。您可以使用此資訊來判斷使用者對檔案和資料夾的存取權限。此資訊有助於判斷使用者對檔案和資料夾的存取權限、或是疑難排解檔案存取問題。

關於這項工作

您可以自訂命令、僅顯示您要查看的資訊。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
顯示指定本機使用者的本機使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -user-name user_name`
顯示本機使用者所屬本機群組的本機使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -membership group_name`

如果您想要...	輸入命令...
顯示與指定儲存虛擬機器（SVM）相關聯之本機使用者的使用者成員資格資訊	`vserver cifs users-and-groups local-user show-membership -vserver` *vserver_name*
顯示指定SVM上所有本機使用者的詳細資訊	`vserver cifs users-and-groups local-user show-membership -instance -vserver` *vserver_name*

範例

以下範例顯示SVM VS1上所有本機使用者的成員資格資訊；使用者「CIFS伺服器管理員」是「BUILTIN\Administrators」群組的成員、而「CIFS伺服器\ sue」是「CIFS伺服器\ g1`」群組的成員：

```
cluster1::> vserver cifs users-and-groups local-user show-membership
-vserver vs1
Vserver    User Name                     Membership
---------- ----------------------------- ------------------------
vs1        CIFS_SERVER\Administrator     BUILTIN\Administrators
           CIFS_SERVER\sue               CIFS_SERVER\g1
```

刪除本機 **ONTAP SMB** 使用者帳戶

如果不再需要本機SMB驗證CIFS伺服器、或決定SVM所含資料的存取權限、您可以從儲存虛擬機器（SVM）刪除本機使用者帳戶。

關於這項工作

刪除本機使用者時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此使用者之檔案和目錄上的Windows安全性描述元。

- 所有對本機使用者的參照都會從成員資格和權限資料庫中移除。
- 標準且知名的使用者（例如Administrator）無法刪除。

步驟

1. 決定您要刪除的本機使用者帳戶名稱： `vserver cifs users-and-groups local-user show -vserver` *vserver_name*
2. 刪除本機使用者： `vserver cifs users-and-groups local-user delete -vserver` *vserver_name* `-user-name` *username_name*
3. 確認已刪除使用者帳戶： `vserver cifs users-and-groups local-user show -vserver` *vserver_name*

範例

下列範例會刪除與SVM VS1相關聯的本機使用者「'CIFS/Server\sue」：

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver  User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
vs1      CIFS_SERVER\sue              Sue   Jones


cluster1::> vserver cifs users-and-groups local-user delete -vserver vs1
-user-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups local-user show -vserver vs1
Vserver      User Name                    Full Name      Description
-------- ---------------------------- -------------- -------------
vs1      CIFS_SERVER\Administrator    James Smith    Built-in administrator
account
```

管理本機群組

修改本地 **ONTAP SMB** 群組

您可以變更現有本機群組的說明、或重新命名群組、以修改現有的本機群組。

如果您想要...	使用命令...
修改本機群組說明	`vserver cifs users-and-groups local-group modify -vserver` *vserver_name* `-group-name` *group_name* `-description text` 如果描述包含空格、則必須以雙引號括住。
重新命名本機群組	`vserver cifs users-and-groups local-group rename -vserver` *vserver_name* `-group-name` *group_name* `-new-group-name` *new_group_name*

範例

下列範例將本機群組「'CIFs_Server\Engineering」重新命名為「'CIFs_Server\Engineering _new'」：

```
cluster1::> vserver cifs users-and-groups local-group rename -vserver vs1
-group-name CIFS_SERVER\engineering -new-group-name
CIFS_SERVER\engineering_new
```

下列範例修改本機群組「'CIFs_Server\Engineering」的說明：

```
cluster1::> vserver cifs users-and-groups local-group modify -vserver vs1
-group-name CIFS_SERVER\engineering -description "New Description"
```

顯示有關 **ONTAP SMB** 本機群組的信息

您可以顯示在叢集或指定儲存虛擬機器（SVM）上設定的所有本機群組清單。此資訊在疑難排解SVM上所含資料的檔案存取問題或SVM上的使用者權限（權限）問題時非常實用。

步驟

1. 執行下列其中一項動作：

如果您想要有關...的資訊	輸入命令...
叢集上的所有本機群組	`vserver cifs users-and-groups local-group show`
SVM上的所有本機群組	`vserver cifs users-and-groups local-group show -vserver` *`vserver_name`*

您可以在執行此命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs`資訊，請參閱。

範例

下列範例顯示SVM VS1上所有本機群組的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver  Group Name                  Description
-------- --------------------------- ----------------------------
vs1      BUILTIN\Administrators      Built-in Administrators group
vs1      BUILTIN\Backup Operators    Backup Operators group
vs1      BUILTIN\Power Users         Restricted administrative privileges
vs1      BUILTIN\Users               All users
vs1      CIFS_SERVER\engineering
vs1      CIFS_SERVER\sales
```

管理本機 **ONTAP SMB** 群組成員資格

您可以新增及移除本機或網域使用者、或新增及移除網域群組、來管理本機群組成員資格。如果您想要根據群組中的存取控制來控制資料存取、或是想要使用者擁有與該群組相關的權限、這很有用。

關於這項工作

新增成員至本機群組的準則：

- 您無法將使用者新增至特殊的_Everyon__群組。

- 您必須先存在本機群組、才能將使用者新增至該群組。
- 使用者必須存在、才能將使用者新增至本機群組。
- 您無法將本機群組新增至其他本機群組。
- 若要將網域使用者或群組新增至本機群組、Data ONTAP 則必須能夠將名稱解析為SID。

從本機群組移除成員的準則：

- 您無法從特殊的_Everyon__群組中移除成員。
- 您要從中移除成員的群組必須存在。
- 必須能夠將您要從群組移除的成員名稱解析為對應的SID。ONTAP

步驟

1. 新增或移除群組中的成員。

如果您想要...	然後使用命令...
新增成員至群組	`vserver cifs users-and-groups local-group add-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要新增至指定本機群組的本機使用者、網域使用者或網域群組的以逗號分隔的清單。
從群組中移除成員	`vserver cifs users-and-groups local-group remove-members -vserver _vserver_name_ -group-name _group_name_ -member-names name[,...]` 您可以指定要從指定本機群組中移除的本機使用者、網域使用者或網域群組的以逗號分隔的清單。

以下範例將本機使用者「'Smb_server\sue」和網域群組「'AD_DOM\DOM_DOM_eng'」新增至SVM VS1上的本機群組「'Smb_server\engin'」：

```
cluster1::> vserver cifs users-and-groups local-group add-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,AD_DOMAIN\dom_eng
```

以下範例將SVM VS1上本機群組「'Smb_server\sue」和「'smb_server\james'」中的本機使用者移除：

```
cluster1::> vserver cifs users-and-groups local-group remove-members
-vserver vs1 -group-name SMB_SERVER\engineering -member-names
SMB_SERVER\sue,SMB_SERVER\james
```

相關資訊

顯示本機群組成員的相關資訊

顯示有關本機群組成員的 **ONTAP SMB** 信息

您可以顯示叢集或指定儲存虛擬機器（SVM）上所設定之本機群組的所有成員清單。在疑難排解檔案存取問題或使用者權限（權限）問題時、此資訊很有用。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入命令...
叢集上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members`
SVM上所有本機群組的成員	`vserver cifs users-and-groups local-group show-members -vserver` *`vserver_name`*

範例

下列範例顯示SVM VS1上所有本機群組成員的相關資訊：

```
cluster1::> vserver cifs users-and-groups local-group show-members
-vserver vs1
Vserver   Group Name                    Members
--------- ---------------------------- ------------------------
vs1       BUILTIN\Administrators       CIFS_SERVER\Administrator
                                       AD_DOMAIN\Domain Admins
                                       AD_DOMAIN\dom_grp1
          BUILTIN\Users                AD_DOMAIN\Domain Users
                                       AD_DOMAIN\dom_usr1
          CIFS_SERVER\engineering      CIFS_SERVER\james
```

刪除本機 **ONTAP SMB** 群組

如果不再需要本機群組來判斷與該SVM相關之資料的存取權限、或不再需要將SVM使用者權限（權限）指派給群組成員、您可以從儲存虛擬機器（SVM）中刪除該群組。

關於這項工作

刪除本機群組時、請謹記下列事項：

- 檔案系統不會變更。

  不會調整參照此群組之檔案和目錄上的Windows安全性描述元。

- 如果群組不存在、則會傳回錯誤。

- 無法刪除特殊的_Everyon__群組。
- 無法刪除內建群組、例如_BUILTIN\Administrators__BUILTIN\Users_。

步驟

1. 在 SVM 上顯示本機群組清單、藉此判斷您要刪除的本機群組名稱：`vserver cifs users-and-groups local-group show -vserver vserver_name`
2. 刪除本機群組：`vserver cifs users-and-groups local-group delete -vserver` *`vserver_name`* `-group-name` *`group_name`*
3. 確認群組已刪除：`vserver cifs users-and-groups local-user show -vserver` *`vserver_name`*

範例

下列範例會刪除與SVM VS1相關聯的本機群組「'CIFs_Server\sales'」：

```
cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- --------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
vs1       CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group delete -vserver vs1
-group-name CIFS_SERVER\sales

cluster1::> vserver cifs users-and-groups local-group show -vserver vs1
Vserver   Group Name                    Description
--------- --------------------------- ----------------------------
vs1       BUILTIN\Administrators       Built-in Administrators group
vs1       BUILTIN\Backup Operators     Backup Operators group
vs1       BUILTIN\Power Users          Restricted administrative
privileges
vs1       BUILTIN\Users                All users
vs1       CIFS_SERVER\engineering
```

更新本機資料庫中的 **ONTAP SMB** 網域使用者和群組名稱

您可以將網域使用者和群組新增至CIFS伺服器的本機群組。這些網域物件會在叢集的本機資料庫中登錄。如果重新命名網域物件、則必須手動更新本機資料庫。

關於這項工作

您必須指定要更新網域名稱的儲存虛擬機器（SVM）名稱。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行適當的行動：

如果您想要更新網域使用者和群組、以及...	使用此命令...
顯示已成功更新且無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver` *vserver_name*
顯示成功更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver` *vserver_name* `-display -failed-only false`
僅顯示無法更新的網域使用者和群組	`vserver cifs users-and-groups update-names -vserver` *vserver_name* `-display -failed-only true`
隱藏更新的所有狀態資訊	`vserver cifs users-and-groups update-names -vserver` *vserver_name* `-suppress -all-output true`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例會更新與儲存虛擬機器（SVM、先前稱為Vserver）VS1相關聯的網域使用者和群組名稱。對於上一次更新、需要更新的是一條相依的名稱鏈：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs users-and-groups update-names -vserver vs1

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-12345
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654322-23456
   Domain:            EXAMPLE2
   Out-of-date Name:  dom_user1
   Updated Name:      dom_user2
   Status:            Successfully updated

   Vserver:           vs1
   SID:               S-1-5-21-123456789-234565432-987654321-123456
   Domain:            EXAMPLE1
   Out-of-date Name:  dom_user3
   Updated Name:      dom_user4
   Status:            Successfully updated; also updated SID "S-1-5-21-
123456789-234565432-987654321-123457"
                      to name "dom_user5"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123458"
                      to name "dom_user6"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123459"
                      to name "dom_user7"; also updated SID "S-1-5-21-
123456789-234565432-987654321-123460"
                      to name "dom_user8"

The command completed successfully. 7 Active Directory objects have been
updated.

cluster1::*> set -privilege admin
```

管理本機權限

向 ONTAP SMB 本機或網域使用者或群組新增權限

您可以新增權限來管理本機或網域使用者或群組的使用者權限。新增的權限會覆寫指派給任何這些物件的預設權限。這可讓您自訂使用者或群組擁有的權限、進而增強安全性。

開始之前

要新增權限的本機或網域使用者或群組必須已經存在。

關於這項工作

新增權限至物件會覆寫該使用者或群組的預設權限。新增權限並不會移除先前新增的權限。

新增權限給本機或網域使用者或群組時、必須謹記下列事項：

- 您可以新增一或多個權限。
- 將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增一或多個權限至本機或網域使用者或群組： `vserver cifs users-and-groups privilege add-privilege -vserver _vserver_name_ -user-or-group-name name -privileges _privilege_[,...]`
2. 確認所需權限已套用至物件： `vserver cifs users-and-groups privilege show -vserver _vserver_name_ -user-or-group-name _name_`

範例

以下範例將「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限新增至儲存虛擬機器（SVM、先前稱為Vserver）VS1上的使用者「'CIFs_Server\sue'」：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege
```

刪除 ONTAP SMB 本機或網域使用者或群組的權限

您可以移除權限、來管理本機或網域使用者或群組的使用者權限。這可讓您自訂使用者和群組擁有的最大權限、進而增強安全性。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

在移除本機或網域使用者或群組的權限時、您必須謹記下列事項：

- 您可以移除一或多個權限。
- 當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。

  如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 移除本機或網域使用者或群組的一或多個權限： `vserver cifs users-and-groups privilege remove-privilege -vserver _vserver_name_ -user-or-group-name _name_ -privileges _privilege_[,...]`
2. 確認已從物件中移除所需的權限： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列範例移除儲存虛擬機器（SVM、前身為Vserver）VS1上使用者「'CIFs_Server\sue」的「'eTcbprivre'」和「'eTakeOwnershipprivatef'」權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue       SeTcbPrivilege
                                SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue -privileges
SeTcbPrivilege,SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- -------------------- -------------------
vs1       CIFS_SERVER\sue       -
```

重設 **ONTAP SMB** 本機或網域使用者和群組的權限

您可以重設本機或網域使用者和群組的權限。當您已修改本機或網域使用者或群組的權限、而且不再需要或需要這些修改時、此功能就很有用。

關於這項工作

重設本機或網域使用者或群組的權限、會移除該物件的任何權限項目。

步驟

1. 重設本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege reset-privilege -vserver vserver_name -user-or-group-name name`

2. 確認物件上的權限已重設： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列範例會重設儲存虛擬機器（SVM、先前稱為Vserver）VS1上使用者「'CIFs_Server\sue」的權限。根據預設、一般使用者沒有與其帳戶相關的權限：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name    Privileges
--------- -------------------- ---------------
vs1       CIFS_SERVER\sue      SeTcbPrivilege
                               SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name CIFS_SERVER\sue

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

下列範例會重設群組「'BUILTIN\管理員'」的權限、有效移除權限項目：

```
cluster1::> vserver cifs users-and-groups privilege show
Vserver   User or Group Name       Privileges
--------- ----------------------- -------------------
vs1       BUILTIN\Administrators   SeRestorePrivilege
                                   SeSecurityPrivilege
                                   SeTakeOwnershipPrivilege

cluster1::> vserver cifs users-and-groups privilege reset-privilege
-vserver vs1 -user-or-group-name BUILTIN\Administrators

cluster1::> vserver cifs users-and-groups privilege show
This table is currently empty.
```

顯示有關 **ONTAP SMB** 權限覆蓋的信息

您可以顯示指派給網域或本機使用者帳戶或群組的自訂權限相關資訊。此資訊可協助您判斷是否套用所需的使用者權限。

步驟

1. 執行下列其中一項動作：

如果您想要顯示有關...的資訊	輸入此命令...
儲存虛擬機器（SVM）上所有網域和本機使用者和群組的自訂權限	`vserver cifs users-and-groups privilege show -vserver vserver_name`
自訂SVM上特定網域或本機使用者和群組的權限	`vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

您可以在執行此命令時選擇其他選用參數。如"指令參考資料ONTAP"需詳細 `vserver cifs users-and-groups privilege show`資訊，請參閱。

範例

下列命令會顯示明確與SVM VS1的本機或網域使用者和群組相關聯的所有權限：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver    User or Group Name     Privileges
---------- ---------------------  ---------------
vs1        BUILTIN\Administrators  SeTakeOwnershipPrivilege
                                   SeRestorePrivilege
vs1        CIFS_SERVER\sue         SeTcbPrivilege
                                   SeTakeOwnershipPrivilege
```

設定略過周遊檢查

了解如何設定 **ONTAP SMB** 繞過遍歷檢查

「略過周遊檢查」是一項使用者權限（也稱為_priv榮幸_）、可決定使用者是否可以周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限。您應該瞭解允許或禁止略過周遊檢查時會發生什麼情況、以及如何為儲存虛擬機器（SVM）上的使用者設定略過周遊檢查。

允許或禁止略過周遊檢查時會發生什麼事

- 如果允許、當使用者嘗試存取檔案時ONTAP 、當決定是否授予或拒絕存取檔案時、不會檢查中繼目錄的周遊權限。
- 如果不允許、ONTAP 則此功能會檢查檔案路徑中所有目錄的周遊（執行）權限。

  如果任何中繼目錄沒有「'X'」（周遊權限）、ONTAP 則無法存取檔案。

設定略過周遊檢查

您可以使用ONTAP CLI或使用此使用者權限設定Active Directory群組原則、來設定略過周遊檢查。

。 `SeChangeNotifyPrivilege` 權限可控制是否允許使用者略過周遊檢查。

- 將它新增至SVM上的本機SMB使用者或群組、或新增至網域使用者或群組、可進行略過周遊檢查。
- 從SVM上的本機SMB使用者或群組或網域使用者或群組中移除此功能、將不允許略過周遊檢查。

根據預設、SVM上的下列BUILTIN群組有權略過周遊檢查：

- `BUILTIN\Administrators`
- `BUILTIN\Power Users`
- `BUILTIN\Backup Operators`
- `BUILTIN\Users`
- `Everyone`

如果您不想讓其中一個群組的成員略過周遊檢查、則必須從群組中移除此權限。

使用CLI在SVM上設定本機SMB使用者和群組的略過周遊檢查時、必須謹記下列事項：

- 如果您想要允許自訂本機或網域群組的成員略過周遊檢查，則必須新增 `SeChangeNotifyPrivilege` 權限給該群組。
- 如果您想要允許個別本機或網域使用者略過周遊檢查，而該使用者不是具有該權限的群組成員，則可以新增 `SeChangeNotifyPrivilege` 該使用者帳戶的權限。
- 您可以移除來停用本機或網域使用者或群組的略過周遊檢查 `SeChangeNotifyPrivilege` 隨時享有特權。

> 若要停用特定本機或網域使用者或群組的略過傳輸檢查、您也必須移除 `SeChangeNotifyPrivilege` 的權限 `Everyone` 群組：

相關資訊

- 允許使用者或群組略過目錄周遊檢查
- 不允許使用者或群組繞過目錄周遊檢查
- 配置卷上的檔案名稱轉換的字元映射
- 建立共用存取控制列表
- 使用儲存層級存取保護來保護檔案存取安全
- 支援的權限清單
- 新增權限給本機或網域使用者或群組

允許使用者或群組繞過 **ONTAP SMB** 目錄遍歷檢查

如果您希望使用者能夠周遊檔案路徑中的所有目錄、即使使用者對周遊目錄沒有權限、您也可以新增 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。根據預設、使用者可以略過目錄周遊檢查。

開始之前

- SVM上必須有SMB伺服器。
- 必須啟用本機使用者和群組SMB伺服器選項。

- 本機或網域使用者或群組 `SeChangeNotifyPrivilege` 新增權限必須已存在。

關於這項工作

將權限新增至網域使用者或群組時ONTAP 、可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增以啟用略過周遊檢查 `SeChangeNotifyPrivilege` 本機或網域使用者或群組的權限： `vserver cifs users-and-groups privilege add-privilege -vserver vserver_name -user-or -group-name name -privileges SeChangeNotifyPrivilege`

   的值 `-user-or-group-name` 參數是本機使用者或群組、或是網域使用者或群組。

2. 確認指定的使用者或群組已啟用略過周遊檢查： `vserver cifs users-and-groups privilege show -vserver vserver_name -user-or-group-name name`

範例

下列命令可讓屬於 “example\eng” 群組的使用者透過新增來略過目錄周遊檢查 `SeChangeNotifyPrivilege` 群組的權限：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\eng -privileges SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ---------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege
```

相關資訊

不允許使用者或群組繞過目錄周遊檢查

禁止使用者或群組繞過 **ONTAP SMB** 目錄遍歷檢查

如果您不希望使用者周遊檔案路徑中的所有目錄、因為使用者對周遊目錄沒有權限、您可以移除 `SeChangeNotifyPrivilege` 本機 SMB 使用者或儲存虛擬機器上群組的權限（ SVM ）。

開始之前

將從中移除權限的本機或網域使用者或群組必須已經存在。

關於這項工作

當移除網域使用者或群組的權限時、ONTAP 可能會聯絡網域控制器來驗證網域使用者或群組。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 不允許略過周遊檢查： `vserver cifs users-and-groups privilege remove-privilege -vserver vserver_name -user-or-group-name name -privileges`

SeChangeNotifyPrivilege

命令會移除 SeChangeNotifyPrivilege 本機或網域使用者或群組的權限、您可以使用的值來指定 -user-or-group-name *name* 參數。

2. 確認指定的使用者或群組已停用略過周遊檢查： vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *name*

範例

下列命令會禁止屬於「'example\eng'」群組的使用者略過目錄周遊檢查：

```
cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege remove-privilege
-vserver vs1 -user-or-group-name EXAMPLE\eng -privileges
SeChangeNotifyPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name    Privileges
--------- --------------------- ----------------------
vs1       EXAMPLE\eng           -
```

相關資訊

允許使用者或群組略過目錄周遊檢查

顯示檔案安全性和稽核原則的相關資訊

了解如何查看 **ONTAP SMB** 檔案安全和稽核策略

您可以在儲存虛擬機器（SVM）上的磁碟區內、顯示有關檔案與目錄安全性的資訊。您可以顯示FlexVol 有關在功能區上稽核原則的資訊。如果已設定、您可以在FlexVol 下列項目上顯示儲存層級存取保護和動態存取控制安全性設定的相關資訊：

顯示檔案安全性的相關資訊

您可以使用FlexVol 下列安全性樣式、顯示套用至Volume和qtree（適用於哪些人）中所含資料的檔案安全性相關資訊：

- NTFS
- UNIX
- 混合

顯示稽核原則的相關資訊

您可以透過FlexVol 下列NAS傳輸協定、顯示稽核原則的相關資訊、以稽核在支援功能上執行的存取事件：

- SMB（所有版本）
- NFSv4.x

顯示儲存層級存取保護（**slag**）安全性的相關資訊

儲存層級的存取保護安全功能可套用FlexVol 至下列安全樣式的物件：

- NTFS
- 混合
- UNIX（如果CIFS伺服器是在包含該磁碟區的SVM上設定）

顯示動態存取控制（**DAC**）安全性的相關資訊

動態存取控制安全功能FlexVol 可套用至包含下列安全樣式的物件：

- NTFS
- 混合（如果物件具有NTFS有效安全性）

相關資訊

- 了解如何使用儲存級別存取防護來保護文件存取
- 顯示有關伺服器上儲存層級存取防護的信息

顯示有關 **NTFS** 安全模式磁碟區上的 **ONTAP SMB** 檔案安全性的信息

您可以在NTFS安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及DOS屬性的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及您要顯示其檔案或資料夾安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

- 由於NTFS安全型磁碟區和qtree在決定檔案存取權限時僅使用NTFS檔案權限、而Windows使用者和群組、因此UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。
- 將顯示具有NTFS安全性的檔案和資料夾的ACL輸出。
- 由於儲存層級的存取保護安全性可在磁碟區根目錄或qtree上設定、因此設定儲存層級存取保護的磁碟區或qtree路徑輸出可能會同時顯示一般檔案ACL和儲存層級的存取保護ACL。
- 如果已針對指定的檔案或目錄路徑設定動態存取控制、則輸出也會顯示動態存取控制ACE的相關資訊。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示有關路徑的安全性資訊 `/vol4` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path /vol4

                                Vserver: vs1
                              File Path: /vol4
                      File Inode Number: 64
                         Security Style: ntfs
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                          ALLOW-Everyone-0x1f01ff
                                          ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下範例顯示有關路徑的安全性資訊、並提供有關路徑的擴充遮罩 `/data/engineering` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path -path
/data/engineering -expand-mask true

                Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
```

```
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
Generic Read
                             .0.. .... .... .... .... .... .... .... =
Generic Write
                             ..0. .... .... .... .... .... .... .... =
Generic Execute
                             ...0 .... .... .... .... .... .... .... =
Generic All
```

```
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...0 .... .... .... .... .... =
Synchronize
                              .... .... .... 0... .... .... .... .... =
Write Owner
```

```
                            .... .... .... .0.. .... .... .... .... =
Write DAC
                            .... .... .... ..0. .... .... .... .... =
Read Control
                            .... .... .... ...0 .... .... .... .... =
Delete
                            .... .... .... .... .... ...0 .... .... =
Write Attributes
                            .... .... .... .... .... .... 0... .... =
Read Attributes
                            .... .... .... .... .... .... .0.. .... =
Delete Child
                            .... .... .... .... .... .... ..0. .... =
Execute
                            .... .... .... .... .... .... ...0 .... =
Write EA
                            .... .... .... .... .... .... .... 0... =
Read EA
                            .... .... .... .... .... .... .... .0.. =
Append
                            .... .... .... .... .... .... .... ..0. =
Write
                            .... .... .... .... .... .... .... ...0 =
Read
```

以下範例顯示具有路徑之磁碟區的安全性資訊、包括儲存層級 Access Guard 安全性資訊 `/datavol1` 在 SVM VS1 中：

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
      File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                           ALLOW-Everyone-0x10000000-OI|CI|IO


                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

相關資訊

- 顯示混合式安全型磁碟區的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

您可以在混合式安全型磁碟區上顯示檔案與目錄安全性的相關資訊、包括安全型態與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及您要顯示其檔案或資料夾安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

- 混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和資料夾、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。
- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。
- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示UNIX檔案權限和儲存層級存取保護ACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則當動態存取控制是針對指定的檔案或目錄路徑設定時、輸出也會顯示動態存取控制ACE的相關資訊。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示有關路徑的安全性資訊 `/projects` 在 SVM VS1 中以擴充遮罩形式呈現。這種混合式安全型路徑具有UNIX有效的安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/projects -expand-mask true

                Vserver: vs1
              File Path: /projects
      File Inode Number: 78
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
           Unix User Id: 0
          Unix Group Id: 1
         Unix Mode Bits: 700
 Unix Mode Bits in Text: rwx------
                   ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/data` 在 SVM VS1 中。這種混合式安全型路徑具有NTFS有效安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path /data

                                Vserver: vs1
                              File Path: /data
                      File Inode Number: 544
                         Security Style: mixed
                        Effective Style: ntfs
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 0
                         Unix Mode Bits: 777
                  Unix Mode Bits in Text: rwxrwxrwx
                                    ACLs: NTFS Security Descriptor
                                          Control:0x8004
                                          Owner:BUILTIN\Administrators
                                          Group:BUILTIN\Administrators
                                          DACL - ACEs
                                            ALLOW-Everyone-0x1f01ff
                                            ALLOW-Everyone-0x10000000-
OI|CI|IO
```

以下範例顯示路徑中有關 Volume 的安全性資訊 `/datavol5` 在 SVM VS1 中。這種混合式安全型磁碟區的最上層具有UNIX有效的安全性。Volume具有儲存層級的存取保護安全性。

```
cluster1::> vserver security file-directory show -vserver vs1 -path
/datavol5
                Vserver: vs1
              File Path: /datavol5
      File Inode Number: 3374
         Security Style: mixed
        Effective Style: unix
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 755
 Unix Mode Bits in Text: rwxr-xr-x
                   ACLs: Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                           AUDIT-EXAMPLE\market-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-BUILTIN\Administrators-0x1f01ff
                           ALLOW-CREATOR OWNER-0x1f01ff
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-EXAMPLE\market-0x1f01ff
```

相關資訊

- 顯示NTFS安全型磁碟區上的檔案安全資訊
- 顯示UNIX安全型磁碟區上的檔案安全資訊

顯示有關 **UNIX** 安全模式磁碟區上的 **ONTAP SMB** 檔案安全性的信息

您可以顯示UNIX安全型磁碟區上的檔案與目錄安全性相關資訊、包括安全性樣式與有效的安全性樣式、套用的權限、以及UNIX擁有者與群組的相關資訊。您可以使用結果來驗證安全性組態、或疑難排解檔案存取問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及您要顯示其檔案或目錄安全性資訊的資料路徑。您可以以摘要形式或詳細清單來顯示輸出。

- UNIX安全型磁碟區和qtree在決定檔案存取權限時、只會使用UNIX檔案權限（模式位元或NFSv4 ACL）。
- ACL輸出只會針對具有NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和目錄、如果只套用模式位元權限（無NFSv4 ACL）、則此欄位為空白。

- 如果使用NFSv4安全性描述元、則不會套用ACL輸出中的擁有者和群組輸出欄位。

  它們只對NTFS安全描述元有意義。

- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`*
更詳細的資料	`vserver security file-directory show -vserver` *`vserver_name`* `-path` *`path`* `-expand-mask true`

範例

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: -
                           Unix User Id: 0
                          Unix Group Id: 1
                          Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

下列範例顯示有關路徑的安全性資訊 `/home` 在 SVM VS1 的擴充遮罩形式中：

```
cluster1::> vserver security file-directory show -vserver vs1 -path /home
-expand-mask true

                                Vserver: vs1
                              File Path: /home
                      File Inode Number: 9590
                         Security Style: unix
                        Effective Style: unix
                         DOS Attributes: 10
                 DOS Attributes in Text: ----D---
               Expanded Dos Attributes: 0x10
                    ...0 .... .... .... = Offline
                    .... ..0. .... .... = Sparse
                    .... .... 0... .... = Normal
                    .... .... ..0. .... = Archive
                    .... .... ...1 .... = Directory
                    .... .... .... .0.. = System
                    .... .... .... ..0. = Hidden
                    .... .... .... ...0 = Read Only
                          Unix User Id: 0
                         Unix Group Id: 1
                         Unix Mode Bits: 700
                 Unix Mode Bits in Text: rwx------
                                   ACLs: -
```

相關資訊

- 顯示有關安全類型捲上的文件安全性的信息
- 顯示混合式安全型磁碟區的檔案安全資訊

ONTAP 指令用於顯示有關 **SMB FlexVol** 磁碟區上的 **NTFS** 稽核策略的信息

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（如果已針對指定的檔案或目錄路徑設定動態存取控制）。
- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

  NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
詳細清單	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示路徑的稽核原則資訊 `/corp` 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 `/datavol1` 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

ONTAP 指令用於顯示有關 **SMB FlexVol** 磁碟區上的 **NFSv4** 稽核策略的信息

您可以FlexVol 使用ONTAP CLI在S什麼 磁碟區上顯示NFSv4稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單（SACL）的相關資訊。

您可以使用結果來驗證安全性組態或疑難排解稽核問題。

關於這項工作

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或目錄路徑。您可以以摘要形式或詳細清單來顯示輸出。

- UNIX安全型磁碟區和qtree僅使用NFSv4 SACL來執行稽核原則。
- 混合式安全型磁碟區中的檔案和目錄、若為UNIX安全型態、則可套用NFSv4稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS的有效安全性、而且可能包含或不包含NFSv4 SACL。
- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般NFSv4檔案和目錄SACL、以及儲存層級存取保護NTFS SACL。
- 由於如果在 SVM 上設定 CIFS 伺服器、則 UNIX 磁碟區或 qtree 上支援儲存層級存取保護安全性、因此輸出可能包含適用於中指定之磁碟區或 qtree 的儲存層級存取保護安全性相關資訊 `-path` 參數。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄安全性設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
更詳細的資料	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示有關路徑的安全性資訊 `/lab` 在 SVM VS1 中。此UNIX安全型路徑具有NFSv4 SACL。

```
cluster::> vserver security file-directory show -vserver vs1 -path /lab

                Vserver: vs1
              File Path: /lab
      File Inode Number: 288
         Security Style: unix
        Effective Style: unix
         DOS Attributes: 11
 DOS Attributes in Text: ----D--R
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 0
 Unix Mode Bits in Text: ---------
                   ACLs: NFSV4 Security Descriptor
                         Control:0x8014
                         SACL - ACEs
                           SUCCESSFUL-S-1-520-0-0xf01ff-SA
                           FAILED-S-1-520-0-0xf01ff-FA
                         DACL - ACEs
                           ALLOW-S-1-520-1-0xf01ff
```

了解如何顯示 **ONTAP SMB** 文件安全和審計策略信息

您可以使用萬用字元（*）來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽核原則相關資訊。

萬用字元（）可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。如果您想要顯示名為「」的特定檔案或目錄資訊、則必須在雙引號（「'」）內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 `/1/` SVM VS1 ：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「*」的檔案資訊 `/vol1/a` SVM VS1 的路徑會以雙引號（""）括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

使用**CLI**管理**SVM**上的**NTFS**檔案安全性、**NTFS**稽核原則及儲存層級存取保護

用於管理 **SMB NTFS** 檔案安全、**NTFS** 稽核原則和儲存層級存取防護的 **ONTAP** 命令

您可以使用CLI管理儲存虛擬機器（SVM）上的NTFS檔案安全性、NTFS稽核原則及儲存層級存取保護。

您可以從SMB用戶端或使用CLI來管理NTFS檔案安全性和稽核原則。不過、使用CLI來設定檔案安全性和稽核原則、就不需要使用遠端用戶端來管理檔案安全性。使用CLI可大幅縮短使用單一命令在許多檔案和資料夾上套用安全性所需的時間。

您可以設定儲存層級的存取防護、ONTAP 這是由SVM Volume套用的另一層安全防護。儲存層級存取保護適用於從所有NAS傳輸協定存取至套用儲存層級存取保護的儲存物件。

儲存層級的存取保護只能從ONTAP 整套CLI進行設定和管理。您無法從SMB用戶端管理儲存層級的存取保護設定。此外、如果您從NFS或SMB用戶端檢視檔案或目錄上的安全性設定、就不會看到儲存層級的存取保護安全性。即使是系統（Windows或UNIX）管理員、也無法從用戶端撤銷儲存層級的存取保護安全性。因此、儲存層級的存取保護功能可為資料存取提供額外的安全層級、並由儲存管理員獨立設定及管理。

> 即使儲存層級存取保護僅支援NTFS存取權限、ONTAP 但如果UNIX使用者對應至擁有該磁碟區的SVM上的Windows使用者、則可在套用Storage層級存取保護的磁碟區上執行安全性檢查、以透過NFS存取資料。

NTFS安全型磁碟區

NTFS安全型磁碟區和qtree中包含的所有檔案和資料夾都具有NTFS有效安全性。您可以使用 `vserver security file-directory` 命令系列可在 NTFS 安全樣式磁碟區上實作下列類型的安全性：

- 磁碟區中所含檔案和資料夾的檔案權限和稽核原則
- 磁碟區上的儲存層級存取保護安全性

混合式安全型磁碟區

混合式安全型磁碟區和qtree可包含一些具有UNIX有效安全性的檔案和資料夾、並使用UNIX檔案權限、包括模式位元或NFSv4.x ACL和NFSv4.x稽核原則、以及某些具有NTFS有效安全性、並使用NTFS檔案權限和稽核原則的檔案和資料夾。您可以使用 `vserver security file-directory` 命令系列可將下列類型的安全性套用至混合式安全型資料：

- 在混合磁碟區或qtree中、使用NTFS有效安全型態的檔案和資料夾的檔案權限和稽核原則
- 儲存層級的存取保護功能、可用於NTFS和UNIX有效的安全型態磁碟區

UNIX 安全型磁碟區

UNIX安全型磁碟區和qtree包含具有UNIX有效安全性的檔案和資料夾（模式位元或NFSv4.x ACL）。如果您想要使用、請務必謹記下列事項 `vserver security file-directory` 在 UNIX 安全型磁碟區上實作安全功能的命令系列：

- 。 `vserver security file-directory` 命令系列無法用於管理 UNIX 安全性樣式磁碟區和 qtree 上的 UNIX 檔案安全性和稽核原則。
- 您可以使用 `vserver security file-directory` 命令系列可在 UNIX 安全性型磁碟區上設定儲存層級存取保護、前提是目標磁碟區的 SVM 包含 CIFS 伺服器。

相關資訊

- 了解如何查看文件安全和審核策略
- 在伺服器上建立 NTFS 安全描述符
- 配置和應用審核策略到檔案和資料夾的命令
- 了解如何使用儲存級別存取防護來保護文件存取

用於設定 **SMB** 檔案和資料夾安全性的 **ONTAP** 命令

由於您可以在本機套用及管理檔案與資料夾安全性、而無需遠端用戶端介入、因此您可以大幅縮短設定大量檔案或資料夾的大量安全性所需的時間。

在下列使用案例中、您可以使用CLI設定檔案和資料夾的安全性：

- 在大型企業環境中儲存檔案、例如在主目錄中儲存檔案
- 資料移轉
- Windows網域變更
- 跨NTFS檔案系統的檔案安全性與稽核原則標準化

了解使用 **ONTAP** 命令設定 **SMB** 檔案和資料夾安全性時的限制

使用CLI設定檔案和資料夾安全性時、您必須注意特定限制。

- 。 `vserver security file-directory` Command Family 不支援設定 NFSv4 ACL 。

  您只能將NTFS安全性描述元套用至NTFS檔案和資料夾。

使用安全描述符應用 **ONTAP SMB** 檔案和資料夾安全性

安全性描述元包含存取控制清單、可決定使用者可對檔案和資料夾執行的動作、以及使用者存取檔案和資料夾時所稽核的項目。

- 權限

  物件擁有者允許或拒絕權限、並決定物件（使用者、群組或電腦物件）可對指定的檔案或資料夾執行哪些動作。

- 安全性描述元

  安全性描述元是包含安全性資訊的資料結構、可定義與檔案或資料夾相關的權限。

- 存取控制清單（**ACL**）

  存取控制清單是安全性描述元中所包含的清單、其中包含使用者、群組或電腦物件可在套用安全性描述元的檔案或資料夾上執行哪些動作的相關資訊。安全性描述元可包含下列兩種ACL：

  - 判別存取控制清單（DACL）
  - 系統存取控制清單（SACL）

- 任意存取控制清單（**DACL**）

  DACL包含使用者、群組和電腦物件的「小島嶼」清單、這些使用者、群組和電腦物件均可存取或拒絕存取檔案或資料夾上的動作。DACL包含零個以上的存取控制項目（ACE）。

- 系統存取控制清單（**SACL**）

  SACL包含已記錄成功或失敗稽核事件之使用者、群組及電腦物件的「小島嶼」清單。SACL包含零個以上的存取控制項目（ACE）。

- 存取控制項目（**ACE**）

  ACE是DACL或SACL中的個別項目：

  - DACL存取控制項目會指定特定使用者、群組或電腦物件所允許或拒絕的存取權限。
  - SACL存取控制項目會指定在稽核特定使用者、群組或電腦物件執行的指定動作時、要記錄的成功或失敗事件。

- 權限繼承

  權限繼承說明如何將安全性描述元中定義的權限、從父物件傳播到物件。子物件只會繼承可繼承的權限。在父物件上設定權限時、您可以決定資料夾、子資料夾和檔案是否可以使用「套用至」來繼承它們 `this-`

folder、 `sub-folders`和「檔案」。

相關資訊

- "SMB與NFS稽核與安全性追蹤"
- 配置和應用審核策略到檔案和資料夾的命令

了解如何在 **ONTAP SVM** 災難復原目標上套用使用本機 **SMB** 使用者或群組的檔案目錄策略

如果您的檔案目錄原則組態在安全性描述元、DACL或SACL項目中使用本機使用者或群組、則在ID捨棄組態中的儲存虛擬機器（SVM）災難恢復目的地上套用檔案目錄原則之前、必須謹記一些準則。

您可以為SVM設定災難恢復組態、讓來源叢集上的來源SVM將資料和組態從來源SVM複寫到目的地叢集上的目的地SVM。

您可以設定兩種SVM災難恢復類型之一：

- 身分識別保留

  有了這項組態、SVM和CIFS伺服器的身分識別就會保留下來。

- 身分識別已捨棄

  使用此組態時、SVM和CIFS伺服器的身分識別將不會保留。在此案例中、目的地SVM上的SVM和CIFS伺服器名稱與來源SVM上的SVM和CIFS伺服器名稱不同。

身分識別捨棄組態的準則

在身分識別捨棄組態中、對於包含本機使用者、群組和權限組態的SVM來源、必須變更本機網域名稱（本機CIFS伺服器名稱）、以符合SVM目的地上的CIFS伺服器名稱。例如、如果來源SVM名稱為「'VS1'」、CIFS伺服器名稱為「'CIFS1'」、目的地SVM名稱為「'VS1_DST'」、CIFS伺服器名稱為「'CIFS1_DST'」、則本機使用者的本機網域名稱會自動變更為「CIFS1\user1'上的Cdst_Dst：」

```
cluster1::> vserver cifs users-and-groups local-user show -vserver vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1          CIFS1\Administrator                     Built-in
administrator account
vs1          CIFS1\user1              -              -

cluster1dst::> vserver cifs users-and-groups local-user show -vserver
vs1_dst

Vserver      User Name                Full Name      Description
------------ ------------------------ -------------- -------------
vs1_dst      CIFS1_DST\Administrator                 Built-in
administrator account
vs1_dst      CIFS1_DST\user1          -              -
```

雖然本機使用者和群組資料庫中的本機使用者和群組名稱會自動變更、但檔案目錄原則組態中的本機使用者或群組名稱不會自動變更（使用在 CLI 上設定的原則） `vserver security file-directory` Command Family ）。

例如、如果您已設定 DACL 項目、其中會顯示「 'VS1' 」 `-account` 參數設為「 'CIFS1\user1' 」、目的地 SVM 上的設定不會自動變更、以反映目的地的 CIFS 伺服器名稱。

```
cluster1::> vserver security file-directory ntfs dacl show -vserver vs1

Vserver: vs1
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    CIFS1\user1      allow    full-control      this-folder

cluster1::> vserver security file-directory ntfs dacl show -vserver
vs1_dst

Vserver: vs1_dst
  NTFS Security Descriptor Name: sd1

    Account Name     Access   Access             Apply To
                     Type     Rights
    --------------   -------  -------            -----------
    **CIFS1**\user1          allow    full-control      this-folder
```

您必須使用 `vserver security file-directory modify` 手動將 CIFS 伺服器名稱變更為目的地 CIFS 伺服器名稱的命令。

包含帳戶參數的檔案目錄原則組態元件

有三個檔案目錄原則組態元件可以使用參數設定、這些設定可以包含本機使用者或群組：

- 安全性描述元

  您可以選擇性地指定安全性描述元的擁有者和安全性描述元擁有者的主要群組。如果安全性描述元使用本機使用者或群組做為擁有者和主要群組項目、則必須修改安全性描述元、才能在帳戶名稱中使用目的地SVM。您可以使用 `vserver security file-directory ntfs modify` 命令以對帳戶名稱進行任何必要的變更。

- DACL項目

  每個DACL項目都必須與一個帳戶相關聯。您必須修改任何使用本機使用者或群組帳戶的DACL、才能使用目的地SVM名稱。由於您無法修改現有DACL項目的帳戶名稱、因此您必須從安全性描述元中移除任何具有本機使用者或群組的DACL項目、以修正的目的地帳戶名稱建立新的DACL項目、並將這些新的DACL項目與適當的安全性描述元建立關聯。

- SACL 項目

  每個SACL項目都必須與帳戶建立關聯。您必須修改任何使用本機使用者或群組帳戶的SACL、才能使用目的地SVM名稱。由於您無法修改現有SACL項目的帳戶名稱、因此您必須從安全性描述元中移除具有本機使用者或群組的任何SACL項目、以修正的目的地帳戶名稱建立新的SACL項目、並將這些新的SACL項目與適當的安全性描述元建立關聯。

套用原則之前、您必須對檔案目錄原則組態中使用的本機使用者或群組進行任何必要的變更、否則套用工作會失敗。

使用**CLI**在**NTFS**檔案和資料夾上設定及套用檔案安全性

在 **ONTAP SMB** 伺服器上建立 **NTFS** 安全性描述符

建立NTFS安全性描述元（檔案安全性原則）是設定NTFS存取控制清單（ACL）並套用至儲存虛擬機器（SVM）內的檔案和資料夾的第一步。您可以將安全性描述元與原則工作中的檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案

物件	存取類型	存取權限	權限的套用位置
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需詳細資訊，請參閱 "指令參考資料ONTAP"。

將 **NTFS DACL** 存取控制項目新增至 **ONTAP SMB** 伺服器上的 **NTFS** 安全性描述符

將DACL（判別存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是設定及套用NTFS ACL至檔案或資料夾的第二步驟。每個項目都會識別允許或拒絕存取的物件、並定義物件可以或無法對ACE中定義的檔案或資料夾執行的操作。

關於這項工作

您可以將一或多個 ACE 新增至安全性描述元的 DACL 。

如果安全性描述元包含具有現有 ACE 的 DACL 、則命令會將新的 ACE 新增至 DACL 。如果安全性描述元不包含DACL、則命令會建立DACL並新增新的ACE。

您可以選擇自訂 DACL 項目、方法是指定要允許或拒絕中指定之帳戶的權限 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 DACL 項目的權限、則預設會將權限設定為 `Full Control`。

您可以指定如何套用繼承、以選擇性地自訂DACL項目。

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 將 DACL 項目新增至安全性描述元： `vserver security file-directory ntfs dacl add`

```
-vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account
name_or_SIDoptional_parameters

vserver security file-directory ntfs dacl add -ntfs-sd sd1 -access-type deny
-account domain\joe -rights full-control -apply-to this-folder -vserver vs1
```

2. 驗證 DACL 項目是否正確：`vserver security file-directory ntfs dacl show -vserver vserver_name -ntfs-sd SD_name -access-type {allow|deny} -account name_or_SID`

```
vserver security file-directory ntfs dacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                Vserver: vs1
Security Descriptor Name: sd1
           Allow or Deny: deny
     Account Name or SID: DOMAIN\joe
           Access Rights: full-control
  Advanced Access Rights: -
                Apply To: this-folder
           Access Rights: full-control
```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs dacl`資訊，請參閱。

建立 **ONTAP SMB** 安全性策略

為SVM建立檔案安全性原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個SVM建立關聯（包含NTFS安全型磁碟區或混合式安全型磁碟區）。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver           Policy Name
------------      ---------------
     vs1               policy1
```

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

  即使原則可以包含多項工作、您也無法將原則設定為同時包含檔案目錄和儲存層級的存取保護工作。原則必須包含所有儲存層級的存取保護工作或所有檔案目錄工作。

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

將工作新增至安全性原則時、您必須指定下列四個必要參數：

- SVM名稱
- 原則名稱
- 路徑
- 與路徑相關聯的安全性描述元

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式

- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 將具有相關安全性描述元的工作新增至安全性原則： `vserver security file-directory policy task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd SD_nameoptional_parameters`

   `file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

   ```
   vserver security file-directory policy task add -vserver vs1 -policy-name policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2 -index-num 1 -access-control file-directory
   ```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

   ```
   vserver security file-directory policy task show
   ```

   ```
   Vserver: vs1
   Policy: policy1

   Index    File/Folder    Access           Security   NTFS        NTFS
   Security
            Path           Control          Type       Mode
   Descriptor Name
   -----    --------       -----------      --------   ------
   ----------------
   1        /home/dir1     file-directory   ntfs       propagate   sd2
   ```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

應用 **ONTAP SMB** 安全性策略

將檔案安全性原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後步驟。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

   `vserver security file-directory apply -vserver vs1 -policy-name policy1`

   原則套用工作已排程、並傳回工作ID。

   ```
   [Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id 53322" command to view the status of the operation
   ```

監控 ONTAP SMB 安全性策略作業

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   `vserver security file-directory job show -vserver vs1`

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證 ONTAP SMB 檔案安全性

您可以驗證檔案安全性設定、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的設定。

關於這項工作

您必須提供SVM名稱、其中包含資料、以及您要驗證安全性設定之檔案和資料夾的路徑。您可以使用選用的 `-expand-mask` 顯示安全性設定詳細資訊的參數。

步驟

1. 顯示檔案和資料夾安全性設定： `vserver security file-directory show -vserver vserver_name -path path [-expand-mask true]`

```
vserver security file-directory show -vserver vs1 -path /data/engineering
-expand-mask true
```

```
         Vserver: vs1
              File Path: /data/engineering
      File Inode Number: 5544
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: 0x10
     ...0 .... .... .... = Offline
     .... ..0. .... .... = Sparse
     .... .... 0... .... = Normal
     .... .... ..0. .... = Archive
     .... .... ...1 .... = Directory
     .... .... .... .0.. = System
     .... .... .... ..0. = Hidden
     .... .... .... ...0 = Read Only
          Unix User Id: 0
         Unix Group Id: 0
        Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8004

                             1... .... .... .... = Self Relative
                             .0.. .... .... .... = RM Control Valid
                             ..0. .... .... .... = SACL Protected
                             ...0 .... .... .... = DACL Protected
                             .... 0... .... .... = SACL Inherited
                             .... .0.. .... .... = DACL Inherited
                             .... ..0. .... .... = SACL Inherit Required
                             .... ...0 .... .... = DACL Inherit Required
                             .... .... ..0. .... = SACL Defaulted
                             .... .... ...0 .... = SACL Present
                             .... .... .... 0... = DACL Defaulted
                             .... .... .... .1.. = DACL Present
                             .... .... .... ..0. = Group Defaulted
                             .... .... .... ...0 = Owner Defaulted

                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         DACL - ACEs
                           ALLOW-Everyone-0x1f01ff
                             0... .... .... .... .... .... .... .... =
```

```
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...0 .... .... .... .... .... .... .... =
Generic All
                              .... ...0 .... .... .... .... .... .... =
System Security
                              .... .... ...1 .... .... .... .... .... =
Synchronize
                              .... .... .... 1... .... .... .... .... =
Write Owner
                              .... .... .... .1.. .... .... .... .... =
Write DAC
                              .... .... .... ..1. .... .... .... .... =
Read Control
                              .... .... .... ...1 .... .... .... .... =
Delete
                              .... .... .... .... .... ...1 .... .... =
Write Attributes
                              .... .... .... .... .... .... 1... .... =
Read Attributes
                              .... .... .... .... .... .... .1.. .... =
Delete Child
                              .... .... .... .... .... .... ..1. .... =
Execute
                              .... .... .... .... .... .... ...1 .... =
Write EA
                              .... .... .... .... .... .... .... 1... =
Read EA
                              .... .... .... .... .... .... .... .1.. =
Append
                              .... .... .... .... .... .... .... ..1. =
Write
                              .... .... .... .... .... .... .... ...1 =
Read

                            ALLOW-Everyone-0x10000000-OI|CI|IO
                              0... .... .... .... .... .... .... .... =
Generic Read
                              .0.. .... .... .... .... .... .... .... =
Generic Write
                              ..0. .... .... .... .... .... .... .... =
Generic Execute
                              ...1 .... .... .... .... .... .... .... =
```

```
Generic All
                                .... ...0 .... .... .... .... .... .... =
System Security
                                .... .... ...0 .... .... .... .... .... =
Synchronize
                                .... .... .... 0... .... .... .... .... =
Write Owner
                                .... .... .... .0.. .... .... .... .... =
Write DAC
                                .... .... .... ..0. .... .... .... .... =
Read Control
                                .... .... .... ...0 .... .... .... .... =
Delete
                                .... .... .... .... .... ...0 .... .... =
Write Attributes
                                .... .... .... .... .... .... 0... .... =
Read Attributes
                                .... .... .... .... .... .... .0.. .... =
Delete Child
                                .... .... .... .... .... .... ..0. .... =
Execute
                                .... .... .... .... .... .... ...0 .... =
Write EA
                                .... .... .... .... .... .... .... 0... =
Read EA
                                .... .... .... .... .... .... .... .0.. =
Append
                                .... .... .... .... .... .... .... ..0. =
Write
                                .... .... .... .... .... .... .... ...0 =
Read
```

使用**CLI**設定稽核原則並套用至**NTFS**檔案和資料夾

用於設定 **SMB** 稽核策略並將其套用至 **NTFS** 檔案和資料夾的 **ONTAP** 命令

使用ONTAP CLI時、您必須執行幾個步驟、才能將稽核原則套用至NTFS檔案和資料夾。首先、您要建立NTFS安全性描述元、然後將SACL新增至安全性描述元。接下來您要建立安全性原則並新增原則工作。然後將安全性原則套用至儲存虛擬機器（SVM）。

關於這項工作

套用安全性原則之後、您可以監控安全性原則工作、然後驗證套用的稽核原則設定。

套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

相關資訊

- 了解如何使用儲存級別存取防護來保護文件存取
- 了解使用命令設定 SMB 檔案和資料夾安全性時的限制
- 使用安全描述符來應用檔案和資料夾安全性
- "SMB與NFS稽核與安全性追蹤"
- 在伺服器上建立 NTFS 安全描述符

在 **ONTAP SMB** 伺服器上建立 **NTFS** 安全性描述符

建立NTFS安全性描述元稽核原則是設定NTFS存取控制清單（ACL）並套用至位於SVM內的檔案和資料夾的第一步。您將在原則工作中、將安全性描述元與檔案或資料夾路徑建立關聯。

關於這項工作

您可以針對位於NTFS安全型磁碟區內的檔案和資料夾、或是位於混合式安全型磁碟區上的檔案和資料夾、建立NTFS安全性描述元。

根據預設、建立安全性描述元時、會將四個判別存取控制清單（DACL）存取控制項目（ACE）新增至該安全性描述元。四個預設的ACE如下所示：

物件	存取類型	存取權限	權限的套用位置
內建\系統管理員	允許	完全控制	此資料夾、子資料夾、檔案
內建\使用者	允許	完全控制	此資料夾、子資料夾、檔案
建立者擁有者	允許	完全控制	此資料夾、子資料夾、檔案
NT AUTHORITY\系統	允許	完全控制	此資料夾、子資料夾、檔案

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全性描述元的擁有者
- 擁有者的主要群組
- 原始控制旗標

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 如果您要使用進階參數、請將權限等級設為進階： `set -privilege advanced`

2. 建立安全性描述元： `vserver security file-directory ntfs create -vserver vserver_name -ntfs-sd SD_nameoptional_parameters`

   `vserver security file-directory ntfs create -ntfs-sd sd1 -vserver vs1 -owner DOMAIN\joe`

3. 驗證安全描述元組態是否正確： `vserver security file-directory ntfs show -vserver vserver_name -ntfs-sd SD_name`

   ```
   vserver security file-directory ntfs show -vserver vs1 -ntfs-sd sd1
   ```

   ```
                                   Vserver: vs1
                        Security Descriptor Name: sd1
                  Owner of the Security Descriptor: DOMAIN\joe
   ```

4. 如果您處於進階權限層級、請返回管理權限層級： `set -privilege admin`

將 **NTFS SACL** 存取控制項目新增至 **ONTAP SMB** 伺服器上的 **NTFS** 安全性描述符

將SACL（系統存取控制清單）存取控制項目（ACE）新增至NTFS安全性描述元、是在SVM中為檔案或資料夾建立NTFS稽核原則的第二步驟。每個項目都會識別您要稽核的使用者或群組。SACL項目會定義您要稽核成功或失敗的存取嘗試。

關於這項工作

您可以將一個或多個ACE新增至安全性描述元的SACL。

如果安全性描述元包含具有現有ACE的SACL、則命令會將新的ACE新增至SACL。如果安全性描述元未包含SACL、則命令會建立SACL並將新的ACE新增至其中。

您可以指定要稽核中所指定帳戶成功或失敗事件的權限、以設定 SACL 項目 `-account` 參數。有三種互不相容的方法可以指定權限：

- 權利
- 進階權限
- 原始權限（進階權限）

如果您未指定 SACL 項目的權限、則預設設定為 `Full Control`。

您可以選擇自訂 SACL 項目、方法是指定如何使用套用繼承 `apply to` 參數。如果您未指定此參數、預設值為將此SACL項目套用至此資料夾、子資料夾及檔案。

步驟

1. 將 SACL 項目新增至安全性描述元： `vserver security file-directory ntfs sacl add -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SIDoptional_parameters`

```
vserver security file-directory ntfs sacl add -ntfs-sd sd1 -access-type
failure -account domain\joe -rights full-control -apply-to this-folder
-vserver vs1
```

2. 驗證 SACL 項目是否正確：`vserver security file-directory ntfs sacl show -vserver vserver_name -ntfs-sd SD_name -access-type {failure|success} -account name_or_SID`

```
vserver security file-directory ntfs sacl show -vserver vs1 -ntfs-sd sd1
-access-type deny -account domain\joe
```

```
                                Vserver: vs1
                    Security Descriptor Name: sd1
        Access type for Specified Access Rights: failure
                        Account Name or SID: DOMAIN\joe
                              Access Rights: full-control
                     Advanced Access Rights: -
                                   Apply To: this-folder
                              Access Rights: full-control
```

建立 **ONTAP SMB** 安全性策略

建立儲存虛擬機器（SVM）的稽核原則、是設定及套用ACL至檔案或資料夾的第三個步驟。原則可做為各種工作的容器、其中每項工作都是可套用至檔案或資料夾的單一項目。您可以稍後將工作新增至安全性原則。

關於這項工作

您新增至安全性原則的工作包含NTFS安全性描述元與檔案或資料夾路徑之間的關聯。因此、您應該將安全性原則與每個儲存虛擬機器（SVM）（包含NTFS安全型磁碟區或混合式安全型磁碟區）建立關聯。

步驟

1. 建立安全性原則：`vserver security file-directory policy create -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory policy create -policy-name policy1 -vserver
vs1
```

2. 驗證安全性原則：`vserver security file-directory policy show`

```
vserver security file-directory policy show
   Vserver          Policy Name
 ------------     --------------
     vs1              policy1
```

建立原則工作並將其新增至安全性原則、是設定及套用ACL至SVM中的檔案或資料夾的第四個步驟。當您建立原則工作時、會將工作與安全性原則建立關聯。您可以將一或多個工作項目新增至安全性原則。

關於這項工作

安全性原則是工作的容器。工作指的是單一作業、可透過安全性原則對具有NTFS或混合式安全性的檔案或資料夾（或是在設定儲存層級存取保護時、對磁碟區物件執行）。

工作有兩種類型：

- 檔案與目錄工作

  用於指定將安全性描述元套用至指定檔案和資料夾的工作。透過檔案和目錄工作所套用的ACL、可透過SMB用戶端或ONTAP CLI進行管理。

- 儲存層級的存取保護工作

  用於指定將儲存層級存取保護安全性描述元套用至指定磁碟區的工作。透過儲存層級存取保護工作套用的ACL只能透過ONTAP CLI進行管理。

工作包含檔案（或資料夾）或一組檔案（或資料夾）的安全性組態定義。原則中的每項工作都會以路徑唯一識別。在單一原則中、每個路徑只能有一項工作。原則不能有重複的工作項目。

新增工作至原則的準則：

- 每個原則最多可有10、000個工作項目。
- 原則可以包含一或多個工作。

  即使原則可以包含多項工作、您也無法將原則設定為同時包含檔案目錄和儲存層級的存取保護工作。原則必須包含所有儲存層級的存取保護工作或所有檔案目錄工作。

- 儲存層級的存取保護用於限制權限。

  它永遠不會提供額外的存取權限。

您可以使用下列選用參數來自訂安全性描述元組態：

- 安全類型
- 傳播模式
- 索引位置
- 存取控制類型

儲存層級存取保護會忽略任何選用參數的值。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

步驟

1. 將具有相關安全性描述元的工作新增至安全性原則： `vserver security file-directory policy`

```
task add -vserver vserver_name -policy-name policy_name -path path -ntfs-sd
SD_nameoptional_parameters
```

`file-directory` 為的預設值 `-access-control` 參數。設定檔案和目錄存取工作時、可選擇指定存取控制類型。

```
vserver security file-directory policy task add -vserver vs1 -policy-name
policy1 -path /home/dir1 -security-type ntfs -ntfs-mode propagate -ntfs-sd sd2
-index-num 1 -access-control file-directory
```

2. 驗證原則工作組態： `vserver security file-directory policy task show -vserver vserver_name -policy-name policy_name -path path`

```
vserver security file-directory policy task show
```

```
Vserver: vs1
Policy: policy1

Index    File/Folder    Access           Security   NTFS       NTFS
Security
         Path           Control          Type       Mode
Descriptor Name
-----    --------       -----------      --------   ------
----------------
1        /home/dir1     file-directory   ntfs       propagate  sd2
```

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

應用 **ONTAP SMB** 安全性策略

將稽核原則套用到SVM是建立NTFS ACL並套用到檔案或資料夾的最後一步。

關於這項工作

您可以將安全性原則中定義的安全性設定套用至FlexVol 駐留在各處的NTFS檔案和資料夾（NTFS或混合式安全樣式）。

> 套用稽核原則和相關的SACL時、會覆寫任何現有的DACL。套用安全性原則及其相關的DACL時、會覆寫任何現有的DACL。您應該在建立及套用新的安全性原則之前、先檢閱現有的安全性原則。

步驟

1. 套用安全性原則： `vserver security file-directory apply -vserver vserver_name -policy-name policy_name`

```
vserver security file-directory apply -vserver vs1 -policy-name policy1
```

原則套用工作已排程、並傳回工作ID。

```
[Job 53322]Job is queued: Fsecurity Apply. Use the "Job show 53322 -id
53322" command to view the status of the operation
```

監控 ONTAP SMB 安全性策略作業

將安全性原則套用至儲存虛擬機器（SVM）時、您可以監控安全性原則工作、以監控工作進度。如果您想要確定安全性原則的應用是否成功、這項功能就很有幫助。如果您的工作執行時間很長、而您要將大量安全性套用到大量的檔案和資料夾、這也很有幫助。

關於這項工作

若要顯示安全性原則工作的詳細資訊、您應該使用 `-instance` 參數。

步驟

1. 監控安全性原則工作： `vserver security file-directory job show -vserver vserver_name`

   ```
   vserver security file-directory job show -vserver vs1
   ```

   ```
   Job ID Name                 Vserver    Node           State
   ------ -------------------- ---------- -------------- ----------
   53322  Fsecurity Apply      vs1        node1          Success
          Description: File Directory Security Apply Job
   ```

驗證 ONTAP SMB 稽核策略

您可以驗證稽核原則、確認您套用安全性原則的儲存虛擬機器（SVM）上的檔案或資料夾具有所需的稽核安全性設定。

關於這項工作

您可以使用 `vserver security file-directory show` 顯示稽核原則資訊的命令。您必須提供SVM名稱、其中包含您要顯示其檔案或資料夾稽核原則資訊的資料、以及其路徑。

步驟

1. 顯示稽核原則設定： `vserver security file-directory show -vserver vserver_name -path path`

範例

下列命令會顯示套用至SVM VS1路徑「/corp」的稽核原則資訊。這條路徑既成功、也套用成功/失敗的SACL項目：

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp

                Vserver: vs1
              File Path: /corp
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

了解如何管理 **ONTAP SMB** 安全性策略作業

如果存在安全性原則工作、在某些情況下、您將無法修改該安全性原則或指派給該原則的工作。您應該瞭解可以修改或無法修改安全性原則的條件、以便成功修改原則。原則的修改包括新增、移除或修改指派給原則的工作、以及刪除或修改原則。

如果該原則的工作存在、且該工作處於下列狀態、則您無法修改安全性原則或指派給該原則的工作：

- 工作正在執行或進行中。
- 工作已暫停。
- 工作會恢復並處於執行中狀態。
- 如果工作正在等待容錯移轉到另一個節點。

在下列情況下、如果安全性原則有工作存在、您可以成功修改該安全性原則或指派給該原則的工作：

- 原則工作已停止。
- 原則工作已成功完成。

用於管理 **SMB** 伺服器上的 **NTFS** 安全描述符的 **ONTAP** 命令

管理安全性描述元時、會ONTAP 有特定的指令檔。您可以建立、修改、刪除及顯示安全性描述元的相關資訊。

如果您想要...	使用此命令...
建立NTFS安全性描述元	`vserver security file-directory ntfs create`
修改現有的NTFS安全性描述元	`vserver security file-directory ntfs modify`
顯示現有NTFS安全性描述元的相關資訊	`vserver security file-directory ntfs show`
刪除NTFS安全性描述元	`vserver security file-directory ntfs delete`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs`資訊，請參閱。

用於管理 **SMB** 伺服器上的 **NTFS DACL** 存取控制項目的 **ONTAP** 命令

管理ONTAP DACL存取控制項目（ACE）時、會有特定的功能不完整的指令。您可以隨時將ACE新增至NTFS DACL。您也可以在DACL中修改、刪除及顯示有關ACE的資訊、來管理現有的NTFS DACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS DACL	`vserver security file-directory ntfs dacl add`
修改NTFS DACL中的現有ACE	`vserver security file-directory ntfs dacl modify`
顯示NTFS DACL中現有ACE的相關資訊	`vserver security file-directory ntfs dacl show`
從NTFS DACL移除現有的ACE	`vserver security file-directory ntfs dacl remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs dacl`資訊，請參閱。

用於管理 **SMB** 伺服器上的 **NTFS SACL** 存取控制項目的 **ONTAP** 命令

管理ONTAP SACL存取控制項目（ACE）時、會有特定的功能不完整的命令。您可以隨時將ACE新增至NTFS SACL。您也可以在SACL中修改、刪除及顯示有關ACE的資訊、來管

理現有的NTFS SACL。

如果您想要...	使用此命令...
建立ACE並將其新增至NTFS SACL	`vserver security file-directory ntfs sacl add`
修改NTFS SACL中的現有ACE	`vserver security file-directory ntfs sacl modify`
顯示NTFS SACL中現有ACE的相關資訊	`vserver security file-directory ntfs sacl show`
從NTFS SACL移除現有的ACE	`vserver security file-directory ntfs sacl remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory ntfs sacl`資訊，請參閱。

用於管理 **SMB** 安全性原則的 **ONTAP** 命令

管理安全性原則時、會ONTAP 有特定的指令檔。您可以顯示原則的相關資訊、也可以刪除原則。您無法修改安全性原則。

如果您想要...	使用此命令...
建立安全性原則	`vserver security file-directory policy create`
顯示安全性原則的相關資訊	`vserver security file-directory policy show`
刪除安全性原則	`vserver security file-directory policy delete`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy`資訊，請參閱。

用於管理 **SMB** 安全性原則任務的 **ONTAP** 命令

有一些用來新增、修改、移除及顯示安全性原則工作相關資訊的指令。ONTAP

如果您想要...	使用此命令...
新增安全性原則工作	`vserver security file-directory policy task add`

如果您想要...	使用此命令...
修改安全性原則工作	`vserver security file-directory policy task modify`
顯示安全性原則工作的相關資訊	`vserver security file-directory policy task show`
移除安全性原則工作	`vserver security file-directory policy task remove`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory policy task`資訊，請參閱。

用於管理 **SMB** 安全性原則作業的 **ONTAP** 指令

有一些用來暫停、恢復、停止及顯示安全性原則工作資訊的指令。ONTAP

如果您想要...	使用此命令...
暫停安全性原則工作	`vserver security file-directory job pause -vserver vserver_name -id integer`
恢復安全原則工作	`vserver security file-directory job resume -vserver vserver_name -id integer`
顯示安全性原則工作的相關資訊	`vserver security file-directory job show -vserver vserver_name` 您可以使用此命令來判斷工作的工作 ID 。
停止安全性原則工作	`vserver security file-directory job stop -vserver vserver_name -id integer`

如"指令參考資料ONTAP"需詳細 `vserver security file-directory job`資訊，請參閱。

設定**SMB**共用的中繼資料快取

了解 **ONTAP SMB** 元資料緩存

中繼資料快取可讓SMB 1.0用戶端上的檔案屬性快取、更快存取檔案和資料夾屬性。您可以啟用或停用每個共用區的屬性快取。如果啟用中繼資料快取、您也可以設定快取項目的即時時間。如果用戶端透過SMB 2.x或SMB 3.0連線至共用區、則不需要設定中繼資料快取。

啟用時、SMB中繼資料快取會在有限的時間內儲存路徑和檔案屬性資料。這可為具有一般工作負載的SMB 1.0用戶端提升SMB效能。

對於某些工作、SMB會建立大量的流量、包括多個相同的路徑和檔案中繼資料查詢。您可以使用SMB中繼資料

快取來從快取擷取資訊、藉此減少備援查詢的數量、並改善SMB 1.0用戶端的效能。

> 雖然不太可能、但中繼資料快取可能會將過時的資訊提供給SMB 1.0用戶端。如果您的環境負擔不起這項風險、則不應啟用此功能。

啟用 **ONTAP SMB** 元資料緩存

您可以啟用SMB中繼資料快取、以改善SMB 1.0用戶端的SMB效能。根據預設、SMB中繼資料快取會停用。

步驟

1. 執行所需的動作：

如果您想要...	輸入命令...
建立共用時啟用SMB中繼資料快取	`vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties attributecache`
在現有共用區上啟用SMB中繼資料快取	`vserver cifs share properties add -vserver` *`vserver_name`* `-share-name` *`share_name`* `-share-properties attributecache`

相關資訊

- 配置元資料快取條目的生存期
- 新增或刪除現有共享的共享屬性

配置 **ONTAP SMB** 元資料快取條目的生命週期

您可以設定SMB中繼資料快取項目的生命週期、以最佳化環境中的SMB中繼資料快取效能。預設值為 10 秒。

開始之前

您必須啟用SMB中繼資料快取功能。如果未啟用SMB中繼資料快取、則不會使用SMB快取TTL設定。

步驟

1. 執行所需的動作：

如果您想要在下列情況下設定**SMB**中繼資料快取項目的生命週期...	輸入命令...
建立共用區	`vserver cifs share -create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-attribute-cache-ttl [integerh][integerm][integers]`

如果您想要在下列情況下設定**SMB**中繼資料快取項目的生命週期...	輸入命令...
修改現有的共用區	`vserver cifs share -modify -vserver` *`vserver_name`* `-share-name` *`share_name`* `-attribute-cache-ttl [integerh][integerm][integers]`

您可以在建立或修改共用時指定其他共用組態選項和屬性。如"指令參考資料ONTAP"需詳細 `vserver cifs share`資訊，請參閱。

管理檔案鎖定

了解協定之間的 **ONTAP SMB** 檔案鎖定

檔案鎖定是用戶端應用程式用來防止使用者存取先前由其他使用者開啟的檔案的方法。如何鎖定檔案取決於用戶端的傳輸協定。ONTAP

如果用戶端是NFS用戶端、則鎖定為建議事項；如果用戶端是SMB用戶端、則鎖定為必要項目。

由於NFS與SMB檔案鎖定之間的差異、NFS用戶端可能無法存取先前由SMB應用程式開啟的檔案。

當NFS用戶端嘗試存取SMB應用程式鎖定的檔案時、會發生下列情況：

- 在混合或 NTFS 磁碟區中、檔案處理作業、例如 `rm`、 `rmdir`和 `mv` 可能導致 NFS 應用程式失敗。
- SMB拒絕讀取和拒絕寫入開啟模式會分別拒絕NFS讀取和寫入作業。
- 當檔案的寫入範圍遭專屬SMB bytelock鎖定時、NFS寫入作業會失敗。
- 取消連結
  - 對於 NTFS 檔案系統、支援 SMB 和 CIFS 刪除作業。

    檔案將在上次關閉後移除。
  - 不支援 NFS 取消連結作業。

    不支援此功能、因為需要 NTFS 和 SMB 的語言、而且 NFS 不支援上次的「刪除 - 關閉」作業。
  - 對於 UNIX 檔案系統、支援取消連結作業。

    支援此功能、因為需要 NFS 和 UNIX 的語言。
- 重新命名
  - 對於 NTFS 檔案系統、如果目的地檔案是從 SMB 或 CIFS 開啟、則可以重新命名目的地檔案。
  - 不支援 NFS 重新命名。

    不支援此功能、因為需要 NTFS 和 SMB 的語言。

在UNIX安全型磁碟區中、NFS取消連結和重新命名作業會忽略SMB鎖定狀態、並允許存取檔案。UNIX安全型磁

碟區上的所有其他NFS作業都會遵守SMB鎖定狀態。

了解 **ONTAP SMB** 唯讀位

唯讀位元是逐一檔案設定、以反映檔案是可寫入（停用）或唯讀（啟用）。

使用Windows的SMB用戶端可以設定每個檔案的唯讀位元。NFS用戶端不會設定每個檔案的唯讀位元、因為NFS用戶端沒有任何使用每個檔案唯讀位元的傳輸協定作業。

當使用Windows的SMB用戶端建立檔案時、可以在檔案上設定唯讀位元。ONTAP在NFS用戶端和SMB用戶端之間共用檔案時、也可以設定唯讀位元。ONTAP有些軟體在NFS用戶端和SMB用戶端使用時、需要啟用唯讀位元。

為了在NFS用戶端和SMB用戶端之間共用的檔案上保留適當的讀取和寫入權限、它會根據下列規則來處理唯讀位元：ONTAP

- NFS會將任何啟用唯讀位元的檔案視為未啟用寫入權限位元。
- 如果NFS用戶端停用所有寫入權限位元、且至少有一個位元先前已啟用、ONTAP 則會啟用該檔案的唯讀位元。
- 如果NFS用戶端啟用任何寫入權限位元、ONTAP 則無法使用該檔案的唯讀位元。
- 如果已啟用檔案的唯讀位元、且NFS用戶端嘗試探索檔案的權限、則檔案的權限位元不會傳送至NFS用戶端；ONTAP 而是將權限位元傳送至NFS用戶端、並遮罩寫入權限位元。
- 如果已啟用檔案的唯讀位元、且SMB用戶端停用唯讀位元、ONTAP 則會啟用檔案的擁有者寫入權限位元。
- 啟用唯讀位元的檔案只能由root寫入。

唯讀位元以下列方式與 ACL 和 Unix 模式位元互動：

當檔案設定了唯讀位元：

- 該文件的 ACL 不會發生任何變更。 NFS用戶端將看到與設定唯讀位元之前相同的 ACL。
- 任何允許對檔案進行寫入存取的 Unix 模式位元都會被忽略。
- NFS 和 SMB 用戶端都可以讀取該文件，但不能修改它。
- ACL 和 UNIX 模式位元將被忽略，取而代之的是唯讀位元。這意味著，即使 ACL 允許寫入訪問，只讀位元也會阻止修改。

當檔案未設定唯讀位元：

- ONTAP根據 ACL 和 UNIX 模式位元決定存取權限。
  - 如果 ACL 或 UNIX 模式位元拒絕寫入訪問，則 NFS 和 SMB 用戶端無法修改該檔案。
  - 如果 ACL 和 UNIX 模式位元均不拒絕寫入訪問，則 NFS 和 SMB 用戶端可以修改該檔案。

檔案權限的變更會立即在SMB用戶端上生效、但如果NFS用戶端啟用屬性快取、則可能不會立即在NFS用戶端上生效。

ONTAP 在處理共用路徑元件上的鎖定時，與 **Windows** 有何不同

不像Windows、ONTAP 在檔案開啟時、不會鎖定開啟檔案路徑的每個元件。此行為也會

影響SMB共用路徑。

由於無法鎖定路徑的每個元件、因此可以重新命名開啟檔案或共用區上方的路徑元件、這可能會對某些應用程式造成問題、也可能導致SMB組態中的共用路徑無效。ONTAP這可能導致無法存取共用區。

為了避免重新命名路徑元件所造成的問題、您可以套用安全性設定、防止使用者或應用程式重新命名重要目錄。

顯示有關 **ONTAP SMB** 鎖的信息

您可以顯示目前檔案鎖定的相關資訊、包括鎖定的類型、鎖定狀態、位元組範圍鎖定、共用鎖定模式、委派鎖定及投機鎖定的詳細資料、以及鎖定是以耐久或持續的控點開啟。

關於這項工作

無法針對透過NFSv4或NFSv4.1建立的鎖定顯示用戶端IP位址。

依預設、命令會顯示所有鎖定的相關資訊。您可以使用命令參數來顯示特定儲存虛擬機器（SVM）的鎖定資訊、或是根據其他條件篩選命令的輸出。

。`vserver locks show` 命令會顯示四種鎖定類型的相關資訊：

- 位元組範圍鎖定、僅鎖定部分檔案。
- 共用鎖定、可鎖定開啟的檔案。
- 投機鎖定、可控制SMB上的用戶端快取。
- 委派：透過NFSv4.x控制用戶端快取

藉由指定選用參數、您可以決定每種鎖定類型的重要資訊。如"指令參考資料ONTAP"需詳細 `vserver locks show`資訊，請參閱。

步驟

1. 使用顯示鎖定的相關資訊 `vserver locks show` 命令。

範例

以下範例顯示具有路徑之檔案上 NFSv4 鎖定的摘要資訊 `/vol1/file1`。共享鎖定存取模式為WRITE拒絕_nONE、且鎖定是以寫入委派授予的：

```
cluster1::> vserver locks show

Vserver: vs0
Volume  Object Path               LIF         Protocol  Lock Type   Client
------- ------------------------- ----------- --------- -----------
-------
vol1    /vol1/file1               lif1        nfsv4     share-level -
               Sharelock Mode: write-deny_none
                                                         delegation  -
               Delegation Type: write
```

以下範例顯示有關 SMB 鎖定的詳細 oplock 和共享鎖定資訊、這些資訊位於具有路徑的檔案上

/data2/data2_2/intro.pptx。對於IP位址為10.3.1.3的用戶端、檔案上會以寫入拒絕的共用鎖定存取模式授予可持久使用的控制代碼。批次oplock層級的租賃oplock已授予：

```
cluster1::> vserver locks show -instance -path /data2/data2_2/intro.pptx

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/intro.pptx
                  Lock UUID: 553cf484-7030-4998-88d3-1125adbba0b7
              Lock Protocol: cifs
                  Lock Type: share-level
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
              Oplock Level: -
   Shared Lock Access Mode: write-deny_none
       Shared Lock is Soft: false
           Delegation Type: -
            Client Address: 10.3.1.3
              SMB Open Type: durable
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000

                    Vserver: vs1
                     Volume: data2_2
          Logical Interface: lif2
                Object Path: /data2/data2_2/test.pptx
                  Lock UUID: 302fd7b1-f7bf-47ae-9981-f0dcb6a224f9
              Lock Protocol: cifs
                  Lock Type: op-lock
   Node Holding Lock State: node3
                 Lock State: granted
  Bytelock Starting Offset: -
    Number of Bytes Locked: -
     Bytelock is Mandatory: -
     Bytelock is Exclusive: -
     Bytelock is Superlock: -
          Bytelock is Soft: -
```

```
               Oplock Level: batch
   Shared Lock Access Mode: -
       Shared Lock is Soft: -
           Delegation Type: -
            Client Address: 10.3.1.3
             SMB Open Type: -
         SMB Connect State: connected
SMB Expiration Time (Secs): -
         SMB Open Group ID:
78a90c59d45ae211998100059a3c7a00a007f70da0f8ffffcd445b0300000000
```

打破 ONTAP SMB 鎖

當檔案鎖定阻礙用戶端存取檔案時、您可以顯示目前保留的鎖定資訊、然後中斷特定鎖定。您可能需要中斷鎖定的案例包括偵錯應用程式。

關於這項工作

此 `vserver locks break`命令僅適用於進階權限層級及更高層級。如"指令參考資料ONTAP"需詳細 `vserver locks break`資訊，請參閱。

步驟

1. 若要尋找打破鎖定所需的資訊、請使用 `vserver locks show` 命令。

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

2. 將權限層級設為進階： `set -privilege advanced`
3. 執行下列其中一項動作：

如果您要指定...來中斷鎖定	輸入命令...
SVM名稱、Volume名稱、LIF名稱及檔案路徑	`vserver locks break -vserver vserver_name -volume volume_name -path path -lif lif`
鎖定ID	`vserver locks break -lockid UUID`

4. 返回管理權限層級： `set -privilege admin`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

監控SMB活動

顯示 ONTAP SMB 會話訊息

您可以顯示已建立SMB工作階段的相關資訊、包括SMB連線和工作階段ID、以及使用工作階段之工作站的IP位址。您可以顯示工作階段SMB傳輸協定版本的相關資訊、以及持續可用的保護層級、協助您識別工作階段是否支援不中斷營運。

關於這項工作

您可以在SVM上以摘要形式顯示所有工作階段的資訊。不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊：

- 您可以使用選用的 `-fields` 參數顯示有關所選欄位的輸出。

  您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

- 您可以使用 `-instance` 顯示已建立 SMB 工作階段的詳細資訊的參數。
- 您可以使用 `-fields` 參數或 `-instance` 參數可以單獨使用、也可以搭配其他選用參數使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
以摘要形式顯示SVM上的所有工作階段	`vserver cifs session show -vserver vserver_name`
在指定的連線ID上	`vserver cifs session show -vserver vserver_name -connection-id integer`
從指定的工作站IP位址	`vserver cifs session show -vserver vserver_name -address workstation_IP_address`
在指定的LIF IP位址上	`vserver cifs session show -vserver vserver_name -lif-address LIF_IP_address`
在指定的節點上	`vserver cifs session show -vserver vserver_name -node {node_name
local}`	從指定的Windows使用者
`vserver cifs session show -vserver vserver_name -windows-user domain_name\\user_name`	使用指定的驗證機制
`vserver cifs session show -vserver vserver_name -auth-mechanism {NTLMv1	NTLMv2
Kerberos	Anonymous}`
使用指定的傳輸協定版本	`vserver cifs session show -vserver vserver_name -protocol-version {SMB1
SMB2	SMB2_1

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
SMB3	SMB3_1}`  [NOTE] ==== 持續可用的保護功能和SMB多通道功能僅適用於SMB 3.0及更新版本的工作階段。若要在所有合格的工作階段中檢視其狀態、您應該指定此參數、並將值設為 `SMB3` 或更新版本。 ====
提供特定等級的持續可用保護	`vserver cifs session show -vserver vserver_name -continuously-available {No
Yes	Partial}`  [NOTE] ==== 如果持續可用的狀態為 `Partial`這表示工作階段至少包含一個開啟的持續可用檔案、但工作階段有一些檔案無法以持續可用的保護開啟。您可以使用 `vserver cifs sessions file show` 命令來判斷已建立工作階段上的哪些檔案未以持續可用的保護開啟。 ====
具有指定的SMB簽署工作階段狀態	`vserver cifs session show -vserver vserver_name -is-session-signed {true

範例

下列命令會顯示SVM VS1上從IP位址為10.1.1的工作站所建立之工作階段的工作階段資訊：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

下列命令會顯示SVM VS1具有持續可用保護之工作階段的詳細工作階段資訊。連線是使用網域帳戶建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
            Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

下列命令會顯示SVM VS1上使用SMB 3.0和SMB多通道之工作階段的工作階段資訊。在此範例中、使用者使用LIF IP位址從具有SMB 3.0功能的用戶端連線到此共用區、因此驗證機制預設為NTLMv2。連線必須使用Kerberos驗證、才能以持續可用的保護進行連線。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

相關資訊

顯示開啟SMB檔案的相關資訊

顯示有關開啟的 **ONTAP SMB** 檔案的信息

您可以顯示開啟SMB檔案的相關資訊、包括SMB連線和工作階段ID、託管磁碟區、共用名稱和共用路徑。您可以顯示檔案持續可用保護層級的相關資訊、這有助於判斷開啟的檔案是否處於支援不中斷營運的狀態。

關於這項工作

您可以在已建立的SMB工作階段中顯示開啟檔案的相關資訊。當您需要判斷SMB工作階段中特定檔案的SMB工作階段資訊時、所顯示的資訊非常有用。

例如、如果您有 SMB 工作階段、其中某些開啟的檔案會以持續可用的保護開啟、有些則無法以持續可用的保護開啟（的值） `-continuously-available` 欄位輸入 `vserver cifs session show` 命令輸出為 `Partial`）、您可以使用此命令來判斷哪些檔案無法持續使用。

您可以使用、以摘要形式顯示已建立的儲存虛擬機器（ SVM ） SMB 工作階段上所有開啟檔案的資訊 `vserver cifs session file show` 不含任何選用參數的命令。

不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊。如果您只想檢視開啟檔案的一小部分資訊、這項功能就很有幫助。

- 您可以使用選用的 `-fields` 參數、可在您選擇的欄位上顯示輸出。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

- 您可以使用 `-instance` 顯示開啟 SMB 檔案的詳細資訊的參數。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
在SVM上以摘要形式顯示	`vserver cifs session file show -vserver vserver_name`
在指定的節點上	`vserver cifs session file show -vserver vserver_name -node {node_name
local}`	在指定的檔案ID上
`vserver cifs session file show -vserver vserver_name -file-id integer`	在指定的SMB連線ID上
`vserver cifs session file show -vserver vserver_name -connection-id integer`	在指定的SMB工作階段ID上
`vserver cifs session file show -vserver vserver_name -session-id integer`	在指定的託管Aggregate上
`vserver cifs session file show -vserver vserver_name -hosting -aggregate aggregate_name`	在指定的磁碟區上
`vserver cifs session file show -vserver vserver_name -hosting-volume volume_name`	在指定的SMB共用區上
`vserver cifs session file show -vserver vserver_name -share share_name`	在指定的SMB路徑上
`vserver cifs session file show -vserver vserver_name -path path`	提供指定等級的持續可用保護

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
`vserver cifs session file show -vserver vserver_name -continuously-available {No	Yes}`  [NOTE] ==== 如果持續可用的狀態為 `No`這表示這些開啟的檔案無法不中斷地從接管和恢復恢復。在高可用度關係中、他們也無法從合作夥伴之間的一般Aggregate重新配置中恢復。 ====
指定的重新連線狀態	`vserver cifs session file show -vserver vserver_name -reconnected {No

您可以使用其他選用參數來精簡輸出結果。如"指令參考資料ONTAP"需詳細 `vserver cifs session file show` 資訊，請參閱。

範例

下列範例顯示SVM VS1上開啟檔案的相關資訊：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:        node1
Vserver:     vs1
Connection: 3151274158
Session:     1
File     File       Open Hosting               Continuously
ID       Type       Mode Volume    Share       Available
-------- ---------- ---- --------- ----------- ------------
41       Regular    r    data      data        Yes
Path: \mytest.rtf
```

下列範例顯示SVM VS1上開啟檔案ID為82的SMB檔案的詳細資訊：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

相關資訊

顯示會話訊息

確定 **ONTAP SMB** 伺服器上可用的統計資料、物件和計數器

在取得CIFS、SMB、稽核和BranchCache雜湊統計資料的相關資訊及監控效能之前、您必須先知道哪些物件和計數器可供您取得資料。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您想要判斷...	輸入...
可用的物件	`statistics catalog object show`
可用的特定物件	`statistics catalog object show -object object_name`
可用的計數器	`statistics catalog counter show -object object_name`

   如需詳細資訊 `statistics catalog object show`，包括可使用的物件和計數器"指令參考資料ONTAP"，請參閱。

3. 返回管理權限層級： `set -privilege admin`

範例

下列命令會顯示與叢集中CIFS和SMB存取相關之所選統計物件的說明、如進階權限層級所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

下列命令會顯示的一些計數器相關資訊 `cifs` 進階權限層級的物件：

此範例不會顯示的所有可用計數器 `cifs` 物件；輸出被截斷。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

相關資訊

- 顯示統計資料

- "統計目錄計數器顯示對象"
- "統計開始"

顯示 **ONTAP SMB** 統計資料

您可以顯示各種統計資料、包括CIFS和SMB、稽核和BranchCache雜湊的統計資料、以監控效能並診斷問題。

開始之前

您必須使用收集資料樣本 `statistics start` 和 `statistics stop` 顯示物件相關資訊之前的命令。

詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您要顯示下列項目的統計資料...	輸入...
SMB的所有版本	`statistics show -object cifs`
SMB 1.0	`statistics show -object smb1`
SMB 2.x和SMB 3.0	`statistics show -object smb2`
節點的CIFS子系統	`statistics show -object nblade_cifs`
多重傳輸協定稽核	`statistics show -object audit_ng`
BranchCache雜湊服務	`statistics show -object hashd`
動態DNS	`statistics show -object ddns_update`

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

3. 返回管理權限層級： `set -privilege admin`

相關資訊

- 確定伺服器上可用的統計資料、物件和計數器
- 監控SMB簽署的工作階段統計資料
- 顯示BranchCache統計資料
- 使用統計資料來監控自動節點參照活動
- "Microsoft Hyper-V和SQL Server的SMB組態"

- "效能監控設定"

部署SMB用戶端型服務

使用離線檔案來允許快取檔案以供離線使用

了解如何使用離線檔案來允許快取 **ONTAP SMB** 檔案以供離線使用

支援Microsoft離線檔案功能（或用戶端快取）、可在本機主機上快取檔案以供離線使用。ONTAP即使使用者與網路中斷連線、仍可使用離線檔案功能繼續處理檔案。

您可以指定Windows使用者文件和程式是自動快取到共用區、還是必須手動選取檔案以供快取。預設會針對新共用啟用手動快取。離線使用的檔案會同步處理至Windows用戶端的本機磁碟。當連線至特定儲存系統共用區的網路連線恢復時、就會發生同步。

由於離線檔案和資料夾的存取權限與儲存在CIFS伺服器上的檔案和資料夾版本相同、因此使用者必須對儲存在CIFS伺服器上的檔案和資料夾擁有足夠的權限、才能對離線檔案和資料夾執行動作。

當使用者和網路上的其他人變更同一個檔案時、使用者可以將檔案的本機版本儲存到網路、保留其他版本、或同時儲存兩者。如果使用者同時保留這兩個版本、則會在本機儲存含有本機使用者變更的新檔案、而快取的檔案會被保存在CIFS伺服器上的檔案版本變更所覆寫。

您可以使用共用組態設定、逐一設定離線檔案。您可以在建立或修改共用時、從四個離線資料夾組態中選擇一個：

- 無快取

  停用共用區的用戶端快取。檔案和資料夾不會自動在本機用戶端上快取、而且使用者無法選擇在本機快取檔案或資料夾。

- 手動快取

  可手動選取要快取至共用區的檔案。這是預設設定。根據預設、不會在本機用戶端上快取任何檔案或資料夾。使用者可以選擇要在本機快取以供離線使用的檔案和資料夾。

- 自動文件快取

  可讓使用者文件自動快取至共用區。只有存取的檔案和資料夾才會在本機快取。

- 自動程式快取

  可讓程式和使用者文件自動快取至共用區。只有存取的檔案、資料夾和程式才會在本機快取。此外、此設定可讓用戶端執行本機快取的可執行檔、即使連線到網路也沒問題。

如需在Windows伺服器和用戶端上設定離線檔案的詳細資訊、請參閱Microsoft TechNet資源庫。

相關資訊

- 使用漫遊設定檔、將使用者設定檔集中儲存在與SVM相關的CIFS伺服器上
- 了解如何使用資料夾重新導向在伺服器上儲存數據
- 了解如何使用 BranchCache 在分公司快取共享內容

- "Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解使用離線 **ONTAP SMB** 檔案的要求

在CIFS伺服器上使用Microsoft離線檔案功能之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援該功能。

版本需求**ONTAP**

發行支援離線檔案。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的離線檔案。

Windows用戶端需求

Windows用戶端必須支援離線檔案。

如需哪些Windows用戶端支援離線檔案功能的最新資訊、請參閱互通性對照表。

"mysupport.netapp.com/matrix"

部署離線 **ONTAP SMB** 檔案的指南

當您在具有的主目錄共用上部署離線檔案時、需要瞭解一些重要準則 `showsnapshot` 在主目錄上共用屬性集。

如果 `showsnapshot`共用內容是在已設定離線檔案的主目錄共用上設定， `Windows` 用戶端會快取使用者主目錄資料夾下的所有快照 `~snapshot`。

如果下列其中一項為真，則 Windows 用戶端會快取主目錄下的所有快照：

- 使用者可從用戶端離線使用主目錄。

  的內容 `~snapshot` 主目錄中的資料夾會隨附並可供離線使用。

- 使用者可設定資料夾重新導向以重新導向等資料夾 `My Documents` 位於 CIFS 伺服器共用上主目錄的根目錄。

  某些Windows用戶端可能會自動讓重新導向的資料夾離線使用。如果資料夾重新導向至主目錄的根目錄、則會重新導向 `~snapshot` 資料夾包含在快取的離線內容中。

> 應避免將資料夾包含在離線檔案中的離線檔案部署 `~snapshot`。資料夾中的快照 `~snapshot`包含磁碟區上 ONTAP 建立快照的所有資料。因此，建立資料夾的離線複本 `~snapshot`會消耗用戶端上的大量本機儲存空間，在離線檔案同步期間消耗網路頻寬，並增加同步離線檔案所需的時間。

您可以在ONTAP 建立SMB共用時、或隨時修改現有的SMB共用時、指定四個離線檔案設定之一、使用支援的還原CLI來設定離線檔案。手動離線檔案支援為預設設定。

關於這項工作

設定離線檔案支援時、您可以選擇下列四種離線檔案設定之一：

設定	說明
`none`	不允許Windows用戶端快取此共用區上的任何檔案。
`manual`	可讓Windows用戶端上的使用者手動選取要快取的檔案。
`documents`	允許Windows用戶端快取使用者用於離線存取的使用者文件。
`programs`	允許Windows用戶端快取使用者用於離線存取的程式。即使共用可用、用戶端仍可在離線模式下使用快取的程式檔案。

您只能選擇一個離線檔案設定。如果您修改現有SMB共用區上的離線檔案設定、新的離線檔案設定會取代原始設定。其他現有的SMB共用組態設定和共用內容不會移除或取代。它們會一直有效、直到明確移除或變更為止。

步驟

1. 執行適當的行動：

如果您要設定離線檔案於…	輸入命令…
新的SMB共用區	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -offline-files {none
manual	documents
programs}`	現有的SMB共用區
`vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files {none	manual
documents	programs}`

2. 確認 SMB 共用組態正確無誤：`vserver cifs share show -vserver vserver_name -share -name share_name -instance`

範例

下列命令會建立名為「 data1 」的 SMB 共用、並將離線檔案設為 `documents`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -comment "Offline files" -offline-files documents

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: documents
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

下列命令會將離線檔案設定變更為、以修改名為「 data1 」的現有 SMB 共用 `manual` 以及新增檔案和目錄模式建立遮罩的值：

```
cluster1::> vserver cifs share modify -vserver vs1 -share-name data1
-offline-files manual -file-umask 644 -dir-umask 777

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
          CIFS Server NetBIOS Name: VS1
                             Path: /data1
                  Share Properties: oplocks
                                    browsable
                                    changenotify
                Symlink Properties: enable
           File Mode Creation Mask: 644
      Directory Mode Creation Mask: 777
                   Share Comment: Offline files
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相關資訊

新增或刪除現有共享的共享屬性

使用電腦管理 **MMC** 設定 **ONTAP SMB** 共享上的離線文件支持

如果您想要允許使用者在本機快取檔案以供離線使用、您可以使用電腦管理MMC（Microsoft管理主控台）來設定離線檔案支援。

步驟

1. 若要在Windows伺服器上開啟MMC、請在Windows檔案總管中、以滑鼠右鍵按一下本機電腦的圖示、然後選取*管理*。
2. 在左側面板上、選取*電腦管理*。
3. 選取*「行動*」>*「連線到另一台電腦*」。

   「選取電腦」對話方塊隨即出現。

4. 輸入CIFS伺服器名稱、或按一下*瀏覽*以尋找CIFS伺服器。

   如果CIFS伺服器名稱與儲存虛擬機器（SVM）主機名稱相同、請輸入SVM名稱。如果CIFS伺服器名稱與SVM主機名稱不同、請輸入CIFS伺服器名稱。

5. 按一下「確定」。
6. 在主控台樹狀目錄中、按一下「系統工具」>「共用資料夾」。
7. 按一下*共享*。
8. 在結果窗格中、以滑鼠右鍵按一下共用區。
9. 按一下*「內容」*。

   顯示所選共用的內容。

10. 在*一般*索引標籤中、按一下*離線設定*。

    「離線設定」對話方塊隨即出現。

11. 視需要設定離線可用度選項。
12. 按一下「確定」。

使用漫遊設定檔、將使用者設定檔集中儲存在與**SVM**相關的**SMB**伺服器上

了解如何使用漫遊設定檔集中儲存 **ONTAP SMB** 使用者設定檔

支援將Windows漫遊設定檔儲存在與儲存虛擬機器（SVM）相關聯的CIFS伺服器上。ONTAP設定使用者漫遊設定檔可為使用者帶來許多優勢、例如無論使用者登入的位置為何、自動提供資源可用度。漫遊設定檔也能簡化使用者設定檔的管理。

漫遊使用者設定檔具有下列優點：

- 自動資源可用度

  當使用者登入網路上執行Windows 8、Windows 7、Windows 2000或Windows XP的任何電腦時、就會自動使用該使用者的唯一設定檔。使用者不需要在網路上使用的每部電腦上建立設定檔。

- 簡化電腦更換作業

  由於使用者的所有設定檔資訊都是在網路上個別維護、因此使用者的設定檔可以輕鬆下載到新的替換電腦上。當使用者第一次登入新電腦時、使用者設定檔的伺服器複本會複製到新電腦。

相關資訊

- 了解如何使用離線檔案來快取檔案以供離線使用
- 了解如何使用資料夾重新導向在伺服器上儲存數據

了解使用漫遊 **ONTAP SMB** 設定檔的要求

在您將Microsoft的漫遊設定檔搭配CIFS伺服器使用之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援此功能。

版本需求**ONTAP**

支援漫遊設定檔。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的漫遊設定檔。

Windows用戶端需求

在使用者使用漫遊設定檔之前、Windows用戶端必須支援此功能。

如需哪些Windows用戶端支援漫遊設定檔的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

透過 Active Directory 使用者和電腦 MMC 設定漫遊 ONTAP SMB 設定檔

如果您想要在使用者登入網路上的任何電腦時、自動讓使用者的設定檔可供使用、您可以透過Active Directory使用者和電腦MMC嵌入式管理單元來設定漫遊設定檔。如果您在 Windows Server 上設定漫遊設定檔、則可以使用 Active Directory 管理中心。

步驟

1. 在 Windows 伺服器上、開啟 Active Directory 使用者和電腦 MMC （或 Windows 伺服器上的 Active Directory 管理中心）。
2. 找出您要設定漫遊設定檔的使用者。
3. 在使用者上按一下滑鼠右鍵、然後按一下「內容」。
4. 在 * 設定檔 * 索引標籤上、輸入您要儲存使用者漫遊設定檔之共用的設定檔路徑、然後輸入 `%username%`。

   例如、設定檔路徑可能如下： `\\vs1.example.com\profiles\%username%`。使用者第一次登入時、 `%username%` 以使用者名稱取代。

   > 在路徑中 `\\vs1.example.com\profiles\%username%`、 `profiles` 是儲存虛擬機器（ SVM ） VS1 上具有「 Everyone 完全控制」權限的共用名稱。

5. 按一下「確定」。

使用資料夾重新導向將資料儲存在SMB伺服器上

了解如何使用資料夾重新導向在 ONTAP SMB 伺服器上儲存數據

支援Microsoft資料夾重新導向、可讓使用者或系統管理員將本機資料夾路徑重新導向至CIFS伺服器上的位置。ONTAP即使資料儲存在SMB共用區、重新導向的資料夾仍會顯示為儲存在本機Windows用戶端上。

資料夾重新導向主要是針對已部署主目錄、且想要維持與現有主目錄環境相容性的組織。

- `Documents`、 `Desktop`和 `Start Menu` 是您可以重新導向的資料夾範例。
- 使用者可以從Windows用戶端重新導向資料夾。
- 系統管理員可以在Active Directory中設定GPO、集中設定及管理資料夾重新導向。
- 如果系統管理員已設定漫遊設定檔、資料夾重新導向可讓系統管理員將使用者資料與設定檔資料分開。

- 系統管理員可以同時使用資料夾重新導向和離線檔案、將本機資料夾的資料儲存區重新導向至CIFS伺服器、同時允許使用者在本機快取內容。

相關資訊

- 了解如何使用離線檔案來快取檔案以供離線使用
- 使用漫遊設定檔、將使用者設定檔集中儲存在與SVM相關的CIFS伺服器上

了解使用 **ONTAP SMB** 資料夾重新導向的要求

在您將Microsoft的資料夾重新導向用於CIFS伺服器之前、您必須先知道ONTAP 哪些版本的支援功能、以及哪些Windows用戶端支援此功能。

版本需求**ONTAP**

支援Microsoft資料夾重新導向。ONTAP

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援Microsoft在所有SMB版本上的資料夾重新導向。

Windows用戶端需求

在使用者使用Microsoft的資料夾重新導向之前、Windows用戶端必須支援此功能。

如需哪些Windows用戶端支援資料夾重新導向的最新資訊、請參閱互通性對照表。

"mysupport.netapp.com/matrix"

使用 **Windows** 屬性配置 **ONTAP SMB** 資料夾重新導向

您可以使用Windows內容視窗來設定資料夾重新導向。使用此方法的優點是Windows使用者可以設定資料夾重新導向、而無需SVM管理員的協助。

步驟

1. 在Windows檔案總管中、以滑鼠右鍵按一下您要重新導向至網路共用的資料夾。
2. 按一下*「內容」*。

   顯示所選共用的內容。

3. 在*捷徑*索引標籤中、按一下*目標*、然後指定您要重新導向所選資料夾的網路位置路徑。

   例如、如果您要將資料夾重新導向至 `data` 對應至之主目錄中的資料夾 `Q:\`、請指定 `Q:\data` 成為目標。

4. 按一下「確定」。

   如需設定離線資料夾的詳細資訊、請參閱Microsoft TechNet資源庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解如何使用 **SMB 2.x** 從 **Windows** 用戶端存取 **ONTAP ~snapshot** 目錄

您使用 SMB 2.x 從 Windows 用戶端存取目錄的方法與 SMB 1.0 使用的方法 `~snapshot` 不同。使用 SMB 2.x 連線成功存取儲存在快照中的資料時，您必須瞭解如何存取 `~snapshot`目錄。

SVM 管理員可控制 Windows 用戶端上的使用者是否可以檢視及存取 `~snapshot` 啟用或停用、即可在共用上建立目錄 `showsnapshot` 使用 vserver CIFS 共用內容系列中的命令來共用內容。

> `showsnapshot`停用共用內容時，使用 `SMB 2.x` 的 `Windows` 用戶端上的使用者無法檢視 `~snapshot`目錄，也無法存取目錄中的快照，即使手動輸入目錄路徑或目錄中的特定快照 `~snapshot`也 `~snapshot`一樣。

當 `showsnapshot` 共用內容已啟用、使用 SMB 2.x 的 Windows 用戶端上的使用者仍無法檢視 `~snapshot` 目錄位於共享區的根目錄、或位於共享區根目錄下的任何交會或目錄內。不過、連線至共用之後、使用者就可以存取隱藏的 `~snapshot` 手動附加目錄 `\~snapshot` 至共用路徑的結尾。隱藏的 `~snapshot` 目錄可從兩個入口點存取：

- 位於共用區的根目錄
- 在共享空間的每個交會點

隱藏的 `~snapshot` 無法從共享區內的非連接子目錄存取目錄。

範例

使用下列範例所示的組態、 Windows 用戶端上有 SMB 2.x 連線至「 'eng' 」共用的使用者可以存取 `~snapshot` 手動附加目錄 `\~snapshot` 到共享區根目錄和路徑中每個連接點的共享路徑。隱藏的 `~snapshot` 目錄可從下列三個路徑存取：

- `\\vs1\eng\~snapshot`
- `\\vs1\eng\projects1\~snapshot`
- `\\vs1\eng\projects2\~snapshot`

```
cluster1::> volume show -vserver vs1 -fields volume,junction-path
vserver volume       junction-path
------- ------------ ----------------------------------------
vs1     vs1_root      /
vs1     vs1_vol1      /eng
vs1     vs1_vol2      /eng/projects1
vs1     vs1_vol3      /eng/projects2

cluster1::> vserver cifs share show
Vserver  Share   Path     Properties    Comment  ACL
-------- ------  -------  ----------    -------- ----------
vs1      eng     /eng     oplocks       -        Everyone / Full Control
                          changenotify
                          browsable
                          showsnapshot
```

使用舊版還原檔案和資料夾

了解如何使用先前的版本還原 **ONTAP SMB** 檔案和資料夾

使用 Microsoft 舊版的功能適用於支援某種形式的快照並啟用快照的檔案系統。Snapshot技術是ONTAP 不可或缺的一部分。使用者可以使用 Microsoft 舊版功能，從 Windows 用戶端的快照中復原檔案和資料夾。

舊版功能可讓使用者瀏覽快照或從快照還原資料，而無需儲存管理員介入。無法設定舊版。此功能一律啟用。如果儲存管理員已在共用上提供快照，則使用者可以使用舊版來執行下列工作：

- 恢復意外刪除的檔案。
- 從意外覆寫檔案中恢復。
- 在工作時比較檔案版本。

儲存在快照中的資料是唯讀的。使用者必須將檔案複本儲存到其他位置、才能對檔案進行任何變更。快照會定期刪除；因此，如果使用者想要無限期保留舊版檔案，則需要建立舊版檔案的複本。

使用 **Microsoft** 早期版本的 **ONTAP SMB** 需求

在您將舊版CIFS伺服器搭配使用之前、您必須先知道ONTAP 哪些版本的支援哪些版本的支援、以及哪些Windows用戶端支援哪些版本。您也需要知道快照設定需求。

版本需求**ONTAP**

支援舊版。

SMB傳輸協定版本需求

對於儲存虛擬機器（SVM）、ONTAP 支援所有SMB版本上的舊版。

Windows用戶端需求

使用者必須先支援此功能，才能使用舊版存取快照中的資料。

如需哪些Windows用戶端支援舊版的最新資訊、請參閱互通性對照表。

"NetApp 互通性對照表工具"

快照設定需求

若要使用舊版存取快照中的資料，啟用的快照原則必須與包含資料的磁碟區相關聯，用戶端必須能夠存取快照資料，而且快照必須存在。

使用 **Windows Previous Versions** 標籤檢視和管理 **ONTAP SMB** 快照數據

Windows 用戶端機器上的使用者可以使用 Windows 內容視窗上的舊版索引標籤來還原快照中儲存的資料，而不需要儲存虛擬機器（ SVM ）管理員介入。

關於這項工作

如果管理員已在包含共享區的磁碟區上啟用快照，且管理員將共用區設定為顯示快照，則您只能使用「舊版」索引標籤來檢視和管理儲存在 SVM 上資料快照中的資料。

步驟

1. 在Windows檔案總管中、顯示儲存在CIFS伺服器上之資料對應磁碟機的內容。
2. 以滑鼠右鍵按一下您要檢視或管理其快照的對應網路磁碟機中的檔案或資料夾。
3. 按一下*「內容」*。

   隨即顯示所選檔案或資料夾的內容。

4. 按一下*舊版*索引標籤。

   所選檔案或資料夾的可用快照清單會顯示在資料夾版本：方塊中。列出的快照會以快照名稱首碼和建立時間戳記來識別。

5. 在「資料夾版本：」方塊中、以滑鼠右鍵按一下您要管理的檔案或資料夾複本。
6. 執行適當的行動：

如果您想要...	請執行下列動作...
檢視該快照的資料	按一下「開啟」。
從該快照建立資料複本	按一下 * 複本 * 。

   快照中的資料是唯讀的。如果您想要修改「舊版」索引標籤中所列的檔案和資料夾、則必須將您要修改的檔案和資料夾複本儲存到可寫入的位置、並對複本進行修改。

7. 管理完快照資料後，按一下 * 確定 * ，關閉 * 內容 * 對話方塊。

   如需使用 [舊版] 索引標籤檢視及管理快照資料的詳細資訊，請參閱 Microsoft TechNet Library 。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

確定 **ONTAP SMB** 快照是否可供先前版本使用

只有在已啟用的快照原則套用至包含共用的磁碟區，且磁碟區組態允許存取快照時，才能從「舊版」索引標籤檢視快照。判斷快照可用度有助於協助使用者存取舊版。

步驟

1. 判斷共用資料所在的磁碟區是否已啟用自動快照，以及用戶端是否可存取快照目錄： `volume show -vserver vserver-name -volume volume-name -fields vserver,volume,snapdir-access,snapshot-policy,snapshot-count`

   輸出會顯示與磁碟區相關的快照原則，是否啟用用戶端快照目錄存取，以及可用快照的數量。

2. 判斷是否已啟用相關的快照原則： `volume snapshot policy show -policy policy-name`
3. 列出可用的快照： `volume snapshot show -volume volume_name`

   如需設定及管理快照原則和快照排程的詳細資訊，請參閱"資料保護"。

範例

以下範例顯示與名為「 data1 」的磁碟區相關的快照原則資訊，該磁碟區包含「 data1 」上的共用資料和可用快照。

```
cluster1::> volume show -vserver vs1 -volume data1 -fields
vserver,volume,snapshot-policy,snapdir-access,snapshot-count
vserver  volume snapdir-access snapshot-policy snapshot-count
-------- ------ -------------- --------------- --------------
vs1      data1  true           default         10

cluster1::> volume snapshot policy show -policy default
Vserver: cluster1
                   Number of Is
Policy Name        Schedules Enabled Comment
------------------ --------- ------- ---------------------------------
default                     3 true    Default policy with hourly, daily &
weekly schedules.
    Schedule         Count     Prefix                  SnapMirror Label
    ---------------- -----     ----------------------- -------------------
    hourly               6     hourly                  -
    daily                2     daily                   daily
    weekly               2     weekly                  weekly

cluster1::> volume snapshot show -volume data1
                                                                 ---Blocks---
Vserver  Volume  Snapshot                  State        Size Total% Used%
-------- ------- ------------------------- -------- -------- ------ -----
vs1      data1
                 weekly.2012-12-16_0015    valid       408KB     0%    1%
                 daily.2012-12-22_0010     valid       420KB     0%    1%
                 daily.2012-12-23_0010     valid       192KB     0%    0%
                 weekly.2012-12-23_0015    valid       360KB     0%    1%
                 hourly.2012-12-23_1405    valid       196KB     0%    0%
                 hourly.2012-12-23_1505    valid       196KB     0%    0%
                 hourly.2012-12-23_1605    valid       212KB     0%    0%
                 hourly.2012-12-23_1705    valid       136KB     0%    0%
                 hourly.2012-12-23_1805    valid       200KB     0%    0%
                 hourly.2012-12-23_1905    valid       184KB     0%    0%
```

相關資訊

- 建立快照配置以啟用先前版本的訪問
- "資料保護"

建立 ONTAP SMB 快照配置以啟用先前版本的訪問

只要啟用用戶端對快照的存取權，且快照存在，舊版功能就永遠可用。如果您的快照組態不符合這些需求，您可以建立一個快照組態，

步驟

1. 如果包含您要允許舊版存取之共用區的磁碟區沒有相關聯的快照原則，請將快照原則與磁碟區建立關聯，然後使用命令加以啟用 `volume modify`。

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

2. 使用命令將選項設定為 `true`，以 `-snap-dir`啟用快照的存取 `volume modify`。

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

3. 使用和 `volume snapshot policy show`命令確認已啟用快照原則，且已啟用快照目錄的存取 `volume show`。

   深入瞭解 `volume show`及 `volume snapshot policy show` "指令參考資料ONTAP"。

   如需設定及管理快照原則和快照排程的詳細資訊，請參閱"資料保護"。

相關資訊

"資料保護"

了解如何還原包含 **ONTAP SMB** 連線點的先前版本目錄

使用舊版還原包含連接點的資料夾時、請務必謹記某些準則。

使用舊版還原具有子資料夾的子資料夾時、還原可能會因為而失敗 `Access Denied` 錯誤。

您可以使用來判斷您嘗試還原的資料夾是否包含連接 `vol show` 命令 `-parent` 選項。您也可以使用 `vserver security trace` 建立檔案與資料夾存取問題詳細記錄的命令。

相關資訊

在NAS命名空間中建立及管理資料磁碟區

部署SMB伺服器型服務

管理主目錄

了解如何在 **ONTAP SMB** 伺服器上啟用動態主目錄

利用支援支援的主目錄、您可以根據連線的使用者及一組變數、設定對應至不同目錄的SMB共用區。ONTAP您可以使用幾個主目錄參數來設定一個共用區、以定義使用者在入口點（共享區）和主目錄（SVM上的目錄）之間的關係、而非為每個使用者建立個別的共用區。

以訪客使用者身分登入的使用者沒有主目錄、也無法存取其他使用者的主目錄。有四個變數可決定使用者如何對應至目錄：

- 共享名稱

  這是您建立的共用名稱、使用者可連線至該共用。您必須設定此共用的主目錄屬性。

  共用名稱可以使用下列動態名稱：

- `%w` （使用者的 Windows 使用者名稱）
- `%d` （使用者的 Windows 網域名稱）
- `%u` （使用者對應的 UNIX 使用者名稱）
  若要讓共用名稱在所有主目錄中都是唯一的、共用名稱必須包含/`%w` 或 `%u` 變動。共用名稱可以同時包含 `%d` 和/`%w` 變數（例如、 `%d/%w`）、或共享區名稱可以包含靜態部分和可變部分（例如 hom_ ）/`%w`）。

- 共享路徑

  這是由共用定義的相對路徑、因此會與其中一個共用名稱相關聯、並附加到每個搜尋路徑、以從SVM根目錄產生使用者的完整主目錄路徑。它可以是靜態的（例如、 `home`）、動態（例如、 `%w`）、或兩者的組合（例如、 `eng/%w`）。

- 搜尋路徑

  這是從SVM根目錄開始的一組絕對路徑、您可以指定這些路徑來引導ONTAP 針對主目錄進行搜尋。您可以使用命令來指定一或多個搜尋路徑 `vserver cifs home-directory search-path add`。如果您指定多個搜尋路徑、ONTAP 則在找到有效路徑之前、將會依照指定的順序嘗試這些路徑。如"指令參考資料ONTAP"需詳細 `vserver cifs home-directory search-path add`資訊，請參閱。

- 目錄

  這是您為使用者建立的使用者主目錄。目錄名稱通常是使用者的名稱。您必須在搜尋路徑所定義的其中一個目錄中建立主目錄。

舉例來說、請考慮下列設定：

- 使用者：John Smith
- 使用者網域：Acme
- 使用者名稱：jsmith
- SVM名稱：VS1
- 主目錄共用名稱 #1 ： hom_ `%w` - 共享路徑： `%w`
- 主目錄共用名稱 #2 ： `%w` - 共享路徑： `%d/%w`
- 搜尋路徑 #1 ： `/vol0home/home`
- 搜尋路徑 #2 ： `/vol1home/home`
- 搜尋路徑 #3 ： `/vol2home/home`
- 主目錄： `/vol1home/home/jsmith`

案例 1 ：使用者連線至 `\\vs1\home_jsmith`。這會比對第一個主目錄共用名稱、並產生相對路徑 `jsmith`。ONTAP 現在會搜尋名為的目錄 `jsmith` 依序檢查每個搜尋路徑：

- `/vol0home/home/jsmith` 不存在；請繼續搜尋路徑 #2 。
- `/vol1home/home/jsmith` 存在；因此不會核取搜尋路徑 #3 ；使用者現在已連線至其主目錄。

案例 2 ：使用者連線至 `\\vs1\jsmith`。這會比對第二個主目錄共用名稱、並產生相對路徑 `acme/jsmith`。ONTAP 現在會搜尋名為的目錄 `acme/jsmith` 依序檢查每個搜尋路徑：

- `/vol0home/home/acme/jsmith` 不存在；請繼續搜尋路徑 #2 。
- `/vol1home/home/acme/jsmith` 不存在；請繼續搜尋路徑 #3 。
- `/vol2home/home/acme/jsmith` 不存在；主目錄不存在；因此連線失敗。

主目錄共用

新增 ONTAP SMB 主目錄共享

如果您想要使用SMB主目錄功能、則必須將至少一個共用新增至共用內容中包含的主目錄內容。

關於這項工作

您可以在使用建立共用時建立主目錄共用 `vserver cifs share create` 命令、或者您可以隨時使用將現有共用變更為主目錄共用 `vserver cifs share modify` 命令。

若要建立主目錄共用、您必須包含 `homedirectory` 中的值 `-share-properties` 建立或修改共用時的選項。您可以使用使用者連線至其主目錄時動態擴充的變數來指定共用名稱和共用路徑。您可以在路徑中使用的可用變數有 `%w`、 `%d`和 `%u`，分別對應於 Windows 使用者名稱、網域及對應的 UNIX 使用者名稱。

步驟

1. 新增主目錄共用：
   `vserver cifs share create -vserver` *`vserver_name`* `-share-name` *`share_name`* `-path` *`path`* `-share-properties homedirectory[,…]`

   `-vserver vserver` 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   `-share-name` *`share-name`* 指定主目錄共用名稱。

   除了包含其中一個必要的變數之外、如果共用名稱包含其中一個文字字串 `%w`、 `%u`或 `%d`，您必須在文字字串前面加上 % （百分比）字元，以防止 ONTAP 將文字字串視為變數（例如， `%%w`）。

   - 共用名稱必須包含 `%w` 或 `%u` 變動。
   - 共用名稱也可以包含 `%d` 變數（例如、 `%d/%w`）或共享區名稱中的靜態部分（例如 home1_/`%w`）。
   - 如果系統管理員使用該共用區來連線至其他使用者的主目錄、或是允許使用者連線至其他使用者的主目錄、則動態共用名稱模式的前面必須有一個字首符號（~）。

     。 `vserver cifs home-directory modify` 用於透過設定來啟用此存取 `-is-home-dirs -access-for-admin-enabled` 選項 `true`）或設定進階選項 `-is-home-dirs-access-for -public-enabled` 至 `true`。

   `-path path` 指定主目錄的相對路徑。

`-share-properties homedirectory[,…]` 指定該共用的共用內容。您必須指定 `homedirectory` 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

1. 使用確認您已成功新增主目錄共用 `vserver cifs share show` 命令。

範例

下列命令會建立名為的主目錄共用 `%w`。。 `oplocks`、 `browsable`和 `changenotify` 除了設定之外、還會設定共用內容 `homedirectory` 共用屬性。

此範例不會顯示SVM上所有共用的輸出。輸出被截短。

```
cluster1::> vserver cifs share create -vserver vs1 -share-name %w -path %w
-share-properties oplocks,browsable,changenotify,homedirectory

vs1::> vserver cifs share show -vserver vs1
Vserver     Share     Path          Properties     Comment  ACL
----------- --------- ------------ -------------- -------- -----------
vs1         %w        %w            oplocks        -        Everyone / Full
Control
                                    browsable
                                    changenotify
                                    homedirectory
```

相關資訊

- 新增主目錄搜尋路徑
- 在伺服器上使用自動節點引用的要求和指南
- 管理使用者主目錄的可訪問性

了解主目錄共享的唯一 **ONTAP SMB** 使用者名稱要求

使用建立主目錄共用時、請務必指定唯一的使用者名稱 `%w` （ Windows 使用者名稱）或 `%u` （ UNIX 使用者名稱）可動態產生共用的變數。共用名稱會對應至您的使用者名稱。

靜態共用區名稱和使用者名稱相同時、可能會發生兩個問題：

- 當使用者使用列出叢集上的共用時 `net view` 命令會顯示兩個具有相同使用者名稱的共用。
- 當使用者連線至該共用名稱時、該使用者一律會連線至靜態共用區、而且無法以相同名稱存取主目錄共用區。

例如、有一個名稱為「管理員」的共用區、您有一個「管理員」Windows使用者名稱。如果您建立主目錄共用並連線至該共用區、就會連線至「管理員」靜態共用區、而非「管理員」主目錄共用區。

您可以依照下列任一步驟、以重複的共用名稱來解決此問題：

- 重新命名靜態共用、使其不再與使用者的主目錄共用發生衝突。
- 為使用者提供新的使用者名稱、使其不再與靜態共用名稱衝突。
- 建立 CIFS 主目錄共用時、請使用靜態名稱、例如「 'home' 」、而非使用 `%w` 避免與共用名稱衝突的參數。

了解升級後靜態 **ONTAP SMB** 主目錄共用名稱會發生什麼情況

主目錄共用名稱必須包含 `%w` 或 `%u` 動態變數。您應該瞭ONTAP 解現有靜態主目錄共用名

稱在升級至更新需求的版本的版本時、會發生什麼變化。

如果您的主目錄組態包含靜態共用名稱、而且您升級到ONTAP 了某個版本、靜態主目錄共用名稱將不會變更、而且仍然有效。但是、您無法建立任何不包含的新主目錄共用 `%w` 或 `%u` 變動。

使用者的主目錄共用名稱必須包含其中一個變數、才能確保主目錄組態中的每個共用名稱都是唯一的。如果需要、您可以將靜態主目錄共用名稱變更為包含其中一種的名稱 `%w` 或 `%u` 變動。

新增 **ONTAP SMB** 主目錄搜尋路徑

如果您想要使用ONTAP 支援功能的SMB主目錄、您必須至少新增一個主目錄搜尋路徑。

關於這項工作

您可以使用新增主目錄搜尋路徑 `vserver cifs home-directory search-path add` 命令。

。 `vserver cifs home-directory search-path add` 命令會檢查中指定的路徑 `-path` 命令執行期間的選項。如果指定的路徑不存在、命令會產生訊息、提示您是否要繼續。您可以自行選擇 `y` 或 `n`。如果您選擇 `y` 若要繼續、 ONTAP 會建立搜尋路徑。不過、您必須先建立目錄結構、才能在主目錄組態中使用搜尋路徑。如果您選擇不繼續、則命令會失敗；不會建立搜尋路徑。接著您可以建立路徑目錄結構、然後重新執行 `vserver cifs home-directory search-path add` 命令。

步驟

1. 新增主目錄搜尋路徑： `vserver cifs home-directory search-path add -vserver vserver -path path`
2. 請確認您已使用成功新增搜尋路徑 `vserver cifs home-directory search-path show` 命令。

範例

下列範例新增路徑 `/home1` 移至 SVM VS1 上的主目錄組態。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

vs1::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

下列範例會嘗試新增路徑 `/home2` 移至 SVM VS1 上的主目錄組態。路徑不存在。您可以選擇不繼續。

```
cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home2
Warning: The specified path "/home2" does not exist in the namespace
         belonging to Vserver "vs1".
Do you want to continue? {y|n}: n
```

相關資訊

使用 **%w** 和 **%d** 變數建立 **ONTAP SMB** 主目錄配置

您可以使用建立主目錄組態 `%w` 和 `%d` 變數。然後使用者可以使用動態建立的共用區連線到他們的主共用區。

步驟

1. 建立 qtree 以包含使用者的主目錄： `volume qtree create -vserver vserver_name -qtree -path qtree_path`
2. 驗證 qtree 是否使用正確的安全樣式： `volume qtree show`
3. 如果 qtree 未使用所需的安全樣式、請使用變更安全樣式 `volume qtree security` 命令。
4. 新增主目錄共用： `vserver cifs share create -vserver vserver -share-name %w -path %d/%w -share-properties homedirectory\[,...\]`

   `-vserver vserver` 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   `-share-name %w` 指定主目錄共用名稱。當每位使用者連線至其主目錄時、系統會動態建立共用名稱。ONTAP共用名稱的格式為_windows_user_name_。

   `-path %d/%w` 指定主目錄的相對路徑。當每個使用者連線至其主目錄時、會動態建立相對路徑、其格式為_domain/windows_user_name_。

   `-share-properties homedirectory[,…]+` 指定該共用的共用內容。您必須指定 `homedirectory` 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

5. 使用確認共用具有所需的組態 `vserver cifs share show` 命令。
6. 新增主目錄搜尋路徑： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver` *`vserver-name`* 指定要在其中新增搜尋路徑的啟用 CIFS 的 SVM 。

   `-path` *`path`* 指定搜尋路徑的絕對目錄路徑。

7. 請確認您已使用成功新增搜尋路徑 `vserver cifs home-directory search-path show` 命令。
8. 對於擁有主目錄的使用者、請在qtree或指定包含主目錄的磁碟區中建立對應的目錄。

   例如、如果您使用的路徑建立 qtree `/vol/vol1/users` 而您要建立目錄的使用者名稱是 mydomain\user1 、您可以建立具有下列路徑的目錄： `/vol/vol1/users/mydomain/user1`。

   如果您在上建立一個名為「 'home1' 」的 Volume `/home1`，您可以使用以下路徑建立目錄： `/home1/mydomain/user1`。

9. 確認使用者可以透過對應磁碟機或使用UNC路徑連線、成功連線至主共用區。

   例如、如果使用者 mydomain\user1 想要連線到步驟 8 中建立的 SVM VS1 目錄、則 user1 會使用 UNC 路徑連線 `\\vs1\user1`。

範例

下列範例中的命令會以下列設定建立主目錄組態：

- 共享區名稱為%W.
- 相對主目錄路徑為%d/%w
- 用於包含主目錄的搜尋路徑、 `/home1`，是設定為 NTFS 安全性樣式的磁碟區。
- 組態是在SVM VS1上建立。

當使用者從Windows主機存取其主目錄時、您可以使用此類型的主目錄組態。當使用者從Windows和UNIX主機存取其主目錄時、您也可以使用此類組態、而檔案系統管理員則使用Windows型使用者和群組來控制對檔案系統的存取。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path
%d/%w -share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %w

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %d/%w
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1
```

相關資訊

- 使用%u變數設定主目錄

- 了解其他主目錄配置
- 顯示有關使用者主目錄路徑的信息

使用 **%u** 變數設定 **ONTAP SMB** 主目錄

您可以建立主目錄組態、在其中使用指定共用名稱 `%w` 變數、但您使用 `%u` 可指定主目錄共用的相對路徑的變數。然後使用者可以使用使用Windows使用者名稱所建立的動態共用來連線到他們的主共用區、而不需要知道主目錄的實際名稱或路徑。

步驟

1. 建立 qtree 以包含使用者的主目錄： `volume qtree create -vserver vserver_name -qtree -path qtree_path`
2. 驗證 qtree 是否使用正確的安全樣式： `volume qtree show`
3. 如果 qtree 未使用所需的安全樣式、請使用變更安全樣式 `volume qtree security` 命令。
4. 新增主目錄共用： `vserver cifs share create -vserver vserver -share-name %w -path %u -share-properties homedirectory ,...]`

   `-vserver vserver` 指定要新增搜尋路徑的 CIFS 儲存虛擬機器（ SVM ）。

   `-share-name %w` 指定主目錄共用名稱。當每個使用者連線至其主目錄時、就會動態建立共用名稱、格式為_windows_user_name_。

   > 您也可以使用 `%u` 的變數 `-share-name` 選項。這會建立使用對應UNIX使用者名稱的相對共用路徑。

   `-path %u` 指定主目錄的相對路徑。當每個使用者連線至其主目錄時、會動態建立相對路徑、其格式為_Mapped_UNIX/user_name_。

   > 此選項的值也可以包含靜態元素。例如、 `eng/%u`。

   `-share-properties homedirectory\[,...\]` 指定該共用的共用內容。您必須指定 `homedirectory` 價值。您可以使用以逗號分隔的清單來指定其他共用屬性。

5. 使用確認共用具有所需的組態 `vserver cifs share show` 命令。
6. 新增主目錄搜尋路徑： `vserver cifs home-directory search-path add -vserver vserver -path path`

   `-vserver vserver` 指定要在其中新增搜尋路徑的啟用 CIFS 的 SVM 。

   `-path path` 指定搜尋路徑的絕對目錄路徑。

7. 請確認您已使用成功新增搜尋路徑 `vserver cifs home-directory search-path show` 命令。
8. 如果 UNIX 使用者不存在、請使用建立 UNIX 使用者 `vserver services unix-user create` 命令。

   > 對應Windows使用者名稱的UNIX使用者名稱必須存在、才能對應使用者。

9. 使用下列命令建立 Windows 使用者與 UNIX 使用者的名稱對應： `vserver name-mapping create -vserver vserver_name -direction win-unix -priority integer -pattern windows_user_name -replacement unix_user_name`

   如果已存在將Windows使用者對應至UNIX使用者的名稱對應、則不必執行對應步驟。

   Windows使用者名稱會對應至對應的UNIX使用者名稱。當Windows使用者連線至其主目錄共用時、他們會連線至動態建立的主目錄、其中共用名稱對應於Windows使用者名稱、但不知道該目錄名稱對應於UNIX使用者名稱。

10. 對於擁有主目錄的使用者、請在qtree或指定包含主目錄的磁碟區中建立對應的目錄。

    例如、如果您使用的路徑建立 qtree `/vol/vol1/users` 而您要建立其目錄的使用者對應 UNIX 使用者名稱是「 unixuser1 」、則您可以建立具有下列路徑的目錄： `/vol/vol1/users/unixuser1`。

    如果您在上建立一個名為「 'home1' 」的 Volume `/home1`，您可以使用以下路徑建立目錄： `/home1/unixuser1`。

11. 確認使用者可以透過對應磁碟機或使用UNC路徑連線、成功連線至主共用區。

    例如、如果使用者 mydomain\user1 對應至 UNIX 使用者 unixuser1 、並想要連線至步驟 10 中建立的 SVM VS1 目錄、則 user1 會使用 UNC 路徑進行連線 `\\vs1\user1`。

範例

下列範例中的命令會以下列設定建立主目錄組態：

- 共享區名稱為%W.
- 相對主目錄路徑為%u
- 用於包含主目錄的搜尋路徑、 `/home1`，是設定為 UNIX 安全樣式的 Volume 。
- 組態是在SVM VS1上建立。

當使用者從Windows主機或Windows和UNIX主機存取其主目錄時、您可以使用此類型的主目錄組態、而檔案系統管理員則使用UNIX使用者和群組來控制檔案系統的存取。

```
cluster::> vserver cifs share create -vserver vs1 -share-name %w -path %u
-share-properties oplocks,browsable,changenotify,homedirectory

cluster::> vserver cifs share show -vserver vs1 -share-name %u

                      Vserver: vs1
                        Share: %w
     CIFS Server NetBIOS Name: VS1
                         Path: %u
             Share Properties: oplocks
                               browsable
                               changenotify
                               homedirectory
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster::> vserver cifs home-directory search-path add -vserver vs1 -path
/home1

cluster::> vserver cifs home-directory search-path show -vserver vs1
Vserver     Position Path
----------- -------- -----------------
vs1         1        /home1

cluster::> vserver name-mapping create -vserver vs1 -direction win-unix
-position 5 -pattern user1 -replacement unixuser1

cluster::> vserver name-mapping show -pattern user1
Vserver        Direction Position
-------------- --------- --------
vs1            win-unix  5        Pattern: user1
                               Replacement: unixuser1
```

相關資訊

- 使用 %w 和 %d 變數建立主目錄配置
- 了解其他主目錄配置
- 顯示有關使用者主目錄路徑的信息

了解其他 **ONTAP SMB** 主目錄配置

您可以使用建立其他主目錄組態 `%w`、 `%d`和 `%u` 變數、可讓您自訂主目錄組態以滿足您的需求。

您可以使用共用名稱和搜尋路徑中的變數和靜態字串組合、來建立許多主目錄組態。下表提供一些範例、說明如何建立不同的主目錄組態：

建立時間的路徑 `/vol1/user` 包含主目錄 ...	共用命令...
建立共用路徑 `\\vs1\~win_username` 將使用者導向 `/vol1/user/win_username`	`vserver cifs share create -share-name ~%w -path %w -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 `\\vs1\win_username` 將使用者導向 `/vol1/user/domain/win_username`	`vserver cifs share create -share-name %w -path %d/%w -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 `\\vs1\win_username` 將使用者導向 `/vol1/user/unix_username`	`vserver cifs share create -share-name %w -path %u -share-properties oplocks,browsable,changenotify,homedirectory`
建立共用路徑 `\\vs1\unix_username` 將使用者導向 `/vol1/user/unix_username`	`vserver cifs share create -share-name %u -path %u -share-properties oplocks,browsable,changenotify,homedirectory`

用於管理 **SMB** 搜尋路徑的 **ONTAP** 命令

針對ONTAP SMB主目錄組態、有特定的支援功能可用來管理搜尋路徑。例如、您可以使用命令來新增、移除及顯示搜尋路徑的相關資訊。還有一個命令可用來變更搜尋路徑順序。

如果您想要...	使用此命令...
新增搜尋路徑	`vserver cifs home-directory search-path add`
顯示搜尋路徑	`vserver cifs home-directory search-path show`
變更搜尋路徑順序	`vserver cifs home-directory search-path reorder`

如果您想要...	使用此命令...
移除搜尋路徑	`vserver cifs home-directory search-path remove`

如"指令參考資料ONTAP"需詳細 `vserver cifs home-directory search-path`資訊，請參閱。

顯示有關 **ONTAP SMB** 使用者主目錄路徑的信息

您可以在儲存虛擬機器（SVM）上顯示SMB使用者的主目錄路徑、如果您已設定多個CIFS主目錄路徑、而且想要查看哪個路徑包含使用者的主目錄、就可以使用該路徑。

步驟

1. 使用顯示主目錄路徑 `vserver cifs home-directory show-user` 命令。

```
vserver cifs home-directory show-user -vserver vs1 -username user1
```

```
Vserver      User                 Home Dir Path
-----------  -------------------  ----------------------
vs1          user1                /home/user1
```

相關資訊

管理使用者主目錄的可訪問性

管理 **ONTAP SMB** 使用者主目錄的可存取性

根據預設、使用者的主目錄只能由該使用者存取。如果共用區的動態名稱前面有一個波狀符號（｛cilde｝）、您可以啟用或停用Windows系統管理員或任何其他使用者對使用者主目錄的存取（公共存取）。

開始之前

儲存虛擬機器（SVM）上的主目錄共用必須以動態共用名稱進行設定、並在名稱前面加上一個波狀符號（｛波狀符號｝）。下列案例說明共用命名需求：

主目錄共用名稱	連線至共用區的命令範例
{tilde} %d {tilde} %w	`net use * \\IPaddress\~domain~user/u:credentials`
{tilde} %w	`net use * \\IPaddress\~user/u:credentials`
{tilde} abc {tilde} %w	`net use * \\IPaddress\abc~user/u:credentials`

步驟

1. 執行適當的行動：

如果您要啟用或停用存取使用者主目錄的權限、以便...	輸入下列項目...
Windows系統管理員	`vserver cifs home-directory modify -vserver` *`vserver_name`* `-is-home-dirs -access-for-admin-enabled {true|false}` 預設值為 `true`。
任何使用者（公共存取）	a. 將權限等級設為進階：`set -privilege advanced` b. 啟用或停用存取：`vserver cifs home-directory modify -vserver` *vserver_name* -is-home-dirs -access-for-public-enabled {true

下列範例可讓使用者的主目錄公開存取：

```
set -privilege advanced
vserver cifs home-directory modify -vserver vs1 -is-home-dirs-access-for-public
-enabled true
set -privilege admin
```

相關資訊

顯示有關使用者主目錄路徑的信息

設定SMB用戶端存取UNIX符號連結

了解如何提供 ONTAP SMB 用戶端對 UNIX 符號連結的訪問

符號連結是在UNIX環境中建立的檔案、其中包含對其他檔案或目錄的參照。如果用戶端存取符號連結、用戶端會重新導向至符號連結所指的目標檔案或目錄。支援相對和絕對符號連結、包括連結（與本機檔案系統外部目標的絕對連結）ONTAP 。

支援SMB用戶端追蹤SVM上設定的UNIX符號連結。ONTAP此功能為選用功能、您可以使用在每個共享區的基礎上進行設定 `-symlink-properties` 的選項 `vserver cifs share create` 命令、並提供下列其中一項設定：

- 已啟用讀寫存取權
- 啟用唯讀存取
- 隱藏SMB用戶端的符號連結來停用
- 停用時無法存取SMB用戶端的符號連結

如果您在共用區上啟用符號連結、則相對符號連結無需進一步設定即可運作。

如果您在共用區上啟用符號連結、絕對符號連結將無法立即運作。您必須先在符號連結的UNIX路徑與目的地SMB路徑之間建立對應。建立絕對符號連結對應時、您可以指定它是本機連結或_widelink_；widelinks可以是其他儲存裝置上檔案系統的連結、也可以是連結、連結到同ONTAP 一個支援相同效能的系統上、分別裝載於不

同SVM中的檔案系統。建立wideink時、必須包含用戶端要追蹤的資訊、也就是建立重新分析點、讓用戶端探索目錄交會點。如果您在本機共用區以外建立檔案或目錄的絕對符號連結、但將「局部」設為「本機」、ONTAP則不允許存取目標。

> 如果用戶端嘗試刪除本機符號連結（絕對或相對）、則只會刪除符號連結、而不會刪除目標檔案或目錄。但是、如果用戶端嘗試刪除widelink、可能會刪除實際的目標檔案或是welink參照的目錄。由於用戶端可以明確開啟SVM外部的目標檔案或目錄、並將其刪除、所以無法控制此功能。ONTAP

- 重新分析點與**ONTAP** 不支援檔案系統服務

  _重新 分析點_是NTFS檔案系統物件、可選擇性地與檔案一起儲存在磁碟區上。重新分析點可讓SMB用戶端在使用NTFS樣式磁碟區時、接收增強或延伸的檔案系統服務。重新分析點由標準標記組成、可識別重新分析點的類型、以及SMB用戶端可擷取的重新分析點內容、以供用戶端進一步處理。在可用於延伸檔案系統功能的物件類型中、ONTAP 使用重新分析點標籤來實作NTFS符號連結和目錄交會點的支援。無法瞭解重新分析點內容的SMB用戶端只要忽略它、而不提供重新分析點可能啟用的延伸檔案系統服務。

- 目錄交會點與**ONTAP** 符號連結的支援

  目錄交會點是檔案系統目錄結構中的位置、可用來參照儲存檔案的替代位置、無論是在不同路徑（符號連結）或是個別儲存設備（widelinks）上。支援SMB的伺服器將目錄交會點以重新分析點的形式提供給Windows用戶端、讓有能力的用戶端在經過目錄交會點時、能夠從無法修復的點內容。ONTAP ONTAP因此、他們可以瀏覽並連線到不同的路徑或儲存裝置、就像它們是同一個檔案系統的一部分。

- *使用重新分析點選項*來啟用wideink支援

  此 `-is-use-junctions-as-reparse-points-enabled`選項在 ONTAP 9 中預設為啟用。由於並非所有 SMB 用戶端都支援 Widelink，因此啟用該資訊的選項可根據每個協定版本進行設定。這允許管理員同時適應受支援和不受支援的 SMB 用戶端。您必須啟用該選項 `-widelink-as-reparse-point-versions`對於使用寬連結存取共享的每個用戶端協定；預設值為 SMB1。

相關資訊

- "Windows 備份應用程式和 Unix 風格的符號連結"
- "Microsoft文件：重新分析點"

為 **ONTAP SMB** 存取配置 **UNIX** 符號連結時的限制

在設定UNIX符號連結進行SMB存取時、您必須注意特定限制。

限制	說明
45	使用CIFS伺服器名稱的FQDN時、可以指定的CIFS伺服器名稱長度上限。 您也可以將CIFS伺服器名稱指定為僅限15個字元的NetBios名稱。
80	共用名稱的最大長度。

限制	說明
256	在建立符號連結或修改現有符號連結的 UNIX 路徑時、您可以指定的 UNIX 路徑長度上限。 UNIX 路徑必須以「」開頭/`" (slash) and end with a “/” 。開頭和結尾的斜槓都會算作256個字元限制的一部分。
256	當您建立符號連結或修改現有符號連結的 CIFS 路徑時、可以指定的 CIFS 路徑長度上限。 CIFS 路徑必須以「」開頭/`" (slash) and end with a “/” 。開頭和結尾的斜槓都會算作256個字元限制的一部分。

相關資訊

為共享建立符號連結映射

控制 **ONTAP SMB** 伺服器上的自動 **DFS** 廣告

CIFS伺服器選項可控制連線至共用時、如何向SMB用戶端通告DFS功能。由於當用戶端透過SMB存取符號連結時、使用的是DFS轉介、因此您應該瞭解停用或啟用此選項時會有什麼影響。ONTAP

CIFS伺服器選項可決定CIFS伺服器是否自動向SMB用戶端通告其具備的DFS功能。根據預設、此選項會啟用、而且CIFS伺服器一律會向SMB用戶端通告它具有DFS-功能（即使連線至停用符號連結存取權的共用區）。如果您想要CIFS伺服器只在連接到已啟用符號連結存取權限的共用時、才向用戶端通告它具有DFS-功能、您可以停用此選項。

您應該注意停用此選項時會發生什麼情況：

- 符號連結的共用組態不變。
- 如果共用參數設定為允許符號連結存取（讀寫存取或唯讀存取）、則CIFS伺服器會將DFS功能通告給連線至該共用的用戶端。

  用戶端連線和符號連結存取不中斷地繼續進行。

- 如果共用參數設定為不允許符號連結存取（停用存取或如果共用參數值為null）、則CIFS伺服器不會向連線至該共用的用戶端通告DFS功能。

  由於用戶端已快取CIFS伺服器可支援的資訊、而且不再廣告、因此在停用CIFS伺服器選項之後、連線至停用符號連結存取的共用區的用戶端、可能無法存取這些共用區。停用此選項之後、您可能需要重新開機連線至這些共用的用戶端、以便清除快取的資訊。

這些變更不適用於SMB 1.0連線。

在 **ONTAP SMB** 共用上設定 **UNIX** 符號連結支持

您可以在建立SMB共用時或隨時修改現有SMB共用時、指定符號連結共用屬性設定、以設定SMB共用上的UNIX符號連結支援。UNIX符號連結支援預設為啟用。您也可以停用共用區上的UNIX符號連結支援。

關於這項工作

設定SMB共用的UNIX符號連結支援時、您可以選擇下列其中一項設定：

設定	說明
`enable` （已過時 * ）	指定啟用符號連結以進行讀寫存取。
`read_only` （已過時 * ）	指定啟用symlink進行唯讀存取。此設定不適用於無線連結。Wielink存取永遠是讀寫的。
`hide` （已過時 * ）	指定SMB用戶端無法看到symlink。
`no-strict-security`	指定用戶端在共用邊界之外追蹤symlink。
`symlinks`	指定在本機啟用symlink以進行讀寫存取。即使使用 CIFS 選項、也不會產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `true`。這是預設設定。
`symlinks-and-widelinks`	指定本機symlink和widelinks以進行讀寫存取。即使使用 CIFS 選項、也會同時為本機 symlink 和 wedelinks 產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `false`。
`disable`	指定停用symlink和widelinks。即使使用 CIFS 選項、也不會產生 DFS 通告 `is-advertise-dfs-enabled` 設為 `true`。
"" （ null 、未設定）	停用共用區上的符號連結。
- （未設定）	停用共用區上的符號連結。

*啟用_、隱藏_和唯讀_參數已過時、未來發行ONTAP 版的更新版可能會移除。

步驟

1. 設定或停用符號連結支援：

如果是...	輸入...
新的SMB共用區	`+vserver cifs share create -vserver vserver_name -share-name share_name -path path -symlink -properties {enable
hide	read-only
""	-
symlinks	symlinks-and-widelinks

如果是...	輸入...
disable},...]+`	現有的SMB共用區
`+vserver cifs share modify -vserver vserver_name -share-name share_name -symlink-properties {enable	hide
read-only	""
-	symlinks
symlinks-and-widelinks	disable},...]+`

2. 確認 SMB 共用組態正確無誤： `vserver cifs share show -vserver vserver_name -share -name share_name -instance`

範例

下列命令會建立名為「 data1 」的 SMB 共用、並將 UNIX 符號連結組態設定為 `enable` ：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data1 -path
/data1 -symlink-properties enable

cluster1::> vserver cifs share show -vserver vs1 -share-name data1
-instance

                          Vserver: vs1
                            Share: data1
         CIFS Server NetBIOS Name: VS1
                             Path: /data1
                Share Properties: oplocks
                                  browsable
                                  changenotify
              Symlink Properties: enable
          File Mode Creation Mask: -
     Directory Mode Creation Mask: -
                   Share Comment: -
                       Share ACL: Everyone / Full Control
    File Attribute Cache Lifetime: -
                     Volume Name: -
                   Offline Files: manual
    Vscan File-Operations Profile: standard
Maximum Tree Connections on Share: 4294967295
       UNIX Group for File Create: -
```

相關資訊

為共享建立符號連結映射

您可以建立SMB共用的UNIX符號連結對應。您可以建立相對符號連結、以參照檔案或資料夾與其父資料夾的相對位置、也可以建立絕對符號連結、以使用絕對路徑來參照檔案或資料夾。

關於這項工作

如果您使用SMB 2.x、就無法從Mac OS X用戶端存取Widgelinks當使用者嘗試從Mac OS X用戶端使用wideinks連線至共用時、嘗試會失敗。不過、如果您使用SMB 1、則可以將wideinks與Mac OS X用戶端搭配使用。

步驟

1. 若要建立 SMB 共用的符號連結對應： `vserver cifs symlink create -vserver virtual_server_name -unix-path path -share-name share_name -cifs-path path [-cifs-server server_name] [-locality {local|free|widelink}] [-home-directory {true|false}]`

   `-vserver virtual_server_name` 指定儲存虛擬機器（ SVM ）名稱。

   `-unix-path path` 指定 UNIX 路徑。UNIX 路徑必須以斜線開頭 (/) 、且必須以斜線結尾 (/) 。

   `-share-name share_name` 指定要對應的 SMB 共用名稱。

   `-cifs-path path` 指定 CIFS 路徑。CIFS 路徑必須以斜線開頭 (/) 、且必須以斜線結尾 (/) 。

   `-cifs-server server_name` 指定 CIFS 伺服器名稱。CIFS伺服器名稱可以指定為DNS名稱（例如mynetwork.cifs.server.com） 、IP位址或NetBios名稱。您可以使用來判斷 NetBIOS 名稱 `vserver cifs show` 命令。如果未指定此選用參數、預設值為本機CIFS伺服器的NetBios名稱。

   `-locality local|free|widelink}` 指定要建立本機連結、免費連結或寬符號連結。本機符號連結會對應至本機SMB共用區。免費的符號連結可以對應到本機SMB伺服器上的任何位置。廣泛的符號連結會對應到網路上的任何SMB共用區。如果您未指定此選用參數、則預設值為 `local` 。

   `-home-directory true false}` 指定目標共用是否為主目錄。即使此參數為選用參數、您仍必須將此參數設為 `true` 當目標共用設定為主目錄時。預設值為 `false` 。

範例

下列命令會在名為VS1的SVM上建立符號連結對應。它有 UNIX 路徑 `/src/` 、 SMB 共享名稱「 'SOURCE' 」 、 CIFS 路徑 `/mycompany/source/`和 CIFS 伺服器 IP 位址 123.123.123.123 、這是一種有線連結。

```
cluster1::> vserver cifs symlink create -vserver vs1 -unix-path /src/
-share-name SOURCE -cifs-path "/mycompany/source/" -cifs-server
123.123.123.123 -locality widelink
```

相關資訊

在共享上配置 UNIX 符號連結支持

用於管理 **SMB** 符號連結映射的 **ONTAP** 命令

有特定ONTAP 的功能可用來管理符號連結對應。

如果您想要...	使用此命令...
建立符號連結對應	`vserver cifs symlink create`
顯示符號連結對應的相關資訊	`vserver cifs symlink show`
修改符號連結對應	`vserver cifs symlink modify`
刪除符號連結對應	`vserver cifs symlink delete`

如"指令參考資料ONTAP"需詳細 `vserver cifs symlink`資訊，請參閱。

ONTAP SMB 伺服器上的 **Windows** 備份應用程式和 **Unix** 樣式符號鏈接

當在 Windows 上執行的備份應用程式遇到 Unix 樣式的符號連結（ symlink ）時、會追蹤連結並備份資料。從 ONTAP 9.15.1 開始、您可以選擇備份 symlinks 而非資料。ONTAP FlexGroup Volume 和 FlexVols 完全支援此功能。

總覽

在您變更 ONTAP 在 Windows 備份作業期間處理符號連結的方式之前、您應該先熟悉這些優點、主要概念和組態選項。

效益

當此功能停用或無法使用時、系統會周遊每個 symlink 、並備份其連結的資料。因此、有時可能會備份不必要的資料、在某些情況下、應用程式可能會在迴圈中結束。備份 symlinks 可避免這些問題。由於 symlink 檔案與大多數情況下的資料相比非常小、因此備份所需的時間較短。由於 IO 作業減少、叢集的整體效能也可以改善。

Windows 伺服器環境

此功能支援在 Windows 上執行的備份應用程式。使用前、您應該先瞭解環境的相關技術層面。

延伸屬性

Windows 支援延伸屬性（ EA ）、這些屬性共同構成與檔案相關的額外中繼資料（選擇性）。這些屬性由多種應用程式使用、例如 Windows Subsystem for Linux 、如所述 "WSL 的檔案權限"。從 ONTAP 讀取資料時、應用程式可以要求每個檔案的延伸屬性。

啟用此功能時、會在延伸屬性中傳回符號連結。因此、備份應用程式必須提供用於儲存中繼資料的標準 EA 支援。部分 Windows 公用程式支援並保留延伸屬性。不過、如果備份軟體不支援備份及還原延伸屬性、則不會保留與每個檔案相關的中繼資料、也無法正確處理符號連結。

Windows 組態

在 Microsoft Windows 伺服器上執行的備份應用程式可獲得特殊權限、讓它們略過一般檔案安全性。這通常是透過將應用程式新增至 Backup Operators 群組來完成。應用程式接著可視需要備份及還原檔案、並執行其他相關

的系統作業。備份應用程式使用的 SMB 傳輸協定有細微的變更、 ONTAP 可以在讀取和寫入資料時偵測到這些變更。

需求

symlink 備份功能有多項需求、包括：

- 您的叢集正在執行 ONTAP 9.15.1 或更新版本。
- 已獲授特殊備份權限的 Windows 備份應用程式。
- 備份應用程式也必須支援延伸屬性、並在備份作業期間要求這些屬性。
- ONTAP symlink 備份功能已針對適用的資料 SVM 啟用。

組態選項

除了 ONTAP CLI 之外、您也可以使用 REST API 來管理此功能。如需詳細資訊、請參閱 "ONTAP REST API 與自動化的新功能" 。決定 ONTAP 處理 Unix 型符號連結的方式的組態、必須針對每個 SVM 分別執行。

啟用 **ONTAP** 中的 **symlink** 備份功能

已使用 ONTAP 9.15.1 將組態選項導入現有的 CLI 命令。您可以使用此選項來啟用或停用 Unix 樣式的 symlink 處理。

開始之前

查看基本 [需求]。此外：

- 能夠將 CLI 權限提升至進階層級。
- 判斷您要修改的資料 SVM 。SVM `vs1` 用於範例命令。

步驟

1. 設定進階權限等級。

```
set privilege advanced
```

2. 啟用 symlink 檔案備份。

```
vserver cifs options modify -vserver vs1 -is-backup-symlink-enabled true
```

使用**BranchCache**快取分公司的**SMB**共用內容

了解如何使用 **BranchCache** 在分公司快取 **ONTAP SMB** 共享內容

Microsoft開發了BranchCache、以便在要求用戶端的本機電腦上快取內容。實施BranchCache可降低廣域網路（WAN）的使用率、並在分公司使用者使用SMB存取儲存在儲存虛擬機器（SVM）上的內容時、提供更佳的存取回應時間。ONTAP

如果您設定了BranchCache、Windows BranchCache用戶端會先從SVM擷取內容、然後快取分公司電腦上的內容。如果分公司中另一個啟用了BranchCache的用戶端要求相同的內容、SVM會先驗證並授權要求的使用者。然後SVM會判斷快取內容是否仍為最新狀態、如果是、則會傳送有關快取內容的用戶端中繼資料。然後用戶端會使用中繼資料、直接從本機快取擷取內容。

相關資訊

了解如何使用離線檔案來快取檔案以供離線使用

要求與準則

了解 **ONTAP SMB BranchCache** 版本支持

您應該知道ONTAP 哪些版本的BranchCache支援哪些版本。

支援BranchCache 1和增強的BranchCache 2：ONTAP

- 在SMB伺服器上為儲存虛擬機器（SVM）設定BranchCache時、您可以啟用BranchCache 1、BranchCache 2或所有版本。

  根據預設、所有版本都會啟用。

- 如果只啟用了BranchCache 2、遠端辦公室Windows用戶端機器必須支援BranchCache 2。

  只有SMB 3.0或更新版本的用戶端支援BranchCache 2。

如需更多關於BranchCache版本的資訊，請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

了解 **ONTAP SMB** 網路協定支援要求

您必須瞭解實作ONTAP 《Sing Sof BranchCache》（英文）的網路傳輸協定需求。

您可以ONTAP 使用SMB 2.1或更新版本、在使用SMB 2.1或更新版本的IPv4和IPv6網路上實作「S21：快取」功能。

參與BranchCache實作的所有CIFS伺服器和分公司機器、都必須啟用SMB 2.1或更新的傳輸協定。SMB 2.1具有允許用戶端參與BranchCache環境的傳輸協定延伸功能。這是支援BranchCache的最低SMB傳輸協定版本。SMB 2.1支援版本BranchCache第1版。

如果您要使用BranchCache第2版、SMB 3.0是支援的最低版本。參與BranchCache 2實作的所有CIFS伺服器和分公司機器、都必須啟用SMB 3.0或更新版本。

如果您的遠端辦公室中有部分用戶端僅支援SMB 2.1、而部分用戶端支援SMB 3.0、您可以在CIFS伺服器上實作一項BranchCache組態、以同時在BranchCache 1和BranchCache 2上提供快取支援。

雖然Microsoft BranchCache功能同時支援使用HTTP / HTTPS和SMB傳輸協定做為檔案存取傳輸協定、ONTAP 但支援使用SMB。

了解 **ONTAP SMB** 和 **Windows** 主機版本需求

在設定BranchCache之前、Windows主機和分公司必須符合特定的版本需求。ONTAP

在設定BranchCache之前、您必須確保ONTAP 叢集和參與的分公司用戶端上的版本支援SMB 2.1或更新版本、並支援BranchCache功能。如果您設定「主控快取」模式、也必須確保您使用支援的主機作為快取伺服器。

下列ONTAP 版本的支援包含BranchCache 1和Windows主機：

- 內容伺服器：儲存虛擬機器（SVM）ONTAP 、含
- 快取伺服器：Windows Server 2008 R2或Windows Server 2012或更新版本
- 對等端點或用戶端：Windows 7 Enterprise、Windows 7 Ultimate、Windows 8、Windows Server 2008 R2或Windows Server 2012或更新版本

下列ONTAP 版本的支援及Windows主機均支援BranchCache 2：

- 內容伺服器：SVM with ONTAP SfSIf
- 快取伺服器：Windows Server 2012或更新版本
- 對等端點或用戶端：Windows 8或Windows Server 2012或更新版本

了解 **ONTAP SMB** 使 **BranchCache** 哈希無效的原因

規劃ONTAP 您的BranchCache組態時、瞭解為什麼不驗證雜湊會有幫助。它可協助您決定應該設定哪種操作模式、並協助您選擇要啟用的共用區。

必須管理BranchCache雜湊、才能確保雜湊有效。ONTAP如果雜湊無效、ONTAP 則在下次要求內容時、如果仍然啟用了BranchCache、則無法驗證雜湊並計算新雜湊。

由於下列原因、導致雜湊失效：ONTAP

- 伺服器金鑰已修改。

  如果伺服器金鑰已修改、ONTAP 則無法驗證雜湊存放區中的所有雜湊。

- 由於已達到BranchCache雜湊存放區的最大大小、因此會從快取中清除雜湊。

  這是可調整的參數、可加以修改以符合您的業務需求。

- 檔案會透過SMB或NFS存取進行修改。
- 已計算雜湊的檔案會使用還原 `snap restore` 命令。
- 包含已啟用 BranchCache 之 SMB 共用的磁碟區會使用還原 `snap restore` 命令。

了解如何選擇 **ONTAP SMB** 雜湊儲存位置

設定BranchCache時、您可以選擇要儲存雜湊的位置、以及雜湊存放區的大小。瞭解在選擇雜湊存放區位置和大小時的準則、有助於在啟用CIFS的SVM上規劃您的BranchCache組態。

- 您應該在允許更新atime的磁碟區上找到雜湊存放區。

  雜湊檔案的存取時間是用來將經常存取的檔案保留在雜湊存放區中。如果停用atime更新、建立時間就會用於此用途。最好使用atime來追蹤經常使用的檔案。

- 您無法將雜湊儲存在唯讀檔案系統上、例如SnapMirror目的地和SnapLock SnapMirror Volume。
- 如果達到雜湊存放區的最大大小、則會清除舊雜湊、以便留出新雜湊的空間。

  您可以增加雜湊存放區的最大大小、以減少從快取排清的雜湊量。

- 如果您儲存雜湊的磁碟區無法使用或已滿、或是叢集內通訊發生問題、導致無法擷取雜湊資訊、則無法使用BranchCache服務。

  磁碟區可能無法使用、因為它離線、或是儲存管理員為雜湊存放區指定新位置。

  這不會造成檔案存取問題。如果存取雜湊存放區受到阻礙、ONTAP 則將Microsoft定義的錯誤傳回給用戶端、這會導致用戶端使用一般SMB讀取要求來要求檔案。

相關資訊

- 在伺服器上設定 BranchCache
- 修改共享上的 BranchCache 配置

了解 **ONTAP SMB BranchCache** 建議

在您設定BranchCache之前、在決定要啟用什麼SMB共用區的時候、您應該謹記一些建議。

在決定要使用哪種操作模式、以及要啟用BranchCache的SMB共用區時、請謹記下列建議：

- 當要遠端快取的資料經常變更時、會降低BranchCache的優點。
- 對於包含檔案內容的共用區而言、具有很大的好處、這些檔案內容可由多個遠端辦公室用戶端重複使用、或是由單一遠端使用者重複存取的檔案內容。
- 請考慮為唯讀內容啟用快取，例如快照和 SnapMirror 目的地中的資料。

設定**BranchCache**

了解 **ONTAP SMB BranchCache** 配置

您可以在SMB伺服器上使用ONTAP flexf命令 來設定BranchCache。若要實作BranchCache、您也必須在要快取內容的分公司設定用戶端、以及選擇性地設定裝載的快取伺服器。

如果您將BranchCache設定為依共用區啟用快取、則必須在要提供BranchCache快取服務的SMB共用區上啟用BranchCache。

配置 **ONTAP SMB BranchCache** 的要求

在滿足某些先決條件之後、您可以設定BranchCache。

在為SVM設定CIFS伺服器上的BranchCache之前、必須符合下列需求：

- 叢集中的所有節點都必須安裝此程式。ONTAP
- CIFS 必須獲得授權、而且必須設定 SMB 伺服器。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。
- 必須設定IPv4或IPv6網路連線。
- 對於BranchCache 1、必須啟用SMB 2.1或更新版本。
- 對於BranchCache 2、必須啟用SMB 3.0、且遠端Windows用戶端必須支援BranchCache 2。

在 **ONTAP SMB** 伺服器上設定 **BranchCache**

您可以設定在每個共用區基礎上提供BranchCache服務。或者、您也可以設定在所有SMB共用區上自動啟用快取。

關於這項工作

您可以在SVM上設定BranchCache。

- 如果您想要針對CIFS伺服器上所有SMB共用區內的所有內容提供快取服務、可以建立All共享區的BranchCache組態。
- 如果您想要針對CIFS伺服器上所選SMB共用區內的內容提供快取服務、可以建立每個共用區的BranchCache組態。

在設定BranchCache時、您必須指定下列參數：

必要參數	說明
*SVM*名稱	以每個SVM為基礎來設定BranchCache。您必須指定要在哪些CIFS型SVM上設定BranchCache服務。
散列存放區路徑	BranchCache雜湊儲存在SVM磁碟區的一般檔案中。您必須指定ONTAP 要將雜湊資料儲存在其中的現有目錄路徑。您必須將BranchCache雜湊路徑設定為可讀寫。不允許使用唯讀路徑，例如快照目錄。您可以將雜湊資料儲存在包含其他資料的磁碟區中、也可以建立獨立的磁碟區來儲存雜湊資料。 如果SVM是SVM災難恢復來源、則雜湊路徑無法位於根磁碟區上。這是因為根磁碟區並未複寫到災難恢復目的地。 雜湊路徑可以包含空白和任何有效的檔案名稱字元。

您可以選擇性地指定下列參數：

選用參數	說明
支援的版本	支援BranchCache 1和2。ONTAP您可以啟用版本1、版本2或兩者。預設為啟用這兩個版本。
雜湊存放區的最大大小_	您可以指定雜湊資料存放區的大小。如果雜湊資料超過此值、ONTAP 則用更新的雜湊來刪除舊的雜湊。雜湊存放區的預設大小為1 GB。如果未以過度積極的方式捨棄雜湊、則會使BranchCache的效能更有效率。如果您判斷雜湊存放區已滿而經常捨棄雜湊、可以修改BranchCache組態來增加雜湊存放區大小。
伺服器金鑰	您可以指定一個伺服器機碼，讓BranchCache服務用來防止用戶端模擬BranchCache伺服器。如果未指定伺服器金鑰、則會在建立BranchCache組態時隨機產生一個金鑰。您可以將伺服器金鑰設定為特定值、以便在多個伺服器為相同檔案提供BranchCache資料時、用戶端可以使用相同伺服器金鑰來自任何伺服器的雜湊。如果伺服器金鑰包含任何空格、則必須以引號括住伺服器金鑰。
操作模式	預設是以每個共用為基礎來啟用BranchCache。 • 若要建立 BranchCache 組態，讓您以每個共用為基礎啟用 BranchCache ，您可以指定此選用參數，也可以指定 `per-share`。 • 若要在所有共用上自動啟用 BranchCache 、您必須將作業模式設定為 `all-shares`。

步驟

1. 視需要啟用SMB 2.1和3.0：
   a. 將權限層級設為進階： `set -privilege advanced`
   b. 檢查設定的 SVM SMB 設定、判斷是否已啟用所有必要的 SMB 版本： `vserver cifs options show -vserver vserver_name`
   c. 如有必要、請啟用 SMB 2.1 ： `vserver cifs options modify -vserver vserver_name -smb2-enabled true`

      命令可同時啟用SMB 2.0和SMB 2.1。

   d. 如有必要、請啟用 SMB 3.0 ： `vserver cifs options modify -vserver vserver_name -smb3-enabled true`
   e. 返回管理權限層級： `set -privilege admin`
2. 設定 BranchCache ： `vserver cifs branchcache create -vserver vserver_name -hash-store-path path [-hash-store-max-size {integer[KB|MB|GB|TB|PB]}] [-versions {v1-enable|v2-enable|enable-all] [-server-key text] -operating-mode {per-share|all-shares}`

指定的雜湊儲存路徑必須存在、而且必須位於SVM管理的磁碟區上。路徑也必須位於可讀寫磁碟區上。如果路徑為唯讀或不存在、則命令會失敗。

如果您想在其他SVM BranchCache組態中使用相同的伺服器機碼、請記錄您輸入的伺服器機碼值。當您顯示有關BranchCache組態的資訊時、不會顯示伺服器機碼。

3. 驗證 BranchCache 組態是否正確： `vserver cifs branchcache show -vserver vserver_name`

範例

下列命令可驗證是否同時啟用SMB 2.1和3.0、並設定BranchCache在SVM VS1的所有SMB共用區上自動啟用快取：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true


cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key" -operating-mode all-shares

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                      Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: all_shares
```

下列命令可驗證是否同時啟用SMB 2.1和3.0、設定在SVM VS1上啟用每個共用區的快取、並驗證BranchCache組態：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled
vserver smb2-enabled smb3-enabled
------- ------------ ------------
vs1     true         true

cluster1::*> set -privilege admin

cluster1::> vserver cifs branchcache create -vserver vs1 -hash-store-path
/hash_data -hash-store-max-size 20GB -versions enable-all -server-key "my
server key"

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

相關資訊

- 了解 BranchCache 版本支持
- 了解如何在遠端辦公室配置 BranchCache
- 建立啟用BranchCache的SMB共用區
- 在現有共享上啟用 BranchCache
- 修改共享上的 BranchCache 配置
- 了解如何停用共用上的 BranchCache
- 刪除共享上的 BranchCache 配置

了解如何在 **ONTAP SMB** 中的遠端辦公室設定 **BranchCache**

在SMB伺服器上設定了BranchCache之後、您必須在用戶端電腦上安裝及設定BranchCache、並選擇性地在遠端辦公室的快取伺服器上進行設定。Microsoft提供在遠端辦公室設定BranchCache的說明。

Microsoft BranchCache網站上有設定分公司用戶端的指示、以及選用快取伺服器以使用BranchCache的指示。

"Microsoft BranchCache文件：新功能"

設定啟用了**BranchCache**的**SMB**共用區

了解如何設定啟用 **BranchCache** 的 **ONTAP SMB** 共享

在SMB伺服器和分公司設定了BranchCache之後、您可以在SMB共用區上啟用內含您要允許分公司用戶端快取內容的BranchCache。

您可以在SMB伺服器上的所有SMB共用區上啟用「BranchCache快取」、或是以每個共用區為基礎來啟用「BranchCache快取」。

- 如果您以每共用區為基礎來啟用BranchCache、您可以在建立共用區或修改現有共用區時啟用BranchCache。

  如果您啟用現有SMB共用區的快取、ONTAP 只要您在該共用區上啟用了「BranchCache」、就會立即開始運算雜湊、並將中繼資料傳送給要求內容的用戶端。

- 如果隨後在該共用區上啟用了BranchCache、則任何與共用區有SMB連線的用戶端都不會獲得BranchCache支援。

  此版本可在SMB工作階段設定時、針對共用區通告BranchCache支援。ONTAP啟用了BranchCache之後、已建立工作階段的用戶端必須中斷連線並重新連線、才能使用此共用區的快取內容。

> ⓘ 如果SMB共用區上的BranchCache後來停用、ONTAP 則停止傳送中繼資料給要求的用戶端。需要資料的用戶端會直接從內容伺服器（SMB伺服器）擷取資料。

建立啟用 **BranchCache** 的 **ONTAP SMB** 共享

您可以在建立共用時、透過設定在 SMB 共用上啟用 BranchCache `branchcache` 共用屬性。

關於這項工作

- 如果在SMB共用區上啟用了BranchCache、則共用區必須將離線檔案組態設定為手動快取。

  這是您建立共用時的預設設定。

- 您也可以在建立啟用了BranchCache的共用時指定其他選用的共用參數。
- 您可以設定 `branchcache` 即使在儲存虛擬機器（ SVM ）上未設定和啟用 BranchCache 、也會在共用上顯示內容。

  不過、如果您想要共用區提供快取內容、則必須在SVM上設定及啟用BranchCache。

- 因為使用時並未套用預設共用屬性至共用 `-share-properties` 參數、除了、您還必須指定要套用至共用的所有其他共用屬性 `branchcache` 使用以逗號分隔的清單來共用屬性。
- 如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。

步驟

1. 建立啟用 BranchCache 的 SMB 共用區：

```
vserver cifs share create -vserver vserver_name -share-name share_name -path
path -share-properties branchcache[,…]
```

2. 使用確認 SMB 共用上的 BranchCache 共用屬性已設定 `vserver cifs share show` 命令。

範例

下列命令會建立一個已啟用 BranchCache 的 SMB 共用，名稱為「 dATA 」，路徑為 `/data` 在 SVM VS1 上。根據預設，離線檔案設定為 `manual`：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name data -path
/data -share-properties branchcache,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name data
                      Vserver: vs1
                        Share: data
     CIFS Server NetBIOS Name: VS1
                         Path: /data
            Share Properties: branchcache
                              oplocks
                              browsable
                              changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: data
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相關資訊

在單一共用上停用 BranchCache

在現有 **ONTAP SMB** 共用上啟用 **BranchCache**

您可以新增、在現有的 SMB 共用上啟用 BranchCache `branchcache` 將屬性共用至現有的共用屬性清單。

關於這項工作

- 如果在SMB共用區上啟用了BranchCache、則共用區必須將離線檔案組態設定為手動快取。

  如果現有共用的離線檔案設定未設定為手動快取、您必須修改共用區來設定。

- 您可以設定 `branchcache` 即使在儲存虛擬機器（ SVM ）上未設定和啟用 BranchCache 、也會在共用上顯示內容。

不過、如果您想要共用區提供快取內容、則必須在SVM上設定及啟用BranchCache。

- 當您新增時 `branchcache` 共用屬性、現有的共用設定和共用屬性都會保留。

  會將BranchCache共用屬性新增至現有的共用屬性清單。如"指令參考資料ONTAP"需詳細 `vserver cifs share properties add`資訊，請參閱。

步驟

1. 如有必要、請設定離線檔案共用設定以手動快取：
   a. 使用來判斷離線檔案共用設定 `vserver cifs share show` 命令。
   b. 如果未將離線檔案共用設定設為手動、請將其變更為所需的值： `vserver cifs share modify -vserver vserver_name -share-name share_name -offline-files manual`
2. 在現有的 SMB 共用上啟用 BranchCache ： `vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties branchcache`
3. 確認已在 SMB 共用上設定 BranchCache 共用屬性： `vserver cifs share show -vserver vserver_name -share-name share_name`

範例

下列命令會在路徑為的現有 SMB 共用「 'data2 」上啟用 BranchCache `/data2` 在 SVM VS1 上：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              showsnapshot
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties add  -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              showsnapshot
                              changenotify
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

相關資訊

- 新增或刪除現有共享的共享屬性
- 在單一共用上停用 BranchCache

管理及監控**BranchCache**組態

修改 ONTAP SMB 共用上的 BranchCache 配置

您可以修改SVM上的BranchCache服務組態、包括變更雜湊存放區目錄路徑、雜湊存放區最大目錄大小、作業模式、以及支援哪些版本的BranchCache。您也可以增加包含雜湊存放區的磁碟區大小。

步驟

1. 執行適當的行動：

如果您想要...	輸入下列項目...
修改雜湊存放區目錄大小	`vserver cifs branchcache modify -vserver vserver_name -hash-store-max-size {integer[KB
MB	GB
TB	PB]}`
增加包含雜湊存放區的磁碟區大小	`volume size -vserver vserver_name -volume volume_name -new-size new_size[k
m	g
t]` 如果包含雜湊儲存區的磁碟區已滿、您可能可以增加磁碟區的大小。您可以將新的Volume大小指定為數字、然後再指定單位。 深入瞭解 "管理FlexVol 功能"	修改雜湊存放區目錄路徑
`vserver cifs branchcache modify -vserver vserver_name -hash-store-path path -flush-hashes {true	false}` 如果SVM是SVM災難恢復來源、則雜湊路徑無法位於根磁碟區上。這是因為根磁碟區並未複寫到災難恢復目的地。  BranchCache雜湊路徑可以包含空白和任何有效的檔案名稱字元。  如果您修改雜湊路徑、 `-flush-hashes` 是必要參數、可指定 ONTAP 是否要清除原始雜湊儲存位置的雜湊。您可以為設定下列值 `-flush-hashes` 參數：  如果您指定 **`true`**， **ONTAP** 會刪除原始位置的雜湊，並在啟用 **BranchCache** 的用戶端提出新要求時，在新位置建立新的雜湊。 如果您指定 `false`，則不會清除雜湊。 + 在這種情況下、您可以選擇稍後再重複使用現有的雜湊、方法是將雜湊存放區路徑變更回原始位置。

如果您想要...	輸入下列項目...
變更操作模式	`vserver cifs branchcache modify -vserver vserver_name -operating-mode {per-share
all-shares	disable}` 修改操作模式時、請注意下列事項： 設定**SMB**工作階段時、會針對共用區通告**BranchCache**支援**ONTAP** 。 啟用了BranchCache之後、已建立工作階段的用戶端必須中斷連線並重新連線、才能使用此共用區的快取內容。
變更支援的BranchCache版本	`vserver cifs branchcache modify -vserver vserver_name -versions {v1-enable
v2-enable	enable-all}`

2. 使用驗證組態變更 `vserver cifs branchcache show` 命令。

顯示有關 **ONTAP SMB** 共享上的 **BranchCache** 配置的信息

您可以在儲存虛擬機器（SVM）上顯示有關BranchCache組態的資訊、這些資訊可在驗證組態或在修改組態之前判斷目前設定時使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示...	輸入此命令...
關於所有SVM上的BranchCache組態的摘要資訊	`vserver cifs branchcache show`
有關特定SVM組態的詳細資訊	`vserver cifs branchcache show -vserver` *`vserver_name`*

範例

下列範例顯示SVM VS1上的BranchCache組態相關資訊：

```
cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
  Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

變更 **ONTAP SMB BranchCache** 伺服器金鑰

您可以修改儲存虛擬機器（SVM）上的BranchCache組態、並指定不同的伺服器金鑰、藉此變更BranchCache伺服器金鑰。

關於這項工作

您可以將伺服器金鑰設定為特定值、以便在多個伺服器為相同檔案提供BranchCache資料時、用戶端可以使用相同伺服器金鑰來自任何伺服器的雜湊。

變更伺服器金鑰時、您也必須清除雜湊快取。在清除雜湊之後、ONTAP 當啟用了BranchCache的用戶端發出新要求時、會建立新的雜湊。

步驟

1. 使用下列命令變更伺服器金鑰： `vserver cifs branchcache modify -vserver vserver_name -server-key text -flush-hashes true`

   設定新的伺服器金鑰時、您也必須指定 `-flush-hashes` 並將值設為 `true`。

2. 使用驗證 BranchCache 組態是否正確 `vserver cifs branchcache show` 命令。

範例

下列範例設定新的伺服器金鑰、其中包含空格並清除SVM VS1上的雜湊快取：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -server-key "new
vserver secret" -flush-hashes true

cluster1::> vserver cifs branchcache show -vserver vs1

                                    Vserver: vs1
            Supported BranchCache Versions: enable_all
                       Path to Hash Store: /hash_data
            Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
          CIFS BranchCache Operating Modes: per_share
```

相關資訊

在指定的 **ONTAP SMB** 路徑上預先計算 **BranchCache** 哈希

您可以將BranchCache服務設定為預先計算單一檔案、目錄或目錄結構中所有檔案的雜湊。如果您想要在關閉非尖峰時段內、針對啟用了BranchCache的共用區中的資料運算雜湊、這項功能就很有幫助。

關於這項工作

如果您想在顯示雜湊統計資料之前收集資料範例、則必須使用 `statistics start` 和選用 `statistics stop` 命令。

- 您必須指定要預先計算雜湊的儲存虛擬機器（SVM）和路徑。
- 您也必須指定是否要以循環方式計算雜湊。
- 如果您想要以遞迴方式計算雜湊、則BranchCache服務會在指定路徑下遍歷整個目錄樹狀結構、並針對每個符合條件的物件來計算雜湊。

  詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

步驟

1. 視需要預先運算雜湊：

如果您想要預先計算雜湊...	輸入命令...
單一檔案或目錄	`vserver cifs branchcache hash-create -vserver vserver_name -path path -recurse false`
以循環方式處理目錄結構中的所有檔案	`vserver cifs branchcache hash-create -vserver vserver_name -path absolute_path -recurse true`

2. 使用驗證正在計算雜湊 `statistics` 命令：

   a. 顯示的統計資料 `hashd` 所需 SVM 執行個體上的物件： `statistics show -object hashd -instance vserver_name`

   b. 重複執行命令、確認所建立的雜湊數量增加。

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

範例

下列範例會在路徑上建立雜湊 `/data` 以及 SVM VS1 上所有包含的檔案和子目錄：

```
cluster1::> vserver cifs branchcache hash-create -vserver vs1 -path /data
-recurse true

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       85
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -

cluster1::> statistics show -object hashd -instance vs1
Object: hashd
Instance: vs1
Start-time: 9/6/2012 19:09:54
End-time: 9/6/2012 19:11:15
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_created                                       92
    branchcache_hash_files_replaced                                 0
    branchcache_hash_rejected                                       0
    branchcache_hash_store_bytes                                    0
    branchcache_hash_store_size                                     0
    instance_name                                                 vs1
    node_name                                                   node1
    node_uuid
                               11111111-1111-1111-1111-111111111111
    process_name                                                    -
```

相關資訊

- "效能監控設定"

從 ONTAP SMB SVM BranchCache 哈希存儲中刷新哈希

您可以清除儲存虛擬機器（SVM）上的BranchCache雜湊存放區中的所有快取雜湊。如果您已變更分公司的BranchCache組態、這項功能就很有用。例如、如果您最近將快取模式從分散式快取重新設定為託管式快取模式、就會想要清除雜湊存放區。

關於這項工作

在清除雜湊之後、ONTAP 當啟用了BranchCache的用戶端發出新要求時、會建立新的雜湊。

步驟

1. 清除 BranchCache 雜湊存放區的雜湊： `vserver cifs branchcache hash-flush -vserver` *`vserver_name`*

   ```
   vserver cifs branchcache hash-flush -vserver vs1
   ```

顯示 ONTAP SMB BranchCache 統計訊息

您可以顯示BranchCache統計資料、以識別快取效能的表現、判斷您的組態是否提供快取內容給用戶端、並判斷是否刪除雜湊檔案、以留出空間來儲存較新的雜湊資料。

關於這項工作

。 `hashd` 統計資料物件包含提供有關 BranchCache 雜湊統計資訊的計數器。。 `cifs` 統計資料物件包含提供與 BranchCache 相關活動之統計資訊的計數器。您可以在進階權限層級收集及顯示這些物件的相關資訊。

步驟

1. 將權限層級設為進階： `set -privilege advanced`

   ```
   cluster1::> set -privilege advanced

   Warning: These advanced commands are potentially dangerous; use them
   only when directed to do so by support personnel.
   Do you want to continue? {y|n}: y
   ```

2. 使用顯示與 BranchCache 相關的計數器 `statistics catalog counter show` 命令。

   ```
   cluster1::*> statistics catalog counter show -object hashd

   Object: hashd
       Counter                     Description
       --------------------------
   ----------------------------------------------
       branchcache_hash_created    Number of times a request to generate
                                   BranchCache hash for a file succeeded.
       branchcache_hash_files_replaced
                                   Number of times a BranchCache hash file
   ```

```
was
                                deleted to make room for more recent
hash
                                data. This happens if the hash store
size is
                                exceeded.
    branchcache_hash_rejected   Number of times a request to generate
                                BranchCache hash data failed.
    branchcache_hash_store_bytes
                                Total number of bytes used to store hash
data.
    branchcache_hash_store_size Total space used to store BranchCache
hash
                                data for the Vserver.
    instance_name               Instance Name
    instance_uuid               Instance UUID
    node_name                   System node name
    node_uuid                   System node id
9 entries were displayed.

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
-------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    avg_junction_depth          Average number of junctions crossed by
SMB
                                and SMB2 path-based commands
    branchcache_hash_fetch_fail Total number of times a request to fetch
hash
                                data failed. These are failures when
                                attempting to read existing hash data.
It
                                does not include attempts to fetch hash
data
                                that has not yet been generated.
    branchcache_hash_fetch_ok   Total number of times a request to fetch
hash
```

```
                                    data succeeded.
    branchcache_hash_sent_bytes Total number of bytes sent to clients
                                    requesting hashes.
    branchcache_missing_hash_bytes
                                    Total number of bytes of data that had
to be
                                    read by the client because the hash for
that
                                    content was not available on the server.
    ....Output truncated....
```

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

3. 使用收集與 BranchCache 相關的統計資料 `statistics start` 和 `statistics stop` 命令。

```
cluster1::*> statistics start -object cifs -vserver vs1 -sample-id 11
Statistics collection is being started for Sample-id: 11

cluster1::*> statistics stop -sample-id 11
Statistics collection is being stopped for Sample-id: 11
```

詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

4. 使用顯示收集的 BranchCache 統計資料 `statistics show` 命令。

```
cluster1::*> statistics show -object cifs -counter
branchcache_hash_sent_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0
    branchcache_hash_sent_bytes                                     0

cluster1::*> statistics show -object cifs -counter
branchcache_missing_hash_bytes -sample-id 11

Object: cifs
Instance: vs1
Start-time: 12/26/2012 19:50:24
End-time: 12/26/2012 19:51:01
Cluster: cluster1

    Counter                                                     Value
    -------------------------------- --------------------------------
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
    branchcache_missing_hash_bytes                                  0
```

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

5. 返回管理權限層級： `set -privilege admin`

```
cluster1::*> set -privilege admin
```

相關資訊

- 顯示統計資料
- "效能監控設定"
- "統計開始"
- "統計停止"

了解 ONTAP SMB 對 BranchCache 群組原則物件的支持

支援BranchCache群組原則物件（GPO）、可集中管理某些BranchCache組態參數。ONTAP有兩個GPO用於BranchCache：「BranchCache GPO的雜湊發佈」和「BranchCache GPO的雜湊版本支援」。

- *《BranchCache GPO*雜湊》發佈

  BranchCache GPO 的雜湊發佈會對應到 `-operating-mode` 參數。當發生GPO更新時、此值會套用至群組原則所套用之組織單位（OU）內的儲存虛擬機器（SVM）物件。

- *支援BranchCache GPO *的雜湊版本

  BranchCache GPO 的雜湊版本支援對應到 `-versions` 參數。當發生GPO更新時、此值會套用至群組原則套用至的組織單位內所包含的SVM物件。

相關資訊

了解如何將群組原則物件套用至 SMB 伺服器

顯示有關 ONTAP SMB BranchCache 群組原則物件的信息

您可以顯示有關CIFS伺服器的群組原則物件（GPO）組態資訊、以判斷是否為CIFS伺服器所屬的網域定義了BranchCache GPO、如果是、允許的設定為何。您也可以決定是否將BranchCache GPO設定套用至CIFS伺服器。

關於這項工作

即使在CIFS伺服器所屬的網域中定義了GPO設定、但不一定會套用至包含CIFS型儲存虛擬機器（SVM）的組織單位（OU）。套用的GPO設定是套用至CIFS型SVM的所有已定義GPO的子集。透過GPO套用的BranchCache設定會覆寫透過CLI套用的設定。

步驟

1. 使用顯示 Active Directory 網域的已定義 BranchCache GPO 設定 `vserver cifs group-policy show-defined` 命令。

   此範例不會顯示命令的所有可用輸出欄位。輸出被截短。

```
cluster1::> vserver cifs group-policy show-defined -vserver vs1

Vserver: vs1
----------------------------
       GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication for Mode BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]
```

2. 使用顯示套用至 CIFS 伺服器的 BranchCache GPO 設定 `vserver cifs group-policy show-applied` 命令。」

此範例不會顯示命令的所有可用輸出欄位。輸出被截短。

```
cluster1::> vserver cifs group-policy show-applied -vserver vs1

Vserver: vs1
----------------------------
     GPO Name: Default Domain Policy
       Level: Domain
      Status: enabled
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
  [...]

    GPO Name: Resultant Set of Policy
       Level: RSOP
  Advanced Audit Settings:
      Object Access:
          Central Access Policy Staging: failure
  Registry Settings:
      Refresh Time Interval: 22
      Refresh Random Offset: 8
      Hash Publication Mode for BranchCache: per-share
      Hash Version Support for BranchCache: version1
 [...]
```

相關資訊

- 在伺服器上啟用或停用 GPO 支援
- "Vserver CIFS群組原則顯示定義"
- "已套用Vserver CIFS群組原則"

停用SMB共用區上的BranchCache

了解如何在 **ONTAP SMB** 共用上停用 **BranchCache**

如果您不想在某些SMB共用區上提供BranchCache快取服務、但稍後可能想要在這些共用區上提供快取服務、可以逐一停用BranchCache。如果您已將BranchCache設定為在所有共用區上提供快取功能、但想要暫時停用所有快取服務、您可以修改BranchCache組態、以停止在所有共用區上自動快取。

如果SMB共用區上的BranchCache在第一次啟用後即停用、ONTAP 則停止傳送中繼資料給要求的用戶端。需要

資料的用戶端會直接從內容伺服器（儲存虛擬機器（SVM）上的CIFS伺服器）擷取資料。

相關資訊

了解如何設定啟用 BranchCache 的共享

在單一 ONTAP SMB 共用上停用 BranchCache

如果您不想在先前提供快取內容的某些共用區上提供快取服務、可以停用現有SMB共用區上的BranchCache。

步驟

1. 輸入下列命令：`vserver cifs share properties remove -vserver vserver_name -share -name share_name -share-properties branchcache`

   會移除BranchCache共用內容。其他已套用的共用內容仍會維持有效。

範例

下列命令會在名為「data2」的現有SMB共用區上停用BranchCache：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
                              branchcache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
data2 -share-properties branchcache

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data2
            Share Properties: oplocks
                              browsable
                              changenotify
                              attributecache
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

停止所有 **ONTAP SMB** 共享上的自動緩存

如果您的BranchCache組態自動啟用每個儲存虛擬機器（SVM）上所有SMB共用區的快取、您可以修改BranchCache組態、停止自動快取所有SMB共用區的內容。

關於這項工作

若要停止在所有SMB共用區上自動快取、請將「BranchCache」作業模式變更為「每個共用快取」。

步驟

1. 設定 BranchCache 以停止所有 SMB 共用上的自動快取： `vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
2. 驗證 BranchCache 組態是否正確： `vserver cifs branchcache show -vserver vserver_name`

範例

下列命令會變更儲存虛擬機器（SVM、先前稱為Vserver）VS1上的BranchCache組態、以停止所有SMB共用區上的自動快取：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
per-share

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: per_share
```

停用或啟用**SVM**上的**BranchCache**

了解在 **ONTAP SMB** 伺服器上停用或重新啟用 **BranchCache** 時會發生什麼情況

如果您先前已設定了BranchCache、但不想讓分公司用戶端使用快取內容、可以停用CIFS伺服器上的快取功能。您必須知道停用BranchCache時會發生什麼情況。

停用BranchCache時ONTAP 、無法再計算雜湊或將中繼資料傳送至要求的用戶端。不過、檔案存取不會中斷。其後、啟用BranchCache的用戶端要求中繼資料資訊以供其存取內容時ONTAP 、會以Microsoft定義的錯誤回應、導致用戶端傳送第二個要求、要求提供實際內容。為了回應內容要求、CIFS伺服器會傳送儲存在儲存虛擬機器（SVM）上的實際內容。

在CIFS伺服器上停用了BranchCache之後、SMB共用區不會通告BranchCache功能。若要存取新SMB連線上的資料、用戶端會進行一般讀取SMB要求。

您可以隨時在CIFS伺服器上重新啟用BranchCache。

- 由於停用BranchCache時並未刪除雜湊存放區、ONTAP 所以只要所要求的雜湊仍然有效、即可在重新啟

用BranchCache後、在回覆雜湊要求時使用儲存的雜湊。

- 在停用BranchCache期間，任何已建立SMB連線至啟用了BranchCache的共用區的用戶端，如果隨後重新啟用了BranchCache，則不會取得BranchCache支援。

  這是因為ONTAP 在設定SMB工作階段時、會針對共用區通告BranchCache支援。在停用了BranchCache的情況下、建立已啟用BranchCache之共用區工作階段的用戶端、必須中斷連線並重新連線、才能使用此共用區的快取內容。

> 如果您不想在CIFS伺服器上停用BranchCache之後儲存雜湊存放區、可以手動刪除它。如果重新啟用了BranchCache、您必須確定雜湊存放區目錄存在。重新啟用BranchCache之後、啟用BranchCache的共用區會通告BranchCache功能。支援BranchCache的用戶端在提出新要求時、會建立新的雜湊。ONTAP

在 **ONTAP SMB** 共用上停用或啟用 **BranchCache**

您可以將 BranchCache 作業模式變更為、以停用儲存虛擬機器（ SVM ）上的 BranchCache `disabled`。您可以隨時啟用BranchCache、只要將作業模式變更為每個共用區提供BranchCache服務、或自動為所有共用區提供。

步驟

1. 執行適當的命令：

如果您想要...	然後輸入下列內容...
停用BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode disable`
啟用每個共用區的BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode per-share`
啟用所有共用區的BranchCache	`vserver cifs branchcache modify -vserver vserver_name -operating-mode all-shares`

2. 確認已使用所需的設定來設定 BranchCache 作業模式： `vserver cifs branchcache show -vserver vserver_name`

範例

下列範例停用SVM VS1上的BranchCache：

```
cluster1::> vserver cifs branchcache modify -vserver vs1 -operating-mode
disable

cluster1::> vserver cifs branchcache show -vserver vs1

                                Vserver: vs1
          Supported BranchCache Versions: enable_all
                     Path to Hash Store: /hash_data
          Maximum Size of the Hash Store: 20GB
Encryption Key Used to Secure the Hashes: -
        CIFS BranchCache Operating Modes: disable
```

刪除SVM上的BranchCache組態

了解刪除 ONTAP SMB 共用上的 BranchCache 配置時會發生什麼

如果您先前已設定了BranchCache、但不想讓儲存虛擬機器（SVM）繼續提供快取內容、可以刪除CIFS伺服器上的BranchCache組態。您必須知道刪除組態時會發生什麼事。

當您刪除組態時、ONTAP S什麼 會從叢集移除該SVM的組態資訊、然後停止BranchCache服務。您可以選擇ONTAP 是否應刪除SVM上的雜湊存放區。

刪除BranchCache組態不會中斷啟用BranchCache的用戶端存取。其後、啟用BranchCache的用戶端要求現有SMB連線上已快取內容的中繼資料資訊時ONTAP 、由於Microsoft定義的錯誤、導致用戶端傳送第二個要求、要求提供實際內容。為了回應內容要求、CIFS伺服器會傳送儲存在SVM上的實際內容

在刪除BranchCache組態之後、SMB共用區不會通告BranchCache功能。若要存取先前未使用新SMB連線快取的內容、用戶端會進行一般讀取SMB要求。

刪除 ONTAP SMB 共用上的 BranchCache 配置

您用於刪除儲存虛擬機器（SVM）上的BranchCache服務的命令、會因您要刪除或保留現有雜湊而有所不同。

步驟

1. 執行適當的命令：

如果您想要...	然後輸入下列內容...
刪除BranchCache組態並刪除現有的雜湊	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes true`
刪除BranchCache組態、但保留現有的雜湊	`vserver cifs branchcache delete -vserver vserver_name -flush-hashes false`

範例

下列範例會刪除SVM VS1上的BranchCache組態、並刪除所有現有的雜湊：

```
cluster1::> vserver cifs branchcache delete -vserver vs1 -flush-hashes
true
```

了解恢復時 **ONTAP SMB BranchCache** 會發生什麼情況

請務必瞭解ONTAP 當您將不支援BranchCache的版本還原為版本時、會發生什麼情況。

- 當您回復ONTAP 到不支援BranchCache的版本時、SMB共用區不會向啟用BranchCache的用戶端通告BranchCache功能、因此用戶端不會要求雜湊資訊。

  而是使用一般SMB讀取要求來要求實際內容。為了回應內容要求、 SMB 伺服器會傳送儲存虛擬機器（ SVM ）上儲存的實際內容。

- 當主控雜湊存放區的節點還原至不支援BranchCache的版本時、儲存管理員需要使用還原期間列印的命令、手動還原BranchCache組態。

  此命令會刪除BranchCache組態和雜湊。

  還原完成後、儲存管理員可視需要手動刪除包含雜湊存放區的目錄。

相關資訊

刪除共享上的 BranchCache 配置

提升**Microsoft**遠端複製效能

了解 **ONTAP SMB** 伺服器上的 **Microsoft** 遠端複製效能改進

Microsoft卸載資料傳輸（ODX）也稱為_copy offload_、可在相容的儲存裝置內或之間直接傳輸資料、而無需透過主機電腦傳輸資料。

支援適用於SMB與SAN傳輸協定的ODX。ONTAP來源可以是CIFS伺服器或LUN、目的地可以是CIFS伺服器或LUN。

在非ODX檔案傳輸中、資料會從來源讀取、並透過網路傳輸到用戶端電腦。用戶端電腦會透過網路將資料傳輸回目的地。總而言之、用戶端電腦會從來源讀取資料、然後寫入目的地。使用ODX檔案傳輸時、資料會直接從來源複製到目的地。

由於ODX卸載複本是直接在來源與目的地儲存設備之間執行、因此效能優勢顯著。實現的效能效益包括加快來源與目的地之間的複製時間、降低用戶端上的資源使用率（CPU、記憶體）、以及降低網路I/O頻寬使用率。

對於SMB環境、此功能只有在用戶端和儲存伺服器均支援SMB 3.0和ODX功能時才能使用。對於SAN環境、此功能僅在用戶端和儲存伺服器均支援ODX功能時才可使用。支援ODX並自動且透明地啟用ODX的用戶端電腦、可在移動或複製檔案時使用卸載檔案傳輸。無論您是透過Windows檔案總管拖放檔案、還是使用命令列檔案複製命令、或是用戶端應用程式啟動檔案複製要求、都會使用ODX。

相關資訊

- 了解如何透過使用自動定位提供自動節點推薦來提高客戶端回應時間
- "Microsoft Hyper-V和SQL Server的SMB組態"

了解 **ONTAP SMB** 伺服器上的 **ODX**

ODX複本卸載使用權杖型機制、在啟用ODX的CIFS伺服器內或之間讀取和寫入資料。CIFS伺服器不會透過主機路由傳送資料、而是傳送代表資料的小Token給用戶端。ODX用戶端會將該權杖呈現給目的地伺服器、然後再將該權杖所代表的資料從來源傳輸到目的地。

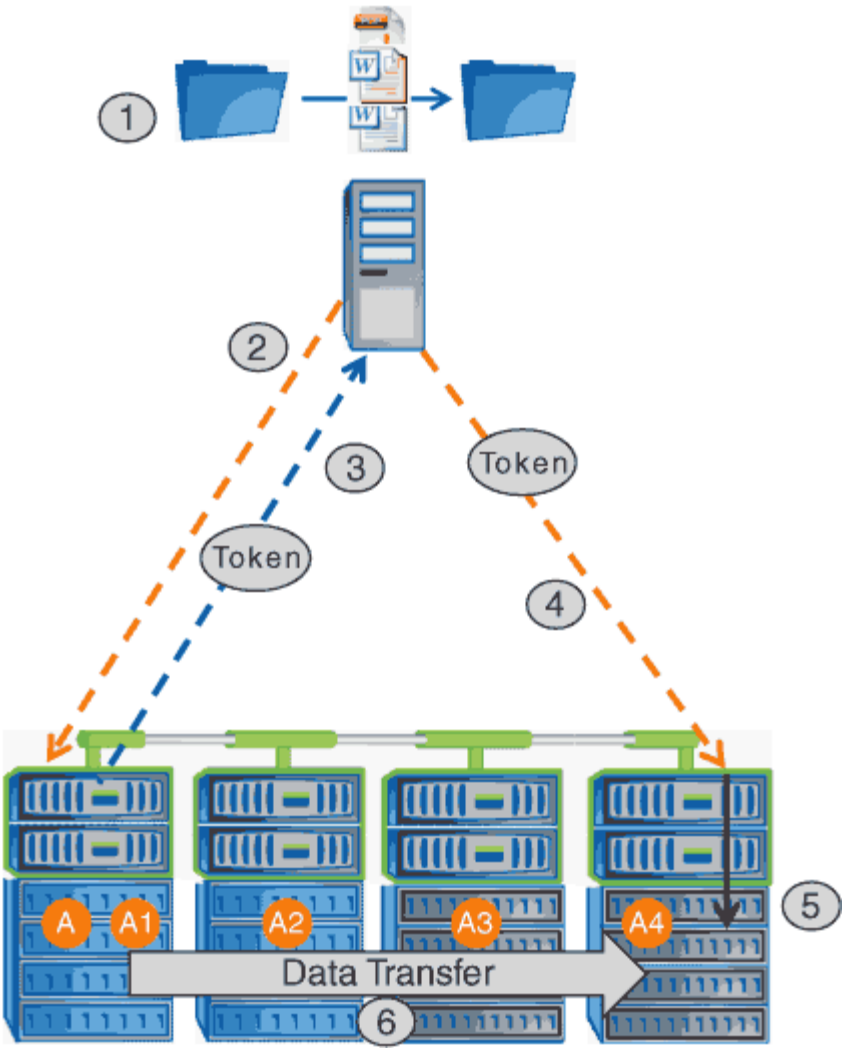
當ODX用戶端得知CIFS伺服器具備ODX功能時、它會開啟來源檔案、並從CIFS伺服器要求權杖。開啟目的地檔案之後、用戶端會使用權杖指示伺服器將資料直接從來源複製到目的地。

來源與目的地可以位於相同的儲存虛擬機器（SVM）或不同的SVM上、視複製作業的範圍而定。

此權杖可做為資料的時間點表示。例如、當您在儲存位置之間複製資料時、代表資料區段的權杖會傳回要求的用戶端、用戶端會將該用戶端複製到目的地、因此不需要透過用戶端複製基礎資料。

支援代表8 MB資料的權杖。ONTAP使用多個權杖執行大於8 MB的ODX複本、每個權杖代表8 MB的資料。

下圖說明ODX複製作業的相關步驟：



1. 使用者可以使用Windows檔案總管、命令列介面、或是虛擬機器移轉的一部分、或是應用程式啟動檔案複本或移動、來複製或移動檔案。
2. 具備ODX功能的用戶端會自動將此傳輸要求轉譯為ODX要求。

   傳送至CIFS伺服器的ODX要求包含權杖要求。
3. 如果在CIFS伺服器上啟用ODX、而且連線是透過SMB 3.0、則CIFS伺服器會產生權杖、這是資料在來源上的邏輯表示。
4. 用戶端會收到代表資料的權杖、並隨寫入要求一起傳送至目的地CIFS伺服器。

   這是唯一透過網路從來源複製到用戶端、然後從用戶端複製到目的地的資料。
5. 權杖會傳送至儲存子系統。
6. SVM會在內部執行複本或移動。

   如果複製或移動的檔案大於8 MB、則需要多個權杖才能執行複本。視需要執行步驟2至6以完成複本。

如果ODX卸載複本發生故障、複本或移動作業會回復為複本或移動作業的傳統讀取和寫入。同樣地、如果目的地CIFS伺服器不支援ODX或ODX已停用、則複製或移動作業會回溯到複製或移動作業的傳統讀取和寫入。

在 **ONTAP SMB** 伺服器上使用 **ODX** 的要求

在您使用ODX卸載儲存虛擬機器（SVM）的複本之前、您必須先瞭解某些需求。

版本需求**ONTAP**

發行版支援ODX進行複本卸載。ONTAP

SMB版本需求

- 支援ODX搭配SMB 3.0及更新版本。ONTAP
- 必須在CIFS伺服器上啟用SMB 3.0、才能啟用ODX：
  - 如果尚未啟用ODX、啟用ODX也會啟用SMB 3.0。
  - 停用SMB 3.0也會停用ODX。

Windows伺服器與用戶端需求

在使用ODX卸載複本之前、Windows用戶端必須支援此功能。

- "NetApp 互通性對照表"包含支援的 Windows 用戶端的最新資訊。

Volume需求

- 來源磁碟區至少必須為1.25 GB。
- 如果您使用壓縮磁碟區、壓縮類型必須是可調適的、而且只支援8K大小的壓縮群組。

  不支援次要壓縮類型。

在 **ONTAP SMB** 伺服器上使用 **ODX** 的指南

在使用ODX進行複本卸載之前、您必須先瞭解準則。例如、您需要知道可以使用ODX的磁碟區類型、而且需要瞭解叢集內和叢集間ODX的考量。

Volume準則

- 您無法使用ODX進行下列Volume組態的複本卸載：
  - 來源Volume大小低於1.25 GB

    磁碟區大小必須大於或等於1.25 GB、才能使用ODX。
  - 唯讀磁碟區

    ODX不適用於位於負載共享鏡像或SnapMirror或SnapVault 目的地Volume中的檔案和資料夾。
  - 如果來源Volume未進行重複資料刪除
- ODX複本僅支援叢集內複本。

  您無法使用ODX將檔案或資料夾複製到其他叢集中的磁碟區。

其他準則

- 在SMB環境中、若要使用ODX進行複本卸載、檔案必須大於或等於256 KB。

  較小的檔案會使用傳統的複製作業來傳輸。

- ODX複製卸載會在複製程序中使用重複資料刪除技術。

  如果您不想在複製或移動資料時於SVM磁碟區上執行重複資料刪除、則應停用該SVM上的ODX複本卸載。

- 執行資料傳輸的應用程式必須寫入以支援ODX。

  支援ODX的應用程式作業包括：

  - Hyper-V 管理作業，例如建立及轉換虛擬硬碟（ VHD ），管理快照，以及在虛擬機器之間複製檔案
  - Windows檔案總管作業
  - Windows PowerShell複製命令
  - Windows命令提示字元複製命令

    Windows命令提示字元的Robocopy支援ODX。

    應用程式必須在支援ODX的Windows伺服器或用戶端上執行。

+
如需Windows伺服器和用戶端上支援的ODX應用程式的詳細資訊、請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

ONTAP SMB 伺服器上 **ODX** 的用例

您應該瞭解在SVM上使用ODX的使用案例、以便判斷ODX在何種情況下可為您提供效能優勢。

支援ODX的Windows伺服器和用戶端使用複本卸載做為在遠端伺服器上複製資料的預設方法。如果Windows伺服器或用戶端不支援ODX、或ODX複本卸載在任何時間點都失敗、則複本或移動作業會回溯到複本或移動作業的傳統讀取和寫入。

下列使用案例支援使用ODX複本和移動：

- Volume內

  來源與目的地檔案或LUN位於同一個磁碟區內。

- 磁碟區間、相同節點、相同SVM

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料歸同一個SVM所有。

- 磁碟區間、不同節點、相同SVM

來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料歸同一個SVM所有。

- SVM之間、相同節點

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料由不同的SVM擁有。

- SVM之間、不同節點

  來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料由不同的SVM擁有。

- 叢集間

  來源和目的地LUN位於不同的磁碟區、位於不同的叢集節點上。這僅適用於SAN、不適用於CIFS。

還有一些特殊使用案例：

- 藉由ONTAP 採用流通不整的ODX技術、您可以使用ODX在SMB共享區與FC或iSCSI附加虛擬磁碟機之間複製檔案。

  您可以使用Windows檔案總管、Windows CLI或PowerShell、Hyper-V或其他支援ODX的應用程式、使用ODX複製卸載功能在SMB共用區和連線LUN之間順暢地複製或移動檔案、前提是SMB共用區和LUN位於同一個叢集上。

- Hyper-V針對ODX複製卸載提供了一些額外的使用案例：

  - 您可以使用ODX複本卸載傳遞搭配Hyper-V、在虛擬硬碟（VHD）檔案內或之間複製資料、或在同一個叢集內的對應SMB共用區和連接的iSCSI LUN之間複製資料。

    如此一來、從客體作業系統的複本就能傳遞到基礎儲存設備。

  - 建立固定大小的VHD時、ODX會使用已知的零權杖、以零初始化磁碟。
  - 如果來源與目的地儲存設備位於同一個叢集、則ODX複本卸載可用於虛擬機器儲存移轉。

> 若要利用ODX複本卸載傳遞與Hyper-V的使用案例、來賓作業系統必須支援ODX、而來賓作業系統的磁碟必須是支援ODX的儲存設備（SMB或SAN）所支援的SCSI磁碟。客體作業系統上的IDE磁碟不支援ODX傳遞。

在 **ONTAP SMB** 伺服器上啟用或停用 **ODX**

您可以在儲存虛擬機器（SVM）上啟用或停用ODX。預設為啟用支援ODX複本卸載（若同時啟用SMB 3.0）。

開始之前

必須啟用SMB 3.0。

關於這項工作

如果您停用SMB 3.0、ONTAP 則不支援SMB ODX。如果您重新啟用SMB 3.0、則必須手動重新啟用SMB ODX。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 執行下列其中一項動作：

如果您想要**ODX**複本卸載...	輸入命令...
已啟用	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -copy-offload-enabled false`

3. 返回管理權限層級： `set -privilege admin`

範例

下列範例可在SVM VS1上啟用ODX複製卸載：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster1::*> set -privilege admin
```

相關資訊

可用的伺服器選項

透過自動定位提供SMB自動節點參照、縮短用戶端回應時間

了解如何透過使用自動定位提供 **ONTAP SMB** 自動節點引用來縮短客戶端回應時間

「自動定位」使用SMB自動節點參照來提升儲存虛擬機器（SVM）上的SMB用戶端效能。自動節點參照會自動將要求的用戶端重新導向至裝載資料所在磁碟區之節點SVM上的LIF、進而改善用戶端回應時間。

當SMB用戶端連線至裝載於SVM上的SMB共用時、它可能會使用不擁有所要求資料的節點上的LIF進行連線。用戶端所連接的節點會使用叢集網路存取其他節點所擁有的資料。如果SMB連線使用位於包含所要求資料之節點上的LIF、用戶端就能獲得更快的回應時間：

- 提供此功能的方法是使用Microsoft Dfs轉介來通知SMB用戶端命名空間中所要求的檔案或資料夾位於其他位置。ONTAP

當節點判斷包含資料的節點上是否有任一SVM LIF時、就會進行參照。

- 支援自動節點參照、可用於IPV4和IPv6 LIF IP位址。
- 參照是根據用戶端所連線之共用區根的位置而進行。
- 參照發生在SMB交涉期間。

參照會在建立連線之前進行。將SMB用戶端指向目標節點之後ONTAP 、就會建立連線、然後用戶端從該點透過參照的LIF路徑存取資料。這可讓用戶端更快存取資料、避免額外的叢集通訊。

> 如果共享區跨越多個交會點、而部分交會則是包含在其他節點上的磁碟區、則共用區內的資料會分散在多個節點上。由於支援從本機介面轉介至共享區根目錄、因此、必須使用叢集網路來擷取這些非本機磁碟區內的資料。ONTAP ONTAP 有了這種命名空間架構、自動節點參照可能無法提供顯著的效能效益。

如果託管資料的節點沒有可用的LIF、ONTAP 則使用用戶端選擇的LIF來建立連線。在SMB用戶端開啟檔案之後、它會繼續透過相同的參照連線來存取檔案。

如果CIFS伺服器因故無法進行轉介、則不會中斷SMB服務。建立SMB連線時、會如同未啟用自動節點參照。

相關資訊

提升Microsoft遠端複製效能

在 **ONTAP SMB** 伺服器上使用自動節點引用的要求和準則

在您使用SMB自動節點參照（也稱為_autosocure_）之前、您必須先瞭解某些需求、包括ONTAP 哪些版本的支援功能。您也必須瞭解支援的SMB傳輸協定版本及其他特定準則。

版本與授權要求**ONTAP**

- 叢集中的所有節點都必須執行ONTAP 支援自動節點參照的版本的支援功能。
- 必須在SMB共用區上啟用Widgelinks、才能使用自動定位功能。
- CIFS必須獲得授權、且SVM上必須有SMB伺服器。SMB 授權隨附於"ONTAP One"。如果您沒有 ONTAP One 且未安裝授權、請聯絡您的銷售代表。

SMB傳輸協定版本需求

- 對於SVM、ONTAP 此功能支援在所有SMB版本上自動轉介節點。

SMB用戶端需求

支援的所有Microsoft用戶端ONTAP 均支援SMB自動節點轉介。

互通性對照表包含Windows用戶ONTAP 端所支援的最新資訊。

"NetApp 互通性對照表工具"

資料**LIF**需求

如果您想要使用資料LIF做為SMB用戶端的潛在參照、則必須同時啟用NFS和CIFS來建立資料生命期。

如果目標節點包含僅針對NFS傳輸協定啟用或僅針對SMB傳輸協定啟用的資料LIF、則自動節點參照可能無法運作。

如果不符合此要求、資料存取將不受影響。SMB用戶端會使用用戶端用來連線至SVM的原始LIF來對應共用區。

建立參照**SMB**連線時的**NTLM**驗證需求

必須允許在包含CIFS伺服器的網域和包含要使用自動節點參照之用戶端的網域上進行NTLM驗證。

進行轉介時、SMB伺服器會將IP位址指向Windows用戶端。由於使用IP位址進行連線時會使用NTLM驗證、因此不會針對參照的連線執行Kerberos驗證。

發生這種情況的原因是 Windows 用戶端無法建立 Kerberos 所使用的服務主體名稱（屬於表單 `service/NetBIOS name` 和 `service/FQDN`）、這表示用戶端無法向服務要求 Kerberos 票證。

使用主目錄功能自動節點參照的準則

當共用區設定為啟用主目錄共用屬性時、可以針對主目錄組態設定一或多個主目錄搜尋路徑。搜尋路徑可指向包含SVM磁碟區的每個節點上所包含的磁碟區。用戶端會接收參照、如果有作用中的本機資料LIF可用、則會透過主使用者主目錄的本機參照LIF連線。

當SMB 1.0用戶端存取啟用自動節點參照的動態主目錄時、有一些準則。這是因為SMB 1.0用戶端需要在驗證之前自動進行節點參照、SMB伺服器才有使用者名稱。不過、如果下列陳述屬實、SMB主目錄存取功能可在SMB 1.0用戶端正常運作：

- SMB主目錄設定為使用簡單名稱、例如「`%w'（Windows`使用者名稱）」或「%u」（對應的UNIX使用者名稱）、而非網域名稱樣式名稱、例如「`%d\%w」（網域名稱\使用者名稱）。
- 建立主目錄共用時、CIFS主目錄共用名稱會設定變數（「'%w'」或「'%u'」）、而非靜態名稱、例如「'home'」。

對於SMB 2.x和SMB 3.0用戶端、使用自動節點參照來存取主目錄時、沒有特別的準則。

在**CIFS**伺服器上停用自動節點參照的準則（含現有參照連線）

如果您在啟用此選項之後停用自動節點參照、則目前連線至參照LIF的用戶端會保留參照的連線。由於支援使用DFS轉介做為SMB自動節點轉介的機制、因此在停用此選項之後、用戶端甚至可以重新連線到參照的LIF、直到用戶端的快取DFS參照 逾時為止。ONTAP即使還原ONTAP 至不支援自動節點參照的版本、也一樣。用戶端會繼續使用參照、直到來自用戶端快取的Dfs參照逾時為止。

Autolocation會使用SMB自動節點參照、將用戶端轉介至擁有SVM資料磁碟區的節點上的LIF、藉此提高SMB用戶端效能。當SMB用戶端連線至裝載於SVM上的SMB共用時、它可能會使用不擁有所要求資料的節點上的LIF來連線、並使用叢集互連網路來擷取資料。如果SMB連線使用位於包含所要求資料之節點上的LIF、用戶端就能獲得更快的回應時間。

提供此功能的方法是使用Microsoft分散式檔案系統（Dfs）轉介來通知SMB用戶端命名空間中所要求的檔案或資料夾位於其他位置。ONTAP當節點判斷包含資料的節點上有SVM LIF時、就會進行參照。參照是根據用戶端所連線之共用區根的位置而進行。

參照發生在SMB交涉期間。參照會在建立連線之前進行。將SMB用戶端指向目標節點之後ONTAP 、就會建立連

線、然後用戶端從該點透過參照的LIF路徑存取資料。這可讓用戶端更快存取資料、避免額外的叢集通訊。

在**Mac OS**用戶端上使用自動節點參照的準則

Mac OS X用戶端不支援SMB自動節點轉介、即使Mac OS支援Microsoft的分散式檔案系統（DFs）。Windows用戶端在連線至SMB共用區之前、會先提出一個Dfs參照要求。提供資料LIF的參照、可在裝載所要求資料的同一個節點上找到、進而改善用戶端回應時間。ONTAP雖然Mac OS支援DFS,Mac OS用戶端在此領域的行為與Windows用戶端並不完全相同。

相關資訊

- 了解如何在伺服器上啟用動態主目錄
- "網路管理"
- "NetApp 互通性對照表工具"

支援 **ONTAP SMB** 自動節點引用

在啟用SMB自動節點參照之前、您應該注意某些ONTAP 功能不支援參照。

- 下列類型的磁碟區不支援SMB自動節點參照：
  - 負載共用鏡像的唯讀成員
  - 資料保護鏡射的目的地Volume
- 節點參照不會隨著LIF移動而移動。

  如果用戶端使用SMB 2.x或SMB 3.0連線上的參照連線、而資料LIF在不中斷營運的情況下移動、即使LIF不再是資料的本機連線、用戶端仍會繼續使用相同的參照連線。

- 節點參照不會隨著磁碟區移動而移動。

  如果用戶端透過任何SMB連線使用參照連線、而發生磁碟區移動、則即使磁碟區不再與資料LIF位於同一個節點、用戶端仍會繼續使用相同的參照連線。

啟用或停用 **ONTAP SMB** 自動節點引用

您可以啟用SMB自動節點參照、以提升SMB用戶端存取效能。如果您不想ONTAP 讓使用者向SMB用戶端轉介資料、可以停用自動節點轉介。

開始之前

CIFS伺服器必須設定並在儲存虛擬機器（SVM）上執行。

關於這項工作

SMB自動節點參照功能預設為停用。您可以視需要在每個SVM上啟用或停用此功能。

此選項適用於進階權限層級。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 視需要啟用或停用SMB自動節點參照：

如果您想要SMB自動節點參照...	輸入下列命令...
已啟用	`vserver cifs options modify -vserver vserver_name -is-referral-enabled true`
已停用	`vserver cifs options modify -vserver vserver_name -is-referral-enabled false`

選項設定會對新的SMB工作階段生效。具有現有連線的用戶端只能在現有快取逾時過期時使用節點參照。

3. 切換至管理員權限層級： `set -privilege admin`

相關資訊

可用的伺服器選項

使用統計資料監控 **ONTAP SMB** 自動節點參考活動

若要判斷要參照多少 SMB 連線、您可以使用監控自動節點參照活動 `statistics` 命令。透過監控轉介、您可以判斷自動轉介在裝載共用的節點上尋找連線的程度、以及是否應重新分配資料生命量、以提供對CIFS伺服器上共用區的更佳本機存取。

關於這項工作

。 `cifs` 物件在進階權限層級提供數個計數器、可在監控 SMB 自動節點參照時提供協助：

- `node_referral_issued`

  在用戶端使用與共用根節點不同的節點所主控的LIF連線之後、已向共用根節點發出參照的用戶端數目。

- `node_referral_local`

  使用裝載共用根目錄之同一個節點所裝載之LIF進行連線的用戶端數目。本機存取通常可提供最佳效能。

- `node_referral_not_possible`

  使用與共用根節點不同的節點所裝載的LIF進行連線之後、尚未向裝載共用根目錄的節點發出轉介的用戶端數目。這是因為找不到共用根節點的作用中資料LIF。

- `node_referral_remote`

  使用裝載於共享根目錄之節點不同之節點的LIF所連線的用戶端數目。遠端存取可能導致效能降低。

您可以在儲存虛擬機器（SVM）上收集及檢視特定時間段（範例）的資料、以監控自動節點參照統計資料。如果不停止資料收集、您可以檢視範例中的資料。停止資料收集可提供固定的範例。不停止資料收集可讓您取得更新的資料、以便與先前的查詢進行比較。這項比較可協助您識別效能趨勢。

評估及使用您從收集到的資訊 `statistics` 命令、您應該瞭解用戶端在環境中的發佈。

步驟

1. 將權限層級設為進階： `set -privilege advanced`
2. 使用檢視自動節點參照統計資料 `statistics` 命令。

   此範例透過收集和檢視取樣期間的資料來檢視自動節點參照統計資料：

   a. 開始收藏： `statistics start -object cifs -instance vs1 -sample-id sample1`

   ```
   Statistics collection is being started for Sample-id: sample1
   ```

   b. 等待所需的收集時間到。

   c. 停止集合： `statistics stop -sample-id sample1`

   ```
   Statistics collection is being stopped for Sample-id: sample1
   ```

   詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

   d. 檢視自動節點參照統計資料： `statistics show -sample-id sample1 -counter` **`node`**

   ```
   Object: cifs
   Instance: vs1
   Start-time: 2/4/2013 19:27:02
   End-time: 2/4/2013 19:30:11
   Cluster: cluster1

       Counter                                     Value
       --------------------------- ----------------------------
       node_name                                   node1
       node_referral_issued                            0
       node_referral_local                             1
       node_referral_not_possible                      2
       node_referral_remote                            2
       ...

       node_name                                   node2
       node_referral_issued                            2
       node_referral_local                             1
       node_referral_not_possible                      0
       node_referral_remote                            2
       ...
   ```

   輸出會顯示所有參與SVM VS1的節點計數器。為了清楚起見、範例中僅提供與自動節點參照統計資料相關的輸出欄位。

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

3. 返回管理權限層級： `set -privilege admin`

相關資訊

- 顯示統計資料
- "效能監控設定"

使用 **Windows** 用戶端監控用戶端 **ONTAP SMB** 自動節點參考訊息

若要從用戶端的角度判斷要進行哪些轉介、您可以使用 Windows `dfsutil.exe` 公用程式：

Windows 7 及更新版本用戶端隨附的遠端伺服器管理工具（ RSAT ）套件包含 `dfsutil.exe` 公用程式：使用此公用程式、您可以顯示參照快取內容的相關資訊、以及檢視用戶端目前所使用之每個參照的相關資訊。您也可以使用公用程式清除用戶端的參照快取。如需詳細資訊、請參閱Microsoft TechNet程式庫。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

利用存取型列舉、為共享區提供資料夾安全性

透過基於存取的枚舉在共用上提供 **ONTAP SMB** 資料夾安全性

在SMB共用區上啟用存取型列舉（ABE）時、沒有權限存取共用區中所含資料夾或檔案的使用者（無論是透過個別或群組權限限制）、不會看到其環境中顯示的共用資源、不過共用區本身仍為可見。

傳統共用內容可讓您指定哪些使用者（個別或群組）有權檢視或修改共用區中包含的檔案或資料夾。不過、這些資料夾不允許您控制共用區內的資料夾或檔案是否可供無權存取的使用者查看。如果共用區中的這些資料夾或檔案名稱描述敏感資訊、例如客戶名稱或開發中的產品、可能會造成問題。

存取型列舉（ABE）可延伸共用內容、以包括共用區內的檔案與資料夾列舉。因此、Abe可讓您根據使用者存取權限、篩選共用區內的檔案和資料夾顯示。也就是所有使用者都能看到共用區本身、但共用區內的檔案和資料夾可能會顯示給指定使用者、或是隱藏給指定使用者。除了保護工作環境中的敏感資訊、ABE還能讓您簡化大型目錄結構的顯示、讓不需要存取完整內容的使用者受益。例如、共用區本身對所有使用者都是可見的、但共用區內的檔案和資料夾可能會顯示或隱藏。

深入瞭解 "使用SMB/CIFS存取型列舉時的效能影響"。

在 **ONTAP SMB** 共用上啟用或停用基於存取的枚舉

您可以在SMB共用區上啟用或停用存取型列舉（ABE）、以允許或防止使用者看到他們無權存取的共用資源。

關於這項工作

依預設、ABE為停用狀態。

步驟

1. 執行下列其中一項動作：

如果您想要...	輸入命令...
在新共用區上啟用ABE	`vserver cifs share create -vserver vserver_name -share-name share_name -path path -share -properties access-based-enumeration`建立 SMB 共用時，您可以指定其他選用的共用設定和其他共用內容。如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。
在現有共用區上啟用ABE	`vserver cifs share properties add -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 保留現有的共用內容。ABE共用屬性會新增至現有的共用屬性清單。
停用現有共用區上的ABE	`vserver cifs share properties remove -vserver vserver_name -share-name share_name -share-properties access-based-enumeration` 其他共用內容將會保留。只有ABE共用內容會從共用內容清單中移除。

2. 使用確認共用組態正確無誤 `vserver cifs share show` 命令。

範例

以下範例建立名為「銷售」的 ABE SMB 共用、路徑為 `/sales` 在 SVM VS1 上。共用即會建立於 `access-based-enumeration` 做為共享內容：

```
cluster1::> vserver cifs share create -vserver vs1 -share-name sales -path
/sales  -share-properties access-based-
enumeration,oplocks,browsable,changenotify

cluster1::> vserver cifs share show -vserver vs1 -share-name sales

                      Vserver: vs1
                        Share: sales
     CIFS Server NetBIOS Name: VS1
                         Path: /sales
             Share Properties: access-based-enumeration
                               oplocks
                               browsable
                               changenotify
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

下列範例新增 `access-based-enumeration` 將內容共用至名為「 data2 」的 SMB 共用區：

```
cluster1::> vserver cifs share properties add -vserver vs1 -share-name
data2 -share-properties access-based-enumeration

cluster1::> vserver cifs share show -vserver vs1 -share-name data2 -fields
share-name,share-properties
server  share-name share-properties
------- ---------- ------------------------------------------------------
vs1     data2      oplocks,browsable,changenotify,access-based-enumeration
```

相關資訊

新增或刪除現有共享的共享屬性

在 **ONTAP SMB** 共用上啟用或停用 **Windows** 用戶端的基於存取的枚舉

您可以從Windows用戶端啟用或停用SMB共用上的存取型列舉（ABE）、讓您無需連線至CIFS伺服器即可設定此共用設定。

。 `abecmd` Windows Server 和 Windows 用戶端的新版本不提供公用程式。它是Windows Server 2008的一部分。Windows Server 2008支援服務已於2020年1月14日終止。

步驟

1. 從支援 ABE 的 Windows 用戶端輸入下列命令： `abecmd [/enable | /disable] [/server CIFS_server_name] {/all | share_name}`

   如需更多關於的資訊、請參閱 `abecmd` 命令、請參閱 Windows 用戶端文件。

NFS和SMB檔案及目錄命名相依性

了解 **ONTAP NFS** 和 **SMB** 檔案和目錄命名依賴關係

檔案和目錄命名慣例取決於網路用戶端的作業系統和檔案共用傳輸協定、以及ONTAP 在叢集和用戶端上的語言設定。

作業系統和檔案共用傳輸協定決定下列事項：

- 檔案名稱可使用的字元
- 檔案名稱的大小寫敏感度

根據發行版的資訊、支援檔案、目錄和qtree名稱中的多位元組字元。ONTAP ONTAP

了解 **ONTAP SMB** 檔案或目錄名稱的有效字符

如果您從具有不同作業系統的用戶端存取檔案或目錄、則應使用兩個作業系統中有效的字元。

例如、如果您使用UNIX建立檔案或目錄、請勿在名稱中使用分號（：）、因為在MS－DOS檔案或目錄名稱中不允許使用分號。由於有效字元的限制因作業系統而異、請參閱用戶端作業系統的說明文件、以取得有關禁止字元的詳細資訊。

多協定環境中 **ONTAP SMB** 檔案和目錄名稱的大小寫敏感性

檔案和目錄名稱對NFS用戶端區分大小寫、對SMB用戶端則不區分大小寫、但大小寫保留。您必須瞭解多重傳輸協定環境的影響、以及在建立SMB共用區時指定路徑以及存取共用區內資料時、可能需要採取的行動。

如果 SMB 用戶端建立名為的目錄 `testdir`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `testdir`。不過、如果 SMB 使用者稍後嘗試建立目錄名稱 `TESTDIR`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的目錄 `TESTDIR`NFS 和 SMB 用戶端會以不同方式顯示目錄名稱、如下所示：

- 例如、在 NFS 用戶端上、您會看到兩個目錄名稱都是建立的 `testdir` 和 `TESTDIR`，因爲目錄名稱區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個目錄。一個目錄有基礎檔案名稱。其他目錄會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `testdir` 和 `TESTDI~1`。

- ONTAP 會建立 `TESTDI~1` 用於區分兩個目錄的目錄名稱。

  在這種情況下、您必須在建立或修改儲存虛擬機器（SVM）上的共用區時、使用8.3名稱來指定共用路徑。

同樣地、如果 SMB 用戶端建立檔案 `test.txt`， SMB 和 NFS 用戶端都會將檔案名稱顯示為 `text.txt`。不過、如果 SMB 使用者稍後嘗試建立 `Test.txt`，不允許使用該名稱，因爲對於 SMB 客戶端，該名稱當前存在。如果 NFS 使用者稍後建立名為的檔案 `Test.txt`NFS 和 SMB 用戶端會以不同方式顯示檔案名稱、如下所示：

- 在 NFS 用戶端上、您會看到兩個檔案名稱都是建立的、 `test.txt` 和 `Test.txt`，因爲文件名區分大小寫。
- SMB用戶端使用8.3名稱來區分這兩個檔案。一個檔案有基礎檔案名稱。其他檔案會指派8.3檔名。
  - 在 SMB 用戶端上、您會看到 `test.txt` 和 `TEST~1.TXT`。
  - ONTAP 會建立 `TEST~1.TXT` 檔案名稱可區分這兩個檔案。

> 如果您已使用vserver CIFS字元對應命令啟用或修改字元對應、則通常不區分大小寫的Windows查詢會變成區分大小寫。

了解如何建立 **ONTAP SMB** 檔案和目錄名稱

在任何可從SMB用戶端存取的目錄中、利用此程式建立並維護兩個檔案或目錄名稱：原始的長名稱和8.3格式的名稱。ONTAP

若檔案或目錄名稱超過八個字元名稱或三個字元副檔名限制（檔案）、ONTAP 則會產生8.3格式的名稱、如下所示：

- 如果名稱超過六個字元、則會將原始檔案或目錄名稱刪減為六個字元。
- 它會在檔案或目錄名稱中附加一個或多個數字（從一到五）、這些名稱在被截短後不再是唯一的。

  如果因為有五個以上的相似名稱而導致號碼不足、就會建立一個與原始名稱無關的唯一名稱。

- 如果是檔案、則會將副檔名縮短為三個字元。

例如、如果 NFS 用戶端建立名為的檔案 `specifications.html`，由 ONTAP 建立的 8.3 格式檔案名稱為 `specif~1.htm`。如果此名稱已經存在、ONTAP 則在檔案名稱結尾處使用不同的編號。例如、如果 NFS 用戶端接著建立另一個名為的檔案 `specifications_new.html`的 `8.3` 格式 `specifications_new.html` 是 `specif~2.htm`。

了解 **ONTAP SMB** 多位元組檔案、目錄和 **qtree** 名稱

從支援4位元組的UTF-8編碼名稱開始、即可建立及顯示包含基本多語言平面（BMP）以外之統一碼輔助字元的檔案、目錄和樹狀名稱。ONTAP在早期版本中、這些補充字元無法在多重傳輸協定環境中正確顯示。

若要啟用 4 位元組 UTF-8 編碼名稱的支援、可使用新的 *utf8mb4* 語言代碼 `vserver` 和 `volume` 命令系列。

您必須以下列其中一種方式建立新的Volume：

- 設定音量 `-language` 選項明確： `volume create -language utf8mb4 {…}`
- 繼承 Volume `-language` SVM 中的選項、此選項已針對選項建立或修改： `vserver [create|modify] -language utf8mb4 {…}``volume create {…}`
- 在 ONTAP 9.6 及更早版本中、您無法修改現有的 Volume 以支援 utf8mb4 ；您必須建立新的 utf8mb4 就緒磁碟區、然後使用用戶端型複本工具移轉資料。

  您可以更新SVM以取得utf8mb4支援、但現有磁碟區仍保留其原始語言代碼。

  如果您使用的是 ONTAP 9.7P1 或更新版本、您可以透過支援要求修改 utf8mb4 的現有磁碟區。如需詳細資訊、請參閱 "是否可以在 ONTAP 中建立後變更 Volume 語言？"。

- 從 ONTAP 9.8 開始、您可以使用 `[-language <Language code>]` 將 Volume 語言從 *.UTF-8 變更為 utf8mb4 的參數。若要變更 Volume 的語言、請聯絡 "NetApp支援"。

> ⓘ 目前不支援使用4位元組utf-8字元的LUN名稱。

- 在Windows檔案系統應用程式中、通常會使用16位元的統一碼轉換格式（UTF-16）來表示統一碼字元資料、在使用8位元的統一碼轉換格式（UTF-8）的NFS檔案系統中則代表統一碼字元資料。

  在發行版不含更新版本的版本中、Windows用戶端所建立的名稱（包括UTF-16輔助字元）會正確顯示給其他Windows用戶端、但不會正確轉譯為適用於NFS用戶端的UTF-8。ONTAP同樣地、已建立NFS用戶端的名稱若含有UTF-8補充字元、則無法正確轉譯為適用於Windows用戶端的UTF-16。

- 當您在執行ONTAP 包含有效或無效補充字元的系統上建立檔案名稱時ONTAP 、不接受檔案名稱、並傳回無效的檔案名稱錯誤。

  若要避免此問題、請在檔案名稱中僅使用BMP字元、避免使用補充字元、或升級ONTAP 至版本號（或更新版本）。

從ONTAP 功能表9開始、qtree名稱中允許使用統一碼字元。

- 您可以使用 `volume qtree` 命令系列或系統管理程式來設定或修改 qtree 名稱。
- qtree名稱可以包含多位元組的統一碼格式字元、例如日文和中文字元。
- 在版本不含支援的版本中、僅支援使用BMP字元（也就是可以以3個位元組表示的字元）ONTAP 。

> ⓘ 在發行版之前的版本中、qtree父磁碟區的交會路徑可以包含qtree和含有統一碼字元的目錄名稱。ONTAP。 `volume show` 當父磁碟區具有 UTF-8 語言設定時、命令會正確顯示這些名稱。不過、如果父Volume語言不是UTF-8語言設定之一、則會使用數值NFS替代名稱來顯示交會路徑的某些部分。

- 在9.5及更新版本中、如果qtree位於啟用utf8mb4的Volume中、則qtree名稱中支援4位元組字元。

為磁碟區上的 **ONTAP SMB** 檔案名稱轉換設定字元映射

NFS用戶端可以建立檔案名稱、其中包含對SMB用戶端和某些Windows應用程式無效的字元。您可以設定磁碟區上檔案名稱轉譯的字元對應、讓SMB用戶端能夠存取NFS名稱、否則將無效。

關於這項工作

當SMB用戶端存取NFS用戶端所建立的檔案時、ONTAP 即可查看檔案名稱。如果名稱不是有效的SMB檔案名稱（例如、如果名稱有內嵌的結腸「」字元）、ONTAP 則無法返回每個檔案所保留的8.3檔名。不過、這會對將重要資訊編碼成長檔名的應用程式造成問題。

因此、如果您要在不同作業系統上的用戶端之間共用檔案、則應該在兩個作業系統中都有效的檔案名稱中使用字元。

不過、如果您有NFS用戶端建立的檔案名稱包含SMB用戶端無效檔案名稱的字元、您可以定義將無效NFS字元轉換成SMB和某些Windows應用程式所接受的統一碼字元的對應。例如、此功能支援CATIA MCAD和Mathatica應用程式、以及其他有此需求的應用程式。

您可以依Volume設定字元對應。

在磁碟區上設定字元對應時、必須謹記下列事項：

- 字元對應不會套用至交叉點。

  您必須明確設定每個交會Volume的字元對應。

- 您必須確定用於表示無效或非法字元的unicode字元是通常不會出現在檔案名稱中的字元、否則會產生不必要的對應。

  例如、如果您嘗試將一個分號（：）對應至連字號（-）、但檔案名稱中正確使用連字號（-）、則嘗試存取名為「a-b」的檔案的Windows用戶端會將其要求對應至NFS名稱「a:b」（而非所需結果）。

- 套用字元對應之後、如果對應仍包含無效的Windows字元、ONTAP 則將還原為Windows 8.3檔名。
- 在FPolicy通知、NAS稽核記錄和安全追蹤訊息中、會顯示對應的檔案名稱。
- 建立DP類型的SnapMirror關係時、來源磁碟區的字元對應不會複寫到目的地DP磁碟區。
- 區分大小寫：由於對應的Windows名稱會變成NFS名稱、因此名稱的查詢會遵循NFS語義。這包括NFS查詢區分大小寫。這表示存取對應共用的應用程式不得仰賴Windows不區分大小寫的行為。但是8.3名稱是可用的、而且不區分大小寫。
- 部分或無效對應：在將名稱對應至執行目錄列舉（「dir」）的用戶端之後、會檢查所產生的UNICODE名稱是否為Windows有效性。如果該名稱中仍有無效字元、或Windows的名稱無效（例如結尾為「.」或空白）、則會傳回8.3名稱而非無效名稱。

步驟

1. 設定字元對應：+

`vserver cifs character-mapping create -vserver` *`vserver_name`* `-volume` *`volume_name`* `-mapping` *`mapping_text`*`, … +`

對應包含以「」分隔的來源目標字元配對清單。這些字元是以十六進位數字輸入的統一碼字元。例如：3c：E03C。+

每個值的第一個值 `mapping_text` 以冒號分隔的配對是您要轉譯之 NFS 字元的十六進位值、第二個值是 SMB 使用的 Unicode 值。對應配對必須是唯一的（一對一對應應該存在）。

- 來源對應+

下表顯示來源對應的允許UNICODE字元集：

+

統一碼字元	列印字元	說明
01-0x19	不適用	非列印控制字元
0x5C		反斜槓
x3A.	：	結腸
0X2A	*	星號
x3F	？	問號
x22	"	引號
x3C	<	小於
x3E	>	大於
x7C		
垂直線	0xB1	±

- 目標對應

  您可以在下列範圍內指定「Private Use Area」（私有使用區域）中的目標字元：u+E0000…U+F8FF。

範例

下列命令會在儲存虛擬機器（SVM）VS1上、針對名為「dATA」的磁碟區建立字元對應：

```
cluster1::> vserver cifs character-mapping create -volume data -mapping
3c:e17c,3e:f17d,2a:f745
cluster1::> vserver cifs character-mapping show

Vserver         Volume Name  Character Mapping
--------------  -----------  ------------------------------------------
vs1             data         3c:e17c, 3e:f17d, 2a:f745
```

相關資訊

了解如何在命名空間中建立和管理資料卷

用於管理 **SMB** 檔案名稱轉換的字元對映的 **ONTAP** 命令

您可以建立、修改、顯示有關資訊、或刪除FlexVol 在支援使用於支援SMB檔案名稱轉譯的檔案字元對應、來管理字元對應。

如果您想要...	使用此命令...
建立新的檔案字元對應	`vserver cifs character-mapping create`
顯示檔案字元對應的相關資訊	`vserver cifs character-mapping show`
修改現有的檔案字元對應	`vserver cifs character-mapping modify`
刪除檔案字元對應	`vserver cifs character-mapping delete`

如"指令參考資料ONTAP"需詳細 `vserver cifs character-mapping`資訊，請參閱。

相關資訊

配置卷上的檔案名稱轉換的字元映射

提供S3用戶端對NAS資料的存取

了解ONTAP S3 多協定支持

從ONTAP S廳9.12.1開始、您可以讓執行S3傳輸協定的用戶端存取使用NFS和SMB傳輸協定的用戶端所獲得的相同資料、而無需重新格式化。這項功能可讓NAS資料繼續提供給NAS用戶端、同時將物件資料呈現給執行S3應用程式（例如資料採礦和人工智慧）的S3用戶端。

S3多重傳輸協定功能可解決兩種使用案例：

1. 使用S3用戶端存取現有的NAS資料

   如果您現有的資料是使用傳統 NAS 用戶端（NFS 或 SMB）建立的，並且位於 NAS 磁碟區（FlexVol 或FlexGroup磁碟區）上，則您可以使用 S3 用戶端上的分析工具來存取此資料。

2. 後端儲存設備、適用於能夠使用NAS和S3傳輸協定執行I/O的現代化用戶端

   您可以為 Spark 和 Kafka 等可以使用 NAS 和 S3 協定讀取和寫入相同資料的應用程式提供整合存取。

S3 多重傳輸協定支援的運作方式

ONTAP多重協定支援可讓您將相同的資料集呈現為檔案層次結構或儲存桶中的物件。為此， ONTAP創建了“S3 NAS 儲存桶”，允許 S3 用戶端使用 S3 物件請求建立、讀取、刪除和枚舉 NAS 儲存中的檔案。此映射符合 NAS 安全性配置，遵守檔案和目錄存取權限以及根據需要寫入安全性審計追蹤。

這項對應是透過將指定的NAS目錄階層呈現為S3儲存區來完成。目錄階層中的每個檔案都會以S3物件表示、其

名稱會相對於對應的目錄向下、而目錄邊界則以斜槓字元（'/'）表示。

ONTAP 定義的 S3 使用者可存取此儲存設備，受對應至 NAS 目錄的儲存區所定義的儲存區原則所規範。若要達到此目的、必須在S3使用者和SMB/NFS使用者之間定義對應。SMB/NFS使用者的認證資料將用於NAS權限檢查、並包含在這些存取所產生的任何稽核記錄中。

當SMB或NFS用戶端建立時、檔案會立即放在目錄中、因此在寫入任何資料之前、用戶端可以看到。S3用戶端會預期不同的語義、在寫入新物件的所有資料之前、新物件不會顯示在命名空間中。S3與NAS儲存設備之間的這種對應會使用S3語義建立檔案、在S3建立命令完成之前、將檔案保持在外部不可見的狀態。

S3 NAS儲存區的資料保護

S3 NAS「儲存桶」只是 S3 用戶端的 NAS 資料映射，它們不是標準的 S3 儲存桶。因此，無需使用NetApp SnapMirror S3 功能來保護 S3 NAS 儲存桶。相反，您可以使用SnapMirror非同步磁碟區複製來保護包含 S3 NAS 儲存桶的磁碟區。不支援SnapMirror同步和 SVM 災難復原。

從 ONTAP 9.14.1 開始、 MetroCluster IP 和 FC 組態的鏡射和無鏡射集合體均支援 S3 NAS 貯體。

瞭解 "SnapMirror 非同步"。

稽核**S3 NAS**儲存區

由於S3 NAS儲存區並非傳統的S3儲存區、因此無法將S3稽核設定為稽核其存取。深入瞭解 "S3稽核"。

不過、在S3 NAS儲存區中對應的NAS檔案和目錄、仍可使用傳統ONTAP 的還原稽核程序來稽核存取事件。因此S3作業可觸發NAS稽核事件、但有下列例外：

- 如果S3原則組態（群組或儲存區原則）拒絕S3用戶端存取、則不會啟動事件的NAS稽核。這是因為在進行SVM稽核檢查之前、會先檢查S3權限。
- 如果S3 Get要求的目標檔案大小為0、0內容會傳回Get要求、而且不會記錄讀取存取權。
- 如果S3 Get要求的目標檔案位於使用者沒有周遊權限的資料夾中、則存取嘗試會失敗、而且不會記錄事件。

深入瞭解 "稽核SVM上的NAS事件"。

物件多部分上傳

從 ONTAP 9.16.1 開始，在基礎 FlexGroup Volume 上啟用時， S3 NAS 儲存區支援物件多部分上傳"進階容量平衡"。

在 NAS 檔案儲存設備上的物件多部分上傳，可讓 S3 傳輸協定用戶端將大型物件上傳成較小的部分。物件多部分上傳具有下列優點：

- 它可讓物件平行上傳。
- 如果上傳失敗或暫停，只有尚未上傳的零件需要上傳。不需要重新啟動整個物件的上傳。
- 如果事先不知道物件大小（例如，仍在寫入大型物件時），用戶端可以立即開始上傳物件的部分，並在建立整個物件之後完成上傳。

> S3 NAS 儲存桶中的多部分物件必須以整數大小對齊，不能使用部分大小。例如，一個部分可以是 4MB 或 4GB 或類似大小。一個部分不能使用部分或小於 MB 的大小，例如 4.5MB 或 4000.5MB。

多部分上傳支援下列 S3 動作：

- AbortMultiPart上 傳
- 完成多個部分上傳
- CopyObject（從ONTAP 9.17.1 開始）
- 建立多個部分上傳

  從ONTAP 9.17.1 開始，CreateMultipartUpload 支援標記和使用者元資料鍵/值對。

- 清單多個部分上傳
- 上傳零件

S3 NAS 儲存區不支援依零件編號取得（「 partnumber=xx 」）。而是傳回完整物件。

S3與NAS互通性

除了此處列出的項目、不支援標準NAS和S3功能。ONTAP

S3 NAS儲存區目前不支援NAS功能

資料層**FabricPool**

S3 NAS 貯體無法設定為 FabricPool 的容量層。

S3 NAS 儲存區目前不支援 S3 行動和功能

行動

- ByPassGovernanceRetention
- 刪除 BucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- GetBucketObjectLockConfiguration
- GetBucketVersion
- GetObjectRetention
- ListBucketVersion作業
- ListObjectVerions
- PuttBucketLifecycleConfiguration
- PuttBucketVersion
- PutObjectLockConfiguration
- PutObjectRetention

在 S3 NAS 儲存區中使用 S3 時，不支援這些 S3 行動。使用原生 S3 時"正常支援"，這些動作是。

AWS使用者中繼資料

- 從ONTAP 9.17.1 開始，支援具有多部分物件的元資料。
- 從ONTAP 9.16.1 開始，支援包含單部分物件的元資料。
- 對於 ONTAP 9.15.1 及更早版本，作為 S3 使用者中繼資料一部分所接收的金鑰值配對，不會與物件資料一起儲存在磁碟上。
- 對於 ONTAP 9.15.1 及更早版本，會忽略前置字元為「 x-amz-meta 」的要求標頭。

AWS標籤

- 從ONTAP 9.17.1 開始，支援具有多部分物件的標籤。
- 從ONTAP 9.16.1 開始，支援包含單部分物件的標籤。
- 對於 Put 物件和 Multifart 初始化要求的 ONTAP 9.15.1 及更早版本，會忽略前置「 x-amz-tagging 」的標頭。
- 對於 ONTAP 9.15.1 及更早版本，以「標記查詢字串」來更新現有檔案（「放置」，「取得」及「刪除」要求）上的標記要求會遭到拒絕，並出現錯誤。

版本管理

無法在庫位對應組態中指定版本管理。

- 包含非null版本規格（版本Id=xyz query-string）的要求會收到錯誤回應。
- 系統會拒絕影響儲存區版本設定狀態的要求、但會顯示錯誤。

了解**ONTAP S3** 用戶端存取的 **NAS** 資料需求

請務必瞭解、在對應NAS檔案和目錄以進行S3存取時、會有一些固有的不相容問題。在使用S3 NAS儲存區進行服務之前、可能需要先調整NAS檔案階層。

S3 NAS儲存區使用S3儲存區語法對應該目錄、讓S3存取NAS目錄、而目錄樹狀結構中的檔案則視為物件。物件名稱是與S3儲存區組態中指定之目錄相關的檔案斜槓分隔路徑名稱。

當使用S3 NAS儲存區來處理檔案和目錄時、這種對應會帶來一些需求：

- S3名稱限制為1024位元組、因此無法使用S3存取路徑名稱較長的檔案。
- 檔案和目錄名稱限制為255個字元、因此物件名稱不能包含超過255個連續的非斜槓（「/」）字元
- 以反斜槓（「\」）字元分隔的SMB路徑名稱、會以包含正斜槓（「/」）字元的物件名稱顯示在S3上。
- 一些合法的 S3 物件名稱對不能在映射的 NAS 目錄樹中共存。例如，合法的 S3 物件名稱「part1/part2」和「part1/part2/part3」會對應到 NAS 目錄樹中不能同時存在的文件，因為「part1/part2」在第一個名稱中是文件，而在另一個名稱中是目錄。
  - 如果「part1/part2」是現有文件，則 S3 建立「part1/part2/part3」將會失敗。
  - 如果「part1/part2/part3」是現有文件，則 S3 建立或刪除「part1/part2」將會失敗。
  - 與現有物件名稱相符的S3物件建立會取代預先存在的物件（在未版本化的儲存區中）；該物件保留在NAS中、但需要完全相符的物件。上述範例不會移除現有物件、因為名稱發生衝突時、它們不相符。

雖然物件儲存旨在支援大量任意名稱，但如果將大量名稱放在一個目錄中，NAS 目錄結構可能會遇到效能問題。特別是，不帶斜線（'/'）字元的名稱都將被放入 NAS 映射的根目錄中。大量使用非「NAS 友善」名稱的應

用程式最好託管在實際的物件儲存桶上，而不是 NAS 映射上。

在ONTAP SVM 上啟用 S3 協定存取 NAS 數據

啟用S3傳輸協定存取、包括確保啟用NAS的SVM符合與啟用S3的伺服器相同的需求、包括新增物件存放區伺服器、以及驗證網路和驗證需求。

對於新ONTAP 的版本、建議您在將SVM設定為將NAS資料提供給用戶端之後、啟用SVM的S3傳輸協定存取。若要深入瞭解NAS傳輸協定組態、請參閱：

- "NFS 組態"
- "SMB 組態"

開始之前

啟用S3傳輸協定之前、必須先設定下列項目：

- S3 傳輸協定和所需的 NAS 傳輸協定（ NFS 、 SMB 或兩者）均已獲得授權。
- SVM是針對所需的NAS傳輸協定進行設定。
- NFS和/或SMB伺服器存在。
- 已設定DNS及任何其他必要服務。
- NAS資料正在匯出或共享至用戶端系統。

關於這項工作

需要憑證授權單位（CA）憑證、才能啟用從S3用戶端到啟用S3的SVM的HTTPS流量。可以使用三種來源的CA憑證：

- SVM上的全新ONTAP 自我簽署憑證。
- SVM上現有ONTAP 的自我簽署憑證。
- 第三方憑證。

您可以將相同的資料生命量用於S3/NAS儲存區、以用於處理NAS資料。如果需要特定IP位址、請參閱 "建立資料生命量"。需要S3服務資料原則才能在LIF上啟用S3資料流量；您可以修改SVM的現有服務原則以納入S3。

當您建立S3物件伺服器時、應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將用於S3存取。S3伺服器FQDN不得以儲存區名稱開頭。

系統管理員

1. 在已設定NAS傳輸協定的儲存VM上啟用S3。
   a. 按一下 * 儲存 > 儲存 VM* 、選取 NAS 就緒的儲存 VM 、按一下「設定」、然後按一下 S3 下的。
   b. 選取憑證類型。無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。
   c. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 驗證SVM是否允許S3傳輸協定：+
   `vserver show -fields allowed-protocols`
2. 記錄此SVM的公開金鑰憑證。+
   如果需要新的 ONTAP 自我簽署憑證、請參閱 "在SVM上建立並安裝CA憑證"。
3. 更新服務資料原則
   a. 顯示SVM +的服務資料原則
      `network interface service-policy show -vserver svm_name`

      如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。
   b. 新增 `data-core` 和 `data-s3-server services` （如果不存在）。+
      `network interface service-policy add-service -vserver svm_name -policy policy_name -service data-core,data-s3-server`
4. 確認SVM上的資料生命量符合您的需求：+
   `network interface show -vserver svm_name`

   如"指令參考資料ONTAP"需詳細 `network interface show`資訊，請參閱。
5. 建立S3伺服器：+
   `vserver object-store-server create -vserver svm_name -object-store-server s3_server_fqdn -certificate-name ca_cert_name -comment text [additional_options]`

您可以在建立S3伺服器時或稍後隨時指定其他選項。

- 預設會在連接埠443上啟用HTTPS。您可以使用-secure-listener-port選項來變更連接埠號碼。+
  啟用HTTPS時、需要CA憑證才能與SSL/TLS適當整合。從 ONTAP 9.15.1 開始、 S3 物件儲存支援 TLS 1.3 。
- HTTP預設為停用；啟用時、伺服器會偵聽連接埠80。您可以使用-is啟用http的選項來啟用它、或使用-listener-port選項來變更連接埠編號。+
  啟用HTTP時、所有的要求和回應都會以純文字透過網路傳送。

  1. 驗證是否已根據需要配置S3：+

```
vserver object-store-server show
```

- 範例 *
  下列命令可驗證所有物件儲存伺服器的組態值：
  `cluster1::> vserver object-store-server show`

```
Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                 Secure Listener Port For HTTPS: 443
                                   HTTP Enabled: false
                                  HTTPS Enabled: true
              Certificate for HTTPS Connections: svm1_ca
                                        Comment: Server comment
```

相關資訊

- "網路介面服務原則附加服務"

建立ONTAP S3 NAS 儲存桶

S3 NAS 儲存桶是 S3 儲存桶名稱和 NAS 路徑之間的對應。 S3NAS 儲存桶可讓您提供具有現有磁碟區和目錄結構的 SVM 命名空間的任何部分的 S3 存取權。

開始之前

- S3物件伺服器是在包含NAS資料的SVM中設定。
- NAS資料符合 "S3用戶端存取需求"。

關於這項工作

您可以設定S3 NAS儲存區、以指定SVM根目錄中的任何一組檔案和目錄。

您也可以根據下列任一參數組合、設定允許或禁止存取NAS資料的儲存區原則：

- 檔案與目錄
- 使用者與群組權限
- S3作業

例如，您可以設定一個儲存桶原則，授予大量使用者唯讀資料存取權限，以及另一個儲存桶原則，允許有限群組對該資料的子集執行作業。

從 ONTAP 9.18.1 開始，您可以建立 NAS 儲存桶，使應用程式能夠使用 S3 協定存取 FlexCache 磁碟區上的資料。叢集中的所有節點都必須執行 ONTAP 9.18.1 或更新版本。在使用 S3 協定存取 FlexCache 磁碟區之前，您必須將 `-is-s3-enabled`**選項設定為** `true` "在 FlexCache 磁碟區上"。此參數預設設定為 `false`。

從ONTAP 9.17.1 開始，您可以直接將 S3 NAS 儲存桶連結到卷，而無需通過連接路徑。預設情況下，NAS 磁

碟區上的 S3 儲存桶與連線路徑關聯， ONTAP管理員可以隨時變更該連線路徑。這些變更可能會中斷 S3 儲存桶的運作。從ONTAP 9.17.1 開始，您可以使用 `-is-nas-path-mutable false`選項 `vserver object-store-server bucket create`指令用於啟用 S3 NAS 儲存桶與磁碟區的連結。預設情況下，`-is-nas-path-mutable`設定為 `true 。

由於 S3 NAS「儲存桶」是映射而不是 S3 儲存桶，因此標準 S3 儲存桶的以下屬性不適用於 S3 NAS 儲存桶。

- **agger-list \ aggr-list-multiplier \ storage** 服務層級 **\ volume \ size \ exclain-aggr-list \ qos-policy-tgroup**
  設定 S3 NAS 儲存區時、不會建立任何磁碟區或 qtree 。
- **role \ is -protected ** 是 **-protected-on-ontap ** 是 **-protected-on-cloud** + S3 NAS 儲存桶不受SnapMirror S3 保護或鏡像，而是使用卷粒度上可用的常規SnapMirror保護。
- * 版本管理狀態 * + NAS 磁碟區通常都有快照技術可供儲存不同版本。不過、S3 NAS儲存區目前無法使用版本管理功能。
- * 邏輯使用的 \ 物件計數 *
  NAS 磁碟區可透過 Volume 命令取得等效的統計資料。
- 多部分物件 + 從ONTAP 9.16.1 開始，當 S3 NAS 儲存桶支援多部分物件時"進階容量平衡"在底層FlexGroup磁碟區上啟用。高級容量平衡只能在FlexGroup磁碟區上啟用。無法在FlexVol磁碟區上啟用。

步驟

您可以使用 System Manager 或ONTAP CLI 建立 NAS 儲存桶。

系統管理員

在支援 NAS 的儲存 VM 上新增新的 S3 NAS 儲存區。

1. 按一下「儲存設備>桶」、然後按一下「新增」。
2. 輸入S3 NAS儲存區的名稱、然後選取儲存VM、不要輸入大小、然後按一下*其他選項*。
3. 輸入有效的路徑名稱、或按一下「瀏覽」從有效路徑名稱清單中選取。+
當您輸入有效的路徑名稱時、與 S3 NAS 組態無關的選項將會隱藏。
4. 如果您已將S3使用者對應至NAS使用者和建立的群組、您可以設定其權限、然後按一下*「儲存*」。+
您必須先將 S3 使用者對應至 NAS 使用者、才能在此步驟中設定權限。

否則、請按一下*「Save（儲存）」*完成S3 NAS儲存區組態。

CLI

1. 在包含 NAS 檔案系統的 SVM 中建立 S3 NAS 儲存桶。+
```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -type nas -nas-path <junction_path> -is-nas-path-mutable
true|false [-comment <text>]
```

範例 1：建立 S3 NAS 儲存桶

```
cluster1::> vserver object-store-server bucket create -bucket testbucket
-type nas -path /vol1
```

範例 2：建立 S3 NAS 儲存桶並將儲存桶連結到卷

```
vserver object-store-server bucket create -vserver vs1 -bucket nasbucket1
-type nas -nas-path /pathA/dir1 -is-nas-path-mutable false
```

啟用**ONTAP S3** 用戶端用戶

為了讓 S3 用戶端用戶能夠存取 NAS 數據，您必須將 S3 使用者名稱對應到相應的 NAS 用戶，然後使用儲存桶服務策略授予他們存取 NAS 資料的權限。

開始之前

用戶端存取的使用者名稱（LINUX/UNIX、Windows 和 S3 用戶端使用者）必須已經存在。

您應該知道一些 S3 功能是"S3 NAS 儲存區不支援"。

關於這項工作

將S3使用者名稱對應至對應的Linux/UNIX或Windows使用者、可在S3用戶端存取NAS檔案時、對這些檔案進行授權檢查。S3到NAS的對應是透過提供S3使用者名稱_Pattern_來指定、此名稱可以用單一名稱或POSIX規則運算式來表示、也可以用Linux/UNIX或Windows使用者名稱_Replacement來表示。

如果不存在名稱對應、則會使用預設名稱對應、其中S3使用者名稱本身將做為UNIX使用者名稱和Windows使用者名稱。您可以使用修改UNIX和Windows的預設使用者名稱對應 `vserver object-store-server modify` 命令。

僅支援本機名稱對應組態、不支援LDAP。

S3使用者對應至NAS使用者之後、您可以將權限授予使用者、以指定他們有權存取的資源（目錄和檔案）、以及允許或不允許他們在其中執行的動作。

系統管理員

1. 為UNIX或Windows用戶端（或兩者）建立本機名稱對應。
   a. 按一下「儲存設備>桶」、然後選取啟用S3/NAS的儲存VM。
   b. 選擇 * 設定 * 、然後按一下 → * 名稱對應 * （在 * 主機使用者和群組 * 下）。
   c. 在「* S3至Windows 」或「 S3至UNIX*」方塊（或兩者）中、按一下「* Add 」（*新增）、然後輸入所需的* Pattern*（S3）和*置換*（NAS）使用者名稱。
2. 建立庫位原則以提供用戶端存取。
   a. 按一下 * 儲存空間 > 鏟斗 * 、按一下 ⋮ 所需 S3 貯體旁的、然後按一下 * 編輯 * 。
   b. 按一下「新增」並提供所需的值。
      - 主體：提供S3使用者名稱或使用預設值（所有使用者）。
      - 效果-選擇*允許*或*拒絕*。
      - 動作-輸入這些使用者和資源的動作。物件存放區伺服器目前支援S3 NAS儲存區的一組資源作業包括：GetObject、PuttObject、Delete Object、ListBucket、GetBucketAcl、GetObjectAcl、GetObjectTagging、PuttObjectTagging、刪除ObjectTagging、GetBucketLocation、 GetBuckettions版本管理、PuttBucket版本 管理和ListBucketVerions。此參數可接受萬用字元。
      - 資源：輸入允許或拒絕動作的資料夾或檔案路徑、或使用預設值（儲存庫的根目錄）。

CLI

1. 為UNIX或Windows用戶端（或兩者）建立本機名稱對應。+
   `vserver name-mapping create -vserver svm_name> -direction {s3-win|s3-unix} -position` *`integer`* `-pattern` *`s3_user_name`* `-replacement` *`nas_user_name`*
   - `-position` -對應評估的優先順序編號；請輸入1或2。
   - `-pattern` - S3使用者名稱或規則運算式
   - `-replacement` - Windows或UNIX使用者名稱

範例+

```
vserver name-mapping create -direction s3-win -position 1 -pattern s3_user_1
-replacement win_user_1
vserver name-mapping create -direction s3-unix -position 2 -pattern s3_user_1
-replacement unix_user_1
```

1. 建立庫位原則以提供用戶端存取。+
   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {deny|allow} -action list_of_actions -principal list_of_users_or_groups -resource [-sid alphanumeric_text]`
   - `-effect {deny|allow}` -指定當使用者要求採取行動時、是否允許或拒絕存取。
   - `-action <Action>, …`- 指定允許或拒絕的資源作業。物件存放區伺服器目前支援 S3 NAS 貯體的資源作業集包括： GetObject 、 PutObject 、 DeleteObject 、 ListBucket 、 GetBucketAcl 、 GetObjectAcl 和 GetBucketLocation 。此參數可接受萬用字元。
   - `-principal <Objectstore Principal>, …` -根據此參數中指定的物件存放區伺服器使用者或群組、驗證要求存取的使用者。

- 將字首群組/新增至群組名稱、即可指定物件存放區伺服器群組。
- `-principal -`（連字號字元）可授予所有使用者存取權。

◦ `-resource <text>, …` -指定已設定允許/拒絕權限的儲存區、資料夾或物件。此參數可接受萬用字元。

◦ `[-sid <SID>]` -為物件存放區伺服器區段原則聲明指定選用的文字註解。

範例+

```
cluster1::> vserver object-store-server bucket policy add-statement -bucket
testbucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,
GetBucketLocation,GetBucketPolicy,PutBucketPolicy,DeleteBucketPolicy
-principal user1 -resource testbucket,testbucket/* sid "FullAccessForUser1"

cluster1::> vserver object-store-server bucket policy statement create
-vserver vs1 -bucket bucket1 -effect allow -action GetObject -principal -
-resource bucket1/readme/* -sid "ReadAccessToReadmeForAllUsers"
```

Microsoft Hyper-V和SQL Server的SMB組態

Microsoft Hyper-V與SQL Server的SMB組態總覽

利用支援支援的功能、您可以透過SMB傳輸協定、為兩個Microsoft應用程式啟用不中斷營運：Microsoft Hyper-V和Microsoft SQL Server。ONTAP

如果您想在下列情況下實作SMB不中斷營運、請使用這些程序：

- 已設定基本SMB傳輸協定檔案存取。
- 您想要啟用位於SVM中的SMB 3.0或更新版本檔案共用、以儲存下列物件：
  - Hyper-V虛擬機器檔案
  - SQL Server系統資料庫

相關資訊

如需 ONTAP 技術及與外部服務互動的其他資訊、請參閱下列技術報告（ TR ）： "NetApp技術報告4172：Microsoft Hyper-V over SMB 3.0 with ONTAP NetApp最佳實務做法" ** "NetApp技術報告4369..適用於Microsoft SQL Server的最佳實務做法、SnapManager 以及適用於SQL Server with叢集Data ONTAP 式的版本"

設定ONTAP 適用於Microsoft Hyper-V和SQL Server over SMB解決方案的支援功能

您可以使用持續可用的SMB 3.0及更新版本檔案共用、將Hyper-V虛擬機器檔案或SQL Server系統資料庫及使用者資料庫儲存在位於SVM的磁碟區上、同時為計畫性和非計畫性事件提供不中斷營運（NDOS）。

Microsoft Hyper-V over SMB

若要建立Hyper-V over SMB解決方案、您必須先設定ONTAP 支援功能以提供Microsoft Hyper-V伺服器的儲存服務。此外、您也必須設定Microsoft叢集（如果使用叢集式組態）、Hyper-V伺服器、持續可用的SMB 3.0連線至CIFS伺服器所託管的共用、以及選擇性的備份服務、以保護儲存在SVM磁碟區上的虛擬機器檔案。

Hyper-V伺服器必須在Windows 2012 Server或更新版本上設定。支援獨立式和叢集式Hyper-V伺服器組態。

- 如需建立Microsoft叢集和Hyper-V伺服器的相關資訊、請參閱Microsoft網站。
- 適用於 Hyper-V 的 SnapManager 是一款主機型應用程式，可協助快速，快照型備份服務，專為透過 SMB 組態與 Hyper-V 整合而設計。

  如需SnapManager 在SMB組態上搭配Hyper-V使用的相關資訊、請參閱《SnapManager 適用於Hyper-V的_E__安裝與管理指南》。

Microsoft SQL Server over SMB

若要透過SMB建立SQL Server解決方案、您必須先設定ONTAP 支援功能、為Microsoft SQL Server應用程式提供儲存服務。此外、您也必須設定Microsoft叢集（如果使用叢集式組態）。接著您可以在Windows伺服器上安裝及設定SQL Server、並建立持續可用的SMB 3.0連線、以連線至CIFS伺服器所託管的共用區。您可以選擇性地設定備份服務、以保護儲存在SVM磁碟區上的資料庫檔案。

SQL Server必須安裝並設定於Windows 2012 Server或更新版本。支援獨立式和叢集式組態。

- 如需建立Microsoft叢集及安裝及設定SQL Server的相關資訊、請參閱Microsoft網站。
- 適用於 Microsoft SQL Server 的 SnapCenter 外掛程式是一種主機型應用程式，可促進快速的快照型備份服務，其設計可透過 SMB 組態與 SQL Server 整合。

  如需使用SnapCenter 適用於Microsoft SQL Server的解決方案的資訊、請參閱 "適用於Microsoft SQL Server的支援外掛程式SnapCenter" 文件。

不中斷營運：透過**SMB**執行**Hyper-V**和**SQL Server**

Hyper-V和**SQL Server**在**SMB**上的不中斷營運意味著什麼

Hyper-V與SQL Server在SMB上的不中斷營運、是指結合各種功能、讓應用程式伺服器與所包含的虛擬機器或資料庫維持線上狀態、並在許多管理工作期間提供持續可用度。這包括儲存基礎架構的計畫性和非計畫性停機。

透過SMB支援的應用程式伺服器不中斷營運包括：

- 計畫性接管與恢復
- 非計畫性接管
- 升級
- 計畫性集合體重新配置（ARL）
- LIF移轉與容錯移轉

- 計畫性Volume搬移

可在**SMB**上執行不中斷營運的傳輸協定

隨著SMB 3.0的推出、Microsoft已發行新的傳輸協定、提供必要的功能、以支援Hyper-V和SQL Server在SMB上的不中斷營運。

透過SMB為應用程式伺服器提供不中斷營運時、可使用下列通訊協定：ONTAP

- SMB 3.0
- 見證人

關於**Hyper-V**和**SQL Server**在**SMB**上不中斷營運的重要概念

在設定Hyper-V或SQL Server over SMB解決方案之前、您應該先瞭解一些關於不中斷營運（NDOS）的概念。

- 持續可用的共享區

  擁有持續可用共用內容集的SMB 3.0共用區。透過持續可用的共用區連線的用戶端、可在接管、恢復及集合重新配置等中斷事件中繼續運作。

- 節點

  屬於叢集成員的單一控制器。為了區分SFO配對中的兩個節點、一個節點有時稱為「*local node*」、另一個節點有時稱為「*Partner node*」或「*remRemote node*」。儲存設備的主要擁有者是本機節點。當主要擁有者故障時、可控制儲存設備的次要擁有者是合作夥伴節點。每個節點都是其儲存設備的主要擁有者、也是其合作夥伴儲存設備的次要擁有者。

- 不中斷的集合體重新配置

  能夠在叢集的SFO配對內的合作夥伴節點之間移動集合體、而不會中斷用戶端應用程式。

- 不中斷的容錯移轉

  請參閱_Takeove_。

- 不中斷的**LIF**移轉

  能夠執行LIF移轉、而不會中斷透過該LIF連線至叢集的用戶端應用程式。對於SMB連線、這僅適用於使用SMB 2.0或更新版本連線的用戶端。

- 不中斷營運

  能夠執行ONTAP 重大的非資料管理與升級作業、並在不中斷用戶端應用程式的情況下、承受節點故障。此術語指的是不中斷接管、不中斷升級和不中斷營運的整體移轉功能集合。

- 不中斷升級

  能夠在不中斷應用程式的情況下升級節點硬體或軟體。

- 不中斷磁碟區移動

  能夠在整個叢集內自由移動磁碟區、而不會中斷使用該磁碟區的任何應用程式。對於SMB連線、所有SMB版本都支援不中斷營運的Volume移動。

- 持續處理

  SMB 3.0的屬性、可在中斷連線時、讓持續可用的連線以透明方式重新連線至CIFS伺服器。與耐久的處理程序類似、CIFS伺服器會在與連線用戶端的通訊中斷後、持續維護處理程序一段時間。然而、持續性的處理能力比持久性的處理能力更強。除了讓用戶端有機會在重新連線後60秒內回收處理、CIFS伺服器也會在60秒內拒絕任何其他用戶端存取要求存取檔案的權限。

  關於持續處理的資訊會鏡射到SFO合作夥伴的持續儲存設備上、這可讓持續處理中斷連線的用戶端在發生SFO合作夥伴取得節點儲存設備所有權的事件後、回收持久處理。除了在LIF移動時提供不中斷營運（可持久處理支援）之外、持續控點還可提供不中斷營運的接管、恢復及集合重新定位功能。

- * SFO贈品*

  從接管事件中恢復時、將集合體傳回其主位置。

- * SFO配對*

  一對節點、其控制器設定為在兩個節點之一停止運作時、為彼此提供資料。視系統機型而定、兩個控制器都可以放在單一機箱中、或是控制器可以放在不同的機箱中。在雙節點叢集中稱為HA配對。

- 接管

  當儲存設備的主要擁有者故障時、合作夥伴控制儲存設備的程序。在SFO環境中、容錯移轉和接管是同義詞。

SMB 3.0功能如何支援透過**SMB**共用進行不中斷營運

SMB 3.0提供關鍵功能、可支援透過SMB共用區執行Hyper-V和SQL Server不中斷營運。其中包括 `continuously-available` 共用屬性和一種稱為 *Persistent Handle* 的檔案處理方式、可讓 SMB 用戶端回收檔案開啟狀態、並以透明方式重新建立 SMB 連線。

可將持續處理權授予具有SMB 3.0功能的用戶端、這些用戶端會使用持續可用的共用內容集連線至共用區。如果SMB工作階段中斷連線、CIFS伺服器會保留持續處理狀態的相關資訊。CIFS伺服器會在允許用戶端重新連線的60秒期間、封鎖其他用戶端要求、讓具有持續控制代碼的用戶端在網路中斷連線後、得以回收處理代碼。具有持續控點的用戶端可以使用儲存虛擬機器（SVM）上的其中一個資料LIF來重新連線、方法是透過相同的LIF或不同的LIF來重新連線。

集合重新定位、接管和恢復都會發生在SFO配對之間。為了無縫管理中斷連線和重新連線工作階段與具有持續處理程序的檔案、合作夥伴節點會保留一份所有持續處理鎖定資訊的複本。無論活動是計畫性或非計畫性的、SFO合作夥伴都能不中斷地管理持續處理重新連線。有了這項新功能、連接到CIFS伺服器的SMB 3.0連線、就能以透明且不中斷營運的方式、容錯移轉到另一個指派給SVM的資料LIF、而這是過去發生的破壞性事件。

雖然使用持續性控點可讓CIFS伺服器以透明方式容錯移轉SMB 3.0連線、但如果故障導致Hyper-V應用程式容錯移轉至Windows Server叢集中的另一個節點、用戶端就無法回收這些中斷連線控點的檔案控點。在此案例中、如果在不同節點上重新啟動Hyper-V應用程式、處於中斷連線狀態的檔案處理程序可能會封鎖其存取。「容錯移轉叢集」是SMB 3.0的一部分、可提供機制來使過時且相互衝突的處理程序失效。使用此機制、Hyper-V叢集可在Hyper-V叢集節點故障時快速恢復。

見證傳輸協定為SMB 3.0持續可用的共用（CA共用）提供增強的用戶端容錯移轉功能。見證可縮短容錯移轉的速度、因為它會跳過LIF容錯移轉恢復期間。當節點無法使用時、它會通知應用程式伺服器、而不需要等待SMB 3.0連線逾時。

容錯移轉是無縫的、因為用戶端上執行的應用程式並未察覺發生容錯移轉。如果見證無法使用、容錯移轉作業仍會成功執行、但沒有見證的容錯移轉效率較低。

滿足下列需求時、可進行見證增強容錯移轉：

- 它只能與啟用SMB 3.0的SMB 3.0型CIFS伺服器搭配使用。
- 共用區必須使用SMB 3.0、並設定持續可用度共用內容。
- 應用程式伺服器所連接之節點的SFO合作夥伴、必須至少有一個作業資料LIF指派給應用程式伺服器的儲存虛擬機器（SVM）。

> ⓘ 見證協議在SFO配對之間運作。由於LIF可以移轉至叢集內的任何節點、因此任何節點都可能需要成為其SFO合作夥伴的見證人。 如果應用程式伺服器的SVM託管資料在合作夥伴節點上沒有作用中的資料LIF、見證傳輸協定就無法在指定節點上提供SMB連線的快速容錯移轉。因此、叢集中的每個節點必須至少有一個資料LIF、才能讓裝載其中一個組態的每個SVM使用。

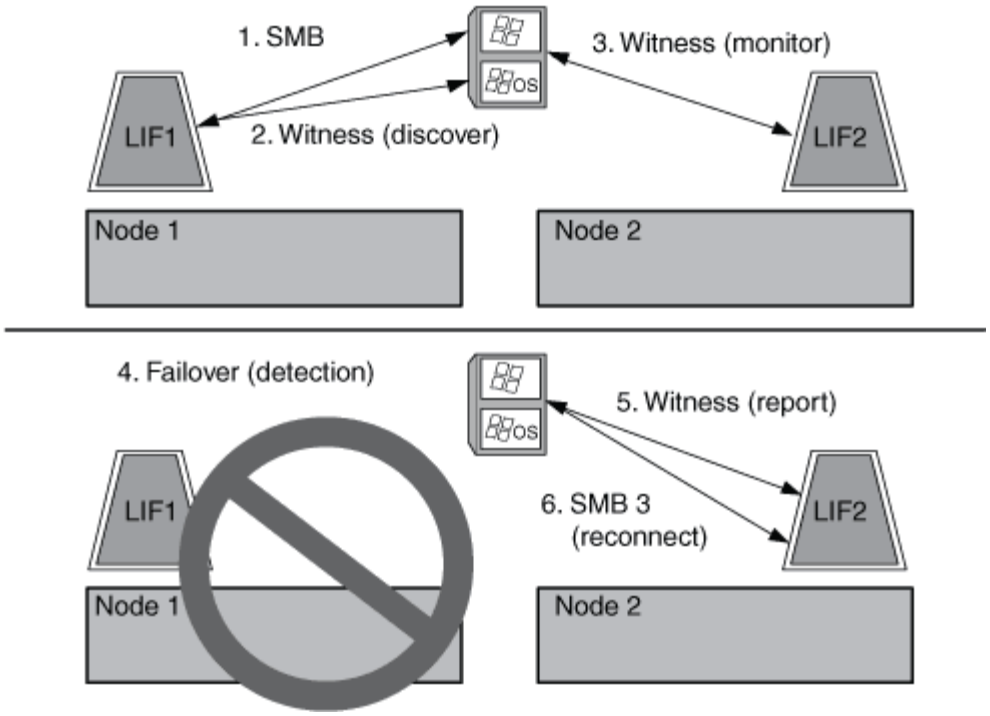
- 應用程式伺服器必須使用儲存在DNS中的CIFS伺服器名稱來連線至CIFS伺服器、而非使用個別的LIF IP位址。

見證協定的運作方式

利用節點的SFO合作夥伴作為見證人、實作見證協議。ONTAP如果發生故障、合作夥伴會快速偵測故障、並通知SMB用戶端。

見證傳輸協定使用下列程序提供增強的容錯移轉：

1. 當應用程式伺服器建立與Node1的持續可用SMB連線時、CIFS伺服器會通知應用程式伺服器有覆核人可用。
2. 應用程式伺服器從Node1要求見證伺服器的IP位址、並接收指派給儲存虛擬機器（SVM）的Node2（SFO合作夥伴）資料LIF IP位址清單。
3. 應用程式伺服器會選擇其中一個IP位址、建立節點2的見證連線、並在節點1上持續可用的連線必須移動時登錄以通知。
4. 如果節點1上發生容錯移轉事件、見證可簡化容錯移轉事件、但不涉及還原。
5. 見證會偵測容錯移轉事件、並透過見證連線通知應用程式伺服器SMB連線必須移至節點2。
6. 應用程式伺服器會將SMB工作階段移至節點2、並在不中斷用戶端存取的情況下恢復連線。



使用遠端**VSS**進行共用型備份

利用遠端**VSS**總覽進行共享型備份

您可以使用遠端VSS、對儲存在CIFS伺服器上的Hyper-V虛擬機器檔案執行共用型備份。

Microsoft遠端VSS（Volume陰影複製服務）是現有Microsoft VSS基礎架構的延伸。有了遠端VSS、Microsoft已擴充VSS基礎架構、以支援SMB共用的陰影複製。此外、 Hyper-V 等伺服器應用程式也能將 VHD 檔案儲存在 SMB 檔案共用上。有了這些副檔名、就能為儲存資料和組態檔案在共享區上的虛擬機器取得應用程式一致的陰影複本。

遠端**VSS**概念

您應該瞭解一些必要概念、瞭解如何透過SMB組態搭配Hyper-V來使用遠端VSS（Volume陰影複製服務）。

- * VSS（Volume陰影複製服務）*

  一種Microsoft技術、用於在特定時間點、在特定磁碟區上製作資料的備份複本或快照。VSS可協調資料伺服器、備份應用程式和儲存管理軟體、以支援建立及管理一致的備份。

- 遠端**VSS**（遠端**Volume**陰影複製服務）

  一種Microsoft技術、用於在透過SMB 3.0共用存取資料的特定時間點、取得資料一致狀態的共用型資料備份複本。也稱為_ Volume陰影複製服務_。

- 陰影複製

  共享區中包含的一組重複資料、可在明確定義的即時時間內完成。陰影複製可用來建立一致的資料時間點備份、讓系統或應用程式能夠繼續更新原始磁碟區上的資料。

- 陰影複製集

  一或多個陰影複本的集合、每個陰影複本對應一個共用。陰影複製集中的陰影複製代表必須在相同作業中備份的所有共用。啟用VSS的應用程式上的VSS用戶端會識別要包含在集合中的陰影複本。

- 陰影複製集自動恢復

  備份程序的一部分、用於啟用VSS的遠端備份應用程式、其中包含陰影複製的複本目錄會使時間點保持一致。在備份開始時、應用程式上的VSS用戶端會觸發應用程式對排定要備份的資料（Hyper-V的虛擬機器檔案）執行軟體檢查點。然後VSS用戶端可讓應用程式繼續執行。建立陰影複製集之後、遠端VSS會將陰影複製集設為可寫入、並將可寫入的複本公開給應用程式。應用程式會使用先前取得的軟體檢查點執行自動還原、以準備陰影複製集以供備份。自動還原功能可復原自建立檢查點以來對檔案和目錄所做的變更、使陰影複製達到一致的狀態。自動還原是啟用VSS備份的選用步驟。

- 陰影複製**ID**

  唯一識別陰影複製的GUID。

- 陰影複製集**ID**

  唯一識別陰影複製識別碼集合到同一部伺服器的GUID。

- *適用於Hyper-V * SnapManager

  此軟體可自動化及簡化Microsoft Windows Server 2012 Hyper-V的備份與還原作業適用於Hyper-V的支援使用遠端VSS搭配自動還原功能、可透過SMB共用區來備份Hyper-V檔案。SnapManager

相關資訊

關於Hyper-V和SQL Server在SMB上不中斷營運的重要概念

使用遠端VSS進行共用型備份

遠端**VSS**使用的目錄結構範例

遠端VSS會在建立陰影複製時、遍歷儲存Hyper-V虛擬機器檔案的目錄結構。請務必瞭解適當的目錄結構、以便成功建立虛擬機器檔案的備份。

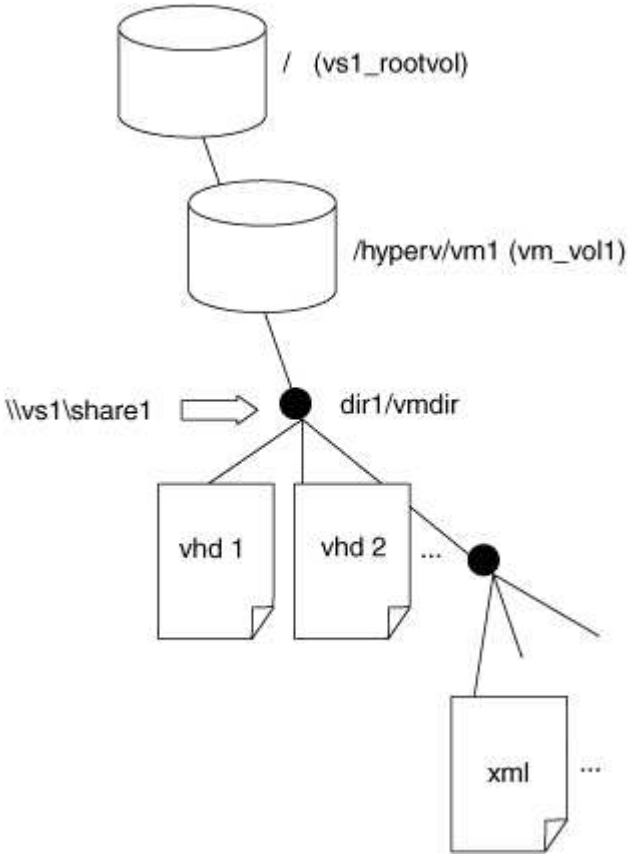
成功建立陰影複製所支援的目錄結構符合下列需求：

- 只有目錄和一般檔案存在於用來儲存虛擬機器檔案的目錄結構中。

  目錄結構不包含交會、連結或非一般檔案。

- 虛擬機器的所有檔案都位於單一共用區內。
- 用於儲存虛擬機器檔案的目錄結構不會超過陰影複製目錄的設定深度。
- 共用區的根目錄僅包含虛擬機器檔案或目錄。

在下圖中、建立名為 VM_vol1 的磁碟區時、會在其上建立連接點 `/hyperv/vm1` 儲存虛擬機器（ SVM ） VS1 上。包含虛擬機器檔案的子目錄會建立在交會點之下。Hyper-V 伺服器的虛擬機器檔案是透過具有路徑的共享 1 來存取 `/hyperv/vm1/dir1/vmdir`。陰影複製服務會建立所有虛擬機器檔案的陰影複製、這些檔案都包含在共享區1（直到陰影複製目錄設定的深度）下的目錄結構中。



適用於**Hyper-V**的解決方案**SnapManager** 如何透過**SMB**管理**Hyper-V**的遠端**VSS**型備份

您可以使用SnapManager 支援Hyper-V的支援功能來管理遠端VSS型備份服務。使用支援Hyper-V的託管備份服務來建立空間效率極高的備份集、有許多好處SnapManager 。

針對Hyper-V託管備份進行的最佳化包括：SnapManager

- 支援VMware的整合功能可在探索SMB共用位置時提供效能最佳化。SnapDrive ONTAP

  提供含有共享區所在Volume名稱的功能。ONTAP SnapDrive

- 針對Hyper-V、指定陰影複製服務需要複製的SMB共用中虛擬機器檔案清單。SnapManager

  藉由提供目標式虛擬機器檔案清單、陰影複製服務不需要建立共用中所有檔案的陰影複製。

- 儲存虛擬機器（ SVM ）會保留 SnapManager 的快照，以供 Hyper-V 用於還原。

  沒有備份階段。備份是節省空間的快照。

適用於Hyper-V的支援透過SMB為HyperV提供備份與還原功能、程序如下：SnapManager

1. 準備陰影複製作業

   適用於Hyper-V應用程式的VSS用戶端會設定陰影複製集。SnapManagerVSS用戶端會收集陰影複製集中要包含哪些共享的資訊、並將此資訊提供ONTAP 給效益管理系統。一組可能包含一或多個陰影複製、而一個陰影複製對應一個共用區。

2. 建立陰影複製集（如果使用自動還原）

   針對陰影複製集中的每個共用區ONTAP 、它會建立陰影複製、並使陰影複製可寫入。

3. 揭露陰影複製集

   在建立陰影複製之後ONTAP 、它們會暴露SnapManager 於適用於Hyper-V的功能、讓應用程式的VSS寫入器能夠執行自動還原。

4. 自動恢復陰影複製集

   在建立陰影複製集期間、備份集內的檔案會有一段時間發生作用中變更。應用程式的VSS寫入器必須更新陰影複本、以確保在備份前處於完全一致的狀態。

   自動還原的執行方式取決於應用程式。遠端VSS不涉及此階段。

5. 完成並清除陰影複製集

   VSS用戶端會在ONTAP 完成自動還原之後通知功能不全。陰影複製集會設為唯讀、然後準備好備份。使用SnapManager for Hyper-V 進行備份時，快照中的檔案會成為備份；因此，在備份階段，會為備份集中包含共用區的每個磁碟區建立快照。備份完成後、陰影複製集會從CIFS伺服器移除。

ODX複製卸載如何透過SMB共用搭配Hyper-V和SQL Server使用

卸載資料傳輸（ODX）也稱為_copy offload_、可在相容儲存裝置內或之間直接傳輸資料、而無需透過主機電腦傳輸資料。透過SMB安裝、在應用程式伺服器上執行複製作業時、利用VMware版複製卸載功能可為您帶來效能優勢。ONTAP

在非ODX檔案傳輸中、資料會從來源CIFS伺服器讀取、並透過網路傳輸至用戶端電腦。用戶端電腦會透過網路將資料傳輸回目的地CIFS伺服器。總而言之、用戶端電腦會從來源讀取資料、然後寫入目的地。使用ODX檔案傳輸時、資料會直接從來源複製到目的地。

由於ODX卸載複本是直接在來源與目的地儲存設備之間執行、因此效能優勢顯著。實現的效能效益包括加快來源與目的地之間的複製時間、降低用戶端上的資源使用率（CPU、記憶體）、以及降低網路I/O頻寬使用率。

```
 ONTAP ODX copy offload is supported on both SAN LUNs and SMB 3.0
continuously available connections.
```

下列使用案例支援使用ODX複本和移動：

- Volume內

  來源與目的地檔案或LUN位於同一個磁碟區內。

- 磁碟區間、相同節點、相同儲存虛擬機器（SVM）

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料歸同一個SVM所有。

- 磁碟區間、不同節點、相同SVM

來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料歸同一個SVM所有。

- SVM之間、相同節點

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料由不同的SVM擁有。

- SVM之間、不同節點

  來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料由不同的SVM擁有。

Hyper-V解決方案的ODX複製卸載特定使用案例包括：

- 您可以使用ODX複本卸載傳遞搭配Hyper-V、在虛擬硬碟（VHD）檔案內或之間複製資料、或在同一個叢集內的對應SMB共用區和連接的iSCSI LUN之間複製資料。

  如此一來、從客體作業系統的複本就能傳遞到基礎儲存設備。

- 建立固定大小的VHD時、ODX會使用已知的零權杖、以零初始化磁碟。
- 如果來源與目的地儲存設備位於同一個叢集、則ODX複本卸載可用於虛擬機器儲存移轉。

> ⓘ 若要利用ODX複本卸載傳遞與Hyper-V的使用案例、來賓作業系統必須支援ODX、而來賓作業系統的磁碟必須是支援ODX的儲存設備（SMB或SAN）所支援的SCSI磁碟。客體作業系統上的IDE磁碟不支援ODX傳遞。

SQL Server解決方案的ODX複製卸載特定使用案例包括：

- 您可以使用ODX複製卸載、在對應的SMB共用區之間、或是在同一個叢集內的SMB共用區與連線的iSCSI LUN之間匯出及匯入SQL Server資料庫。
- 如果來源與目的地儲存設備位於同一個叢集、則ODX複製卸載可用於資料庫匯出與匯入。

組態需求與考量

不需提供授權與授權**ONTAP**

在建立SQL Server或Hyper-V over SMB解決方案以在SVM上執行不中斷營運時、您必須瞭解ONTAP 特定的功能與授權需求。

版本需求**ONTAP**

- Hyper-V over SMB

  支援在SMB共用區上執行不中斷營運、以在Windows 2012或更新版本上執行Hyper-V。ONTAP

- SQL Server over SMB

  支援在SMB共用區上執行不中斷營運、適用於在Windows 2012或更新版本上執行的SQL Server 2012或更新版本。ONTAP

如需ONTAP 有關支援版本的支援、如需在SMB共用區上執行不中斷營運的更新資訊、請參閱互通性對照表（Interoperability Matrix）。

"NetApp 互通性對照表工具"

授權要求

需要下列授權：

- CIFS
- FlexClone（僅適用於SMB上的Hyper-V）

  如果使用遠端VSS進行備份、則需要此授權。陰影複製服務使用FlexClone來建立檔案的時間點複本、以便在建立備份時使用。

  如果您使用不使用遠端VSS的備份方法、則FlexClone授權為選用項目。

FlexClone 授權包含在"ONTAP One"中。如果您沒有 ONTAP One 、您應該"確認已安裝必要的授權"、以及"安裝它們"（如有必要）。

網路與資料**LIF**需求

在建立SQL Server或Hyper-V over SMB組態以進行不中斷營運時、您必須瞭解特定的網路和資料LIF需求）。

網路傳輸協定需求

- 支援IPV4和IPv6網路。
- 需要SMB 3.0或更新版本。

  SMB 3.0提供所需的功能、可建立持續可用的SMB連線、以提供不中斷營運的必要功能。

- DNS伺服器必須包含將CIFS伺服器名稱對應至指派給儲存虛擬機器（SVM）上資料LIF的IP位址的項目。

  在存取虛擬機器或資料庫檔案時、Hyper-V或SQL Server應用程式伺服器通常會透過多個資料生命體建立多個連線。為了正常運作、應用程式伺服器必須使用CIFS伺服器名稱來建立這類多個SMB連線、而非建立多個唯一IP位址的連線。

  見證也需要使用CIFS伺服器的DNS名稱、而非個別的LIF IP位址。

  從支援支援中小企業多通道技術的中小企業組態開始ONTAP 、您就能改善Hyper-V和SQL伺服器的處理量和容錯能力。若要這麼做、您必須在叢集和用戶端上部署多個1G、10G或更大的NIC。

資料**LIF**需求

- 透過SMB解決方案託管應用程式伺服器的SVM、必須在叢集中的每個節點上至少有一個作業資料LIF。

  SVM資料LIF可容錯移轉至叢集內的其他資料連接埠、包括目前未裝載應用程式伺服器所存取資料的節點。此外、由於見證節點永遠是應用程式伺服器所連接節點的SFO合作夥伴、因此叢集中的每個節點都是潛在的見證節點。

- 資料生命期不得設定為自動還原。

在接管或恢復事件之後、您應該手動將資料生命期還原至其主連接埠。

- 所有資料LIF IP位址都必須在DNS中有一個項目、而且所有項目都必須解析為CIFS伺服器名稱。

  應用程式伺服器必須使用CIFS伺服器名稱連線至SMB共用區。請勿將應用程式伺服器設定為使用 LIF IP 位址進行連線。

- 如果CIFS伺服器名稱與SVM名稱不同、則DNS項目必須解析為CIFS伺服器名稱。

SMB伺服器與磁碟區需求、適用於**SMB**上的**Hyper-V**

在建立Hyper-V over SMB組態以實現不中斷營運時、您必須注意特定的SMB伺服器和磁碟區需求。

SMB 伺服器需求

- 必須啟用SMB 3.0。

  此功能預設為啟用。

- 預設UNIX使用者CIFS伺服器選項必須設定有效的UNIX使用者帳戶。

  應用程式伺服器會在建立SMB連線時使用機器帳戶。由於所有SMB存取都需要Windows使用者成功對應至UNIX使用者帳戶或預設UNIX使用者帳戶、ONTAP 所以無法將應用程式伺服器的機器帳戶對應至預設的UNIX使用者帳戶。

- 必須停用自動節點參照（此功能預設為停用）。

  如果您想要使用自動節點參照來存取Hyper-V機器檔案以外的資料、則必須為該資料建立個別的SVM。

- 必須在SMB伺服器所屬的網域中同時允許Kerberos和NTLM驗證。

  不針對遠端VSS通告Kerberos服務、因此應將網域設定為允許使用NTLM。ONTAP

- 必須啟用陰影複製功能。

  此功能預設為啟用。

- 陰影複製服務在建立陰影複製時所使用的Windows網域帳戶、必須是SMB伺服器本機BUILTIN\Administrator或BUILTIN\Backup Operators群組的成員。

Volume需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

  若要使用持續可用的SMB連線、為應用程式伺服器提供NDOS、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並透過SMB共用區直接用於NDOS。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區的NDOS中使用、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 若要成功執行陰影複製作業、您必須在磁碟區上有足夠的可用空間。

可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。此需求僅適用於具有自動還原功能的陰影複製。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

SMB伺服器和磁碟區需求、適用於**SMB**以上的**SQL Server**

在透過SMB組態建立SQL Server以進行不中斷營運時、您必須瞭解特定的SMB伺服器和磁碟區需求。

SMB 伺服器需求

- 必須啟用SMB 3.0。

  此功能預設為啟用。

- 預設UNIX使用者CIFS伺服器選項必須設定有效的UNIX使用者帳戶。

  應用程式伺服器會在建立SMB連線時使用機器帳戶。由於所有SMB存取都需要Windows使用者成功對應至UNIX使用者帳戶或預設UNIX使用者帳戶、ONTAP 所以無法將應用程式伺服器的機器帳戶對應至預設的UNIX使用者帳戶。

  此外、SQL Server使用網域使用者做為SQL Server服務帳戶。服務帳戶也必須對應至預設的UNIX使用者。

- 必須停用自動節點參照（此功能預設為停用）。

  如果您想要使用自動節點參照來存取SQL Server資料庫檔案以外的資料、則必須為該資料建立個別的SVM。

- 用於將SQL Server安裝在ONTAP 更新上的Windows使用者帳戶必須指派SeSecurityPrivilege權限。

  此權限指派給SMB伺服器本機BUILTIN\Administrator群組。

Volume需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

  若要使用持續可用的SMB連線、為應用程式伺服器提供NDOS、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並透過SMB共用區直接用於NDOS。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區的NDOS中使用、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 雖然包含資料庫檔案的磁碟區可以包含連接點、但在建立資料庫目錄結構時、SQL Server不會交叉連接點。
- 為了讓Microsoft SQL Server備份作業順利完成、您必須在磁碟區上有足夠的可用空間。SnapCenter

  SQL Server資料庫檔案所在的磁碟區必須夠大、足以容納資料庫目錄結構、以及位於共用區內的所有內含檔案。

相關資訊

"Microsoft TechNet程式庫：technet.microsoft.com/en-us/library/"

持續可用的**SMB Hyper-V**共用需求與考量

在設定支援不中斷營運的Hyper-V over SMB組態的持續可用共用時、您必須瞭解特定的需求與考量。

共用需求

- 應用程式伺服器使用的共用必須設定為持續可用的內容集。

  連線至持續可用共用區的應用程式伺服器會接收持續的處理常式、以便在發生中斷事件（例如接管、恢復和集合重新配置）之後、不中斷地重新連線至SMB共用區、並回收檔案鎖定。

- 如果您想要使用啟用遠端VSS的備份服務、就無法將Hyper-V檔案放入包含連接的共用中。

  在自動還原案例中、如果在瀏覽共用區時遇到交會、陰影複製建立就會失敗。在非自動還原案例中、陰影複製建立並不會失敗、但交會不會指向任何內容。

- 如果您想要使用啟用遠端VSS的備份服務進行自動還原、就無法將Hyper-V檔案放入包含下列項目的共用區：
  - symlinks、hardlink或widelinks
  - 非一般檔案

    如果要陰影複製的共用區中有任何連結或非一般檔案、陰影複製建立就會失敗。此需求僅適用於具有自動還原功能的陰影複製。

  - 若要成功執行陰影複製作業、您必須在磁碟區上有足夠的可用空間（僅適用於SMB上的Hyper-V）。

    可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。此需求僅適用於具有自動還原功能的陰影複製。

- 應用程式伺服器所使用的持續可用共用區不得設定下列共用內容：
  - 主目錄
  - 屬性快取
  - BranchCache

考量

- 持續可用的共用支援配額。
- Hyper-V over SMB組態不支援下列功能：
  - 稽核
  - FPolicy
- 不會在與的 SMB 共用上執行病毒掃描 `continuously-availability` 參數設為 `Yes`。

持續可用的**SQL Server**與**SMB**之間的共用需求和考量

在設定支援不中斷營運的SMB組態上的SQL Server持續可用共用時、您必須瞭解特定的需求和考量。

共用需求

- 用於儲存虛擬機器檔案的磁碟區必須建立為NTFS安全型磁碟區。

  若要使用持續可用的SMB連線、為應用程式伺服器提供不中斷營運的作業、包含共用區的磁碟區必須是NTFS磁碟區。此外、它必須永遠是NTFS磁碟區。您無法將混合式安全型磁碟區或UNIX安全型磁碟區變更為NTFS安全型磁碟區、並將其直接用於透過SMB共用進行不中斷營運的作業。如果您將混合式安全型磁碟區變更為NTFS安全型磁碟區、並打算在SMB共用區上執行不中斷營運作業、則必須手動將ACL放在磁碟區頂端、並將該ACL傳播至所有內含的檔案和資料夾。否則、如果來源或目的地磁碟區最初建立為混合或UNIX安全型磁碟區、之後改為NTFS安全型態、則將檔案移至另一個磁碟區的虛擬機器移轉或資料庫檔案匯出及匯入可能會失敗。

- 應用程式伺服器使用的共用必須設定為持續可用的內容集。

  連線至持續可用共用區的應用程式伺服器會接收持續的處理常式、以便在發生中斷事件（例如接管、恢復和集合重新配置）之後、不中斷地重新連線至SMB共用區、並回收檔案鎖定。

- 雖然包含資料庫檔案的磁碟區可以包含連接點、但在建立資料庫目錄結構時、SQL Server不會交叉連接點。
- 為了讓Microsoft SQL Server作業順利完成、您必須在磁碟區上有足夠的可用空間。SnapCenter

  SQL Server資料庫檔案所在的磁碟區必須夠大、足以容納資料庫目錄結構、以及位於共用區內的所有內含檔案。

- 應用程式伺服器所使用的持續可用共用區不得設定下列共用內容：
  - 主目錄
  - 屬性快取
  - BranchCache

分享考量

- 持續可用的共用支援配額。
- 下列功能不支援SQL Server over SMB組態：
  - 稽核
  - FPolicy
- 不會在與的 SMB 共用上執行病毒掃描 `continuously-availability` 共用屬性集。

基於**SMB**組態的**Hyper-V**遠端**VSS**考量

在使用支援遠端VSS的備份解決方案進行Hyper-V over SMB組態時、您必須注意某些考量事項。

一般遠端**VSS**考量

- 每個Microsoft應用程式伺服器最多可設定64個共用區。

  如果陰影複製集中有超過64個共用區、陰影複製作業就會失敗。這是Microsoft的要求。

- 每部CIFS伺服器只允許一個作用中的陰影複製集。

  如果在同一部CIFS伺服器上持續執行陰影複製作業、陰影複製作業將會失敗。這是Microsoft的要求。

- 在遠端VSS建立陰影複製的目錄結構中、不允許任何交會。
  - 在自動還原案例中、如果在瀏覽共用區時遇到交會、陰影複製建立將會失敗。
  - 在非自動還原案例中、陰影複製建立並不會失敗、但交會不會指向任何內容。

遠端**VSS**考量、僅適用於具有自動還原功能的陰影複製

某些限制僅適用於具有自動還原功能的陰影複製。

- 建立陰影複製時、最多可允許五個子目錄的目錄深度。

  這是陰影複製服務建立陰影複製備份集的目錄深度。如果包含虛擬機器檔案的目錄巢狀深於五個層級、陰影複製建立就會失敗。這是為了限制複製共用時的目錄周遊。您可以使用CIFS伺服器選項來變更最大目錄深度。

- 磁碟區上的可用空間量必須足夠。

  可用空間必須至少與陰影複製備份集中所含共用區內的所有檔案、目錄及子目錄所使用的總空間相同。

- 在遠端VSS建立陰影複製的目錄結構中、不允許任何連結或非一般檔案。

  如果共用區中有任何連結或非一般檔案到陰影複製、陰影複製建立就會失敗。複製程序不支援。

- 目錄不允許使用NFSv4 ACL。

  雖然建立陰影複製會保留檔案上的NFSv4 ACL、但目錄上的NFSv4 ACL會遺失。

- 建立陰影複製集的時間上限為60秒。

  Microsoft規格允許建立陰影複製集的時間上限為60秒。如果VSS用戶端在此時間內無法建立陰影複製集、陰影複製作業將會失敗、因此會限制陰影複製集中的檔案數量。備份集中可包含的檔案或虛擬機器實際數量各不相同、這個數目取決於許多因素、而且必須針對每個客戶環境來決定。

SQL Server和**Hyper-V**在**SMB**上的**ODX**複製卸載需求

如果您想要移轉虛擬機器檔案、或直接從來源匯出及匯入資料庫檔案至目的地儲存位置、而不想透過應用程式伺服器傳送資料、則必須啟用ODX複本卸載。您必須瞭解使用ODX複製卸載搭配SQL Server和Hyper-V over SMB解決方案的特定需求。

使用ODX複本卸載可提供顯著的效能效益。此CIFS伺服器選項預設為啟用。

- 必須啟用SMB 3.0才能使用ODX複本卸載。

- 來源磁碟區至少必須為1.25 GB。
- 必須在使用複本卸載的磁碟區上啟用重複資料刪除功能。
- 如果您使用壓縮磁碟區、壓縮類型必須是可調適的、而且只支援8K大小的壓縮群組。

  不支援次要壓縮類型

- 若要使用ODX複本卸載來移轉磁碟內和磁碟之間的Hyper-V來賓、必須將Hyper-V伺服器設定為使用SCSI磁碟。

  預設是設定IDE磁碟、但如果使用IDE磁碟建立磁碟、則移轉來賓時ODX複製卸載無法運作。

SQL Server與Hyper-V over SMB組態的建議

為了確保SQL Server和Hyper-V over SMB組態健全且可運作、您必須熟悉建議的最佳實務做法、才能設定解決方案。

一般建議

- 將應用程式伺服器檔案與一般使用者資料分開。

  如果可能、請將整個儲存虛擬機器（SVM）及其儲存設備用於應用程式伺服器的資料。

- 為獲得最佳效能、請勿在用於儲存應用程式伺服器資料的SVM上啟用SMB簽署。
- 為獲得最佳效能及改善容錯能力、SMB多通道可在ONTAP 單一SMB工作階段中、在VMware與用戶端之間提供多重連線。
- 請勿在Hyper-V或SQL Server中使用的任何共享區上、透過SMB組態建立持續可用的共享區。
- 停用用於持續可用性之共用的變更通知。
- 請勿在執行Volume搬移的同時執行Aggregate重新配置（ARL）、因為ARL有會暫停某些作業的階段。
- 對於Hyper-V over SMB解決方案、請在建立叢集式虛擬機器時、使用來賓iSCSI磁碟機。共享 `.VHDX` ONTAP SMB 共用中的 Hyper-V over SMB 不支援檔案。

透過SMB組態規劃Hyper-V或SQL Server

完成**Volume**組態工作表

這份工作表提供一種簡單的方法、可記錄在建立SQL Server磁碟區和SMB上Hyper-V組態時所需的值。

對於每個Volume、您必須指定下列資訊：

- 儲存虛擬機器（SVM）名稱

  所有磁碟區的SVM名稱都相同。

- Volume名稱
- Aggregate名稱

您可以在叢集中任何節點上的集合體上建立磁碟區。

- 尺寸
- 交會路徑

建立用於儲存應用程式伺服器資料的磁碟區時、請謹記下列事項：

- 如果根磁碟區沒有NTFS安全樣式、則在建立磁碟區時、必須將安全樣式指定為NTFS。

  根據預設、磁碟區會繼承SVM根磁碟區的安全樣式。

- 磁碟區應設定預設磁碟區空間保證。
- 您可以選擇性地設定自動調整空間大小的管理設定。
- 您應該將確定快照空間保留的選項設置爲 `0`。
- 必須停用套用至磁碟區的快照原則。

  如果 SVM 快照原則已停用，則不需要為磁碟區指定快照原則。這些磁碟區會繼承 SVM 的快照原則。如果 SVM 的快照原則未停用，且設定為建立快照，則必須在 Volume 層級指定快照原則，且該原則必須停用。陰影複製服務型備份和 SQL Server 備份可管理快照的建立和刪除。

- 您無法為磁碟區設定負載共用鏡像。

您應選擇要在其中建立應用程式伺服器所使用之共用區的交會路徑、以便共用入口點下方不會有結定的磁碟區。

例如、如果您想要將虛擬機器檔案儲存在四個名為「vol1」、「vol2」、「vol3」和「vol4」的磁碟區、您可以建立範例中所示的命名空間。接著您可以在下列路徑為應用程式伺服器建立共用： `/data1/vol1`、`/data1/vol2`、 `/data2/vol3`和 `/data2/vol4`。

```
                    Junction                       Junction
Vserver Volume      Active   Junction Path         Path Source
------- ----------- -------- -------------------   -----------
vs1     data1        true     /data1               RW_volume
vs1     vol1         true     /data1/vol1          RW_volume
vs1     vol2         true     /data1/vol2          RW_volume
vs1     data2        true     /data2               RW_volume
vs1     vol3         true     /data2/vol3          RW_volume
vs1     vol4         true     /data2/vol4          RW_volume
```

資訊類型	價值
Volume 1：*Volume*名稱、*Aggregate*、大小、交會路徑	
Volume 2 ： Volume 名稱、 Aggregate 、大小、交會路徑 _	

資訊類型	價值
Volume 3 ： Volume 名稱、 Aggregate 、大小、交會路徑 _	
Volume 4 ： Volume 名稱、 Aggregate 、大小、交會路徑 _	
Volume 5 ： Volume 名稱、 Aggregate 、大小、交會路徑 _	
Volume 6 ： Volume 名稱、 Aggregate 、大小、交會路徑 _	
其他磁碟區：磁碟區名稱、*Aggregate*、大小、交會路徑	

完成**SMB**共用組態工作表

使用這份工作表單來記錄在建立SQL Server和Hyper-V over SMB組態的持續可用SMB共用時所需的值。

SMB的相關資訊會共用內容和組態設定

對於每個共用區、您必須指定下列資訊：

- 儲存虛擬機器（SVM）名稱

  SVM名稱與所有共用相同

- 共用名稱
- 路徑
- 共用內容

  您必須設定下列兩個共用內容：

  - `oplocks`
  - `continuously-available`

不得設定下列共用內容：

- `homedirectory attributecache`
- `branchcache`
- `access-based-enumeration`
  - 必須停用 symlinks （的值） `-symlink-properties` 參數必須為 null （「」）。

如果您使用遠端VSS來備份Hyper-V檔案、則在從Hyper-V伺服器建立SMB連線至儲存虛擬機器檔案的儲存位置時、選擇要使用的共用路徑非常重要。雖然可以在命名空間的任何點建立共用、但Hyper-V伺服器使用的共用路徑不應包含輔助磁碟區。陰影複製作業無法在包含交會點的共用路徑上執行。

建立資料庫目錄結構時、SQL Server無法跨交會。您不應該為包含交會點的SQL Server建立共用路徑。

例如、如果您想要將虛擬機器檔案或資料庫檔案儲存在磁碟區 “vol1” 、 “vol2” 、 “vol3” 及 “vol4” 上、請在下列路徑為應用程式伺服器建立共用： `/data1/vol1`、 `/data1/vol2`、 `/data2/vol3`和 `/data2/vol4`。

```
                    Junction                          Junction
Vserver Volume      Active   Junction Path            Path Source
------- ----------- -------- -------------------      -----------
vs1     data1        true     /data1                  RW_volume
vs1     vol1         true     /data1/vol1             RW_volume
vs1     vol2         true     /data1/vol2             RW_volume
vs1     data2        true     /data2                  RW_volume
vs1     vol3         true     /data2/vol3             RW_volume
vs1     vol4         true     /data2/vol4             RW_volume
```

雖然您可以在和 `/data2`路徑上建立共用以進行管理，但 `/data1`請勿將應用程式伺服器設定為使用這些共用來儲存資料。

規劃工作表

資訊類型	價值
Volume 1：*SMB*共用名稱和路徑	
Volume 2 ： SMB 共享名稱和路徑 _	
_Volume 3：SMB共用名稱和路徑	
Volume 4：*SMB*共用名稱與路徑	
Volume 5 ： SMB 共享名稱和路徑 _	
Volume 6 ： SMB 共享名稱和路徑 _	
Volume 7 ： SMB 共享名稱和路徑 _	
其他磁碟區：*SMB*共用名稱和路徑	

利用ONTAP Hyper-V和SQL Server、透過SMB建立不中斷營運的支援組態

利用ONTAP Hyper-V和SQL Server over SMB總覽建立不中斷營運的支援組態

您必須執行幾ONTAP 個支援功能的組態步驟、才能準備好在SMB上執行不中斷營運的Hyper-V和SQL Server安裝。

在您透過ONTAP SMB建立不中斷營運的Hyper-V和SQL Server的支援功能之前、必須先完成下列工作：

- 必須在叢集上設定時間服務。
- 必須為SVM設定網路。
- 必須建立SVM。
- 必須在SVM上設定資料LIF介面。
- 必須在SVM上設定DNS。
- 必須為SVM設定所需的名稱服務。
- 必須建立 SMB 伺服器。

相關資訊

透過SMB組態規劃Hyper-V或SQL Server

組態需求與考量

驗證是否同時允許Kerberos和NTLMv2驗證（Hyper-V over SMB共享）

Hyper-V over SMB的不中斷營運需要資料SVM和Hyper-V伺服器上的CIFS伺服器同時允許Kerberos和NTLMv2驗證。您必須驗證CIFS伺服器和Hyper-V伺服器上的設定、以控制允許的驗證方法。

關於這項工作

建立持續可用的共用連線時、必須進行Kerberos驗證。遠端VSS程序的一部分使用了NTLMv2驗證。因此、Hyper-V over SMB組態必須支援使用這兩種驗證方法的連線。

下列設定必須設定為允許Kerberos和NTLMv2驗證：

- 必須在儲存虛擬機器（SVM）上停用SMB的匯出原則。

在SVM上一律會啟用Kerberos和NTLMv2驗證、但匯出原則可用來根據驗證方法來限制存取。

SMB的匯出原則是選用的、預設為停用。如果停用匯出原則、則CIFS伺服器預設會允許Kerberos和NTLMv2驗證。

- CIFS伺服器和Hyper-V伺服器所屬的網域必須同時允許Kerberos和NTLMv2驗證。

Active Directory網域預設會啟用Kerberos驗證。不過、可以使用「安全性原則」設定或「群組原則」來禁止NTLMv2驗證。

步驟

1. 請執行下列步驟、確認SVM上的匯出原則已停用：
   a. 將權限層級設為進階：

      set -privilege advanced

   b. 確認 `-is-exportpolicy-enabled` CIFS 伺服器選項設為 `false`：

      vserver cifs options show -vserver *vserver_name* -fields vserver,is-exportpolicy-enabled

   c. 返回管理權限層級：

      set -privilege admin

2. 如果未停用SMB的匯出原則、請停用這些原則：

   vserver cifs options modify -vserver *vserver_name* -is-exportpolicy-enabled false

3. 確認網域中同時允許使用NTLMv2和Kerberos驗證。

   如需判斷網域中允許使用哪些驗證方法的相關資訊，請參閱Microsoft TechNet程式庫。

4. 如果網域不允許NTMLv2驗證、請使用Microsoft文件中所述的其中一種方法來啟用NTLMv2驗證。

範例

下列命令可驗證SVM VS1上的SMB匯出原則是否已停用：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields vserver,is-
exportpolicy-enabled

vserver  is-exportpolicy-enabled
-------- ------------------------
vs1      false

cluster1::*> set -privilege admin
```

確認網域帳戶對應至 **ONTAP** 中的預設 **UNIX** 使用者

Hyper-V和SQL Server使用網域帳戶建立SMB連線、以連線至持續可用的共用區。若要成功建立連線、電腦帳戶必須成功對應至UNIX使用者。完成此作業最方便的方法是將電腦帳戶對應至預設UNIX使用者。

關於這項工作

Hyper-V和SQL Server使用網域電腦帳戶建立SMB連線。此外、SQL Server也會使用網域使用者帳戶做為進行SMB連線的服務帳戶。

建立儲存虛擬機器 (SVM) 時，ONTAP 會自動建立名為 `pcuser` （UID 為 `65534`) 和名為 `pcuser` （GID 為 `65534` ），並將預設使用者新增至 `pcuser`團體。如果您要在將叢集升級Data ONTAP 至S8.2之前、在現有的AnSVM上設定Hyper-V over SMB解決方案、則預設使用者和群組可能不存在。如果沒有、您必須先建立這些項目、才能設定CIFS伺服器的預設UNIX使用者。

步驟

1. 判斷是否有預設的UNIX使用者：

```
vserver cifs options show -vserver <vserver_name>
```

2. 如果未設定預設使用者選項、請判斷是否有UNIX使用者可以指定為預設UNIX使用者：

```
vserver services unix-user show -vserver <vserver_name>
```

3. 如果未設定預設用戶選項，且沒有可指定為預設 UNIX 用戶的 UNIX 用戶，則建立預設群組和預設 UNIX 用戶，並將預設用戶新增至該群組。

   通常，預設使用者的使用者名稱是“pcuser”，並且必須分配 UID `65534` .預設群組一般被賦予群組名稱“pcuser”。指派給群組的 GID 必須是 `65534`。

   a. 建立預設群組：

```
vserver services unix-group create -vserver <vserver_name> -name
pcuser -id 65534
```

   b. 建立預設使用者、並將預設使用者新增至預設群組：

```
vserver services unix-user create -vserver <vserver_name> -user
pcuser -id 65534 -primary-gid 65534
```

   c. 確認已正確設定預設使用者和預設群組：

```
vserver services unix-user show -vserver <vserver_name>
```

```
vserver services unix-group show -vserver <vserver_name> -members
```

4. 如果未設定CIFS伺服器的預設使用者、請執行下列步驟：

a. 設定預設使用者：

```
vserver cifs options modify -vserver <vserver_name> -default-unix
-user pcuser
```

b. 確認預設UNIX使用者已正確設定：

```
vserver cifs options show -vserver <vserver_name>
```

5. 若要驗證應用程式伺服器的電腦帳戶是否正確對應至預設使用者、請將磁碟機對應至 SVM 上的共用、然後使用確認 Windows 使用者與 UNIX 使用者的對應 `vserver cifs session show` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver cifs options`資訊，請參閱。

範例

。 `pcuser`使用者被指定為 SVM vs1 上的 CIFS 伺服器的預設使用者。

```
cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : -
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -



cluster1::> vserver services unix-user show
          User            User   Group  Full
Vserver   Name            ID     ID     Name
--------- --------------- ------ ------ ----------------
vs1       nobody          65535  65535  -
vs1       pcuser          65534  65534  -
vs1       root            0      1      -

cluster1::> vserver services unix-group show -members
Vserver        Name                ID
vs1            daemon              1
       Users: -
vs1            nobody              65535
```

```
       Users: -
vs1            pcuser              65534
       Users: -
vs1            root                0
       Users: -

cluster1::> vserver cifs options modify -vserver vs1 -default-unix-user
pcuser

cluster1::> vserver cifs options show

Vserver: vs1

  Client Session Timeout : 900
  Default Unix Group     : -
  Default Unix User      : pcuser
  Guest Unix User        : -
  Read Grants Exec       : disabled
  Read Only Delete       : disabled
  WINS Servers           : -
```

確認**SVM**根磁碟區的安全樣式已設定為**NTFS**

為了確保Hyper-V和SQL Server在SMB上的不中斷營運成功、磁碟區必須以NTFS安全型態建立。由於根磁碟區的安全性樣式預設會套用至儲存虛擬機器（SVM）上建立的磁碟區、因此根磁碟區的安全性樣式應設定為NTFS。

關於這項工作

- 您可以在建立SVM時指定根磁碟區的安全樣式。
- 如果建立 SVM 時根磁碟區未設定為 NTFS 安全樣式、您可以稍後使用變更安全樣式 `volume modify` 命令。

步驟

1. 判斷SVM根磁碟區目前的安全樣式：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

2. 如果根磁碟區不是NTFS安全型磁碟區、請將安全樣式變更為NTFS：

   volume modify -vserver *vserver_name* -volume root_volume_name -security-style ntfs

3. 確認SVM根磁碟區已設定為NTFS安全樣式：

   volume show -vserver *vserver_name* -fields vserver,volume,security-style

範例

下列命令可驗證SVM VS1上的根磁碟區安全樣式是否為NTFS：

```
cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   unix

cluster1::> volume modify -vserver vs1 -volume vs1_root -security-style
ntfs

cluster1::> volume show -vserver vs1 -fields vserver,volume,security-style
vserver  volume     security-style
-------- ---------- --------------
vs1      vs1_root   ntfs
```

確認已設定必要的**CIFS**伺服器選項

您必須確認已根據Hyper-V和SQL Server在SMB上的不中斷營運需求、啟用並設定所需的CIFS伺服器選項。

關於這項工作

- 必須啟用SMB 2.x和SMB 3.0。
- 必須啟用ODX複本卸載、才能使用效能提升的複本卸載功能。
- 如果Hyper-V over SMB解決方案使用支援遠端VSS的備份服務（僅限Hyper-V）、則必須啟用VSS陰影複製服務。

步驟

1. 確認儲存虛擬機器（SVM）上已啟用所需的CIFS伺服器選項：
   a. 將權限層級設為進階：

      set -privilege advanced

   b. 輸入下列命令：

      vserver cifs options show -vserver *vserver_name*

      下列選項應設定為 `true`：

      - `-smb2-enabled`
      - `-smb3-enabled`
      - `-copy-offload-enabled`
      - `-shadowcopy-enabled` （僅適用於 Hyper-V ）
2. 如果任何選項未設定為 `true`，請執行下列步驟：
   a. 將它們設為 `true` 使用 `vserver cifs options modify` 命令。

b. 確認選項已設定為 `true` 使用 `vserver cifs options show` 命令。

3. 返回管理權限層級：

```
set -privilege admin
```

範例

下列命令可驗證SVM VS1上是否已啟用Hyper-V over SMB組態所需的選項。在此範例中、ODX複本卸載必須啟用、才能符合選項需求。

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options show -vserver vs1 -fields smb2-
enabled,smb3-enabled,copy-offload-enabled,shadowcopy-enabled
vserver smb2-enabled smb3-enabled copy-offload-enabled shadowcopy-enabled
------- ------------ ------------ -------------------- ------------------
vs1     true         true         false                true

cluster-1::*> vserver cifs options modify -vserver vs1 -copy-offload
-enabled true

cluster-1::*> vserver cifs options show -vserver vs1 -fields copy-offload-
enabled
vserver  copy-offload-enabled
-------- --------------------
vs1      true

cluster1::*> set -privilege admin
```

設定**SMB**多通道以獲得效能與備援

從支援支援支援的9.4開始ONTAP 、您可以設定SMB多通道、ONTAP 在單一SMB工作階段中、在支援的情況下提供多個連接功能。這樣做可改善Hyper-V和SQL Server在SMB組態上的處理量和容錯能力。

開始之前

只有當用戶端在SMB 3.0或更新版本上進行交涉時、才能使用SMB多通道功能。根據預設、SMB 3.0及更新版本會在ONTAP 支援SMB的伺服器上啟用。

關於這項工作

如果ONTAP 在故障叢集上識別出適當的組態、SMB用戶端會自動偵測並使用多個網路連線。

SMB工作階段中的同時連線數目取決於您已部署的NIC：

- *用戶端和ONTAP 叢集上的1G NIC *

  用戶端每個NIC建立一個連線、並將工作階段連結至所有連線。

- *用戶端與ONTAP 支援叢集*上的10G與更大容量NIC

  用戶端每個NIC最多可建立四個連線、並將工作階段連結至所有連線。用戶端可在多個10G和更大容量的NIC上建立連線。

您也可以修改下列參數（進階權限）：

- `-max-connections-per-session`

  每個多通道工作階段允許的最大連線數。預設為32個連線。

  如果您想要啟用比預設值更多的連線、則必須對用戶端組態進行類似的調整、也就是預設的32個連線。

- `-max-lifs-per-session`

  每個多通道工作階段所通告的網路介面數量上限。預設為256個網路介面。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 在SMB伺服器上啟用SMB多通道：

```
vserver cifs options modify -vserver <vserver_name> -is-multichannel
-enabled true
```

3. 驗證ONTAP 此功能是否回報SMB多通道工作階段：

```
vserver cifs session show
```

4. 返回管理權限層級：

```
set -privilege admin
```

範例

下列範例顯示所有SMB工作階段的相關資訊、顯示單一工作階段的多個連線：

```
cluster1::> vserver cifs session show
Node:    node1
Vserver: vs1
Connection Session                                          Open
Idle
IDs        ID      Workstation      Windows User          Files
Time
---------- ------- ---------------- ---------------- ---------
---------------
138683,
138684,
138685     1       10.1.1.1         DOMAIN\                   0
4s
                                    Administrator
```

下列範例顯示使用工作階段ID 1之SMB工作階段的詳細資訊：

```
cluster1::> vserver cifs session show -session-id 1 -instance

Vserver: vs1
                            Node: node1
                      Session ID: 1
                  Connection IDs: 138683,138684,138685
               Connection Count: 3
   Incoming Data LIF IP Address: 192.1.1.1
         Workstation IP Address: 10.1.1.1
       Authentication Mechanism: NTLMv1
          User Authenticated as: domain-user
                   Windows User: DOMAIN\administrator
                      UNIX User: root
                    Open Shares: 2
                     Open Files: 5
                     Open Other: 0
                  Connected Time: 5s
                       Idle Time: 5s
               Protocol Version: SMB3
         Continuously Available: No
              Is Session Signed: false
                   NetBIOS Name: -
```

建立**NTFS**資料磁碟區

您必須先在儲存虛擬機器（SVM）上建立NTFS資料磁碟區、然後才能透過SMB應用程式伺服器設定持續可用的共用區、以便搭配Hyper-V或SQL Server使用。使用Volume組態工

作表建立資料磁碟區。

關於這項工作

您可以使用選用參數來自訂資料Volume。如需自訂磁碟區的詳細資訊、請參閱 "邏輯儲存管理"。

建立資料磁碟區時、不應在包含下列項目的磁碟區內建立交會點：

- Hyper-V檔案ONTAP 、用於製作陰影複製
- 使用SQL Server備份的SQL Server資料庫檔案

> 如果您不慎建立使用混合式或UNIX安全性樣式的磁碟區、則無法將磁碟區變更為NTFS安全性樣式磁碟區、然後直接使用它來建立持續可用的共用區、以利不中斷營運。除非將組態中使用的磁碟區建立為NTFS安全型磁碟區、否則Hyper-V和SQL Server在SMB上的不中斷營運將無法正常運作。您必須刪除磁碟區並以NTFS安全型態重新建立磁碟區、 或者、您也可以在Windows主機上對應磁碟區、並在磁碟區頂端套用ACL、然後將ACL傳播到磁碟區中的所有檔案和資料夾。

步驟

1. 輸入適當的命令來建立資料Volume：

如果您想要在**SVM**中建立磁碟區、而根磁碟區的安全樣式是...	輸入命令...
NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB] -junction-path path`
非NTFS	`volume create -vserver vserver_name -volume volume_name -aggregate aggregate_name -size integer[KB|MB|GB|TB|PB]- security-style ntfs -junction-path path`

2. 驗證Volume組態是否正確：

```
volume show -vserver vserver_name -volume volume_name
```

建立持續可用的**SMB**共用區

建立資料磁碟區之後、您可以建立持續可用的共用區、讓應用程式伺服器用來存取Hyper-V虛擬機器、組態檔和SQL Server資料庫檔案。您應該在建立SMB共用時使用共用組態工作表。

步驟

1. 顯示現有資料磁碟區及其交會路徑的相關資訊：

```
volume show -vserver vserver_name -junction
```

2. 建立持續可用的SMB共用區：

vserver cifs share create -vserver *vserver_name* -share-name *share_name* -path *path* -share-properties oplocks,continuously-available -symlink "" [-comment text]

- 您可以選擇性地將註解新增至共用組態。
- 根據預設、離線檔案共用屬性是在共用上設定、並設為 `manual`。
- ONTAP 會建立具有 Windows 預設共用權限的共用 `Everyone` / `Full Control`。

3. 針對共用組態工作表中的所有共用重複上一個步驟。
4. 使用確認您的組態正確無誤 `vserver cifs share show` 命令。
5. 將磁碟機對應至每個共用區、並使用* Windows內容*視窗設定檔案權限、即可在持續可用的共用區上設定NTFS檔案權限。

範例

下列命令可在儲存虛擬機器（SVM、先前稱為Vserver）VS1上建立名為「data2」的持續可用共用區。透過設定、符號連結會停用 `-symlink` 參數至 `""`：

```
cluster1::> volume show -vserver vs1 -junction
                      Junction                  Junction
Vserver   Volume      Active   Junction Path    Path Source
--------- ----------- -------- ---------------- ------------
vs1       data        true     /data            RW_volume
vs1       data1       true     /data/data1      RW_volume
vs1       data2       true     /data/data2      RW_volume
vs1       vs1_root    -        /                -

cluster1::> vserver cifs share create -vserver vs1 -share-name data2 -path
/data/data2 -share-properties oplocks,continuously-available -symlink ""

cluster1::> vserver cifs share show -vserver vs1 -share-name data2

                      Vserver: vs1
                        Share: data2
     CIFS Server NetBIOS Name: VS1
                         Path: /data/data2
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

將**SeSecurityPrivilege**權限新增至使用者帳戶（適用於**SMB**共用的**SQL Server**）

用於安裝SQL伺服器的網域使用者帳戶必須指派「eSecurity權限」權限、才能在CIFS伺服器上執行某些動作、而這些動作需要預設未指派給網域使用者的權限。

開始之前

用於安裝SQL Server的網域帳戶必須已經存在。

關於這項工作

將權限新增至SQL Server安裝程式的帳戶時ONTAP 、可能會聯絡網域控制器來驗證帳戶。如果無法聯絡網域控制器、則指令可能會失敗ONTAP 。

步驟

1. 新增「eSecurity權限」權限：

vserver cifs users-and-groups privilege add-privilege -vserver *vserver_name* -user-or-group-name *account_name* -privileges SeSecurityPrivilege

的值 `-user-or-group-name` 參數是用於安裝 SQL Server 的網域使用者帳戶名稱。

2. 確認已將權限套用至帳戶：

vserver cifs users-and-groups privilege show -vserver *vserver_name* -user-or-group-name *account_name*

範例

下列命令會在儲存虛擬機器（SVM）VS1的範例網域中、將「『安全性權限』」權限新增至SQL Server安裝程式的帳戶：

```
cluster1::> vserver cifs users-and-groups privilege add-privilege -vserver
vs1 -user-or-group-name EXAMPLE\SQLinstaller -privileges
SeSecurityPrivilege

cluster1::> vserver cifs users-and-groups privilege show -vserver vs1
Vserver   User or Group Name           Privileges
--------- ---------------------       ---------------
vs1       EXAMPLE\SQLinstaller        SeSecurityPrivilege
```

設定**VSS**陰影複製目錄深度（適用於**SMB**共用上的**Hyper-V**）

您也可以在SMB共用區內設定最大目錄深度、以便建立陰影複製。如果您想要手動控制ONTAP 子目錄的最大層級、以便在其中建立陰影複製、則此參數非常實用。

開始之前

必須啟用VSS陰影複製功能。

關於這項工作

預設為建立最多五個子目錄的陰影複本。如果值設為 `0`， ONTAP 會為所有子目錄建立陰影複本。

> 雖然您可以指定陰影複製集目錄深度包含五個子目錄或所有子目錄、但Microsoft要求陰影複製集建立必須在60秒內完成。如果目前無法完成陰影複製集建立、則陰影複製集會失敗。您選擇的陰影複製目錄深度不得導致建立時間超過時間限制。

步驟

1. 將權限層級設為進階：

set -privilege advanced

2. 將VSS陰影複製目錄深度設定為所需的層級：

vserver cifs options modify -vserver *vserver_name* -shadowcopy-dir-depth integer

```
vserver cifs options modify -vserver vs1 -shadowcopy-dir-depth 6
```

3. 返回管理權限層級：

```
set -privilege admin
```

透過SMB組態管理Hyper-V和SQL Server

設定現有共用以確保持續可用度

您可以修改現有的共用區、使其成為持續可用的共用區、讓Hyper-V和SQL Server應用程式伺服器在不中斷營運的情況下存取Hyper-V虛擬機器和組態檔、以及SQL Server資料庫檔案。

關於這項工作

如果共用具有下列特性、您就無法將現有共用區用作持續可用的共用區、以便透過SMB與應用程式伺服器進行不中斷營運：

- 如果是 `homedirectory` 共用屬性是在該共用上設定
- 如果共用包含已啟用的symlink或wdelinks
- 如果共用區包含位於共用根目錄下方的輔助磁碟區

您必須確認下列兩個共用參數設定正確：

- 。 `-offline-files` 參數設為任一 `manual` （預設）或 `none`。
- 必須停用symlink。

必須設定下列共用內容：

- `continuously-available`
- `oplocks`

不得設定下列共用內容。如果目前共用內容清單中有這些內容、則必須從持續可用的共用區中移除：

- `attributecache`
- `branchcache`

步驟

1. 顯示目前的共用參數設定和目前設定的共用內容清單：

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
```

2. 如有必要、請使用命令修改共用參數以停用 symlink 、並將離線檔案設為手動 `vserver cifs share modify` 。
   - 您可以設定的值來停用符號連結 `-symlink` 參數至 `""`。

。您可以設定 `-offline-files` 指定參數至正確的設定 `manual`。

3. 新增 Share 屬性、並視需要新增 `continuously-available` `oplocks` Share 屬性：

```
vserver cifs share properties add -vserver <vserver_name> -share-name
<share_name> -share-properties continuously-available[,oplock]
```

如果是 `oplocks` 尚未設定共用屬性、您必須將其與一起新增 `continuously-available` 共用屬性。

4. 移除持續可用共用區上不支援的任何共用內容：

```
vserver cifs share properties remove -vserver <vserver_name> -share-name
<share_name> -share-properties properties[,...]
```

您可以使用以逗號分隔的清單來指定共用屬性、以移除一或多個共用屬性。

5. 確認 `-symlink` 和 `-offline-files` 參數設定正確：

```
vserver cifs share show -vserver <vserver_name> -share-name <share_name>
-fields symlink-properties,offline-files
```

6. 確認已設定的共用內容清單正確無誤：

```
vserver cifs share properties show -vserver <vserver_name> -share-name
<share_name>
```

範例

以下範例說明如何在儲存虛擬機器（ SVM ）「 VS1 」上、針對 NDOS 設定名為「 share1 」的現有共享區、並透過 SMB 設定應用程式伺服器：

- 將參數設定為、即可在共用區上停用 symlinks `-symlink ""`。
- 。 `-offline-file` 參數已修改並設為 `manual`。
- 。 `continuously-available` 共用屬性即會新增至共用。
- 。 `oplocks` 共用屬性已在共用屬性清單中、因此不需要新增。
- 。 `attributecache` 共用內容即會從共用中移除。
- 。 `browsable` 對於透過 SMB 與應用程式伺服器使用的 NDOS 持續可用共用區、則可選用 Share 屬性、並保留為其中一個共用屬性。

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1

                      Vserver: vs1
                        Share: share1
     CIFS Server NetBIOS Name: vs1
                         Path: /data
             Share Properties: oplocks
                               browsable
                               attributecache
           Symlink Properties: enable
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: 10s
                  Volume Name: data
                Offline Files: documents
Vscan File-Operations Profile: standard

cluster1::> vserver cifs share modify -vserver vs1 -share-name share1
-offline-file manual -symlink ""

cluster1::> vserver cifs share properties add -vserver vs1 -share-name
share1 -share-properties continuously-available

cluster1::> vserver cifs share properties remove -vserver vs1 -share-name
share1 -share-properties attributecache

cluster1::> vserver cifs share show -vserver vs1 -share-name share1
-fields symlink-properties,offline-files
vserver  share-name symlink-properties offline-files
-------- ---------- ------------------ -------------
vs1      share1    -                  manual

cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1

         Vserver: vs1
           Share: share1
Share Properties: oplocks
                  browsable
                  continuously-available
```

啟用或停用適用於**SMB**備份上**Hyper-V**的**VSS**陰影複製

如果您使用支援VSS的備份應用程式來備份儲存在SMB共用區上的Hyper-V虛擬機器檔案、則必須啟用VSS陰影複製。如果您不使用支援VSS的備份應用程式、可以停用VSS陰影複製。預設為啟用VSS陰影複製。

關於這項工作

您可以隨時啟用或停用VSS陰影複製。

步驟

1. 將權限層級設為進階：

   set -privilege advanced

2. 執行下列其中一項動作：

如果您想要**VSS**陰影複製...	輸入命令...
已啟用	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled true**
已停用	**vserver cifs options modify -vserver *vserver_name* -shadowcopy-enabled false**

3. 返回管理權限層級：

   set -privilege admin

範例

下列命令可在SVM VS1上啟用VSS陰影複製：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support personnel.
Do you wish to continue? (y or n): y

cluster1::*> vserver cifs options modify -vserver vs1 -shadowcopy-enabled
true

cluster1::*> set -privilege admin
```

使用統計資料、透過**SMB**監控**Hyper-V**和**SQL Server**活動

判斷 **ONTAP** 中可用的統計資料物件和計數器

在取得CIFS、SMB、稽核和BranchCache雜湊統計資料的相關資訊及監控效能之前、您必

須先知道哪些物件和計數器可供您取得資料。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 執行下列其中一項動作：

如果您想要判斷...	輸入...
可用的物件	`statistics catalog object show`
可用的特定物件	`statistics catalog object show -object` *`object_name`*
可用的計數器	`statistics catalog counter show -object` *`object_name`*

   詳細了解 `statistics catalog object show`和 `statistics catalog counter show`在"指令參考資料ONTAP" 。

3. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

下列命令會顯示與叢集中CIFS和SMB存取相關之所選統計物件的說明、如進階權限層級所示：

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog object show -object audit
    audit_ng                    CM object for exporting audit_ng
performance counters

cluster1::*> statistics catalog object show -object cifs
    cifs                        The CIFS object reports activity of the
                                Common Internet File System protocol
                                ...

cluster1::*> statistics catalog object show -object nblade_cifs
    nblade_cifs                 The Common Internet File System (CIFS)
                                protocol is an implementation of the
Server
                                ...

cluster1::*> statistics catalog object show -object smb1
    smb1                        These counters report activity from the
SMB
                                revision of the protocol. For information
                                ...

cluster1::*> statistics catalog object show -object smb2
    smb2                        These counters report activity from the
                                SMB2/SMB3 revision of the protocol. For
                                ...

cluster1::*> statistics catalog object show -object hashd
    hashd                       The hashd object provides counters to
measure
                                the performance of the BranchCache hash
daemon.
cluster1::*> set -privilege admin
```

下列命令會顯示的一些計數器相關資訊 `cifs` 進階權限層級的物件：

> 此範例不會顯示的所有可用計數器 `cifs` 物件；輸出被截斷。

```
cluster1::> set -privilege advanced

Warning: These advanced commands are potentially dangerous; use them only
when directed to do so by support personnel.
Do you want to continue? {y|n}: y

cluster1::*> statistics catalog counter show -object cifs

Object: cifs
    Counter                     Description
    --------------------------
--------------------------------------------
    active_searches             Number of active searches over SMB and
SMB2
    auth_reject_too_many        Authentication refused after too many
                                requests were made in rapid succession
    avg_directory_depth         Average number of directories crossed by
SMB
                                and SMB2 path-based commands
    ...                         ...

cluster2::> statistics start -object client -sample-id
Object: client
    Counter                                                     Value
    -------------------------------- --------------------------------
    cifs_ops                                                        0
    cifs_read_ops                                                   0
    cifs_read_recv_ops                                              0
    cifs_read_recv_size                                            0B
    cifs_read_size                                                 0B
    cifs_write_ops                                                  0
    cifs_write_recv_ops                                             0
    cifs_write_recv_size                                           0B
    cifs_write_size                                                0B
    instance_name                                vserver_1:10.72.205.179
    instance_uuid                                       2:10.72.205.179
    local_ops                                                       0
    mount_ops                                                       0


[...]
```

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

在 **ONTAP** 中顯示 **SMB** 統計資料

您可以顯示各種SMB統計資料、以監控效能及診斷問題。

步驟

1. 使用 `statistics start` 和選用 `statistics stop` 用於收集資料範例的命令。
2. 執行下列其中一項動作：

如果您要顯示下列項目的統計資料...	輸入下列命令...
SMB的所有版本	**`statistics show -object cifs`**
SMB 1.0	**`statistics show -object smb1`**
SMB 2.x和SMB 3.0	**`statistics show -object smb2`**
節點的 SMB 子系統	**`statistics show -object nblade_cifs`**

相關資訊

- "統計數據顯示"
- "統計開始"
- "統計停止"

驗證組態是否能夠不中斷營運

使用健全狀況監控來判斷不中斷營運狀態是否健全

健全狀況監控提供有關整個叢集系統健全狀況狀態的資訊。健全狀況監視器會透過SMB組態監控Hyper-V和SQL Server、以確保應用程式伺服器的營運不中斷（NDOS）。如果狀態為降級、您可以檢視問題的詳細資料、包括可能原因和建議的還原動作。

有多個健全狀況監視器。此功能可監控個別健全狀況監視器的整體系統健全狀況和健全狀況。ONTAP節點連線能力健全狀況監視器包含CIFS/NDO子系統。監視器有一組健全狀況原則、可在特定實體狀況可能導致中斷時觸發警示、如果發生中斷情況、則會產生警示並提供修正行動的相關資訊。對於SMB組態而言、會針對下列兩種情況產生警示：

警示**ID**	嚴重性	條件
`HaNotReadyCifsNdo_Alert`	主要	節點上某個集合體中某個磁碟區所裝載的一或多個檔案、已透過持續可用的SMB共用區開啟、並承諾在發生故障時持續存在；不過、HA與該合作夥伴的關係可能未設定或不健全。

警示ID	嚴重性	條件
NoStandbyLifCifsNdo_Alert	次要	儲存虛擬機器（SVM）正透過節點主動透過SMB提供資料、且持續在持續可用的共用區上開啟SMB檔案；然而、其合作夥伴節點並未揭露SVM的任何作用中資料生命期。

使用系統健全狀況監控來顯示不中斷營運狀態

您可以使用 `system health` 顯示叢集整體系統健全狀況和 CIFS-n 子系統健全狀況的相關資訊、回應警示、設定未來警示、以及顯示如何設定健全狀況監控的資訊。

步驟

1. 執行適當的動作來監控健全狀況：

如果您要顯示...	輸入命令...
系統的健全狀況、反映個別健全狀況監視器的整體狀態	**system health status show**
CIFS/NDO子系統健全狀況的相關資訊	**system health subsystem show -subsystem CIFS-NDO -instance**

2. 顯示有關CIFS/n警示監控如何設定的資訊、方法是執行適當的動作：

如果您想要顯示有關...的資訊	輸入命令...
CIFS/NDO子系統的健全狀況監視器組態與狀態、例如受監控的節點、初始化狀態和狀態	**system health config show -subsystem CIFS-NDO**
CIF-NDO會發出健全狀況監視器可能產生的警示	**system health alert definition show -subsystem CIFS-NDO**
CIF-NDO健全狀況監視原則、可決定何時發出警示	**system health policy definition show -monitor node-connect**

使用 `-instance` 顯示詳細資訊的參數。

範例

下列輸出顯示有關叢集和CIFS/n子系統整體健全狀況狀態的資訊：

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

cluster1::> system health subsystem show -instance -subsystem CIFS-NDO

                   Subsystem: CIFS-NDO
                      Health: ok
        Initialization State: initialized
Number of Outstanding Alerts: 0
 Number of Suppressed Alerts: 0
                        Node: node2
  Subsystem Refresh Interval: 5m
```

下列輸出顯示CIFS/n子系統健全狀況監視器的組態與狀態詳細資訊：

```
cluster1::> system health config show -subsystem CIFS-NDO -instance

                           Node: node1
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0

                           Node: node2
                        Monitor: node-connect
                      Subsystem: SAS-connect, HA-health, CIFS-NDO
                         Health: ok
                 Monitor Version: 2.0
             Policy File Version: 1.0
                        Context: node_context
                     Aggregator: system-connect
                       Resource: SasAdapter, SasDisk, SasShelf,
HaNodePair,
                                 HaICMailbox, CifsNdoNode,
CifsNdoNodeVserver
Subsystem Initialization Status: initialized
    Subordinate Policy Versions: 1.0 SAS, 1.0 SAS multiple adapters, 1.0,
1.0
```

驗證持續可用的**SMB**共用組態

為了支援不中斷營運、Hyper-V和SQL Server SMB共用必須設定為持續可用的共用。此外、您還必須檢查其他某些共用設定。您應該確認共用已正確設定、以便在發生計畫性或非計畫性的中斷事件時、為應用程式伺服器提供無縫且不中斷營運的作業。

關於這項工作

您必須確認下列兩個共用參數設定正確：

- 。 `-offline-files` 參數設為任一 `manual` （預設）或 `none`。
- 必須停用symlink。

若要正常執行不中斷營運、必須設定下列共用內容：

- `continuously-available`
- `oplocks`

不得設定下列共用內容：

- `homedirectory`
- `attributecache`
- `branchcache`
- `access-based-enumeration`

步驟

1. 確認離線檔案已設定為 `manual` 或 `disabled` 而且會停用符號連結：

   vserver cifs shares show -vserver *vserver_name*

2. 確認SMB共用區已設定為持續可用度：

   vserver cifs shares properties show -vserver *vserver_name*

範例

下列範例顯示儲存虛擬機器（SVM、先前稱為Vserver）VS1上名稱為「shafre1」的共用區設定。離線檔案設為 `manual` 且會停用符號連結（在中以連字號指定） `Symlink Properties` 欄位輸出）：

```
cluster1::> vserver cifs share show -vserver vs1 -share-name share1
                     Vserver: vs1
                       Share: share1
     CIFS Server NetBIOS Name: VS1
                        Path: /data/share1
             Share Properties: oplocks
                               continuously-available
           Symlink Properties: -
      File Mode Creation Mask: -
 Directory Mode Creation Mask: -
                Share Comment: -
                    Share ACL: Everyone / Full Control
File Attribute Cache Lifetime: -
                  Volume Name: -
                Offline Files: manual
Vscan File-Operations Profile: standard
```

下列範例顯示SVM VS1上名為「shafre1」之共用區的共用內容：

```
cluster1::> vserver cifs share properties show -vserver vs1 -share-name
share1
Vserver    Share   Properties
---------  ------  ----------
vs1        share1  oplocks
                   continuously-available
```

驗證**LIF**狀態

即使您將採用Hyper-V的儲存虛擬機器（SVM）和SQL Server設定為採用SMB組態、以在叢集中的每個節點上擁有生命、在日常作業期間、某些生命體可能會移至另一個節點上的連接埠。您必須驗證LIF狀態、並採取任何必要的修正行動。

關於這項工作

若要提供無縫且不中斷營運的作業支援、叢集中的每個節點必須至少有一個LIF用於SVM、而且所有LIF都必須與主連接埠相關聯。如果部分已設定的生命期目前未與其主連接埠建立關聯、您必須修正任何連接埠問題、然後將生命期還原至其主連接埠。

步驟

1. 顯示SVM的已設定LIF相關資訊：

   network interface show -vserver *vserver_name*

   在此範例中、「lif1」不在主連接埠上。

   ```
   network interface show -vserver vs1
   ```

   ```
               Logical    Status     Network          Current     Current Is
   Vserver     Interface  Admin/Oper Address/Mask     Node        Port
   Home
   ----------- ---------- ---------- ---------------- ----------- -------
   ----
   vs1
               lif1         up/up    10.0.0.128/24    node2       e0d
   false
               lif2         up/up    10.0.0.129/24    node2       e0d
   true
   ```

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

2. 如果部分生命區不在其主連接埠上、請執行下列步驟：

   a. 針對每個LIF、判斷LIF的主連接埠：

      network interface show -vserver *vserver_name* -lif *lif_name* -fields home-node,home-port

network interface show -vserver vs1 -lif lif1 -fields home-node,home-port

```
vserver lif  home-node  home-port
------- ---- ---------- ---------
vs1     lif1 node1      e0d
```

b. 針對每個LIF、判斷LIF的主連接埠是否正常運作：

network port show -node *node_name* -port *port* -fields port,link

`network port show -node node1 -port e0d -fields port,link`

```
node       port link
---------- ---- ----
node1      e0d  up
```

在此範例中、「 lif1 」應移轉回其主連接埠、 `node1:e0d`。

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

3. 如果生命期相關聯的任何主連接埠網路介面未處於 `up`狀態，請解決此問題，使這些介面正常運作。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
4. 如有需要、請將I生命 回復至主連接埠：

network interface revert -vserver *vserver_name* -lif *lif_name*

network interface revert -vserver vs1 -lif lif1

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

5. 確認叢集中的每個節點都有SVM的作用中LIF：

network interface show -vserver *vserver_name*

network interface show -vserver vs1

```
            Logical    Status     Network           Current    Current Is
Vserver     Interface  Admin/Oper Address/Mask      Node       Port
Home
----------- ---------- ---------- ---------------- ---------- -------
----
vs1
            lif1         up/up    10.0.0.128/24    node1      e0d
true
            lif2         up/up    10.0.0.129/24    node2      e0d
true
```

判斷SMB工作階段是否持續可用

顯示SMB工作階段資訊

您可以顯示已建立SMB工作階段的相關資訊、包括SMB連線和工作階段ID、以及使用工作階段之工作站的IP位址。您可以顯示工作階段SMB傳輸協定版本的相關資訊、以及持續可用的保護層級、協助您識別工作階段是否支援不中斷營運。

關於這項工作

您可以在SVM上以摘要形式顯示所有工作階段的資訊。不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊：

- 您可以使用選用的 `-fields` 參數顯示有關所選欄位的輸出。

  您可以輸入 `-fields ?` 決定您可以使用哪些欄位。

- 您可以使用 `-instance` 顯示已建立 SMB 工作階段的詳細資訊的參數。
- 您可以使用 `-fields` 參數或 `-instance` 參數可以單獨使用、也可以搭配其他選用參數使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示SMB工作階段資訊...	輸入下列命令...
以摘要形式顯示SVM上的所有工作階段	**vserver cifs session show -vserver *vserver_name***
在指定的連線ID上	**vserver cifs session show -vserver *vserver_name* -connection-id integer**
從指定的工作站IP位址	**vserver cifs session show -vserver *vserver_name* -address *workstation_IP_address***

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
在指定的LIF IP位址上	**vserver cifs session show -vserver *vserver_name* -lif -address *LIF_IP_address***
在指定的節點上	`*vserver cifs session show -vserver *vserver_name* -node {node_name
local}*`	從指定的Windows使用者
vserver cifs session show -vserver *vserver_name* -windows-user *user_name* 的格式 `user_name` 是 `[domain]\user`。	使用指定的驗證機制
vserver cifs session show -vserver *vserver_name* -auth -mechanism authentication_mechanism 的價值 `-auth -mechanism` 可以是下列其中一項： • `NTLMv1` • `NTLMv2` • `Kerberos` • `Anonymous`	使用指定的傳輸協定版本

如果您要顯示**SMB**工作階段資訊...	輸入下列命令...
vserver cifs session show -vserver *vserver_name* -protocol-version protocol_version 的價值 `-protocol -version` 可以是下列其中一項： • `SMB1` • `SMB2` • `SMB2_1` • `SMB3` • `SMB3_1` 持續可用的保護功能和SMB多通道功能僅適用於SMB 3.0及更新版本的工作階段。若要在所有合格的工作階段中檢視其狀態、您應該指定此參數、並將值設為 `SMB3` 或更新版本。	提供特定等級的持續可用保護

如果您要顯示SMB工作階段資訊...	輸入下列命令...
vserver cifs session show -vserver *vserver_name* -continuously -available *continuously_available_protection_level* 的價值 `-continuously -available` 可以是下列其中一項： • `No` • `Yes` • `Partial` 如果持續可用的狀態為 `Partial`，這表示工作階段至少包含一個開啟的持續可用檔案、但工作階段有一些檔案無法以持續可用的保護開啟。您可以使用 `vserver cifs sessions file show` 命令來判斷已建立工作階段上的哪些檔案未以持續可用的保護開啟。	具有指定的SMB簽署工作階段狀態

範例

下列命令會顯示SVM VS1上從IP位址為10.1.1.1的工作站所建立之工作階段的工作階段資訊：

```
cluster1::> vserver cifs session show -address 10.1.1.1
Node:    node1
Vserver: vs1
Connection Session                                    Open         Idle
ID         ID      Workstation      Windows User    Files        Time
---------- ------- ---------------- ------------- ------- ------------
3151272279,
3151272280,
3151272281  1       10.1.1.1         DOMAIN\joe          2          23s
```

下列命令會顯示SVM VS1具有持續可用保護之工作階段的詳細工作階段資訊。連線是使用網域帳戶建立的。

```
cluster1::> vserver cifs session show -instance -continuously-available
Yes

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
               Connection ID: 3151274158
Incoming Data LIF IP Address: 10.2.1.1
      Workstation IP address: 10.1.1.2
    Authentication Mechanism: Kerberos
                Windows User: DOMAIN\SERVER1$
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 1
                  Open Other: 0
              Connected Time: 10m 43s
                   Idle Time: 1m 19s
           Protocol Version: SMB3
      Continuously Available: Yes
           Is Session Signed: false
       User Authenticated as: domain-user
                 NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

下列命令會顯示SVM VS1上使用SMB 3.0和SMB多通道之工作階段的工作階段資訊。在此範例中、使用者使用LIF IP位址從具有SMB 3.0功能的用戶端連線到此共用區、因此驗證機制預設為NTLMv2。連線必須使用Kerberos驗證、才能以持續可用的保護進行連線。

```
cluster1::> vserver cifs session show -instance -protocol-version SMB3

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
              **Connection IDs: 3151272607,31512726078,3151272609
            Connection Count: 3**
Incoming Data LIF IP Address: 10.2.1.2
      Workstation IP address: 10.1.1.3
    Authentication Mechanism: NTLMv2
                Windows User: DOMAIN\administrator
                   UNIX User: pcuser
                 Open Shares: 1
                  Open Files: 0
                  Open Other: 0
              Connected Time: 6m 22s
                   Idle Time: 5m 42s
           Protocol Version: SMB3
      Continuously Available: No
           Is Session Signed: false
       User Authenticated as: domain-user
                NetBIOS Name: -
       SMB Encryption Status: Unencrypted
```

顯示在 **ONTAP** 中開啟 **SMB** 檔案的相關資訊

您可以顯示開啟SMB檔案的相關資訊、包括SMB連線和工作階段ID、託管磁碟區、共用名稱和共用路徑。您也可以顯示檔案持續可用保護層級的相關資訊、這有助於判斷開啟的檔案是否處於支援不中斷營運的狀態。

關於這項工作

您可以在已建立的SMB工作階段中顯示開啟檔案的相關資訊。當您需要判斷SMB工作階段中特定檔案的SMB工作階段資訊時、所顯示的資訊非常有用。

例如、如果您有 SMB 工作階段、其中某些開啟的檔案會以持續可用的保護開啟、有些則無法以持續可用的保護開啟（的值） `-continuously-available` 欄位輸入 `vserver cifs session show` 命令輸出為 `Partial`）、您可以使用此命令來判斷哪些檔案無法持續使用。

您可以使用、以摘要形式顯示已建立的儲存虛擬機器（ SVM ） SMB 工作階段上所有開啟檔案的資訊 `vserver cifs session file show` 不含任何選用參數的命令。

不過、在許多情況下、傳回的輸出量很大。您可以指定選用參數、自訂輸出中顯示的資訊。如果您只想檢視開啟檔案的一小部分資訊、這項功能就很有幫助。

- 您可以使用選用的 `-fields` 參數、可在您選擇的欄位上顯示輸出。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

- 您可以使用 `-instance` 顯示開啟 SMB 檔案的詳細資訊的參數。

  您可以單獨使用此參數、也可以搭配其他選用參數一起使用。

步驟

1. 執行下列其中一項動作：

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
在SVM上以摘要形式顯示	**vserver cifs session file show -vserver *vserver_name***
在指定的節點上	`*vserver cifs session file show -vserver *vserver_name* -node {node_name
local}*`	在指定的檔案ID上
vserver cifs session file show -vserver *vserver_name* -file-id integer	在指定的SMB連線ID上
vserver cifs session file show -vserver *vserver_name* -connection-id integer	在指定的SMB工作階段ID上
vserver cifs session file show -vserver *vserver_name* -session-id integer	在指定的託管Aggregate上
vserver cifs session file show -vserver *vserver_name* -hosting -aggregate *aggregate_name*	在指定的磁碟區上
vserver cifs session file show -vserver *vserver_name* -hosting-volume *volume_name*	在指定的SMB共用區上
vserver cifs session file show -vserver *vserver_name* -share *share_name*	在指定的SMB路徑上
vserver cifs session file show -vserver *vserver_name* -path *path*	提供指定等級的持續可用保護

如果您要顯示開啟的**SMB**檔案...	輸入下列命令...
**`vserver cifs session file show -vserver *vserver_name* -continuously -available *continuously_available_status***  的價值 `-continuously-available` 可以是下列其中一項：  • `No` • `Yes`  如果持續可用的狀態為 `No`這表示這些開啟的檔案無法不中斷地從接管和恢復恢復。在高可用度關係中、他們也無法從合作夥伴之間的一般Aggregate重新配置中恢復。	指定的重新連線狀態

您可以使用其他選用參數來精簡輸出結果。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

範例

下列範例顯示SVM VS1上開啟檔案的相關資訊：

```
cluster1::> vserver cifs session file show -vserver vs1
Node:        node1
Vserver:     vs1
Connection: 3151274158
Session:     1
File     File       Open Hosting              Continuously
ID       Type       Mode Volume    Share      Available
-------- ---------- ---- --------- ---------- ------------
41       Regular    r    data      data       Yes
Path: \mytest.rtf
```

下列範例顯示SVM VS1上開啟檔案ID為82的SMB檔案的詳細資訊：

```
cluster1::> vserver cifs session file show -vserver vs1 -file-id 82
-instance

                  Node: node1
               Vserver: vs1
               File ID: 82
         Connection ID: 104617
            Session ID: 1
             File Type: Regular
             Open Mode: rw
Aggregate Hosting File: aggr1
   Volume Hosting File: data1
            CIFS Share: data1
  Path from CIFS Share: windows\win8\test\test.txt
            Share Mode: rw
           Range Locks: 1
Continuously Available: Yes
           Reconnected: No
```

SAN 儲存管理

SAN概念

使用iSCSI進行SAN資源配置

在SAN環境中、儲存系統是具有儲存目標裝置的目標系統。對於iSCSI和FC、儲存目標裝置稱為LUN（邏輯單元）。對於光纖通道上的非揮發性記憶體Express（NVMe）、儲存目標裝置稱為命名空間。

您可以建立iSCSI和FC的LUN、或建立NVMe的命名空間、來設定儲存設備。然後、主機使用網際網路小型電腦系統介面（iSCSI）或光纖通道（FC）傳輸協定網路來存取LUN或命名空間。

若要連線至iSCSI網路、主機可以使用標準乙太網路介面卡（NIC）、TCP卸載引擎（TOE）卡搭配軟體啟動器、整合式網路介面卡（CNA）或專用iSCSI主機匯流排介面卡（HBA）。

若要連線至FC網路、主機需要FC HBA或CNA。

支援的FC傳輸協定包括：

- FC
- FCoE
- NVMe

iSCSI目標節點網路連線和名稱

iSCSI目標節點可透過多種方式連線至網路：

- 透過乙太網路介面、使用整合至ONTAP 整個功能的軟體。
- 透過多個系統介面、搭配用於iSCSI的介面、也能傳輸SMB和NFS等其他傳輸協定的流量。
- 使用統一化目標介面卡（UTA）或整合式網路介面卡（CNA）。

每個iSCSI節點都必須有節點名稱。

iSCSI節點名稱的兩種格式（或類型指示符）是_iqn_和_EUI_。SVM iSCSI目標一律使用iqn類型的指定器。啟動器可以使用iqn-type或EUI-type標示器。

儲存系統節點名稱

每個執行iSCSI的SVM都會根據反轉網域名稱和唯一編碼編號、提供預設節點名稱。

節點名稱會以下列格式顯示：

iqn.1992-08.com.netapp:sn.*unique-encoding-number*

以下範例顯示具有唯一編碼編號的儲存系統預設節點名稱：

```
iqn.1992-08.com.netapp:sn.812921059e6c11e097b3123478563412:vs.6
```

iSCSI的TCP連接埠

iSCSI傳輸協定在ONTAP 中設定為使用TCP連接埠編號3260。

不支援變更iSCSI的連接埠號碼。ONTAP連接埠編號3260已登錄為iSCSI規格的一部分、不得用於任何其他應用程式或服務。

相關資訊

"NetApp文件：ONTAP 《SAN主機組態》"

iSCSI服務管理

iSCSI服務管理

您可以使用管理儲存虛擬機器（ SVM ） iSCSI 邏輯介面上 iSCSI 服務的可用性 `vserver iscsi interface enable` 或 `vserver iscsi interface disable` 命令。

依預設、iSCSI服務會在所有iSCSI邏輯介面上啟用。

如何在主機上實作iSCSI

iSCSI可以使用硬體或軟體在主機上實作。

您可以使用下列其中一種方法來實作iSCSI：

- 使用使用主機標準乙太網路介面的啟動器軟體。
- 透過iSCSI主機匯流排介面卡（HBA）：iSCSI HBA在主機作業系統中顯示為具有本機磁碟的SCSI磁碟介面卡。
- 使用可卸載TCP/IP處理的TCP卸載引擎（TOE）介面卡。

  iSCSI傳輸協定處理仍由主機軟體執行。

iSCSI驗證的運作方式

在iSCSI工作階段的初始階段、啟動器會傳送登入要求至儲存系統、以開始iSCSI工作階段。然後儲存系統會允許或拒絕登入要求、或是判斷不需要登入。

iSCSI驗證方法包括：

- 挑戰握手驗證傳輸協定（CHAP）：啟動器使用CHAP使用者名稱和密碼登入。

  您可以指定CHAP密碼或產生一個十六進位密碼。CHAP使用者名稱和密碼有兩種類型：

  - 傳入：儲存系統會驗證啟動器。

如果您使用CHAP驗證、則需要輸入設定。

- Outbound（傳出）：這是一項選用設定、可讓啟動器驗證儲存系統。

  只有在儲存系統上定義傳入使用者名稱和密碼時、才能使用傳出設定。

- Deny（拒絕）-拒絕啟動器存取儲存系統。
- 無-儲存系統不需要對啟動器進行驗證。

您可以定義啟動器清單及其驗證方法。您也可以定義適用於此清單以外之啟動器的預設驗證方法。

相關資訊

"Windows多重路徑選項Data ONTAP 、包含下列功能：Fibre Channel和iSCSI"

iSCSI啟動器安全管理

提供許多功能來管理iSCSI啟動器的安全性。ONTAP您可以定義iSCSI啟動器清單及每個啟動器的驗證方法、在驗證清單中顯示啟動器及其相關的驗證方法、從驗證清單中新增及移除啟動器、以及為清單中未列出的啟動器定義預設iSCSI啟動器驗證方法。

iSCSI端點隔離

現有的 iSCSI 安全命令可以接受 IP 位址範圍或多個 IP 位址。

所有iSCSI啟動器在建立工作階段或與目標連線時、都必須提供起始IP位址。如果來源IP位址不受支援或不明、這項新功能可防止啟動器登入叢集、提供獨特的識別配置。來自不受支援或未知IP位址的任何啟動器、都會在iSCSI工作階段層拒絕其登入、使啟動器無法存取叢集內的任何LUN或磁碟區。

使用兩個新命令來實作這項新功能、以協助管理預先存在的項目。

新增啟動器位址範圍

透過新增 IP 位址範圍或多個 IP 位址來改善 iSCSI 啟動器的安全管理 `vserver iscsi security add-initiator-address-range` 命令。

```
cluster1::> vserver iscsi security add-initiator-address-range
```

移除啟動器位址範圍

使用移除 IP 位址範圍或多個 IP 位址 `vserver iscsi security remove-initiator-address-range` 命令。

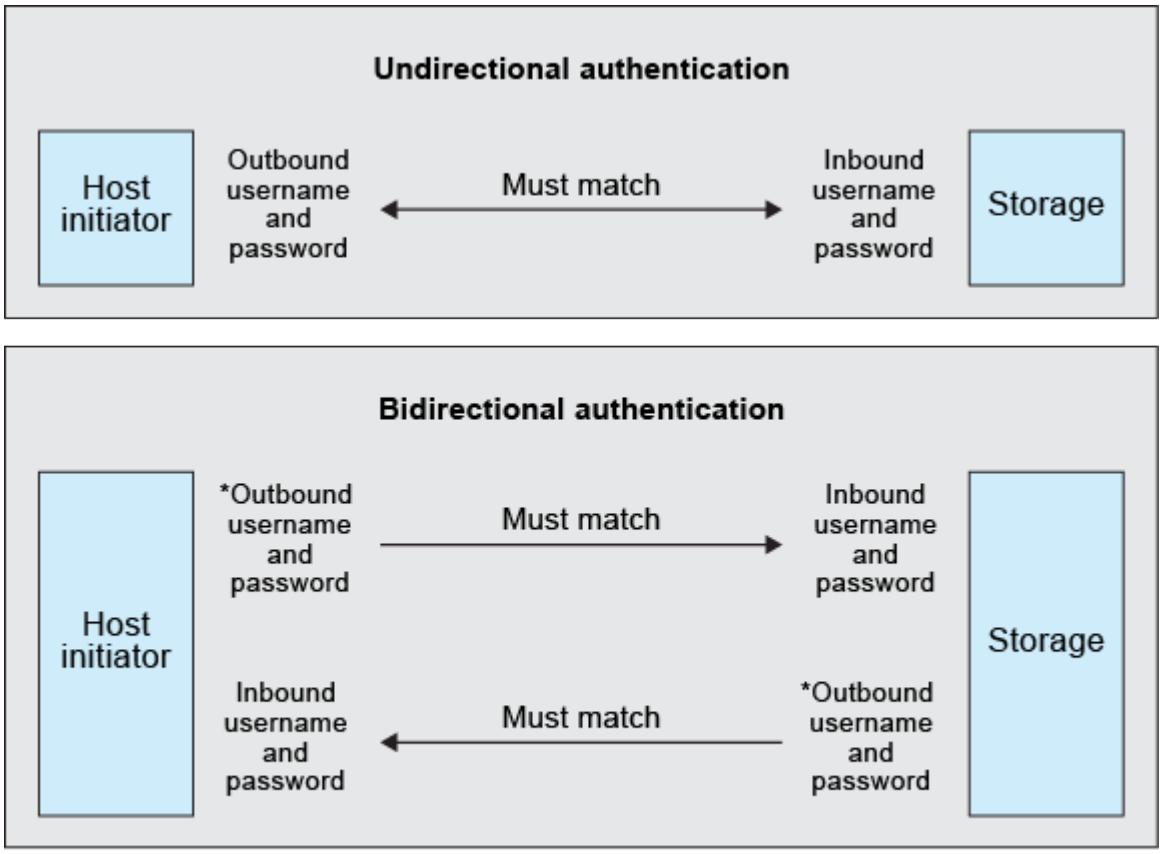
```
cluster1::> vserver iscsi security remove-initiator-address-range
```

了解**ONTAP**中 **iSCSI** 啟動器的 **CHAP** 驗證

Challenge Handshake驗證傳輸協定（CHAP）可在iSCSI啟動器與目標之間進行驗證通訊。使用CHAP驗證時、您可以在啟動器和儲存系統上定義CHAP使用者名稱和密碼。

在iSCSI工作階段的初始階段、啟動器會傳送登入要求至儲存系統以開始工作階段。登入要求包括啟動器

的CHAP使用者名稱和CHAP演算法。儲存系統會回應CHAP挑戰。啟動器會提供CHAP回應。儲存系統會驗證回應並驗證啟動器。CHAP密碼用於計算回應。



驗證	傳出	傳入	匹配？
單向	主機啟動器使用者名稱和密碼	儲存使用者名稱和密碼	必須匹配
雙向	主機啟動器使用者名稱和密碼	儲存使用者名稱和密碼	必須匹配
雙向	儲存使用者名稱和密碼	主機啟動器使用者名稱和密碼	必須匹配

主機啟動器的出站使用者名稱和密碼必須與儲存系統的出站使用者名稱和密碼不同。

使用**CHAP**驗證的準則

使用 CHAP 驗證時請遵循以下準則。

- 如果您在儲存系統上定義傳入使用者名稱和密碼、則必須在啟動器上使用相同的使用者名稱和密碼進行傳出CHAP設定。如果您也在儲存系統上定義傳出使用者名稱和密碼以啟用雙向驗證、則必須在啟動器上使用相同的使用者名稱和密碼來進行傳入CHAP設定。
- 儲存系統上的傳入和傳出設定不能使用相同的使用者名稱和密碼。
- CHAP使用者名稱可以是1到128位元組。

  系統不允許使用者名為空。

- CHAP密碼（機密）可為1至512位元組。

  密碼可以是十六進制值或字串。對於十六進位值，您應該輸入帶有“0x”或“0X”前綴的值。

  系統不允許使用空密碼。

> 支援使用特殊字元、非英文字母、數字和空格來輸入CHAP密碼（機密）ONTAP 。 不過、這會受到主機限制。 如果您的特定主機不允許使用其中任何一項、就無法使用。
>
> 例如、如果未使用IPsec加密、Microsoft iSCSI軟體啟動器會要求啟動器和目標CHAP密碼至少為12個位元組。無論是否使用IPsec、密碼長度上限為16位元組。
>
> 有關其他限制，請參閱啟動器的文件。

如何使用**iSCSI**介面存取清單來限制啟動器介面、可提高效能與安全性

iSCSI介面存取清單可用來限制啟動器可存取的SVM中的生命量、進而提升效能與安全性。

當啟動器開始使用 iSCSI 的探索工作階段時 `SendTargets` 命令會接收與存取清單中的 LIF （網路介面）相關聯的 IP 位址。根據預設、所有啟動器都能存取SVM中的所有iSCSI LIF。您可以使用存取清單來限制啟動器可存取的SVM中的lifs數目。

ONTAP 中的網際網路儲存名稱服務（ **iSNS** ）

網際網路儲存名稱服務（iSNS）是一種傳輸協定、可在TCP/IP儲存網路上自動探索及管理iSCSI裝置。iSNS伺服器會維護網路上作用中iSCSI裝置的相關資訊、包括其IP位址、iSCSI節點名稱IQN及入口網站群組。

您可以從協力廠商取得iSNS伺服器。如果您的網路上有已設定且已啟用可供啟動器和目標使用的ISS-伺服器、您可以使用儲存虛擬機器（SVM）的管理LIF、在ISSVM伺服器上登錄該SVM的所有iSCSI LIF。登錄完成後、iSCSI啟動器可查詢iSNS伺服器、以探索該特定SVM的所有生命期。

如果您決定使用iSNS服務、則必須確保儲存虛擬機器（SVM）已正確登錄至網際網路儲存名稱服務（iSNS）伺服器。

如果網路上沒有iSNS伺服器、則必須手動設定每個目標、使主機可見。

什麼是**iSNS**伺服器

iSNS伺服器使用網際網路儲存名稱服務（SNSs）傳輸協定來維護網路上作用中iSCSI裝置的相關資訊、包括其IP位址、iSCSI節點名稱（IQN）和入口網站群組。

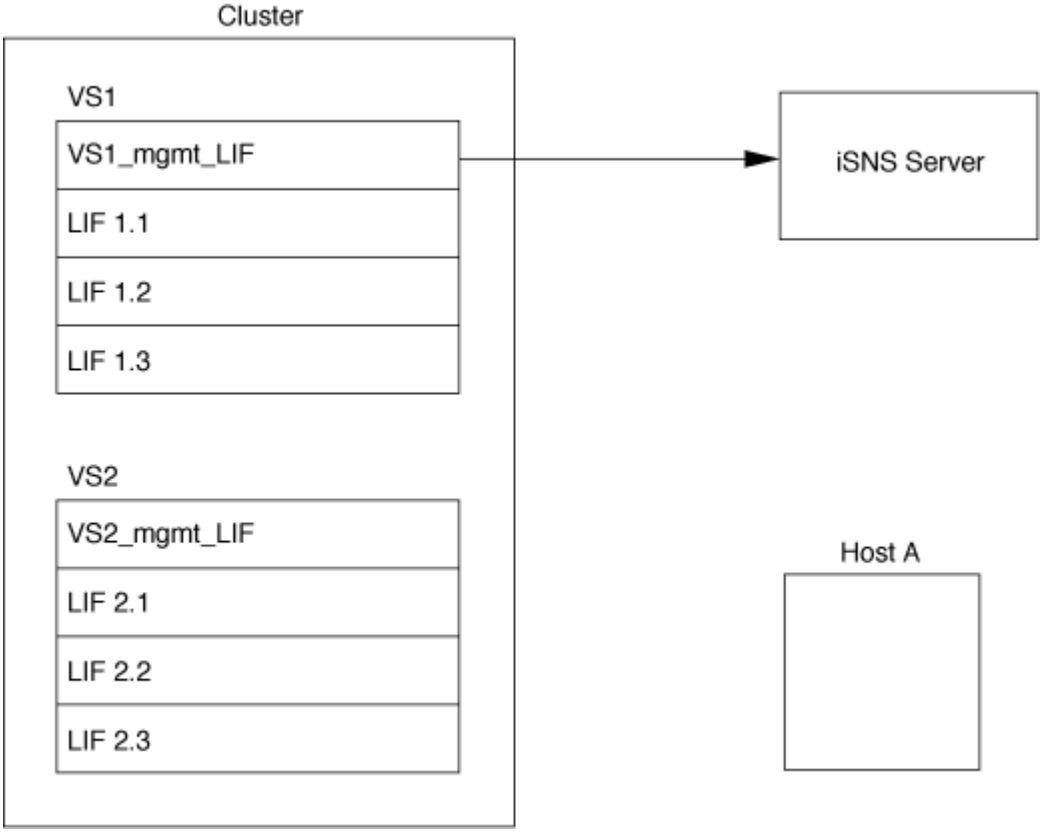
透過iSNS傳輸協定、可自動探索及管理IP儲存網路上的iSCSI裝置。iSCSI啟動器可查詢iSNS伺服器以探索iSCSI目標裝置。

NetApp不供應或經銷iSNS伺服器。您可以向NetApp支援的廠商取得這些伺服器。

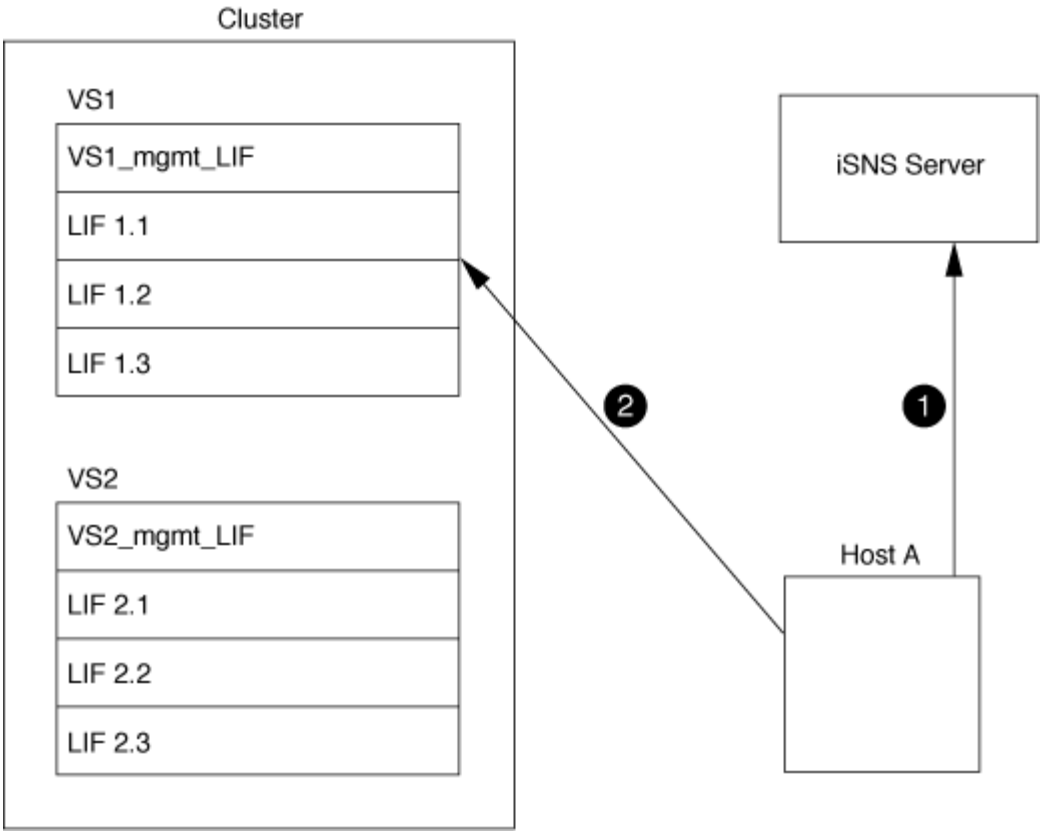
SVM如何與**iSNS**伺服器互動

透過SVM管理LIF、iSNS伺服器可與每個儲存虛擬機器（SVM）進行通訊。管理LIF會將所有iSCSI目標節點名稱、別名及入口網站資訊登錄至特定SVM的iSNS服務。

在以下範例中、 SVM 「 'VS1' 」使用 SVM 管理 LIF 「 'VS1_mgmt_lif' 」向 iSNS 伺服器註冊。在登錄到iSNS期間、SVM會透過SVM管理LIF將所有iSCSI LIF傳送到iSNS伺服器。一旦完成 iSNS 登錄、則 iSNS 伺服器會在「 VS1 」中列出所有服務 iSCSI 的生命體清單。如果叢集包含多個SVM、則每個SVM都必須分別向iSNS伺服器註冊、才能使用iSNS服務。



在下一個範例中、當 iSNS 伺服器完成目標的登錄後、主機 A 可以透過 iSNS 伺服器探索「 VS1 」的所有生命、如步驟 1 所示。在主機 A 完成「 VS1 」的生命探索後、主機 A 可以建立與「 VS1 」中任何生命的連線、如步驟 2 所示。在管理層將 "`VS2` 的 "`VS2_mgmt_LIF" 註冊到 iSNS 伺服器之前、主機 A 並未偵測到 "'VS2'" 中的任何生命。



不過、如果您定義介面存取清單、主機只能使用介面存取清單中定義的lifs來存取目標。

初始設定完iSNS之後ONTAP 、當SVM組態設定變更時、Sesfe會自動更新iSNS伺服器。

在您進行組態變更和 ONTAP 將更新傳送至 iSNS 伺服器之間、可能會發生幾分鐘的延遲。強制立即更新 iSNS 伺服器上的 iSNS 資訊： `vserver iscsi isns update`。如"指令參考資料ONTAP"需詳細 `vserver iscsi isns update`資訊，請參閱。

管理**iSNS**的命令

支援支援支援管理您的iSNS服務的命令。ONTAP

如果您想要...	使用此命令...
設定iSNS服務	`vserver iscsi isns create`
啟動iSNS服務	`vserver iscsi isns start`
修改iSNS服務	`vserver iscsi isns modify`
顯示iSNS服務組態	`vserver iscsi isns show`
強制更新已登錄的iSNS資訊	`vserver iscsi isns update`
停止iSNS服務	`vserver iscsi isns stop`

移除iSNS服務	`vserver iscsi isns delete`
查看命令的手冊頁	`man command name`

如"指令參考資料ONTAP"需詳細 `vserver iscsi isns`資訊，請參閱。

使用FC進行SAN資源配置

您應該瞭解ONTAP 瞭解如何實作FC SAN所需的重要概念。

FC目標節點如何連線至網路

儲存系統和主機都有介面卡、以便使用纜線連接至FC交換器。

當節點連線至FC SAN時、每個SVM會向交換器光纖名稱服務註冊其LIF的全球連接埠名稱（WWPN）。SVM的WWNN和每個LIF的WWPN會自動由ONTAP SSI.指派。

> 不支援從具有FC的主機直接連線至節點、需要使用NPIV、這需要使用交換器。在iSCSI工作階段中、通訊可用於網路路由或直接連線的連線。不過ONTAP 、這兩種方法都支援使用支援。

如何識別FC節點

使用FC設定的每個SVM都會以全球節點名稱（WWNN）來識別。

如何使用WWPN

WWPN可識別SVM中設定為支援FC的每個LIF。這些生命體使用叢集中每個節點的實體 FC 連接埠，這些連接埠可以是 FC 目標卡， UTA 或 UTA2 ，在節點中設定為 FC 或 FCoE 。

- 建立啟動器群組

  主機HBA的WWPN用於建立啟動器群組（igroup）。igroup用於控制主機對特定LUN的存取。您可以指定FC網路中啟動器的WWPN集合、以建立igroup。當您將儲存系統上的LUN對應至igroup時、可以將該群組中的所有啟動器授予該LUN的存取權。如果主機的WWPN不在對應至LUN的igroup中、則該主機無法存取LUN。這表示LUN不會在該主機上顯示為磁碟。

  您也可以建立連接埠集、使LUN僅在特定目標連接埠上可見。連接埠集由一組FC目標連接埠組成。您可以將igroup繫結至連接埠集。igroup中的任何主機只能透過連接埠集內的目標連接埠來存取LUN。

- 獨特識別FC生命里數

  WWPN可唯一識別每個FC邏輯介面。主機作業系統使用WWNN和WWPN的組合來識別SVM和FC LIF。有些作業系統需要持續連結、以確保LUN在主機上顯示為相同的目標ID。

全球名稱指派的運作方式

全球名稱會依ONTAP 序建立於此。不過ONTAP 、由於選擇此類產品的方式、因此可能會以非循序的順序指派。

每個介面卡都有預先設定的WWPN和WWNN、但ONTAP 不使用這些預先設定的值。而是ONTAP 根據內建乙太網路連接埠的MAC位址、指派自己的WWPN或WWNN。

指派全球名稱時、可能會因為下列原因而顯示為非連續名稱：

- 在叢集中的所有節點和儲存虛擬機器（SVM）之間指派全球名稱。
- 已釋出的全球名稱將會回收並新增回可用名稱集區。

如何識別**FC**交換器

Fibre Channel交換器的裝置本身具有一個全球節點名稱（WWNN）、其每個連接埠都有一個全球連接埠名稱（WWPN）。

例如、下圖顯示如何將WWPN指派給16埠Brocade交換器上的每個連接埠。如需特定交換器的連接埠編號方式詳細資訊、請參閱該交換器廠商提供的文件。

連接埠 * 0* 、 WWPN 20 ： **00** ： 00 ： 60 ： 69 ： 51 ： 06 ： b4

連接埠 * 1 * 、 WWPN 20 ： **01** ： 00 ： 60 ： 69 ： 51 ： 06 ： b4

連接埠* 14*、WWPN 20：* 0e**：00：60：69：51：06：b4

連接埠* 15*、WWPN 20：* 0f*：00：60：69：51：06：b4

採用**NVMe**的**SAN**資源配置

從ONTAP 支援的支援功能支援使用支援的功能為SAN環境、從支援的功能為支援的功能為2個9.4。NVMe / FC可讓儲存管理員配置命名空間和子系統、然後將命名空間對應至子系統、類似於LUN的資源配置方式、以及LUN對應至FC和iSCSI的igroup。

NVMe命名空間是一組可格式化為邏輯區塊的非揮發性記憶體。命名空間相當於FC和iSCSI傳輸協定的LUN、而NVMe子系統類似於igroup。NVMe子系統可與啟動器建立關聯、以便相關的啟動器存取子系統內的命名空間。

ⓘ 雖然功能類似、但NVMe命名空間不支援LUN支援的所有功能。

從支援NVMe的主機型資料存取、需要取得從功能支援到功能的許可證。ONTAP如果ONTAP NVMe是在更新至ONTAP 版本號9.5之後啟用、系統會給予90天的寬限期以取得授權。如果您有"ONTAP One"、則會隨附NVMe 授權。您可以使用下列命令來啟用授權：

```
system license add -license-code NVMe_license_key
```

相關資訊

"NetApp技術報告4684：實作及設定採用NVMe / FC的現代化SAN"

SAN 磁碟區

關於SAN Volume總覽

提供三種基本的Volume資源配置選項：完整資源配置、精簡資源配置和半密集資源配置。ONTAP每個選項都會使用不同的方法來管理Volume空間、以及ONTAP 有關資訊區塊共享技術的空間需求。瞭解這些選項的運作方式、讓您可以選擇最適合您環境的選項。

> 不建議將SAN LUN和NAS共用放在相同FlexVol 的支援區內。您應該特別為FlexVol SAN LUN配置個別的功能區、並應將個別FlexVol 的功能區專門配置給NAS共享區。這可簡化管理與複寫部署、並與FlexVol 支援的功能相似Active IQ Unified Manager （前身OnCommand 為《統一化管理程式》）。

資源隨需配置

建立精簡配置的磁碟區時ONTAP 、建立磁碟區時、不需要保留任何額外空間。當資料寫入磁碟區時、磁碟區會從Aggregate要求所需的儲存設備、以配合寫入作業。使用精簡配置的磁碟區可讓您過度使用Aggregate、這可能會導致磁碟區無法在Aggregate用盡可用空間時、保護所需的空間。

您可以透過設定精簡配置的 FlexVol Volume 來建立它 `-space-guarantee` 選項 `none`。

為磁碟區進行完整資源配置

建立完整資源配置的Volume時ONTAP 、功能組會從集合區中保留足夠的儲存空間、以確保磁碟區中的任何區塊都能隨時寫入。當您將磁碟區設定為使用完整資源配置時、您可以運用ONTAP 任何一套功能（例如壓縮和重複資料刪除）來抵銷較大的前置儲存需求。

您可以透過設定完整佈建的 FlexVol Volume 來建立它 `-space-slo` （服務層級目標）選項 `thick`。

磁碟區的半厚資源配置

建立使用半厚資源配置的磁碟區時ONTAP 、由集合區中的儲存空間來考慮磁碟區大小。如果磁碟區因為區塊共用技術使用區塊而耗盡可用空間， ONTAP 會盡力刪除保護資料物件（快照， FlexClone 檔案和 LUN ），以釋放它們所擁有的空間。只要ONTAP 用足夠快的速度刪除保護資料物件、以跟上覆寫所需的空間、寫入作業就會繼續成功。這稱為「盡力」寫入保證。

*注意：*使用半厚資源配置的磁碟區不支援下列功能：

- 儲存效率技術，例如重複資料刪除，壓縮和壓縮
- Microsoft卸載資料傳輸（ODX）

您可以透過設定半完整佈建的 FlexVol Volume 來建立它 `-space-slo` （服務層級目標）選項 `semi-thick`。

與空間保留檔案和LUN搭配使用

空間保留檔案或LUN是在建立儲存設備時配置的檔案或LUN。過去、NetApp使用「精簡配置LUN」一詞來表示停用空間保留的LUN（非空間保留LUN）。

*附註：*非空間保留的檔案一般不會稱為「精簡配置檔案」。

下表摘要說明三種Volume資源配置選項如何搭配空間保留檔案和LUN使用的主要差異：

Volume資源配置	**LUN /**檔案空間保留	覆寫	保護資料	儲存效率[3]
厚	支援	保證為1^	保證	支援
精簡	無效果	無	保證	支援
半厚	支援	盡力量：1^	盡最大努力	不支援

附註

1. 若要保證覆寫或提供盡力覆寫保證、必須在LUN或檔案上啟用空間保留。
2. 保護資料包括快照，標記為自動刪除的 FlexClone 檔案和 LUN （備份複本）。
3. 儲存效率包括重複資料刪除、壓縮、任何未標示為自動刪除（作用中複本）的FlexClone檔案和LUN、以及FlexClone子檔案（用於複本卸載）。

支援**SCSI**精簡配置**LUN**

支援T10 SCSI精簡配置LUN、以及NetApp精簡配置LUN。ONTAPT10 SCSI精簡配置可讓主機應用程式支援SCSI功能、包括用於區塊環境的LUN空間回收和LUN空間監控功能。您的SCSI主機軟體必須支援T10 SCSI精簡配置。

您使用的是 ONTAP `space-allocation` 設定以啟用 / 停用 LUN 上 T10 精簡配置的支援。您使用的是 ONTAP `space-allocation enable` 在 LUN 上啟用 T10 SCSI 精簡配置的設定。

這 `[-space-allocation {enabled|disabled}]`命令"指令參考資料ONTAP"有更多資訊來啟用/停用對 T10 精簡配置的支援以及如何在 LUN 上啟用 T10 SCSI 精簡配置。

設定**Volume**資源配置選項

您可以設定磁碟區以進行精簡配置、完整配置或半密集配置。

關於這項工作

設定 `-space-slo` 選項 `thick` 確保下列事項：

- 整個磁碟區會預先配置在Aggregate中。您無法使用 `volume create` 或 `volume modify` 用於設定 Volume 的命令 `-space-guarantee` 選項。
- 保留覆寫所需的空間100%。您無法使用 `volume modify` 用於設定 Volume 的命令 `-fractional -reserve` 選項

設定 `-space-slo` 選項 `semi-thick` 確保下列事項：

- 整個磁碟區會預先配置在Aggregate中。您無法使用 `volume create` 或 `volume modify` 用於設定 Volume 的命令 `-space-guarantee` 選項。
- 不會保留空間進行覆寫。您可以使用 `volume modify` 用於設定 Volume 的命令 `-fractional-reserve` 選項。

- 自動刪除快照已啟用。

步驟

1. 設定Volume資源配置選項：

   ```
   volume create -vserver vserver_name -volume volume_name -aggregate
   aggregate_name -space-slo none|thick|semi-thick -space-guarantee none|volume
   ```

   。 `-space-guarantee` 選項預設為 `none` 適用於 AFF 系統和非 AFF DP 磁碟區。否則、預設為 `volume`。對於現有的 FlexVol 磁碟區、請使用 `volume modify` 用於設定資源配置選項的命令。

   下列命令可在SVM VS1上設定vol1以進行精簡配置：

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-guarantee
   none
   ```

   下列命令可在SVM VS1上設定vol1以進行完整資源配置：

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo thick
   ```

   下列命令可在SVM VS1上設定vol1以進行半厚資源配置：

   ```
   cluster1::> volume create –vserver vs1 -volume vol1 -space-slo semi-
   thick
   ```

SAN Volume組態選項

您必須在包含LUN的磁碟區上設定各種選項。設定Volume選項的方式、決定了Volume中LUN可用的空間量。

自動擴充

您可以啟用或停用自動擴充。如果啟用、則AutoGROW可ONTAP 自動將磁碟區大小增加至您預先決定的最大大小。包含的Aggregate中必須有可用空間、才能支援Volume的自動成長。因此、如果您啟用自動擴充、則必須監控內含Aggregate中的可用空間、並視需要新增更多空間。

無法觸發自動擴充以支援建立快照。如果您嘗試建立快照，但磁碟區空間不足，即使啟用自動擴充功能，快照建立也會失敗。

如果停用自動擴充、磁碟區的大小將維持不變。

自動縮小

您可以啟用或停用自動縮小。如果您啟用、當ONTAP 磁碟區的空間用量減少預先決定的臨界值時、自動縮小功能可讓流通量自動減少磁碟區的整體大小。如此可觸發磁碟區、自動釋放未使用的可用空間、進而提高儲存效率。

Snapshot自動刪除

發生下列其中一種情況時， Snapshot 自動刪除會自動刪除快照：

- 磁碟區幾乎已滿。
- 快照保留空間即將滿。
- 覆寫保留空間已滿。

您可以設定快照自動刪除，將快照從最舊到最新，或從最新到最舊刪除。Snapshot 自動刪除不會刪除與複製磁碟區或 LUN 中快照連結的快照。

如果您的磁碟區需要額外空間，而且您已啟用自動擴充和快照自動刪除功能，則根據預設， ONTAP 會先觸發自動擴充來嘗試取得所需空間。如果沒有透過自動擴充取得足夠的空間，則會觸發快照自動刪除。

Snapshot保留

Snapshot Reserve 定義磁碟區中保留給快照的空間量。分配給快照保留的空間不可用於任何其他用途。如果已使用分配給快照保留的所有空間，則快照會開始佔用磁碟區上的額外空間。

在**SAN**環境中移動磁碟區的需求

在移動包含LUN或命名空間的磁碟區之前、您必須符合特定需求。

- 對於包含一個或多個LUN的磁碟區、每個LUN（l生命 體）至少應有兩個路徑連線至叢集中的每個節點。

  如此可消除單點故障、並讓系統在元件故障時仍能繼續運作。

- 對於包含命名空間的磁碟區、叢集必須執行ONTAP 的是32個以上版本的版本。

  執行ONTAP Sfor Sfor 9.5的NVMe組態不支援Volume Move。

設定部分保留的考量事項

部分保留（也稱為_LUN覆寫保留區_）可讓您關閉FlexVol 針對空間保留LUN和位於一個實體磁碟區中檔案的覆寫保留。這有助於將儲存使用率最大化、但如果您的環境因為空間不足而導致寫入作業失敗、則必須瞭解此組態所帶來的需求。

百分比保留設定是以百分比表示、唯一有效的值是 `0` 和 `100` 百分比。「部分保留」設定是Volume的屬性。

將部分保留設為 `0` 提高儲存使用率。然而、如果磁碟區的可用空間不足、存取位於磁碟區中資料的應用程式可能會發生資料中斷、即使將磁碟區保證設定為 `volume`。不過、只要有適當的Volume組態和使用、就能將寫入失敗的機率降至最低。ONTAP 為將部分保留設為的磁碟區提供「盡力」寫入保證 `0` 當滿足下列所有要求時：

- 重複資料刪除功能未在使用中
- 壓縮未在使用中
- FlexClone子檔案未在使用中
- 所有FlexClone檔案和FlexClone LUN均已啟用自動刪除功能

  這不是預設設定。您必須明確啟用自動刪除功能、無論是在建立時或是在建立FlexClone檔案或FlexClone

LUN之後加以修改。

- 不使用ODX和FlexClone複本卸載
- Volume 擔保設為 `volume`
- 檔案或 LUN 空間保留為 `enabled`
- Volume Snapshot 保留已設定為 `0`
- Volume Snapshot 自動刪除的 `enabled`**承諾層級為** `destroy`，的銷毀清單，`lun_clone,vol_clone,cifs_share,file_clone,sfsr`**以及觸發程序** `volume`

  此設定也可確保在必要時刪除FlexClone檔案和FlexClone LUN。

請注意，如果您的變更率很高，在極少數情況下，快照自動刪除可能會落後，導致磁碟區空間不足，即使使用上述所有必要的組態設定亦然。

此外，您也可以選擇使用 Volume 自動擴充功能來降低自動刪除磁碟區快照的可能性。如果啟用自動擴充功能、則必須監控相關聯Aggregate中的可用空間。如果 Aggregate 已滿，而磁碟區無法成長，則可能會在磁碟區的可用空間耗盡時刪除更多快照。

如果您無法滿足上述所有組態需求、而且需要確保磁碟區不會用盡空間、則必須將磁碟區的「部分保留」設定設為 `100`。這需要更多的可用空間、但保證資料修改作業即使在使用上述技術時仍能順利完成。

「部分保留」設定的預設值和允許值取決於Volume的保證：

Volume保證	預設的部分保留	允許的值
Volume	100	0 、 100
無	0%	0 、 100

SAN 主機端空間管理

在精簡配置的環境中，主機端空間管理可完成從主機檔案系統中釋放的儲存系統管理空間的程序。

主機檔案系統包含中繼資料、可追蹤哪些區塊可用於儲存新資料、哪些區塊包含不可覆寫的有效資料。此中繼資料儲存在 LUN 或命名空間內。在主機檔案系統中刪除檔案時、檔案系統中繼資料會更新、以將該檔案的區塊標示為可用空間。接著會重新計算檔案系統可用空間總計、以納入新釋出的區塊。對儲存系統而言、這些中繼資料更新與主機執行的任何其他寫入內容沒有任何不同。因此、儲存系統並未察覺有任何刪除作業。

這會在主機報告的可用空間量與基礎儲存系統報告的可用空間量之間產生差異。例如、假設您的儲存系統已將新配置的200-GB LUN指派給您的主機。主機和儲存系統都會報告200 GB的可用空間。然後、您的主機會寫入100 GB的資料。此時、主機和儲存系統都會報告100 GB的已用空間和100 GB的未使用空間。

然後從主機刪除50 GB的資料。此時、您的主機會回報50 GB的已用空間和150 GB的未使用空間。不過、您的儲存系統會回報100 GB的已用空間和100 GB的未使用空間。

主機端空間管理使用各種方法來協調主機與儲存系統之間的空間差異。

利用支援功能簡化主機管理SnapCenter

您可以使用SnapCenter 支援功能的支援軟體來簡化與iSCSI和FC儲存設備相關的部分管理和資料保護工作。適用於Windows和UNIX主機的選用管理套件。SnapCenter

您可以使用 SnapCenter 軟體，從儲存資源池輕鬆建立虛擬磁碟，這些資源池可分散於多個儲存系統，並可自動化儲存資源配置工作，並簡化從快照建立快照和複本的程序，使其與主機資料一致。

如需詳細資訊、請參閱NetApp產品文件 "SnapCenter"。

相關連結

"啟用 SAN 通訊協定的 ONTAP 空間分配"

關於igroup

啟動器群組（igroup）是FC傳輸協定主機WWPN或iSCSI主機節點名稱的表格。您可以定義igroup並將其對應至LUN、以控制哪些啟動器可以存取LUN。

一般而言、您希望主機的所有啟動器連接埠或軟體啟動器都能存取LUN。如果您使用多重路徑軟體或擁有叢集式主機、則每個叢集主機的每個啟動器連接埠或軟體啟動器都需要通往相同LUN的備援路徑。

您可以建立igroup來指定在建立LUN之前或之後、哪些啟動器可以存取LUN、但必須先建立igroup、才能將LUN對應至igroup。

啟動器群組可以有多個啟動器、而且多個igroup可以有相同的啟動器。不過、您無法將LUN對應到具有相同啟動器的多個igroup。啟動器不能是不同ostypes的igroup成員。

igroup如何提供LUN存取的範例

您可以建立多個igroup來定義主機可用的LUN。例如、如果您有主機叢集、可以使用igroup來確保叢集中的一部主機或叢集中的所有主機都能看到特定的LUN。

下表說明四個igroup如何存取四個不同主機存取儲存系統的LUN。叢集式主機（主機3和主機4）均為相同igroup（群組3）的成員、可存取對應至此igroup的LUN。名為Group4的igroup包含Host4的WWPN、用於儲存合作夥伴無法看到的本機資訊。

具有HBA WWPN、IQN或EUI的主機	igroup	WWPN、IQN、EUI新增至igroup	對應至igroup的LUN
主機1、單一路徑（iSCSI軟體啟動器） iqn.1991-05.com.microsoft:host1	群組1	iqn.1991-05.com.microsoft:host1	`/vol/vol2/lun1`

具有**HBA WWPN**、**IQN**或**EUI**的主機	**igroup**	**WWPN**、**IQN**、**EUI**新增至**igroup**	對應至**igroup**的**LUN**
主機2、多重路徑（兩個HBA） 10：00：00：00：C9：2b：6b：3c 10：00：00：00：C9：2b：02：3c	群組2	10：00：00：00：C9：2b：6b：3c 10：00：00：00：C9：2b：02：3c	`/vol/vol2/lun2`
主機3、多重路徑、與主機4叢集 10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 32 ： 1b 10：00：00：00：C9：2b：41：02	群組3	10 ： 00 ： 00 ： 00 ： c9 ： 2b ： 32 ： 1b 10：00：00：00：C9：2b：41：02 10：00：00：00：C9：2b:51：2c 10：00：00：00：C9：2b：47：A2	`/vol/vol2/qtree1/lun3`
主機4、多重路徑、叢集式（主機3看不到） 10：00：00：00：C9：2b:51：2c 10：00：00：00：C9：2b：47：A2	群組4.	10：00：00：00：C9：2b:51：2c 10：00：00：00：C9：2b：47：A2	`/vol/vol2/qtree2/lun4` `/vol/vol2/qtree1/lun5`

指定**igroup**的啟動器**WWPN**和**iSCSI**節點名稱

您可以在建立igroup時指定啟動器的iSCSI節點名稱和WWPN、也可以稍後新增。如果您選擇在建立LUN時指定啟動器iSCSI節點名稱和WWPN、則可視需要於稍後移除。

請依照主機公用程式文件中的指示取得WWPN、並尋找與特定主機相關的iSCSI節點名稱。對於執行ESX軟體的主機、請使用虛擬儲存主控台。

使用虛擬化**SAN**環境的優點

使用儲存虛擬機器（SVM）和LIF來建立虛擬化環境、可讓您將SAN環境擴充至叢集中的所有節點。

- 分散式管理

  您可以登入SVM中的任何節點、以管理叢集中的所有節點。

- 增加資料存取

  有了MPIO和ALUA、您就能透過SVM的任何作用中iSCSI或FC LIF存取資料。

- 受控制的LUN存取

  如果您使用的是SLM/連接埠集、則可以限制啟動器可用來存取LUN的生命期。

改善**VMware VAAI**的**ESX**主機效能

當ESX主機執行ESX 4.1或更新版本時、支援特定的VMware vStorage API for Array Integration（VAAI）功能。ONTAP這些功能有助於將作業從ESX主機卸載到儲存系統、並提高網路處理量。ESX主機會在正確的環境中自動啟用這些功能。

VAAI功能支援下列SCSI命令：

- `EXTENDED_COPY`

  此功能可讓主機在LUN或LUN之間開始傳輸資料、而無需讓主機參與資料傳輸。如此可節省ESX CPU週期並提高網路處理量。延伸複本功能也稱為「複本卸載」、適用於複製虛擬機器等情況。當ESX主機叫用時、複本卸載功能會複製儲存系統內的資料、而非透過主機網路。複本卸載會以下列方式傳輸資料：

  - 在LUN內
  - 在磁碟區內的LUN之間
  - 儲存虛擬機器（SVM）內不同磁碟區上的LUN之間
  - 在叢集內不同 SVM 上的 LUN 之間
    如果無法叫用此功能、 ESX 主機會自動使用標準讀寫命令來執行複製作業。

- `WRITE_SAME`

  此功能可卸載將重複模式（如全部零）寫入儲存陣列的工作。ESX主機在零填檔案等作業中使用此功能。

- `COMPARE_AND_WRITE`

  這項功能會略過某些檔案存取並行限制、以加速啟動虛擬機器等作業。

使用**VAAI**環境的需求

VAAI功能是ESX作業系統的一部分、當您設定正確的環境時、ESX主機會自動啟動該功能。

環境需求如下：

- ESX主機必須執行ESX 4.1或更新版本。
- 託管VMware資料存放區的NetApp儲存系統必須執行ONTAP VMware。
- （僅限複本卸載）VMware複本作業的來源和目的地必須裝載在同一個叢集內的相同儲存系統上。

> ⓘ 複本卸載功能目前不支援在不同儲存系統上裝載的VMware資料存放區之間複製資料。

判斷**ESX**是否支援**VAAI**功能

若要確認ESX作業系統是否支援VAAI功能、您可以檢查vSphere Client或使用任何其他方法來存取主機。根據預設、支援SCSI命令。ONTAP

您可以檢查ESX主機的進階設定、以判斷是否已啟用VAAI功能。下表指出哪些SCSI命令與ESX控制名稱相對應。

SCSI 命令	**ESX**控制名稱（**VAAI**功能）
extended複製	`HardwareAcceleratedMove`
寫入相同	`HardwareAcceleratedInit`
比較與寫入	`HardwareAcceleratedLocking`

SAN 複製卸載

Microsoft卸載資料傳輸（**ODX**）

Microsoft卸載資料傳輸（ODX）也稱為_copy offload_、可在儲存裝置內或相容儲存裝置之間直接傳輸資料、而無需透過主機電腦傳輸資料。

VMware與Microsoft支援複本卸載作業、以提升效能與網路處理量。您必須設定系統以符合VMware和Windows作業系統環境的需求、才能使用各自的複本卸載功能。

在虛擬化環境中使用 VMware 和 Microsoft 複製卸載時，您的 LUN 必須對齊。未對齊的 LUN 會降低效能。"了解更多關於未對齊 LUN 的信息"。

支援適用於SMB與SAN傳輸協定的ODX。ONTAP

在非ODX檔案傳輸中、資料會從來源讀取、並透過網路傳輸至主機。主機會透過網路將資料傳輸回目的地。在ODX檔案傳輸中、資料會直接從來源複製到目的地、而不會通過主機。

由於 ODX 卸載複本是直接在來源與目的地之間執行、因此如果在同一個磁碟區內執行複本、就能獲得顯著的效能效益、包括相同磁碟區複本的複本時間更快、用戶端 CPU 與記憶體的使用率降低、以及網路 I/O 頻寬使用率降低。如果複本是跨磁碟區的、則相較於主機型複本、效能可能不會大幅提升。

對於SAN環境、ODX只有在主機和儲存系統均支援時才能使用。支援ODX並自動且透明地啟用ODX的用戶端電腦、可在移動或複製檔案時使用卸載檔案傳輸。無論您是透過Windows檔案總管拖放檔案、還是使用命令列檔案複製命令、或是用戶端應用程式啟動檔案複製要求、都會使用ODX。

使用**ODX**的需求

如果您打算使用ODX進行複本卸載、則必須熟悉Volume支援考量、系統需求及軟體功能需求。

若要使用ODX、您的系統必須具備下列條件：

- ONTAP

  在支援的ONTAP 版本的支援中、會自動啟用ODX。

- 來源Volume下限為2 GB

  為獲得最佳效能、來源磁碟區應大於260 GB。

- Windows用戶端上的ODX支援

  ODX在Windows Server 2012或更新版本以及Windows 8或更新版本中均受支援。互通性對照表包含有關支援的Windows用戶端的最新資訊。

  "NetApp 互通性對照表工具"

- 複製ODX的應用程式支援

  執行資料傳輸的應用程式必須支援ODX。支援ODX的應用程式作業包括：

  - Hyper-V 管理作業，例如建立及轉換虛擬硬碟（ VHD ），管理快照，以及在虛擬機器之間複製檔案
  - Windows檔案總管作業
  - Windows PowerShell複製命令
  - Windows命令提示字元複製命令
    Microsoft TechNet Library 包含更多關於 Windows 伺服器和用戶端上支援的 ODX 應用程式的資訊。

- 如果使用壓縮磁碟區、壓縮群組大小必須為8K。

  不支援32K壓縮群組大小。

ODX不適用於下列磁碟區類型：

- 容量低於2 GB的來源磁碟區
- 唯讀磁碟區
- "資料量FlexCache"

  FlexCache 原始磁碟區支援 ODX 。

- "半厚的已配置磁碟區"

特殊系統檔案需求

您可以刪除qtree中找到的ODX檔案。除非技術支援人員告訴您，否則請勿移除或修改任何其他 ODX 系統檔案。

使用ODX功能時、系統的每個磁碟區都有ODX系統檔案。這些檔案可讓ODX傳輸期間所使用的資料以時間點表示。下列系統檔案位於每個磁碟區的根層級、其中包含已卸載資料的LUN或檔案：

- `.copy-offload` （隱藏目錄）
- `.tokens` （檔案位於隱藏的下方 `.copy-offload` 目錄）

您可以使用 `copy-offload delete-tokens -path dir_path -node` *`node_name`* 刪除包含 ODX 檔案的 qtree 的命令。

ODX的使用案例

您應該瞭解在SVM上使用ODX的使用案例、以便判斷ODX在何種情況下可為您提供效能優勢。

支援ODX的Windows伺服器和用戶端使用複本卸載做為在遠端伺服器上複製資料的預設方法。如果Windows伺服器或用戶端不支援ODX、或ODX複本卸載在任何時間點都失敗、則複本或移動作業會回溯到複本或移動作業的傳統讀取和寫入。

下列使用案例支援使用ODX複本和移動：

- Volume內

  來源與目的地檔案或LUN位於同一個磁碟區內。

- 磁碟區間、相同節點、相同SVM

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料歸同一個SVM所有。

- 磁碟區間、不同節點、相同SVM

  來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料歸同一個SVM所有。

- SVM之間、相同節點

  來源與目的地檔案或LUN位於同一個節點上的不同磁碟區。資料由不同的SVM擁有。

- SVM之間、不同節點

  來源與目的地檔案或LUN位於不同節點上的不同磁碟區。資料由不同的SVM擁有。

- 叢集間

  來源和目的地LUN位於不同的磁碟區、位於不同的叢集節點上。這僅支援 SAN 、不適用於 SMB 。

還有一些特殊使用案例：

- 藉由ONTAP 採用流通不整的ODX技術、您可以使用ODX在SMB共享區與FC或iSCSI附加虛擬磁碟機之間複製檔案。

  您可以使用Windows檔案總管、Windows CLI或PowerShell、Hyper-V或其他支援ODX的應用程式、使用ODX複製卸載功能在SMB共用區和連線LUN之間順暢地複製或移動檔案、前提是SMB共用區和LUN位於同一個叢集上。

- Hyper-V針對ODX複製卸載提供了一些額外的使用案例：

  - 您可以使用ODX複本卸載傳遞搭配Hyper-V、在虛擬硬碟（VHD）檔案內或之間複製資料、或在同一個叢集內的對應SMB共用區和連接的iSCSI LUN之間複製資料。

    如此一來、從客體作業系統的複本就能傳遞到基礎儲存設備。

  - 建立固定大小的VHD時、ODX會使用已知的零權杖、以零初始化磁碟。
  - 如果來源與目的地儲存設備位於同一個叢集、則ODX複本卸載可用於虛擬機器儲存移轉。

若要利用ODX複本卸載傳遞與Hyper-V的使用案例、來賓作業系統必須支援ODX、而來賓作業系統的磁碟必須是支援ODX的儲存設備（SMB或SAN）所支援的SCSI磁碟。客體作業系統上的IDE磁碟不支援ODX傳遞。

了解 **NVMe** 複製卸載

NVMe 複製卸載功能可讓 NVMe 主機將複製作業從其 CPU 解除安裝至ONTAP儲存控制器的 CPU。主機可以將資料從一個 NVMe 命名空間複製到另一個 NVMe 命名空間，同時將其 CPU 資源保留給應用程式工作負載。

例如，假設您需要重新平衡儲存工作負載以改善效能分佈。這需要您遷移 10 台虛擬機器 (VM)，其中包含 45 個 NVMe 命名空間，每個命名空間的平均大小為 500 GB。這意味著你需要複製大約 22.5 TB 的資料。主機無需使用自身的 CPU 進行資料遷移，而是可以使用 NVMe 複製卸載功能，從而避免在資料複製期間佔用 CPU 資源來處理應用程式工作負載。

NVMe 複製卸載支援和限制

從ONTAP 9.18.1 開始支援 NVMe 複製卸載。 ONTAP無法啟動 NVMe 複製卸載；它必須由主機支援和啟動。

以下限制適用於使用ONTAP進行的 NVMe 複製卸載作業：

- 支援的最大複製操作大小為 16MB。
- 資料只能在同一子系統內的 NVMe 命名空間之間遷移。
- 資料只能在同一高可用性 (HA) 對中的節點之間遷移。

SAN管理

SAN 資源配置

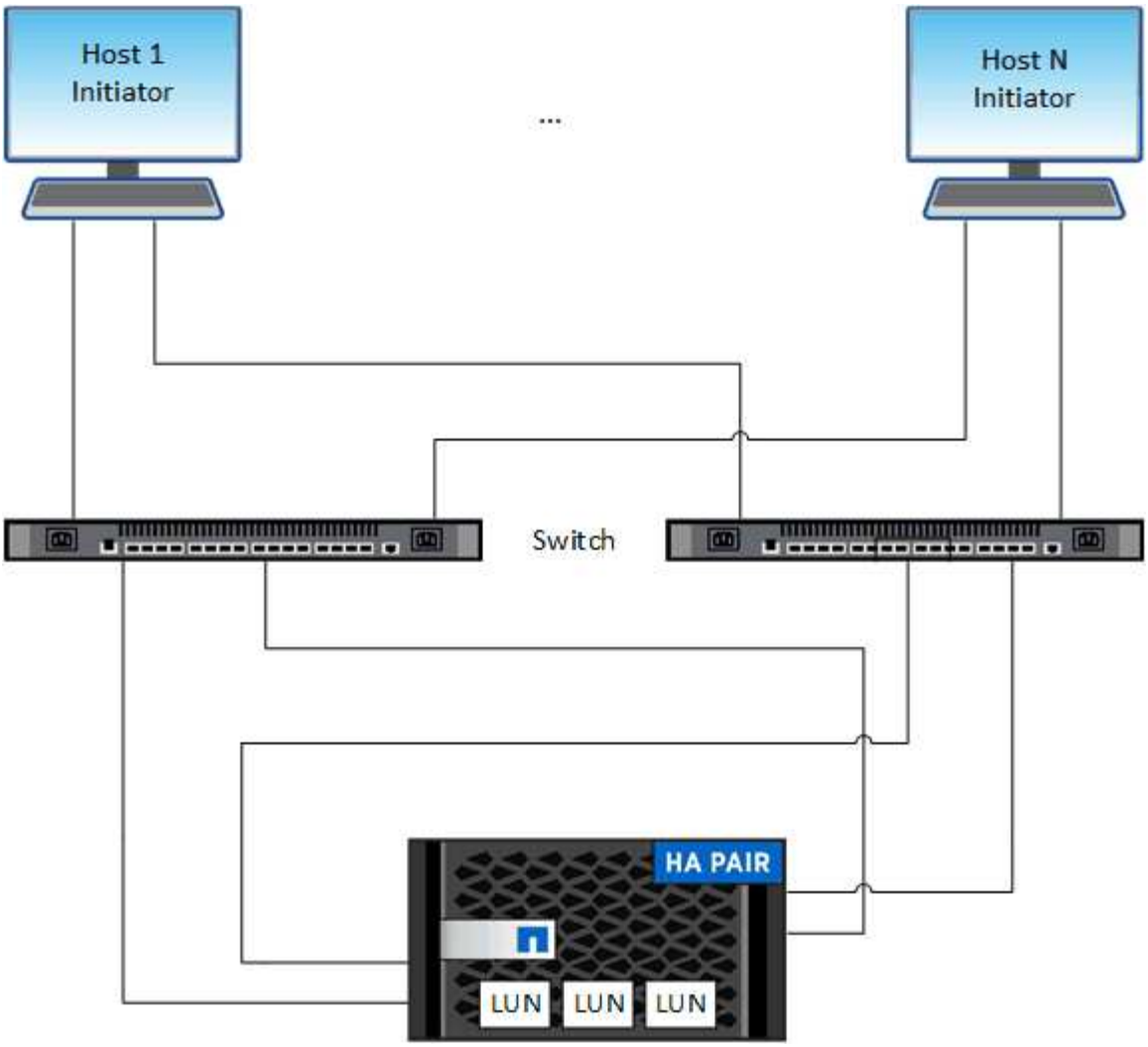
SAN管理總覽

本節內容說明如何在ONTAP 更新版本的更新版本中、使用支援更新版本ONTAP 的指令行介面（CLI）和系統管理程式來設定及管理SAN環境。

如果您使用的是經典系統管理程式（僅ONTAP 適用於更新版本的版本）、請參閱下列主題：

- "iSCSI傳輸協定"
- "FC/FCoE傳輸協定"

您可以使用iSCSI和FC傳輸協定、在SAN環境中提供儲存設備。



使用iSCSI和FC時、儲存目標稱為LUN（邏輯單元）、並以標準區塊裝置形式呈現給主機。 您可以建立LUN、然後將其對應至啟動器群組（igroup）。 啟動器群組是FC主機WWP和iSCSI主機節點名稱的表格、可控制哪些啟動器可以存取哪些LUN。

FC目標會透過FC交換器和主機端介面卡連線至網路、並以全球連接埠名稱（WWPN）來識別。 iSCSI 目標透過標準乙太網路介面卡（ NIC ）、 TCP 卸載引擎（ TOE ）卡（含軟體啟動器）、融合式網路介面卡（ CNA ）或專用主機胸片介面卡（ HBA ）連線至網路、並由 iSCSI 合格名稱（ IQN ）識別。

以取得更多資訊

如果您有 ASA R2 儲存系統（ ASA A1K ， ASA A90 ， ASA A70 ， ASA A50 ， ASA A30 或 ASA A20 ），請參閱"ASA R2 儲存系統文件"。

瞭解 **All Flash SAN Array** 組態

NetApp All Flash SAN Array （ ASA ）從 ONTAP 9.7 開始提供。 ASA是純Flash SAN解決方案、以獲證實AFF 的NetApp平台為建置基礎。

ASA 平台包括以下內容：

- ASA A150
- ASA A250

- ASA A400
- ASA A800
- ASA A900
- ASA C250
- ASA C400
- ASA C800

> 從 ONTAP 9.16.0 開始， ASA R2 系統（ ASA A1K ， ASA A90 ， ASA A70 ， ASA A50 ， ASA A30 或 ASA A20 ）提供專為僅限 SAN 客戶所設計的簡化 ONTAP 體驗。如果您使用的是 ASA R2 系統，請參閱"ASA R2 系統文件"。

ASA 平台使用對稱的雙主動式多重路徑。所有路徑都是主動/最佳化的、因此在發生儲存容錯移轉時、主機不需要等待容錯移轉路徑的ALUA轉換、即可恢復I/O如此可縮短容錯移轉的時間。

設定**ASA** 一個功能完善的

All Flash SAN Arrays （ ASA ）的設定程序與非 ASA 系統相同。

System Manager會引導您完成初始化叢集、建立本機層級、設定通訊協定、以及為ASA 您的支援資源配置儲存設備所需的程序。

開始設定 ONTAP 叢集。

支援主機設定與公用程式**ASA**

設定 All Flash SAN Array （ ASA ）的主機設定與所有其他 SAN 主機的主機設定相同。

您可以下載 "NetApp主機公用程式軟體" 支援網站上的特定主機。

辨**ASA** 識出一套系統的方法

您可以ASA 使用System Manager或ONTAP 使用指令行介面（CLI）來識別出一個無法辨識的系統。

- * 從 System Manager 儀表板 * ：按一下 * 叢集 > 總覽 * 、然後選取系統節點。
- 特性 * 會顯示為 * All Flash SAN Array * 。
- * 從 CLI * ：輸入 `san config show` 命令。

  對於 ASA 系統、「 All Flash SAN Array 」值會傳回為 TRUE 。

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

相關資訊

- "技術報告 4968 ： NetApp All SAN 陣列資料可用度與完整性"
- "NetApp 技術報告 4080 ：現代 SAN 的最佳實務做法"

設定**FCoE**的交換器

您必須先為FCoE設定交換器、FC服務才能在現有的乙太網路基礎架構上執行。

開始之前

- 您的SAN組態必須受到支援。

  如需支援組態的詳細資訊、請參閱 "NetApp 互通性對照表工具"。

- 您的儲存系統必須安裝統一化目標介面卡（UTA）。

  如果您使用的是 UTA2 、則必須將其設定為 `cna` 模式。

- 主機上必須安裝整合式網路卡（CNA）。

步驟

1. 請使用交換器文件來設定FCoE的交換器。
2. 確認叢集中每個節點的 DCB 設定都已正確設定。

   ```
   run -node node1 -command dcb show
   ```

   DCB設定值是在交換器上設定的。如果設定不正確、請參閱交換器文件。

3. 驗證當 FC 目標連接埠的線上狀態為時、 FCoE 登入是否正常運作 `true`。

   ```
   fcp adapter show -fields node,adapter,status,state,speed,fabric-
   established,physical-protocol
   ```

   如果 FC 目標連接埠的線上狀態為 `false`，請參閱交換器文件。

相關資訊

- "NetApp 互通性對照表工具"
- "NetApp技術報告3800：乙太網路光纖通道（FCoE）端點對端點部署指南"
- "Cisco MDS 9000 NX-OS與SAN-OS軟體組態指南"
- "Brocade產品"

系統需求

設定LUN包括建立LUN、建立igroup、以及將LUN對應至igroup。您的系統必須符合特定先決條件、才能設定LUN。

- 互通性對照表必須列出您所支援的SAN組態。
- 您的SAN環境必須符合中指定的SAN主機和控制器組態限制 "NetApp Hardware Universe" 適用於ONTAP 您的版本的

- 必須安裝受支援版本的主機公用程式。

  主機公用程式文件提供更多資訊。

- 您必須在LUN所屬節點和所屬節點的HA合作夥伴上擁有SAN生命里數。

相關資訊

- "NetApp 互通性對照表工具"
- "SAN主機組態ONTAP"
- "NetApp技術報告4017：Fibre Channel SAN最佳實務做法"

建立**LUN**之前的須知事項

開始在叢集上設定 LUN 之前，您必須先檢閱這些 LUN 準則。

為何實際**LUN**大小會稍有不同

您應該注意下列有關LUN大小的資訊。

- 當您建立LUN時、LUN的實際大小可能會因LUN的作業系統類型而稍有不同。LUN建立後、無法修改LUN OS類型。
- 如果您以最大 LUN 大小建立 LUN 、請注意、 LUN 的實際大小可能會稍微小一些。將限制捨位至稍低的值。ONTAP
- 每個LUN的中繼資料在包含的Aggregate中需要約64 KB的空間。建立LUN時、您必須確保包含的Aggregate有足夠的空間來容納LUN的中繼資料。如果Aggregate沒有足夠的空間來容納LUN的中繼資料、則部分主機可能無法存取LUN。

指派**LUN ID**的準則

通常、預設LUN ID以0開頭、並以1為增量指派給每個額外的對應LUN。主機會將LUN ID與LUN的位置和路徑名稱建立關聯。有效LUN ID編號的範圍取決於主機。如需詳細資訊、請參閱主機公用程式隨附的文件。

將**LUN**對應至**igroup**的準則

- 您只能將LUN對應至igroup一次。
- 最佳實務做法是透過 igroup 將 LUN 對應至僅一個特定的啟動器。
- 您可以將單一啟動器新增至多個igroup、但啟動器只能對應至一個LUN。
- 您無法對對應至相同igroup的兩個LUN使用相同的LUN ID。
- igroup和連接埠集應該使用相同的傳輸協定類型。

驗證並新增您的傳輸協定**FC**或**iSCSI**授權

在使用FC或iSCSI啟用儲存虛擬機器（SVM）的區塊存取之前、您必須先取得授權。FC 和 iSCSI 授權隨附於"ONTAP One"。

範例 **14.** 步驟

系統管理員

如果您沒有 ONTAP 、請使用 ONTAP 系統管理員（ 9.7 及更新版本）驗證並新增 FC 或 iSCSI 授權。

1. 在 System Manager 中、選取 * 叢集 > 設定 > 授權 *
2. 如果未列出授權、請選取並輸入授權

金鑰。
3. 選取*「Add*」 。

CLI

如果您沒有 ONTAP 、請使用 ONTAP CLI 驗證並新增 FC 或 iSCSI 授權。

1. 確認您擁有FC或iSCSI的有效授權。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. 如果您沒有FC或iSCSI的有效授權、請新增授權代碼。

```
license add -license-code <your_license_code>
```

配置**SAN**儲存設備

此程序會在已設定FC或iSCSI傳輸協定的現有儲存VM上建立新的LUN。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"來配置您的儲存。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

如果您需要建立新的儲存VM並設定FC或iSCSI傳輸協定、請參閱 "設定SVM for FC" 或 "設定SVM for iSCSI"。

如果未啟用FC授權、則LIF和SVM似乎處於線上狀態、但作業狀態為停機。

LUN在您的主機上顯示為磁碟裝置。

在LUN建立期間、一律會啟用非對稱邏輯單元存取（ALUA）。您無法變更ALUA設定。

您必須為SVM中的所有FC LIF使用單一啟動器分區、才能裝載啟動器。

從ONTAP 供應儲存設備開始、預設會啟用QoS。您可以在資源配置程序期間或稍後時間停用 QoS 、或選擇自訂 QoS 原則。

範例 **15.** 步驟

系統管理員

使用FC或iSCSI傳輸協定搭配ONTAP 使用支援《支援系統管理程式》（9.7及更新版本）、建立LUN、為SAN主機提供儲存設備。

若要使用 System Manager Classic （ 9.7 及更早版本提供）完成此工作、請參閱 "適用於Red Hat Enterprise Linux的iSCSI組態"

步驟

1. 在主機上安裝適當"SAN主機公用程式"的。
2. 在System Manager中、按一下* Storage > LUN*、然後按一下* Add*。
3. 輸入建立LUN所需的資訊。
4. 視ONTAP 您的版本而定、您可以按一下*更多選項*來執行下列任何一項。

選項	從開始提供
• 將QoS原則指派給LUN、而非父Volume ◦ 更多選項>儲存與最佳化 ◦ 選擇*效能服務層級*。 ◦ 若要將QoS原則套用至個別LUN而非整個磁碟區、請選取*將這些效能限制強制套用至每個LUN*。 根據預設、效能限制會套用至Volume層級。	零點9.10.1 ONTAP
• 使用現有的啟動器群組建立新的啟動器群組 ◦ 更多選項>主機資訊 ◦ 使用現有的啟動器群組*選取*新的啟動器群組。 包含其他 igroup 的 igroup 作業系統類型在建立之後無法變更。	部分9.9.1 ONTAP
• 將說明新增至igroup或主機啟動器 此說明可做為igroup或主機啟動器的別名。 ◦ 更多選項>主機資訊	部分9.9.1 ONTAP

• 在現有磁碟區上建立LUN 根據預設、新的LUN會建立在新的Volume中。 ◦ 更多選項>新增**LUN** ◦ 選擇*組相關LUN*。	部分9.9.1 ONTAP
• 停用QoS或選擇自訂QoS原則 ◦ 更多選項>儲存與最佳化 ◦ 選擇*效能服務層級*。 在 ONTAP 9.9.1 及更新版本中、如果您選取自訂 QoS 原則、也可以選取手動放置在指定的本機層。	部分9.8 ONTAP

5. 對於FC、請根據WWPN對FC交換器進行分區。每個啟動器使用一個區域、並在每個區域中包含所有目標連接埠。
6. 探索主機上的LUN。

   對於 VMware vSphere 、請使用虛擬儲存主控台（ VSC ）來探索及初始化 LUN 。
7. 初始化 LUN 並選擇性建立檔案系統。
8. 確認主機可以在LUN上寫入和讀取資料。

CLI

使用FC或iSCSI傳輸協定搭配ONTAP 使用CLI建立LUN、為SAN主機提供儲存空間。

1. 確認您擁有 FC 或 iSCSI 的授權。

```
system license show
```

```
Package           Type    Description           Expiration
 ----------------- ------- ---------------------
--------------------
 Base              site    Cluster Base License  -
 NFS               site    NFS License           -
 CIFS              site    CIFS License          -
 iSCSI             site    iSCSI License         -
 FCP               site    FCP License           -
```

2. 如果您沒有 FC 或 iSCSI 授權、請使用 `license add` 命令。

```
license add -license-code <your_license_code>
```

3. 在SVM上啟用您的傳輸協定服務：

   ◦ iSCSI ： *

   ```
   vserver iscsi create -vserver <svm_name> -target-alias <svm_name>
   ```

   ◦ 代表 FC ： *

```
vserver fcp create -vserver <svm_name> -status-admin up
```

4. 在每個節點上為SVM建立兩個生命期：

```
network interface create -vserver <svm_name> -lif <lif_name> -role
data -data-protocol <iscsi|fc> -home-node <node_name> -home-port
<port_name> -address <ip_address> -netmask <netmask>
```

   NetApp為每個SVM服務資料的每個節點至少支援一個iSCSI或FC LIF。不過、備援需要每個節點兩個生命期。對於 iSCSI 、建議您在不同的乙太網路中、每個節點至少設定兩個生命期。

5. 確認您的生命已建立、且其操作狀態為 `online`：

```
network interface show -vserver <svm_name> <lif_name>
```

6. 建立LUN：

```
lun create -vserver <svm_name> -volume <volume_name> -lun <lun_name>
-size <lun_size> -ostype linux -space-reserve <enabled|disabled>
```

   您的LUN名稱不得超過255個字元、且不得包含空格。

   在磁碟區中建立LUN時、NVFIL選項會自動啟用。

7. 建立您的igroup：

```
igroup create -vserver <svm_name> -igroup <igroup_name> -protocol
<fcp|iscsi|mixed> -ostype linux -initiator <initiator_name>
```

8. 將LUN對應至igroup：

```
lun mapping create -vserver <svm_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. 驗證LUN的設定是否正確：

```
lun show -vserver <svm_name>
```

10. （可選） "建立連接埠集並繫結至igroup"。
11. 請遵循主機文件中的步驟、在特定主機上啟用區塊存取。
12. 使用主機公用程式完成FC或iSCSI對應、並探索主機上的LUN。

相關資訊

- "SAN管理總覽"
- "SAN主機組態ONTAP"
- "在System Manager中檢視及管理SAN啟動器群組"
- "NetApp技術報告4017：Fibre Channel SAN最佳實務做法"

NVMe資源配置

NVMe總覽

您可以使用非揮發性記憶體Express（NVMe）傳輸協定、在SAN環境中提供儲存設備。NVMe傳輸協定已針對固態儲存設備的效能最佳化。

對於NVMe、儲存目標稱為命名空間。 NVMe命名空間是一組非揮發性儲存設備、可格式化為邏輯區塊、並以標準區塊裝置呈現給主機。 您可以建立命名空間和子系統、然後將命名空間對應至子系統、就像是將LUN配置及對應至FC和iSCSI的igroup一樣。

NVMe目標是透過使用FC交換器的標準FC基礎架構、或使用乙太網路交換器和主機端介面卡的標準TCP基礎架構、連線至網路。

NVMe支援會因ONTAP 您的版本的不相同而有所差異。 請參閱 "NVMe支援與限制" 以取得詳細資料。

什麼是NVMe

非揮發性記憶體Express（NVMe）傳輸協定是用於存取非揮發性儲存媒體的傳輸協定。

NVMe over Fabrics（NVMeoF）是NVMe規格定義的延伸、可透過PCIe以外的連線進行NVMe型通訊。此介面可讓外部儲存機箱連線至伺服器。

NVMe的設計可讓您有效率地存取以非揮發性記憶體建置的儲存裝置、從Flash技術到效能更高的持續記憶體技術、都能輕鬆存取。因此、它的限制與專為硬碟機設計的儲存傳輸協定並不相同。Flash和固態裝置（SSD）是一種非揮發性記憶體（NVM）。NVM是一種記憶體類型、可在停電期間保留內容。NVMe是存取該記憶體的方法。

NVMe的優點包括提升資料傳輸的速度、生產力、處理量和容量。具體特性包括：

- NVMe的設計可容納多達64、000個佇列。

  每個佇列最多可有64000個並行命令。

- NVMe由多家硬體與軟體廠商支援
- NMVe採用Flash技術、可加快回應時間、提高生產力
- NVMe可針對傳送至SSD的每個「REquest」、要求多個資料要求。

  NVMe解碼「資源要求」所需的時間較短、而且不需要在多執行緒程式中鎖定執行緒。

- NVMe支援的功能可防止CPU層級出現瓶頸、並可在系統擴充時提供大幅擴充性。

關於**NVMe**命名空間

NVMe命名空間是一組可格式化為邏輯區塊的非揮發性記憶體（NVM）。當儲存虛擬機器設定為使用NVMe傳輸協定、且相當於FC和iSCSI傳輸協定的LUN時、就會使用命名空間。

一個或多個命名空間已配置並連線至NVMe主機。每個命名空間都可支援不同的區塊大小。

NVMe傳輸協定可透過多個控制器存取命名空間。使用大多數作業系統都支援的NVMe驅動程式、固態磁碟機（SSD）命名空間會顯示為標準區塊裝置、可在不做任何修改的情況下部署檔案系統和應用程式。

命名空間ID（NSID）是控制器用來提供命名空間存取權的識別碼。設定主機或主機群組的NSID時、您也可以設定主機存取磁碟區的功能。邏輯區塊一次只能對應至單一主機群組、而指定的主機群組沒有任何重複的NSs。

關於**NVMe**子系統

NVMe子系統包含一或多個NVMe控制器、命名空間、NVM子系統連接埠、NVM儲存媒體、以及控制器與NVM儲存媒體之間的介面。建立NVMe命名空間時、預設不會對應至子系統。您也可以選擇將其對應為新的或現有的子系統。

相關資訊

- 瞭解 "配置NVMe儲存設備"ASA 、 AFF 和 FAS 系統
- 瞭解 "將 NVMe 命名空間對應至子系統"ASA AFF 和 FAS 系統的。
- "設定SAN主機和雲端用戶端"
- 瞭解 "配置 SAN 儲存設備"ASA R2 （ ASA A1K ， ASA A90 ， ASA A70 ， ASA A50 ， ASA A30 或 ASA A20 ）儲存系統。

NVMe授權需求

從支援NVMe 9.5開始ONTAP 需要授權。如果ONTAP NVMe是在更新至ONTAP 版本號9.5之後啟用、系統會給予90天的寬限期以取得授權。

您可以使用下列命令來啟用授權：

```
system license add -license-code NVMe_license_key
```

NVMe 組態、支援和限制

從 ONTAP 9.4 開始 "非揮發性記憶體高速（ NVMe ）" 傳輸協定適用於 SAN 環境。FC-NVMe採用與傳統FC網路相同的實體設定和分區實務做法、但相較於FC-SCSI、可提供更高的頻寬、增加IOPs並縮短延遲。

NVMe 支援和限制會因您的 ONTAP 版本、平台和組態而異。如需特定組態的詳細資訊、請參閱 "NetApp 互通性對照表工具"。如需支援的限制、請參閱 "Hardware Universe"。

每個叢集的最大節點數可在 * 支援的平台混合 * 下的 Hardware Universe 中使用。

組態

- 您可以使用單一架構或 Multifabric 來設定 NVMe 組態。
- 您應該為每個支援SAN的SVM設定一個管理LIF。
- 不支援使用異質FC交換器架構、但內嵌刀鋒交換器除外。

  上會列出特定例外狀況 "NetApp 互通性對照表工具"。

- 串聯、部分網狀、全網狀、核心邊緣和導向架構都是將FC交換器連接至光纖的業界標準方法、而且都受到支援。

  一個網路可由一或多個交換器組成、而且儲存控制器可連接至多個交換器。

功能

您的 ONTAP 版本支援下列 NVMe 功能。

從ONTAP 無到無…開始	NVMe 支援
9.17.1	• SnapMirror主動同步 NVMe/FC 和 NVMe/TCP 主機訪問，適用於 VMware 工作負載。
9.15.1..	• NVMe / TCP 上的四節點 MetroCluster IP 組態
9.14.1.	• 設定子系統的主機優先順序（主機層級 QoS ）
9.12.1	• NVMe / FC 上的四節點 MetroCluster IP 組態 • ONTAP 9.12.1 之前的前端 NVMe 網路不支援 MetroCluster 組態。 • NVMe / TCP 不支援 MetroCluster 組態。
9.10.1	調整命名空間大小
9.9.1	• 命名空間與 LUN 共存於同一個磁碟區

9.8	• 協定共存 SCSI 、 NAS 和 NVMe 通訊協定可以存在於同一個儲存虛擬機器（ SVM ）上。 在 ONTAP 9.8 之前、 NVMe 可以是 SVM 上唯一的傳輸協定。
9.6%	• 512 位元組區塊和 4096 位元組區塊用於命名空間 預設值為4096。只有當主機作業系統不支援4096位元組區塊時、才應使用512。 • 使用對應命名空間來移動 Volume
9.5.	• 多重路徑HA配對容錯移轉/恢復

通訊協定

支援下列 NVMe 通訊協定。

傳輸協定	從ONTAP 無到無…開始	允許者…
TCP	9.10.1	預設
FC	9.4.	預設

從 ONTAP 9.8 開始、您可以在同一個儲存虛擬機器（ SVM ）上設定 SCSI 、 NAS 和 NVMe 通訊協定。
在 ONTAP 9.7 及更早版本中、 NVMe 可能是 SVM 上唯一的傳輸協定。

命名空間

使用 NVMe 命名空間時、您應該注意下列事項：

- 對於 ONTAP 9.15.1 及更早版本， ONTAP 不支援 NVMe 資料集管理（取消分配）命令來進行空間回收。
- 您無法使用 SnapRestore 從 LUN 還原命名空間、反之亦然。
- 命名空間的空間保證與所含磁碟區的空間保證相同。
- 您無法在從以 7-Mode 運作的 Data ONTAP 進行磁碟區轉換時建立命名空間。
- 命名空間不支援下列項目：
  - 重新命名
  - 跨Volume移動
  - 跨Volume複本
  - 隨需複製

其他限制

NVMe組態不支援下列**ONTAP** 功能：

- 虛擬儲存主控台
- 持續保留

下列項目僅適用於執行**ONTAP** 下列功能的節點：

- NVMe LIF和命名空間必須裝載在同一個節點上。
- NVMe服務必須在建立NVMe LIF之前建立。

相關資訊

"現代 SAN 的最佳實務做法"

設定**NVMe**的儲存**VM**

如果您要在節點上使用NVMe傳輸協定、則必須針對NVMe專門設定SVM。

開始之前

您的FC或乙太網路介面卡必須支援NVMe。支援的介面卡列於 "NetApp Hardware Universe"。

範例 **16.** 步驟

系統管理員

使用ONTAP 「支援NVMe的儲存虛擬機器」（9.7及更新版本）。

在新的儲存**VM**上設定**NVMe**	在現有儲存**VM**上設定**NVMe**
1. 在System Manager中、按一下* Storage > Storage VM*、然後按一下* Add*。 2. 輸入儲存VM的名稱。 3. 選擇* NVMe 作為*存取傳輸協定。 4. 選取*啟用NVMe/FC*或*啟用NVMe/TCP*和*儲存*。	1. 在System Manager中、按一下* Storage > Storage VM*。 2. 按一下您要設定的儲存VM。 3. 按一下 * 設定 * 索引標籤、然後按一下 NVMe 通訊協定旁的。 4. 選取*啟用NVMe/FC*或*啟用NVMe/TCP*和*儲存*。

CLI

使用ONTAP 支援NVMe的CLI設定儲存VM。

1. 如果您不想使用現有的SVM、請建立一個：

```
vserver create -vserver <SVM_name>
```

   a. 驗證是否已建立SVM：

```
vserver show
```

2. 請確認叢集中已安裝支援NVMe或TCP的介面卡：

   NVMe ：

```
network fcp adapter show -data-protocols-supported fc-nvme
```

   對於 TCP ：

```
network port show
```

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

3. 如果您執行ONTAP 的是SVM 9.7或更早版本、請移除SVM的所有傳輸協定：

```
vserver remove-protocols -vserver <SVM_name> -protocols
iscsi,fcp,nfs,cifs,ndmp
```

從ONTAP 功能支援的9.8開始、新增NVMe時不需要移除其他傳輸協定。

4. 將NVMe傳輸協定新增至SVM：

```
vserver add-protocols -vserver <SVM_name> -protocols nvme
```

5. 如果您執行ONTAP 的是SVM上的支援版本、請確認NVMe是SVM上唯一允許的傳輸協定：

```
vserver show -vserver <SVM_name> -fields allowed-protocols
```

NVMe 應該是唯一顯示在下的傳輸協定 `allowed protocols` 欄位。

6. 建立NVMe服務：

```
vserver nvme create -vserver <SVM_name>
```

7. 驗證NVMe服務是否已建立：

```
vserver nvme show -vserver <SVM_name>
```

`Administrative Status`SVM 的應列爲 `up`
。如link:https://docs.netapp.com/us-en/ontap-cli/up.html["
指令參考資料ONTAP"^]需詳細 `up`資訊，請參閱。

8. 建立NVMe / FC LIF：
   - 對於 ONTAP 9.9.1 或更早版本、 FC ：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - 對於 ONTAP 9.10.1 或更高版本，FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-tcp | default-data-nvme-fc>
-data-protocol <fc-nvme> -home-node <home_node> -home-port
<home_port> -status-admin up -failover-policy disabled -firewall
-policy data -auto-revert false -failover-group <failover_group>
-is-dns-update-enabled false
```

- 對於 ONTAP 9.10.1 或更高版本，TCP：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

9. 在HA合作夥伴節點上建立NVMe / FC LIF：
   - 對於 ONTAP 9.9.1 或更早版本、 FC ：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-role data -data-protocol fc-nvme -home-node <home_node> -home
-port <home_port>
```

   - 對於 ONTAP 9.10.1 或更高版本，FC：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-service-policy <default-data-nvme-fc> -data-protocol <fc-nvme>
-home-node <home_node> -home-port <home_port> -status-admin up
-failover-policy disabled -firewall-policy data -auto-revert
false -failover-group <failover_group> -is-dns-update-enabled
false
```

   - 對於 ONTAP 9.10.1 或更高版本，TCP：

```
network interface create -vserver <SVM_name> -lif <lif_name>
-address <ip address> -netmask <netmask_value> -service-policy
<default-data-nvme-tcp> -data-protocol <nvme-tcp> -home-node
<home_node> -home-port <home_port> -status-admin up -failover
-policy disabled -firewall-policy data -auto-revert false
-failover-group <failover_group> -is-dns-update-enabled false
```

10. 確認已建立NVMe / FC LIF：

```
network interface show -vserver <SVM_name>
```

11. 在LIF所在的同一個節點上建立Volume：

```
vol create -vserver <SVM_name> -volume <vol_name> -aggregate
<aggregate_name> -size <volume_size>
```

如果顯示有關自動效率原則的警告訊息、則可以安全地忽略該訊息。

配置**NVMe**儲存設備

請使用這些步驟、為現有儲存 VM 上任何 NVMe 支援的主機建立命名空間並配置儲存空間。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"來配置您的儲存。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

從ONTAP 供應儲存設備開始、預設會啟用QoS。您可以在資源配置程序期間或稍後停用QoS或選擇自訂QoS原則。

開始之前

您的儲存VM必須設定為NVMe、而且您的FC或TCP傳輸應該已經設定完成。

系統管理員

使用「支援系統管理程式」（9.7及更新版本）建立命名空間、以使用NVMe傳輸協定來提供儲存設備ONTAP 。

步驟

1. 在系統管理員中、按一下*儲存設備> NVMe命名空間*、然後按一下*新增*。

   如果您需要建立新的子系統、請按一下*「更多選項」*。

2. 如果您執行ONTAP 的是支援功能的9.8或更新版本、而您想要停用QoS或選擇自訂QoS原則、請按一下*更多選項*、然後在*儲存與最佳化*下選取*效能服務層級*。
3. 將FC交換器分區至WWPN。每個啟動器使用一個區域、並在每個區域中包含所有目標連接埠。
4. 在主機上探索新命名空間。
5. 初始化命名空間並使用檔案系統進行格式化。
6. 確認主機可以在命名空間上寫入和讀取資料。

CLI

使用ONTAP 支援功能的CLI建立命名空間、以使用NVMe傳輸協定來提供儲存設備。

此程序會在已針對NVMe傳輸協定設定的現有儲存VM上建立NVMe命名空間和子系統、然後將命名空間對應至子系統、以便從主機系統存取資料。

如果您需要設定NVMe的儲存VM、請參閱 "設定NVMe的SVM"。

步驟

1. 確認SVM已設定為NVMe：

   ```
   vserver show -vserver <svm_name> -fields allowed-protocols
   ```

   `NVMe` 應顯示在下 `allowed-protocols` 欄位。

2. 建立NVMe命名空間：

   > 您使用參數所參照的磁碟區必須已經存在，否則您必須先建立一個磁碟區 `-path`，才能執行此命令。

   ```
   vserver nvme namespace create -vserver <svm_name> -path <path> -size
   <size_of_namespace> -ostype <OS_type>
   ```

3. 建立NVMe子系統：

```
vserver nvme subsystem create -vserver <svm_name> -subsystem
<name_of_subsystem> -ostype <OS_type>
```

NVMe子系統名稱區分大小寫。必須包含1到96個字元。允許使用特殊字元。

4. 驗證子系統是否已建立：

```
vserver nvme subsystem show -vserver <svm_name>
```

。 `nvme` 子系統應顯示在 `Subsystem` 欄位。

5. 從主機取得NQN。
6. 將主機NQN新增至子系統：

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN>
```

7. 將命名空間對應至子系統：

```
vserver nvme subsystem map add -vserver <svm_name> -subsystem
<subsystem_name> -path <path>
```

命名空間只能對應至單一子系統。

8. 確認命名空間已對應至子系統：

```
vserver nvme namespace show -vserver <svm_name> -instance
```

子系統應列為 `Attached subsystem`。

將**NVMe**命名空間對應至子系統

將 NVMe 命名空間對應至子系統可讓您從主機存取資料。 您可以在佈建儲存設備時、將 NVMe 命名空間對應至子系統、也可以在儲存設備佈建之後進行。

從ONTAP 9.17.1 開始，如果您使用SnapMirror主動同步配置，則可以在將主機新增至 NVMe 子系統時，將 SVM 新增至主機作為近端虛擬伺服器。 NVMe子系統中命名空間的主動最佳化路徑僅從配置為近端虛擬伺服器的 SVM 發佈到主機。

從 ONTAP 9.14.1 開始、您可以優先分配特定主機的資源。根據預設、當主機新增至 NVMe 子系統時、會給予一般優先順序。您可以使用 ONTAP 命令列介面（ CLI ）手動將預設優先順序從一般變更為高。 指派高優先順

序的主機會分配較大的 I/O 佇列數和佇列深度。

> 如果您想要將 ONTAP 9.13.1 或更早版本中新增至子系統的主機設為高優先順序、您可以 變更主機優先順序。

開始之前

您的命名空間和子系統應該已經建立。如果您需要建立命名空間和子系統、請參閱 "配置NVMe儲存設備"。

映射 NVMe 命名空間

步驟

1. 從主機取得NQN。
2. 將主機NQN新增至子系統：

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
```

如果您要將主機的預設優先順序從一般變更為高，請使用 `-priority high`選項。此選項從 ONTAP 9.14.1 開始提供。如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host add`資訊，請參閱。

如果您想要新增 SVM 作為 `proximal-vserver`在將主機新增至SnapMirror主動同步設定中的 NVMe 子系統時，您可以使用 `-proximal-vservers`選項。此選項從ONTAP 9.17.1 開始可用。您可以新增來源 SVM 或目標 SVM，或同時新增兩者。執行此命令的 SVM 是預設 SVM。

3. 將命名空間對應至子系統：

```
vserver nvme subsystem map add -vserver <SVM_name> -subsystem
<subsystem_name> -path <path>
```

命名空間只能對應至單一子系統。如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem map add`資訊，請參閱。

4. 確認命名空間已對應至子系統：

```
vserver nvme namespace show -vserver <SVM_name> -instance
```

子系統應列示為 `Attached subsystem`。如"指令參考資料ONTAP"需詳細 `vserver nvme namespace show`資訊，請參閱。

管理LUN

編輯LUN QoS原則群組

從 ONTAP 9.10.1 開始，您可以使用系統管理員同時在多個 LUN 上指派或刪除服務品質

(QoS) 原則。

> 如果QoS原則是在磁碟區層級指派、則必須在磁碟區層級進行變更。 您只能在LUN層級編輯QoS原則（如果原先是在LUN層級指派）。

步驟

1. 在System Manager中、按一下* Storage > LUN*。
2. 選取您要編輯的LUN。

   如果您一次編輯多個LUN、則LUN必須屬於同一個儲存虛擬機器（SVM）。如果您選取的LUN不屬於同一個SVM、則不會顯示編輯QoS原則群組的選項。

3. 按一下*更多*並選取*編輯QoS原則群組*。

將**LUN**轉換成命名空間

從ONTAP 《支援支援支援支援服務的支援服務：支援支援ONTAP 服務」的功能、從功能性的9.11.1開始、您可以使用支援服務器的CLI、將現有的LUN就地轉換為NVMe命名空間。

開始之前

- 指定的LUN不應有任何現有的igroup對應。
- LUN 不應位於 MetroCluster 配置的 SVM 中或 SnapMirror 活動同步關係中。
- LUN不應是傳輸協定端點或繫結至傳輸協定端點。
- LUN不應具有非零前置碼和/或後置串流。
- LUN不應是Snapshot的一部分、也不應是SnapMirror關係的目的地端、做為唯讀LUN。

步驟

1. 將 LUN 轉換為 NVMe 命名空間：

```
vserver nvme namespace convert-from-lun -vserver -lun-path
```

使**LUN**離線

從《Syl9.10.1》開始、ONTAP 您可以使用System Manager將LUN離線。在發行版《僅供參考》9.10.1之前ONTAP 、您必須使用ONTAP CLI使LUN離線。

系統管理員

步驟

1. 在System Manager中、按一下* Storage（儲存設備）>LUN*。
2. 使單一LUN或多個LUN離線

如果您想...	執行此操作...
使單一LUN離線	在 LUN 名稱旁、按一下 ⋮ 並選取 * 離線 * 。
使多個LUN離線	1. 選取您要離線的LUN。 2. 按一下*更多*並選取*離線*。

CLI

使用CLI時、一次只能讓一個LUN離線。

步驟

1. 使 LUN 離線：

```
lun offline <lun_name> -vserver <SVM_name>
```

在 **ONTAP** 中調整 **LUN** 大小

您可以增加或減少LUN的大小。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"增加儲存單元的大小。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

ⓘ 無法調整Solaris LUN的大小。

增加**LUN**的大小

LUN的大小取決ONTAP 於您的版本。

版本ONTAP	最大LUN大小
ONTAP 9.12.1P2 及更新版本	AFF 、 FAS 和 ASA 平台為 128 TB
更新版本ONTAP	• 128 TB （適用於 All Flash SAN Array （ ASA ）平台） • 非 ASA 平台為 16 TB

ONTAP 9.5 、 9.6 、 9.7	16TB
更新版本ONTAP	原始LUN大小的10倍、但不超過16TB、即最大LUN大小。 例如、如果您建立100 GB LUN、則只能將其擴充至1、000 GB。 LUN的實際最大大小可能不恰好為16TB。 將限制捨位至稍低的值。ONTAP

您不需要將LUN離線以增加大小。不過、增加大小之後、您必須重新掃描主機上的LUN、讓主機識別大小的變更。

範例 **17.** 步驟

系統管理員

利用ONTAP 《不含更新版本的系統管理程式》（9.7及更新版本）來增加LUN的大小。

1. 在System Manager中、按一下* Storage > LUN*。
2. 按一下 ⋮ 並選取 * 編輯 * 。
3. 在*儲存與最佳化*之下、增加LUN的大小並*儲存*。

CLI

利用NetApp CLI增加LUN的大小ONTAP 。

1. 增加LUN的大小：

```
lun resize -vserver <SVM_name> -volume <volume_name> -lun <lun_name>
-size <lun_size>
```

如"指令參考資料ONTAP"需詳細 `lun resize`資訊，請參閱。

2. 驗證LUN大小是否增加：

```
lun show -vserver <SVM_name>
```

將LUN的實際最大大小捨去執行的作業系統、使其稍微低於預期值。ONTAP此外、實際LUN大小可能會因LUN的作業系統類型而稍有不同。若要取得正確的調整大小值、請在進階模式中執行下列命令：

```
set -unit B

lun show -fields max-resize-size -volume volume_name -lun lun_name
```

+
如"指令參考資料ONTAP"需詳細 `lun show`資訊，請參閱。

1. 重新掃描主機上的LUN。
2. 遵循主機文件、讓主機檔案系統能夠看到新建立的LUN大小。

減少**LUN**的大小

在減少LUN大小之前、主機必須先將包含LUN資料的區塊移轉到較小LUN大小的邊界。您應該使用 SnapCenter 之類的工具、確保正確減少 LUN 、而不會截斷包含 LUN 資料的區塊。不建議手動減少LUN大小。

當您減少LUN的大小後、ONTAP 即可自動通知啟動器LUN大小已減少。不過、主機可能需要採取其他步驟、才能辨識新的LUN大小。如需減少主機檔案結構大小的特定資訊、請參閱主機文件。

移動**LUN**

您可以在儲存虛擬機器（SVM）內的磁碟區之間移動LUN、但無法跨SVM移動LUN。在SVM內跨磁碟區移動的LUN會立即移動、而且不會中斷連線。

開始之前

如果您的 LUN 使用選擇性 LUN 對應（ SLM ）、您應該 "修改 SLM 報告節點清單" 在您移動 LUN 之前、包括目的地節點及其 HA 合作夥伴。

關於這項工作

在LUN搬移期間、不會保留重複資料刪除、壓縮及壓縮等儲存效率功能。必須在LUN移動完成後重新套用。

透過快照進行資料保護時，資料會在磁碟區層級執行。因此、當您搬移LUN時、LUN屬於目的地Volume的資料保護配置。如果您沒有為目的地磁碟區建立快照，則不會建立 LUN 的快照。此外， LUN 的所有快照都會保留在原始磁碟區中，直到刪除這些快照為止。

您無法將LUN移至下列磁碟區：

- SnapMirror目的地Volume
- SVM根磁碟區

您無法移動下列類型的LUN：

- 已從檔案建立的LUN
- 處於NVFail狀態的LUN
- 處於負載共享關係中的LUN
- 傳輸協定端點類別LUN

當叢集中的節點執行不同的ONTAP版本時，只有當來源磁碟區的版本高於目標磁碟區的版本時，您才可以在不同節點上的磁碟區之間移動 LUN。例如，如果來源磁碟區的節點運行的是ONTAP 9.15.1，而目標磁碟區的節點執行的是ONTAP 9.16.1，則您無法移動 LUN。您可以在執行相同ONTAP版本的節點上的磁碟區之間移動 LUN。

對於1 TB或更大的Solaris OS類型LUN、主機在LUN移動期間可能會發生逾時。對於此類型的LUN、您應該先卸載LUN、然後再開始移動。

範例 **18.** 步驟

系統管理員

使用ONTAP NetApp System Manager（9.7及更新版本）搬移LUN。

從ONTAP 《事物》9.10.1開始、您可以在移動單一LUN時、使用System Manager建立新的Volume。 在《支援資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表：更新資料表。ONTAP

步驟

1. 在System Manager中、按一下* Storage（儲存設備）>LUN*。
2. 在您要移動的 LUN 上按一下滑鼠右鍵、然後按一下 ⋮ 並選取 * 移動 LUN* 。

   在《S209.10.1》中、選取以將LUN移至*現有Volume *或*新Volume *。ONTAP

   如果您選擇建立新的Volume、請提供Volume規格。

3. 按一下*移動*。

CLI

使用ONTAP NetApp CLI移動LUN。

1. 移動LUN：

   ```
   lun move start
   ```

   在極短的期間內、LUN會顯示在來源和目的地磁碟區上。這是預期的做法、並在行動完成後予以解決。

2. 追蹤移動狀態並確認成功完成：

   ```
   lun move show
   ```

相關資訊

- "選擇性LUN對應"

刪除**LUN**

如果不再需要LUN、您可以從儲存虛擬機器（SVM）刪除LUN。

開始之前

必須先從其igroup取消對應LUN、才能將其刪除。

步驟

1. 確認應用程式或主機未使用LUN。
2. 從igroup取消對應LUN：

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<LUN_name> -igroup <igroup_name>
```

3. 刪除 LUN ：

```
lun delete -vserver <SVM_name> -volume <volume_name> -lun <LUN_name>
```

4. 確認您已刪除 LUN ：

```
lun show -vserver <SVM_name>
```

```
Vserver   Path              State    Mapped  Type     Size
--------- ----------------- -------- ------- -------- ------
vs5       /vol/vol16/lun8   online   mapped  windows  10.00GB
```

複製**LUN**之前須知

在複製LUN之前、您應該注意某些事項。

叢集管理員可以使用、在叢集中的儲存虛擬機器（ SVM ）之間複製 LUN `lun copy` 命令。叢集管理員必須使用建立儲存虛擬機器（ SVM ）對等關係 `vserver peer create` 執行跨 SVM LUN 複製作業之前的命令。來源磁碟區中必須有足夠空間可用於SIS複製。

快照中的 LUN 可作為命令的來源 LUN `lun copy` 。當您使用命令複製 LUN `lun copy` 時， LUN 複本會立即可供讀寫存取。建立LUN複本後、來源LUN將維持不變。來源LUN和LUN複本均以不同LUN序號的唯一LUN形式存在。對來源LUN所做的變更不會反映在LUN複本中、而對LUN複本所做的變更不會反映在來源LUN中。來源LUN的LUN對應不會複製到新的LUN；必須對應LUN複本。

透過快照進行資料保護時，資料會在磁碟區層級執行。因此、如果您將LUN複製到與來源LUN磁碟區不同的磁碟區、則目的地LUN將受目的地磁碟區的資料保護方案所管制。如果您沒有為目的地磁碟區建立快照，則不會建立 LUN 複本的快照。

複製LUN是不中斷營運的作業。

您無法複製下列類型的LUN：

- 已從檔案建立的LUN
- 處於NVFIL狀態的LUN
- 處於負載共享關係中的LUN

- 傳輸協定端點類別LUN

如"指令參考資料ONTAP"需詳細 `lun copy`資訊，請參閱。

檢查**LUN**的已設定和已用空間

瞭解LUN所使用的已設定空間和實際空間、有助於判斷空間回收時可回收的空間量、包含資料的保留空間量、以及配置的總大小與LUN實際使用的大小。

步驟

1. 檢視已設定空間與LUN實際使用空間：

   ```
   lun show
   ```

   以下範例顯示VS3儲存虛擬機器（SVM）中LUN使用的空間與實際空間的設定空間：

   ```
   lun show -vserver vs3 -fields path, size, size-used, space-reserve
   ```

   ```
   vserver path                    size    space-reserve size-used
   ------- ------------------      ------- ------------- ---------
   vs3     /vol/vol0/lun1          50.01GB disabled      25.00GB
   vs3     /vol/vol0/lun1_backup   50.01GB disabled      32.15GB
   vs3     /vol/vol0/lun2          75.00GB disabled      0B
   vs3     /vol/volspace/lun0      5.00GB  enabled       4.50GB
   4 entries were displayed.
   ```

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

使用**Storage QoS**控制及監控**LUN**的**I/O**效能

您可以將LUN指派給Storage QoS原則群組、藉此控制LUN的輸入/輸出（I/O）效能。您可以控制I/O效能、確保工作負載達到特定的效能目標、或是調節對其他工作負載造成負面影響的工作負載。

關於這項工作

原則群組會強制執行最大處理量限制（例如100 MB/s）。您可以建立原則群組而不指定最大處理量、以便在控制工作負載之前監控效能。

您也可以將FlexVol 含有VMware磁碟區和LUN的儲存虛擬機器（SVM）指派給原則群組。

請注意下列有關將LUN指派給原則群組的需求：

- LUN必須由原則群組所屬的SVM所包含。

  您可以在建立原則群組時指定SVM。

- 如果您將LUN指派給原則群組、則無法將包含Volume或SVM的LUN指派給原則群組。

如需如何使用Storage QoS的詳細資訊、請參閱 "系統管理參考資料"。

步驟

1. 使用 `qos policy-group create` 建立原則群組的命令。

   如"指令參考資料ONTAP"需詳細 `qos policy-group create`資訊，請參閱。

2. 使用 `lun create` 命令或 `lun modify` 命令 `-qos-policy-group` 將 LUN 指派給原則群組的參數。

   如"指令參考資料ONTAP"需詳細 `lun`資訊，請參閱。

3. 使用 `qos statistics` 檢視效能資料的命令。
4. 如有必要、請使用 `qos policy-group modify` 命令來調整原則群組的最大處理量限制。

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

可有效監控**LUN**的工具

我們提供各種工具、協助您有效監控LUN、避免空間不足。

- 利用免費工具、您可以管理環境中所有叢集的所有儲存設備。Active IQ Unified Manager
- System Manager是ONTAP 內建於支援功能的圖形化使用者介面、可讓您在叢集層級手動管理儲存需求。
- 支援以單一檢視方式顯示儲存基礎架構、並可讓您設定自動監控、警示及報告LUN、磁碟區及集合體的儲存空間不足的時間。OnCommand Insight

轉換**LUN**的功能與限制

在SAN環境中、將7-Mode Volume移轉至ONTAP VMware時、需要中斷服務。您需要關閉主機才能完成轉換。轉換完成後、您必須先更新主機組態、才能開始ONTAP 在VMware中提供資料

您需要排定維護時間、以便關閉主機並完成轉換。

LUN已從Data ONTAP 以7-Mode運作的VMware移轉至ONTAP 支援VMware的功能和限制、會影響LUN的管理方式。

您可以使用轉換的LUN執行下列作業：

- 使用檢視 LUN `lun show` 命令
- 使用檢視從 7-Mode 磁碟區轉換的 LUN 庫存 `transition 7-mode show` 命令
- 從 7-Mode 快照還原磁碟區

  還原磁碟區會轉換快照中擷取的所有 LUN

- 使用命令從 7-Mode 快照還原單一 LUN `snapshot restore-file`
- 在 7-Mode 快照中建立 LUN 的複本
- 從 7-Mode 快照中擷取的 LUN 還原一系列區塊

- 使用 7-Mode 快照建立磁碟區的 FlexClone

您無法對轉換的LUN執行下列動作：

- 存取磁碟區中擷取的快照備份 LUN 複本

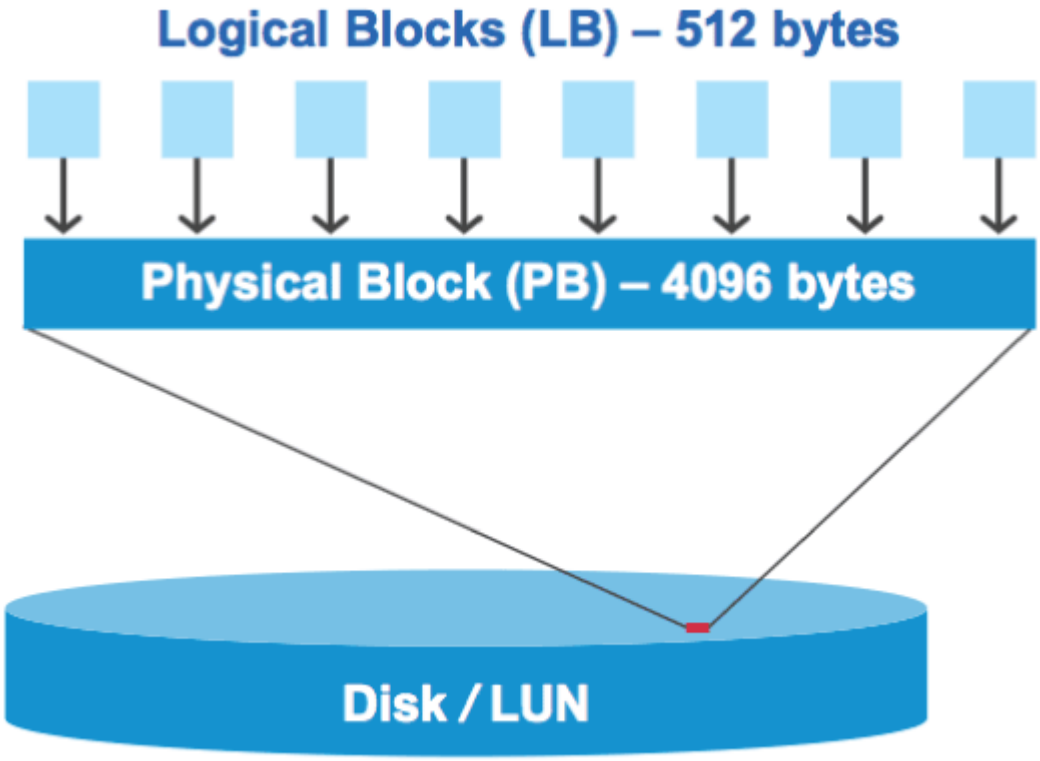
相關資訊

- "複本型轉換"
- "LUN顯示"

正確對齊**LUN**的**I/O**不一致概觀

可能會在正確對齊的LUN上報告I/O不一致。ONTAP一般而言、只要您確信LUN已正確配置且分割表正確無誤、就可以忽略這些錯誤對齊警告。

LUN和硬碟均以區塊形式提供儲存設備。由於主機上磁碟的區塊大小為512位元組、因此LUN會向主機顯示該大小的區塊、而實際上是使用較大的4-KB區塊來儲存資料。主機使用的512位元組資料區塊稱為邏輯區塊。LUN用來儲存資料的4-KB資料區塊稱為實體區塊。這表示每個4-KB實體區塊中有八個512位元組的邏輯區塊。



主機作業系統可在任何邏輯區塊開始讀取或寫入I/O作業。只有在實體區塊的第一個邏輯區塊開始時、才會將I/O作業視為已對齊。如果I/O作業是從邏輯區塊開始、而邏輯區塊並非實體區塊的開頭、則I/O會被視為未對齊。自動偵測錯誤對齊、並在LUN上報告。ONTAP然而、I/O不一致的存在並不一定代表LUN也未對齊。可能會在正確對齊的LUN上報告未對齊的I/O。

如果您需要進一步調查，請參閱"NetApp知識庫：如何辨識 LUN 上未對齊的 IO？"

如需修正對齊問題的工具相關資訊、請參閱下列文件：+

- "Windows Unified Host Utilities 7.1"
- "配置 SAN 儲存文件"

使用**LUN OS**類型實現**I/O**對齊

對於 ONTAP 9.7 或更早版本、您應該使用建議的 ONTAP LUN `ostype` 最符合您作業系統的值、以符合您的作業系統分割配置、達到 I/O 一致性。

主機作業系統所採用的分割區配置是造成I/O錯誤的主要因素。某些 ONTAP LUN `ostype` 值使用特殊偏移值「前置字元」來啟用主機作業系統所使用的預設分割配置。

在某些情況下、可能需要使用自訂的分割表來達成I/O對齊。不過、對於 `ostype` 值大於 "`prefix'" 的值 `0`，自訂分割區可能會產生未對齊的 I/O

有關在ONTAP 9.7 或更早版本中配置的 LUN 的更多信息，請參見"NetApp知識庫：如何辨識 LUN 上未對齊的IO"。

根據預設、在 ONTAP 9.8 或更新版本中配置的新 LUN 、其前置碼和後置碼大小為零、適用於所有 LUN OS 類型。依預設、 I/O 應與支援的主機作業系統一致。

Linux的特殊**I/O**對齊考量

Linux發行版本提供多種方式來使用LUN、包括做為資料庫、各種Volume Manager和檔案系統的原始裝置。當用作原始設備或邏輯Volume中的實體Volume時、不需要在LUN上建立分割區。

對於RHEL 5及更早版本、以及SLES 10及更早版本、如果不使用Volume Manager、您應該將LUN分割成一個以對齊偏移開始的分割區、亦即八個邏輯區塊中的一個甚至多個區段。

Solaris LUN的特殊**I/O**對齊考量

在決定是否應該使用時、您需要考量各種因素 `solaris` ostype 或 `solaris_efi` ostype 。

請參閱 "《Solaris主機公用程式安裝與管理指南》" 以取得詳細資訊。

ESX開機**LUN**報告未對齊

用作ESX開機LUN的LUN通常會以ONTAP 未對齊的方式回報。ESX會在開機LUN上建立多個分割區、因此很難對齊。未對齊的ESX開機LUN通常不是效能問題、因為未對齊的I/O總容量很小。假設 LUN 已與 VMware 正確配置 `ostype`、不需採取任何行動。

相關資訊

"適用於VMware vSphere、其他虛擬環境和NetApp儲存系統的客體VM檔案系統分割區/磁碟對齊"

解決**LUN**離線問題的方法

當沒有空間可供寫入時、LUN會離線以保留資料完整性。LUN空間不足、可能會因為各種原因而離線、您可以透過多種方法來解決此問題。

如果...	您可以...
Aggregate已滿	• 新增更多磁碟。 • 使用 `volume modify` 用於壓縮具有可用空間的磁碟區的命令。 • 如果您有可用空間的空間保證磁碟區、請將磁碟區空間保證變更為 `none` 使用 `volume modify` 命令。
Volume已滿、但包含的Aggregate中有可用空間	• 如需空間保證磁碟區、請使用 `volume modify` 命令來增加磁碟區大小。 • 對於精簡配置的磁碟區、請使用 `volume modify` 命令以增加磁碟區的最大大小。 如果未啟用 Volume 自動擴充、請使用 `volume modify -autogrow-mode` 以啟用它。 • 使用命令手動刪除快照，或使用 `volume snapshot autodelete modify`命令自動刪除 `volume snapshot delete`快照。

相關資訊

"磁碟與本機層（Aggregate）管理"

"邏輯儲存管理"

疑難排解主機上看不到的**iSCSI LUN**

iSCSI LUN在主機上顯示為本機磁碟。如果儲存系統LUN無法作為主機上的磁碟使用、您應該確認組態設定。

組態設定	處理方式
纜線	確認主機與儲存系統之間的纜線已正確連接。
網路連線能力	驗證主機與儲存系統之間是否有TCP/IP連線。 • 從儲存系統命令列ping用於iSCSI的主機介面： `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`* • 從主機命令列ping用於iSCSI的儲存系統介面： `ping -node` *`node_name`* `-destination` *`host_ip_address_for_iSCSI`*

組態設定	處理方式
系統需求	確認組態的元件符合資格。此外、請確認您擁有正確的主機作業系統（OS）Service Pack層級、啟動器版本、ONTAP 版本、以及其他系統需求。互通性對照表包含最新的系統需求。
巨型框架	如果您在組態中使用巨型框架、請確認網路路徑中的所有裝置都已啟用巨型框架：主機乙太網路NIC、儲存系統及任何交換器。
iSCSI服務狀態	確認iSCSI服務已獲得授權、並已在儲存系統上啟動。
啟動器登入	確認啟動器已登入儲存系統。如果是 `iscsi initiator show` 命令輸出顯示沒有啟動器登入、請檢查主機上的啟動器組態。此外、請確認儲存系統已設定為啟動器的目標。
iSCSI節點名稱（IQN）	確認您在igroup組態中使用正確的啟動器節點名稱。在主機上、您可以使用啟動器工具和命令來顯示啟動器節點名稱。在igroup和主機上設定的啟動器節點名稱必須相符。
LUN對應	確認LUN已對應至igroup。在儲存系統主控台上、您可以使用下列其中一個命令： • `lun mapping show` 顯示所有 LUN 及其對應的 igroup 。 • `lun mapping show -igroup` 顯示對應至特定 igroup 的 LUN 。
iSCSI LIF已啟用	確認iSCSI邏輯介面已啟用。

相關資訊

- "NetApp 互通性對照表工具"
- "LUN對應顯示"

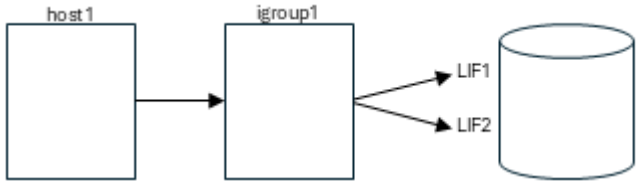
管理igroup和portSet

使用連接埠集和**igroup**來限制**LUN**存取的方法

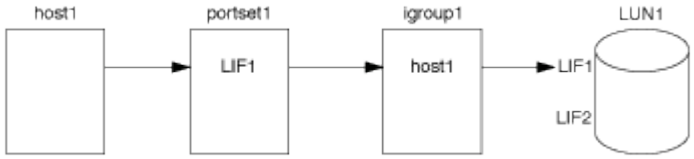
除了使用選擇性LUN對應（SLM）之外、您也可以透過igroup和portSet來限制對LUN的存取。

PortSet可與SLA搭配使用、進一步限制特定目標對特定啟動器的存取。當使用具有連接埠集的SLM, LUN將可在擁有LUN的節點及該節點的HA合作夥伴的連接埠集中的一組lifs上存取。

在下列範例中，host1 沒有連接埠集。如果沒有連接埠集，主機 1 可以透過 LIF1 和 LIF2 存取 LUN1。



您可以使用連接埠集來限制對 LUN1 的存取。在下列範例中，主機 1 只能透過 LIF1 存取 LUN1。但是，主機 1 無法透過 LIF2 存取 LUN1，因為 LIF2 不在連接埠集 1 中。



相關資訊

- 選擇性LUN對應
- 建立連接埠集並繫結至igroup

檢視及管理**SAN**啟動器和群組

您可以使用System Manager來檢視及管理啟動器群組（igroup）和啟動器。

關於這項工作

- 啟動器群組會識別哪些主機可以存取儲存系統上的特定LUN。
- 建立啟動器和啟動器群組之後、您也可以編輯或刪除它們。
- 若要管理SAN啟動器群組和啟動器、您可以執行下列工作：
  - [view-manage-san-igroups]
  - [view-manage-san-inits]

檢視及管理**SAN**啟動器群組

您可以使用System Manager檢視啟動器群組（igroup）清單。從清單中、您可以執行其他作業。

步驟

1. 在System Manager中、按一下*主機> SAN啟動器群組*。

   此頁面會顯示啟動器群組（igroup）清單。如果清單很大、您可以按一下頁面右下角的頁碼來檢視清單的其他頁面。

   這些欄會顯示有關階層的各種資訊。從9.11.1開始、也會顯示igroup的連線狀態。將游標暫留在狀態警示上以檢視詳細資料。

2. （選用）：按一下清單右上角的圖示、即可執行下列工作：
   - 搜尋
   - *下載*清單。
   - *顯示*或*隱藏*欄位。
   - *篩選*清單中的資料。
3. 您可以從清單執行作業：
   - 按一下 + Add 以新增群組。
   - 按一下igroup名稱以檢視* Overview *頁面、其中顯示igroup的詳細資料。

在「總覽」頁面上、您可以檢視與igroup相關聯的LUN、也可以啟動建立LUN及對應LUN的作業。按一下「所有**SAN**啟動器」以返回主清單。

- 將游標移至 igroup 上方、然後按一下 ⋮ igroup 名稱旁的以編輯或刪除 igroup 。
- 將游標暫留在igroup名稱左側的區域上、然後勾選核取方塊。如果您按一下「**+**新增至啟動器群組」、您可以將該igroup新增至其他igroup。
- 在* Storage VM*欄中、按一下儲存VM的名稱以檢視其詳細資料。

檢視及管理**SAN**啟動器

您可以使用System Manager來檢視啟動器清單。從清單中、您可以執行其他作業。

步驟

1. 在System Manager中、按一下*主機> SAN啟動器群組*。

   此頁面會顯示啟動器群組（igroup）清單。

2. 若要檢視啟動器、請執行下列步驟：

   - 按一下「* FC啟動器*」索引標籤以檢視FC啟動器清單。
   - 按一下「* iSCSI啟動器*」索引標籤以檢視iSCSI啟動器清單。

     這些欄會顯示啟動器的各種資訊。

   從9.11.1開始、也會顯示啟動器的連線狀態。將游標暫留在狀態警示上以檢視詳細資料。

3. （選用）：按一下清單右上角的圖示、即可執行下列工作：
   - *搜尋*特定啟動器的清單。
   - *下載*清單。
   - *顯示*或*隱藏*欄位。
   - *篩選*清單中的資料。

建立巢狀 **igroup**

從ONTAP 《支援範圍》9.9.1開始、您可以建立一個由其他現有igroup所組成的igroup。

1. 在System Manager中、按一下*主機> SAN啟動器群組*、然後按一下*新增*。
2. 輸入igroup * Name*和* Description*。

   此說明可做為igroup別名。

3. 選擇* Storage VM*和* Host作業系統*。

   建立igroup之後、無法變更巢狀igroup的OS類型。

4. 在*啟動器群組成員*下、選取*現有的啟動器群組*。

您可以使用*搜尋*來尋找並選取您要新增的啟動器群組。

將igroup對應至多個LUN

從功能支援的9.9開始、您可以將igroup同時對應到兩個以上的LUN。ONTAP

1. 在System Manager中、按一下* Storage > LUN*。
2. 選取您要對應的LUN。
3. 按一下*更多*、然後按一下*對應至啟動器群組*。

選取的igroup會新增至選取的LUN。不會覆寫先前存在的對應。

建立連接埠集並繫結至igroup

除了使用以外 "選擇性LUN對應（SLM)"，您可以建立連接埠集並將連接埠集繫結至igroup，以進一步限制啟動器可用來存取LUN的LIF。

如果您未將連接埠集繫結至igroup、則igroup中的所有啟動器都可以透過擁有LUN的節點上的所有LIF及所屬節點的HA合作夥伴來存取對應的LUN。

開始之前

您必須至少有一個LIF和一個igroup。

除非您使用介面群組、否則建議將兩個生命段用於iSCSI和FC的備援。建議介面群組只使用一個LIF。

關於這項工作

當節點上有兩個以上的生命期、而且您想將特定啟動器限制在某個生命期的子集時、將連接埠集與SLMs搭配使用是很有利的。如果沒有連接埠集、則所有擁有LUN的節點和擁有節點HA合作夥伴、能夠存取LUN的啟動器、都能存取節點上的所有目標。

範例 **19.** 步驟

系統管理員

從ONTAP 《Sys9.10.1》開始、您可以使用System Manager來建立連接埠集、並將其連結至igroup。

如果您需要建立連接埠集、並將其連結ONTAP 至版本低於9.10.1的版本中的igroup、您必須使用ONTAP 該CLI程序。

從 ONTAP 9.12.1 開始，如果您沒有現有連接埠集，則必須使用 ONTAP CLI 程序建立第一個連接埠集。

1. 在System Manager中、按一下「網路>總覽> **Portset**」、然後按一下「新增」。
2. 輸入新連接埠集的資訊、然後按一下「新增」。
3. 按一下*主機> SAN啟動器群組*。
4. 若要將連接埠集繫結至新的igroup、請按一下「新增」。

   若要將連接埠集繫結至現有的 igroup 、請選取 igroup 、按一下、然後按一 ⋮ 下 * 編輯啟動器群組 * 。

相關資訊

"檢視及管理啟動器和igroup"

CLI

1. 建立包含適當lifs的連接埠集：

   ```
   portset create -vserver vserver_name -portset portset_name -protocol
   protocol -port-name port_name
   ```

   如果您使用的是 FC 、請指定 `protocol` 參數為 `fcp`。如果您使用的是 iSCSI 、請指定 `protocol` 參數為 `iscsi`。

2. 將igroup繫結至連接埠集：

   ```
   lun igroup bind -vserver vserver_name -igroup igroup_name -portset
   portset_name
   ```

   如"指令參考資料ONTAP"需詳細 `lun igroup bind`資訊，請參閱。

3. 驗證連接埠集和LIF是否正確：

   ```
   portset show -vserver vserver_name
   ```

   ```
   Vserver   Portset   Protocol Port Names    Igroups
   --------- --------- -------- ------------ --------
   vs3       portset0  iscsi    lif0,lif1    igroup1
   ```

管理連接埠集

此外 "選擇性LUN對應（SLM)"，您可以使用連接埠集來進一步限制啟動器存取LUN時可以使用哪些lifs。

從ONTAP 《銷售資訊》9.10.1開始、您可以使用System Manager來變更與連接埠集相關的網路介面、以及刪除連接埠集。

變更與連接埠集相關的網路介面

1. 在 System Manager 中、選取 * 網路 > 總覽 > Portsets* 。
2. 選擇要編輯的端口集，然後選擇 * 編輯端口集 * 。

刪除連接埠集

1. 在System Manager中、按一下* Network > Overview > PortSet*。
2. 若要刪除單一連接埠集、請選取連接埠集、然後選取 * 刪除連接埠集 * 。

   若要刪除多個連接埠集、請選取連接埠集、然後按一下*刪除*。

選擇性**LUN**對應總覽

選擇性LUN對應（SLM）可減少從主機到LUN的路徑數量。使用SLM,當建立新的LUN對應時,只能透過擁有LUN及其HA合作夥伴的節點上的路徑來存取LUN。

在每個主機上、可管理單一igroup、也可支援不中斷營運的LUN移動作業、不需要處理連接埠集或重新對應LUN。

"PortSets" 可與 SLM 搭配使用、進一步限制特定目標對特定啟動器的存取。當使用具有連接埠集的SLM, LUN將可在擁有LUN的節點及該節點的HA合作夥伴的連接埠集中的一組lifs上存取。

在所有新LUN對應上、預設會啟用「SLM"。

確定是否在**LUN**對應上啟用了「**SLA**」

如果您的環境中有在 ONTAP 9 版本中建立的 LUN 組合、以及從舊版轉換而來的 LUN 、您可能需要判斷特定 LUN 上是否已啟用選擇性 LUN 對應（ SLM ）。

您可以使用的輸出中顯示的資訊 `lun mapping show -fields reporting-nodes, node` 命令以判斷是否已在 LUN 對應上啟用 SLM 。如果未啟用 SLM 、命令輸出的「移轉節點」欄下方的儲存格中會顯示「 - 」。如果啓用了 SLM ，則在“移植節點”列中顯示在“節點”列下的節點列表將重複出現。

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

修改「**SLM-**報告節點」清單

如果您要將LUN或包含LUN的磁碟區移至同一個叢集內的另一個高可用度（HA）配對、則在開始移動之前、應先修改選擇性LUN對應（SLM）報告節點清單、以確保維持作用中、最佳化的LUN路徑。

步驟

1. 將目的地節點及其合作夥伴節點新增至Aggregate或Volume的報告節點清單：

```
lun mapping add-reporting-nodes -vserver <vserver_name> -path <lun_path>
-igroup <igroup_name> [-destination-aggregate <aggregate_name>|-
destination-volume <volume_name>]
```

如果您有一致的命名慣例，則可以使用而非來同時修改多個 LUN 對應 `igroup_prefix* igroup_name`。

2. 重新掃描主機以探索新增的路徑。
3. 如果您的作業系統需要它、請將新路徑新增至多重路徑網路I/O（MPIO）組態。
4. 執行所需移動作業的命令、並等待作業完成。
5. 確認I/O是透過主動/最佳化路徑進行服務：

```
lun mapping show -fields reporting-nodes
```

6. 從報告節點清單中移除先前的LUN擁有者及其合作夥伴節點：

```
lun mapping remove-reporting-nodes -vserver <vserver_name> -path
<lun_path> -igroup <igroup_name> -remote-nodes
```

7. 驗證LUN是否已從現有LUN對應中移除：

```
lun mapping show -fields reporting-nodes
```

8. 移除主機作業系統的任何過時裝置項目。
9. 如有必要、請變更任何多重路徑組態檔。
10. 重新掃描主機以驗證是否移除舊路徑。+
如需重新掃描主機的特定步驟、請參閱主機文件。

管理iSCSI傳輸協定

設定您的網路以獲得最佳效能

乙太網路的效能差異極大。您可以選取特定組態值、將用於iSCSI的網路效能最大化。

步驟

1. 將主機和儲存連接埠連接至同一個網路。

   最好連線至相同的交換器。不應使用路由。

2. 選取可用的最高速度連接埠、並將其專用於iSCSI。

10 GbE連接埠是最佳選擇。1 GbE連接埠為最低值。

3. 停用所有連接埠的乙太網路流量控制。

   您應該會看到 "網路管理" 用於使用CLI設定乙太網路連接埠流量控制。

4. 啟用巨型框架（通常為9000的MTU）。

   資料路徑中的所有裝置、包括啟動器、目標和交換器、都必須支援巨型框架。否則、啟用巨型框架實際上會大幅降低網路效能。

設定**SVM for iSCSI**

若要設定iSCSI的儲存虛擬機器（SVM）、您必須為SVM建立生命期、並將iSCSI傳輸協定指派給這些生命期。

關於這項工作

每個使用iSCSI傳輸協定處理資料的SVM、每個節點至少需要一個iSCSI LIF。為了提供備援、您應該在每個節點上建立至少兩個生命期。

範例 **20.** 步驟

系統管理員

使用ONTAP NetApp System Manager（9.7及更新版本）設定iSCSI儲存VM。

在新的儲存**VM**上設定**iSCSI**	在現有儲存**VM**上設定**iSCSI**
1. 在System Manager中、按一下* Storage > Storage VM*、然後按一下* Add*。 2. 輸入儲存VM的名稱。 3. 選擇* iSCSI 作為*存取傳輸協定。 4. 按一下「啟用**iSCSI**」、然後輸入網路介面的IP位址和子網路遮罩。 +每個節點至少應有兩個網路介面。 5. 按一下「 * 儲存 * 」。	1. 在System Manager中、按一下* Storage > Storage VM*。 2. 按一下您要設定的儲存VM。 3. 按一下 * 設定 * 索引標籤、然後按一下 iSCSI 傳輸協定旁的。 4. 按一下「啟用**iSCSI**」、然後輸入網路介面的IP位址和子網路遮罩。 +每個節點至少應有兩個網路介面。 5. 按一下「 * 儲存 * 」。

CLI

使用ONTAP CLI設定iSCSI的儲存VM。

1. 讓SVM聆聽iSCSI流量：

   ```
   vserver iscsi create -vserver vserver_name -target-alias vserver_name
   ```

2. 在每個節點上建立要用於iSCSI的SVM LIF：

   - 適用於32、9.6及更新版本：ONTAP

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol iscsi -service-policy default-data-iscsi -home-node node_name
     -home-port port_name -address ip_address -netmask netmask
     ```

   - 適用於更新版本的版本：ONTAP

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol iscsi -home-node node_name -home-port port_name -address
     ip_address -netmask netmask
     ```

3. 請確認您已正確設定lifs：

   ```
   network interface show -vserver vserver_name
   ```

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

4. 確認iSCSI已啟動並正在執行、以及該SVM的目標IQN：

   ```
   vserver iscsi show -vserver vserver_name
   ```

5. 從您的主機建立iSCSI工作階段至您的生命期。

相關資訊

- "NetApp 技術報告 4080 ：現代 SAN 的最佳實務做法"

定義啟動器的安全性原則方法

您可以定義啟動器及其驗證方法的清單。您也可以修改適用於未使用者定義驗證方法之啟動器的預設驗證方法。

關於這項工作

您可以使用產品中的安全原則演算法來產生獨特的密碼、也可以手動指定您要使用的密碼。

並非所有的啟動器都支援十六進位CHAP密碼。

步驟

1. 使用 `vserver iscsi security create` 命令以建立啟動器的安全性原則方法。

   ```
   vserver iscsi security create -vserver vs2 -initiator iqn.1991-
   05.com.microsoft:host1 -auth-type CHAP -user-name bob1 -outbound-user-name
   bob2
   ```

2. 依照螢幕命令新增密碼。

   為啟動器iqn.1991-05.com.microsoft:host1建立安全性原則方法、其中包含傳入和傳出的CHAP使用者名稱和密碼。

相關資訊

- iSCSI驗證的運作方式
- CHAP 驗證

刪除**SVM**的**iSCSI**服務

如果不再需要、您可以刪除儲存虛擬機器（SVM）的iSCSI服務。

開始之前

在刪除iSCSI服務之前、iSCSI服務的管理狀態必須為「直接」狀態。您可以使用將管理狀態移至向下 `vserver iscsi modify` 命令。

步驟

1. 使用 `vserver iscsi modify` 停止 I/O 至 LUN 的命令。

   ```
   vserver iscsi modify -vserver vs1 -status-admin down
   ```

2. 使用 `vserver iscsi delete` 從 SVM 移除 iSCSI 服務的命令。

   ```
   vserver iscsi delete -vserver vs_1
   ```

3. 使用 `vserver iscsi show command` 確認您已從 SVM 刪除 iSCSI 服務。

```
vserver iscsi show -vserver vs1
```

取得更多**iSCSI**工作階段錯誤還原的詳細資料

提高iSCSI工作階段錯誤還原層級可讓您接收更多有關iSCSI錯誤還原的詳細資訊。使用較高的錯誤恢復層級可能會稍微降低iSCSI工作階段效能。

關於這項工作

根據預設、ONTAP 針對iSCSI工作階段設定使用錯誤恢復層級0。如果您使用的啟動器已符合錯誤恢復層級1或2的資格、您可以選擇增加錯誤恢復層級。修改後的工作階段錯誤還原層級只會影響新建立的工作階段、不會影響現有的工作階段。

從 ONTAP 9.4 開始 `max-error-recovery-level` 中不支援選項 `iscsi show` 和 `iscsi modify` 命令。

步驟

1. 進入進階模式：

   ```
   set -privilege advanced
   ```

2. 使用驗證目前的設定 `iscsi show` 命令。

   ```
   iscsi show -vserver vs3 -fields max-error-recovery-level
   ```

   ```
   vserver max-error-recovery-level
   ------- ------------------------
   vs3     0
   ```

3. 使用變更錯誤恢復層級 `iscsi modify` 命令。

   ```
   iscsi modify -vserver vs3 -max-error-recovery-level 2
   ```

向**ISSVM**伺服器登錄**SVM**

您可以使用 `vserver iscsi isns` 設定儲存虛擬機器（ SVM ）以向 iSNS 伺服器登錄的命令。

關於這項工作

。 `vserver iscsi isns create` 命令可設定 SVM 以向 iSNS 伺服器註冊。SVM不提供可讓您設定或管理iSNS伺服器的命令。若要管理iSNS伺服器、您可以使用伺服器管理工具、或是廠商為iSNS伺服器提供的介面。

步驟

1. 在您的iSNS伺服器上、確定您的iSNS服務已啟動且可供服務使用。
2. 在資料連接埠上建立SVM管理LIF：

   ```
   network interface create -vserver SVM_name -lif lif_name -role data -data
   -protocol none -home-node home_node_name -home-port home_port -address
   ```

IP_address -netmask *network_mask*

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

3. 在SVM上建立iSCSI服務（如果尚未存在）：

   `vserver iscsi create -vserver *SVM_name*`

4. 確認iSCSI服務已成功建立：

   `iscsi show -vserver *SVM_name*`

5. 驗證SVM是否存在預設路由：

   `network route show -vserver *SVM_name*`

6. 如果SVM不存在預設路由、請建立預設路由：

   `network route create -vserver *SVM_name* -destination *destination* -gateway *gateway*`

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

7. 設定SVM以註冊至iSNS服務：

   `vserver iscsi isns create -vserver *SVM_name* -address *IP_address*`

   同時支援IPv4和IPv6位址系列。iSNS伺服器的位址系列必須與SVM管理LIF的位址系列相同。

   例如、您無法將具有IPV4位址的ANSVM管理LIF連線至具有IPv6位址的iSNS伺服器。

8. 驗證iSNS服務是否正在執行：

   `vserver iscsi isns show -vserver *SVM_name*`

9. 如果未執行iSNS服務、請啟動它：

   `vserver iscsi isns start -vserver *SVM_name*`

解決儲存系統上的**iSCSI**錯誤訊息

您可以使用檢視許多與 iSCSI 相關的常見錯誤訊息 `event log show` 命令。您需要知道這些訊息的意義、以及如何解決這些訊息所識別的問題。

下表包含最常見的錯誤訊息、以及解決問題的指示：

訊息	說明	處理方式
`ISCSI: network interface identifier disabled for use; incoming connection discarded`	介面上未啟用iSCSI服務。	您可以使用 `iscsi interface enable` 用於在介面上啟用 iSCSI 服務的命令。例如： `iscsi interface enable -vserver vs1 -lif lif1`
`ISCSI: Authentication failed for initiator nodename`	未針對指定的啟動器正確設定CHAP。	您應該檢查CHAP設定；您無法在儲存系統上使用相同的使用者名稱和密碼來進行傳入和傳出設定： • 儲存系統上的傳入認證資料必須與啟動器上的傳出認證資料相符。 • 儲存系統上的傳出認證資料必須與啟動器上的傳入認證資料相符。

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

啟用或停用自動 **iSCSI LIF** 容錯移轉

升級至 ONTAP 9.11.1 或更新版本後、您應該手動在 ONTAP 9.10.1 或更新版本中建立的所有 iSCSI 生命體上啟用自動 LIF 容錯移轉。

從 ONTAP 9.11.1 開始、您可以在 All Flash SAN Array 平台上、為 iSCSI 生命週期啟用自動 LIF 容錯移轉。如果發生儲存設備容錯移轉、 iSCSI LIF 會自動從其主節點或連接埠移轉至其 HA 合作夥伴節點或連接埠、然後在容錯移轉完成後再移回。 或者、如果 iSCSI LIF 連接埠變得不正常、 LIF 會自動移轉至目前主節點的健全連接埠、然後在連接埠再次正常運作後、再移回原始連接埠。 可讓在 iSCSI 上執行的 SAN 工作負載在發生容錯移轉後更快恢復 I/O 服務。

在 ONTAP 9.11.1 及更新版本中、如果符合下列其中一項條件、則預設會針對自動 LIF 容錯移轉啟用新建立的 iSCSI 生命體：

- SVM 上沒有 iSCSI 生命
- SVM 上的所有 iSCSI 生命都已啟用、可自動進行 LIF 容錯移轉

啟用自動 **iSCSI LIF** 容錯移轉

根據預設、在 ONTAP 9.10.1 及更早版本中建立的 iSCSI 生命權不會啟用自動 LIF 容錯移轉。 如果 SVM 上的 iSCSI 生命期未啟用自動 LIF 容錯移轉、則新建立的生命期也不會啟用自動 LIF 容錯移轉。 如果未啟用自動 LIF 容錯移轉、且發生容錯移轉事件、則 iSCSI 生命將不會移轉。

深入瞭解 "LIF 容錯移轉與恢復"。

步驟

1. 啟用 iSCSI LIF 的自動容錯移轉：

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy sfo-partner-only -auto-revert true
```

若要更新 SVM 上的所有 iSCSI 生命期、請使用 `-lif*` 而非 `lif`。

停用自動 **iSCSI LIF** 容錯移轉

如果您先前已在 ONTAP 9.10.1 或更早版本所建立的 iSCSI 生命負載上啟用自動 iSCSI LIF 容錯移轉、您可以選擇將其停用。

步驟

1. 停用 iSCSI LIF 的自動容錯移轉：

```
network interface modify -vserver <SVM_name> -lif <iscsi_lif> -failover
-policy disabled -auto-revert false
```

若要更新 SVM 上的所有 iSCSI 生命期、請使用 `-lif*` 而非 `lif`。

相關資訊

- "建立LIF"
- 手動 "移轉 LIF"
- 手動 "將 LIF 還原至其主連接埠"
- "在LIF上設定容錯移轉設定"

管理**FC**傳輸協定

設定**SVM for FC**

若要設定FC的儲存虛擬機器（SVM）、您必須為SVM建立生命期、並將FC傳輸協定指派給這些生命期。

開始之前

您必須擁有 FC 許可證（"隨附於 ONTAP One"），並且必須啓用該許可證。如果未啟用 FC 授權、則生命體與 SVM 會顯示為線上、但作業狀態為 `down`。您必須啟用FC服務、才能讓您的LIF和SVM正常運作。您必須為SVM中的所有FC LIF使用單一啟動器分區、才能裝載啟動器。

關於這項工作

NetApp為每個以FC傳輸協定提供資料的SVM、每個節點至少支援一個FC LIF。 每個節點必須使用兩個LIF和兩個Fabric、每個節點必須附加一個LIF。這可在節點層和網路上提供備援功能。

範例 **21.** 步驟

系統管理員

使用ONTAP NetApp System Manager（9.7及更新版本）設定iSCSI儲存VM。

在新的儲存**VM**上設定**FC**	在現有的儲存**VM**上設定**FC**
1. 在System Manager中、按一下* Storage > Storage VM*、然後按一下* Add*。 2. 輸入儲存VM的名稱。 3. 選擇* FC*作為*存取傳輸協定*。 4. 按一下 * 啟用 FC* 。 + FC連接埠會自動指派。 5. 按一下「 * 儲存 * 」 。	1. 在System Manager中、按一下* Storage > Storage VM*。 2. 按一下您要設定的儲存VM。 3. 按一下 * 設定 * 標籤、然後按一下 FC 傳輸協定旁的。 4. 按一下「啟用**FC**」、然後輸入網路介面的IP位址和子網路遮罩。 + FC連接埠會自動指派。 5. 按一下「 * 儲存 * 」 。

CLI

1. 在SVM上啟用FC服務：

   ```
   vserver fcp create -vserver vserver_name -status-admin up
   ```

2. 在每個服務FC的節點上為SVM建立兩個生命期：

   - 適用於32、9.6及更新版本：ONTAP

     ```
     network interface create -vserver vserver_name -lif lif_name -data
     -protocol fcp -service-policy default-data-fcp -home-node node_name
     -home-port port_name -address ip_address -netmask netmask -status-admin
     up
     ```

   - 適用於更新版本的版本：ONTAP

     ```
     network interface create -vserver vserver_name -lif lif_name -role data
     -data-protocol fcp -home-node node_name -home-port port
     ```

3. 確認您的生命已建立、且其操作狀態為 `online`：

   ```
   network interface show -vserver vserver_name lif_name
   ```

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

相關資訊

- "NetApp支援"
- "NetApp 互通性對照表工具"
- 叢集SAN環境中的LIF考量

刪除**SVM**的**FC**服務

您可以刪除不再需要的儲存虛擬機器（SVM）FC服務。

開始之前

在刪除SVM的FC服務之前、管理狀態必須為「直接」。您可以使用將管理狀態設為「關閉」 `vserver fcp modify` 命令或 `vserver fcp stop` 命令。

步驟

1. 使用 `vserver fcp stop` 停止 I/O 至 LUN 的命令。

   ```
   vserver fcp stop -vserver vs_1
   ```

2. 使用 `vserver fcp delete` 從 SVM 移除服務的命令。

   ```
   vserver fcp delete -vserver vs_1
   ```

3. 使用 `vserver fcp show` 若要確認您已從 SVM 刪除 FC 服務：

   ```
   vserver fcp show -vserver vs_1
   ```

FCoE巨型框架的建議**MTU**組態

對於乙太網路光纖通道（FCoE）、CNA乙太網路介面卡部分的巨型框架應設定為9000 MTU。CNA FCoE介面卡部分的巨型框架應設定為1500 MTU以上。只有在啟動器、目標和所有介入交換器支援並設定為使用巨型框架時、才設定巨型框架。

管理**NVMe**傳輸協定

啟動**SVM**的**NVMe**服務

在儲存虛擬機器（SVM）上使用NVMe傳輸協定之前、您必須先在SVM上啟動NVMe服務。

開始之前

您的系統必須允許NVMe做為傳輸協定。

支援下列NVMe傳輸協定：

傳輸協定	開始於…	允許者…
TCP	零點9.10.1 ONTAP	預設
FCP	ONTAP 9.4	預設

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 驗證NVMe是否可做為傳輸協定：

   ```
   vserver nvme show
   ```

3. 建立NVMe傳輸協定服務：

   ```
   vserver nvme create
   ```

4. 在SVM上啟動NVMe傳輸協定服務：

   ```
   vserver nvme modify -status -admin up
   ```

從**SVM**刪除**NVMe**服務

如有需要、您可以從儲存虛擬機器（SVM）刪除NVMe服務。

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 停止SVM上的NVMe服務：

   ```
   vserver nvme modify -status -admin down
   ```

3. 刪除NVMe服務：

   ```
   vserver nvme delete
   ```

調整命名空間大小

從ONTAP 版本號《支援》（2019）9.10.1開始、您可以使用ONTAP 支援的CLI來增加或減少NVMe命名空間的大小。您可以使用System Manager來增加NVMe命名空間的大小。

增加命名空間的大小

系統管理員

1. 按一下「儲存設備**> NVMe**命名空間」。
2. 在您要增加的命名空間上按一下，然後按一 ⋮ 下 **Edit** 。
3. 在* capaciam*下、變更命名空間的大小。

CLI

1. 輸入下列命令： `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `-size` *`new_size_of_namespace`*

減少命名空間的大小

您必須使用ONTAP NVMe-CLI來減少NVMe命名空間的大小。

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 減少命名空間的大小：

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

將命名空間轉換成**LUN**

從 ONTAP 9.11.1 開始、您可以使用 ONTAP CLI 將現有的 NVMe 命名空間就地轉換為 LUN 。

開始之前

- 指定的NVMe命名空間不應有任何現有的子系統對應。
- 命名空間不應是Snapshot的一部分、也不應是SnapMirror關係的目的地端、做為唯讀命名空間。
- 由於NVMe命名空間僅支援特定平台和網路卡、因此此功能僅適用於特定硬體。

步驟

1. 輸入下列命令、將 NVMe 命名空間轉換為 LUN ：

   ```
   lun convert-from-namespace -vserver -namespace-path
   ```

   如"指令參考資料ONTAP"需詳細 `lun convert-from-namespace`資訊，請參閱。

透過 **NVMe** 設定頻內驗證

從 ONTAP 9.12.1 開始、您可以使用 ONTAP 命令列介面（ CLI ）、透過 NVMe / TCP 和 NVMe / FC 傳輸協定、使用 DH-HMAC-CHAP 驗證、在 NVMe 主機和控制器之間設定頻內（安全）雙向和單向驗證。從 ONTAP 9.14.1 開始、可在系統管理員中設定頻內驗證。

若要設定頻內驗證、每個主機或控制器都必須與 DH-HMAC-CHAP 金鑰相關聯、此金鑰是 NVMe 主機或控制器的 NQN 組合、以及系統管理員所設定的驗證密碼。若要讓 NVMe 主機或控制器驗證其對等端點、它必須知道與對等端點相關的金鑰。

在單向驗證中、會為主機設定秘密金鑰、但不會為控制器設定。在雙向驗證中、會為主機和控制器設定秘密金鑰。

SHA-256 是預設的雜湊功能、 2048 位元是預設的 DH 群組。

系統管理員

從 ONTAP 9.14.1 開始、您可以使用系統管理員來設定頻內驗證、同時建立或更新 NVMe 子系統、建立或複製 NVMe 命名空間、或使用新的 NVMe 命名空間來新增一致性群組。

步驟

1. 在 System Manager 中、按一下 * 主機 > NVMe Subsystem* 、然後按一下 * 新增 * 。
2. 新增 NVMe 子系統名稱、然後選取儲存 VM 和主機作業系統。
3. 輸入主機 NQN 。
4. 選取主機 NQN 旁的 * 使用頻內驗證 * 。
5. 提供主機密碼和控制器密碼。

   DH-HMAC-CHAP 金鑰是 NVMe 主機或控制器的 NQN 組合、也是系統管理員設定的驗證密碼。

6. 為每個主機選取偏好的雜湊功能和 DH 群組。

   如果您未選取雜湊函數和 DH 群組、則 SHA-256 會指派為預設雜湊函數、而 2048 位元會指派為預設的 DH 群組。

7. 或者、按一下 * 新增 * 、並視需要重複步驟以新增更多主機。
8. 按一下「 * 儲存 * 」。
9. 若要確認已啟用頻內驗證、請按一下 * 系統管理員 > 主機 > NVMe 子系統 > Grid > Peek view* 。

   主機名稱旁的透明金鑰圖示表示已啟用單向模式。主機名稱旁的不透明金鑰表示已啟用雙向模式。

CLI

步驟

1. 將DH-HMAP-CHAP驗證新增至NVMe子系統：

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host add`資訊，請參閱。

2. 確認DH-HMAC CHAP驗證傳輸協定已新增至您的主機：

   ```
   vserver nvme subsystem host show
   ```

```
  [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
  [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
  [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host show`資訊，請參閱。

3. 確認DH-HMAC CHAP驗證是在NVMe控制器建立期間執行：

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

相關資訊

- "vserver nvme 子系統控制器顯示"

停用 **NVMe** 的頻內驗證

如果您已使用 DH-HMAC-CHAP 在 NVMe 上設定頻內驗證、您可以選擇隨時停用。

如果您要從 ONTAP 9.12.1 或更新版本還原至 ONTAP 9.12.0 或更新版本、則必須先停用頻內驗證、才能還原。如果未停用使用 DH-HMAC-CHAP 的頻內驗證、還原將會失敗。

步驟

1. 從子系統移除主機、以停用DH-HMAP-CHAP驗證：

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. 確認DH-HMAP-CHAP驗證傳輸協定已從主機移除：

```
vserver nvme subsystem host show
```

3. 無需驗證即可將主機重新新增回子系統：

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

為 **NVMe / TCP** 設定 **TLS** 安全通道

從ONTAP 9.16.1 開始，您可以為 NVMe/TCP 連線設定 TLS 安全通道。您可以使用系統管理員或ONTAP CLI 新增啟用了 TLS 的新 NVMe 子系統，或為現有的 NVMe 子系統啟用 TLS。ONTAP不支援 TLS 硬體卸載。

系統管理員

從 ONTAP 9 開始。 16.1 開始，您可以使用系統管理員來設定 NVMe / TCP 連線的 TLS ，同時建立或更新 NVMe 子系統，建立或複製 NVMe 命名空間，或使用新的 NVMe 命名空間來新增一致性群組。

步驟

1. 在 System Manager 中、按一下 * 主機 > NVMe Subsystem* 、然後按一下 * 新增 * 。
2. 新增 NVMe 子系統名稱、然後選取儲存 VM 和主機作業系統。
3. 輸入主機 NQN 。
4. 選取主機 NQN 旁的 * 需要傳輸層安全性（ TLS ） * 。
5. 提供預先共用金鑰（ PSK ）。
6. 按一下「 * 儲存 * 」。
7. 若要確認 TLS 安全通道已啟用，請選取 * 系統管理員 > 主機 > NVMe 子系統 > Grid > Peek view* 。

CLI

步驟

1. 新增支援 TLS 安全通道的 NVMe 子系統主機。您可以使用 `tls-configured-psk`爭論：

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. 確認 NVMe 子系統主機已設定為 TLS 安全通道。您可以選擇性地使用 `tls-key-type`引數僅顯示使用該金鑰類型的主機：

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. 確認 NVMe 子系統主機控制器已設定為 TLS 安全通道。您可以選擇性地使用任何 `tls-key-type`， `tls-identity`或 `tls-cipher`引數來僅顯示具有這些 TLS 屬性的控制器：

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

相關資訊

- "Vserver NVMe 子系統"

停用 **NVMe / TCP** 的 **TLS** 安全通道

從 ONTAP 9 。 16.1 開始，您可以為 NVMe / TCP 連線設定 TLS 安全通道。如果您已為 NVMe / TCP 連線設定 TLS 安全通道，您可以選擇隨時停用它。

步驟

1. 從子系統移除主機以停用 TLS 安全通道：

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. 確認已從主機移除 TLS 安全通道：

```
vserver nvme subsystem host show
```

3. 將主機新增回沒有 TLS 安全通道的子系統：

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

相關資訊

- "Vserver NVMe 子系統主機"

變更 **NVMe** 主機優先順序

從 ONTAP 9.14.1 開始、您可以設定 NVMe 子系統、以優先分配特定主機的資源。根據預設、當主機新增至子系統時、會將其指派為一般優先順序。指派高優先順序的主機會分配較大的 I/O 佇列數和佇列深度。

您可以使用 ONTAP 命令列介面（ CLI ）手動將預設優先順序從一般變更為高。 若要變更指派給主機的優先順序、您必須從子系統移除主機、然後將其重新新增。

步驟

1. 確認主機優先順序設定為一般：

```
vserver nvme show-host-priority
```

   如"指令參考資料ONTAP"需詳細 `vserver nvme show-host-priority`資訊，請參閱。

2. 從子系統中移除主機：

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host remove`資訊，請參閱。

3. 確認主機已從子系統中移除：

```
vserver nvme subsystem host show
```

如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host show`資訊，請參閱。

4. 將主機新增回具有高優先順序的子系統：

```
vserver nvme subsystem host add -vserver <SVM_name> -subsystem
<subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
-priority high
```

如"指令參考資料ONTAP"需詳細 `vserver nvme subsystem host add`資訊，請參閱。

在 **ONTAP** 中管理 **NVMe / TCP** 控制器的自動主機探索

從 ONTAP 9.14.1 開始，在 IP 架構中，使用 NVMe / TCP 傳輸協定的控制器主機探索會依預設自動執行。

啟用 **NVMe / TCP** 控制器的自動主機探索

如果您先前已停用自動主機探索、但您的需求已變更、則可以重新啟用。

步驟

1. 進入進階權限模式：

```
set -privilege advanced
```

2. 啟用自動探索：

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. 確認已啟用 NVMe / TCP 控制器的自動探索。

```
vserver nvme show -fields mdns-service-discovery-enabled
```

停用 NVMe / TCP 控制器的自動主機探索

如果您不需要主機自動探索 NVMe / TCP 控制器、也不需要偵測到網路上的多點傳送流量、則應該停用此功能。

步驟

1. 進入進階權限模式：

```
set -privilege advanced
```

2. 停用自動探索：

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. 確認已停用 NVMe / TCP 控制器的自動探索。

```
vserver nvme show -fields mdns-service-discovery-enabled
```

在 ONTAP 中停用 NVMe 主機虛擬機器識別碼

從 ONTAP 9.14.1 開始， ONTAP 預設支援 NVMe / FC 主機透過唯一識別碼識別虛擬機器，以及針對 NVMe / FC 主機監控虛擬機器資源使用率的能力。這可強化主機端報告和疑難排解。

您可以使用 bootarg 來停用此功能。查看"NetApp知識庫：如何在ONTAP中停用 NVMe 主機虛擬機器識別符"。

使用FC介面卡管理系統

使用FC介面卡管理系統

可使用命令來管理內建的FC介面卡和FC介面卡。這些命令可用來設定介面卡模式、顯示介面卡資訊、以及變更速度。

大多數儲存系統都有板載 FC 適配器，可以配置為啟動器或目標。您也可以使用配置為啟動器或目標的 FC 適配器。啟動器連接到後端磁碟架，並可能連接到外部儲存陣列。目標僅連接到 FC 交換器。 FC 目標 HBA 連接埠和交換器連接埠速度都應設定為相同的值，而不應設定為自動。

相關資訊

"SAN 組態"

用於管理FC介面卡的命令

您可以使用FC命令來管理儲存控制器的FC目標介面卡、FC啟動器介面卡和內建FC介面卡。相同的命令也用於管理FC傳輸協定和FC-NVMe傳輸協定的FC介面卡。

FC啟動器介面卡命令只能在節點層級運作。您必須使用 `run -node node_name` 使用 FC 啟動器介面卡命令之前的命令。

用於管理**FC**目標介面卡的命令

如果您想要...	使用此命令...
在節點上顯示FC介面卡資訊	`network fcp adapter show`
修改FC目標介面卡參數	`network fcp adapter modify`
顯示FC傳輸協定流量資訊	`run -node node_name sysstat -f`
顯示FC傳輸協定已執行多久	`run -node node_name uptime`
顯示介面卡組態與狀態	`run -node node_name sysconfig -v adapter`
驗證安裝了哪些擴充卡、以及是否有任何組態錯誤	`run -node node_name sysconfig -ac`
查看命令的手冊頁	`man <command_name>`

用於管理**FC**啟動器介面卡的命令

如果您想要...	使用此命令...
顯示節點中所有啟動器及其介面卡的資訊	`run -node node_name storage show adapter`
顯示介面卡組態與狀態	`run -node node_name sysconfig -v adapter`
驗證安裝了哪些擴充卡、以及是否有任何組態錯誤	`run -node node_name sysconfig -ac`

用於管理內建**FC**介面卡的命令

如果您想要...	使用此命令...
顯示內建FC連接埠的狀態	`run -node node_name system hardware unified-connect show`

相關資訊

- "網路 FCP 介面卡"

設定**FC**介面卡

每個內建FC連接埠都可個別設定為啟動器或目標。某些FC介面卡上的連接埠也可以個別設定為目標連接埠或啟動器連接埠、就像內建FC連接埠一樣。可設定為目標模式的介面卡清單可在中取得 "NetApp Hardware Universe"。

目標模式用於將連接埠連接到 FC 啟動器。啟動器模式用於將連接埠連接到磁帶磁碟機、磁帶庫或具有外部 LUN 匯入 (FLI) 功能的第三方儲存。

在設定FC傳輸協定和FC-NVMe傳輸協定的FC介面卡時、也會使用相同的步驟。不過、只有某些FC介面卡支援FC-NVMe。請參閱 "NetApp Hardware Universe" 以取得支援FC-NVMe傳輸協定的介面卡清單。

將**FC**介面卡設定為目標模式

步驟

1. 使介面卡離線：

   ```
   node run -node node_name storage disable adapter adapter_name
   ```

   如果介面卡未離線、您也可以從系統上適當的介面卡連接埠拔下纜線。

2. 將介面卡從啟動器變更為目標：

   ```
   system hardware unified-connect modify -t target -node node_name adapter
   adapter_name
   ```

3. 重新啟動裝載您所變更介面卡的節點。
4. 驗證目標連接埠的組態是否正確：

   ```
   network fcp adapter show -node node_name
   ```

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

5. 將介面卡上線：

   ```
   network fcp adapter modify -node node_name -adapter adapter_port -state up
   ```

將**FC**介面卡設定為啟動器模式

開始之前

- 介面卡上的LIF必須從其成員所在的任何連接埠集中移除。
- 使用要修改之實體連接埠的所有儲存虛擬機器（SVM）LIF、必須先移轉或銷毀、才能將實體連接埠的特性從目標變更為啟動器。

NVMe / FC支援啟動器模式。

步驟

1. 移除介面卡上的所有LIF：

```
network interface delete -vserver SVM_name -lif LIF_name,LIF_name
```

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

2. 讓介面卡離線：

```
network fcp adapter modify -node node_name -adapter adapter_port -status-admin down
```

如果介面卡未離線、您也可以從系統上適當的介面卡連接埠拔下纜線。

3. 將介面卡從目標變更為啟動器：

```
system hardware unified-connect modify -t initiator adapter_port
```

4. 重新啟動裝載您所變更介面卡的節點。
5. 驗證FC連接埠的組態設定是否正確：

```
system hardware unified-connect show
```

6. 將介面卡重新連線：

```
node run -node node_name storage enable adapter adapter_port
```

檢視介面卡設定

您可以使用特定命令來檢視您的FC/UTA介面卡相關資訊。

FC目標介面卡

步驟

1. 使用 `network fcp adapter show` 顯示介面卡資訊的命令： `network fcp adapter show -instance -node node1 -adapter 0a`

輸出會顯示所使用之每個插槽的系統組態資訊和介面卡資訊。

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

統一化目標介面卡（**UTA**）**X1143A-R6**

步驟

1. 在不連接纜線的情況下啟動控制器。
2. 執行 `system hardware unified-connect show` 命令查看連接埠組態和模組。
3. 在設定CNA和連接埠之前、請先檢視連接埠資訊。

將**UTA2**連接埠從**CNA**模式變更為**FC**模式

您應該將UTA2連接埠從「融合式網路介面卡」（CNA）模式變更為「光纖通道」（FC）

模式、以支援FC啟動器和FC目標模式。當您需要變更連接埠與網路的實體媒體時、應該將特性設定從CNA模式變更為FC模式。

步驟

1. 使介面卡離線：

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin down`

2. 變更連接埠模式：

   `ucadmin modify -node node_name -adapter adapter_name -mode fcp`

3. 重新啟動節點、然後將介面卡上線：

   `network fcp adapter modify -node node_name -adapter adapter_name -status-admin up`

4. 請通知您的管理員或VIF管理程式、視情況刪除或移除連接埠：

   - 如果連接埠作為LIF的主連接埠、介面群組（ifgrp）或主機VLAN的成員、則管理員應執行下列動作：

     i. 移動LIF、從ifgrp移除連接埠、或分別刪除VLAN。

     ii. 執行以手動刪除連接埠 `network port delete` 命令。

     如果是 `network port delete` 命令失敗、系統管理員應解決錯誤、然後再次執行命令。

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

   - 如果連接埠不是LIF的主連接埠、不是ifgrp的成員、也不是主控VLAN、則VIF管理程式應在重新開機時從記錄中移除連接埠。

     如果 VIF 管理程式未移除連接埠、則管理員必須在重新開機後使用手動移除連接埠 `network port delete` 命令。

```
net-f8040-34::> network port show

    Node: net-f8040-34-01
                                                            Speed(Mbps)
Health
    Port      IPspace      Broadcast Domain Link MTU  Admin/Oper
Status
    --------- ------------ ---------------- ---- ---- -----------
--------
    ...
    e0i       Default      Default          down 1500  auto/10    -
    e0f       Default      Default          down 1500  auto/10    -
    ...
```

```
    net-f8040-34::> ucadmin show
                               Current  Current    Pending  Pending
Admin
    Node            Adapter   Mode     Type       Mode     Type
Status
    ------------    -------   -------  ---------  -------  ---------
-----------
    net-f8040-34-01   0e       cna      target     -        -
offline
    net-f8040-34-01   0f       cna      target     -        -
offline
    ...

    net-f8040-34::> network interface create -vs net-f8040-34 -lif m
-role
node-mgmt-home-node net-f8040-34-01 -home-port e0e -address 10.1.1.1
-netmask 255.255.255.0


    net-f8040-34::> network interface show -fields home-port, curr-
port

    vserver lif                    home-port curr-port
    ------- ---------------------- --------- ---------
    Cluster net-f8040-34-01_clus1 e0a       e0a
    Cluster net-f8040-34-01_clus2 e0b       e0b
    Cluster net-f8040-34-01_clus3 e0c       e0c
    Cluster net-f8040-34-01_clus4 e0d       e0d
    net-f8040-34
            cluster_mgmt           e0M       e0M
    net-f8040-34
            m                      e0e       e0i
    net-f8040-34
            net-f8040-34-01_mgmt1 e0M       e0M
    7 entries were displayed.

    net-f8040-34::> ucadmin modify local 0e fc

    Warning: Mode on adapter 0e and also adapter 0f will be changed
to fc.
    Do you want to continue? {y|n}: y
    Any changes will take effect after rebooting the system. Use the
"system node reboot" command to reboot.

    net-f8040-34::> reboot local
      (system node reboot)
```

```
Warning: Are you sure you want to reboot node "net-f8040-34-01"?
{y|n}: y
```

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

5. 確認您已安裝正確的SFP+：

   `network fcp adapter show -instance -node -adapter`

   對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該先使用8 GB SFP或16 GB SFP、再變更節點上的組態。

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

相關資訊

- "網路介面"

變更**CNA/UTA2**目標介面卡光纖模組

您應該變更統一化目標介面卡（CNA/UTA2）上的光學模組、以支援您為介面卡選取的特性設定模式。

步驟

1. 驗證卡中使用的目前SFP+。接著、將目前的SFP+替換為適當的SFP+、以符合偏好的特性設定（FC或CNA）。
2. 從X1143A-R6介面卡移除目前的光纖模組。
3. 針對您偏好的個人化模式（FC或CNA）光纖插入正確的模組。
4. 確認您已安裝正確的SFP+：

   `network fcp adapter show -instance -node -adapter`

   支援的SFP+模組和Cisco品牌銅線（雙軸纜線）均列於_SES__中Hardware Universe 。

相關資訊

- "NetApp Hardware Universe"
- "顯示網路FCP介面卡"

支援的**X1143A-R6**介面卡連接埠組態

FC目標模式是X1143A-R6介面卡連接埠的預設組態。不過、此介面卡上的連接埠可以設定為10-Gb乙太網路和FCoE連接埠、也可以設定為16-Gb FC連接埠。

當X1143A-R6介面卡設定為乙太網路和FCoE時、可在相同的10-GbE連接埠上支援並行NIC和FCoE目標流量。如果設定為FC、則可針對FC目標或FC啟動器模式個別設定每個共用相同ASIC的雙埠配對。這表示單一X1143A-R6介面卡可在一個雙埠配對上支援FC目標模式、在另一個雙埠配對上支援FC啟動器模式。

相關資訊

"NetApp Hardware Universe"

"SAN 組態"

設定連接埠

若要設定統一化目標介面卡（X1143A-R6）、您必須在相同的特性設定模式下、在同一個晶片上設定兩個鄰近的連接埠。

步驟

1. 使用設定光纖通道（ FC ）或融合式網路介面卡（ CNA ）所需的連接埠 `system node hardware unified-connect modify` 命令。
2. 連接FC或10 Gb乙太網路適用的纜線。
3. 確認您已安裝正確的SFP+：

   ```
   network fcp adapter show -instance -node -adapter
   ```

   對於CNA、您應該使用10Gb乙太網路SFP。對於FC、您應該使用8 GB SFP或16 GB SFP、視所連接的FC架構而定。

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

使用**X1133A-R6**介面卡時、請避免連線中斷

您可以使用備援路徑將系統設定為獨立的X1133A-R6 HBA、以避免在連接埠故障時中斷連線。

X1133A-R6 HBA是一個4埠、16 GB FC介面卡、由兩個2埠配對組成。X1133A-R6介面卡可設定為目標模式或啟動器模式。每個2埠配對都由單一ASIC支援（例如、ASIC 1上的連接埠1和連接埠2、ASIC 2上的連接埠3和連接埠4）。單一ASIC上的兩個連接埠都必須設定為以相同模式運作、無論是目標模式或啟動器模式。如果ASIC支援配對時發生錯誤、配對中的兩個連接埠都會離線。

為了避免這種連線中斷、您可以設定系統的備援路徑來分隔X1133A-R6 HBA、或是使用備援路徑來連接至HBA上不同的ASIC所支援的連接埠。

管理所有**SAN**傳輸協定的生命量

管理所有**SAN**傳輸協定的生命量

啟動器必須使用多重路徑 I/O （ MPIO ）和非對稱式邏輯單元存取（ ALUA ）、才能在 SAN 環境中為叢集提供容錯移轉功能。如果某個節點發生故障、則lifs不會移轉或假設故障的合作夥伴節點IP位址。而在主機上使用ALUA的MPIO軟體則負責選取適當的路徑、以便透過LIF存取LUN。

您需要使用邏輯介面（lifs）、從HA配對中的每個節點建立一或多個iSCSI路徑、以便存取由HA配對服務的LUN。 您應該為每個支援SAN的儲存虛擬機器（SVM）設定一個管理LIF。

支援直接連線或使用乙太網路交換器進行連線。您必須為這兩種連線類型建立生命。

- 您應該為每個支援SAN的儲存虛擬機器（SVM）設定一個管理LIF。
  您可以為每個節點設定兩個生命期、每個節點一個用於FC的網路、另一個用於iSCSI的乙太網路。

建立生命體後、即可從連接埠集移除生命體、移至儲存虛擬機器（ SVM ）內的不同節點、並刪除生命體。

相關資訊

- "設定生命總覽"
- "建立LIF"

在 **ONTAP** 中設定 **NVMe LIF**

設定NVMe LIF時、必須符合特定需求。

開始之前

NVMe必須受您建立LIF的FC介面卡支援。中列出支援的介面卡 "Hardware Universe"。

關於這項工作

從 ONTAP 9.12.1 及更新版本開始，您最多可在 12 個節點上，為每個節點設定兩個 NVMe 生命週期。在 ONTAP 9.11.1 及更早版本中、您最多可以在兩個節點上、為每個節點設定兩個 NVMe 生命期。

建立NVMe LIF時適用下列規則：

- NVMe可以是資料生命里的唯一資料傳輸協定。
- 您應該為每個支援SAN的SVM設定一個管理LIF。
- 對於 ONTAP 9.5 或更新版本、您必須在包含命名空間的節點和節點的 HA 合作夥伴上設定 NVMe LIF 。
- 僅適用於下列項目：ONTAP
  - NVMe LIF和命名空間必須裝載在同一個節點上。
  - 每個SVM只能設定一個NVMe資料LIF。

步驟

1. 建立LIF：

```
network interface create -vserver <SVM_name> -lif <LIF_name> -role
<LIF_role> -data-protocol {fc-nvme|nvme-tcp} -home-node <home_node>
-home-port <home_port>
```

   NVMe / TCP 可從 ONTAP 9.10.1 及更新版本開始使用。

2. 確認LIF已建立：

```
network interface show -vserver <SVM_name>
```

建立之後、 NVMe / TCP 生命會在連接埠 8009 上聆聽探索。

相關資訊

- "網路介面"

移轉**SAN LIF**之前的須知事項

只有在變更叢集內容（例如將節點新增至叢集或從叢集刪除節點）時、才需要執行LIF移動。如果您執行LIF移動、就不需要在叢集的附加主機和新的目標介面之間重新分區FC架構或建立新的iSCSI工作階段。

您無法使用移動 SAN LIF `network interface move` 命令。若要執行SAN LIF移動、必須將LIF離線、將LIF移至不同的主節點或連接埠、然後將其重新連線至新位置。非對稱邏輯單元存取（ALUA）提供備援路徑和自動路徑選擇、是ONTAP 任何一套SAN解決方案的一部分。因此、當LIF離線進行移動時、不會中斷I/O。主機只需重試、然後將I/O移至另一個LIF。

使用LIF移動、您可以在不中斷營運的情況下執行下列動作：

- 以對存取LUN資料的主機而言透明的方式、以升級的HA配對取代叢集的一對HA
- 升級目標介面卡
- 將儲存虛擬機器（SVM）的資源從叢集中的一組節點移至叢集中的另一組節點

從連接埠集移除**SAN LIF**

如果您要刪除或移動的LIF位於連接埠集中、則必須先從連接埠集中移除LIF、才能刪除或移動LIF。

關於這項工作

只有在連接埠集中有一個LIF時、才需要執行下列程序中的步驟1。如果連接埠集繫結至啟動器群組、則無法移除連接埠集中的最後一個LIF。否則、如果連接埠集內有多個LIF、您可以從步驟2開始。

步驟

1. 如果連接埠集中只有一個 LIF 、請使用 `lun igroup unbind` 從啟動器群組解除連接埠集的命令。

   當您從連接埠集解除啟動器群組的連結時、啟動器群組中的所有啟動器都能存取所有對應至所有網路介面上啟動器群組的所有目標LUN。

   ```
   cluster1::>lun igroup unbind -vserver vs1 -igroup ig1
   ```

   如"指令參考資料ONTAP"需詳細 `lun igroup unbind`資訊，請參閱。

2. 使用 `lun portset remove` 從連接埠集移除 LIF 的命令。

   ```
   cluster1::> port set remove -vserver vs1 -portset ps1 -port-name lif1
   ```

   如"指令參考資料ONTAP"需詳細 `lun portset remove`資訊，請參閱。

移動**SAN LIF**

如果節點需要離線、您可以移動SAN LIF來保留其組態資訊（例如WWPN）、並避免重新

分區交換器架構。由於SAN LIF必須在移動之前離線、因此主機流量必須仰賴主機多重路徑軟體、才能提供不中斷營運的LUN存取。您可以將SAN LIF移至叢集中的任何節點、但無法在儲存虛擬機器（SVM）之間移動SAN LIF。

開始之前

如果LIF是連接埠集的成員、則LIF必須已從連接埠集移除、才能將LIF移至其他節點。

關於這項工作

您要移動之LIF的目的地節點和實體連接埠必須位於相同的FC架構或乙太網路上。如果您將LIF移至尚未適當分區的其他Fabric、或將LIF移至iSCSI啟動器與目標之間沒有連線的乙太網路網路、則當您將LUN重新連線時、LUN將無法存取。

步驟

1. 檢視LIF的管理和作業狀態：

   `network interface show -vserver vserver_name`

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

2. 將 LIF 的狀態變更為 `down` （離線）：

   `network interface modify -vserver vserver_name -lif LIF_name -status-admin down`

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

3. 為LIF指派新的節點和連接埠：

   `network interface modify -vserver vserver_name -lif LIF_name -home-node node_name -home-port port_name`

4. 將 LIF 的狀態變更為 `up` （線上）：

   `network interface modify -vserver vserver_name -lif LIF_name -status-admin up`

   如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。

5. 驗證您的變更：

   `network interface show -vserver vserver_name`

刪除**SAN**環境中的**LIF**

在刪除LIF之前、您應確保連線至LIF的主機可以透過其他路徑存取LUN。

開始之前

如果您要刪除的LIF是連接埠集的成員、則必須先從連接埠集移除LIF、才能刪除LIF。

系統管理員

使用ONTAP 「不含更新版本的系統管理程式」刪除LIF（9.7及更新版本）。

步驟

1. 在System Manager中、按一下*網路>總覽*、然後選取*網路介面*。
2. 選取您要從中刪除LIF的儲存VM。
3. 按一下 ⋮ 並選取 * 刪除 * 。

CLI

使用ONTAP NetApp CLI刪除LIF。

步驟

1. 確認要刪除的LIF和目前連接埠名稱：

   ```
   network interface show -vserver vserver_name
   ```

2. 刪除LIF：

   ```
   network interface delete

   network interface delete -vserver vs1 -lif lif1
   ```

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

3. 確認您已刪除LIF：

   ```
   network interface show

   network interface show -vserver vs1
   ```

   ```
   Logical  Status     Network                       Current   Current Is
   Vserver  Interface  Admin/Oper Address/Mask       Node      Port
   Home
   -------  ---------- ---------- ----------------- --------- -------
   ----
   vs1
            lif2       up/up      192.168.2.72/24   node-01   e0b
   true
            lif3       up/up      192.168.2.73/24   node-01   e0b
   true
   ```

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

將節點新增至叢集的SAN LIF需求

將節點新增至叢集時、您必須注意某些考量事項。

- 在新節點上建立LUN之前、您必須視需要在新節點上建立LIF。
- 您必須依照主機堆疊和傳輸協定的規定、從主機探索這些生命點。
- 您必須在新節點上建立LIF、以便在不使用叢集互連網路的情況下、能夠進行LUN和磁碟區移動。

設定iSCSI LIF、將FQDN傳回主機iSCSI SendTargets探索作業

從ONTAP 功能支援功能支援的版本開始、iSCSI LIF可設定為在主機作業系統傳送iSCSI SendTargets探索作業時、傳回完整網域名稱（FQDN）。當主機OS與儲存服務之間有網路位址轉譯（NAT）裝置時、傳回FQDN很有用。

關於這項工作

NAT裝置一端的IP位址在另一端毫無意義、但FQDN在兩端都具有意義。

所有主機作業系統上的FQDN值互通性限制為128個字元。

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 設定iSCSI LIF以傳回FQDN：

   ```
   vserver iscsi interface modify -vserver SVM_name -lif iscsi_LIF_name
   -sendtargets_fqdn FQDN
   ```

   在下列範例中、iSCSI LIF設定為傳回storagehost-005.example.com做為FQDN。

   ```
   vserver iscsi interface modify -vserver vs1 -lif vs1_iscsi1 -sendtargets-fqdn
   storagehost-005.example.com
   ```

3. 驗證sendTarget是否為FQDN：

   ```
   vserver iscsi interface show -vserver SVM_name -fields sendtargets-fqdn
   ```

   在此範例中、storagehost-005.example.com會顯示在「endtargets-FQDN」輸出欄位中。

   ```
   cluster::vserver*> vserver iscsi interface show -vserver vs1 -fields
   sendtargets-fqdn
   vserver lif         sendtargets-fqdn
   ------- ----------- ---------------------------
   vs1     vs1_iscsi1 storagehost-005.example.com
   vs1     vs1_iscsi2 storagehost-006.example.com
   ```

相關資訊

"指令參考資料ONTAP"

啟用 SAN 通訊協定的 ONTAP 空間分配

ONTAP 空間分配可協助您防止 LUN 或 NVMe 命名空間用盡時離線，並讓 SAN 主機回收空間。

ONTAP 對空間分配的支援是根據您的 SAN 傳輸協定和 ONTAP 版本而定。從 ONTAP 9.16.1 開始，預設會針對新建立的 LUN 和所有命名空間，啟用 iSCSI ， FC 和 NVMe 通訊協定的空間分配。

版本ONTAP	通訊協定	空間分配是 ...
9.16.1 或更新版本	• iSCSI • FC • NVMe	預設會針對新建立的 LUN 和所有命名空間啟用
9.15.1..	• iSCSI • FC	預設會啟用新建立的 LUN
	NVMe	不支援
9.14.1 及更早版本	• iSCSI • FC	對於新建立的 LUN ，預設為停用
	NVMe	不支援

啟用空間分配時：

- 如果 LUN 或命名空間用盡， ONTAP 會與主機通訊，表示沒有可用的空間可用於寫入作業。因此， LUN 或命名空間仍保持在線上狀態，讀取作業仍會繼續提供服務。視主機組態而定，主機會重試寫入作業，直到成功或主機檔案系統離線為止。當 LUN 或命名空間有額外可用空間時，寫入作業就會恢復。

  如果未啟用空間分配，當 LUN 或命名空間用盡時，所有 I/O 作業都會失敗， LUN 或命名空間會離線；必須解決空間問題，才能恢復正常作業。主機上也可能需要重新掃描 LUN 裝置、才能將路徑和裝置還原至作業狀態。

- 主機可以執行 SCSI 或 NVMe `UNMAP` （有時稱為 `TRIM`）作業。取消對應作業可讓主機識別不再需要的資料區塊，因為這些區塊不再包含有效資料。識別通常發生在檔案刪除之後。然後、儲存系統就可以取消分配這些資料區塊、以便在其他地方使用這些空間。這種分配方式可大幅提升整體儲存效率、尤其是在資料週轉率高的檔案系統方面。

開始之前

啟用空間分配需要主機組態、以便在無法完成寫入時正確處理空間分配錯誤。若要使用 SCSI 或 NVMe `UNMAP` ，則需要使用符合 SCSI SBC-3 標準定義的邏輯區塊資源配置。

當您啟用空間分配時，下列主機目前支援精簡配置：

- Citrix XenServer 6.5及更新版本

- VMware ESXi 5.0 及更新版本
- Oracle Linux 6.2 UEK 核心及更新版本
- Red Hat Enterprise Linux 6.2及更新版本
- SUSE Linux Enterprise Server 11 及更新版本
- Solaris 11.1 及更新版本
- Windows

關於這項工作

當您將叢集升級至 ONTAP 9 · 15.1 或更新版本時，無論主機類型為何，在軟體升級之前建立的所有 LUN 的空間分配設定在升級後都會保持不變。例如、如果在 ONTAP 9.13.1 中為停用空間分配的 VMware 主機建立 LUN 、則在升級至 ONTAP 9.15.1 之後、該 LUN 上的空間分配仍會停用。

步驟

1. 啟用空間分配：

```
lun modify -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-space-allocation enabled
```

2. 確認已啟用空間分配：

```
lun show -vserver <vserver_name> -volume <volume_name> -lun <lun_name>
-fields space-allocation
```

3. 確認主機作業系統上已啟用空間分配。

> 某些主機組態，包括某些版本的 VMware ESXi ，可以自動辨識設定變更，而且不需要使用者介入。其他組態可能需要重新掃描裝置。某些檔案系統和磁碟區管理員可能需要額外的特定設定，才能使用進行空間回收 `SCSI UNMAP`。可能需要重新掛載檔案系統或完整的作業系統重新開機。請參閱特定主機的文件以取得指引。

VMware ESXi 8.x 及更新版本 **NVMe** 主機的主機組態

如果您的 VMware 主機使用 NVMe 傳輸協定執行 ESXi 8.x 或更新版本，則在 ONTAP 中啟用空間分配之後，您應該在主機上執行下列步驟。

步驟

1. 在 ESXi 主機上，確認 DSM 已停用：

   ```
   esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
   ```

   預期值為 0 。

2. 啟用 NVMe DSM ：

```
esxcfg-advcfg -s 1 /Scsi/NvmeUseDsmTp4040
```

3. 確認 DSM 已啟用：

```
esxcfg-advcfg -g /SCSi/NVmeUseDsmTp4040
```

預期值為 1 。

相關連結

深入瞭解 "ESXi 8.x 搭配 ONTAP 的 NVMe 主機組態"。

建議的Volume與檔案或LUN組態組合

建議的Volume與檔案或LUN組態組合總覽

根據您的應用程式和管理需求、FlexVol 您可以使用特定的功能組合來搭配使用。瞭解這些組合的優點與成本、有助於判斷適合您環境的磁碟區與LUN組態組合。

建議使用下列磁碟區和LUN組態組合：

- 保留空間的檔案或LUN、具有完整磁碟區資源配置
- 非空間保留的檔案或LUN、採用精簡磁碟區資源配置
- 使用半厚磁碟區資源配置的空間保留檔案或LUN

您可以在LUN上搭配任何這些組態組合使用SCSI精簡配置。

保留空間的檔案或LUN、具有完整磁碟區資源配置

效益：

- 保證空間保留檔案內的所有寫入作業、不會因為空間不足而失敗。
- 磁碟區上的儲存效率和資料保護技術沒有任何限制。

成本與限制：

- 必須在Aggregate up Front預留足夠的空間、以支援最厚的已配置磁碟區。
- 在LUN建立時、從磁碟區配置的空間大小為LUN大小的兩倍。

非空間保留的檔案或LUN、採用精簡磁碟區資源配置

效益：

- 磁碟區上的儲存效率和資料保護技術沒有任何限制。
- 空間只會在使用時分配。

成本與限制：

- 寫入作業無法保證；如果磁碟區的可用空間不足、則寫入作業可能會失敗。

- 您必須有效管理Aggregate中的可用空間、以避免Aggregate耗盡可用空間。

使用半厚磁碟區資源配置的空間保留檔案或**LUN**

效益：

前端保留空間比大型磁碟區資源配置少、而且仍提供盡力寫入保證。

成本與限制：

- 使用此選項時、寫入作業可能會失敗。

  您可以適當平衡磁碟區中的可用空間與資料波動性、藉此降低此風險。

- 您無法仰賴資料保護物件的保留，例如快照， FlexClone 檔案和 LUN 。
- 您無法使用ONTAP 無法自動刪除的功能、包括重複資料刪除、壓縮及ODX/Copy卸載。

針對您的環境、判斷正確的**Volume**與**LUN**組態組合

回答幾個有關您環境的基本問題、有助於判斷FlexVol 最適合您環境的支援功能。

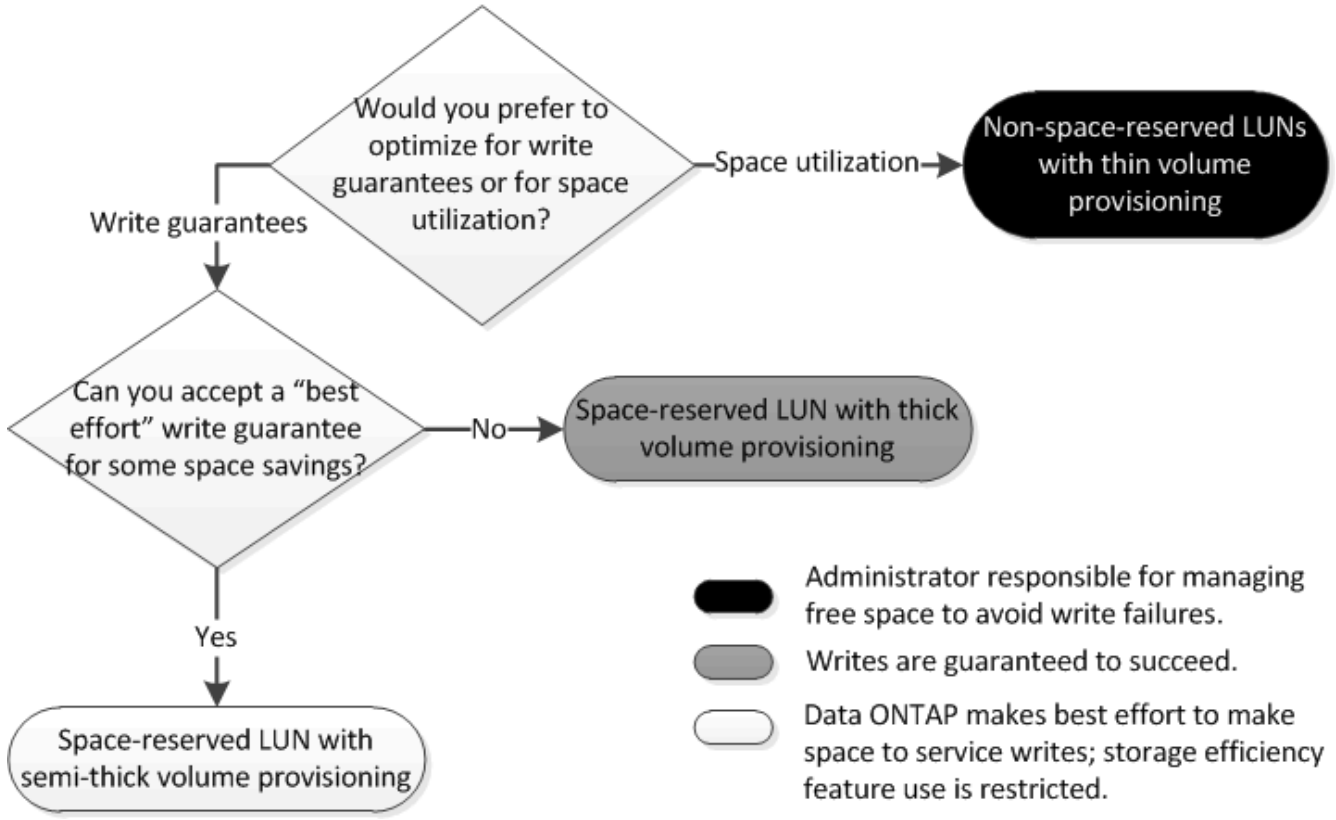
關於這項工作

您可以最佳化LUN和Volume組態、以達到最大的儲存使用率、或是保證寫入安全。根據您對儲存使用率的需求、以及您快速監控及補充可用空間的能力、您必須判斷FlexVol 適合您安裝的適用的版本。

您不需要為每個LUN分別建立磁碟區。

步驟

1. 請使用下列診斷樹來判斷環境的最佳Volume與LUN組態組合：



計算**LUN**的資料成長率

您需要知道LUN資料隨著時間成長的速度、才能判斷您應該使用空間保留LUN或非空間保留LUN。

關於這項工作

如果您的資料成長率持續偏高、則保留空間的LUN可能是您的最佳選擇。如果您的資料成長率較低、則應考慮非空間保留的LUN。

您可以使用OnCommand Insight 諸如VMware等工具來計算資料成長率、也可以手動計算。下列步驟適用於手動計算。

步驟

1. 設定空間保留LUN。
2. 監控LUN上的資料一段設定時間、例如一週。

   請確定您的監控期間足夠長、足以代表資料成長中經常發生的成長。例如、您可能在每個月結束時、都有大量的資料成長。

3. 每天以GB為單位記錄資料成長量。
4. 在您的監控期間結束時、將每天的總計加在一起、然後除以監控期間的天數。

   這項計算會產生您的平均成長率。

範例

在此範例中、您需要200 GB LUN。您決定監控LUN一週、並記錄下列每日資料變更：

- 星期日：20 GB
- 星期一：18 GB
- 星期二：17 GB
- 星期三：20 GB
- 星期四：20 GB
- 星期五：23 GB
- 星期六：22 GB

在此範例中、您的成長率為（20 + 18 + 17 + 20 + 20 + 23 + 22）/ 7 =每天20 GB。

空間保留檔案的組態設定、或是具有完整配置磁碟區的**LUN**

這個支援實體磁碟區和檔案或LUN組態的組合、能夠使用儲存效率技術、而且不需要主動監控可用空間、因為前面會配置足夠的空間。FlexVol

若要使用完整資源配置、在磁碟區中設定空間保留檔案或LUN、必須執行下列設定：

Volume設定	價值
保證	Volume
部分保留	100
Snapshot保留	任何
Snapshot自動刪除	選用
自動擴充	選用；如果啟用、則必須主動監控Aggregate可用空間。

檔案或**LUN**設定	價值
保留空間	已啟用

非空間保留檔案或使用精簡配置磁碟區的**LUN**組態設定

此一實體磁碟區與檔案或LUN組態組合需要最少的儲存容量預先配置、但需要主動式可用空間管理、以避免空間不足造成錯誤。FlexVol

若要在精簡配置的Volume中設定非空間保留的檔案或LUN、必須執行下列設定：

Volume設定	價值
保證	無
部分保留	0%
Snapshot保留	任何
Snapshot自動刪除	選用
自動擴充	選用

檔案或**LUN**設定	價值
保留空間	已停用

其他考量

當磁碟區或Aggregate空間不足時、寫入檔案或LUN的作業可能會失敗。

如果您不想主動監控磁碟區和Aggregate的可用空間、則應針對磁碟區啟用「自動擴充」、並將磁碟區的最大大小設為集合體的大小。在此組態中、您必須主動監控Aggregate可用空間、但不需要監控磁碟區中的可用空間。

空間保留檔案或**LUN**的組態設定、含半厚磁碟區資源配置

這個支援實體磁碟區和檔案或LUN的組態組合、需要較少的儲存設備、而不需要預先配置完整的組合、但會限制您可用於該磁碟區的效率技術。FlexVol此組態組合會盡力執行覆寫。

若要使用半厚資源配置、在磁碟區中設定空間保留LUN、必須執行下列設定：

Volume設定	價值
保證	Volume
部分保留	0%
Snapshot保留	0%
Snapshot自動刪除	在上、只要承諾銷毀層級、就會顯示一個銷毀清單、其中包含所有物件、設定為Volume的觸發程序、以及所有啟用自動刪除的FlexClone LUN和FlexClone檔案。
自動擴充	選用；如果啟用、則必須主動監控Aggregate可用空間。

檔案或LUN設定	價值
保留空間	已啟用

技術限制

您無法將下列Volume儲存效率技術用於此組態組合：

- 壓縮
- 重複資料刪除
- ODX與FlexClone複製卸載
- FlexClone LUN和FlexClone檔案未標示為自動刪除（作用中複本）
- FlexClone子檔案
- ODX/Copy卸載

其他考量

使用此組態組合時、必須考量下列事實：

- 當支援該 LUN 的磁碟區空間不足時，保護資料（ FlexClone LUN 和檔案，快照）就會遭到銷毀。
- 當磁碟區的可用空間不足時、寫入作業可能會逾時並失敗。

根據預設AFF 、對不支援的平台啟用壓縮。您必須明確停用壓縮任何想要在AFF 某個平台上使用半厚資源配置的Volume。

SAN 資料保護

瞭解適用於 SAN 環境的 ONTAP 資料保護方法

您可以製作資料複本來保護資料、以便在意外刪除、應用程式當機、資料毀損或災難發生時、能夠進行還原。根據您的資料保護和備份需求、ONTAP 支援各種方法來保護資料。

SnapMirror 主動同步

從通用供應ONTAP 功能的支援範圍而言、從提供零恢復時間目標（零RTO）或透明應用程式容錯移轉（TAF）開始、即可在SAN環境中自動容錯移轉業務關鍵應用程式。SnapMirror 主動同步需要在具有兩個 AFF 叢集或兩個 All Flash SAN Array （ ASA ）叢集的組態中安裝 ONTAP Mediator 1.2 。

"SnapMirror 主動同步"

Snapshot

可讓您手動或自動建立，排程及維護 LUN 的多個備份。快照只會使用少量的額外磁碟區空間，而且不會產生效能成本。如果您的 LUN 資料遭到意外修改或刪除，則可從最新的快照中輕鬆快速地還原該資料。

FlexClone LUN（需要**FlexClone**授權）

提供作用中磁碟區或快照中另一個 LUN 的時間點可寫入複本。可以獨立修改實體複本及其父複本、而不會影響彼此。

（需要授權）**SnapRestore**

可讓您從整個磁碟區上的快照執行快速，節省空間的隨需資料恢復。無需重新啟動儲存系統、您就可以使用SnapRestore 效益管理功能將LUN還原至先前保留的狀態。

資料保護鏡射複本（需要**SnapMirror**授權）

可讓您定期在磁碟區上建立資料快照，透過區域或廣域網路將這些快照複製到合作夥伴磁碟區（通常在其他叢集上），並保留這些快照，藉此提供非同步災難恢復功能。如果來源磁碟區上的資料毀損或遺失，合作夥伴磁碟區上的鏡射複本可從上次快照時起，提供資料的快速可用性和還原。

還原備份（需要**SnapMirror**授權）**SnapVault**

提供儲存效率與長期保留備份的功能。SnapVault 關係可讓您將選定的磁碟區快照備份至目的地磁碟區，並保留備份。

如果您執行磁帶備份和歸檔作業、您可以對SnapVault 已備份到該二線磁碟區的資料執行備份。

適用於**Windows**或**UNIX**（需取得授權）**SnapDrive SnapDrive**

可直接從 Windows 或 UNIX 主機設定 LUN 存取，管理 LUN ，以及管理儲存系統快照。

原生磁帶備份與還原

支援大部分現有的磁帶機、ONTAP 以及磁帶廠商動態新增新裝置支援的方法。此外、支援遠端磁磁帶（RMT）傳輸協定、可將備份與還原功能備份至任何功能強大的系統。ONTAP

相關資訊

"NetApp文件：SnapDrive 適用於UNIX的解決方案" "NetApp文件：SnapDrive 適用於Windows（目前版本）" "使用磁帶備份來保護資料"

從 **ONTAP** 快照還原單一 **LUN**

您可以從快照還原單一 LUN ，而無需還原包含單一 LUN 的整個磁碟區。您可以將LUN還原到原位或磁碟區中的新路徑。此作業只會還原單一LUN、而不會影響磁碟區中的其他檔案或LUN。您也可以使用串流還原檔案。

開始之前

- 您的磁碟區必須有足夠的空間才能完成還原作業：
  - 如果還原的是空間保留LUN、其中部分保留為0%、則需要還原LUN的一倍大小。
  - 如果還原的是空間保留LUN、而部分保留空間為100%、則需要還原LUN的兩倍大小。
  - 如果您要還原非空間保留LUN、則只需要用於還原LUN的實際空間。
- 必須已建立目的地 LUN 的快照。

如果還原作業失敗、則目的地LUN可能會被刪減。在這種情況下，您可以使用快照來防止資料遺失。

- 必須已建立來源 LUN 的快照。

  在極少數情況下、LUN還原可能會失敗、使來源LUN無法使用。如果發生這種情況，您可以使用快照將 LUN 恢復到還原嘗試之前的狀態。

- 目的地LUN和來源LUN必須具有相同的作業系統類型。

  如果您的目的地LUN與來源LUN的作業系統類型不同、則在還原作業之後、主機可能會失去對目的地LUN的資料存取權。

步驟

1. 從主機停止對LUN的所有主機存取。
2. 卸載主機上的LUN、使主機無法存取LUN。
3. 取消LUN對應：

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. 決定您要將 LUN 還原至的快照：

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. 在還原 LUN 之前建立 LUN 的快照：

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

6. 還原磁碟區中的指定LUN：

```
volume snapshot restore-file -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name> -path <lun_path>
```

7. 請依照畫面上的步驟進行。
8. 如有必要、請將LUN上線：

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

9. 如有必要、請重新對應LUN：

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

10. 從主機重新掛載LUN。
11. 從主機重新啟動對LUN的存取。

從 **ONTAP** 快照還原磁碟區中的所有 **LUN**

您可以使用 `volume snapshot restore`命令，從快照還原指定磁碟區中的所有 LUN 。

步驟

1. 從主機停止對LUN的所有主機存取。

   若使用SnapRestore 不停止所有主機存取磁碟區中的LUN、可能會導致資料毀損和系統錯誤。

2. 卸載該主機上的LUN、使主機無法存取LUN。
3. 取消對應LUN：

```
lun mapping delete -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

4. 決定您要還原磁碟區的快照：

```
volume snapshot show -vserver <SVM_name> -volume <volume_name>
```

5. 將您的權限設定變更為進階：

```
set -privilege advanced
```

6. 還原資料：

```
volume snapshot restore -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot_name>
```

7. 請依照畫面上的指示操作。
8. 重新對應LUN：

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup_name>
```

9. 驗證LUN是否處於線上狀態：

```
lun show -vserver <SVM_name> -path <lun_path> -fields state
```

10. 如果LUN不在線上、請將其上線：

```
lun modify -vserver <SVM_name> -path <lun_path> -state online
```

11. 將您的權限設定變更為admin：

```
set -privilege admin
```

12. 從主機重新掛載LUN。
13. 從主機重新啟動對LUN的存取。

使用 **ONTAP FlexClone LUN** 保護您的資料

FlexClone LUN 是作用中磁碟區或快照中另一個 LUN 的時間點可寫入複本。可獨立修改實體複本及其父複本、而不會影響彼此。

您可以使用FlexClone LUN來建立LUN的多個讀寫複本。

建立 **FlexClone LUN** 的理由

- 您需要建立LUN的暫用複本、以供測試之用。
- 您必須為其他使用者提供一份資料複本、而不讓他們存取正式作業資料。
- 您想要建立資料庫的複本、以便進行操作和投影作業、同時以未變更的形式保留原始資料。
- 您想要存取LUN資料的特定子集（磁碟區群組中的特定邏輯磁碟區或檔案系統、 或檔案系統中的特定檔案或檔案集）、然後複製到原始LUN、而不還原原始LUN中的其餘資料。這適用於支援同時掛載LUN和LUN複本的作業系統。SnapDrive for UNIX 支援此功能 `snap connect` 命令。
- 您需要使用相同作業系統的多個SAN開機主機。

FlexClone LUN最初與其父LUN共享空間。根據預設、FlexClone LUN會繼承父LUN的空間保留屬性。例如、如果父LUN為非保留空間、則FlexClone LUN預設也不會保留空間。不過、您可以從父LUN（空間保留LUN）建立非空間保留的FlexClone LUN。

當您複製 LUN 時，會在背景中進行區塊共用，而且在區塊共用完成之前，您無法建立磁碟區快照。

您必須設定磁碟區、才能使用啟用 FlexClone LUN 自動刪除功能 `volume snapshot autodelete modify` 命令。否則、如果您想要自動刪除FlexClone LUN、但未將該磁碟區設定為FlexClone自動刪除、則不會刪除任何FlexClone LUN。

當您建立FlexClone LUN時、FlexClone LUN自動刪除功能預設為停用。您必須在每個FlexClone LUN上手動啟用、才能自動刪除FlexClone LUN。如果您使用半厚磁碟區資源配置、且想要此選項提供「最佳努力」寫入保證、則必須讓_all_ FlexClone LUN可供自動刪除。

當您從快照建立 FlexClone LUN 時， LUN 會使用節省空間的背景程序，自動從快照分割，使 LUN 不會繼續依賴快照或佔用任何額外空間。如果此背景分割尚未完成，而且此快照會自動刪除，即使您已停用該 FlexClone LUN 的 FlexClone 自動刪除功能，該 FlexClone LUN 也會被刪除。背景分割完成後，即使刪除了 FlexClone LUN ，也不會刪除該快照。

相關資訊

- "建立 FlexClone LUN"
- "設定 FlexVol volume 以自動刪除 FlexClone LUN"
- "防止自動刪除 FlexClone LUN"

在SnapVault SAN環境中設定及使用靜態備份

瞭解 **SAN** 環境中的 **ONTAP SnapVault** 備份

SAN環境中的支援組態和使用與NAS環境中的組態和使用非常類似、但在SAN環境中還原LUN需要一些特殊程序。SnapVault

還原備份包含來源Volume的一組唯讀複本。SnapVault在SAN環境中、您一律將整個磁碟區備份到SnapVault 不屬於個別LUN的二線磁碟區。

建立SnapVault 和初始化包含LUN的主要Volume與做SnapVault 為支援的次要Volume之間的支援性關係的程序、與FlexVol 用於檔案傳輸協定的支援使用的流程相同。本程序將在中詳細說明 "資料保護"。

在建立快照並將其複製到 SnapVault 次要 Volume 之前，請務必確保備份的 LUN 處於一致的狀態。使用 SnapCenter 自動建立快照，可確保備份的 LUN 完整且可由原始應用程式使用。

有三個基本選項可從SnapVault 一個不二元磁碟區還原LUN：

- 您可以直接從SnapVault 「支援」二級磁碟區對應LUN、並將主機連線至LUN、以存取LUN的內容。

  LUN 是唯讀的，您只能從 SnapVault 備份中的最新快照進行對應。持續保留和其他LUN中繼資料將會遺失。如果需要、您可以使用主機上的複製程式、將LUN內容複製回原始LUN（如果仍可存取）。

  LUN的序號與來源LUN不同。

- 您可以將 SnapVault 次要 Volume 中的任何快照複製到新的讀寫磁碟區。

  然後、您可以對應磁碟區中的任何LUN、並將主機連線至LUN、以存取LUN的內容。如果需要、您可以使用主機上的複製程式、將LUN內容複製回原始LUN（如果仍可存取）。

- 您可以從 SnapVault 次要磁碟區中的任何快照，還原包含 LUN 的整個磁碟區。

  還原整個磁碟區會取代磁碟區中的所有LUN及任何檔案。快照建立後所建立的任何新 LUN 都會遺失。

  LUN會保留對應、序號、UUID及持續保留。

從 **ONTAP SnapVault** 備份存取唯讀 **LUN** 複本

您可以從 SnapVault 備份中的最新快照存取 LUN 的唯讀複本。LUN ID、路徑和序號與來

源LUN不同、必須先對應。持續保留、LUN對應和igroup不會複寫到SnapVault 位元二的Volume。

開始之前

- 必須初始化 SnapVault 關係，且 SnapVault 次要磁碟區中的最新快照必須包含所需的 LUN 。
- 包含SnapVault 此功能的儲存虛擬機器（SVM）必須具有一個或多個LIF、並可從用於存取LUN複本的主機存取所需的SAN傳輸協定。
- 如果您打算直接從SnapVault 「不二重複資料」磁碟區存取LUN複本、則必須SnapVault 事先在「不二重複資料」上建立群組。

  您無需SnapVault 先還原或複製包含LUN的磁碟區、即可直接從「還原次要磁碟區」存取LUN。

關於這項工作

如果在從先前快照對應 LUN 時，新快照已新增至 SnapVault 次要磁碟區，則對應 LUN 的內容會變更。LUN 仍會以相同的識別碼對應，但資料是從新的快照擷取。如果LUN大小變更、部分主機會自動偵測大小變更；Windows主機需要重新掃描磁碟、才能接收任何大小變更。

步驟

1. 列出 SnapVault 次要磁碟區中的可用 LUN 。

   ```
   lun show
   ```

   在此範例中、您可以同時查看主要Volume srcvolA中的原始LUN、SnapVault 以及《支援還原的次要Volume dstvolB：

   ```
   cluster::> lun show

   Vserver   Path                State   Mapped   Type          Size
   --------  ------------------  ------  -------  --------      -------
   vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
   vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
   vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
   vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
   vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
   vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

   6 entries were displayed.
   ```

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

2. 如果包含 SnapVault 次要 Volume 的 SVM 上尚未存在所需主機的 igroup ，請建立 igroup 。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <ostype> -initiator <initiator_name>
```

此命令會為使用iSCSI傳輸協定的Windows主機建立igroup：

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

3. 將所需的 LUN 複本對應至 igroup 。

```
lun mapping create -vserver <SVM_name> -path <LUN_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB -path /vol/dstvolB/lun_A
  -igroup temp_igroup
```

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

4. 將主機連接至LUN、並視需要存取LUN的內容。

從 **ONTAP SnapVault** 備份還原單一 **LUN**

您可以將單一LUN還原至新位置或原始位置。您可以從 SnapVault 次要 Volume 中的任何快照還原。若要將LUN還原至原始位置、請先將其還原至新位置、然後再將其複製。

開始之前

- 必須初始化 SnapVault 關係，且 SnapVault 次要 Volume 必須包含適當的快照才能還原。
- 包含SnapVault 不支援的二線磁碟區的儲存虛擬機器（SVM）必須具有一個或多個具備所需SAN傳輸協定的LIF、才能從用於存取LUN複本的主機存取。
- igroup必須已存在SnapVault 於SVM上。

關於這項工作

此程序包括從 SnapVault 次要 Volume 中的快照建立讀寫磁碟區複本。您可以直接從實體複本使用LUN、也可以選擇將LUN內容複製回原始LUN位置。

實體複本中的LUN路徑和序號與原始LUN不同。不保留持續保留。

步驟

1. 驗證包含 SnapVault 備份的次要磁碟區。

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                        Snapmirrored
                                Idle       -         true    -
```

2. 識別您要從其中還原 LUN 的快照。

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

3. 從所需的快照建立讀寫複本

```
volume clone create -vserver <SVM_name> -flexclone <flexclone_name>
-type <type> -parent-volume <parent_volume_name> -parent-snapshot
<snapshot_name>
```

磁碟區複製是以SnapVault 相同的Aggregate建立、如同使用支援功能進行備份。集合體中必須有足夠的空間來儲存實體複本。

```
cluster::> volume clone create -vserver vserverB
  -flexclone dstvolB_clone -type RW -parent-volume dstvolB
  -parent-snapshot daily.2013-02-10_0010
[Job 108] Job succeeded: Successful
```

4. 列出磁碟區複製中的 LUN 。

```
lun show -vserver <SVM_name> -volume <flexclone_volume_name>
```

```
cluster::> lun show -vserver vserverB -volume dstvolB_clone

Vserver   Path                      State   Mapped   Type
--------- ------------------------  ------- -------- --------
vserverB  /vol/dstvolB_clone/lun_A  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_B  online  unmapped windows
vserverB  /vol/dstvolB_clone/lun_C  online  unmapped windows

3 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `lun show`資訊，請參閱。

5. 如果包含 SnapVault 備份的 SVM 上尚未存在所需主機的 igroup ，請建立 igroup 。

```
igroup create -vserver <SVM_name> -igroup <igroup_name> -protocol
<protocol> -ostype <os_type> -initiator <initiator_name>
```

此範例為使用iSCSI傳輸協定的Windows主機建立igroup：

```
cluster::> igroup create -vserver vserverB -igroup temp_igroup
  -protocol iscsi -ostype windows
  -initiator iqn.1991-05.com.microsoft:hostA
```

6. 將所需的 LUN 複本對應至 igroup 。

```
lun mapping create -vserver <SVM_name> -path <lun_path> -igroup
<igroup_name>
```

```
cluster::> lun mapping create -vserver vserverB
  -path /vol/dstvolB_clone/lun_C -igroup temp_igroup
```

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

7. 將主機連接至LUN、並視需要存取LUN的內容。

LUN為讀寫、可用於取代原始LUN。由於LUN序號不同、因此主機會將其解譯為與原始LUN不同的LUN。

8. 使用主機上的複製程式、將LUN內容複製回原始LUN。

相關資訊

- "SnapMirror 顯示"

從 **ONTAP SnapVault** 備份還原磁碟區中的所有 **LUN**

如果一個磁碟區中的一個或多個LUN需要從SnapVault 還原備份、您可以還原整個磁碟區。還原磁碟區會影響磁碟區中的所有LUN。

開始之前

必須初始化 SnapVault 關係，且 SnapVault 次要 Volume 必須包含適當的快照才能還原。

關於這項工作

還原整個磁碟區會將磁碟區恢復到建立快照時的狀態。如果在快照之後將 LUN 新增至磁碟區，則會在還原程序期間移除該 LUN 。

還原磁碟區之後、LUN會保留對應至還原前所對應的igroup。LUN 對應可能與快照時的對應不同。保留來自主機叢集之LUN的持續保留。

步驟

1. 停止磁碟區中所有LUN的I/O。
2. 驗證包含 SnapVault 次要 Volume 的次要 Volume 。

```
snapmirror show
```

```
cluster::> snapmirror show

Source          Dest     Mirror  Relation  Total             Last
Path     Type   Path     State   Status    Progress  Healthy Updated
-------- ---- --------- ------- --------- --------- ------- -------
vserverA:srcvolA
         XDP  vserverB:dstvolB
                         Snapmirrored
                                 Idle       -         true    -
```

3. 識別您要還原的快照。

```
volume snapshot show
```

```
cluster::> volume snapshot show

Vserver  Volume  Snapshot                State Size   Total% Used%
-------- ------- ---------------------- ----- ------ ------ -----
vserverB
         dstvolB
                 snap2.2013-02-10_0010  valid  124KB     0%    0%
                 snap1.2013-02-10_0015 valid  112KB     0%    0%
                 snap2.2013-02-11_0010  valid  164KB     0%    0%
```

4. 指定要使用的快照。

```
snapmirror restore -destination-path <destination_path> -source-path
<source_path> -source-snapshot <snapshot_name>
```

您指定的還原目的地是您要還原的原始Volume。

```
cluster::> snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB -source-snapshot daily.2013-02-10_0010

Warning: All data newer than Snapshot copy hourly.2013-02-11_1205 on
volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.
```

5. 如果您要在主機叢集之間共用LUN、請從受影響的主機還原LUN上的持續保留。

從**SnapVault** 無法還原的備份還原磁碟區

在以下範例中，名為 LUN_D 的 LUN 會在建立快照後新增至磁碟區。從快照還原整個磁碟區之後，就不會再顯示 LUN_D 。

在中 `lun show` 命令輸出中、您可以在主磁碟區 srcvolA 中看到 LUN 、以及在 SnapVault 次要磁碟區 dstvolB 中看到這些 LUN 的唯讀複本。在不支援支援的情況下、沒有LUN_D的複本SnapVault 。

```
cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_D  online  mapped   windows  250.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

7 entries were displayed.

cluster::>snapmirror restore -destination-path vserverA:srcvolA
  -source-path vserverB:dstvolB
  -source-snapshot daily.2013-02-10_0010

Warning: All data newer than snapshot hourly.2013-02-11_1205
on volume vserverA:src_volA will be deleted.
Do you want to continue? {y|n}: y
[Job 98] Job is queued: snapmirror restore from source
"vserverB:dstvolB" for the snapshot daily.2013-02-10_0010.

cluster::> lun show
Vserver   Path                 State   Mapped   Type          Size
--------- ------------------   ------- -------- --------      -------
vserverA  /vol/srcvolA/lun_A  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_B  online  mapped   windows  300.0GB
vserverA  /vol/srcvolA/lun_C  online  mapped   windows  300.0GB
vserverB  /vol/dstvolB/lun_A  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_B  online  unmapped windows  300.0GB
vserverB  /vol/dstvolB/lun_C  online  unmapped windows  300.0GB

6 entries were displayed.
```

從SnapVault 還原次要Volume還原磁碟區之後、來源Volume不再包含LUN_D還原之後、您不需要重新對應來源磁碟區中的LUN、因為它們仍會對應。

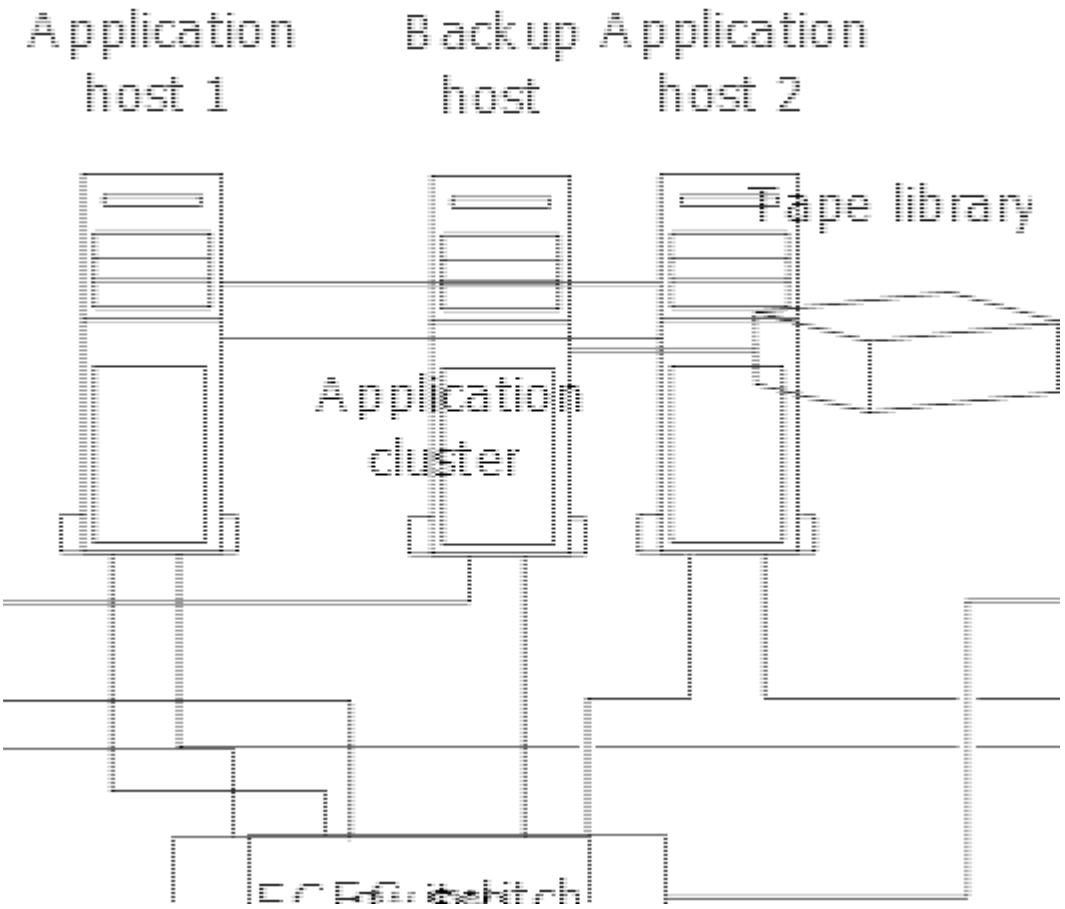
相關資訊

- "SnapMirror還原"
- "SnapMirror 顯示"

將主機備份系統連接至 **ONTAP** 的建議組態

您可以透過獨立的備份主機將SAN系統備份至磁帶、以避免應用程式主機的效能降低。

您必須將SAN和NAS資料分開以供備份之用。下圖顯示主機備份系統至主要儲存系統的建議實體組態。您必須將磁碟區設定為純SAN。LUN可侷限於單一磁碟區、或LUN可分散於多個磁碟區或儲存系統。



主機上的磁碟區可由從儲存系統對應的單一LUN或使用Volume Manager的多個LUN組成、例如HP-UX系統上的VxVM.

使用主機備份系統來保護 **ONTAP** 儲存系統上的 **LUN**

您可以使用快照中的複製 LUN 做為主機備份系統的來源資料。

開始之前

正式作業LUN必須存在、並對應至內含應用程式伺服器WWPN或啟動器節點名稱的igroup。LUN也必須格式化、且可供主機存取

步驟

1. 將主機檔案系統緩衝區的內容儲存至磁碟。

   您可以使用主機作業系統提供的命令、也可以使用SnapDrive 適用於Windows的支援功能或SnapDrive 適用於UNIX的支援功能。您也可以選擇將此步驟納入SAN備份預先處理指令碼。

2. 建立正式作業 LUN 的快照。

```
volume snapshot create -vserver <SVM_name> -volume <volume_name>
-snapshot <snapshot> -comment <comment> -foreground false
```

3. 建立正式作業 LUN 的複本。

```
volume file clone create -vserver <SMV_name> -volume <volume> -source
-path <path> -snapshot-name <snapshot> -destination-path
<destination_path>
```

4. 建立包含備份伺服器 WWPN 的 igroup 。

```
lun igroup create -vserver <SVM_name> -igroup <igroup> -protocol
<protocol> -ostype <os_type> -initiator <initiator>
```

5. 將您在步驟 3 中建立的 LUN 複本對應到備份主機。

```
lun mapping create -vserver <SVM_name> -volume <volume_name> -lun
<lun_name> -igroup <igroup>
```

   您可以選擇將此步驟納入SAN備份應用程式的後處理指令碼。

6. 從主機探索新的LUN、並讓主機使用檔案系統。

   您可以選擇將此步驟納入SAN備份應用程式的後處理指令碼。

7. 使用SAN備份應用程式、將LUN實體複製中的資料從備份主機備份到磁帶。
8. 將 LUN 複製作業離線。

```
lun modify -vserver <SVM_name> -path <path> -state offline
```

9. 移除 LUN 複本。

```
lun delete -vserver <SVM_name> -volume <volume> -lun <lun_name>
```

10. 移除快照。

```
volume snapshot delete -vserver <SVM_name> -volume <volume> -snapshot
<snapshot>
```

SAN組態參考

瞭解 ONTAP SAN 組態

儲存區域網路（ SAN ）是由透過 iSCSI 或 FC 等 SAN 傳輸協定連接至主機的儲存解決方案所組成。您可以設定 SAN 、讓儲存解決方案透過一或多個交換器連接到主機。 如果您使用 iSCSI 、也可以設定 SAN 、讓儲存解決方案直接連接到主機、而無需使用交換器。

在 SAN 中、使用不同作業系統（例如 Windows 、 Linux 或 UNIX ）的多個主機可以同時存取儲存解決方案。您可以使用 "選擇性 LUN 對應" 和 "連接埠集" 限制主機與儲存設備之間的資料存取。

對於 iSCSI 、儲存解決方案與主機之間的網路拓撲稱為網路。 對於 FC 、 FC/NVMe 和 FCoE 、儲存解決方案和主機之間的網路拓撲稱為架構。若要建立備援功能、防止資料存取遺失、您應該在多網路或多架構組態中設定 SAN 搭配 HA 配對。 使用單一節點或單一網路 / 架構的組態並非完全備援、因此不建議使用。

設定 SAN 之後、您就可以了 "為 iSCSI 或 FC 配置儲存設備"或是您可以 "為 FC/NVMe 配置儲存設備"。 然後、您可以連線至主機、開始服務資料。

SAN 傳輸協定支援會因您的 ONTAP 版本、平台和組態而異。如需特定組態的詳細資訊、請參閱 "NetApp 互通性對照表工具"。

相關資訊

- "SAN管理總覽"
- "NVMe 組態、支援和限制"

iSCSI 組態

使用 ONTAP 系統設定 iSCSI 網路

您應該使用高可用度（ HA ）配對來設定 iSCSI 組態、這些配對可直接連接到 iSCSI SAN 主機、或透過一或多個 IP 交換器連接到主機。

"HA 配對" 定義為主動 / 最佳化路徑的報告節點、以及主機用來存取 LUN 的主動 / 未最佳化路徑。使用不同作業系統（例如 Windows 、 Linux 或 UNIX ）的多部主機、可以同時存取儲存設備。 主機需要安裝及設定支援 ALUA 的多重路徑解決方案。可在上驗證支援的作業系統和多重路徑解決方案 "NetApp 互通性對照表工具"。

在多網路組態中、有兩個以上的交換器會將主機連線至儲存系統。 建議使用多網路組態、因為它們完全備援。在單一網路組態中、有一台交換器會將主機連線至儲存系統。 單一網路組態並非完全備援。

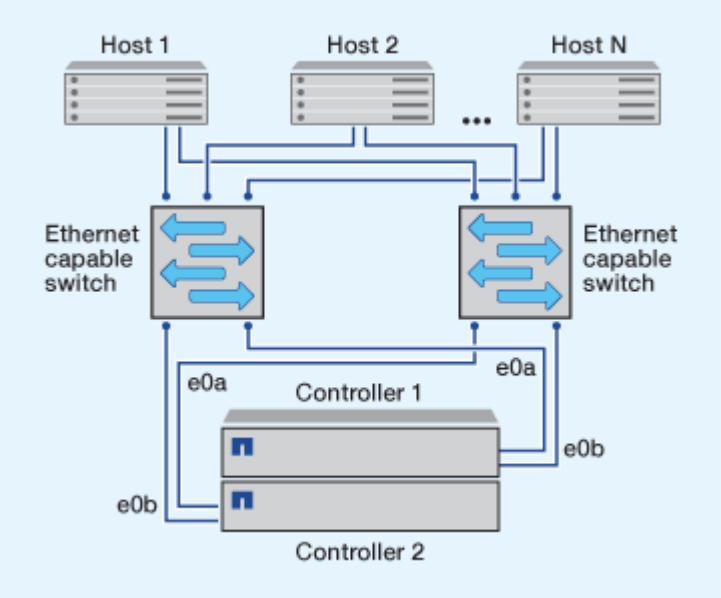
"單節點組態" 不建議使用、因為它們不提供支援容錯和不中斷營運所需的備援功能。

相關資訊

- 瞭解如何"選擇性 LUN 對應（ SLM ）"限制用於存取 HA 配對所擁有 LUN 的路徑。
- 深入瞭解 "SAN LIF"。
- 深入瞭解 "iSCSI 中 VLAN 的優點"。

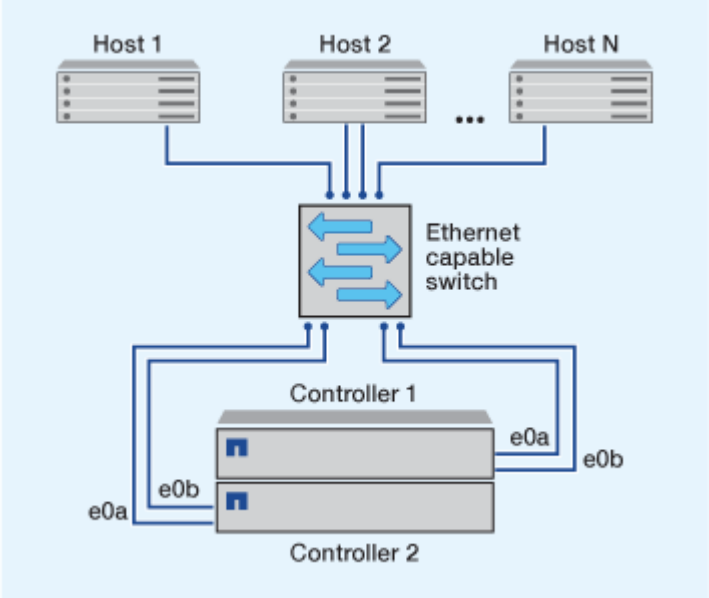
多網路 iSCSI 組態

在多網路HA配對組組態中、兩個或多個交換器會將HA配對連接至一或多個主機。由於有多個交換器、因此此組態完全備援。



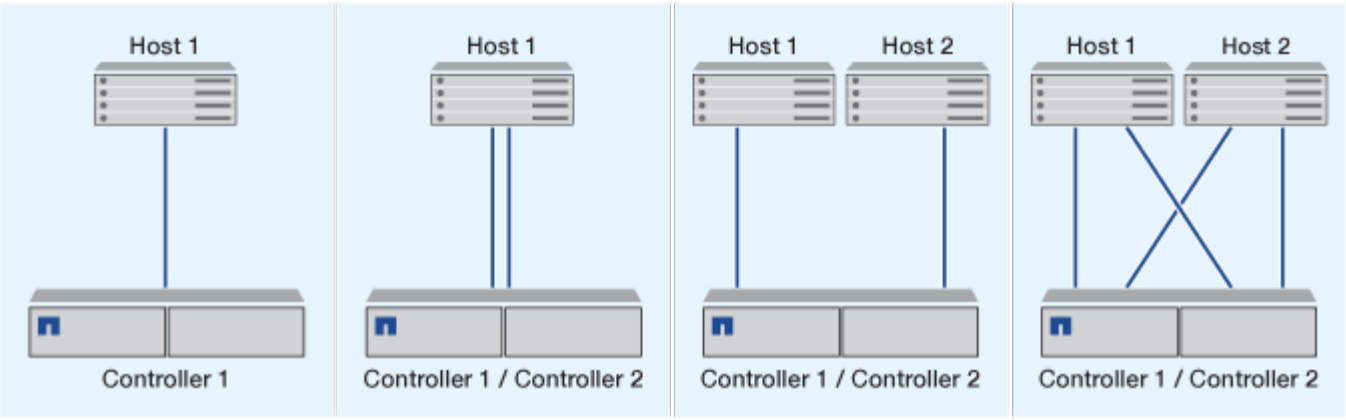
單一網路 iSCSI 組態

在單一網路HA配對組組態中、一台交換器會將HA配對連接至一或多個主機。由於只有一台交換器、因此此組態並未完全備援。



直接附加 iSCSI 組態

在直接附加的組態中、一或多個主機會直接連線至控制器。



在 **iSCSI** 組態中搭配 **ONTAP** 系統使用 **VLAN** 的優點

VLAN由一組交換器連接埠組成、這些交換器連接埠集合在一個廣播網域中。VLAN可以位於單一交換器上、也可以橫跨多個交換器機箱。靜態和動態VLAN可讓您提高安全性、隔離問題、並限制IP網路基礎架構內的可用路徑。

當您在大型IP網路基礎架構中實作VLAN時、會獲得下列效益：

- 提高安全性。

  VLAN可讓您善用現有的基礎架構、同時仍能提供更高的安全性、因為它們會限制乙太網路或IP SAN的不同節點之間的存取。

- 隔離問題、改善乙太網路和IP SAN的可靠性。
- 限制問題空間、縮短問題解決時間。
- 減少通往特定iSCSI目標連接埠的可用路徑數量。
- 減少主機使用的最大路徑數。

  路徑過多會減慢重新連線的速度。如果主機沒有多重路徑解決方案、您可以使用VLAN只允許一條路徑。

動態**VLAN**

動態VLAN是以MAC位址為基礎的。您可以指定要包含的成員的MAC位址、來定義VLAN。

動態VLAN提供靈活度、不需要對應至裝置實體連接至交換器的實體連接埠。您可以在不重新設定VLAN的情況下、將纜線從一個連接埠移至另一個連接埠。

靜態**VLAN**

靜態VLAN是以連接埠為基礎的。交換器和交換器連接埠用於定義VLAN及其成員。

靜態VLAN提供更高的安全性、因為使用媒體存取控制（MAC）偽造不可能違反VLAN。但是、如果有人能夠實體存取交換器、更換纜線並重新設定網路位址、則可以允許存取。

在某些環境中、建立和管理靜態VLAN比動態VLAN更容易。這是因為靜態VLAN只需要指定交換器和連接埠識別碼、而非48位元的MAC位址。此外、您也可以使用VLAN識別碼來標示交換器連接埠範圍。

FC 組態

使用 **ONTAP** 系統設定 **FC** 或 **FC-NVMe** 架構

建議您使用 HA 配對和至少兩台交換器來設定 FC 和 FC-NVMe SAN 主機。 這可在架構和儲存系統層提供備援、以支援容錯能力和不中斷營運。您無法在未使用交換器的情況下、直接將FC或FC-NVMe SAN主機連接至HA配對。

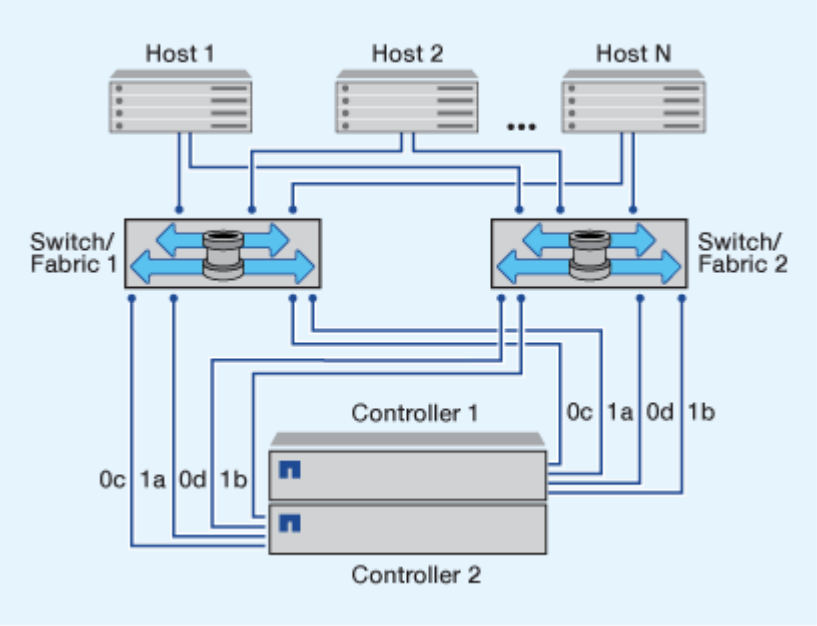
串聯、部分網狀、全網狀、核心邊緣和導向架構都是將FC交換器連接至光纖的業界標準方法、而且都受到支援。 不支援使用異質FC交換器架構、但內嵌刀鋒交換器除外。 上會列出特定例外狀況 "互通性對照表工具"。一個網路可由一或多個交換器組成、而且儲存控制器可連接至多個交換器。

使用不同作業系統（例如 Windows 、 Linux 或 UNIX ）的多個主機、可以同時存取儲存控制器。 主機需要安裝並設定支援的多重路徑解決方案。支援的作業系統和多重路徑解決方案可在互通性對照表工具上驗證。

Multifabric FC 和 **FC-NVMe** 組態

在 Multifabric HA 配對組態中、有兩個或多個交換器會將 HA 配對連線至一或多個主機。為了簡單起見、下列 Multifabric HA 配對圖只顯示兩個 Fabric 、但您可以在任何 Multifabric 組態中擁有兩個以上的 Fabric 。

圖中的 FC 目標連接埠編號（ 0c 、 0d 、 1a 、 1b ）為範例。實際的連接埠編號會因儲存節點的機型和是否使用擴充介面卡而有所不同。

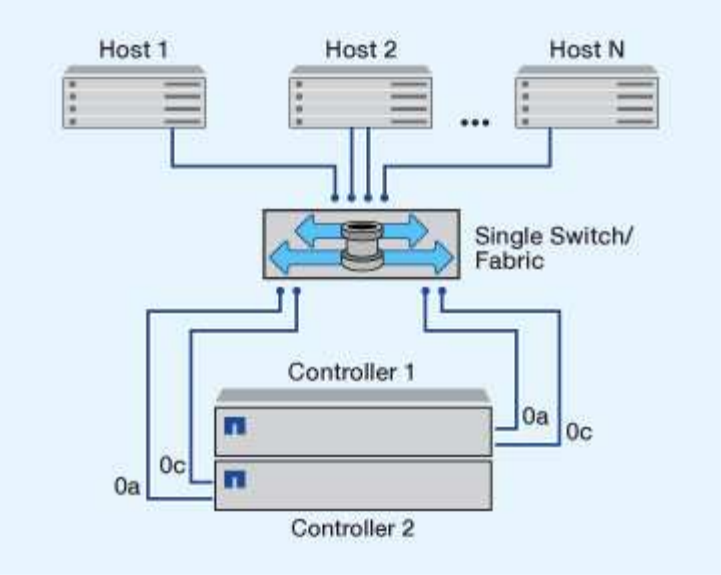


單一架構 **FC** 和 **FC-NVMe** 組態

在單一架構HA配對組組態中、有一個架構可將HA配對中的兩個控制器連接至一或多個主機。由於主機和控制器是透過單一交換器連接、因此單一架構 HA 配對組態並非完全備援。

圖中的 FC 目標連接埠編號（ 0A 、 0c ）為範例。實際的連接埠編號會因儲存節點的機型和是否使用擴充介面卡而有所不同。

所有支援 FC 組態的平台都支援單一架構 HA 配對組態。



"單節點組態" 不建議使用、因為它們不提供支援容錯和不中斷營運所需的備援功能。

相關資訊

- 瞭解如何"選擇性 LUN 對應（ SLM ）"限制用於存取 HA 配對所擁有 LUN 的路徑。
- 深入瞭解 "SAN LIF"。

使用 **ONTAP** 系統設定 **FC** 交換器的最佳實務做法

為獲得最佳效能、您應該在設定FC交換器時考量某些最佳實務做法。

固定連結速度設定是FC交換器組態的最佳實務做法、尤其是大型架構、因為它能為光纖重建提供最佳效能、並大幅節省時間。儘管自動協商提供最大的靈活度、但FC交換器組態並不總是如預期般執行、而且會為整體架構建置順序增加時間。

連接至網路的所有交換器都必須支援N_Port ID虛擬化（NPIV）、而且必須啟用NPIV。使用NPIV向光纖展示FC目標。ONTAP

如需支援哪些環境的詳細資訊、請參閱 "NetApp 互通性對照表工具"。

有關 FC 和 iSCSI 最佳實務做法，請參閱 "NetApp 技術報告 4080 ：現代 SAN 的最佳實務做法"。

ONTAP 系統的建議 **FC** 目標連接埠組態和速度

FC 目標連接埠可設定及用於 FC-NVMe 傳輸協定，其方式與 FC 傳輸協定的設定和使用方式完全相同。FC-NVMe 傳輸協定的支援會因您的平台和 ONTAP 版本而異。使用 NetApp Hardware Universe 驗證支援。

為獲得最佳效能和最高可用度，您應針對特定平台使用中所列的建議目標連接埠組態 "NetApp Hardware Universe"。

具有共享 **ASIC** 的 **FC** 目標連接埠組態

下列平台具有連接埠配對，可與共享的應用程式專用集成電路（ ASIC ）搭配使用。如果您在這些平台上使用擴

充介面卡，您應該設定 FC 連接埠，使它們不會使用相同的 ASIC 進行連線。

控制器	連接埠配對與共享**ASIC**	目標連接埠數量：建議的連接埠
• FAS8200 • 部分A300 AFF	0g+0小時	1 ： 0g 2 ： 0g ， 0 小時
• FAS2720 • FAS2750 • VA220 AFF	0C+0d 0e+0f	1 ： 0C 2 ： 0C ， 0e 3 ： 0C ， 0e ， 0d 4 ： 0C ， 0e ， 0d ， 0f

FC目標連接埠支援的速度

FC目標連接埠可設定為以不同速度執行。指定主機使用的所有目標連接埠都應設定為相同的速度。您應該設定目標連接埠速度、使其符合所連接裝置的速度。請勿將自動協商功能用於連接埠速度。設定為自動協商的連接埠、在接管/恢復或其他中斷之後、重新連線可能需要較長時間。

您可以設定內建連接埠和擴充介面卡、以下列速度執行。每個控制器和擴充介面卡連接埠都可視需要個別設定、以獲得不同的速度。

4 Gb連接埠	**8 Gb** 連接埠	**16 GB**連接埠	**32 GB** 連接埠
• 4 GB • 2 GB • 1 GB	• 8 GB • 4 GB • 2 GB	• 16 GB • 8 GB • 4 GB	• 32 GB • 16 GB • 8 GB

如需支援的介面卡及其支援速度的完整清單，請參閱 "NetApp Hardware Universe"。

設定 **ONTAP FC** 介面卡連接埠

內建 FC 介面卡和某些 FC 擴充卡可以個別設定為啟動器或目標連接埠。其他 FC 擴充介面卡在原廠設定為啟動器或目標，無法變更。透過支援的 UTA2 卡（使用 FC SFP+ 介面卡設定），也可以使用額外的 FC 連接埠。

啟動器連接埠可用於直接連接至後端磁碟櫃，也可能是外部儲存陣列。目標連接埠只能用於連接 FC 交換器。

為 FC 設定的內建連接埠和 CNA/UTA2 連接埠數量會因控制器機型而異。支援的目標擴充介面卡也會因控制器機型而異。如需控制器機型內建 FC 連接埠和支援的目標擴充介面卡的完整清單，請參閱"NetApp Hardware Universe"。

將**FC**介面卡設定為啟動器模式

啟動器模式用於將連接埠連接到磁帶磁碟機、磁帶庫或具有外部 LUN 匯入 (FLI) 功能的第三方儲存。

開始之前

- 介面卡上的LIF必須從其成員所在的任何連接埠集中移除。
- 使用要修改之實體連接埠的所有儲存虛擬機器（SVM）LIF、必須先移轉或銷毀、才能將實體連接埠的特性

從目標變更為啟動器。

NVMe / FC支援啟動器模式。

步驟

1. 移除介面卡上的所有LIF：

```
network interface delete -vserver _SVM_name_ -lif _lif_name_,_lif_name_
```

2. 讓介面卡離線：

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-status-admin down
```

如果介面卡未離線、您也可以從系統上適當的介面卡連接埠拔下纜線。

3. 將介面卡從目標變更為啟動器：

```
system hardware unified-connect modify -t initiator _adapter_port_
```

4. 重新啟動裝載您所變更介面卡的節點。
5. 驗證FC連接埠的組態設定是否正確：

```
system hardware unified-connect show
```

6. 將介面卡重新連線：

```
node run -node _node_name_ storage enable adapter _adapter_port_
```

將FC介面卡設定為目標模式

目標模式用於將連接埠連接至FC啟動器。

同樣的步驟也用於設定 FC 傳輸協定和 FC-NVMe 傳輸協定的 FC 介面卡。不過、只有某些FC介面卡支援FC-NVMe。如需支援 FC-NVMe 傳輸協定的介面卡清單，請參閱"NetApp Hardware Universe"。

步驟

1. 使介面卡離線：

```
node run -node _node_name_ storage disable adapter _adapter_name_
```

如果介面卡未離線、您也可以從系統上適當的介面卡連接埠拔下纜線。

2. 將介面卡從啟動器變更為目標：

```
system node hardware unified-connect modify -t target -node _node_name_
adapter _adapter_name_
```

3. 重新啟動裝載您所變更介面卡的節點。
4. 驗證目標連接埠的組態是否正確：

```
network fcp adapter show -node _node_name_
```

5. 將介面卡上線：

```
network fcp adapter modify -node _node_name_ -adapter _adapter_port_
-state up
```

設定 FC 介面卡速度

您應該設定介面卡目標連接埠速度，使其符合所連接裝置的速度，而非使用自動協商。設定為自動協商的連接埠、在接管/恢復或其他中斷之後、重新連線可能需要較長的時間。

關於這項工作

由於此工作涵蓋叢集中的所有儲存虛擬機器（ SVM ）和所有生命、因此您必須使用 `-home-port` 和 `-home-lif` 限制此作業範圍的參數。如果不使用這些參數、則此作業會套用至叢集中的所有I生命、這可能是不理想的。

開始之前

使用此介面卡做為其主連接埠的所有LIF都必須離線。

步驟

1. 將此介面卡上的所有生命段離線：

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin down
```

2. 使介面卡離線：

```
network fcp adapter modify -node node1 -adapter 0c -state down
```

如果介面卡未離線、您也可以從系統上適當的介面卡連接埠拔下纜線。

3. 判斷連接埠介面卡的最大速度：

```
fcp adapter show -instance
```

您無法修改介面卡速度超過最大速度。

4. 變更介面卡速度：

```
network fcp adapter modify -node node1 -adapter 0c -speed 16
```

5. 將介面卡上線：

```
network fcp adapter modify -node node1 -adapter 0c -state up
```

6. 將介面卡上的所有生命項目上線：

```
network interface modify -vserver * -lif * { -home-node node1 -home-port
0c } -status-admin up
```

用於管理 **FC** 介面卡的 **ONTAP** 命令

您可以使用FC命令來管理儲存控制器的FC目標介面卡、FC啟動器介面卡和內建FC介面卡。相同的命令也用於管理FC傳輸協定和FC-NVMe傳輸協定的FC介面卡。

FC啟動器介面卡命令只能在節點層級運作。您必須使用 `run -node` *`node_name`* 使用 FC 啟動器介面卡命令之前的命令。

用於管理**FC**目標介面卡的命令

如果您想要...	使用此命令...
在節點上顯示FC介面卡資訊	`network fcp adapter show`
修改FC目標介面卡參數	`network fcp adapter modify`
顯示FC傳輸協定流量資訊	`run -node` *`node_name`* `sysstat -f`
顯示FC傳輸協定已執行多久	`run -node` *`node_name`* `uptime`
顯示介面卡組態與狀態	`run -node` *`node_name`* `sysconfig -v` *`adapter`*

如果您想要...	使用此命令...
驗證安裝了哪些擴充卡、以及是否有任何組態錯誤	`run -node node_name sysconfig -ac`
查看命令的手冊頁	`man command_name`

用於管理**FC**啟動器介面卡的命令

如果您想要...	使用此命令...
顯示節點中所有啟動器及其介面卡的資訊	`run -node node_name storage show adapter`
顯示介面卡組態與狀態	`run -node node_name sysconfig -v adapter`
驗證安裝了哪些擴充卡、以及是否有任何組態錯誤	`run -node node_name sysconfig -ac`

用於管理內建**FC**介面卡的命令

如果您想要...	使用此命令...
顯示內建FC連接埠的狀態	`system node hardware unified-connect show`

相關資訊

- "網路 FCP 介面卡"

使用 **X1133A-R6** 介面卡，避免與 **ONTAP** 系統的連線中斷

您可以使用備援路徑將系統設定為獨立的X1133A-R6 HBA、以避免在連接埠故障時中斷連線。

X1133A-R6 HBA是一個4埠、16 GB FC介面卡、由兩個2埠配對組成。X1133A-R6介面卡可設定為目標模式或啟動器模式。每個2埠配對都由單一ASIC支援（例如、ASIC 1上的連接埠1和連接埠2、ASIC 2上的連接埠3和連接埠4）。單一ASIC上的兩個連接埠都必須設定為以相同模式運作、無論是目標模式或啟動器模式。如果ASIC支援配對時發生錯誤、配對中的兩個連接埠都會離線。

為了避免這種連線中斷、您可以設定系統的備援路徑來分隔X1133A-R6 HBA、或是使用備援路徑來連接至HBA上不同的ASIC所支援的連接埠。

FCoE 組態

使用 **ONTAP** 系統設定 **FCoE** 架構

FCoE可透過各種方式使用FCoE交換器進行設定。FCoE不支援直接附加組態。

所有FCoE組態都是雙網路、完全備援、而且需要主機端的多重路徑軟體。在所有FCoE組態中、您可以在啟動器和目標之間的路徑中有多個FCoE和FC交換器、最高可達跳數上限。若要將交換器彼此連線、交換器必須執行支援乙太網路ISL的韌體版本。任何FCoE組態中的每個主機都可以設定不同的作業系統。

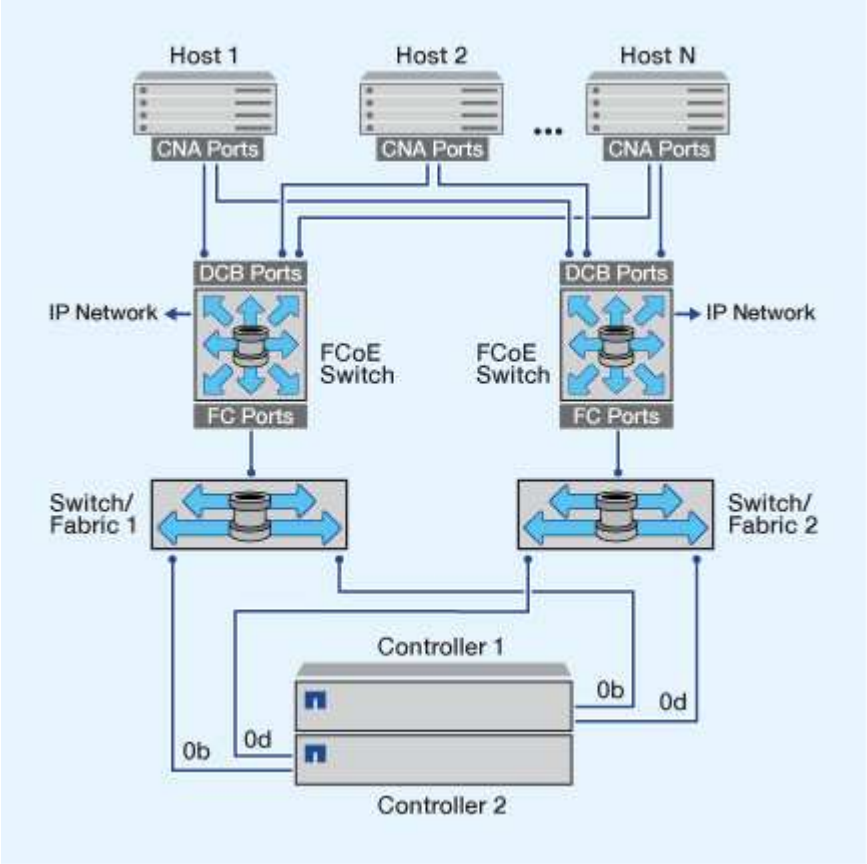
FCoE組態需要明確支援FCoE功能的乙太網路交換器。FCoE組態是透過與FC交換器相同的互通性與品質保證程序來驗證。支援的組態列於互通性對照表中。這些支援組態中包含的部分參數包括交換器機型、可部署在單一架構中的交換器數量、以及支援的交換器韌體版本。

圖示中的FC目標擴充介面卡連接埠編號為範例。實際的連接埠編號可能有所不同、視安裝FCoE目標擴充介面卡的擴充插槽而定。

FCoE啟動器至FC目標

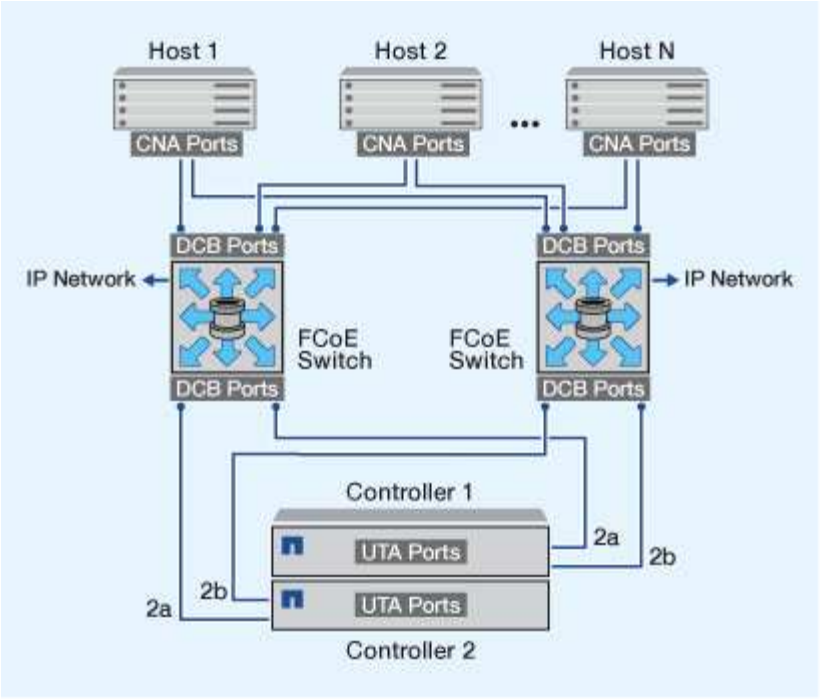
使用FCoE啟動器（CNA）、您可以透過FCoE交換器、將主機連線至HA配對中的兩個控制器、並連接至FC目標連接埠。FCoE交換器也必須具有FC連接埠。主機FCoE啟動器一律會連線至FCoE交換器。FCoE交換器可直接連線至FC目標、或透過FC交換器連線至FC目標。

下圖顯示連接至FCoE交換器的主機CNA、以及連接至HA配對之前連接至FC交換器的主機CNA：



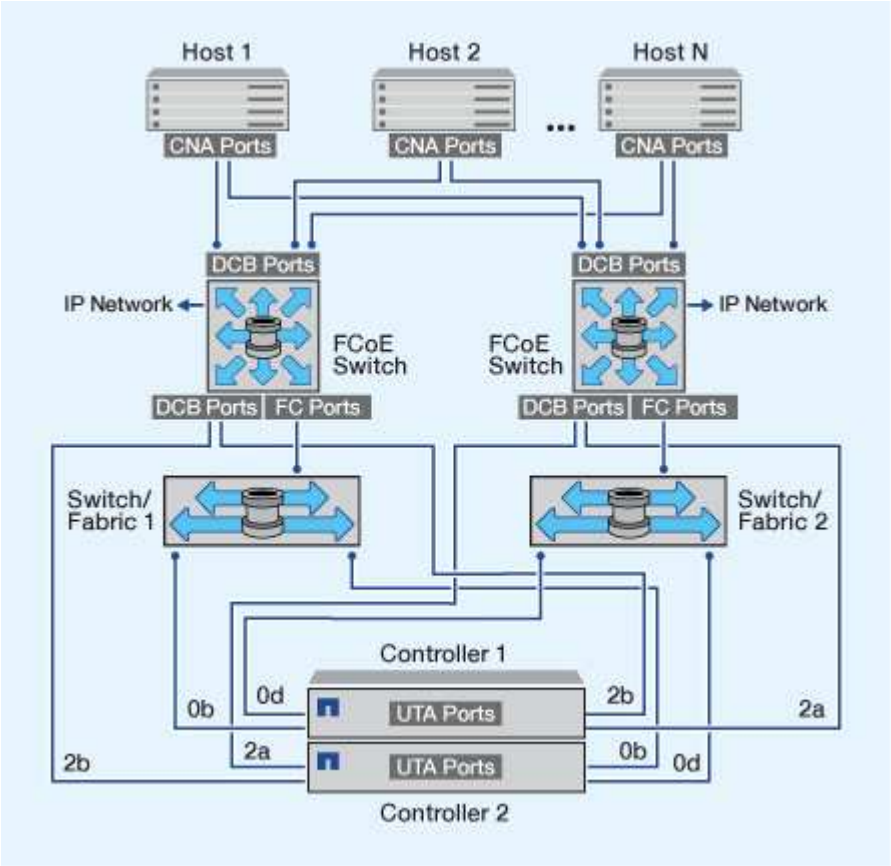
FCoE啟動器至FCoE目標

使用主機FCoE啟動器（CNA）、您可以透過FCoE交換器、將主機連接至HA配對中的兩個控制器、並連接至FCoE目標連接埠（也稱為UTA或UTA2）。



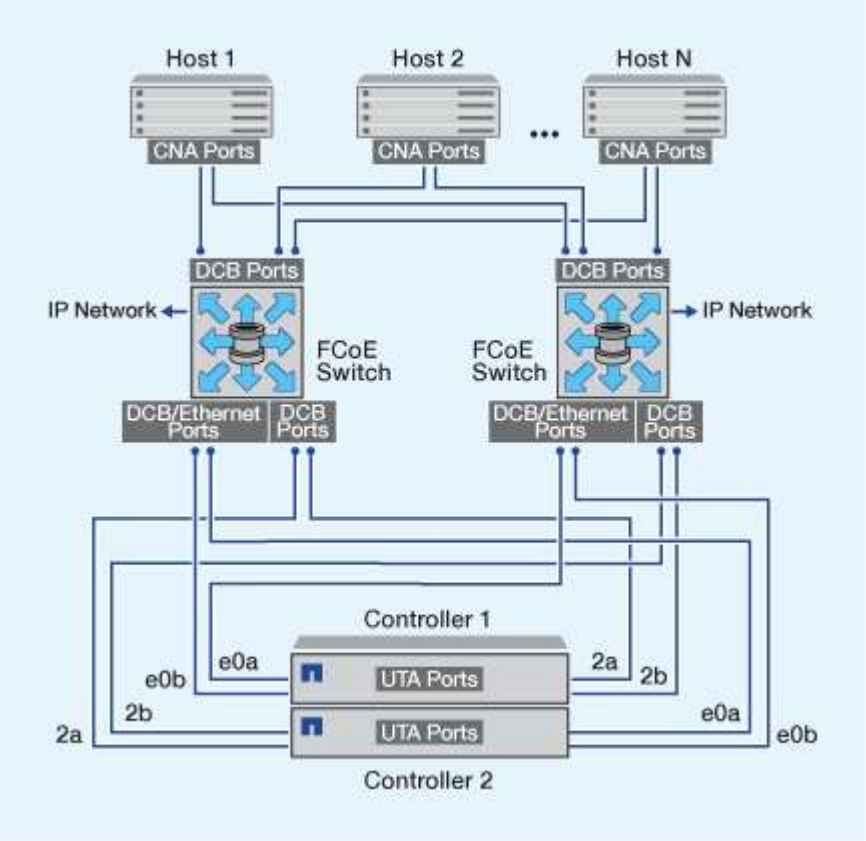
FCoE啟動器至**FCoE**和**FC**目標

使用主機FCoE啟動器（CNA）、您可以透過FCoE交換器、將主機連接至HA配對中的兩個控制器、以及FC目標連接埠（也稱為UTA或UTA2）。



FCoE與IP儲存傳輸協定混合使用

使用主機FCoE啟動器（CNA）、您可以透過FCoE交換器、將主機連接至HA配對中的兩個控制器、並連接至FCoE目標連接埠（也稱為UTA或UTA2）。FCoE連接埠無法使用傳統連結集合到單一交換器。Cisco交換器支援一種特殊類型的連結集合（虛擬連接埠通道）、可支援FCoE。虛擬連接埠通道會將個別連結集合到兩個交換器。您也可以將虛擬連接埠通道用於其他乙太網路流量。用於FCoE以外流量的連接埠（包括NFS、SMB、iSCSI及其他乙太網路流量）可使用FCoE交換器上的一般乙太網路連接埠。



ONTAP 支援的 FCoE 啟動器和目標連接埠組合

支援FCoE與傳統FC啟動器和目標的特定組合。

FCoE啟動器

您可以在主機電腦中使用FCoE啟動器、並在儲存控制器中同時使用FCoE和傳統FC目標。主機FCoE啟動器必須連線至FCoE DCB（資料中心橋接）交換器、不支援直接連線至目標。

下表列出支援的組合：

啟動器	目標	是否支援？
FC	FC	是的
FC	FCoE	是的
FCoE	FC	是的

啟動器	目標	是否支援？
FCoE	FCoE	是的

FCoE目標

無論FC連接埠是附加目標介面卡或內建連接埠、您都可以在儲存控制器上混合使用4-GB、8-GB或16-GB FC連接埠。您可以在同一個儲存控制器中同時擁有FCoE和FC目標介面卡。

合併內建和擴充FC連接埠的規則仍適用。

FC 和 FCoE 分區

瞭解 ONTAP 系統的 FC 和 FCoE 分區

FC、FC-NVMe或FCoE區域是一個邏輯群組、由一個或多個光纖網路內的連接埠組成。若要讓裝置能夠彼此看到，彼此連線，建立工作階段，以及進行通訊，兩個連接埠都必須是相同區域的成員。

分區可限制存取及連線至共用同一區域的端點、進而提高安全性。不在同一區域中的連接埠無法彼此通訊。這可減少或消除啟動器 HBA 之間的串擾。如果發生連線問題，分區有助於將問題隔離到特定的連接埠集，進而縮短解決問題的時間。

分區可減少通往特定連接埠的可用路徑數量，並減少主機與儲存系統之間的路徑數量。例如、某些主機OS多重路徑解決方案對可管理的路徑數量有限制。分區可減少主機可見的路徑數量，使通往主機的路徑不會超過主機作業系統所允許的最大路徑數。

全球名稱型分區

分區根據全球名稱（WWN）指定要包含在區域內的成員的WWN。雖然有些交換器廠商可以使用全球節點名稱（ WWNN ）分區，但在 ONTAP 中分區時，您必須使用全球連接埠名稱（ WWPN ）分區。

必須使用 WWPN 分區，才能正確定義特定連接埠，並有效使用 NPIV 。FC 交換器應使用目標邏輯介面（生命體）的 WWPN 進行分區，而非節點上實體連接埠的 WWPN 。實體連接埠的WWPN以「50」開頭、而LIF的WWPN則以「20」開頭。

WWPN分區可提供靈活度、因為存取不取決於裝置實體連接至網路的位置。您可以將纜線從一個連接埠移至另一個連接埠、而不需重新設定區域。

ONTAP 系統的建議 FC 和 FCoE 分區組態

如果您的主機未安裝多重路徑解決方案，四部或更多主機已連線至 SAN ，或叢集中的節點未實作選擇性 LUN 對應，則應建立分區組態。

在建議的 FC 和 FCoE 分區組態中，每個區域都包含一個啟動器連接埠和一個或多個目標生命體。此組態可讓每個主機啟動器存取任何節點，同時防止存取相同節點的主機看到彼此的連接埠

使用主機啟動器將儲存虛擬機器（ SVM ）的所有生命體新增至區域。這可讓您在不編輯現有區域或建立新區域的情況下、移動磁碟區或LUN。

雙 **Fabric** 分區組態

建議使用雙 Fabric 分區組態，因為它們可防止單一元件故障造成的資料遺失。在雙 Fabric 組態中，每個主機啟動器都會使用不同的交換器連接到叢集中的每個節點。如果有一台交換器無法使用，則資料存取會透過其餘的交換器進行維護。主機需要多重路徑軟體來管理多個路徑。

在下圖中、主機有兩個啟動器、並執行多重路徑軟體。共有兩個區域。"選擇性 LUN 對應（ SLM ）"已設定為將所有節點視為報告節點。

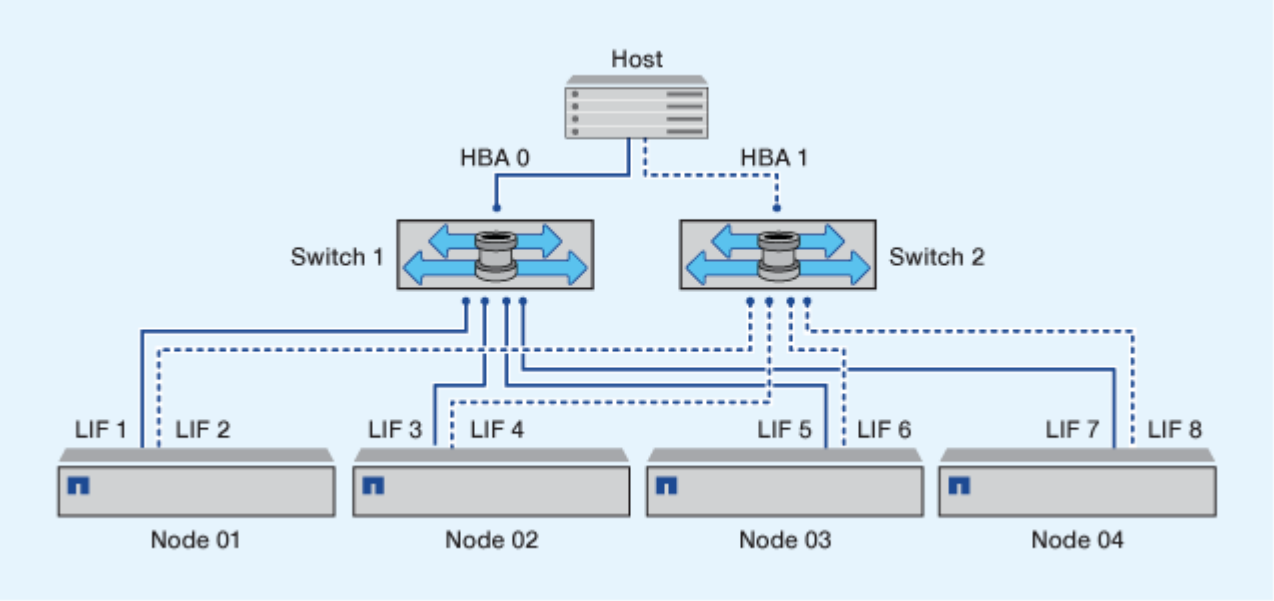
本圖所使用的命名慣例只是一項建議、您可以選擇使用其中一種命名慣例來搭配ONTAP 您的解決方案。

- 區域 1 ： HBA 0 、 LIF_1 、 LIF_3 、 LIF_5 和 LIF_7
- 區域 2 ： HBA 1 、 LIF_2 、 LIF_4 、 LIF_6 和 LIF_8

每個主機啟動器都會透過不同的交換器分區。區域1可透過交換器1存取。區域 2 可透過交換器 2 存取。

每個主機都可以存取每個節點上的 LIF 。如此一來、當節點故障時、主機仍可存取其LUN。SVM 可根據您的 SLM 報告節點組態，存取叢集中每個節點上的所有 iSCSI 和 FC 生命。您可以使用「SLM」、「連接埠集」或「FC交換器分區」來減少從SVM到主機的路徑數目、以及從SVM到LUN的路徑數目。

如果組態包含更多節點，則這些區域中會包含額外節點的生命負載。



主機作業系統和多重路徑軟體必須支援用於存取節點上LUN的路徑數量。

單一網路分區

在單一架構組態中，您可以透過單一交換器，將每個主機啟動器連接至每個儲存節點。不建議使用單一架構分區組態，因為單一元件故障無法防止資料遺失。如果您選擇設定單一架構分區，則每部主機都應該有兩個啟動器用於多重路徑，以在解決方案中提供恢復能力。主機需要多重路徑軟體來管理多個路徑。

每個主機啟動器至少應從啟動器可存取的每個節點中擁有一個 LIF 。分區應至少允許一條路徑從主機啟動器到叢集中的HA節點配對、以提供LUN連線的路徑。這表示主機上的每個啟動器在其區域組態中、每個節點可能只有一個目標LIF。如果叢集中的同一個節點或多個節點需要多重路徑、則每個節點在其區域組態中都會有多個生命

區。如此一來、當節點故障或包含LUN的磁碟區移至不同節點時、主機仍可存取其LUN。這也需要適當設定報告節點。

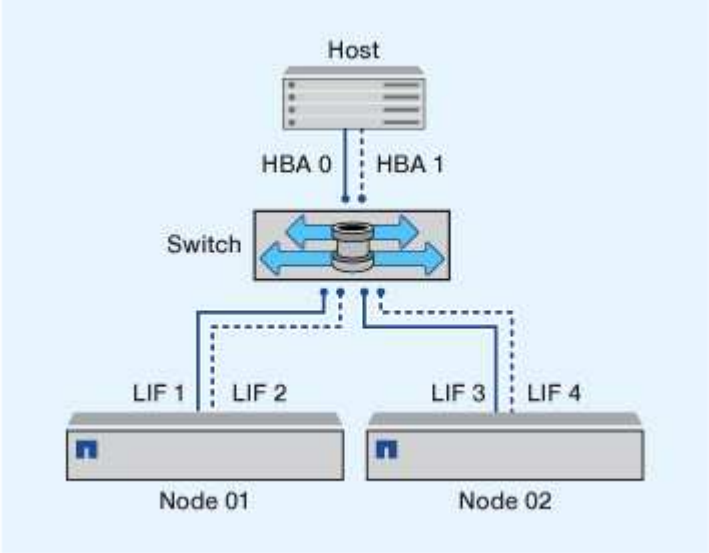
使用Cisco FC和FCoE交換器時、同一個實體連接埠的單一網路區域不得包含多個目標LIF。如果同一個連接埠上有多個LIF連接埠位於同一個區域、則LIF連接埠可能無法從連線中斷中恢復。

在下圖中、主機有兩個啟動器、並執行多重路徑軟體。共有兩個區域：

本圖所使用的命名慣例只是一項建議、您可以選擇使用其中一種命名慣例來搭配ONTAP 您的解決方案。

- 區域1：HBA 0、LIF_1和LIF_3
- 區域 2 ： HBA 1 、 LIF_2 和 LIF_4

如果組態包含更多節點，則這些區域中會包含額外節點的生命負載



在此範例中、您也可以在每個區域中擁有全部四個生命區。在這種情況下、區域如下：

- 區域1：HBA 0、LIF_1、LIF_2、LIF_3和LIF_4
- 區域 2 ： HBA 1 、 LIF_1 、 LIF_2 、 LIF_3 和 LIF_4

主機作業系統和多重路徑軟體必須支援用於存取節點上LUN的支援路徑數量。若要判斷用於存取節點上LUN的路徑數目、請參閱SAN組態限制一節。

Cisco FC和FCoE交換器的分區限制

使用 Cisco FC 和 FCoE 交換器時，某些限制會套用至區域中的實體連接埠和邏輯介面（生命體）。

實體連接埠

- FC-NVMe 和 FC 可以共用相同的 32 GB 實體連接埠
- FC-NVMe 和 FCoE 無法共用相同的實體連接埠
- FC 和 FCoE 可以共用相同的實體連接埠，但其通訊協定生命體必須位於不同的區域。

邏輯介面（生命）

- 區域可以包含來自叢集中每個目標連接埠的 LIF 。

  驗證 SLM 組態，以避免超過允許的主機路徑數量上限。

- 指定連接埠上的每個 LIF 都必須與該連接埠上的其他生命體位於不同的區域
- 不同實體連接埠上的LIF可以位於同一個區域。

連線至 **ONTAP** 和非 **NetApp** 系統的 **SAN** 主機需求

共享的SAN組態定義為同時連接ONTAP 到NetApp儲存系統和其他廠商儲存系統的主機。只要符合多項需求、即可從單一主機存取ONTAP 功能、以及其他廠商的儲存系統。

對於所有的主機作業系統、最佳做法是使用個別的介面卡來連接每個廠商的儲存系統。使用獨立的介面卡可降低驅動程式與設定之間發生衝突的機率。若要連線ONTAP 至某個不支援的儲存系統、介面卡型號、BIOS、韌體和驅動程式必須列於NetApp互通性對照表工具中。

您應該為主機設定必要或建議的逾時值及其他儲存參數。您必須始終安裝NetApp軟體、或是最後套用NetApp設定。

- 對於AIX、您應該套用「互通性對照表工具」中所列之AIX主機公用程式版本的值、以供您的組態使用。
- 對於ESX、您應該使用VMware vSphere的虛擬儲存主控台來套用主機設定。
- 對於HP-UX、您應該使用HP-UX預設儲存設定。
- 對於Linux、您應該針對您的組態、套用Interoperability Matrix Tool（互通性對照表工具）中所列Linux主機公用程式版本的值。
- 對於Solaris、您應該針對您的組態、套用Interoperability Matrix Tool中所列之Solaris Host Utilities版本的值。
- 對於Windows、您應該針對組態安裝Interoperability Matrix Tool中列出的Windows主機公用程式版本。

相關資訊

"NetApp 互通性對照表工具"

SAN組態MetroCluster

ONTAP MetroCluster 環境中支援的 **SAN** 組態

在MetroCluster 使用SAN組態時、您必須注意某些考量因素、才能在支援環境中使用SAN組態。

- 支援的不支援前端FC架構「'route'」vSAN組態。MetroCluster
- 從 ONTAP 9.15.1 開始、 NVMe / TCP 支援四節點 MetroCluster IP 組態。
- 從版本號為209.12.1開始ONTAP 、MetroCluster NVMe / FC支援四節點的「靜態IP」組態。ONTAP 9.12.1之前的前端 NVMe 網路不支援 MetroCluster 組態。
- 其他SAN傳輸協定、例如iSCSI、FC和FCoE、均支援MetroCluster 在各種組態上。
- 使用SAN用戶端組態時、您必須檢查MetroCluster 中所提供的附註中是否包含任何關於功能組態的特殊考量 "NetApp 互通性對照表工具" （僅限部分）IMT 。

- 作業系統和應用程式必須提供120秒的I/O恢復能力、才能支援MetroCluster 非計畫性自動切換、以及斷路器或調解器啟動的切換。
- MetroCluster 組態在前端 FC 架構的兩側使用相同的 WWNN 和 WWPN 。

相關資訊

- "瞭MetroCluster 解資料保護與災難恢復"
- "NetApp知識庫： MetroCluster設定中 AIX 主機支援注意事項有哪些？"
- "NetApp知識庫： MetroCluster配置中的 Solaris 主機支援注意事項"

避免在 **ONTAP MetroCluster** 切換和切換期間連接埠重疊

在SAN環境中、您可以設定前端交換器、以避免舊連接埠離線且新連接埠上線時發生重疊。

在切換期間、在Fabric偵測到災難站台上的FC連接埠離線且已從名稱和目錄服務中移除此連接埠之前、仍在運作中的站台上的FC連接埠可能會登入Fabric。

如果災難上的FC連接埠尚未移除、則在正常運作站台上、FC連接埠的Fabric登入嘗試可能會因為WWPN重複而遭到拒絕。FC交換器的這種行為可以變更、以認可先前裝置的登入、而非現有裝置的登入。您應該驗證此行為對其他Fabric裝置的影響。如需詳細資訊、請聯絡交換器廠商。

根據交換器類型選擇正確的程序。

範例 **22.** 步驟

Cisco交換器

1. 連線至交換器並登入。
2. 進入組態模式：

```
switch# config t
switch(config)#
```

3. 使用新裝置覆寫名稱伺服器資料庫中的第一個裝置項目：

```
switch(config)# no fcns reject-duplicate-pwwn vsan 1
```

4. 在執行NX-OS 8.x的交換器中、確認FLOGI靜止逾時設定為零：

   a. 顯示靜止時間服務：

   ```
   switch(config)# show flogi interval info \| i quiesce
   ```

   ```
   Stats:  fs flogi quiesce timerval:  0
   ```

   b. 如果上一個步驟的輸出並未指出timerval為零、請將其設為零：

   ```
   switch(config)# flogi scale enable
   ```

```
switch(config)$ flogi quiesce timeout 0
```

Brocade交換器

1. 連線至交換器並登入。
2. 輸入 `switchDisable` 命令。
3. 輸入 `configure` 命令、然後按 `y` 出現提示時。

```
 F-Port login parameters (yes, y, no, n): [no] y
```

4. 選擇設定1：

```
- 0: First login take precedence over the second login (default)
- 1: Second login overrides first login.
- 2: the port type determines the behavior
Enforce FLOGI/FDISC login: (0..2) [0] 1
```

5. 回應其餘的提示、或按* Ctrl + D*。
6. 輸入 `switchEnable` 命令。

相關資訊

"執行測試或維護的切換"

ONTAP 支援 SAN 主機多重路徑功能

ONTAP 使用非對稱式邏輯單元存取（ ALUA ）軟體來處理 FC 和 iSCSI 主機的多重路徑。

從 ONTAP 9.5 多重路徑高可用度（ HA ）配對容錯移轉 / 恢復開始，就支援使用非同步命名空間存取（ ANA ）的 NVMe 主機。在 ONTAP 9.4 中， NVMe 只支援從主機到目標的一條路徑，因此應用程式主機必須管理通往 HA 合作夥伴的路徑容錯移轉。

如果您的 SAN 主機可以透過多個路徑存取 LUN 或 NVMe 命名空間，則需要多重路徑軟體。它為作業系統提供單一磁碟，用於通往 LUN 或 NVMe 命名空間的所有路徑。如果沒有它，作業系統就可以將每個路徑視為獨立的磁碟，導致資料毀損。

如果您有下列任一項、您的解決方案就會被視為具有多個路徑：

- 主機中的單一啟動器連接埠、連接到SVM中的多個SAN LIF
- 多個啟動器連接埠、連接至SVM中的單一SAN LIF
- 多個啟動器連接埠連接至SVM中的多個SAN LIF

HA 組態建議使用多重路徑軟體，也稱為 MPIO （多重路徑 I/O ）軟體。除了選擇性 LUN 對應之外，我們也建議使用 FC 交換器分區或連接埠集來限制用於存取 LUN 的路徑。

如需哪些特定主機組態支援ALUA或ANA的相關資訊、請參閱 "NetApp 互通性對照表工具" 和 "SAN主機組態ONTAP" 適用於您的主機作業系統。

從主機到叢集中節點的建議路徑數

從主機到叢集中每個節點的路徑不得超過八條。您也不應超過主機作業系統可支援的路徑總數，以及主機上使用的多重路徑。

每個 LUN 至少應有兩條路徑，透過叢集中的儲存虛擬機器（ SVM ）使用，連接至每個報告節點"選擇性LUN對應（SLM)"。如此可消除單點故障、並讓系統在元件故障時仍能繼續運作。

如果叢集中有四個以上的節點、或是任一節點中的SVM使用四個以上的目標連接埠、 您可以使用下列方法來限制可用於存取節點上LUN的路徑數目、以避免超過建議的八個路徑上限。

- SLM

  在擁有LUN的節點上、以及擁有節點的HA合作夥伴、透過SLMs減少從主機到LUN的路徑數量、只能達到路徑。根據預設、會啟用SLM.

- "適用於iSCSI的PortSet"
- 主機的FC igroup對應

- FC交換器分區

組態限制

確定每個 **ONTAP** 叢集支援的節點和 **SAN** 主機數量上限

每個叢集所支援的節點數量會因您的 ONTAP 版本，控制器機型和叢集節點的傳輸協定而異。可連線至叢集的 SAN 主機數量上限也會因您的特定組態而異。

確定每個叢集支援的節點數上限

如果叢集中的任何節點是針對FC、FC-NVMe、FCoE或iSCSI進行設定、則該叢集僅限於SAN節點限制。根據叢集中控制器的節點限制列於_E__ Hardware Universe 。

步驟

1. 前往 "NetApp Hardware Universe"。
2. 在左上角的 * 首頁 * 旁，選取 * 平台 * ，然後選取平台類型。
3. 選取您的 ONTAP 版本。

   系統會顯示新欄、供您選擇平台。
4. 選擇解決方案中使用的平台。
5. 在 * 選擇您的規格 * 下，取消選取 * 全選 * 。
6. 選擇 * 每個叢集的最大節點數（ NAS/SAN ） * 。
7. 按一下*顯示結果*。

結果

畫面會顯示所選平台的每個叢集節點數上限。

確定您的叢集是否支援更多 **FC** 主機

對於FC和FC-NVMe組態、您應該使用系統中啟動器目標節點（ITN）的數量、來判斷是否可以將更多主機新增至叢集。

ITN代表從主機啟動器到儲存系統目標的一條路徑。FC和FC-NVMe組態中每個節點的ITN數目上限為2、048。如果您低於 ITN 的最大數量，您可以繼續將主機新增至叢集。

若要判斷叢集中使用的ITN數量、請針對叢集中的每個節點執行下列步驟。

步驟

1. 識別指定節點上的所有生命體。
2. 針對節點上的每個LIF執行下列命令：

   ```
   fcp initiator show -fields wwpn, lif
   ```

   命令輸出底部顯示的項目數代表該LIF的ITN數目。

3. 記錄每個LIF顯示的ITN數目。
4. 在叢集中的每個節點上新增每個LIF的ITN數目。

   此總計代表叢集內的ITN數目。

確定您的叢集是否支援更多 **iSCSI** 主機

可直接連線至節點、或可透過一或多個交換器連線的主機數量、取決於可用的乙太網路連接埠數量。可用的乙太網路連接埠數量取決於控制器的機型、以及控制器中安裝的介面卡數量和類型。控制器和介面卡支援的乙太網路連接埠數量可在_E__中找到Hardware Universe 。

對於所有的多節點叢集組態、您必須決定每個節點的iSCSI工作階段數目、以瞭解是否可以將更多主機新增至叢集。只要叢集低於每個節點的iSCSI工作階段上限、您就可以繼續將主機新增至叢集。每個節點的iSCSI工作階段數目上限會因叢集中的控制器類型而異。

步驟

1. 識別節點上的所有目標入口網站群組。
2. 檢查節點上每個目標入口網站群組的iSCSI工作階段數目：

   ```
   iscsi session show -tpgroup _tpgroup_
   ```

   命令輸出底部所顯示的項目數、代表您針對該目標入口網站群組所進行的iSCSI工作階段數目。
3. 記錄每個目標入口網站群組所顯示的iSCSI工作階段數目。
4. 新增節點上每個目標入口網站群組的iSCSI工作階段數目。

   總計代表節點上的iSCSI工作階段數目。

All Flash SAN Array 組態限制與支援

All Flash SAN Array （ ASA ）組態限制與支援因 ONTAP 版本而異。

如需支援組態限制的最新詳細資料、請參閱 "NetApp Hardware Universe"。

> 這些限制適用於 ASA 系統。如果您有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請參閱"ASA R2 系統儲存限制"。

每個叢集的 **SAN** 傳輸協定和支援節點數

支援的 SAN 傳輸協定和每個叢集的最大節點數取決於您是否有非 MetroCluster 或 MetroCluster 組態：

非**MetroCluster**組態

下表顯示 ASA 對 SAN 通訊協定的支援、以及非 MetroCluster 組態中每個叢集支援的節點數：

從**ONTAP** 無到無...開始	傳輸協定支援	每個叢集的最大節點數
9.11.1.	• NVMe / TCP • NVMe / FC	12.
9.10.1	• NVMe / TCP	2.
9.9.1	• NVMe / FC	2.
	• FC • iSCSI	12.
9.7%	• FC • iSCSI	2.

IP組態**MetroCluster**

下表顯示 ASA 對 SAN 通訊協定的支援、以及 MetroCluster IP 組態中每個叢集支援的節點數：

從**ONTAP** 無到無...開始	傳輸協定支援	每個叢集的最大節點數
9.15.1..	• NVMe / TCP	四節點 MetroCluster IP 組態中的每個叢集 2 個節點
9.12.1	• NVMe / FC	四節點 MetroCluster IP 組態中的每個叢集 2 個節點
9.9.1	• FC • iSCSI	8 節點 MetroCluster IP 組態中的每個叢集 4 個節點
9.7%	• FC • iSCSI	四節點 MetroCluster IP 組態中的每個叢集 2 個節點

支援持續連接埠

從 ONTAP 9.8 開始、在設定為使用 FC 傳輸協定的 All Flash SAN 陣列（ ASA ）上、預設會啟用持續連接埠。持續連接埠僅適用於FC、且需要由全球連接埠名稱（WWPN）識別的區域成員資格。

持續連接埠可在高可用度（ HA ）合作夥伴的對應實體連接埠上建立陰影 LIF 、藉此降低移轉的影響。接管節點時、合作夥伴節點上的陰影LIF會採用原始LIF的身分識別、包括WWPNe。在將接管節點的路徑狀態變更為故障之前、陰影LIF會顯示為通往主機MPIO堆疊的主動/最佳化路徑、並會移動I/O。如此可減少I/O中斷、因為即使在儲存容錯移轉作業期間、主機仍會看到相同數量的目標路徑。

對於持續連接埠、HA配對內的下列FCP連接埠特性應該相同：

- FCP連接埠數
- FCP連接埠名稱
- FCP連接埠速度
- FCP LIF WWPN型分區

如果HA配對中有任何特性不相同、就會產生下列EMS訊息：

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

如需持續連接埠的詳細資訊，請參閱"NetApp 技術報告 4080 ：現代 SAN 的最佳實務做法"。

與 **ONTAP** 系統搭配使用的 **FC** 交換器組態限制

Fibre Channel交換器具有最大組態限制、包括每個連接埠、連接埠群組、刀鋒伺服器和交換器所支援的登入次數。交換器廠商會記錄其支援的限制。

每個FC邏輯介面（LIF）都會登入FC交換器連接埠。從節點上的單一目標登入的總次數等於生命量加上基礎實體連接埠的一次登入。請勿超過交換器廠商的登入組態限制或其他組態值。這也適用於在啟用NPIV的虛擬化環境中、主機端使用的啟動器。對於解決方案中使用的目標或啟動器、切勿超過交換器廠商的登入組態限制。

Brocade交換器限制

您可以在_Brocade擴充性指南_中找到Brocade交換器的組態限制。

Cisco Systems交換器限制

您可以在中找到Cisco交換器的組態限制 "Cisco組態限制" Cisco交換器軟體版本指南。

ONTAP 支援的 **FC** 與 **FCoE** 躍點數上限

跳數定義為啟動器（主機）與目標（儲存系統）之間路徑中的交換器數目。主機與儲存系統之間支援的 FC 跳數上限會因交換器供應商而異。

Cisco Systems的文件也將此值稱為SAN架構的_管徑_。

對於FCoE、您可以將FCoE交換器連接至FC交換器。對於端點對端點FCoE連線、FCoE交換器必須執行支援乙太網路交換器間連結（ISL）的韌體版本。

交換器供應商	支援的躍點數
Brocade	• 7適用於FC • 5個FCoE
Cisco	• 7適用於FC • 多達3個交換器可以是FCoE交換器。

計算 **ONTAP FC** 主機的佇列深度

您可能需要調整主機上的FC佇列深度、以達到每個節點和FC連接埠Fan-in的ITN最大值。LUN的最大數目和可連線至FC連接埠的HBA數目、會受到FC目標連接埠上可用佇列深度的限制。

關於這項工作

佇列深度是指一次可在儲存控制器上排入佇列的I/O要求數（SCSI命令）。從主機啟動器HBA到儲存控制器目標介面卡的每個I/O要求都會使用佇列項目。一般而言、較高的佇列深度等於較佳的效能。但是、如果儲存控制器達到最大佇列深度、則儲存控制器會傳回QFULL回應來拒絕傳入命令。如果有大量主機正在存取儲存控制器、您應該謹慎規劃、避免QFULL情況、這會大幅降低系統效能、並可能導致某些系統發生錯誤。

在具有多個啟動器（主機）的組態中、所有主機的佇列深度都應該相似。由於透過相同目標連接埠連接至儲存控制器的主機之間佇列深度不均、因此佇列深度較小的主機無法存取佇列深度較大的主機所提供的資源。

以下是「t調整」佇列深度的一般建議：

- 對於中小型系統、請使用32個HBA佇列深度。
- 對於大型系統、請使用128個HBA佇列深度。
- 對於例外情況或效能測試、請使用佇列深度256以避免可能的佇列問題。
- 所有主機都應將佇列深度設定為類似值、以提供對所有主機的同等存取權。
- 為了避免效能損失或錯誤、儲存控制器的目標FC連接埠佇列深度不可超過。

步驟

1. 計算連接到一個FC目標連接埠之所有主機中的FC啟動器總數。
2. 乘以128。
   - 如果結果小於2、048、請將所有啟動器的佇列深度設為128。
     您有15台主機、其中一台啟動器連接至儲存控制器上的兩個目標連接埠。15 x 128 = 1、920。由於1、920低於總佇列深度限制2、048、因此您可以將所有啟動器的佇列深度設定為128。
   - 如果結果大於2、048、請前往步驟3。
     您有 30 部主機、其中一個啟動器連接至儲存控制器上的兩個目標連接埠。30 x 128 = 3、840。因為3、840大於佇列深度總限制2、048、所以您應該在步驟3下選擇其中一個選項進行補救。
3. 請選擇下列其中一個選項、將更多主機新增至儲存控制器。
   - 選項1：
     i. 新增更多FC目標連接埠。
     ii. 重新分配FC啟動器。
     iii. 重複步驟 1 和 2 。

     所需的佇列深度3、840超過每個連接埠的可用佇列深度。若要解決此問題、您可以將雙埠FC目標介面卡新增至每個控制器、然後重新分區FC交換器、讓30部主機中的15部連接至一組連接埠、其餘15部主機則連接至第二組連接埠。接著、每個連接埠的佇列深度減至15 x 128 = 1、920。
   - 選項 2 ：
     i. 根據預期的I/O需求、將每個主機指定為「大型」或「大型」。
     ii. 將大型啟動器的數量乘以128。

iii. 將小型啟動器的數量乘以32。

iv. 將兩個結果一起新增。

v. 如果結果小於2、048、請將大型主機的佇列深度設為128、而小型主機的佇列深度設為32。

vi. 如果結果仍大於每個連接埠2、048、請減少每個啟動器的佇列深度、直到佇列總深度小於或等於2、048為止。

若要預估達到特定每秒I/O處理量所需的佇列深度、請使用下列公式：

所需佇列深度=（每秒I/O數）x（回應時間）

例如、如果回應時間為3毫秒、每秒需要40、000 I/O、則所需佇列深度= 40、000 x（.003）= 120。

如果您決定將佇列深度限制為基本建議32、則可連線至目標連接埠的主機數量上限為64。不過、如果您決定佇列深度為128、則最多可將16台主機連接至一個目標連接埠。佇列深度越大、單一目標連接埠可支援的主機就越少。如果您的需求無法影響佇列深度、則應該有更多目標連接埠。

所需的佇列深度3、840超過每個連接埠的可用佇列深度。您有10台「大型」主機具有高儲存I/O需求、20台「大型」主機的I/O需求較低。將大型主機上的啟動器佇列深度設為128、並將小型主機上的啟動器佇列深度設為32。

您產生的佇列總深度為（10 x 128）+（20 x 32）= 1、920。

您可以在每個啟動器之間平均分配可用的佇列深度。

每個啟動器產生的佇列深度為2、048÷30 = 68。

修改 **ONTAP SAN** 主機的佇列深度

您可能需要變更主機上的佇列深度，以達到每個節點的 ITN 和 FC 連接埠的最大風扇輸入值。您可以"計算最佳佇列深度"為環境設定。

AIX主機

您可以使用變更 AIX 主機上的佇列深度 `chdev` 命令。使用所做的變更 `chdev` 命令會在重新開機後持續存在。

範例：

- 若要變更hdisk7裝置的佇列深度、請使用下列命令：

  ```
  chdev -l hdisk7 -a queue_depth=32
  ```

- 若要變更fcs0 HBA的佇列深度、請使用下列命令：

  ```
  chdev -l fcs0 -a num_cmd_elems=128
  ```

  的預設值 `num_cmd_elems` 為 200 。最大值為2、048。

可能需要將 HBA 離線才能變更 `num_cmd_elems` 然後使用重新上線 `rmdev -l fcs0 -R` 和 `makdev -l fcs0 -P` 命令。

HP-UX主機

您可以使用核心參數變更 HP-UX 主機上的 LUN 或裝置佇列深度 `scsi_max_qdepth`。您可以使用核心參數變更 HBA 佇列深度 `max_fcp_reqs`。

- 的預設值 `scsi_max_qdepth` 為 8 。最大值為 255 。

  `scsi_max_qdepth` 可以使用在執行中的系統上動態變更 `-u` 選項 `kmtune` 命令。變更將對系統上的所有裝置生效。例如、使用下列命令將LUN佇列深度增加至64：

  ```
  kmtune -u -s scsi_max_qdepth=64
  ```

  您可以使用變更個別裝置檔案的佇列深度 `scsictl` 命令。使用進行變更 `scsictl` 命令在系統重新開機後不會持續執行。若要檢視及變更特定裝置檔案的佇列深度、請執行下列命令：

  ```
  scsictl -a /dev/rdsk/c2t2d0

  scsictl -m queue_depth=16 /dev/rdsk/c2t2d0
  ```

- 的預設值 `max_fcp_reqs` 為 512 。最大值為1024。

  必須重新建立核心、系統必須重新開機才能變更 `max_fcp_reqs` 以生效。例如、若要將HBA佇列深度變更為256、請使用下列命令：

  ```
  kmtune -u -s max_fcp_reqs=256
  ```

Solaris主機

您可以為Solaris主機設定LUN和HBA佇列深度。

- 對於LUN佇列深度：主機上使用的LUN數目乘以每LUN節流（LUN佇列深度）、必須小於或等於主機上的tgt-queue-深度 值。
- 對於 Sun 堆疊中的佇列深度：原生驅動程式不允許每個 LUN 或每個目標使用 `max_throttle` HBA 層級的設定。設定的建議方法 `max_throttle` 原生驅動程式的值位於中的每個裝置類型（ VID_PID ）層級 `/kernel/drv/sd.conf` 和 `/kernel/drv/ssd.conf` 檔案：主機公用程式會將MPxIO組態的值設為64、將Veritas DMP組態的值設為8。

步驟

1. `# cd/kernel/drv`
2. `# vi lpfc.conf`
3. 搜尋 `/tft-queue (/tgt-queue)`

   ```
   tgt-queue-depth=32
   ```

   安裝時、預設值設為32。

4. 根據環境的組態設定所需的值。
5. 儲存檔案。
6. 使用重新啟動主機 `sync; sync; sync; reboot -- -r` 命令。

適用於**QLogic HBA**的**VMware**主機

使用 `esxcfg-module` 變更 HBA 逾時設定的命令。手動更新 `esx.conf` 不建議使用檔案。

步驟

1. 以root使用者身分登入服務主控台。
2. 使用 `#vmkload_mod -l` 用於驗證目前已載入哪個 Qlogic HBA 模組的命令。
3. 對於QLogic HBA的單一執行個體、請執行下列命令：

```
#esxcfg-module -s ql2xmaxqdepth=64 qla2300_707
```

> 此範例使用qla232_707模組。根據的輸出使用適當的模組 `vmkload_mod -l`。

4. 使用下列命令儲存變更：

```
#/usr/sbin/esxcfg-boot -b
```

5. 使用下列命令重新啟動伺服器：

```
#reboot
```

6. 使用下列命令確認變更：
   a. `#esxcfg-module -g qla2300_707`
   b. `qla2300_707 enabled = 1 options = 'ql2xmaxqdepth=64'`

適用於**Emulex HBA**的**VMware**主機

使用 `esxcfg-module` 變更 HBA 逾時設定的命令。手動更新 `esx.conf` 不建議使用檔案。

步驟

1. 以root使用者身分登入服務主控台。
2. 使用 `#vmkload_mod -l grep lpfc` 用於驗證當前裝入哪個 Emulex HBA 的命令。
3. 對於Emulex HBA的單一執行個體、請輸入下列命令：

```
#esxcfg-module -s lpfc0_lun_queue_depth=16 lpfcdd_7xx
```

> 視HBA機型而定、模組可以是lfcdd_7xx或lfcdd_732。上述命令使用lfcdd_7xx模組。您應該根據的結果使用適當的模組 `vmkload_mod -l`。

執行此命令會針對由lfc0代表的HBA、將LUN佇列深度設為16。

4. 對於Emulex HBA的多個執行個體、請執行下列命令：

```
a esxcfg-module -s "lpfc0_lun_queue_depth=16 lpfc1_lun_queue_depth=16"
lpfcdd_7xx
```

lffc0的LUN佇列深度和lffc1的LUN佇列深度設為16。

5. 輸入下列命令：

```
#esxcfg-boot -b
```

6. 使用重新開機 `#reboot`。

適用於**Emulex HBA**的**Windows**主機

在 Windows 主機上、您可以使用 `LPUTILNT` 用於更新 Emulex HBA 佇列深度的公用程式。

步驟

1. 執行 `LPUTILNT` 公用程式位於 `C:\WINNT\system32` 目錄。
2. 從右側的功能表中選取*磁碟機參數*。
3. 向下捲動並按兩下*「QuesteDepth*」。

> 如果您設定*「Queste深度」*大於150、則下列Windows登錄值也必須適當增加：
>
> `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\lpxnds\Parameters\Device\NumberOfRequests`

適用於邏輯**HBA**的**Windows**主機

在 Windows 主機上、您可以使用和 `SANsurfer` HBA 管理程式公用程式、可更新 Qlogic HBA 的佇列深度。

步驟

1. 執行 `SANsurfer` HBA 管理程式公用程式。
2. 按一下「* HBA連接埠*>*設定*」。
3. 按一下清單方塊中的*進階HBA連接埠設定*。
4. 更新 `Execution Throttle` 參數。

適用於**Emulex HBA**的**Linux**主機

您可以更新Linux主機上Emulex HBA的佇列深度。若要在重新開機後持續更新、您必須建立新的RAM磁碟映像、然後重新啟動主機。

步驟

1. 識別要修改的佇列深度參數：

```
modinfo lpfc|grep queue_depth
```

隨即顯示佇列深度參數及其說明清單。視作業系統版本而定、您可以修改下列一或多個佇列深度參數：

- `lpfc_lun_queue_depth`：可排入特定 LUN （ uint ）佇列的 FC 命令數目上限
- `lpfc_hba_queue_depth`：可以排入 lpfc HBA （ uint ）佇列的 FC 命令數目上限
- `lpfc_tgt_queue_depth`：可排入特定目標連接埠（ uint ）佇列的 FC 命令數目上限

  - `lpfc_tgt_queue_depth` 此參數僅適用於 Red Hat Enterprise Linux 7.x 系統、 SUSE Linux Enterprise Server 11 SP4 系統和 12.x 系統。

2. 將佇列深度參數新增至以更新佇列深度 `/etc/modprobe.conf` 適用於 Red Hat Enterprise Linux 5.x 系統和的檔案 `/etc/modprobe.d/scsi.conf` 適用於 Red Hat Enterprise Linux 6.x 或 7.x 系統、或 SUSE Linux Enterprise Server 11.x 或 12.x 系統的檔案。

   視作業系統版本而定、您可以新增下列一或多個命令：

   - `options lpfc lpfc_hba_queue_depth=new_queue_depth`
   - `options lpfc lpfc_lun_queue_depth=new_queue_depth`
   - `options lpfc_tgt_queue_depth=new_queue_depth`

3. 建立新的RAM磁碟映像、然後重新啟動主機、使更新在重新開機後持續更新。

   如需詳細資訊、請參閱 "系統管理" 適用於您的Linux作業系統版本。

4. 確認已針對您修改的每個佇列深度參數更新佇列深度值：

   ```
   root@localhost ~]#cat /sys/class/scsi_host/host5/lpfc_lun_queue_depth
         30
   ```

   此時會顯示佇列深度的目前值。

適用於**QLogic HBA**的**Linux**主機

您可以更新Linux主機上QLogic驅動程式的裝置佇列深度。若要在重新開機後持續更新、您必須建立新的RAM磁碟映像、然後重新啟動主機。您可以使用QLogic HBA管理GUI或命令列介面（CLI）來修改QLogic HBA佇列深度。

本工作說明如何使用QLogic HBA CLI來修改QLogic HBA佇列深度

步驟

1. 識別要修改的裝置佇列深度參數：

   ```
   modinfo qla2xxx | grep ql2xmaxqdepth
   ```

   您只能修改 `ql2xmaxqdepth` 佇列深度參數、表示可為每個 LUN 設定的最大佇列深度。RHEL 7.5及更新版本的預設值為64。RHEL 7.4及更早版本的預設值為32。

```
root@localhost ~]# modinfo qla2xxx|grep ql2xmaxqdepth
parm:       ql2xmaxqdepth:Maximum queue depth to set for each LUN.
Default is 64. (int)
```

2. 更新裝置佇列深度值：
   - 如果您要使修改持續進行、請執行下列步驟：
     i. 新增佇列深度參數至以更新佇列深度 `/etc/modprobe.conf` 適用於 Red Hat Enterprise Linux 5.x 系統和的檔案 `/etc/modprobe.d/scsi.conf` 適用於 Red Hat Enterprise Linux 6.x 或 7.x 系統、或 SUSE Linux Enterprise Server 11.x 或 12.x 系統的檔案： `options qla2xxx ql2xmaxqdepth=new_queue_depth`
     ii. 建立新的RAM磁碟映像、然後重新啟動主機、使更新在重新開機後持續更新。

     如需詳細資訊、請參閱 "系統管理" 適用於您的Linux作業系統版本。
   - 如果您只想修改目前工作階段的參數、請執行下列命令：

     `echo new_queue_depth > /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

     在下列範例中、佇列深度設為128。

```
echo 128 > /sys/module/qla2xxx/parameters/ql2xmaxqdepth
```

3. 確認佇列深度值已更新：

   `cat /sys/module/qla2xxx/parameters/ql2xmaxqdepth`

   此時會顯示佇列深度的目前值。

4. 更新韌體參數以修改 QLogic HBA 佇列深度 `Execution Throttle` 從 QLogic HBA BIOS 。
   a. 登入QLogic HBA管理CLI：

      `/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli`

   b. 從主功能表中、選取 `Adapter Configuration` 選項。

```
[root@localhost ~]#
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli
Using config file:
/opt/QLogic_Corporation/QConvergeConsoleCLI/qaucli.cfg
Installation directory: /opt/QLogic_Corporation/QConvergeConsoleCLI
Working dir: /root

QConvergeConsole

        CLI - Version 2.2.0 (Build 15)

    Main Menu

    1:  Adapter Information
    **2:  Adapter Configuration**
    3:  Adapter Updates
    4:  Adapter Diagnostics
    5:  Monitoring
    6:  FabricCache CLI
    7:  Refresh
    8:  Help
    9:  Exit


        Please Enter Selection: 2
```

c. 從介面卡組態參數清單中、選取 `HBA Parameters` 選項。

```
1:  Adapter Alias
    2:  Adapter Port Alias
    **3:  HBA Parameters**
    4:  Persistent Names (udev)
    5:  Boot Devices Configuration
    6:  Virtual Ports (NPIV)
    7:  Target Link Speed (iiDMA)
    8:  Export (Save) Configuration
    9:  Generate Reports
   10:  Personality
   11:  FEC
(p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 3
```

d. 從HBA連接埠清單中、選取所需的HBA連接埠。

```
Fibre Channel Adapter Configuration

    HBA Model QLE2562 SN: BFD1524C78510
      1: Port   1: WWPN: 21-00-00-24-FF-8D-98-E0 Online
      2: Port   2: WWPN: 21-00-00-24-FF-8D-98-E1 Online
    HBA Model QLE2672 SN: RFE1241G81915
      3: Port   1: WWPN: 21-00-00-0E-1E-09-B7-62 Online
      4: Port   2: WWPN: 21-00-00-0E-1E-09-B7-63 Online


        (p or 0: Previous Menu; m or 98: Main Menu; ex or 99: Quit)
        Please Enter Selection: 1
```

此時會顯示HBA連接埠的詳細資料。

e. 從 HBA 參數功能表中、選取 `Display HBA Parameters` 選項以檢視的目前值 `Execution Throttle` 選項。

的預設值 `Execution Throttle` 選項為 65535 。

```
HBA Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Display HBA Parameters
    2:  Configure HBA Parameters
    3:  Restore Defaults


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 1
-------------------------------------------------------------------------
--------
HBA Instance 2: QLE2562 Port 1 WWPN 21-00-00-24-FF-8D-98-E0 PortID 03-
07-00
Link: Online
```

```
--------------------------------------------------------------------------------
Connection Options              : 2 - Loop Preferred, Otherwise Point-to-
Point
Data Rate                       : Auto
Frame Size                      : 2048
Hard Loop ID                    : 0
Loop Reset Delay (seconds)      : 5
Enable Host HBA BIOS            : Enabled
Enable Hard Loop ID             : Disabled
Enable FC Tape Support          : Enabled
Operation Mode                  : 0 - Interrupt for every I/O completion
Interrupt Delay Timer (100us)   : 0
**Execution Throttle              : 65535**
Login Retry Count               : 8
Port Down Retry Count           : 30
Enable LIP Full Login           : Enabled
Link Down Timeout (seconds)     : 30
Enable Target Reset             : Enabled
LUNs Per Target                 : 128
Out Of Order Frame Assembly     : Disabled
Enable LR Ext. Credits          : Disabled
Enable Fabric Assigned WWN      : N/A

Press <Enter> to continue:
```

a. 按* Enter鍵*繼續。

b. 從 HBA 參數功能表中、選取 `Configure HBA Parameters` 修改 HBA 參數的選項。

c. 從「設定參數」功能表中、選取 `Execute Throttle` 選項並更新此參數的值。

```
Configure Parameters Menu

=====================================================
HBA           : 2 Port: 1
SN            : BFD1524C78510
HBA Model     : QLE2562
HBA Desc.     : QLE2562 PCI Express to 8Gb FC Dual Channel
FW Version    : 8.01.02
WWPN          : 21-00-00-24-FF-8D-98-E0
WWNN          : 20-00-00-24-FF-8D-98-E0
Link          : Online
=====================================================

    1:  Connection Options
    2:  Data Rate
    3:  Frame Size
    4:  Enable HBA Hard Loop ID
    5:  Hard Loop ID
    6:  Loop Reset Delay (seconds)
    7:  Enable BIOS
    8:  Enable Fibre Channel Tape Support
    9:  Operation Mode
   10:  Interrupt Delay Timer (100 microseconds)
   11:  Execution Throttle
   12:  Login Retry Count
   13:  Port Down Retry Count
   14:  Enable LIP Full Login
   15:  Link Down Timeout (seconds)
   16:  Enable Target Reset
   17:  LUNs per Target
   18:  Enable Receive Out Of Order Frame
   19:  Enable LR Ext. Credits
   20:  Commit Changes
   21:  Abort Changes


        (p or 0: Previous Menu; m or 98: Main Menu; x or 99: Quit)
        Please Enter Selection: 11
Enter Execution Throttle [1-65535] [65535]: 65500
```

d. 按* Enter鍵*繼續。

e. 從「設定參數」功能表中、選取 `Commit Changes` 儲存變更的選項。

f. 結束功能表。

S3物件儲存管理

瞭解 ONTAP 9 中的 S3 支援

瞭解 ONTAP S3 組態

從 ONTAP 9.8 開始、您可以在 ONTAP 叢集中啟用 ONTAP Simple Storage Service （ S3 ）物件儲存伺服器、使用熟悉的管理工具、例如 ONTAP System Manager 、快速配置高效能物件儲存設備、以便在 ONTAP 中進行開發與作業、並充分利用 ONTAP 的儲存效率與安全性。

自 2024 年 7 月起、先前以 PDF 格式發佈的技術報告內容已與 ONTAP 產品文件整合。ONTAP S3 文件現在包含來自 _TR-4814 ： ONTAP 最佳實務做法中 S3 的內容。

S3組態搭配System Manager和ONTAP Stri CLI

您可以使用ONTAP System Manager和ONTAP SURE CLI來設定及管理SS3。當您使用System Manager啟用S3並建立貯體時、ONTAP 會選擇最佳實務預設值以簡化組態。如果您需要指定組態參數、可能需要使用ONTAP CLI。 如果您從CLI設定S3伺服器和儲存區、仍可視需要使用System Manager進行管理、反之亦然。

當您使用System Manager建立S3儲存區時ONTAP 、即可設定系統可用的最高預設效能服務層級。例如AFF 、在某個不完善的系統上、預設設定為*極致*。效能服務層級是預先定義的可調整服務品質（QoS）原則群組。您可以指定自訂QoS原則群組或無原則群組、而非其中一個預設服務層級。

預先定義的調適性QoS原則群組包括：

- 極致：適用於預期最低延遲和最高效能的應用程式。
- 效能：適用於效能需求與延遲不佳的應用程式。
- 值：用於處理量與容量比延遲更重要的應用程式。
- 自訂：指定自訂QoS原則或無QoS原則。

如果您選擇*用於分層*、則不會選擇效能服務層級、系統會嘗試選擇低成本媒體、並針對階層式資料提供最佳效能。

另請參閱： "使用調適性QoS原則群組"。

嘗試將此儲存庫配置到具有最適當磁碟的本機層、以符合所選的服務層級。ONTAP不過、如果您需要指定要包含在儲存區中的磁碟、請考慮從CLI設定S3物件儲存、方法是指定本機層（Aggregate）。如果您從CLI設定S3伺服器、仍可視需要使用System Manager來管理。

如果您想要指定要用於儲存區的集合體、只能使用CLI來執行此作業。

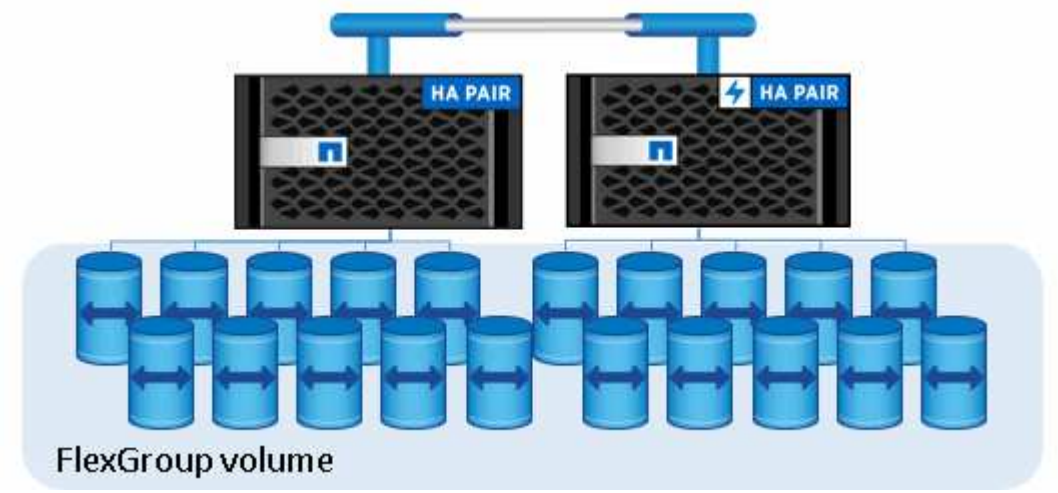
在SS3上設定S3鏟斗Cloud Volumes ONTAP

如果您想要供應Cloud Volumes ONTAP 來自整個部門的庫存箱、強烈建議您手動選取基礎集合體、以確保它們僅使用一個節點。使用兩個節點的集合體可能會影響效能、因為節點將位於不同地理位置的可用度區域、因此容易受到延遲問題的影響。因此Cloud Volumes ONTAP 、在不完善的環境中、您應該 從CLI設定S3儲存區。

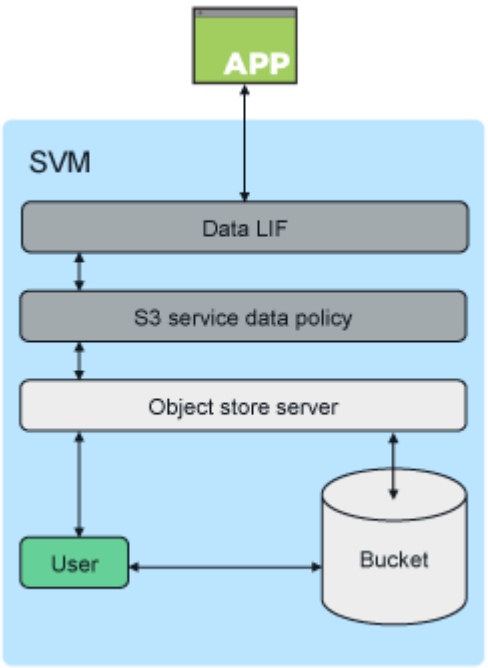
否則Cloud Volumes ONTAP 、在內部Cloud Volumes ONTAP 部署環境中、將以相同的方式設定和維護位於內部部署環境中的S3伺服器。

使用 **FlexGroup Volume** 的 **ONTAP S3** 架構

在 ONTAP 中、貯體的基礎架構是 "流通量FlexGroup"、這是由多個組成成員磁碟區組成、但以單一磁碟區管理的單一命名空間。



透過授權使用者和用戶端應用程式、即可存取儲存庫。



當儲存區僅用於 S3 應用程式（包括用作 FabricPool 端點）時、基礎 FlexGroup Volume 僅支援 S3 傳輸協定。

從 ONTAP 9.12.1 開始， S3 傳輸協定也可以在中啟用，而 S3 "多重傳輸協定 NAS 磁碟區"傳輸協定已預先設定為使用 NAS 傳輸協定。在多重傳輸協定 NAS 磁碟區中啟用 S3 傳輸協定時、用戶端應用程式可以使用 NFS 、 SMB 和 S3 來讀寫資料。

貯體限制

最低容量

最小桶容量由ONTAP平台決定。

- 本地部署平台需要 95GB 記憶體。
- 按需實驗室需要 1.6GB 記憶體。
- ONTAP Select需要 200MB。

最大尺寸

最大桶容量限制為最大FlexGroup尺寸 60PB。

最大桶數

每個FlexGroup磁碟區最多可容納 1000 個桶，或每個集群最多可容納 12,000 個桶（使用 12 個FlexGroup區）。

使用 **ONTAP 9.14.1** 及更新版本自動調整 **FlexGroup** 規模

從 ONTAP 9.14.1 開始，預設的 FlexGroup 尺寸是根據其包含的貯體大小而定。FlexGroup Volume 會隨著貯體的新增或移除而自動增加或縮小。

例如、如果初始 Bucket_A 的資源配置為 100GB 、則 FlexGroup 將會精簡配置為 100GB 。如果另外建立兩個儲存區、儲存容量為 300 GB 的 Bucket_B 、以及容量為 500 GB 的 Bucket_C 、則 FlexGroup 磁碟區將成長至 900 GB 。

（ 100GB 的 Bucket_A + 300GB 的 Bucket_B + 500GB 的 Bucket_C = 900GB ）。

如果刪除 Bucket_A 、基礎 FlexGroup 磁碟區將縮減至 800GB 。

ONTAP 9.13.1 及更早版本中的固定預設 **FlexGroup** 大小

為了提供貯體擴充的容量、 FlexGroup Volume 上所有貯體的總使用容量應小於叢集上可用儲存集合體的 FlexGroup 磁碟區容量上限 33% 。如果無法達成此目標、則所建立的新貯體將配置在新的自動建立 FlexGroup Volume 上。

在 ONTAP 9.14.1 之前、 FlexGroup 大小會根據其環境固定為預設大小：

- ONTAP 中的 1.6PB
- ONTAP Select 中的 100TB

如果叢集沒有足夠的容量來配置預設大小的 FlexGroup Volume 、 ONTAP 會將預設大小減半、直到在現有環境中進行佈建為止。

例如、在 300TB 環境中、 FlexGroup Volume 會自動配置為 200TB （ 1.6PB 、 800TB 和 400TB FlexGroup 磁碟區對於環境而言太大）。

ONTAP S3 主要使用案例

以下是用戶端存取 ONTAP S3 服務的主要使用案例：

- 使用 FabricPool 將非使用中資料分層至 ONTAP 中的儲存區、讓 ONTAP 能夠進行 ONTAP 分層。這兩項功能都支援分層至中的貯 "本機叢集"體、或分層至上的某個貯體 "遠端叢集"。分層至 ONTAP S3 可讓您使用較便宜的 ONTAP 系統來處理非使用中資料、並節省新的 Flash 容量成本、而無需額外的 FabricPool 授權或新技術來管理。
- 從 ONTAP 9.12.1 開始， S3 傳輸協定也可以在中啟用，而 S3 "多重傳輸協定 NAS 磁碟區"傳輸協定已預先設定為使用 NAS 傳輸協定。當在多重傳輸協定 NAS 磁碟區中啟用 S3 傳輸協定時、用戶端應用程式可以使用 S3 、 NFS 和 SMB 讀取和寫入資料、這會開啟多種其他使用案例。最常見的使用案例之一是 NAS 用戶端將資料寫入磁碟區和 S3 用戶端、讀取相同資料並執行分析、商業智慧、機器學習和光學字元辨識等專業工作。

> 如果您想在現有的 ONTAP 叢集上啟用 S3 功能、而不需要額外的硬體和管理功能、則 ONTAP S3 是適當的選擇。NetApp StorageGRID 是 NetApp 的物件儲存旗艦解決方案。StorageGRID 建議用於需要充分利用 S3 行動、進階 ILM 功能或 ONTAP 系統無法達到的容量的原生 S3 應用程式。如需詳細資訊，請參閱 "本文檔StorageGRID"。

相關資訊

"資料區管理FlexGroup"

規劃

支援 S3 物件儲存的 ONTAP 版本與平台

所有使用 ONTAP 9.8 及更新版本的 AFF 、 FAS 及 ONTAP Select 平台均支援 S3 物件儲存。

如同 FC 、 iSCSI 、 NFS 、 NVMe 、 SMB 等其他通訊協定、 S3 需要先安裝授權、才能在 ONTAP 中使用。S3 授權為零成本授權、但必須安裝在升級至 ONTAP 9.8 的系統上。S3 授權可從 NetApp 支援網站上的下載 "主要授權金鑰頁面" 。

新的 ONTAP 9.8 及更新版本系統已預先安裝 S3 授權。

Cloud Volumes ONTAP

除了以下一項之外、在不支援內部部署環境的情況下、將支援的功能與在不支援內部部署環境中相同：ONTAP Cloud Volumes ONTAP

- 在 Cloud Volumes ONTAP 中建立貯體時、應使用 CLI 程序、確保基礎 FlexGroup Volume 僅使用單一節點的集合體。使用來自多個節點的集合體會影響效能、因為節點將位於地理上分離的可用區域、容易發生延遲問題。

雲端供應商	版本**ONTAP**
Google Cloud	更新版本ONTAP
AWS	更新版本ONTAP
Azure	更新版本ONTAP

Amazon FSX for NetApp ONTAP 產品

使用 ONTAP 9.11 及更新版本的 Amazon FSX for NetApp 服務支援 S3 物件儲存。

S3 支援 **MetroCluster**

從 ONTAP 9.14.1 開始、您可以在 MetroCluster IP 和 FC 組態的鏡射集合中、在 SVM 上啟用 S3 物件儲存伺服器。

從ONTAP 《S209.12.1.版」開始、您可以在SVM上啟用S3物件儲存伺服器、並以MetroCluster 無鏡射的Aggregate進行支援、以利執行不鏡射的IP組態。如需 MetroCluster IP 組態中未鏡射集合體限制的詳細資訊，請參閱 "無鏡射Aggregate的考量"。

MetroCluster 組態不支援 SnapMirror S3 。

S3公有預覽**ONTAP** 、以供使用。**9.7**

在S129.7中ONTAP 、S3物件儲存設備是以公開預覽形式推出。該版本不適用於正式作業環境，將不再從ONTAP 9.8 開始更新。只有更新版本的支援功能才支援正式作業環境中的S3物件儲存。ONTAP

使用9.7公用預覽建立的S3儲存桶可在ONTAP 更新版本的支援中使用、但無法利用功能增強功能。如果您有使用9.7公用預覽建立的儲存區、則應將這些儲存區的內容移轉至9.8個儲存區、以增強功能支援、安全性及效能。

支援的動作**ONTAP**

除以下所示者外、支援標準S3 REST API的S3動作。ONTAP如需詳細資訊、請參閱 "Amazon S3 API參考"。

在 ONTAP 中使用原生 S3 儲存區時，特別支援這些 S3 動作。使用時不支援這些動作，例如與版本設定，物件鎖定及其他功能相關的動作"S3 NAS 磁碟區（多重傳輸協定 NAS 磁碟區中的 S3 ）"。

除非針對特定操作另有說明，否則從ONTAP 9.8 開始支援以下常見請求標頭：

- `Authorization`
- `Connection`
- `Content-Length`
- `Content-MD5`
- `Content-Type`
- `Date`
- `Expect`
- `Host`
- `x-amz-date`

鏟斗作業

使用 AWS S3 API 的 ONTAP 支援下列作業：

鏟斗作業	支援從開始**ONTAP**
建立庫位 ONTAP S3 支援此要求的所有常用參數和標頭，以及以下附加標頭： • `x-amz-bucket-object-lock-enabled`	零點9.11.1. ONTAP
刪除Bucket ONTAP S3 支援此請求的所有常用參數和標頭。	零點9.11.1. ONTAP
DeleteBucketCors ONTAP S3 支援此要求的所有常用參數和標頭。	部分9.8 ONTAP
DeleteBucketLifecycle ONTAP S3 支援此要求的所有常用參數和標頭。	部分9.8 ONTAP
刪除BucketPolicy ONTAP S3 支援此請求的所有常用參數和標頭。	ONTAP 9.12.1
GetBucketAcl ONTAP S3 支援此要求的所有常用參數和標頭。	部分9.8 ONTAP
GetBucketCors ONTAP S3 支援此要求的所有常用參數和標頭。	部分9.8 ONTAP
GetBucketLifecycleConfiguration ONTAP S3 支援此請求的所有常用參數和標頭。	ONTAP 9.13.1.12.9.11.9.11. *僅支援到期操作
GetBucketLocation ONTAP S3 支援此要求的所有常用參數和標頭。	零點9.10.1 ONTAP
GetBucketPolicy ONTAP S3 支援此要求的所有常用參數和標頭。	ONTAP 9.12.1
GetBucketVersioning ONTAP S3 支援此要求的所有常用參數和標頭。	零點9.11.1. ONTAP
HeadBucket ONTAP S3 支援此要求的所有常見參數和標頭。	部分9.8 ONTAP
ListAllMyBuckets ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.8 ONTAP
ListBuckets ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.8 ONTAP
ListBucketVersions ONTAP S3 支援此要求的所有常用參數和標頭。	零點9.11.1. ONTAP

鏟斗作業	支援從開始**ONTAP**
推桿	• 零點9.11.1. ONTAP • ONTAP 9.8 - 僅支援 ONTAP REST API
PutBucketCors ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.8 ONTAP
PutBucketLifecycleConfiguration ONTAP S3 支援此要求的所有常用參數和標頭。	ONTAP 9.13.1 * 僅支援過期操作
PutBucketPolicy ONTAP S3 支援此請求的所有常用參數和標頭。	ONTAP 9.12.1
PutBucketVersioning ONTAP S3 支援此請求的所有常用參數和標頭。	零點9.11.1. ONTAP

物件作業

從支援物件中繼資料和標記的ONTAP 支援範圍起、ONTAP 從S9.9開始。

- PutObject 和 CreateMultpartUpload 包含使用的金鑰值配對 `x-amz-meta-<key>.`

  例如： `x-amz-meta-project: ontap_s3`。

- GetObject 和 HeadObject 會傳回使用者定義的中繼資料。
- 不同於中繼資料、標記可以使用下列方式獨立讀取物件：
  - PuttObjectTagging
  - GetObjectTagging
  - 刪除ObjectTagging

從推出支援物件版本管理和相關動作的《S21：ONTAP ONTAP ONTAP

- GetBucketVersion
- listBucketVerions
- PuttBucketVersion

除非針對特定操作另有說明，否則支援以下 URI 查詢參數：

- `versionId`（根據ONTAP 9.12.1 開始的物件操作要求）

物件作業	支援從開始**ONTAP**
AbortMultiPart上 傳 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 查詢參數： `uploadId`	部分9.8 ONTAP

物件作業	支援從開始**ONTAP**
完成多個部分上傳 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 查詢參數： `uploadId`	部分9.8 ONTAP
CopyObject ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加標頭： • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-metadata-directive` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-tagging` • `x-amz-tagging-directive` • `x-amz-meta-<metadata-name>`	ONTAP 9.12.1
建立多個部分上傳 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加標頭： • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	部分9.8 ONTAP

物件作業	支援從開始**ONTAP**
刪除物件 ONTAP S3 支援此要求的所有常用參數和標頭，以及以下附加標頭： • `x-amz-bypass-governance-retention`	部分9.8 ONTAP
DeleteObjects ONTAP S3 支援此要求的所有常用參數和標頭，以及以下附加標頭：* `x-amz-bypass-governance-retention`	零點9.11.1. ONTAP
刪除ObjectTagging ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.9.1 ONTAP
GetObject ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 查詢參數： • `partNumber` • `response-cache-control` • `response-content-disposition` • `response-content-encoding` • `response-content-language` • `response-content-type` • `response-expires` 還有這個附加的請求標頭： • 範圍	部分9.8 ONTAP
GetObjectAcl ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.8 ONTAP
取得物件屬性 ONTAP S3 支援此要求的所有常用參數和標頭，以及以下附加標頭： • `x-amz-object-attributes`	ONTAP 9.17.1
GetObjectRetention ONTAP S3 支援此請求的所有常用參數和標頭。	ONTAP 9.14.1.
GetObjectTagging ONTAP S3 支援此要求的所有常用參數和標頭。	部分9.9.1 ONTAP

物件作業	支援從開始**ONTAP**
HeadObject ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.8 ONTAP
清單多個部分上傳 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `delimiter` • `key-marker` • `max-uploads` • `prefix` • `upload-id-marker`	部分9.8 ONTAP
清單物件 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `delimiter` • `encoding-type` • `marker` • `max-keys` • `prefix`	部分9.8 ONTAP
清單對象V2. ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `continuation-token` • `delimiter` • `encoding-type` • `fetch-owner` • `max-keys` • `prefix` • `start-after`	部分9.8 ONTAP

物件作業	支援從開始**ONTAP**
ListObjectVerions ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `delimiter` • `encoding-type` • `key-marker` • `max-keys` • `prefix` • `version-id-marker`	零點9.11.1. ONTAP
清單零件 ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `max-parts` • `part-number-marker` • `uploadId`	部分9.8 ONTAP
PuttObject ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加標頭： • `Cache-Control` • `Content-Disposition` • `Content-Encoding` • `Content-Language` • `Expires` • `x-amz-tagging` • `x-amz-object-lock-mode` • `x-amz-object-lock-retain-until-date` • `x-amz-meta-<metadata-name>`	部分9.8 ONTAP
PutObjectLockConfiguration ONTAP S3 支援此請求的所有常用參數和標頭。	ONTAP 9.14.1.

物件作業	支援從開始**ONTAP**
PutObjectRetention ONTAP S3 支援此要求的所有常用參數和標頭，以及以下附加標頭： • `x-amz-bypass-governance-retention`	ONTAP 9.14.1.
PutObjectTagging ONTAP S3 支援此請求的所有常用參數和標頭。	部分9.9.1 ONTAP
上傳零件	部分9.8 ONTAP
上傳PartCopy ONTAP S3 支援此請求的所有常用參數和標頭，以及以下附加 URI 參數： • `partNumber` • `uploadId` 以及這些額外的請求標頭： • `x-amz-copy-source` • `x-amz-copy-source-if-match` • `x-amz-copy-source-if-modified-since` • `x-amz-copy-source-if-none-match` • `x-amz-copy-source-if-unmodified-since` • `x-amz-copy-source-range`	ONTAP 9.12.1

群組原則

這些作業並非S3專屬作業、通常與身分識別與管理（IAM）程序相關。支援這些命令、但不使用IAM REST API。ONTAP

- 建立原則
- Attach群組原則

使用者管理

這些作業並非S3專屬作業、通常與IAM程序相關。

- 建立使用者
- 刪除使用者
- 建立群組

- 刪除群組

S3 依版本採取的行動

ONTAP 9.14.1.

ONTAP 9 。 14.1 新增 S3 物件鎖定支援。

不支援合法保留作業（鎖定時未定義保留時間）。

- GetObjectLockConfiguration
- GetObjectRetention
- PutObjectLockConfiguration
- PutObjectRetention

ONTAP 9.13.1.12.9.11.9.11.

ONTAP 9 。 13.1 新增貯體生命週期管理支援。

- 刪除 BucketLifecycleConfiguration
- GetBucketLifecycleConfiguration
- PuttBucketLifecycleConfiguration

ONTAP 9.12.1

ONTAP 9 。 12.1 新增貯體原則的支援、以及複製物件的能力。

- 刪除BucketPolicy
- GetBucketPolicy
- PuttBucketPolicy
- CopyObject
- 上傳PartCopy

零點**9.11.1. ONTAP**

ONTAP 9 。 11.1 新增版本管理，預先簽署的 URL ，區塊上傳的支援，以及一般 S3 行動的支援，例如使用 S3 API 建立和刪除區段。

- ONTAP S3 現在支援使用以下方式對分塊上傳簽名請求進行支持 `x-amz-content-sha256: STREAMING-AWS4-HMAC-SHA256-PAYLOAD`
- ONTAP S3 現在支援使用預先簽署的 URL 來共用物件的用戶端應用程式、或允許其他使用者在不需要使用者認證的情況下上傳物件。
- 建立庫位
- 刪除Bucket
- GetBucketVersion
- listBucketVerions
- 推桿

- PuttBucketVersion
- 刪除物件
- ListObjectVerions

由於基礎 FlexGroup 在第一個儲存區建立之前不會建立、因此必須先在 ONTAP 中建立儲存區、外部用戶端才能使用 CreateBucket 建立儲存區。

零點9.10.1 ONTAP

ONTAP 9 。 10.1 新增對 SnapMirror S3 和 GetBucketLocation 的支援。

- GetBucketLocation

部分9.9.1 ONTAP

ONTAP 9 9.1 為 ONTAP S3 新增物件中繼資料和標記支援。

- PuttObject 和 CreateMultpartUpload 現在包括使用的金鑰值配對 `x-amz-meta-<key>`。例如 `x-amz-meta-project: ontap_s3`：。
- GetObject 和 HeadObject 現在會傳回使用者定義的中繼資料。

標籤也可搭配貯體使用。不同於中繼資料、標記可以使用下列方式獨立讀取物件：

- PuttObjectTagging
- GetObjectTagging
- 刪除ObjectTagging

SS3互通性ONTAP

除了本表所述之外、其他的功能不包括在本S3伺服器ONTAP 上正常互動ONTAP 。

功能區	支援	不支援
Cloud Volumes ONTAP	• Azure用戶端的ONTAP 更新版本 • AWS用戶端採用ONTAP 的是版本更新的版本 • Google Cloud用戶端的ONTAP 更新版本為更新版本	• 適用於任何版本為更新版本的客戶Cloud Volumes ONTAP ONTAP

功能區	支援	不支援
資料保護	• Cloud Sync • 物件鎖定；治理與法規遵循（從 ONTAP 9.14.1 開始） • "物件版本管理" （從 ONTAP 9.11.1 開始） • 無鏡射 MetroCluster 集合體（從 ONTAP 9.12.1 開始） • 鏡射 MetroCluster 集合體（從 ONTAP 9.14.1 開始） • "SnapMirror S3" （從 ONTAP 9.10.1 開始） • SnapMirror （僅限 NAS 磁碟區；從 ONTAP 9.12.1 開始） • SnapLock （僅限 NAS 磁碟區；從 ONTAP 9.14.1 開始）	• 銷毀編碼 • NDMP • SM磁帶 • SnapMirror （同步和非同步） • SnapMirror 雲端 • SVM 災難恢復 • SyncMirror （從ONTAP 9.14.1開始， MetroCluster配置支援SyncMirror映像聚合。MetroClusterMetroCluster之外不支援SyncMirror 。）
加密	• NetApp Aggregate Encryption（NAE） • NetApp Volume Encryption（NVE） • NetApp儲存加密（NSE） • TLS/SSL	• 熔渣
MetroCluster 環境	-	SnapMirror S3
儲存效率	• 重複資料刪除 • 壓縮 • 壓實	• 聚合級效率（位於相同聚合上的成員可以利用跨磁碟區重複資料刪除，但位於不同聚合上的成員則不能） • 包含不含支援的S3鏟斗的實體磁碟區Volume複製FlexGroup ONTAP
服務品質（QoS）	• QoS上限（上限） • QoS最低值（樓層）	-

功能區	支援	不支援
其他功能	• "稽核S3事件" （從ONTAP 版本號《2019年9月10日》開始） • "貯體生命週期管理" （從ONTAP 9.13.1 開始） • FabricPool雲層（僅限原生 S3） • FabricPool本機層（僅限 NAS 磁碟區） • FlexCache 磁碟區（從 ONTAP 9.18.1 開始）	• FPolicy • qtree • 配額 • FabricPool雲層（僅限 NAS 卷） • FabricPool本機層（僅限原生 S3）

經過驗證的 **ONTAP** 中使用 **S3** 的第三方解決方案

S3 是一個通用標準，這並不是受支援應用程式的完整清單——只是與各個合作夥伴合作驗證的解決方案清單。如果未列出您要尋找的解決方案、請聯絡您的 NetApp 客戶代表。

使用原生 **S3** 儲存桶驗證的第三方解決方案

- Amazon SageMaker
- Apache Hadoop S3A 用戶端
- Apache Kafka
- Apache Spark
- CommVault （ V11 ）
- Confluent Kafka
- NetBackup
- Red Hat Quay
- Rukrik
- 雪片
- Trino
- Veeam （ V12 ）

這些解決方案在 ONTAP 中使用原生 S3 儲存桶時經過了專門驗證。其中一些解決方案（例如與版本控制、物件鎖定和其他功能相關的解決方案）正在使用"S3 NAS 磁碟區（多重傳輸協定 NAS 磁碟區中的 S3 ）"。

設定

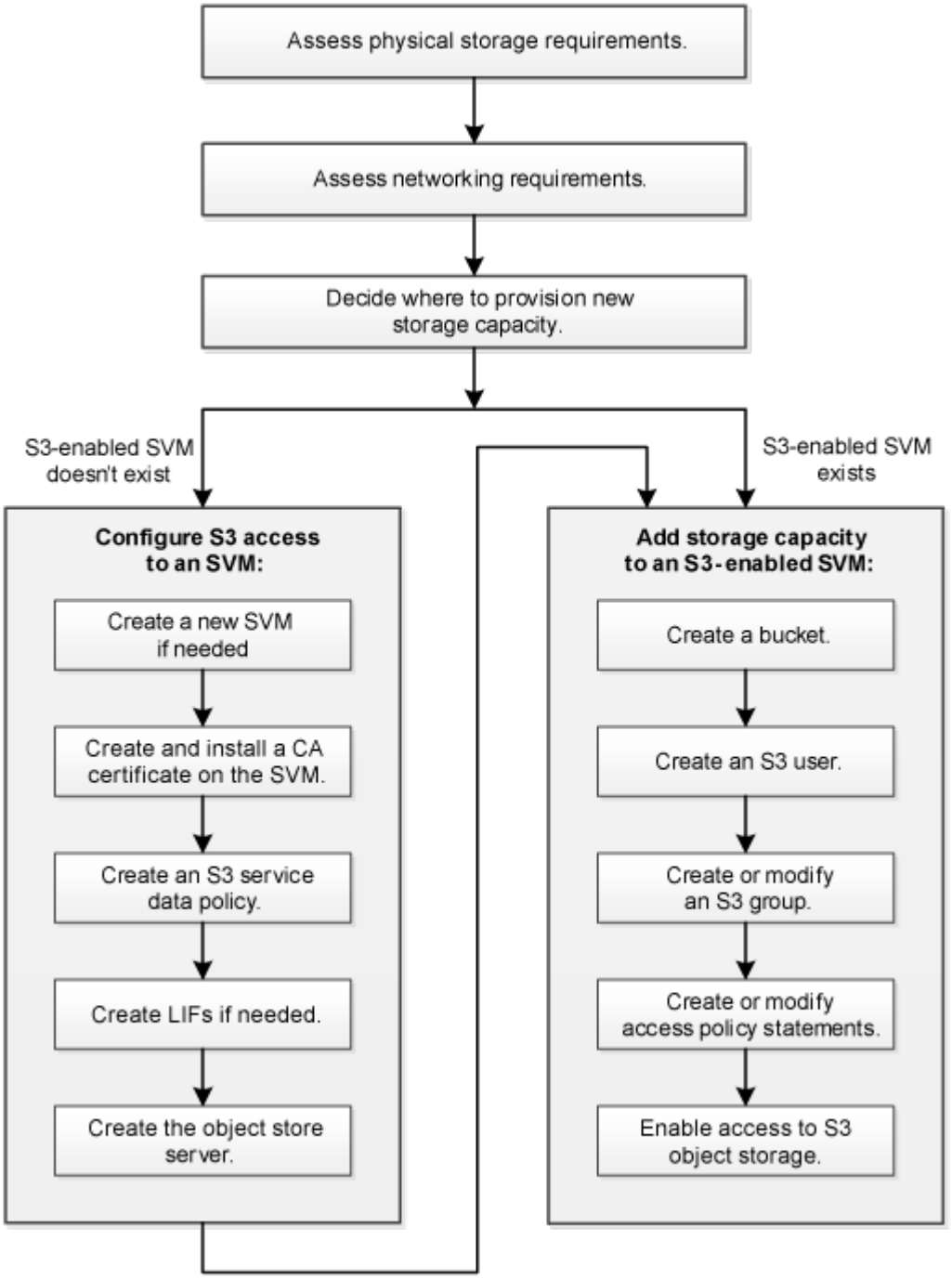
關於**S3**組態程序

ONTAP S3 組態工作流程

設定S3需要評估實體儲存設備和網路需求、然後選擇專屬於您目標的工作流程、包括設定S3存取新的或現有的SVM、或是將儲存庫和使用者新增至已完全設定為S3存取的現有SVM。

需要網路時間協定 (NTP) 配置來確保叢集和用戶端之間的時間同步。客戶端存取通常需要ONTAP S3 物件儲存和客戶端之間的有效時間戳記至少有 15 分鐘的差異。"了解如何設定 NTP" 。

當您使用System Manager設定S3存取新儲存VM時、系統會提示您輸入憑證和網路資訊、儲存VM和S3物件儲存伺服器會在單一作業中建立。



在為用戶端配置S3儲存設備之前、您必須確保現有集合體中有足夠空間可用於新的物件存放區。如果沒有、您可以將磁碟新增至現有的Aggregate、或建立所需類型和位置的新Aggregate。

關於這項工作

當您在啟用 S3 的 SVM 中建立 S3 貯體時、 FlexGroup Volume 即是 "自動建立" 支援該貯體。您可以ONTAP Select 自動讓底層的Aggregate和FlexGroup 架構元件（預設值）使用、也可以FlexGroup 自行選擇底層的Aggregate和架構元件。

如果您決定指定Aggregate和FlexGroup 等元件（例如、如果您對基礎磁碟有特定的效能要求）、您應該確定您的Aggregate組態符合配置FlexGroup 一個可靠的實務做法準則。深入瞭解：

- "資料區管理FlexGroup"
- "NetApp技術報告4571-A：NetApp ONTAP FlexGroup 《關於NetApp的最新資訊》最佳實務做法"

如果您是供應Cloud Volumes ONTAP 來自於整個過程的貯體、強烈建議您手動選取基礎Aggregate、以確保它們僅使用一個節點。使用兩個節點的集合體可能會影響效能、因為節點將位於不同地理位置的可用度區域、因此容易受到延遲問題的影響。 深入瞭解 "打造庫位以供Cloud Volumes ONTAP 使用"。

您可以使用ONTAP VMware S3伺服器來建立本機FabricPool 的功能性分層、也就是在效能層所在的同一個叢集內。舉例來說、如果您將SSD磁碟連接至一個HA配對、而且想要將_Cold資料分層至另一個HA配對中的HDD磁碟、這項功能就很實用。在此使用案例中、S3伺服器和包含本機容量層的儲存區應該與效能層位於不同的HA配對中。單節點和雙節點叢集不支援本機分層。

步驟

1. 顯示現有Aggregate中的可用空間：

   ```
   storage aggregate show
   ```

   如果有一個具有足夠空間或必要節點位置的集合體、請記錄其S3組態名稱。

```
cluster-1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes  RAID Status
--------- -------- --------- ----- ------- ------ ------ -----------
aggr_0     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_1     239.0GB   11.13GB   95% online       1 node1  raid_dp,
                                                        normal
aggr_2     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_3     239.0GB   11.13GB   95% online       1 node2  raid_dp,
                                                        normal
aggr_4     239.0GB   238.9GB   95% online       5 node3  raid_dp,
                                                        normal
aggr_5     239.0GB   239.0GB   95% online       4 node4  raid_dp,
                                                        normal
6 entries were displayed.
```

2. 如果沒有具有足夠空間或必要節點位置的集合體、請使用將磁碟新增至現有的集合體 `storage aggregate add-disks` 或使用建立新的 Aggregate `storage aggregate create` 命令。

相關資訊

- "存儲聚合添加磁碟"
- "儲存聚合創建"

評估 **ONTAP S3** 網路連線需求

將S3儲存設備提供給用戶端之前、您必須確認網路設定正確、以符合S3資源配置需求。

開始之前

必須設定下列叢集網路物件：

- 實體與邏輯連接埠
- 廣播網域
- 子網路（如有需要）
- IPspaces（視需要而定、除了預設IPspace）
- 容錯移轉群組（視需要、以及每個廣播網域的預設容錯移轉群組）
- 外部防火牆

關於這項工作

若要使用遠端FabricPool 的支援能力（雲端）階層和遠端S3用戶端、您必須使用資料SVM並設定資料生命量。對於架構雲端層、您也必須設定叢集間的生命體、不需要叢集對等。FabricPool

對於本機FabricPool 的功能區階層、您必須使用系統SVM（稱為「叢集」）、但LIF組態有兩種選項：

- 您可以使用叢集LIF。

  在此選項中、不需要進一步的LIF組態、但叢集生命期的流量會增加。此外、其他叢集也無法存取本機層級。

- 您可以使用資料和叢集間的LIF。

  此選項需要額外的組態、包括啟用S3傳輸協定的LIF、但也可將本機層作為遠端FabricPool 的異地雲端層存取至其他叢集。

步驟

1. 顯示可用的實體和虛擬連接埠：

   `network port show`

   - 如果可能、您應該使用資料網路速度最高的連接埠。
   - 資料網路中的所有元件必須具有相同的MTU設定、才能獲得最佳效能。

2. 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、請確認該子網路存在且有足夠的可用位址：

   `network subnet show`

   子網路包含屬於同一第3層子網路的IP位址集區。子網路是使用建立的 `network subnet create` 命令。

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

3. 顯示可用的IPspaces：

   `network ipspace show`

   您可以使用預設IPspace或自訂IPspace。

4. 如果您要使用IPv6位址、請確認叢集上已啟用IPv6：

   `network options ipv6 show`

   如有需要、您可以使用啟用 IPv6 `network options ipv6 modify` 命令。

相關資訊

- "網路連接埠顯示"
- "網路選項 IPv6"
- "網路IPSpace展示"
- "建立網路子網路"

決定在何處配置新的 **ONTAP S3** 儲存容量

在建立新的S3儲存區之前、您必須先決定要將它放在新的或現有的SVM中。此決定決定決定您的工作流程。

選擇

- 如果您想要在未啟用S3的新SVM或SVM中配置儲存區、請完成下列主題中的步驟。

  "為S3建立SVM"

  "為S3建立儲存庫"

  雖然S3可以與NFS和SMB共存於SVM中、但如果符合下列其中一項條件、您可以選擇建立新的SVM：

  - 您是第一次在叢集上啟用S3。
  - 您在不想啟用S3支援的叢集中有現有的SVM。
  - 叢集中有一個或多個啟用S3的SVM、您想要另一個具有不同效能特性的S3伺服器。
    在SVM上啟用S3之後、請繼續配置儲存區。

- 如果您想要在現有的S3型SVM上配置初始儲存區或其他儲存區、請完成下列主題中的步驟。

  "為S3建立儲存庫"

設定**S3**對**SVM**的存取

為 **ONTAP S3** 建立 **SVM**

雖然S3可以與SVM中的其他傳輸協定共存、但您可能想要建立新的SVM來隔離命名空間和工作負載。

關於這項工作

如果您僅從SVM提供S3物件儲存設備、則S3伺服器不需要任何DNS組態。不過、如果使用其他通訊協定、您可能會想要在SVM上設定DNS。

當您使用System Manager設定S3存取新儲存VM時、系統會提示您輸入憑證和網路資訊、儲存VM和S3物件儲存伺服器會在單一作業中建立。

範例 **23.** 步驟

系統管理員

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。S3伺服器FQDN不得以儲存區名稱開頭。

您應準備好輸入介面角色資料的IP位址。

如果您使用的是外部CA簽署的憑證、系統會在此程序期間提示您輸入；您也可以選擇使用系統產生的憑證。

1. 在儲存VM上啟用S3。

   a. 新增儲存VM：按一下「儲存設備**>**儲存**VM**」、然後按一下「新增」。

      如果這是沒有現有儲存VM的新系統：請按一下*儀表板>設定傳輸協定*。

   如果您要將 S3 伺服器新增至現有的儲存 VM ：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * S2* 下的。

   a. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   b. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   c. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 確認叢集上的S3已獲得授權：

   ```
   system license show -package s3
   ```

   如果沒有、請聯絡您的銷售代表。

2. 建立SVM：

   ```
   vserver create -vserver <svm_name> -subtype default -rootvolume
   <root_volume_name> -aggregate <aggregate_name> -rootvolume-security
   -style unix -language C.UTF-8 -data-services <data-s3-server>
   -ipspace <ipspace_name>
   ```

- 使用的 UNIX 設定 `-rootvolume-security-style` 選項。
- 使用預設的 C.UTF-8 `-language` 選項。
- 。 `ipspace` 設定為選用項目。

3. 驗證新建立的SVM的組態和狀態：

```
vserver show -vserver <svm_name>
```

。 `Vserver Operational State` 欄位必須顯示 `running` 州/省。如果顯示 `initializing` 狀態、表示有些中繼作業（例如建立根磁碟區）失敗、您必須刪除 SVM 並重新建立它。

範例

下列命令會在IPspace ipspaceA中建立SVM以供資料存取：

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language
C.UTF-8 -data-services data-s3-server -ipspace ipspaceA

[Job 2059] Job succeeded:
Vserver creation completed
```

下列命令顯示 SVM 是以 1 GB 的根磁碟區所建立、而且是自動啟動且位於中 `running` 州/省。根磁碟區具有預設的匯出原則、不含任何規則、因此根磁碟區在建立時不會匯出。根據預設、會建立 vsadmin 使用者帳戶、並位於中 `locked` 州/省。vsadmin角色會指派給預設的vsadmin使用者帳戶。

```
cluster-1::> vserver show -vserver svm1.example.com
                                    Vserver: svm1.example.com
                               Vserver Type: data
                            Vserver Subtype: default
                               Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736
                                Root Volume: root_svm1
                                  Aggregate: aggr1
                                NIS Domain: -
                  Root Volume Security Style: unix
                                 LDAP Client: -
               Default Volume Language Code: C.UTF-8
                             Snapshot Policy: default
                                    Comment:
                               Quota Policy: default
                 List of Aggregates Assigned: -
 Limit on Maximum Number of Volumes allowed: unlimited
                         Vserver Admin State: running
                   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
                          Allowed Protocols: nfs, cifs
                       Disallowed Protocols: -
                           QoS Policy Group: -
                                Config Lock: false
                               IPspace Name: ipspaceA
```

在啟用 **ONTAP S3** 的 **SVM** 上建立並安裝 **CA** 憑證

S3 用戶端需要憑證授權單位 (CA) 憑證才能將 HTTPS 流量傳送到啟用 S3 的 SVM。 CA 憑證在用戶端應用程式和ONTAP物件儲存伺服器之間建立信任關係。在將 ONTAP 用作遠端用戶端可存取的物件儲存之前，您應該在ONTAP上安裝 CA 憑證。

關於這項工作

雖然可以將S3伺服器設定為僅使用HTTP、而且雖然可以設定不需CA憑證的用戶端、但最佳做法是使用ONTAP CA憑證來保護HTTPS流量。

本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

本程序中的指示將建立並安裝ONTAP 一個自我簽署的驗證書。雖然 ONTAP 可以產生自我簽署的憑證，但建議最佳做法是使用協力廠商憑證授權單位所簽署的憑證；如需詳細資訊，請參閱系統管理員驗證文件。

"系統管理員驗證與RBAC"

如"指令參考資料ONTAP"需更多資訊及其他組態選項的詳細 `security certificate`資訊，請參閱。

步驟

1. 建立自我簽署的數位憑證：

   `security certificate create -vserver svm_name -type root-ca -common-name ca_cert_name`

   。 `-type root-ca` 選項會建立及安裝自我簽署的數位憑證、以作為憑證授權單位（ CA ）來簽署其他憑證。

   。 `-common-name` 選項會建立 SVM 的憑證授權單位（ CA ）名稱、並在產生憑證的完整名稱時使用。

   預設的憑證大小為2048位元。

   範例

   ```
   cluster-1::> security certificate create -vserver svm1.example.com -type
   root-ca -common-name svm1_ca

   The certificate's generated name for reference:
   svm1_ca_159D1587CE21E9D4_svm1_ca
   ```

   顯示憑證產生的名稱時、請務必儲存以供此程序的後續步驟使用。

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

2. 產生憑證簽署要求：

   `security certificate generate-csr -common-name s3_server_name [additional_options]`

   。 `-common-name` 簽署要求的參數必須是 S3 伺服器名稱（ FQDN ）。

   如有需要、您可以提供SVM的位置和其他詳細資訊。

   這 `-dns-name`用戶端通常需要該參數來指定提供 DNS 名稱清單的主題備用名稱擴充。

   這 `-ipaddr`客戶端通常需要該參數來指定提供 IP 位址清單的主題備用名稱擴充。

   系統會提示您保留一份憑證要求和私密金鑰、以供日後參考。

   如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

3. 使用SVM_CA簽署CSR以產生S3伺服器的憑證：

   `security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial ca_cert_serial_number [additional_options]`

   輸入您在先前步驟中使用的命令選項：

   - `-ca` — 您在步驟 1 中輸入的 CA 的一般名稱。
   - `-ca-serial` — 步驟 1 中的 CA 序號。例如、如果CA憑證名稱為svm1_ca

_159D1587CE21E9D4_svm1_ca、序號為159D1587CE21E9D4。

根據預設、簽署的憑證將於365天內到期。您可以選取其他值、並指定其他簽署詳細資料。

出現提示時、複製並輸入您在步驟2中儲存的憑證要求字串。

隨即顯示已簽署的憑證、請儲存以供日後使用。

4. 在啟用S3的SVM上安裝簽署的憑證：

   `security certificate install -type server -vserver svm_name`

   出現提示時、請輸入憑證和私密金鑰。

   如果需要憑證鏈結、您可以選擇輸入中繼憑證。

   顯示私密金鑰和CA簽署的數位憑證時、請將其儲存以供日後參考。

5. 取得公開金鑰憑證：

   `security certificate show -vserver svm_name -common-name ca_cert_name -type root-ca -instance`

   儲存公開金鑰憑證以供稍後的用戶端組態使用。

   範例

```
cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca  -instance

                      Name of Vserver: svm1.example.com
           FQDN or Custom Common Name: svm1_ca
          Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                  Type of Certificate: root-ca
     (DEPRECATED)-Certificate Subtype: -
              Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
               Certificate Start Date: Thu May 09 10:58:39 2020
          Certificate Expiration Date: Fri May 08 10:58:39 2021
               Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----
                         Country Name: US
               State or Province Name:
                        Locality Name:
                    Organization Name:
                    Organization Unit:
Contact Administrator's Email Address:
                             Protocol: SSL
                      Hashing Function: SHA256
              Self-Signed Certificate: true
       Is System Internal Certificate: false
```

相關資訊

- "安全性憑證安裝"
- "安全證書展示"
- "安全性憑證簽署"

建立 ONTAP S3 服務資料原則

您可以為S3資料和管理服務建立服務原則。需要S3服務資料原則、才能在LIF上啟用S3資料流量。

關於這項工作

如果您使用資料生命體和叢集間生命體、則需要S3服務資料原則。如果您使用叢集生命體來處理本機分層使用案例、則不需要使用此功能。

當為LIF指定服務原則時、該原則會用來建構LIF的預設角色、容錯移轉原則和資料傳輸協定清單。

雖然可針對SVM和LIF設定多種傳輸協定、但在處理物件資料時、S3是唯一的傳輸協定、是最佳實務做法。

步驟

1. 將權限設定變更為進階：

   ```
   set -privilege advanced
   ```

2. 建立服務資料原則：

   ```
   network interface service-policy create -vserver svm_name -policy policy_name
   -services data-core,data-s3-server
   ```

   。 `data-core` 和 `data-s3-server` 雖然可視需要納入其他服務、但啟用 ONTAP S3 只需要服務。

   如"指令參考資料ONTAP"需詳細 `network interface service-policy create`資訊，請參閱。

為 **ONTAP S3** 建立資料生命

如果您建立新的SVM、您為S3存取所建立的專屬lifs應該是資料lifs。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- 如果您打算使用子網路名稱來配置LIF的IP位址和網路遮罩值、則該子網路必須已經存在。

  子網路包含屬於同一第3層子網路的IP位址集區。它們是使用建立的 `network subnet create` 命令。

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

- LIF服務原則必須已經存在。
- 最佳實務做法是、用於資料存取（資料 S3 伺服器）的生命體和用於管理作業（管理 https ）的生命體應該分開。不應在相同的 LIF 上啟用這兩項服務。
- DNS 記錄應該只有與之相關聯的資料 S3 伺服器的生命體 IP 位址。如果在 DNS 記錄中指定其他生命的 IP 位址，則其他伺服器可能會為 ONTAP S3 要求提供服務，導致非預期的回應或資料遺失。

關於這項工作

- 您可以在同一個網路連接埠上同時建立IPV4和IPv6 LIF。
- 如果叢集中有大量的生命、您可以使用來驗證叢集上支援的 LIF 容量 `network interface capacity show` 命令和 LIF 容量、可透過使用在每個節點上支援 `network interface capacity details show` 命令（進階權限層級）。

  深入瞭解 `network interface capacity show`及 `network interface capacity details show` "指令參考資料ONTAP"。

- 如果您要啟用遠端FabricPool 的靜態容量（雲端）分層、則也必須設定叢集間的LIF。

步驟

1. 建立LIF：

   ```
   network interface create -vserver svm_name -lif lif_name -service-policy
   service_policy_names -home-node node_name -home-port port_name {-address
   ```

IP_address -netmask *IP_address* | -subnet-name *subnet_name*} -firewall-policy data -auto-revert {true|false}

- -home-node 是 LIF 在返回時返回的節點 network interface revert 命令會在LIF上執行。

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

  您也可以指定 LIF 是否應該使用自動還原至主節點和主連接埠 -auto-revert 選項。

- -home-port 是 LIF 在時傳回的實體或邏輯連接埠 network interface revert 命令會在LIF上執行。
- 您可以使用指定 IP 位址 -address 和 -netmask 或是您可以使用從子網路進行分配 -subnet_name 選項。
- 使用子網路提供IP位址和網路遮罩時、如果子網路是使用閘道定義、則使用該子網路建立LIF時、會自動將通往該閘道的預設路由新增至SVM。
- 如果您手動指派IP位址（不使用子網路）、則在不同IP子網路上有用戶端或網域控制器時、可能需要設定通往閘道的預設路由。在中深入瞭解 `network route create`並建立 SVM 內的靜態路由"指令參考資料ONTAP"。
- 適用於 -firewall-policy 選項、請使用相同的預設值 data 成為 LIF 角色。

  如果需要、您可以稍後建立並新增自訂防火牆原則。

  > 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

- -auto-revert 可讓您指定資料 LIF 是否在啟動、管理資料庫狀態變更或建立網路連線等情況下自動還原至其主節點。預設設定為 false`但您可以將其設定為 `false 視環境中的網路管理原則而定。
- 。 -service-policy 選項會指定您建立的資料和管理服務原則、以及您需要的任何其他原則。

2. 如果您要在中指派 IPv6 位址 -address 選項：

   a. 使用 network ndp prefix show 用於查看在各種接口上學習的 RA 前綴列表的命令。

      。 network ndp prefix show 命令可在進階權限層級使用。

   b. 使用格式 prefix:id 手動建構 IPv6 位址。

      prefix 是在各種介面上學習的首碼。

   用於導出 id，選擇隨機 64 位元十六進位數字。

3. 使用確認 LIF 已成功建立 network interface show 命令。
4. 確認已設定的IP位址可連線：

若要驗證...	使用...
IPV4位址	network ping

若要驗證...	使用...
IPv6位址	`network ping6`

範例

下列命令顯示如何建立指派給的 S3 資料 LIF `my-S3-policy` 服務原則：

```
network interface create -vserver svm1.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

下列命令顯示叢集1中的所有LIF。資料生命週期1和資料傳輸3均設定為使用IPv4位址、而資料傳輸4則設定為使用IPv6位址：

```
cluster-1::> network interface show

            Logical    Status     Network          Current      Current Is
Vserver     Interface  Admin/Oper Address/Mask     Node         Port
Home
----------- ---------- ---------- ---------------- ------------ -------
----
cluster-1
            cluster_mgmt up/up    192.0.2.3/24     node-1       e1a
true
node-1
            clus1        up/up    192.0.2.12/24    node-1       e0a
true
            clus2        up/up    192.0.2.13/24    node-1       e0b
true
            mgmt1        up/up    192.0.2.68/24    node-1       e1a
true
node-2
            clus1        up/up    192.0.2.14/24    node-2       e0a
true
            clus2        up/up    192.0.2.15/24    node-2       e0b
true
            mgmt1        up/up    192.0.2.69/24    node-2       e1a
true
vs1.example.com
            datalif1     up/down  192.0.2.145/30   node-1       e1c
true
vs3.example.com
            datalif3     up/up    192.0.2.146/30   node-2       e0c
true
            datalif4     up/up    2001::2/64       node-2       e0c
true
5 entries were displayed.
```

相關資訊

- "網路ping"
- "網路介面"
- "顯示網路NDP前置詞"

使用 **ONTAP S3** 建立叢集間的階層式生命體，以進行遠端 **FabricPool** 分層

如果FabricPool 您使用ONTAP 支援使用支援的物件S3來啟用遠端的功能（雲端）分層、則必須設定叢集間的生命體。您可以在與資料網路共用的連接埠上設定叢集間的LIF。如此可減少叢集間網路所需的連接埠數量。

開始之前

- 基礎實體或邏輯網路連接埠必須設定為管理 `up`狀態。如"指令參考資料ONTAP"需詳細 `up`資訊，請參閱。
- LIF服務原則必須已經存在。

關於這項工作

本機Fabric集區分層或外部S3應用程式不需要叢集間生命體。

步驟

1. 列出叢集中的連接埠：

   ```
   network port show
   ```

   下列範例顯示中的網路連接埠 `cluster01`：

   ```
   cluster01::> network port show
                                                                  Speed
   (Mbps)
   Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
   ------ --------- ------------ ---------------- ----- -------
   ------------
   cluster01-01
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   cluster01-02
          e0a       Cluster      Cluster          up     1500   auto/1000
          e0b       Cluster      Cluster          up     1500   auto/1000
          e0c       Default      Default          up     1500   auto/1000
          e0d       Default      Default          up     1500   auto/1000
   ```

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

2. 在系統SVM上建立叢集間LIF：

   ```
   network interface create -vserver Cluster -lif LIF_name -service-policy
   default-intercluster -home-node node -home-port port -address port_IP -netmask
   netmask
   ```

   以下範例建立叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02`：

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

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

3. 驗證是否已建立叢集間的LIF：

```
network interface show -service-policy default-intercluster
```

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0c
true
```

4. 驗證叢集間的LIF是否為備援：

```
network interface show -service-policy default-intercluster -failover
```

以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在上 `e0c` 連接埠將容錯移轉至 `e0d` 連接埠。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

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

建立 **ONTAP S3** 物件存放區伺服器

與由NAS和SAN伺服器提供的檔案或區塊儲存設備相比、物件儲存伺服ONTAP 器可將資料管理為S3物件ONTAP 。

開始之前

您應準備好將S3伺服器名稱輸入為完整網域名稱（FQDN）、用戶端將使用此名稱來存取S3。FQDN不得以儲存區名稱開頭。使用虛擬代管型存取貯體時、伺服器名稱會用作 `mydomain.com`。例如 `bucketname.mydomain.com`：。

您應該擁有自我簽署的CA憑證（在先前步驟中建立）或由外部CA廠商簽署的憑證。本機分層使用案例不需要CA憑證、因為IP流量只會流經叢集生命體。

關於這項工作

建立物件存放區伺服器時、會建立一個具有UID 0的root使用者。不會為此root使用者產生存取金鑰或秘密金鑰。ONTAP 管理員必須執行 `object-store-server users regenerate-keys` 命令來設定此使用者的存取金鑰和秘密金鑰。

NetApp最佳實務做法是、請勿使用此root使用者。任何使用root使用者存取金鑰或秘密金鑰的用戶端應用程式、都能完整存取物件存放區中的所有儲存區和物件。

如"指令參考資料ONTAP"需詳細 `vserver object-store-server`資訊，請參閱。

範例 **24.** 步驟

系統管理員

如果您要將S3伺服器新增至現有的儲存VM、請使用此程序。若要將S3伺服器新增至新的儲存VM、請參閱"為S3建立儲存SVM"。

您應準備好輸入介面角色資料的IP位址。

1. 在現有的儲存VM上啟用S3。
   a. 選取儲存 VM ：按一下 * 儲存 > 儲存 VM* 、選取儲存 VM 、按一下 * 設定 * 、然後按一下 * S2* 下的。
   b. 按一下「啟用**S2**」、然後輸入「S3伺服器名稱」。
   c. 選取憑證類型。

      無論您是選擇系統產生的憑證、或是自己的憑證、用戶端存取都必須使用此憑證。

   d. 輸入網路介面。
2. 如果您選取系統產生的憑證、則在確認建立新的儲存VM時、會看到憑證資訊。按一下「下載」並儲存以供用戶端存取。
   - 不會再顯示秘密金鑰。
   - 如果您再次需要憑證資訊：按一下*儲存設備>儲存設備VM*、選取儲存設備VM、然後按一下*設定*。

CLI

1. 建立S3伺服器：

   ```
   vserver object-store-server create -vserver svm_name -object-store-server
   s3_server_fqdn -certificate-name server_certificate_name -comment text
   [additional_options]
   ```

   您可以在建立S3伺服器時或稍後隨時指定其他選項。

   - 如果您正在設定本機分層、 SVM 名稱可以是資料 SVM 或系統 SVM （叢集）名稱。
   - 憑證名稱應為伺服器憑證的名稱（終端使用者或葉憑證）、而非伺服器 CA 憑證（中繼或根 CA 憑證）。
   - 預設會在連接埠443上啟用HTTPS。您可以使用變更連接埠號碼 `-secure-listener-port` 選項。

     啟用 HTTPS 時、必須有 CA 憑證才能與 SSL/TLS 正確整合。從 ONTAP 9.15.1 開始、 S3 物件儲存支援 TLS 1.3 。

   - HTTP 預設為停用。啟用時、伺服器會在連接埠 80 上接聽。您可以使用啟用 `-is-http-enabled` 或使用變更連接埠編號 `-listener-port` 選項。

     啟用 HTTP 時、要求和回應會以純文字透過網路傳送。

2. 確認 S3 已設定：

```
vserver object-store-server show
```

範例

此命令可驗證所有物件儲存伺服器的組態值：

```
cluster1::> vserver object-store-server show

            Vserver: vs1

                      Object Store Server Name: s3.example.com
                          Administrative State: up
                        Listener Port For HTTP: 80
                   Secure Listener Port For HTTPS: 443
                                  HTTP Enabled: false
                                 HTTPS Enabled: true
             Certificate for HTTPS Connections: svm1_ca
                                       Comment: Server comment
```

將儲存容量新增至啟用**S3**的**SVM**

建立 **ONTAP S3** 儲存區

S3 物件保留在 _buckets 中。它們不是嵌套在其他目錄內的目錄內的檔案。

開始之前

包含 S3 伺服器的儲存 VM 必須已經存在。

關於這項工作

- 從 ONTAP 9.14.1 開始、在 S3 FlexGroup 磁碟區上建立貯體時、已啟用自動調整大小功能。如此可避免在現有和新的 FlexGroup 磁碟區上建立貯體時過度分配容量。根據下列準則、 FlexGroup 磁碟區的大小會調整為所需的最小大小。所需的最小大小是 FlexGroup Volume 中所有 S3 儲存區的總大小。
  - 從 ONTAP 9.14.1 開始、如果在建立新的儲存區時建立 S3 FlexGroup Volume 、則會以所需的最小大小建立 FlexGroup Volume 。
  - 如果在 ONTAP 9.14.1 之前建立 S3 FlexGroup Volume 、則在 ONTAP 9.14.1 之後建立或刪除的第一個儲存區、會將 FlexGroup 磁碟區調整為所需的最小大小。
  - 如果 S3 FlexGroup Volume 是在 ONTAP 9.14.1 之前建立的、而且已有最低需求大小、則在 ONTAP 9.14.1 之後建立或刪除儲存區、會維持 S3 FlexGroup 磁碟區的大小。
- 儲存服務層級是預先定義的調適性服務品質（QoS）原則群組、具有_value_、_Performance _和_Extreme _預設層級。您也可以定義自訂QoS原則群組、並將其套用至儲存區、而非預設的儲存服務層級之一。如需儲存服務定義的詳細資訊，請參閱"儲存服務定義"。如需效能管理的詳細資訊，請參閱"效能管理"。
  從ONTAP 供應儲存設備開始、預設會啟用QoS。您可以在資源配置程序期間或稍後時間停用 QoS 、或選擇自訂 QoS 原則。
- 如果您正在設定本機容量分層、您可以在資料儲存 VM 中建立貯體和使用者、而不是在 S3 伺服器所在的系統儲存 VM 中建立。

- 若要進行遠端用戶端存取、您必須在啟用S3的儲存VM中設定儲存區。如果您在未啟用S3的儲存VM中建立儲存貯體、則只能用於本機分層。
- 從 ONTAP 9.14.1 開始、您就可以了 "在 MetroCluster 組態中的鏡射或無鏡射 Aggregate 上建立貯體"。
- 在CLI中、當您建立儲存庫時、有兩種資源配置選項：
  - 讓ONTAP Select 底層的集合體和FlexGroup 元件不再存在（預設）
    - 透過自動選取集合體、即可為第一個儲存區建立及設定一個等量磁碟區。ONTAP FlexGroup它會自動選取適用於您平台的最高服務層級、或是您可以指定儲存服務層級。您稍後在儲存 VM 中新增的任何其他貯體、都會有相同的基礎 FlexGroup Volume 。
    - 或者、您也可以指定是否要使用儲存區進行分層、在這種情況ONTAP 下、VMware會嘗試選擇低成本的媒體、為階層式資料提供最佳效能。
  - 您可以選取基礎 Aggregate 和 FlexGroup 元件（需要進階權限命令選項）：您可以選擇手動選取必須建立儲存區和包含 FlexGroup 磁碟區的集合體、然後指定每個集合體的組成數量。新增其他庫位時：
    - 如果您為新的貯體指定集合體和成員、FlexGroup 將會為新的貯體建立新的功能區。
    - 如果您未指定新儲存區的集合體和成員、則新儲存區將會新增至現有FlexGroup 的版本資訊區。請參閱 資料區管理FlexGroup 以取得更多資訊。

      當您在建立貯體時指定集合體和成員時、不會套用預設或自訂的QoS原則群組。您可以稍後使用來執行 `vserver object-store-server bucket modify` 命令。

    如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket modify`資訊，請參閱。

*附註：*如果您是供應Cloud Volumes ONTAP 來自支援對象的鏟斗、則應使用CLI程序。強烈建議您手動選取基礎Aggregate、以確保它們僅使用一個節點。使用兩個節點的集合體可能會影響效能、因為節點將位於不同地理位置的可用度區域、因此容易受到延遲問題的影響。

使用 **ONTAP CLI** 建立 **S3** 儲存區

1. 如果您打算自行選取集合體和 FlexGroup 元件、請將權限等級設為進階（否則管理權限等級就足夠了）：`set -privilege advanced`
2. 建立儲存庫：

   ```
   vserver object-store-server bucket create -vserver <svm_name> -bucket
   <bucket_name> -size [integer{KB|MB|GB|TB|PB}] [-comment text]
   [additional_options]
   ```

   儲存 VM 名稱可以是資料儲存 VM 、也可以是 `Cluster` （系統儲存 VM 名稱）（如果您正在設定本機分層）。

   如果您想ONTAP 要根據效能或使用量來建立儲存庫、請使用下列其中一個選項：

   - 服務層級

     包括 `-storage-service-level` 具有下列其中一個值的選項： `value`、 `performance`或 `extreme`。

   - 分層

包括 `-used-as-capacity-tier true` 選項。

如果您要指定要在其上建立基礎FlexGroup 的流通量的集合體、請使用下列選項：

- `-aggr-list` 參數指定用於 FlexGroup Volume 組成的集合體清單。

  清單中的每個項目都會在指定的Aggregate上建立一個組成項目。您可以多次指定集合體、以便在集合上建立多個成員。

為了在FlexGroup 整個Singfuse Volume中提供一致的效能、所有的集合體都必須使用相同的磁碟類型和RAID群組組組態。

- `-aggr-list-multiplier` 參數會指定在所列的集合體上重複的次數 `-aggr-list` 建立 FlexGroup Volume 時的參數。

  的預設值 `-aggr-list-multiplier` 參數為 4 。

3. 視需要新增QoS原則群組：

   ```
   vserver object-store-server bucket modify -bucket bucket_name -qos-policy
   -group qos_policy_group
   ```

4. 確認儲存庫建立：

   ```
   vserver object-store-server bucket show [-instance]
   ```

範例

以下範例為儲存 VM 建立儲存區 `vs1` 大小 `1TB` 並指定 Aggregate ：

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

使用 System Manager 建立 S3 儲存區

1. 在啟用S3的儲存VM上新增儲存區。
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、然後輸入大小。
      - 如果您此時按一下*「儲存*」、就會以下列預設設定建立儲存區：
        - 除非任何群組原則已經生效、否則不會授予使用者桶的存取權。

          您不應該使用S3 root使用者來管理ONTAP 物件儲存設備並分享其權限、因為它對物件儲存區的存取權限不受限制。而是使用您指派的管理權限來建立使用者或群組。

        - 服務品質（效能）等級、是您系統可用的最高等級。

- 按一下 * 儲存 * 以建立具有這些預設值的貯體。

設定其他權限和限制

您可以按一下「 * 更多選項 * 」來設定物件鎖定、使用者權限和效能層級的設定、或是稍後修改這些設定。

如果您打算使用S3物件存放區FabricPool 來進行分層、請考慮選擇*用於分層*（使用低成本媒體、為階層式資料提供最佳效能）、而非效能服務層級。

如果在貯體上啟用版本設定，則可以使用 S3 用戶端，將物件鎖定保留時間放在物件的特定版本上。鎖定物件的特定版本並不會阻止刪除物件的其他版本。如果您想要啟用物件的版本設定以供稍後恢復、請選取 * 啟用版本管理 * 。如果您啟用貯體上的物件鎖定、預設會啟用版本設定。如需物件版本設定的相關資訊，請參閱 "在適用於 Amazon 的 S3 儲存區中使用版本設定"。

從 9.14.1 開始、 S3 儲存區支援物件鎖定。建立貯體時，必須啟用 S3 物件鎖定。無法在先前存在的貯體上啟用物件鎖定。物件鎖定只能用於原生 S3 使用案例。設定為使用 S3 傳輸協定的多重傳輸協定 NAS 磁碟區應使用 SnapLock 將資料提交至 WORM 儲存設備。S3 物件鎖定需要標準 SnapLock 授權。本授權隨附於"ONTAP One"。

在 ONTAP One 之前、 SnapLock 授權已包含在安全性與法規遵循套件中。安全性與法規遵循套件已不再提供、但仍有效。雖然目前並不需要"升級至 ONTAP One"、但現有客戶仍可選擇。如果您在儲存桶上啟用物件鎖定，您應該"確認已安裝 SnapLock 授權" 。如果未安裝SnapLock許可證，則必須"安裝"啟用物件鎖定之前，請先執行此操作。

當您確認已安裝 SnapLock 授權時、若要保護您的儲存區中的物件、避免遭到刪除或覆寫、請選取 * 啟用物件鎖定 * 。鎖定功能可在所有或特定版本的物件上啟用、而且只有在叢集節點初始化 SnapLock 規範時鐘時才會啟用。請遵循下列步驟：

1. 如果未在叢集的任何節點上初始化 SnapLock 規範時鐘、則會出現 * 初始化 SnapLock 規範時鐘 * 按鈕。按一下 * 初始化 SnapLock Compliance Clock* 、初始化叢集節點上的 SnapLock 規範時鐘。
2. 選取 * Governance * 模式以啟動時間鎖定、允許對物件執行寫入一次、讀取多（ WORM ）權限。即使在 _Governance 模式中、具有特定權限的系統管理員使用者也可以刪除物件。
3. 如果您想要指派更嚴格的物件刪除和更新規則、請選取 * 符合性 * 模式。在此物件鎖定模式中、只有在指定的保留期間完成時、物件才能過期。除非指定保留期間、否則物件會無限期地保持鎖定。
4. 如果您希望鎖定在特定期間內生效、請指定鎖定的保留期限（以天或年為單位）。

> 鎖定適用於版本控制和非版本控制的 S3 貯體。物件鎖定不適用於 NAS 物件。

您可以為貯體設定保護和權限設定、以及效能服務層級。

> 您必須先建立使用者和群組、才能設定權限。

如需相關資訊，請參閱 "為新的儲存貯體建立鏡射"。

確認可存取貯體

在 S3 用戶端應用程式（無論是 ONTAP S3 或外部第三方應用程式）上、您可以輸入下列命令來驗證您對新建立的儲存區的存取：

- S3伺服器CA憑證。
- 使用者的存取金鑰和秘密金鑰。
- S3伺服器FQDN名稱和儲存區名稱。

增加或減少 **ONTAP S3** 貯體尺寸

必要時、您可以增加或減少現有貯體的大小。

步驟

您可以使用系統管理員或 ONTAP CLI 來管理貯體大小。

系統管理員

1. 選擇 * 儲存 > 鏟斗 * 、並找出您要修改的鏟斗。
2. 按一下 ⋮ 貯體名稱旁的、然後選取 * 編輯 * 。
3. 在 * 編輯貯體 * 視窗中、變更貯體的容量。
4. * 儲存 * 。

CLI

1. 變更貯體容量：

```
vserver object-store-server bucket modify -vserver <SVM_name>
-bucket <bucket_name> -size {<integer>[KB|MB|GB|TB|PB]}
```

在 **MetroCluster** 組態中的鏡射或無鏡射集合體上建立 **ONTAP S3** 儲存區

從 ONTAP 9.14.1 開始、您可以在 MetroCluster FC 和 IP 組態中的鏡射或無鏡射集合體上配置貯體。

關於這項工作

- 根據預設、儲存區會配置在鏡射的集合體上。
- 中所述的相同資源配置準則 "建立儲存庫" 適用於在 MetroCluster 環境中建立貯體。
- MetroCluster 環境 * 不 * 支援下列 S3 物件儲存功能：
  - SnapMirror S3
  - S3 貯體生命週期管理
  - S3 物件鎖定在 * 符合性 * 模式

    支援 * Governance * 模式中的 S3 物件鎖定。

  - 本機 FabricPool 分層

開始之前

包含S3伺服器的SVM必須已經存在。

建立貯體的程序

CLI

1. 如果您打算自行選取集合體和 FlexGroup 元件、請將權限等級設為進階（否則管理權限等級就足夠了）：`set -privilege advanced`
2. 建立儲存庫：

   `vserver object-store-server bucket create -vserver <svm_name> -bucket <bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates true/false]`

   設定 `-use-mirrored-aggregates` 選項 `true` 或 `false` 視您要使用鏡射或無鏡射的 Aggregate 而定。

   依預設 `-use-mirrored-aggregates` 選項設定為 `true`。

   - SVM 名稱必須是資料 SVM 。
   - 如果您未指定任何選項、 ONTAP 會建立一個 800GB 儲存庫、並將服務層級設為系統可用的最高層級。
   - 如果您想ONTAP 要根據效能或使用量來建立儲存庫、請使用下列其中一個選項：
     - 服務層級

       包括 `-storage-service-level` 具有下列其中一個值的選項： `value`、 `performance`或 `extreme`。

     - 分層

       包括 `-used-as-capacity-tier true` 選項。
   - 如果您要指定要在其上建立基礎FlexGroup 的流通量的集合體、請使用下列選項：
     - 。 `-aggr-list` 參數指定用於 FlexGroup Volume 組成的集合體清單。

       清單中的每個項目都會在指定的Aggregate上建立一個組成項目。您可以多次指定集合體、以便在集合上建立多個成員。

   為了在FlexGroup 整個Singfuse Volume中提供一致的效能、所有的集合體都必須使用相同的磁碟類型和RAID群組組態。

   - 。 `-aggr-list-multiplier` 參數會指定在所列的集合體上重複的次數 `-aggr-list` 建立 FlexGroup Volume 時的參數。

     的預設值 `-aggr-list-multiplier` 參數為 4 。
3. 視需要新增QoS原則群組：

   `vserver object-store-server bucket modify -bucket *bucket_name* -qos-policy -group *qos_policy_group*`
4. 確認儲存庫建立：

```
vserver object-store-server bucket show [-instance]
```

範例

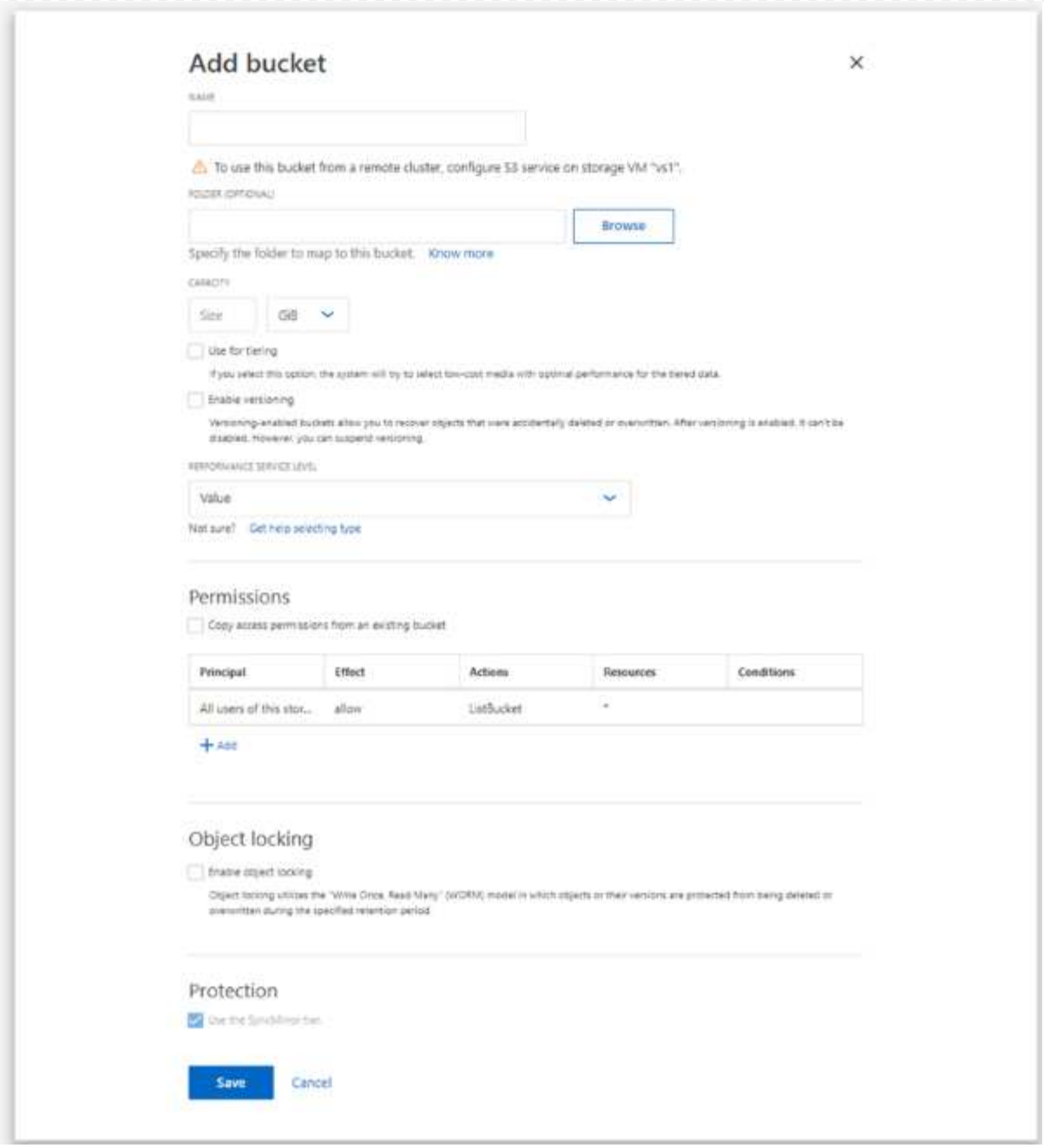
以下範例為鏡射集合體上大小為 1TB 的 SVM VS1 建立貯體：

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket  -size 1TB -use-mirrored-aggregates
true
```

系統管理員

1. 在啟用S3的儲存VM上新增儲存區。
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、然後輸入大小。

      根據預設、儲存區會配置在鏡射的 Aggregate 上。如果您想要在未鏡射的 Aggregate 上建立貯體、請選取 * 更多選項 * 、然後取消核取 * 保護 * 下的 * 使用 SyncMirror 垛層 * 方塊、如下圖所示：



- 如果您此時按一下*「儲存*」、就會以下列預設設定建立儲存區：
  - 除非任何群組原則已經生效、否則不會授予使用者桶的存取權。

    您不應該使用S3 root使用者來管理ONTAP 物件儲存設備並分享其權限、因為它對物件儲存區的存取權限不受限制。而是使用您指派的管理權限來建立使用者或群組。

  - 服務品質（效能）等級、是您系統可用的最高等級。
- 您可以按一下*更多選項*來設定使用者權限和效能層級、或是稍後再修改這些設定。
  - 您必須先建立使用者和群組、才能使用*其他選項*來設定其權限。
  - 如果您打算使用S3物件存放區FabricPool 來進行分層、請考慮選擇*用於分層*（使用低成本媒體、為階層式資料提供最佳效能）、而非效能服務層級。

2. 在 S3 用戶端應用程式（另一個 ONTAP 系統或外部第三方應用程式）上，輸入下列命令以驗證對新儲存庫的存取：
   - S3伺服器CA憑證。
   - 使用者的存取金鑰和秘密金鑰。
   - S3伺服器FQDN名稱和儲存區名稱。

建立 **ONTAP S3** 儲存區生命週期管理規則

從 ONTAP 9.13.1 開始、您可以建立生命週期管理規則、以管理 S3 儲存區的物件生命週期。您可以定義貯體中特定物件的刪除規則、並透過這些規則將這些貯體物件過期。如此一來、您就能符合保留要求、並有效管理整個 S3 物件儲存。

如果您的貯體物件啟用物件鎖定、則物件到期的生命週期管理規則將不會套用至鎖定的物件。如需物件鎖定的相關資訊、請參閱 "建立儲存庫"。

開始之前

- 已啟用S3的SVM必須已存在S3伺服器和儲存區。請參閱 "為S3建立SVM" 以取得更多資訊。
- 在多重傳輸協定 NAS 磁碟區中使用 S3 或在 MetroCluster 組態中使用 S3 時，不支援貯體生命週期管理規則。

關於這項工作

建立生命週期管理規則時、您可以將下列刪除動作套用至貯體物件：

- 刪除目前版本：此動作會使規則所識別的物件過期。如果在貯體上啟用版本設定、 S3 會使所有過期的物件無法使用。如果未啟用版本設定、則此規則會永久刪除物件。CLI 操作是 `Expiration`。
- 刪除非目前版本：此動作指定 S3 何時可永久移除非目前物件。CLI 操作是 `NoncurrentVersionExpiration`。

  非最新版本是根據目前版本的建立或修改時間而定。如果您不小心刪除或覆寫物件，延遲移除非目前物件可能會很有幫助。例如，您可以設定到期規則，在非目前版本變成非目前版本五天後，將其刪除。例如，假設您在 2014 年 1 月 1 日上午 10 ： 30 UTC 時，建立名為（版本 ID `111111`）的物件 `photo.gif`。在 2014 年 1 月 2 日上午 11 ： 30 UTC 時，您意外刪除 `photo.gif`（版本 ID `111111`），這會建立具有新版本 ID （例如版本 ID）的刪除標記 `4857693`。您現在有五天時間可以恢復（版本 ID `111111`）的原始版本 `photo.gif`，然後再進行永久刪除。2014 年 1 月 8 日 00 ： 00 UTC 時，到期的生命週期規則會在非最新版本五天後執行並永久刪除 `photo.gif`（版本 ID `111111`）。

- 刪除過期的刪除標記 - 此動作會刪除過期的物件刪除標記。
  在啟用版本設定的儲存區中、具有刪除標記的物件會成為物件的目前版本。物件不會被刪除、也無法對其執行任何動作。當沒有與這些物件相關的目前版本時、這些物件就會過期。CLI 操作是 `Expiration`。
- 刪除不完整的多部分上傳：此動作會設定允許多部分上傳保持進行中的最長時間（以天為單位）。之後將被刪除。CLI 操作是 `AbortIncompleteMultipartUpload`。

您遵循的程序取決於您使用的介面。使用 ONTAP 9.13 、 1 、您需要使用 CLI 。從 ONTAP 9.14.1 開始、您也可以使用系統管理員。

使用 **CLI** 管理生命週期管理規則

從 ONTAP 9.13.1 開始、您可以使用 ONTAP CLI 建立生命週期管理規則、使 S3 儲存區中的物件過期。

開始之前

對於 CLI 、您需要在建立貯體生命週期管理規則時、定義每個到期動作類型的必填欄位。這些欄位可在初始建立後修改。下表顯示每種行動類型的唯一欄位。

行動類型	唯一欄位
NonCurrentVersionExpiration	• `-non-curr-days` 刪除非目前版本的天數 • `-new-non-curr-versions` - 要保留的最新非最新版本數
過期	• `-obj-age-days` - 建立後的天數、之後可刪除物件的目前版本 • `-obj-exp-date` 物件到期的特定日期 • `-expired-obj-del-markers` - 清理物件刪除標記
AbortIncompleteMultiPart上 傳	• `-after-initiation-days` - 初始化的天數、之後可中止上傳

若要將貯體生命週期管理規則僅套用至特定物件子集、管理員必須在建立規則時設定每個篩選。如果在建立規則時未設定這些篩選條件、則規則會套用至貯體內的所有物件。

所有篩選器都可以在初始建立後修改、但下列項目除外： +

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

步驟

1. 使用 `vserver object-store-server bucket lifecycle-management-rule create` 命令及到期動作類型的必填欄位、以建立您的貯體生命週期管理規則。

範例

下列命令會建立 NonCurrentVersionExpiration Bucket 生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

範例

下列命令會建立到期庫位生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

範例

下列命令會建立一個 AbortIncompleteMultpartUpload 貯體生命週期管理規則：

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```

使用 **System Manager** 管理生命週期管理規則

從 ONTAP 9.14.1 開始、您可以使用系統管理員來過期 S3 物件。您可以新增、編輯及刪除 S3 物件的生命週期管理規則。此外，您也可以匯入為一個貯體建立的生命週期規則，並將其用於其他貯體中的物件。您可以停用作用中規則、稍後再啟用。

新增生命週期管理規則

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要指定到期規則的貯體。
3. 按一下 ⋮ 圖示、然後選取 * 管理生命週期規則 * 。
4. 按一下 * 新增 > 生命週期規則 * 。
5. 在「新增生命週期規則」頁面上、新增規則名稱。
6. 定義規則的範圍、無論您想要規則套用至貯體中的所有物件、或是特定物件。如果您想要指定物件、請至少新增下列其中一個篩選條件：
   a. 字首：指定規則應套用的物件金鑰名稱前置字元。通常是物件的路徑或資料夾。您可以為每個規則輸入一個前置碼。除非提供有效的前置詞、否則規則會套用至貯體中的所有物件。
   b. 標籤：針對規則應套用的物件、指定最多三個金鑰和值配對（標籤）。只有有效的金鑰可用於篩選。此值為選用項目。不過、如果您新增值、請務必僅新增對應金鑰的有效值。
   c. 大小：您可以將範圍限制在物件的最小和最大大小之間。您可以輸入其中一個或兩個值。預設單位為 MIB 。

7. 指定動作：
   a. * 使物件的目前版本過期 * ：設定規則、使所有目前物件在建立後的特定天數或特定日期永遠無法使用。如果選取 * 刪除過期的物件刪除標記 * 選項、則無法使用此選項。
   b. * 永久刪除非目前版本 * ：指定非目前版本刪除的天數，以及保留的版本數。
   c. * 刪除過期的物件刪除標記 * ：選取此動作可刪除具有過期刪除標記的物件、亦即刪除沒有關聯目前物件的標記。

      當您選取「 * 使物件的目前版本過期 * 」選項、並在保留期間之後自動刪除所有物件時、此選項將無法使用。使用物件標籤進行篩選時、也無法使用此選項。

   d. * 刪除不完整的多部份上傳 * ：設定要刪除不完整多部份上傳的天數。如果在指定保留期間內進行中的多個部分上傳失敗、您可以刪除不完整的多個部分上傳。使用物件標籤進行篩選時、此選項將無法使用。
   e. 按一下「 * 儲存 * 」。

匯入生命週期規則

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要匯入到期規則的貯體。
3. 按一下 ⋮ 圖示、然後選取 * 管理生命週期規則 * 。
4. 按一下 * 新增 > 匯入規則 * 。
5. 選取您要從中匯入規則的貯體。將顯示為所選儲存庫所定義的生命週期管理規則。
6. 選取您要匯入的規則。您可以選擇一次選取一個規則、預設選擇是第一個規則。
7. 按一下*匯入*。

編輯、刪除或停用規則

您只能編輯與規則相關的生命週期管理動作。如果使用物件標籤篩選規則、則無法使用 * 刪除過期物件刪除標記 * 和 * 刪除不完整的多部分上傳 * 選項。

當您刪除規則時、該規則將不再套用至先前關聯的物件。

1. 按一下 * 儲存 > 鏟斗 * 。
2. 選取您要編輯、刪除或停用生命週期管理規則的儲存區。
3. 按一下 ⋮ 圖示、然後選取 * 管理生命週期規則 * 。
4. 選取所需規則。您可以一次編輯及停用一個規則。您可以一次刪除多個規則。
5. 選取 * 編輯 * 、 * 刪除 * 或 * 停用 * 、然後完成程序。

建立 **ONTAP S3** 使用者

建立具有特定權限的 S3 使用者。所有 ONTAP 物件存放區都需要使用者授權、才能限制連線至授權用戶端。

開始之前。

啟用 S3 的儲存 VM 必須已經存在。

關於這項工作

S3 使用者可以存取儲存 VM 中的任何儲存區。當您建立 S3 使用者時、也會為使用者產生存取金鑰和秘密金鑰。應與使用者共用這些資源、以及物件存放區的 FQDN 和貯體名稱。

為了提高安全性、從 ONTAP 9.15.1 開始、只有在建立 S3 使用者時才會顯示存取金鑰和秘密金鑰、而且無法再次顯示。如果金鑰遺失，"必須重新產生新金鑰"。

您可以在儲存區原則或物件伺服器原則中、將特定的存取權限授予S3使用者。

當您建立新的物件存放區伺服器時、 ONTAP 會建立 root 使用者（ UID 0 ）、這是具有存取所有儲存區權限的使用者。NetApp 不建議以 root 使用者身分管理 ONTAP S3 、而是建議以特定權限建立管理員使用者角色。

CLI

1. 建立S3使用者：
   `vserver object-store-server user create -vserver svm_name -user user_name -comment [-comment text] -key-time-to-live time`

   - 新增註解是選擇性的。
   - 從 ONTAP 9.14.1 開始、您可以定義金鑰在中有效的時間週期 `-key-time-to-live` 參數。您可以使用此格式新增保留期間、以指出存取金鑰過期的期間：
     `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
     例如、如果您想要輸入一天、兩小時、三分鐘和四秒的保留期間、請將值輸入為 `P1DT2H3M4S`。除非另有說明、金鑰的有效時間不限。

     以下範例建立名稱為的使用者 `sm_user1` 在儲存 VM 上 `vs0`，關鍵保留期為一週。

   ```
   vserver object-store-server user create -vserver vs0 -user sm_user1 -key-time-to-live P1W
   ```

2. 請務必儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

系統管理員

1. 按一下「儲存設備>儲存設備**VM**」。選取您需要新增使用者的儲存 VM 、選取 * 設定 * 、然後按一下 S3 下的。
2. 若要新增使用者、請按一下 * 使用者 > 新增 * 。
3. 輸入使用者名稱。
4. 從 ONTAP 9.14.1 開始、您可以指定為使用者建立之存取金鑰的保留期間。您可以指定金鑰自動過期的保留期間（以天、小時、分鐘或秒為單位）。依預設、此值設為 `0` 這表示金鑰無限期有效。
5. 按一下「 * 儲存 * 」。系統會建立使用者、並為使用者產生存取金鑰和秘密金鑰。
6. 下載或儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

後續步驟

- 建立或修改S3群組

建立或修改 **ONTAP S3** 使用者群組，以控制對儲存區的存取

您可以建立具有適當存取授權的使用者群組、以簡化儲存庫存取。

開始之前

啟用S3的SVM中的S3使用者必須已經存在。

關於這項工作

S3群組中的使用者可以被授予SVM中任何儲存區的存取權、但不能在多個SVM中存取。群組存取權限可透過兩種方式進行設定：

- 在鏟斗層級

  建立S3使用者群組之後、您可以在Bucket原則聲明中指定群組權限、這些權限只會套用至該儲存區。

- 在SVM層級

  建立S3使用者群組之後、您可以在群組定義中指定物件伺服器原則名稱。這些原則會決定群組成員的儲存區和存取權。

系統管理員

1. 編輯儲存 VM ：按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。
2. 新增群組：選取*群組*、然後選取*新增*。
3. 輸入群組名稱、然後從使用者清單中選取。
4. 您可以選取現有的群組原則或立即新增原則、也可以稍後新增原則。

CLI

1. 建立S3群組：
   `vserver object-store-server group create -vserver svm_name -name group_name -users user_name\(s\) [-policies policy_names] [-comment text\]`
   。 `-policies` 在物件存放區中只有一個儲存區的組態中、可以省略選項；群組名稱可以新增至儲存區原則。
   。 `-policies` 選項可在稍後隨一起新增 `vserver object-store-server group modify` 建立物件儲存伺服器原則之後的命令。

重新產生 **ONTAP S3** 金鑰並修改其保留期間

使用者建立期間會自動產生存取金鑰和秘密金鑰、以啟用 S3 用戶端存取。如果金鑰過期或洩漏、您可以重新產生使用者的金鑰。

如需建立存取金鑰的相關資訊、請參閱 "建立S3使用者"。

系統管理員

1. 按一下「儲存設備>儲存設備**VM**」、然後選取儲存設備VM。
2. 在 * 設定 * 索引標籤中、按一下 * S2* 方塊。
3. 在 * 使用者 * 索引標籤中、確認沒有存取金鑰、或金鑰已過期。
4. 如果您需要重新產生金鑰、請按一下 使用者旁邊的、然後按一下 * 重新產生金鑰 * 。
5. 根據預設、產生的金鑰在不確定的時間內有效。從 9.14.1 開始、您可以修改金鑰的保留期間、之後金鑰會自動過期。以天、小時、分鐘或秒為單位輸入保留期間。
6. 按一下「 * 儲存 * 」。金鑰即會重新產生。金鑰保留期間的任何變更都會立即生效。
7. 下載或儲存存取金鑰和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

CLI

1. 執行以重新產生使用者的存取和秘密金鑰 `vserver object-store-server user regenerate-keys` 命令。
2. 根據預設、產生的金鑰會無限期有效。從 9.14.1 開始、您可以修改金鑰的保留期間、之後金鑰會自動過期。您可以使用以下格式新增保留期間：
   `P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
   例如、如果您想要輸入一天、兩小時、三分鐘和四秒的保留期間、請將值輸入為 `P1DT2H3M4S`。

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name
   -user user -key-time-to-live 0
   ```

3. 儲存存取和秘密金鑰。從 S3 用戶端進行存取時、需要使用這些資料。

建立或修改存取原則聲明

瞭解 **ONTAP S3** 儲存區和物件儲存區伺服器原則

使用者和群組對S3資源的存取權是由儲存區和物件存放區伺服器原則所控制。如果您的使用者或群組數量不多、在庫位層級控制存取可能就足夠了、但如果您有許多使用者和群組、則更容易控制物件庫伺服器層級的存取。

將存取規則新增至預設的 **ONTAP S3** 儲存區原則

您可以將存取規則新增至預設的儲存區原則。其存取控制的範圍是包含貯體的範圍、因此當有單一貯體時、最適合使用此功能。

開始之前

已啟用 S3 的儲存 VM 必須已存在、其中包含 S3 伺服器和儲存區。

在授予權限之前、您必須先建立使用者或群組。

關於這項工作

您可以為新使用者和群組新增聲明、也可以修改現有聲明的屬性。如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket policy`資訊，請參閱。

使用者和群組權限可在建立儲存區時或稍後視需要授予。您也可以修改儲存區容量和QoS原則群組指派。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

步驟

1. 編輯儲存桶：按一下「儲存設備>儲存桶」、按一下所需的儲存桶、然後按一下「編輯」。
新增或修改權限時、您可以指定下列參數：
   - 主要：授予存取權的使用者或群組。
   - * effect*：允許或拒絕存取使用者或群組。
   - 動作：特定使用者或群組的儲存庫允許動作。
   - 資源：儲存區內已授予或拒絕存取的物件路徑和名稱。

     預設值*_bucketname_*和*_bucketname/_會授予儲存區中所有物件的存取權。您也可以授與單一物件的存取權、例如***_Bucketname/_** readme.txt*。
   - 條件（選用）：嘗試存取時會評估的運算式。例如、您可以指定允許或拒絕存取的IP位址清單。

> 從 ONTAP 9.14.1 開始、您可以在 * 資源 * 欄位中指定貯體原則的變數。這些變數是預留位置、在評估原則時會以關聯式值取代。例如、 If `${aws:username}` 會指定為原則的變數、然後此變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。

CLI

步驟

1. 在庫位政策中加入聲明：

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid
text] [-index integer]
```

下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取
`-action`	您可以指定 `*` 表示所有動作、或是下列一或多個動作清單： `GetObject`, `PutObject`, `DeleteObject`, `ListBucket`, `GetBucketAcl`,`GetObjectAcl`, `ListBucketMultipartUploads`, 和 `ListMultipartUploadParts`。
`-principal`	一或多個S3使用者或群組的清單。 • 最多可指定10個使用者或群組。 • 如果已指定 S3 群組、則該群組必須採用格式 `group/group_name`. • `*` 可以指定為公開存取、也就是說、無需存取金鑰和秘密金鑰即可存取。 • 如果未指定主體、則會授予儲存 VM 中的所有 S3 使用者存取權。

`-resource`	儲存區及其所包含的任何物件。萬用字元 `*` 和 `?` 可用於形成用於指定資源的規則運算式。對於資源、您可以在原則中指定變數。這些原則變數是預留位置、在評估原則時會以關聯式值取代。

您可以選擇性地指定文字字串做為的註解 `-sid` 選項。

範例

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定允許存取物件儲存區伺服器使用者使用者 1 的讀我資料夾。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal user1 -resource
bucket1/readme/* -sid "fullAccessToReadmeForUser1"
```

以下範例為儲存 VM svm1.example.com 和 Bucket1 建立物件儲存區伺服器貯體原則聲明、指定物件儲存區伺服器群組群組 1 的所有物件存取權。

```
cluster1::> vserver object-store-server bucket policy statement create
-vserver svm1.example.com -bucket bucket1 -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket -principal group/group1
-resource bucket1/* -sid "fullAccessForGroup1"
```

從 ONTAP 9.14.1 開始、您可以指定貯體原則的變數。以下範例為儲存 VM 建立伺服器儲存區原則聲明 `svm1` 和 `bucket1`**和指定** `${aws:username}` 做為原則資源的變數。評估原則時、原則變數會以要求內容使用者名稱取代、並可依照該使用者的設定來執行原則動作。例如、評估下列原則陳述時、`${aws:username}` 替換為執行 S3 作業的使用者。如果是使用者 `user1` 執行作業時、會授予該使用者存取權 `bucket1` 做為 `bucket1/user1/*`。

```
cluster1::> object-store-server bucket policy statement create -vserver
svm1 -bucket bucket1 -effect allow -action * -principal - -resource
bucket1,bucket1/${aws:username}/*##
```

建立或修改 **ONTAP S3** 物件存放區伺服器原則

您可以建立可套用至物件存放區中一或多個儲存區的原則。物件存放區伺服器原則可附加至使用者群組、因此可簡化跨多個資源區的資源存取管理。

開始之前

已啟用S3的SVM必須已存在S3伺服器和儲存區。

關於這項工作

您可以在物件儲存伺服器群組中指定預設或自訂原則、以在SVM層級啟用存取原則。原則只有在群組定義中指定之後才會生效。

使用物件儲存伺服器原則時、您可以在群組定義中指定主體（即使用者和群組）、而非在原則本身中指定主體。

有三種唯讀的預設原則可供存取ONTAP 不完整的S3資源：

- FullAccess
- NoS3 存取
- ReadOnlyAccess

您也可以建立新的自訂原則、然後為新使用者和群組新增陳述式、或是修改現有陳述式的屬性。如"指令參考資料ONTAP"需詳細 `vserver object-store-server policy`資訊，請參閱。

從 ONTAP 9.9.1 開始、如果您計畫在 ONTAP S3 伺服器上支援 AWS 用戶端物件標記功能、就會執行這些動作 `GetObjectTagging`、 `PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

您遵循的程序取決於您使用的介面- System Manager或CLI：

系統管理員

使用**System Manager**建立或修改物件存放區伺服器原則

步驟

1. 編輯儲存 VM ：按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。
2. 新增使用者：按一下*原則*、然後按一下*新增*。
   a. 輸入原則名稱、然後從群組清單中選取。
   b. 選取現有的預設原則或新增原則。

      新增或修改群組原則時、您可以指定下列參數：

      - 群組：授予存取權的群組。
      - 效果：允許或拒絕存取一或多個群組。
      - 行動：特定群組的一個或多個儲存桶中允許的行動。
      - 資源：一或多個儲存區內的物件路徑和名稱、這些儲存區已授予或拒絕存取權限。例如：
        - ***授予對儲存VM中所有儲存區的存取權。
        - * Bucketname*與* Bucketname/*可授予特定儲存區中所有物件的存取權。
        - * Bucketname/readme.txt*可讓您存取特定儲存區中的物件。
   c. 如有需要、請在現有原則中新增陳述式。

CLI

使用**CLI**建立或修改物件存放區伺服器原則

步驟

1. 建立物件儲存伺服器原則：

   ```
   vserver object-store-server policy create -vserver svm_name -policy
   policy_name [-comment text]
   ```

2. 建立原則聲明：

   ```
   vserver object-store-server policy statement create -vserver svm_name
   -policy policy_name -effect {allow|deny} -action object_store_actions
   -resource object_store_resources [-sid text]
   ```

   下列參數定義存取權限：

`-effect`	此聲明可能允許或拒絕存取

`-action`	您可以指定 * 表示所有動作、或是下列一或多個動作清單： `GetObject, PutObject, DeleteObject, ListBucket,GetBucketAcl, GetObjectAcl, ListAllMyBuckets, ListBucketMultipartUploads`，和 `ListMultipartUploadParts`。
`-resource`	儲存區及其所包含的任何物件。萬用字元 * 和 ？可用於形成用於指定資源的規則運算式。

您可以選擇性地指定文字字串做為的註解 `-sid` 選項。

根據預設、新的對帳單會新增至對帳單清單的結尾、並依順序處理。稍後新增或修改說明時、您可以選擇修改說明 `-index` 設定以變更處理順序。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定外部目錄服務以進行 **ONTAP S3** 存取

從 ONTAP 9.14.1 開始、外部目錄的服務已與 ONTAP S3 物件儲存設備整合。這項整合可透過外部目錄服務簡化使用者和存取管理。

您可以為屬於外部目錄服務的使用者群組提供存取 ONTAP 物件儲存環境的權限。輕量型目錄存取傳輸協定（ LDAP ）是與 Active Directory 等目錄服務進行通訊的介面、可為身分識別與存取管理（ IAM ）提供資料庫和服務。若要提供存取權、您必須在 ONTAP S3 環境中設定 LDAP 群組。設定存取權限之後、群組成員就擁有 ONTAP S3 工作區的權限。有關 LDAP 的信息，請參見"了解如何在 ONTAP NFS SVM 上使用 LDAP 名稱服務"。

您也可以將 Active Directory 使用者群組設定為快速繫結模式、以便驗證使用者認證、並透過 LDAP 連線驗證協力廠商和開放原始碼 S3 應用程式。

開始之前

在設定 LDAP 群組及啟用群組存取的快速繫結模式之前、請先確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱。 "設定DNS服務"
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱。 "在 SVM 上安裝自簽名根 CA 憑證"
5. LDAP 用戶端在 SVM 上設定為啟用 TLS 。請參閱"為 ONTAP NFS 存取建立 LDAP 用戶端配置"和"將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯以獲取資訊"。

設定 **S3** 的 **LDAP** 存取

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

深入瞭解 ONTAP 命令參照中的連結： https://docs 。 NetApp 。 ONTAP - CLI/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^] 命令。

2. 使用建立物件儲存庫貯體原則聲明 `principal` 設定為您要授與存取權的 LDAP 群組：

```
object-store-server bucket policy statement create -bucket <bucket-name>
-effect allow -principal nasgroup/<ldap-group-name> -resource <bucket-
name>, <bucket-name>/*
```

範例：下列範例建立的 Bucket 原則陳述式 `buck1`。原則允許 LDAP 群組存取 `group1` 至資源（貯體及其物件） `buck1`。

```
vserver object-store-server bucket policy add-statement -bucket buck1
-effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts,
ListBucketVersions,GetObjectTagging,PutObjectTagging,DeleteObjectTagging
,GetBucketVersioning,PutBucketVersioning -principal nasgroup/group1
-resource buck1, buck1/*
```

3. 驗證 LDAP 群組中的使用者 `group1` 能夠從 S3 用戶端執行 S3 作業。

使用 **LDAP** 快速繫結模式進行驗證

1. 將 LDAP 指定為 SVM 的名稱服務資料庫 _ 、以用於群組、並將密碼指定為 LDAP ：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

深入瞭解 ONTAP 命令參照中的連結： https://docs 。 NetApp 。 ONTAP - CLI/vserver-services-name-service-ns-switch-modify.html[`vserver services name-service ns-switch modify`^] 命令。

2. 確保存取 S3 儲存貯體的 LDAP 使用者具有在儲存庫原則中定義的權限。如需詳細資訊、請參閱 "修改庫位原則"。
3. 確認 LDAP 群組中的使用者可以執行下列作業：

a. 在 S3 用戶端上以下列格式設定存取金鑰：範例 "NTAPFASTBIND"： + base64 編碼（ LDAPUser:password ），結果就是 `NTAPFASTBINDbGRhcHVzZXI6cGFzc3dvcmQ=`這樣 `"NTAPFASTBIND" + base64-encode(user-name:password)`

> S3 用戶端可能會提示輸入秘密金鑰。如果沒有秘密金鑰、則可以輸入至少 16 個字元的任何密碼。

b. 從使用者具有權限的 S3 用戶端執行基本 S3 作業。

Base64 認證

ONTAP S3 的預設組態不包括 HTTP ，而且僅使用 HTTPS 和傳輸層安全性（ TLS ）連線。ONTAP 可以產生自我簽署的憑證，但建議的最佳做法是使用來自協力廠商憑證授權單位（ CA ）的憑證。使用 CA 憑證時，您會在用戶端應用程式和 ONTAP 物件存放區伺服器之間建立信任的關係。

請注意，使用 Base64 編碼的認證資料很容易解碼。使用 HTTPS 可防止中間人封包監聽器擷取編碼認證。

建立預先簽署的 URL 時，請勿使用 LDAP 快速連結模式進行驗證。驗證是以預先簽署的 URL 所包含的 Base64 存取金鑰為基礎。將向解碼 Base64 存取金鑰的任何人顯示使用者名稱和密碼。

驗證方法為 **nsswitch** ， **LDAP** 為啟用範例

```
$curl -siku <user>:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>", "name":<user>,"key_time_to_live":"PT6H3M"}
```

> 將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。

為 **Active Directory** 或 **SMB** 伺服器設定 **S3** 訪問

如果在 Bucket 原則聲明中指定的 nasgroup 或 nasgroup 的使用者沒有 UID 和 GID 集，則找不到這些屬性時，查詢會失敗。Active Directory 使用 SID ，而非 UID 。如果無法將 SID 項目對應至 UID ，則必須將必要資料帶到 ONTAP 。

若要這麼做，請使用"vserver Active Directory建立"，讓 SVM 可以透過 Active Directory 驗證，並取得必要的使用者和群組資訊。

或者，使用"建立Vserver CIFS"在 Active Directory 網域中建立 SMB 伺服器。

如果名稱伺服器和物件儲存使用不同的域名，則可能會遇到查找失敗的情況。為避免尋找失敗， NetApp建議使用 UPN 格式的受信任網域進行資源授權： `nasgroup/group@trusted_domain.com`受信任網域是指已新增至 SMB 伺服器受信任網域清單中的網域。了解如何"新增、刪除和修改首選信任域"在 SMB 伺服器清單中。

當驗證方法是網域且信任的網域是在 **Active Directory** 中設定時，會產生金鑰

將端點與以 UPN 格式指定的使用者一起使用 `s3/services/<svm_uuid>/users` 。範例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user@fqdn>,"key_time_to_live":"PT6H3M"}
```

將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。

當驗證方法為網域且沒有信任的網域時，請產生金鑰

當停用 LDAP 或非 POSIX 使用者尚未設定 UID 和 GID 時，就可以執行此動作。範例：

```
$curl -siku FQDN\\user:<user_password> -X POST
https://<LIF_IP_Address>/api/protocols/s3/services/<SVM_UUID>/users -d
{"comment":"<S3_user_name>",
"name":<user[@fqdn]>,"key_time_to_live":"PT6H3M"}
```

將 API 導向叢集管理 LIF ，而非 SVM 的資料 LIF 。如果您想要允許使用者產生自己的金鑰，您必須將 HTTP 權限新增至其角色，才能使用 Curl 。此權限是 S3 API 權限的補充。如果沒有信任的網域，您只需要將選用的網域值（ @FQDN ）新增至使用者名稱。

讓 **LDAP** 或網域使用者產生自己的 **ONTAP S3** 存取金鑰

從 ONTAP 9.14.1 開始、身為 ONTAP 管理員、您可以建立自訂角色、並將其授予本機或網域群組或輕量型目錄存取傳輸協定（ LDAP ）群組、讓屬於這些群組的使用者能夠產生自己的存取權和機密金鑰、以供 S3 用戶端存取。

您必須在儲存 VM 上執行幾個組態步驟，才能建立自訂角色，並將其指派給啟動 API 以產生存取金鑰的使用者。

如果 LDAP 被停用，您可以"為ONTAP S3 存取設定外部目錄服務"允許使用者產生存取密鑰。

開始之前

請確認下列事項：

1. 已建立啟用 S3 的儲存 VM 、其中包含 S3 伺服器。請參閱 "為S3建立SVM"。
2. 該儲存 VM 中已建立一個儲存區。請參閱 "建立儲存庫"。
3. 在儲存 VM 上設定 DNS 。請參閱。 "設定DNS服務"
4. 儲存 VM 上會安裝 LDAP 伺服器的自我簽署根憑證授權單位（ CA ）憑證。請參閱。 "在 SVM 上安裝自簽名根 CA 憑證"
5. LDAP 用戶端在儲存 VM 上設定為啟用 TLS 。請參閱。 "為 ONTAP NFS 存取建立 LDAP 用戶端配置"
6. 將用戶端組態與虛擬伺服器建立關聯。請參閱。 "將 LDAP 用戶端配置與 ONTAP NFS SVM 關聯"如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

7. 如果您使用的是資料儲存 VM 、請在 VM 上建立管理網路介面（ LIF ）、以及 LIF 的服務原則。深入瞭解 `network interface create`及 `network interface service-policy create` "指令參考資料ONTAP"。

設定使用者以產生存取金鑰

範例 **25.** 步驟

LDAP 用戶

1. 將 LDAP 指定為儲存 VM 的名稱服務資料庫 _ 、以用於群組和 LDAP 密碼：

```
ns-switch modify -vserver <vserver-name> -database group -sources
files,ldap
ns-switch modify -vserver <vserver-name> -database passwd -sources
files,ldap
```

如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch modify`資訊，請參閱。

2. 建立可存取 S3 使用者 REST API 端點的自訂角色：
`security login rest-role create -vserver <vserver-name> -role <custom-role-name> -api "/api/protocols/s3/services/*/users" -access <access-type>`
在此範例中 `s3-role` 角色是針對儲存 VM 上的使用者所產生 `svm-1`，授予所有存取權限、讀取、建立及更新。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

如"指令參考資料ONTAP"需詳細 `security login rest-role create`資訊，請參閱。

3. 使用以下方式建立 LDAP 使用者群組 `security login`命令並新增用於存取 S3 使用者 REST API 端點的新自訂角色。詳細了解 `security login create`在"指令參考資料ONTAP" 。

```
security login create -user-or-group-name <ldap-group-name>
-application http -authentication-method nsswitch -role <custom-
role-name> -is-ns-switch-group yes
```

在此範例中、是 LDAP 群組 `ldap-group-1` 是在中建立的 `svm-1`**以及自訂角色** `s3role` 新增至 IT 以存取 API 端點、並在快速繫結模式中啟用 LDAP 存取。

```
security login create -user-or-group-name ldap-group-1 -application
http -authentication-method nsswitch -role s3role -is-ns-switch
-group yes -second-authentication-method none -vserver svm-1 -is
-ldap-fastbind yes
```

如需更多資訊、請參閱 "使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。

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

將自訂角色新增至 LDAP 群組允許該群組中的使用者對ONTAP進行有限的訪問 `/api/protocols/s3/services/{svm.uuid}/users`端點。透過呼叫 API，LDAP 群組使用者可以產生自己的存取

金鑰和金鑰來存取 S3 用戶端。他們只能為自己產生密鑰，而不能為其他使用者產生密鑰。

網域用戶

1. 建立可以存取 S3 使用者 REST API 端點的自訂角色：

```
security login rest-role create -vserver <vserver-name> -role <custom-
role-name> -api "/api/protocols/s3/services/*/users" -access <access-
type>
```

在此範例中， `s3-role`為儲存虛擬機器上的使用者產生角色 `svm-1` ，授予所有存取權限，即讀取、建立和更新。

```
security login rest-role create -vserver svm-1 -role s3role -api
"/api/protocols/s3/services/*/users" -access all
```

如"指令參考資料ONTAP"需詳細 `security login rest-role create`資訊，請參閱。

1. 使用以下方式建立網域使用者群組 `security login`命令並新增用於存取 S3 使用者 REST API 端點的新自訂角色。詳細了解 `security login create`在"指令參考資料ONTAP" 。

   ```
   security login create -vserver <vserver-name> -user-or-group-name
   domain\<group-name> -application http -authentication-method domain
   -role <custom-role-name>
   ```

   在此範例中，網域組 `domain\group1`創建於 `svm-1`以及自訂角色 `s3role`添加到其中以存取 API 端點。

   ```
   security login create -user-or-group-name domain\group1 -application
   http -authentication-method domain -role s3role -vserver svm-1
   ```

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

將自訂角色新增至網域群組允許該群組中的使用者對ONTAP進行有限的訪問 `/api/protocols/s3/services/{svm.uuid}/users`端點。透過呼叫 API，網域組使用者可以產生自己的存取金鑰和金鑰來存取 S3 用戶端。他們只能為自己產生密鑰，而不能為其他使用者產生密鑰。

做為 **S3** 或 **LDAP** 使用者、產生您自己的存取金鑰

從 ONTAP 9.14.1 開始、如果您的系統管理員已授予您自行產生金鑰的角色、您就可以產生自己的存取權和秘密金鑰、以供存取 S3 用戶端。您只能使用下列 ONTAP REST API 端點自行產生金鑰。

建立 **S3** 使用者並產生金鑰

此 REST API 呼叫使用下列方法和端點。有關此端點的更多信息，請參閱參考 "API 文件" 。

HTTP方法	路徑
貼文	/api/protocols / s3/services / ｛ SVM.uuid ｝ / 使用者

對於網域用戶，請使用以下格式作為 S3 使用者名稱： `user@fqdn` ， 在哪裡 `fqdn`是域的完全限定域名。

Curl範例

```
curl
--request POST \
--location "https://$FQDN_IP /api/protocols/s3/services/{svm.uuid}/users "
\
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
--data '{"name":"user1@example.com"}'
```

Json輸出範例

```
{
  "records": [
    {
      "access_key": "4KX07KF7ML8YNWY01JWG",
      "_links": {
        "next": {
          "href": "/api/resourcelink"
        },
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

為 **S3** 使用者重新產生金鑰

如果 S3 使用者已存在，您可以重新產生其存取金鑰和金鑰。此 REST API 呼叫使用下列方法和端點。

HTTP方法	路徑
修補	/api/protocols/s3/services/{svm.uuid}/使用者/{名稱}

Curl範例

```
curl
--request PATCH \
--location "https://$FQDN_IP
/api/protocols/s3/services/{svm.uuid}/users/{name} " \
--include \
--header "Authorization: Basic $BASIC_AUTH" \
--data '{"regenerate_keys":"True"}'
```

Json輸出範例

```
{
  "records": [
    {
      "access_key": "DX12U609DMRVD8U30Z1M",
      "_links": {
        "self": {
          "href": "/api/resourcelink"
        }
      },
      "name": "user1@example.com",
      "secret_key": "<secret_key_value>"
    }
  ],
  "num_records": "1"
}
```

允許用戶端存取**S3**物件儲存設備

啟用**ONTAP** 對遠端**FabricPool** 分層的支援功能、以存取**S3**

若要將S3用作遠端的不同步容量（雲端）層、則必須由S3管理員向遠端的不同步叢集管理員提供S3伺服器組態的相關資訊。ONTAP FabricPool ONTAP ONTAP

關於這項工作

若要設定FabricPool SURE Cloud階層、必須提供下列S3伺服器資訊：

- 伺服器名稱（FQDN）
- 儲存區名稱
- CA憑證
- 存取金鑰
- 密碼（秘密存取金鑰）

此外、還需要下列網路組態：

- DNS ONTAP 伺服器中必須有一個遠端不完整的S3伺服器主機名稱項目、該伺服器是針對管理SVM設定的、包括S3伺服器的FQDN名稱及其lifs上的IP位址。
- 雖然不需要叢集對等、但必須在本機叢集上設定叢集間生命量。

請參閱FabricPool 《關於將ONTAP S3設定為雲端層的支援文件》。

"使用FabricPool 不實的功能來管理儲存設備層"

啟用**ONTAP** 對本地**FabricPool** 資訊的「支援」功能、以存取「**S3**」

若要將S3用作本地的「不支援能力」層、您必須根據建立的儲存區來定義物件存放區、然後將物件存放區附加至效能層集合體、以建立一個「不支援功能」ONTAP FabricPool FabricPool 。

開始之前

您必須擁有 ONTAP S3 伺服器名稱和貯體名稱、而且 S3 伺服器必須使用叢集生命體（搭配使用）建立 `-vserver Cluster` 參數）。

關於這項工作

物件存放區組態包含有關本機容量層的資訊、包括S3伺服器、儲存區名稱和驗證需求。

建立後的物件存放區組態不得重新關聯至不同的物件存放區或儲存區。您可以為本機層建立多個儲存區、但無法在單一儲存區中建立多個物件存放區。

本地容量層不需要使用此功能的證書。FabricPool

步驟

1. 建立本機容量層的物件存放區：

   ```
   storage aggregate object-store config create -object-store-name store_name
   -ipspace Cluster -provider-type ONTAP_S3 -server S3_server_name -container
   -name bucket_name -access-key access_key -secret-password password
   ```

   - 。 `-container-name` 是您建立的 S3 儲存區。
   - 。 `-access-key` 參數會將要求授權給 ONTAP S3 伺服器。
   - 。 `-secret-password` 參數（秘密存取金鑰）會驗證對 ONTAP S3 伺服器的要求。
   - 您可以設定 `-is-certificate-validation-enabled` 參數至 `false` 停用 ONTAP S3 的憑證檢查。

   ```
   cluster1::> storage aggregate object-store config create
   -object-store-name MyLocalObjStore -ipspace Cluster -provider-type
   ONTAP_S3 -server s3.example.com
   -container-name bucket1 -access-key myS3key -secret-password myS3pass
   ```

2. 顯示並驗證物件存放區組態資訊：

```
storage aggregate object-store config show
```

3. 選用 "使用非作用中的資料報告來判斷Volume中有多少資料處於非作用中狀態"：。

   查看磁碟區中有多少資料處於非作用中狀態、有助於決定哪些Aggregate用於FabricPool 本地分層。

4. 將物件存放區附加至Aggregate：

   ```
   storage aggregate object-store attach -aggregate aggr_name -object-store-name store_name
   ```

   您可以使用 `allow-flexgroup` **`true`** 可附加包含 FlexGroup Volume 成分的集合體。

   ```
   cluster1::> storage aggregate object-store attach
   -aggregate aggr1 -object-store-name MyLocalObjStore
   ```

5. 顯示物件存放區資訊、並驗證附加的物件存放區是否可用：

   ```
   storage aggregate object-store show
   ```

   ```
   cluster1::> storage aggregate object-store show

   Aggregate    Object Store Name    Availability State
   ---------    -----------------    ------------------
   aggr1        MyLocalObjStore      available
   ```

相關資訊

- "存儲聚合物件存儲附加"
- "儲存聚合物件儲存配置創建"
- "儲存聚合物件儲存配置顯示"
- "儲存聚合物件儲存顯示"

啟用 **S3** 用戶端應用程式以存取 **ONTAP S3** 伺服器

若要讓S3用戶端應用程式存取ONTAP S3伺服器、ONTAP 則該管理員必須向S3使用者提供組態資訊。

開始之前

S3用戶端應用程式必須能夠使用ONTAP 下列AWS簽名版本、使用支援驗證的功能：

- 簽名版本4 ONTAP 、更新版本
- 簽名版本2 ONTAP 、更新版本

其他的簽名版本不受ONTAP 支援。

此S3管理員必須已建立S3使用者、並在儲存區原則或物件儲存伺服器原則中、以個別使用者或群組成員的身分授予他們存取權限。ONTAP

S3用戶端應用程式必須能夠解析ONTAP 不支援的S3伺服器名稱、ONTAP 因為該名稱需要由S3管理員提供S3伺服器的正式作業的S3伺服器名稱（FQDN）和IP位址。

關於這項工作

若要存取ONTAP S3儲存區、S3用戶端應用程式的使用者會輸入ONTAP 由S3管理員提供的資訊。

從S9.9開始ONTAP 、ONTAP 支援下列AWS用戶端功能的不支援SS3伺服器：

- 使用者定義的物件中繼資料

  使用PUT（或POST）建立物件時、可將一組金鑰值配對指派給物件做為中繼資料。在物件上執行取得/取得作業時、會傳回使用者定義的中繼資料以及系統中繼資料。

- 物件標記

  您可以指派一組個別的金鑰值配對作為標籤、以便將物件分類。與中繼資料不同的是、標記是以物件的REST API獨立建立和讀取、而且會在物件建立或之後的任何時間執行。

> 若要讓用戶端取得及放置標記資訊、請採取行動 `GetObjectTagging`、`PutObjectTagging`和 `DeleteObjectTagging` 需要使用貯體或群組原則來允許。

如需詳細資訊、請參閱AWS S3文件。

步驟

1. 輸入S3伺服器名稱和CA憑證、以ONTAP 驗證S3用戶端應用程式與S3伺服器。
2. 輸入下列資訊、在S3用戶端應用程式上驗證使用者：
   - S3伺服器名稱（FQDN）和儲存區名稱
   - 使用者的存取金鑰和秘密金鑰

ONTAP S3 儲存服務層級

包含預先定義的儲存服務、這些服務會對應到對應的最低效能因素。ONTAP

叢集或SVM中可用的實際儲存服務集、取決於SVM中組成集合體的儲存設備類型。

下表顯示如何將最低效能因素對應至預先定義的儲存服務：

儲存服務	預期**IOPS**（**SLA**）	尖峰**IOPS**（**SLO**）	最小**Volume IOPS**	預估延遲	預期的**IOPS**是否強制執行？
價值	每 TB 128 個	每 TB 512 個	75	17毫秒	在本網站上：是的AFF 否則：不會

儲存服務	預期**IOPS**（**SLA**）	尖峰**IOPS**（**SLO**）	最小**Volume IOPS**	預估延遲	預期的**IOPS**是否強制執行？
效能	每TB 2048個	每 TB 4096 個	500	2毫秒	是的
極致	每 TB 6144 個	每 TB 12288 個	1000	1毫秒	是的

下表定義每種媒體或節點類型的可用儲存服務層級：

媒體或節點	可用的儲存服務層級
磁碟	價值
虛擬機器磁碟	價值
混合式	價值
容量最佳化的Flash	價值
固態硬碟（SSD）-非AFF	價值
效能最佳化的Flash - SSD（AFF VMware）	極致、效能、價值

為 **ONTAP S3** 貯體設定跨來源資源共享（ **CORS** ）

從 ONTAP 9 。 16.1 開始，您可以設定跨來源資源共用（ CORS ），以允許來自不同網域的用戶端 Web 應用程式存取您的 ONTAP 儲存區。這可讓您使用網頁瀏覽器安全存取貯體物件。

CORS 是以 HTTP 為基礎的架構，可讓一個網頁中定義的指令碼存取不同網域中伺服器的資源。此架構用於安全地繞過 _ 相同來源原則 _ ，這是網路安全的早期基礎。主要概念與術語如下所述。

來源

來源可精確定義資源的位置和身分識別。其表示為下列值的組合：

- URI 方案（傳輸協定）
- 主機名稱（網域名稱或 IP 位址）
- 連接埠號碼

以下是來源的簡單範例： `https://www.mycompany.com:8001` 。當與 CORS 搭配使用來源時，它會識別提出要求的用戶端。

相同來源原則

同一來源原則（ SOP ）是適用於瀏覽器型指令碼的安全概念和限制。只要兩個網頁位於同一個來源，原則就能讓最初從網頁載入的指令碼存取另一個網頁中的資料。這項限制可防止惡意指令碼存取不同來源頁面中的資料。

常見 **CORS** 使用案例

CORS 有幾種一般使用案例。大部分涉及定義完善的跨網域存取執行個體，例如 AJAX 要求，載入字型，樣式表和指令碼，以及跨網域驗證。CORS 也可作為單頁應用程式（ SPA ）的一部分來實作。

HTTP 標頭

CORS 是使用插入 HTTP 要求和回應的標頭來實作。例如，有數個回應標頭可實作存取控制，並指出允許哪些作業，包括方法和標頭。HTTP 要求中存在 *origority* 標頭，將其定義為跨網域要求。CORS 伺服器會使用來源值來找出有效的 CORS 組態。

HTTP 預航要求

這是一項選擇性要求，可用來初步判斷伺服器是否支援 CORS ，包括特定方法和標頭。根據回應， CORS 要求可以完成，也可以不完成。

ONTAP 鏟斗

貯體是根據定義完善的命名空間儲存及存取的物件容器。ONTAP 貯體有兩種類型：

- 可透過 NAS 和 S3 傳輸協定存取的 NAS 貯體
- 只能透過 S3 傳輸協定存取的 S3 貯體

ONTAP 中的 **CORS** 實作

默認情況下， CORS 在 ONTAP 9 · 16.1 和更高版本中啓用。您需要在每個要啟用的 SVM 上設定 CORS 。

> 沒有管理選項可停用 ONTAP 叢集的 CORS 。不過，您可以透過不定義任何規則或刪除所有現有規則來有效停用它。

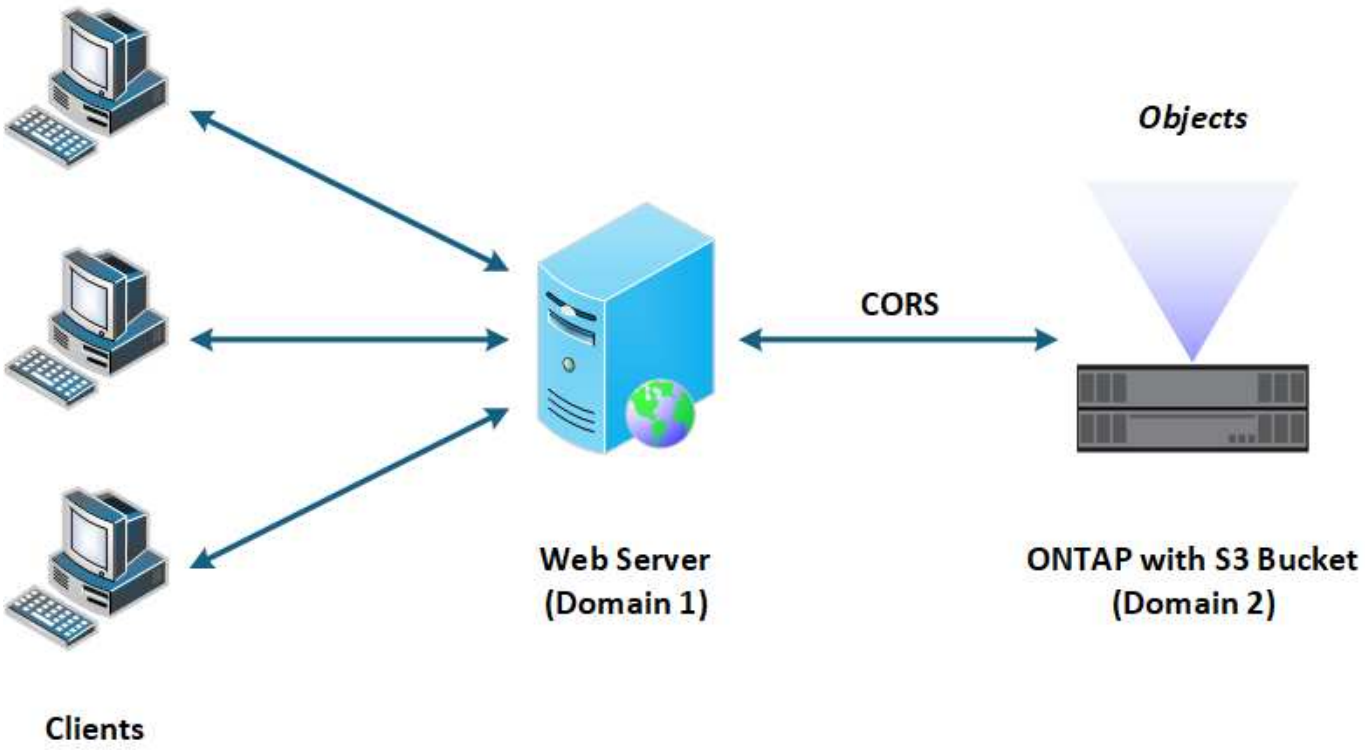
可能的使用案例

ONTAP CORS 實作可啟用多種可能的跨網域資源存取拓撲，包括：

- ONTAP S3 貯體（位於相同或不同的 SVM 或叢集內）
- ONTAP NAS 貯體（位於相同或不同的 SVM 或叢集內）
- ONTAP S3 和 NAS 貯體（位於相同或不同的 SVM 或叢集內）
- ONTAP 貯體和外部廠商貯體
- 不同時區的貯體

高階檢視

以下說明 CORS 如何讓您深入瞭解 ONTAP S3 儲存區。



定義 **CORS** 規則

您必須在 ONTAP 中定義 CORS 規則，才能啟動及使用此功能。

組態動作

ONTAP 支援三個主要組態規則動作：

- 顯示
- 建立
- 刪除

ONTAP 中定義的 CORS 規則有多種屬性，包括 SVM 和儲存庫，以及允許的來源，方法和標頭。

系統管理選項

在 ONTAP 叢集上管理 CORS 時，您有多種選項可供選擇。

指令行介面**ONTAP**

您可以使用命令列介面來設定 CORS 。如需詳細資訊、請參閱 使用 CLI 管理 CORS 。

靜態API ONTAP

您可以使用 ONTAP REST API 來設定 CORS 。沒有新增任何端點來支援 CORS 功能。您可以改用下列現有端點：

```
/api/protocols/s3/services/{svm.uuid}/buckets/{bucket.uuid}
```

如需詳細資訊，請參閱 "ONTAP 自動化文件"。

S3 API

您可以使用 S3 API 在 ONTAP 貯體上建立及刪除 CORS 組態。S3 用戶端管理員需要足夠的 Privileges ，包括：

- 存取或秘密金鑰認證
- 設定在儲存區上的原則，以允許透過 s3api 存取

升級與還原

如果您計畫使用 CORS 來存取 ONTAP S3 儲存區，您應該注意到幾個管理問題。

升級

當所有節點都升級至 9.16.1 時，便支援 CORS 功能。在混合模式叢集中，只有有效叢集版本（ ECV ）為 9.16.1 或更新版本時，才能使用此功能。

還原

從使用者的角度來看，所有 CORS 組態都應該先移除，叢集還原才能繼續進行。在內部，此作業會刪除所有 CORS 資料庫。系統會要求您執行命令，以清除及還原這些資料結構。

使用 CLI 管理 CORS

您可以使用 ONTAP CLI 來管理 CORS 規則。主要作業如下所述。您必須處於 ONTAP * 管理 * 權限層級，才能發出 CORS 命令。

建立

您可以使用命令來定義 CORS 規則 `vserver object-store-server bucket cors-rule create`。如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket cors-rule create`資訊，請參閱。

參數

用於建立規則的參數如下所述。

參數	說明
`vserver`	指定主控建立規則之物件儲存區伺服器儲存區的 SVM （ Vserver ）名稱。
`bucket`	物件存放區伺服器上為其建立規則的貯體名稱。
`index`	可選參數，指出建立規則的物件儲存區伺服器貯體索引。

參數	說明
`rule id`	物件存放區伺服器貯體規則的唯一識別碼。
`allowed-origins`	允許產生跨來源要求的來源清單。
`allowed-methods`	跨來源要求中所允許的 HTTP 方法清單。
`allowed-headers`	跨網域請求中允許的 HTTP 標頭清單。
`expose-headers`	額外標頭清單會傳送 CORS 回應，客戶可從其應用程式存取。
`max-age-in-seconds`	選用參數，指定瀏覽器應快取特定資源的預航回應的時間量。

範例

```
vserver object-store-server bucket cors-rule create -vserver vs1 -bucket
bucket1 -allowed-origins www.myexample.com -allowed-methods GET,DELETE
```

顯示

您可以使用命令 `vserver object-store-server bucket cors-rule show`來顯示目前規則及其內容的清單。如"指令參考資料ONTAP"需詳細 `vserver object-store-server bucket cors-rule show`資訊，請參閱。

包含參數 `-instance`可擴充每個規則的顯示資料。您也可以指定想要的欄位。

範例

```
server object-store-server bucket cors-rule show -instance
```

刪除

您可以使用 delete 命令來移除 CORS 規則的執行個體。您需要 `index`規則的值，因此這是以兩個步驟執行的作業：

1. 發出 `show`命令以顯示規則並擷取其索引。
2. 使用索引值發出刪除。

範例

```
vserver object-store-server bucket cors-rule delete -vserver vs1 -bucket
bucket1 -index 1
```

修改

沒有 CLI 命令可用來修改現有 CORS 規則。若要修改規則，您必須執行下列動作：

1. 刪除現有規則。
2. 使用所需的選項建立新規則。

使用 SnapMirror S3 保護貯體

瞭解 ONTAP SnapMirror S3

從 ONTAP 9.10.1 開始、您可以使用 SnapMirror 鏡射和備份功能、保護 ONTAP S3 物件儲存區中的貯體。與標準 SnapMirror 不同、 SnapMirror S3 可將鏡像與備份複製到非 NetApp 目的地、例如 AWS S3 。

SnapMirror S3 支援從 ONTAP S3 儲存區到下列目的地的主動鏡射和備份層：

目標	支援作用中鏡像和接管？	支援備份與還原？
SS3 ONTAP • 相同SVM中的儲存區 • 位於同一個叢集上不同SVM中的儲存區 • 不同叢集上的SVM儲存區	是的	是的
StorageGRID	否	是的
AWS S3	否	是的
適用於 Azure Cloud Volumes ONTAP	是的	是的
AWS 適用的 Cloud Volumes ONTAP	是的	是的
適用於 Google Cloud Cloud Volumes ONTAP	是的	是的

您可以保護ONTAP 現有的SS3伺服器庫位、也可以立即啟用資料保護功能、建立新的庫位。

SnapMirror S3 要求

- 版本ONTAP

  ONTAP 9.10.1 或更新版本必須在來源叢集和目的地叢集上執行。

  MetroCluster 組態不支援 SnapMirror S3 。

- 授權

  中提供下列授權 "ONTAP One" ONTAP 來源和目的地系統需要軟體套件、才能提供下列存取：

  - ONTAP S3 傳輸協定與儲存設備

- SnapMirror S3 目標為其他 NetApp 物件存放區目標（ ONTAP S3 、 StorageGRID 和 Cloud Volumes ONTAP ）
- SnapMirror S3 目標協力廠商物件儲存區、包括 AWS S3 （可在中取得"ONTAP One 相容性套件"）
- 如果您的叢集執行的是 ONTAP 9.10.1 ，則需要 A "不含授權FabricPool"。

- SS3 ONTAP
  - SS3伺服器必須執行來源和目的地SVM。ONTAP
  - 建議但不需要在裝載S3伺服器的系統上安裝TLS存取的CA憑證。
    - 用於簽署 S3 伺服器憑證的 CA 憑證必須安裝在主控 S3 伺服器之叢集的管理儲存 VM 上。
    - 您可以使用自我簽署的CA憑證或外部CA廠商所簽署的憑證。
    - 如果來源或目的地儲存VM未使用HTTPS接聽、則不需要安裝CA憑證。
- 對等（ONTAP 適用於S3目標）
  - 必須設定叢集間的生命體（用於遠端 ONTAP 目標）、來源叢集和目的地叢集的叢集間生命體可連線至來源和目的地 S3 伺服器資料生命體。
  - 來源和目的地叢集會被處理（用於遠端ONTAP 的不確定目標）。
  - 來源和目的地儲存VM都會被處理（適用於所有ONTAP 的物件）。
- SnapMirror原則
  - 所有 SnapMirror S3 關係都需要 S3 專屬的 SnapMirror 原則、但您可以針對多個關係使用相同的原則。
  - 您可以建立自己的原則或接受預設的*連續*原則、其中包含下列值：
    - 節流（處理量/頻寬上限）-無限。
    - 恢復點目標時間：1小時（3、600秒）。

> 請注意、當兩個 S3 儲存區處於 SnapMirror 關係中時、如果設定了生命週期原則、使物件的目前版本過期（刪除）、則會將相同的動作複寫到合作夥伴儲存區。即使合作夥伴儲存庫為唯讀或被動式、也會發生這種情況。

- 根使用者金鑰 SnapMirror S3 關係需要 Storage VM 根使用者存取金鑰； ONTAP 預設不會指派這些金鑰。首次建立 SnapMirror S3 關係時，必須驗證來源儲存虛擬機器和目標儲存虛擬機器上是否存在金鑰，如果不存在，則必須重新產生金鑰。如果您需要重新產生這些金鑰、您必須確保使用存取和秘密金鑰配對的所有用戶端和SnapMirror物件儲存組態、都會以新的金鑰更新。

如需S3伺服器組態的相關資訊、請參閱下列主題：

- "在儲存VM上啟用S3伺服器"
- "關於 ONTAP S3 組態程序"

如需叢集與儲存VM對等關係的相關資訊、請參閱下列主題：

- "準備鏡射與保存（System Manager、步驟1至6）"
- "叢集與SVM對等（CLI）"

支援的 **SnapMirror** 關係

SnapMirror S3 支援扇出和級聯關係。有關概述，請參閱"横向和串聯資料保護部署" 。

SnapMirror S3 不支援以風扇方式部署（多個來源貯體和單一目的地貯體之間的資料保護關係）。SnapMirror S3 可支援從多個叢集到單一次要叢集的多個儲存區鏡像、但每個來源儲存區都必須在次要叢集上擁有自己的目的地儲存區。

MetroCluster 環境不支援 SnapMirror S3 。

控制對 **S3** 儲存區的存取

建立新的儲存庫時、您可以建立使用者和群組來控制存取。

雖然 SnapMirror S3 會將物件從來源貯體複寫到目的地貯體，但不會將使用者，群組和原則從來源物件存放區複寫到目的地物件存放區。

必須在目的地物件存放區上設定使用者，群組原則，權限及類似元件，以便用戶端在容錯移轉事件期間存取目的地儲存區。

來源和目的地使用者可以使用相同的存取和秘密金鑰，前提是在目的地叢集上建立使用者時，必須手動提供來源金鑰。例如：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

如需詳細資訊、請參閱下列主題：

- "新增S3使用者和群組（系統管理員）"
- "建立S3使用者（CLI）"
- "建立或修改S3群組（CLI）"

將 **S3** 物件鎖定及版本設定搭配 **SnapMirror S3** 使用

您可以在啟用物件鎖定和版本設定的 ONTAP 儲存區上使用 SnapMirror S3 ，但需注意以下幾點：

- 若要在啟用物件鎖定的情況下複寫來源貯體，目的地貯體也必須啟用物件鎖定。此外，來源和目的地都必須啟用版本設定。如此可避免在兩個貯體都有不同的預設保留原則時，將刪除鏡射到目的地貯體。
- S3 SnapMirror 不會複寫物件的歷史版本。只會複寫物件的目前版本。

當物件鎖定物件鏡射至目的地儲存區時，它們會維持其原始保留時間。如果複寫未鎖定的物件，則會採用目的地儲存區的預設保留期間。例如：

- 貯體 A 的預設保留期間為 30 天，而貯體 B 的預設保留期間為 60 天。從 Bucket A 複製到 Bucket B 的物件將維持其 30 天的保留期間，即使它低於 Bucket B 的預設保留期間
- 貯體 A 沒有預設保留期間，而貯體 B 的預設保留期間為 60 天。將解除鎖定的物件從儲存區 A 複寫至儲存區 B 時，將採用 60 天的保留期間。如果物件是在 Bucket A 中手動鎖定，則當複寫到 Bucket B 時，它會維持其原始保留期間

- 貯體 A 的預設保留期間為 30 天，而貯體 B 則沒有預設保留期間。從 Bucket A 複製到 Bucket B 的物件將維持其 30 天的保留期間。

遠端叢集上的鏡射與備份保護

為遠端叢集上的新 **ONTAP S3** 儲存區建立鏡射關係

建立新的 S3 儲存桶時，您可以立即將它們保護到遠端叢集上的 SnapMirror S3 目標。

關於這項工作

您需要在來源和目的地系統上執行工作。

開始之前

- 已完成有關版本、授權和S3伺服器組態的要求ONTAP 。
- 來源與目的地叢集之間存在對等關係、且來源與目的地儲存VM之間存在對等關係。
- 來源與目的地VM需要CA憑證。您可以使用由外部CA廠商簽署的自我簽署CA憑證或憑證。

系統管理員

1. 如果這是此儲存 VM 的第一個 SnapMirror S3 關係、請驗證來源與目的地儲存 VM 的根使用者金鑰是否存在、如果沒有、請重新產生根使用者金鑰：
   a. 按一下「儲存設備>儲存設備**VM**」、然後選取儲存設備VM。
   b. 在 * 設定 * 索引標籤中、按一下 * S2* 方塊。
   c. 在「使用者」索引標籤中、確認root使用者有存取金鑰。
   d. 如果沒有、請按一下 * 根 * 旁的、然後按一下 * 重新產生金鑰 * 。如果金鑰已經存在、請勿重新產生金鑰。
2. 編輯儲存VM以新增使用者、並在來源與目的地儲存VM中新增使用者至群組：

   按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。

   請參閱 "新增S3使用者和群組" 以取得更多資訊。
3. 在來源叢集上，如果您沒有現有策略且不想使用預設策略，請建立 SnapMirror S3 策略：
   a. 按一下「保護>總覽」、然後按一下「本機原則設定」。
   b. 按一下 * 保護原則 * 旁的、然後按一下 * 新增 * 。
      - 輸入原則名稱和說明。
      - 選取原則範圍、叢集或SVM
      - 針對 SnapMirror S3 關係選取 * 持續 * 。
      - 輸入您的* Throttle 和 Recovery Point Objective *值。
4. 利用SnapMirror保護建立儲存庫：
   a. 按一下「儲存設備>桶」、然後按一下「新增」。驗證權限是選用的、但建議使用。
   b. 輸入名稱、選取儲存VM、輸入大小、然後按一下*更多選項*。
   c. 在*權限*下、按一下*新增*。
      - 主體*和*效果：選取對應於使用者群組設定的值、或接受預設值。
      - **Action**- 確保顯示以下值：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 資源 * - 使用預設值 (*bucketname*, *bucketname*/*) 或其他您需要的價值。

        請參閱 "管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。
   d. 在* Protection（保護）下、勾選* Enable SnapMirror（ONTAP 支援SnapMirror（不支援或雲端）*。然後輸入下列值：
      - 目的地
        - 目標：**ONTAP** *《系統》

- 叢集：選取遠端叢集。
- 儲存**VM**：選取遠端叢集上的儲存VM。
- * S3伺服器CA憑證*：複製並貼上_SOURER_憑證的內容。

- 來源
  - * S3伺服器CA憑證：*複製並貼上_destination_憑證的內容。

5. 如果您使用由外部CA廠商簽署的憑證、請勾選*在目的地上使用相同的憑證*。
6. 如果您按一下*目的地設定*、您也可以輸入自己的值來取代庫位名稱、容量和效能服務層級的預設值。
7. 按一下「 * 儲存 * 」。在來源儲存 VM 中建立新的貯體、並將其鏡射至建立目的地儲存 VM 的新貯體。

備份鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的 S3 儲存區、並視需要進行還原。

定義新的或現有貯體的保護設定時、只要來源叢集和目的地叢集執行 ONTAP 9.14.1 或更新版本、且該物件鎖定已在來源貯體上啟用、就可以在目的地貯體上啟用物件鎖定。來源貯體的物件鎖定模式和鎖定保留期限、將適用於目的地貯體上的複寫物件。您也可以在「目標設定 * 」區段中、為目的地貯體定義不同的鎖定保留期間。此保留期間也適用於從來源貯體和 S3 介面複寫的任何非鎖定物件。

如需如何在貯體上啟用物件鎖定的相關資訊、請參閱 "建立儲存庫"。

CLI

1. 如果這是此 SVM 的第一個 SnapMirror S3 關係、請確認來源和目的地 SVM 的根使用者金鑰都存在、如果根使用者金鑰不存在、請重新產生這些金鑰：

   ```
   vserver object-store-server user show
   ```

   確認root使用者有存取金鑰。如果沒有、請輸入：

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   如果金鑰已經存在、請勿重新產生金鑰。

2. 在來源和目的地SVM中建立儲存區：

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. 將存取規則新增至來源和目的地SVM中的預設資源桶原則：

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

範例

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 在來源 SVM 上，如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個：
`snapmirror policy create -vserver *svm_name* -policy policy_name -type continuous [-rpo *integer*] [-throttle *throttle_type*] [-comment *text*] [*additional_options*]`

   參數：

   - 類型 `continuous` - SnapMirror S3 關係的唯一原則類型（必要）。
   - `-rpo` - 指定恢復點目標的時間（以秒爲單位）（可選）。
   - `-throttle` - 指定處理量 / 頻寬的上限（以千位元組 / 秒為單位）（選用）。

     範例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 在來源叢集和目的地叢集的管理SVM上安裝CA伺服器憑證：

   a. 在來源叢集上、安裝簽署 *destination* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver *src_admin_svm* -cert-name *dest_server_certificate*`

   b. 在目的地叢集上、安裝簽署 *SOURC* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver *dest_admin_svm* -cert-name *src_server_certificate*`

   如果您使用由外部CA廠商簽署的憑證、請在來源和目的地管理SVM上安裝相同的憑證。

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

6. 在來源 SVM 上，建立 SnapMirror S3 關係：

   `snapmirror create -source-path *src_svm_name*:/bucket/*bucket_name* -destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

   您可以使用所建立的原則、或接受預設值。

範例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
test-policy
```

7. 驗證鏡射是否為作用中：
   `snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

為遠端叢集上現有的 **ONTAP S3** 儲存區建立鏡射關係

您可以隨時開始保護現有的S3儲存桶、例如、如果您從ONTAP 更新版本早於VMware版9.10.1的S3組態升級。

關於這項工作

您需要在來源叢集和目的地叢集上執行工作。

開始之前

- 已完成有關版本、授權和S3伺服器組態的要求ONTAP 。
- 來源與目的地叢集之間存在對等關係、且來源與目的地儲存VM之間存在對等關係。
- 來源與目的地VM需要CA憑證。您可以使用由外部CA廠商簽署的自我簽署CA憑證或憑證。

步驟

您可以使用系統管理員或 ONTAP CLI 建立鏡射關係。

系統管理員

1. 如果這是此儲存 VM 的第一個 SnapMirror S3 關係、請驗證來源與目的地儲存 VM 的根使用者金鑰是否存在、如果沒有、請重新產生根使用者金鑰：
   a. 選取 * 儲存 > 儲存 VM* 、然後選取儲存 VM 。
   b. 在 * 設定 * 索引標籤中、按一下 * S2* 方塊。
   c. 在「使用者」索引標籤中、確認root使用者有存取金鑰。
   d. 如果沒有、請按一下 * 根 * 旁的、然後按一下 * 重新產生金鑰。 *如果金鑰已經存在、請勿重新產生金鑰。
2. 驗證現有的使用者和群組是否存在、並在來源和目的地儲存 VM 中擁有正確的存取權：選取 * 儲存 > 儲存 VM 、 * 然後選取儲存 VM 、再選取 * 設定 * 索引標籤。最後，找到 **S2** 互動程序，選擇 ，然後選擇 **Users** 選項卡，然後選擇 **Groups** 選項卡以查看用戶和組的訪問設置。

   請參閱 " 新增S3使用者和群組" 以取得更多資訊。
3. 在來源叢集上，如果您沒有現有策略且不想使用預設策略，請建立 SnapMirror S3 策略：
   a. 選取 * 保護 > 總覽 * 、然後按一下 * 本機原則設定 * 。
   b. 選取 * 保護原則 * 旁的、然後按一下 * 新增 * 。
   c. 輸入原則名稱和說明。
   d. 選取原則範圍（叢集或 SVM ）。
   e. 針對 SnapMirror S3 關係選取 * 持續 * 。
   f. 輸入您的* Throttle 和 Recovery Point Objective *值。
4. 確認現有庫位的庫位存取原則仍符合您的需求：
   a. 按一下「儲存設備>桶」、然後選取您要保護的桶。
   b. 在 * 權限 * 索引標籤中、按一下 * 編輯 * 、然後按一下 * 權限 * 下的 * 新增 * 。
      - 主要與影響：選取對應於使用者群組設定的值、或接受預設值。
      - * 操作 * ：確保顯示以下值：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 資源 * ：使用預設值 (*bucketname, bucketname/**) 或其他您需要的價值。

        請參閱 " 管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。
5. 使用 SnapMirror S3 保護功能保護現有貯體：
   a. 按一下「儲存設備」>「庫位」、然後選取您要保護的庫位。
   b. 按一下*保護*並輸入下列值：
      - 目的地
        - 目標 ONTAP ：*系統

- 叢集：選取遠端叢集。
- 儲存**VM**：選取遠端叢集上的儲存VM。
- * S3伺服器CA憑證*：複製並貼上_SOURER_憑證的內容。

- 來源
  - * S3伺服器CA憑證*：複製並貼上_destination_憑證的內容。

6. 如果您使用由外部CA廠商簽署的憑證、請勾選*在目的地上使用相同的憑證*。
7. 如果您按一下*目的地設定*、您也可以輸入自己的值來取代庫位名稱、容量和效能服務層級的預設值。
8. 按一下「 * 儲存 * 」。現有的儲存區會鏡射到目的地儲存 VM 中的新儲存區。

備份鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的 S3 儲存區、並視需要進行還原。

定義新的或現有貯體的保護設定時、只要來源叢集和目的地叢集執行 ONTAP 9.14.1 或更新版本、且該物件鎖定已在來源貯體上啟用、就可以在目的地貯體上啟用物件鎖定。來源貯體的物件鎖定模式和鎖定保留期限、將適用於目的地貯體上的複寫物件。您也可以在「目標設定 * 」區段中、為目的地貯體定義不同的鎖定保留期間。此保留期間也適用於從來源貯體和 S3 介面複寫的任何非鎖定物件。

如需如何在貯體上啟用物件鎖定的相關資訊、請參閱 "建立儲存庫"。

CLI

1. 如果這是此 SVM 的第一個 SnapMirror S3 關係、請確認來源和目的地 SVM 的根使用者金鑰都存在、如果不存在、
   `vserver object-store-server user show`請重新產生這些金鑰： + 確認根使用者有存取金鑰。如果沒有、請輸入：
   `vserver object-store-server user regenerate-keys -vserver *svm_name* -user *root*` + 如果金鑰已經存在、請勿重新產生金鑰。
2. 在目的地SVM上建立一個儲存區、做為鏡射目標：

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. 驗證來源和目的地SVM中預設資源庫原則的存取規則是否正確：

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

   範例

   ```
   src_cluster::> vserver object-store-server bucket policy add-
   statement -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 在來源 SVM 上，如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個：

   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   參數：

   - `continuous`– SnapMirror S3 關係的唯一原則類型（必要）。
   - `-rpo` –指定恢復點目標的時間（以秒爲單位）（可選）。
   - `-throttle` –指定處理量 / 頻寬的上限（以千位元組 / 秒為單位）（選用）。

     範例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 在來源叢集和目的地叢集的管理SVM上安裝CA憑證：

   a. 在來源叢集上、安裝簽署 *destination* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. 在目的地叢集上、安裝簽署 *SOURC* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

   如果您使用由外部CA廠商簽署的憑證、請在來源和目的地管理SVM上安裝相同的憑證。

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

6. 在來源 SVM 上，建立 SnapMirror S3 關係：

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   您可以使用所建立的原則、或接受預設值。

   範例

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-
   bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
   test-policy
   ```

7. 驗證鏡射是否為作用中：
   `snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

從遠端叢集上的目的地 **ONTAP S3** 儲存區接管

如果來源儲存區中的資料無法使用、您可以中斷SnapMirror關係、使目的地儲存區可寫入、並開始提供資料。

關於這項工作

執行接管作業時、來源貯體會轉換為唯讀、而原始目的地貯體會轉換為讀寫、因此會反轉 SnapMirror S3 關係。

當停用的來源貯體再次可用時、 SnapMirror S3 會自動重新同步兩個貯體的內容。不需要像Volume SnapMirror部署所需的那樣、明確重新同步關係。

接管作業必須從遠端叢集啟動。

雖然 SnapMirror S3 會將物件從來源貯體複寫到目的地貯體，但不會將使用者，群組和原則從來源物件存放區複寫到目的地物件存放區。

必須在目的地物件存放區上設定使用者，群組原則，權限及類似元件，以便用戶端在容錯移轉事件期間存取目的地儲存區。

來源和目的地使用者可以使用相同的存取和秘密金鑰，前提是在目的地叢集上建立使用者時，必須手動提供來源金鑰。例如：

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

系統管理員

從無法使用的儲存區進行容錯移轉、並開始提供資料：

1. 按一下 * 保護 > 關係 * 、然後選取 * SnapMirror S2* 。
2. 單擊 ⋮，選擇 *Failover （故障轉移） * ，然後單擊 *Failover （故障轉移） * 。

CLI

1. 針對目的地儲存區啟動容錯移轉作業：
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. 確認容錯移轉作業的狀態：
   `snapmirror show -fields status`

   範例

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/bucket/test-bucket-mirror
```

相關資訊

- "新增S3使用者和群組（系統管理員）"
- "建立S3使用者（CLI）"
- "建立或修改S3群組（CLI）"
- "SnapMirror 故障轉移啟動"
- "SnapMirror 顯示"

從遠端叢集上的目的地 **SVM** 還原 **ONTAP S3** 儲存區

如果來源貯體中的資料遺失或毀損、您可以從目的地貯體還原物件、重新填入資料。

關於這項工作

您可以將目的地庫位還原至現有的庫位或新的庫位。還原作業的目標貯體必須大於目的地貯體的邏輯使用空間。

如果您使用現有的儲存區、則在開始還原作業時必須是空的。 還原不會「回溯」儲存區的時間、而是將先前的內容填入一個空的儲存區。

還原作業必須從遠端叢集啟動。

系統管理員

還原備份的資料：

1. 按一下 * 保護 > 關係 * 、然後選取 * SnapMirror S2* 。
2. 按一下 ⋮ 、然後選取 * 還原 * 。
3. 在*來源*下、選取*現有的Bucket*（預設值）或*新的Bucket*。
   - 若要還原至*現有的Bucket *（預設值）、請完成下列動作：
     - 選取叢集和儲存VM以搜尋現有的儲存區。
     - 選取現有的庫位。
     - 複製並貼上_destination_ S3伺服器CA憑證的內容。
   - 若要還原成*新的Bucket *、請輸入下列值：
     - 用於託管新儲存區的叢集與儲存VM。
     - 新儲存庫的名稱、容量和效能服務層級。
       請參閱 "儲存服務層級" 以取得更多資訊。
     - *destination* S3伺服器CA憑證的內容。
4. 在「目的地」下、複製並貼上_SOURER_S3伺服器CA憑證的內容。
5. 按一下*保護>關係*以監控還原進度。

還原鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的貯體、並視需要進行還原。

您可以將物件鎖定的貯體還原至新的或現有的貯體。您可以在下列案例中選取物件鎖定的貯體作為目的地：

- * 還原至新的貯體 * ：啟用物件鎖定時、可建立同時啟用物件鎖定的貯體來還原貯體。當您還原鎖定的貯體時、會複寫原始貯體的物件鎖定模式和保留期間。您也可以為新的貯體定義不同的鎖定保留期間。此保留期間適用於來自其他來源的未鎖定物件。
- * 還原至現有的貯體 * ：只要現有貯體已啟用版本設定和類似的物件鎖定模式、即可將物件鎖定貯體還原至現有的貯體。保留原始貯體的保有期。
- * 還原未鎖定的貯體 * ：即使在某個貯體上未啟用物件鎖定、您仍可將其還原至已啟用物件鎖定且位於來源叢集上的貯體。當您還原貯體時、所有未鎖定的物件都會被鎖定、而且目的地貯體的保留模式和保有權也會適用於它們。

CLI

1. 建立新的目的地貯體以進行還原。如需更多資訊、請參閱 "為新的 ONTAP S3 儲存區建立雲端備份關係"。
2. 為目的地貯體啟動還原作業：
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

範例

```
dest_cluster::> snapmirror restore -source-path
src_vs1:/bucket/test-bucket -destination-path dest_vs1:/bucket/test-
bucket-mirror
```

如"指令參考資料ONTAP"需詳細 `snapmirror restore`資訊，請參閱。

本機叢集上的鏡射與備份保護

為本機叢集上的新 **ONTAP S3** 儲存區建立鏡射關係

建立新的 S3 儲存桶時，您可以立即將它們保護到同一群集上的 SnapMirror S3 目標。您可以將資料鏡射至不同儲存VM中的儲存區、或將資料鏡射至來源所在的儲存VM。

開始之前

- 已完成有關版本、授權和S3伺服器組態的要求ONTAP 。
- 來源與目的地儲存VM之間存在對等關係。
- 來源與目的地VM需要CA憑證。您可以使用由外部CA廠商簽署的自我簽署CA憑證或憑證。

系統管理員

1. 如果這是此儲存 VM 的第一個 SnapMirror S3 關係、請驗證來源與目的地儲存 VM 的根使用者金鑰是否存在、如果沒有、請重新產生根使用者金鑰：
   a. 按一下「儲存設備>儲存設備**VM**」、然後選取儲存設備VM。
   b. 在 * 設定 * 索引標籤中、按一下 S3 磚。
   c. 在「使用者」索引標籤中、確認root使用者有存取金鑰
   d. 如果沒有、請按一下 * 根 * 旁的、然後按一下 * 重新產生金鑰 * 。如果金鑰已經存在、請勿重新產生金鑰。
2. 編輯儲存 VM 以新增使用者、以及將使用者新增至群組、請在來源和目的地儲存 VM 中：按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。

   請參閱 "新增S3使用者和群組" 以取得更多資訊。
3. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
   a. 按一下 * 保護 > 總覽 * 、然後按一下 * 本機原則設定 * 。
   b. 按一下 * 保護原則 * 旁的、然後按一下 * 新增 * 。
      - 輸入原則名稱和說明。
      - 選取原則範圍、叢集或SVM
      - 針對 SnapMirror S3 關係選取 * 持續 * 。
      - 輸入您的* Throttle 和 Recovery Point Objective *值。
4. 利用SnapMirror保護建立儲存庫：
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、輸入大小、然後按一下*更多選項*。
   c. 在*權限*下、按一下*新增*。驗證權限是選用的、但建議使用。
      - 主體*和*效果：選取對應於使用者群組設定的值、或接受預設值。
      - **Actions** - 確保顯示以下值：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 資源 * - 使用預設值 `(bucketname, bucketname/*)` 或其他您需要的價值

        請參閱 "管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。
   d. 在* Protection（保護）下、勾選* Enable SnapMirror（ONTAP 支援SnapMirror（不支援或雲端）*。然後輸入下列值：
      - 目的地
        - 目標 ONTAP ：*系統
        - 叢集：選取本機叢集。

- * 儲存 VM* ：在本機叢集上選取儲存 VM 。
- * S3伺服器CA憑證*：複製並貼上來源憑證的內容。

- 來源
  - * S3伺服器CA憑證*：複製並貼上目的地憑證的內容。

5. 如果您使用由外部CA廠商簽署的憑證、請勾選*在目的地上使用相同的憑證*。
6. 如果您按一下*目的地設定*、您也可以輸入自己的值來取代庫位名稱、容量和效能服務層級的預設值。
7. 按一下「 * 儲存 * 」。在來源儲存 VM 中建立新的貯體、並將其鏡射至建立目的地儲存 VM 的新貯體。

備份鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的 S3 儲存區、並視需要進行還原。

定義新的或現有貯體的保護設定時、只要來源叢集和目的地叢集執行 ONTAP 9.14.1 或更新版本、且該物件鎖定已在來源貯體上啟用、就可以在目的地貯體上啟用物件鎖定。來源貯體的物件鎖定模式和鎖定保留期限、將適用於目的地貯體上的複寫物件。您也可以在「目標設定 * 」區段中、為目的地貯體定義不同的鎖定保留期間。此保留期間也適用於從來源貯體和 S3 介面複寫的任何非鎖定物件。

如需如何在貯體上啟用物件鎖定的相關資訊、請參閱 "建立儲存庫"。

CLI

1. 如果這是此 SVM 的第一個 SnapMirror S3 關係、請確認來源和目的地 SVM 的根使用者金鑰都存在、如果根使用者金鑰不存在、請重新產生這些金鑰：
   `vserver object-store-server user show`

   確認root使用者有存取金鑰。如果沒有、請輸入：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   如果金鑰已經存在、請勿重新產生金鑰。

2. 在來源和目的地SVM中建立儲存區：

   ```
   vserver object-store-server bucket create -vserver svm_name -bucket
   bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
   [additional_options]
   ```

3. 將存取規則新增至來源和目的地SVM中的預設資源桶原則：

   ```
   vserver object-store-server bucket policy add-statement -vserver svm_name
   -bucket bucket_name -effect {allow|deny} -action object_store_actions
   -principal user_and_group_names -resource object_store_resources [-sid
   text] [-index integer]
   ```

```
src_cluster::> vserver object-store-server bucket policy add-
statement -bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   參數：

   - `continuous`– SnapMirror S3 關係的唯一原則類型（必要）。
   - `-rpo` –指定恢復點目標的時間（以秒爲單位）（可選）。
   - `-throttle` –指定處理量 / 頻寬的上限（以千位元組 / 秒為單位）（選用）。

     範例

     ```
     src_cluster::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 在管理SVM上安裝CA伺服器憑證：
   a. 在管理 SVM 上安裝簽署 *SOURC* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. 在管理 SVM 上安裝簽署 *destination* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`

   如果您使用的是由外部 CA 廠商簽署的憑證、則只需在管理 SVM 上安裝此憑證。

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

6. 創建 SnapMirror S3 關係：
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   您可以使用所建立的原則、或接受預設值。

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
   -policy test-policy
   ```

7. 驗證鏡射是否為作用中：
   `snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

為本機叢集上現有的 **ONTAP S3** 儲存區建立鏡射關係

您可以隨時開始保護同一個叢集上的現有S3儲存區、例如、如果您從ONTAP 早於版本發行版的S3組態升級、您可以將資料鏡射至不同儲存VM中的儲存區、或將資料鏡射至來源所在的儲存VM。

開始之前

- 已完成有關版本、授權和S3伺服器組態的要求ONTAP 。
- 來源與目的地儲存VM之間存在對等關係。
- 來源與目的地VM需要CA憑證。您可以使用由外部CA廠商簽署的自我簽署CA憑證或憑證。

系統管理員

1. 如果這是此儲存 VM 的第一個 SnapMirror S3 關係、請驗證來源與目的地儲存 VM 的根使用者金鑰是否存在、如果沒有、請重新產生根使用者金鑰：
   a. 按一下「儲存設備>儲存設備**VM**」、然後選取儲存設備VM。
   b. 在 * 設定 * 索引標籤中、按一下 * S2* 方塊。
   c. 在「使用者」索引標籤中、確認root使用者有存取金鑰。
   d. 如果沒有、請按一下 * 根 * 旁的、然後按一下 * 重新產生金鑰 * 。如果金鑰已經存在、請勿重新產生金鑰
2. 驗證現有的使用者和群組是否存在、並在來源和目的地儲存 VM 中擁有正確的存取權：選取 * 儲存 > 儲存 VM 、 * 然後選取儲存 VM 、再選取 * 設定 * 索引標籤。最後，找到 **S2** 互動程序，選擇 ，然後選擇 **Users** 選項卡，然後選擇 **Groups** 選項卡以查看用戶和組的訪問設置。

   請參閱 "新增S3使用者和群組" 以取得更多資訊。
3. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
   a. 按一下「保護>總覽」、然後按一下「本機原則設定」。
   b. 按一下 * 保護原則 * 旁的、然後按一下 * 新增 * 。
      - 輸入原則名稱和說明。
      - 選取原則範圍、叢集或SVM
      - 針對 SnapMirror S3 關係選取 * 持續 * 。
      - 輸入您的* Throttle 和 Recovery Point Objective *值。
4. 確認現有庫位的庫位存取原則持續符合您的需求：
   a. 按一下「儲存設備>桶」、然後選取您要保護的桶。
   b. 在 * 權限 * 索引標籤中、按一下 * 編輯 * 、然後按一下 * 權限 * 下的 * 新增 * 。
      - 主體*和*效果：選取對應於使用者群組設定的值、或接受預設值。
      - **Actions** - 確保顯示以下值：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 資源 * - 使用預設值 *(bucketname, bucketname/*)* 或其他您需要的價值。

        請參閱 "管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。
5. 使用 SnapMirror S3 保護現有儲存庫：
   a. 按一下「儲存設備」>「庫位」、然後選取您要保護的庫位。
   b. 按一下*保護*並輸入下列值：
      - 目的地
        - 目標 ONTAP ：*系統

- 叢集：選取本機叢集。
- 儲存**VM**：選取相同或不同的儲存VM。
- * S3伺服器CA憑證*：複製並貼上_SOURER_憑證的內容。

- 來源
  - * S3伺服器CA憑證*：複製並貼上_destination_憑證的內容。

6. 如果您使用由外部CA廠商簽署的憑證、請勾選*在目的地上使用相同的憑證*。
7. 如果您按一下*目的地設定*、您也可以輸入自己的值來取代庫位名稱、容量和效能服務層級的預設值。
8. 按一下「 * 儲存 * 」。現有的儲存區會鏡射到目的地儲存 VM 中的新儲存區。

備份鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的 S3 儲存區、並視需要進行還原。

定義新的或現有貯體的保護設定時、只要來源叢集和目的地叢集執行 ONTAP 9.14.1 或更新版本、且該物件鎖定已在來源貯體上啟用、就可以在目的地貯體上啟用物件鎖定。來源貯體的物件鎖定模式和鎖定保留期限、將適用於目的地貯體上的複寫物件。您也可以在「目標設定 * 」區段中、為目的地貯體定義不同的鎖定保留期間。此保留期間也適用於從來源貯體和 S3 介面複寫的任何非鎖定物件。

如需如何在貯體上啟用物件鎖定的相關資訊、請參閱 "建立儲存庫"。

CLI

1. 如果這是此 SVM 的第一個 SnapMirror S3 關係、請確認來源和目的地 SVM 的根使用者金鑰都存在、如果根使用者金鑰不存在、請重新產生這些金鑰：
   `vserver object-store-server user show`

   確認root使用者有存取金鑰。如果沒有、請輸入：
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   如果金鑰已經存在、請勿重新產生金鑰。

2. 在目的地SVM上建立一個儲存區、做為鏡射目標：

   `vserver object-store-server bucket create -vserver svm_name -bucket dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. 驗證來源和目的地SVM中預設資源庫原則的存取規則是否正確：

   `vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

範例

```
clusterA::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

4. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：

   `snapmirror policy create -vserver` *`svm_name`* `-policy` *`policy_name -type continuous [-rpo _integer`*`] [-throttle` *`throttle_type`*`] [-comment text] [`*`additional_options`*`]`

   參數：

   - `continuous`– SnapMirror S3 關係的唯一原則類型（必要）。
   - `-rpo` –指定恢復點目標的時間（以秒爲單位）（可選）。
   - `-throttle` –指定處理量 / 頻寬的上限（以千位元組 / 秒為單位）（選用）。

     範例

     ```
     clusterA::> snapmirror policy create -vserver vs0 -type
     continuous -rpo 0 -policy test-policy
     ```

5. 在管理SVM上安裝CA伺服器憑證：

   a. 在管理 SVM 上安裝簽署 *SOURC* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`src_server_certificate`*

   b. 在管理 SVM 上安裝簽署 *destination* S3 伺服器憑證的 CA 憑證：
   `security certificate install -type server-ca -vserver` *`admin_svm`* `-cert -name` *`dest_server_certificate`*

   如果您使用的是由外部 CA 廠商簽署的憑證、則只需在管理 SVM 上安裝此憑證。

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

6. 創建 SnapMirror S3 關係：
   `snapmirror create -source-path` *`src_svm_name`*`:/bucket/`*`bucket_name -destination-path` *`dest_peer_svm_name`*`:/bucket/`*`bucket_name`*`, …} [-policy policy_name]`

   您可以使用所建立的原則、或接受預設值。

範例

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. 驗證鏡射是否為作用中：
   `snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

從本機叢集上的目的地 **ONTAP S3** 儲存區接管

如果來源儲存區中的資料無法使用、您可以中斷SnapMirror關係、使目的地儲存區可寫入、並開始提供資料。

關於這項工作

執行接管作業時、來源貯體會轉換為唯讀、而原始目的地貯體會轉換為讀寫、因此會反轉 SnapMirror S3 關係。

當停用的來源貯體再次可用時、 SnapMirror S3 會自動重新同步兩個貯體的內容。您不需要像標準Volume SnapMirror部署一樣、明確地重新同步關係。

如果目的地工作區位於遠端叢集上、則必須從遠端叢集啟動接管作業。

系統管理員

從無法使用的儲存區進行容錯移轉、並開始提供資料：

1. 按一下 * 保護 > 關係 * 、然後選取 * SnapMirror S2* 。
2. 單擊 ⋮，選擇 *Failover （故障轉移） * ，然後單擊 *Failover （故障轉移） * 。

CLI

1. 針對目的地儲存區啟動容錯移轉作業：
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. 確認容錯移轉作業的狀態：
   `snapmirror show -fields status`

範例

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

相關資訊

- "SnapMirror 故障轉移啟動"
- "SnapMirror 顯示"

從本機叢集上的目的地 **SVM** 還原 **ONTAP S3** 儲存區

當來源貯體中的資料遺失或毀損時、您可以從目的地貯體還原物件來重新填入資料。

關於這項工作

您可以將目的地庫位還原至現有的庫位或新的庫位。還原作業的目標貯體必須大於目的地貯體的邏輯使用空間。

如果您使用現有的儲存區、則在開始還原作業時必須是空的。 還原不會「回溯」儲存區的時間、而是將先前的內容填入一個空的儲存區。

還原作業必須從本機叢集啟動。

系統管理員

還原備份資料：

1. 按一下*保護>關係*、然後選取儲存庫。
2. 按一下 ⋮ 、然後選取 * 還原 * 。
3. 在*來源*下、選取*現有的Bucket*（預設值）或*新的Bucket*。
   - 若要還原至*現有的Bucket *（預設值）、請完成下列動作：
     - 選取叢集和儲存VM以搜尋現有的儲存區。
     - 選取現有的庫位。
4. 複製並貼上目的地S3伺服器CA憑證的內容。
   - 若要還原成*新的Bucket *、請輸入下列值：
     - 用於託管新儲存區的叢集與儲存VM。
     - 新儲存庫的名稱、容量和效能服務層級。
       請參閱 "儲存服務層級" 以取得更多資訊。
     - 目的地S3伺服器CA憑證的內容。
5. 在「目的地」下、複製並貼上來源S3伺服器CA憑證的內容。
6. 按一下「保護>關係」以監控還原進度。

還原鎖定的貯體

從 ONTAP 9.14.1 開始、您可以備份鎖定的貯體、並視需要進行還原。

您可以將物件鎖定的貯體還原至新的或現有的貯體。您可以在下列案例中選取物件鎖定的貯體作為目的地：

- * 還原至新的貯體 * ：啟用物件鎖定時、可建立同時啟用物件鎖定的貯體來還原貯體。當您還原鎖定的貯體時、會複寫原始貯體的物件鎖定模式和保留期間。您也可以為新的貯體定義不同的鎖定保留期間。此保留期間適用於來自其他來源的未鎖定物件。
- * 還原至現有的貯體 * ：只要現有貯體已啟用版本設定和類似的物件鎖定模式、即可將物件鎖定貯體還原至現有的貯體。保留原始貯體的保有期。
- * 還原未鎖定的貯體 * ：即使在某個貯體上未啟用物件鎖定、您仍可將其還原至已啟用物件鎖定且位於來源叢集上的貯體。當您還原貯體時、所有未鎖定的物件都會被鎖定、而且目的地貯體的保留模式和保有權也會適用於它們。

CLI

1. 如果您要將物件還原至新的貯體、請建立新的貯體。如需更多資訊、請參閱 "為新的 ONTAP S3 儲存區建立雲端備份關係"。
2. 為目的地貯體啟動還原作業：
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

範例

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

如"指令參考資料ONTAP"需詳細 `snapmirror restore`資訊，請參閱。

利用雲端目標提供備份保護

ONTAP SnapMirror S3 雲端目標關係的需求

確保您的來源和目標環境符合 SnapMirror S3 備份保護雲端目標的要求。

您必須向物件存放區供應商取得有效的帳戶認證、才能存取資料儲存區。

叢集間的生命與 IPspace 應先在叢集上設定、然後叢集才能連線至雲端物件存放區。您應該在每個節點上建立叢集間的生命體、以無縫地將資料從本機儲存設備傳輸到雲端物件儲存區。

如需StorageGRID 瞭解下列資訊、請參閱下列資訊：

- 伺服器名稱、以完整網域名稱（FQDN）或IP位址表示
- 庫位名稱；庫位必須已經存在
- 存取金鑰
- 秘密金鑰

此外，需要使用 `security certificate install`命令。如需詳細資訊、請參閱"安裝CA憑證"您是否使用 StorageGRID 。

對於AWS S3目標、您需要知道下列資訊：

- 伺服器名稱、以完整網域名稱（FQDN）或IP位址表示
- 庫位名稱；庫位必須已經存在
- 存取金鑰
- 秘密金鑰

ONTAP 叢集管理儲存 VM 的 DNS 伺服器必須能夠將 FQDN （如果使用）解析為 IP 位址。

相關資訊

- "安全性憑證安裝"

為新的 **ONTAP S3** 儲存區建立雲端備份關係

建立新的 S3 儲存桶時，您可以立即將它們備份到物件儲存提供者上的 SnapMirror S3 目標儲存桶，該提供者可以是 StorageGRID 系統或 Amazon S3 部署。

開始之前

- 您擁有物件存放區提供者的有效帳戶認證和組態資訊。
- 已在來源系統上設定叢集間網路介面和IPspace。
- •來源儲存 VM 的 DNS 組態必須能夠解析目標的 FQDN 。

系統管理員

1. 編輯儲存VM以新增使用者、並將使用者新增至群組：
   a. 按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 * S2* 下的。

      請參閱 "新增S3使用者和群組" 以取得更多資訊。

2. 在來源系統上新增雲端物件存放區：
   a. 按一下「保護>總覽」、然後選取「雲端物件存放區」。
   b. 按一下「新增」、然後選取「* Amazon S3 」或「 StorageGRID 」。
   c. 輸入下列值：
      - 雲端物件存放區名稱
      - URL樣式（路徑或虛擬託管）
      - 儲存虛擬機器（已啟用S3）
      - 物件存放區伺服器名稱（FQDN）
      - 物件存放區憑證
      - 存取金鑰
      - 秘密金鑰
      - Container（Bucket）名稱
3. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
   a. 按一下 * 保護 > 總覽 * 、然後按一下 * 本機原則設定 * 。
   b. 按一下 * 保護原則 * 旁的、然後按一下 * 新增 * 。
      - 輸入原則名稱和說明。
      - 選取原則範圍、叢集或SVM
      - 針對 SnapMirror S3 關係選取 * 持續 * 。
      - 輸入您的* Throttle 和 Recovery Point Objective *值。
4. 利用SnapMirror保護建立儲存庫：
   a. 按一下「儲存設備>桶」、然後按一下「新增」。
   b. 輸入名稱、選取儲存VM、輸入大小、然後按一下*更多選項*。
   c. 在*權限*下、按一下*新增*。驗證權限是選用的、但建議使用。
      - * Princius* 和 * 效果 * ：選擇對應於您的使用者群組設定的值或接受預設值。
      - * 操作 * ：確保顯示以下值：

        ```
        GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts
        ```

      - * 資源 * ：使用您需要的預設值 `_(bucketname, bucketname/*)`或其他值。

請參閱 "管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。

d. 在* Protection（保護）下、勾選* Enable SnapMirror（ONTAP 支援SnapMirror（不支援或雲端）、選取 Cloud Storage*、然後選取* Cloud Object Store*。

當您按一下*「Save（儲存）」*時、會在來源儲存VM中建立一個新儲存區、並將其備份至雲端物件存放區。

CLI

1. 如果這是此 SVM 的第一個 SnapMirror S3 關係、請確認來源和目的地 SVM 的根使用者金鑰都存在、如果沒有、請重新產生這些金鑰：
`vserver object-store-server user show` + 確認根使用者有存取金鑰。如果沒有、請輸入：
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` + 如果金鑰已經存在、請勿重新產生金鑰。

2. 在來源 SVM 中建立貯體：
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. 將存取規則新增至預設儲存區原則：
`vserver object-store-server bucket policy add-statement -vserver svm_name -bucket bucket_name -effect {allow|deny} -action object_store_actions -principal user_and_group_names -resource object_store_resources [-sid text] [-index integer]`

   範例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   參數：* `type continuous` – SnapMirror S3 關係唯一的原則類型（必要）。* `-rpo` –指定恢復點目標的時間（以秒為單位）（選用）。* `-throttle` –指定處理量 / 頻寬的上限、單位為千位元組 / 秒（選用）。

   範例

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

5. 如果目標是 StorageGRID 系統、請在來源叢集的管理 SVM 上安裝 StorageGRID CA 伺服器憑證：
`security certificate install -type server-ca -vserver src_admin_svm -cert`

`-name storage_grid_server_certificate`

如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

6. 定義 SnapMirror S3 目的地物件存放區：
`snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

參數：* `-object-store-name` –本機 ONTAP 系統上物件儲存區目標的名稱。* `-usage` –用於 `data`此工作流程。* `-provider-type` – `AWS_S3` `SGWS`支援（ `StorageGRID` ）目標。* `-server` –目標伺服器的 FQDN 或 IP 位址。* `-is-ssl-enabled` –啟用 SSL 是選擇性的，但建議使用。+ 深入瞭解 `snapmirror object-store config create` "指令參考資料ONTAP"。

範例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

7. 創建 SnapMirror S3 關係：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

參數：
* `-destination-path` - 您在上一個步驟中建立的物件存放區名稱和固定值 `objstore`。

您可以使用所建立的原則、或接受預設值。

範例

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path sgws-store:/objstore -policy test-policy
```

8. 驗證鏡射是否為作用中：
`snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

為現有的 **ONTAP S3** 儲存區建立雲端備份關係

您可以隨時開始備份現有的S3儲存區、例如、如果您將S3組態從ONTAP 版本更新至版本早於VMware版9.10.1的版本。

開始之前

- 您擁有物件存放區提供者的有效帳戶認證和組態資訊。
- 已在來源系統上設定叢集間網路介面和IPspace。
- 來源儲存VM的DNS組態必須能夠解析目標的FQDN。

系統管理員

1. 確認使用者和群組已正確定義：按一下 * 儲存 > 儲存 VM* 、按一下儲存 VM 、按一下 * 設定 * 、然後按一下 S3 下的。

   請參閱 "新增S3使用者和群組" 以取得更多資訊。

2. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
   a. 按一下「保護>總覽」、然後按一下「本機原則設定」。
   b. 按一下 * 保護原則 * 旁的、然後按一下 * 新增 * 。
   c. 輸入原則名稱和說明。
   d. 選取原則範圍、叢集或SVM
   e. 針對 SnapMirror S3 關係選取 * 持續 * 。
   f. 輸入您的* Thrott*和*恢復點目標值*。
3. 在來源系統上新增雲端物件存放區：
   a. 按一下「保護>總覽」、然後選取「雲端物件存放區」。
   b. 按一下「新增」、然後選取「* Amazon S3 」或「*其他」以供StorageGRID 參考Webscale使用。
   c. 輸入下列值：
      - 雲端物件存放區名稱
      - URL樣式（路徑或虛擬託管）
      - 儲存虛擬機器（已啟用S3）
      - 物件存放區伺服器名稱（FQDN）
      - 物件存放區憑證
      - 存取金鑰
      - 秘密金鑰
      - Container（Bucket）名稱
4. 確認現有庫位的庫位存取原則仍符合您的需求：
   a. 按一下「儲存設備」>「庫位」、然後選取您要保護的庫位。
   b. 在 * 權限 * 索引標籤中、按一下 * 編輯 * 、然後按一下 * 權限 * 下的 * 新增 * 。
      - 主體*和*效果：選取對應於使用者群組設定的值、或接受預設值。
      - **Actions** - 確保顯示以下值：
        `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - * 資源 * - 使用預設值 *(bucketname, bucketname/*)* 或其他您需要的價值。

        請參閱 "管理使用者對儲存區的存取權" 以取得這些欄位的詳細資訊。
5. 使用 SnapMirror S3 備份貯體：
   a. 按一下「儲存設備」>「庫位」、然後選取您要備份的庫位。

b. 按一下「* Protect 」、在「 Target 」下選取「 Cloud Storage*」、然後選取「* Cloud Object Store"（雲端物件存放區）。

當您按一下*「Save（儲存）」*時、現有的儲存區會備份到雲端物件存放區。

CLI

1. 確認預設儲存區原則中的存取規則正確無誤：
   `vserver object-store-server bucket policy add-statement -vserver` *`svm_name`* `-bucket` *`bucket_name`* `-effect {allow|deny} -action` *`object_store_actions`* `-principal` *`user_and_group_names`* `-resource` *`object_store_resources`* `[-sid` *`text`*`] [-index` *`integer`*`]`

   範例

   ```
   clusterA::> vserver object-store-server bucket policy add-statement
   -bucket test-bucket -effect allow -action
   GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. 如果您沒有現有的 SnapMirror S3 策略且不想使用預設策略，請建立一個 SnapMirror S3 策略：
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   參數：* `type continuous` – SnapMirror S3 關係唯一的原則類型（必要）。* `-rpo` –指定恢復點目標的時間（以秒為單位）（選用）。* `-throttle` –指定處理量 / 頻寬的上限、單位為千位元組 / 秒（選用）。

   範例

   ```
   clusterA::> snapmirror policy create -vserver vs0 -type continuous
   -rpo 0 -policy test-policy
   ```

3. 如果目標是 StorageGRID 系統、請在來源叢集的管理 SVM 上安裝 StorageGRID CA 憑證：
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

4. 定義 SnapMirror S3 目的地物件存放區：
   `snapmirror object-store config create -vserver` *`svm_name`* `-object-store-name` *`target_store_name`* `-usage data -provider-type {AWS_S3|SGWS} -server` *`target_FQDN`* `-container-name` *`remote_bucket_name`* `-is-ssl-enabled true -port` *`port_number`* `-access-key target_access_key -secret-password` *`target_secret_key`*

   參數：* `-object-store-name` –本機 ONTAP 系統上物件儲存區目標的名稱。* `-usage` –用於 `data`此工作流程。* `-provider-type` – `AWS_S3 SGWS`支援（ `StorageGRID` ）目標。* `-`

`server` –目標伺服器的 FQDN 或 IP 位址。* `-is-ssl-enabled` –啟用 SSL 是選擇性的，但建議使用。+ 深入瞭解 `snapmirror object-store config create` "指令參考資料ONTAP"。

範例

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS
-server sgws.example.com -container-name target-test-bucket -is-ssl
-enabled true -port 443 -access-key abc123 -secret-password xyz890
```

5. 創建 SnapMirror S3 關係：
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

參數：
* `-destination-path` - 您在上一個步驟中建立的物件存放區名稱和固定值 `objstore`。

您可以使用所建立的原則、或接受預設值。

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. 驗證鏡射是否為作用中：
`snapmirror show -policy-type continuous -fields status`

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"
- "SnapMirror 顯示"

從雲端目標還原 **ONTAP S3** 儲存區

當來源貯體中的資料遺失或毀損時、您可以從目的地貯體還原資料、重新填入資料。

關於這項工作

您可以將目的地庫位還原至現有的庫位或新的庫位。還原作業的目標儲存區必須大於目的地儲存區的邏輯已用空間。

如果您使用現有的儲存區、則在開始還原作業時必須是空的。 還原不會「回溯」儲存區的時間、而是將先前的內容填入一個空的儲存區。

系統管理員

還原備份資料：

1. 按一下 * 保護 > 關係 * 、然後選取 * SnapMirror S2* 。
2. 按一下 ⋮ 、然後選取 * 還原 * 。
3. 在*來源*下、選取*現有的Bucket*（預設值）或*新的Bucket*。
   - 若要還原至*現有的Bucket *（預設值）、請完成下列動作：
     - 選取叢集和儲存VM以搜尋現有的儲存區。
     - 選取現有的庫位。
     - 複製並貼上_destination_ S3伺服器CA憑證的內容。
   - 若要還原成*新的Bucket *、請輸入下列值：
     - 用於託管新儲存區的叢集與儲存VM。
     - 新的儲存庫名稱、容量和效能服務層級。
       請參閱 "儲存服務層級" 以取得更多資訊。
     - 目的地S3伺服器CA憑證的內容。
4. 在「目的地」下、複製並貼上_SOURER_S3伺服器CA憑證的內容。
5. 按一下*保護>關係*以監控還原進度。

CLI程序

1. 建立新的目的地貯體以進行還原。如需詳細資訊、請參閱 "建立儲存庫（雲端目標）的備份關係"。
2. 為目的地貯體啟動還原作業：
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   範例

   下列範例將目的地桶還原至現有的桶。

   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror restore`資訊，請參閱。

修改 **ONTAP SnapMirror S3** 原則

當您想要調整 RPO 和節流值時，可以修改 S3 SnapMirror 原則。

系統管理員

1. 按一下 * 保護 > 關係 * ，然後選取您要修改之關係的保護原則。
2. 按一下 ⋮ 原則名稱旁的，然後按一下 * 編輯 * 。

CLI

修改 SnapMirror S3 策略：

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

參數：

- `-rpo`：指定恢復點目標的時間（以秒爲單位）。
- `-throttle`：指定處理量 / 頻寬的上限（以千位元組 / 秒為單位）。

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy
-rpo 60
```

相關資訊

- "SnapMirror 策略修改"

利用快照保護 S3 資料

瞭解 ONTAP S3 快照

從 ONTAP 9 開始。 16.1 開始，您可以使用 ONTAP 快照技術來產生 ONTAP S3 儲存區的唯讀時間點影像。

使用 S3 快照功能，您可以手動建立快照，或透過快照原則自動產生快照。S3 快照會以 S3 儲存區的形式呈現給 S3 用戶端。您可以透過 S3 用戶端，從快照瀏覽及還原內容。

在 ONTAP 9 。 16.1 中， S3 快照僅擷取 S3 儲存區中物件的目前版本。S3 快照不會擷取非目前版本的版本版本版本的版本儲存區。此外，如果在拍攝快照之後修改物件標籤，則時間點物件標籤不會擷取在快照中。

S3 快照仰賴叢集時間。您應該設定叢集中的 NTP 伺服器來同步時間。如需詳細資訊、請 "管理叢集時間"參閱。

配額與空間使用量

配額會追蹤 S3 儲存區中使用的物件數量和邏輯大小。建立 S3 快照後， S3 快照中擷取的物件會計入所使用的儲存區物件數和大小，直到從檔案系統刪除快照為止。

多部分物件

對於多部分物件，快照中只會擷取最終物件。多部分物件的部分上傳不會擷取在快照中。

在版本化和非版本化的貯體上建立快照

您可以在版本控制和非版本控制的貯體上建立快照。快照一次只包含擷取快照時的目前物件版本。

版本化的儲存區和快照

在啟用物件版本控制的貯體中，快照會保留擷取快照後最新物件版本的內容。不包括貯體中的非最新版本。

請考慮以下範例：在已啟用物件版本設定的儲存區中，物件 `obj1`有版本 `v1` ， `v2` ， `v3` ， `v4` ， `v5` 。您從 `obj1` v3 建立了快照 `snap1`（擷取點的最新版本）。瀏覽 `snap1`時， `obj1`將顯示爲在 v3 中創建內容的對象。將不會傳回舊版的內容。

非目前版本會保留在檔案系統中，直到刪除快照為止。

非版本化的儲存區和快照

在非版本化的貯體中， S3 快照會保留建立快照之前最新提交的內容。

請考慮以下範例：在無法使用物件版本管理的儲存區中，物件 `obj1`已在（ `T1` ， `T2` ， `T3` ， `T4` 和 `T5` ）上覆寫數次。您在 `T3` 和 `T4` 之間建立了 `S3` 快照 `snap1`。瀏覽 `snap1`時 `obj1`，會顯示在 T3 建立的內容。

物件過期與快照

ONTAP S3 物件過期和 S3 快照功能彼此獨立運作。ONTAP 物件過期功能會根據 S3 儲存區定義的生命週期管理規則，使物件版本過期。S3 快照是在建立快照時的某個時間點，貯體物件的靜態複本。

如果在貯體中啟用物件版本設定，當某個物件的特定版本因針對該貯體定義的到期規則而遭到刪除時，如果某個或多個 S3 快照中的版本已擷取為目前版本，則過期物件版本的內容會繼續保留在檔案系統中。只有刪除該快照時，該物件版本才會停止存在於檔案系統中。

同樣地，在停用版本設定的儲存區中，如果根據到期規則刪除物件，但物件仍在部分現有的 S3 快照中擷取，則該物件將保留在檔案系統中。刪除擷取的快照時，物件將從檔案系統中永久移除。

如需 S3 物件到期與生命週期管理的相關資訊"建立貯體生命週期管理規則"，請參閱。

S3 快照的限制

請注意 ONTAP 9 中的下列功能排除項目和案例：

- 您最多可以為 S3 儲存區產生 1023 個快照。
- 將叢集還原為 ONTAP 9 之前的 ONTAP 版本之前，必須先刪除叢集中所有儲存區中的所有 S3 快照和中繼資料。
- 如果您需要刪除包含快照物件的 S3 儲存區，請確定已刪除該儲存區中所有物件的所有對應快照。
- 以下組態不支援 S3 快照：
  - SnapMirror 關係中的庫存箱
  - 在已啟用物件鎖定的貯體上
  - 在NetApp控制台上
  - 在 System Manager 上

- 在 ONTAP MetroCluster 組態中

- 不建議在用作本機或遠端FabricPool容量層的儲存桶上使用 S3 快照。

建立 ONTAP S3 快照

您可以手動產生 S3 快照，或設定快照原則，自動為您建立 S3 快照。快照可做為物件的靜態複本，用於資料備份與還原。為了判斷快照保留的保有權，您可以建立快照原則，以利在指定的時間間隔自動建立快照。

S3 快照可協助您在啟用或不啟用物件版本設定的情況下，保護 S3 儲存區中的物件資料。

當 S3 儲存區中的物件版本設定未啟用時，快照在建立資料保護方面特別有用，因為快照會做為時間點記錄，您可以在舊版物件無法使用時用於還原作業。

關於這項工作

- 下列命名規則適用於快照（手動和自動快照）：
  - S3 快照名稱最多可包含 30 個字元
  - S3 快照名稱只能由小寫字母，數字，點（ . ）和連字號（ - ）組成
  - S3 快照名稱必須以字母或數字結尾
  - S3 快照名稱不能包含子字串 `s3snap`
- 在 S3 傳輸協定的內容中，貯體命名限制將貯體名稱限制為 63 個字元。由於 ONTAP S3 快照透過 S3 傳輸協定以儲存區形式呈現，因此快照儲存區名稱也會受到類似的限制。根據預設，原始貯體名稱會用作基礎貯體名稱。
- 為了更容易識別哪個快照屬於哪個儲存區，快照儲存區名稱包含基礎儲存區名稱，以及預先固定在快照名稱前面的特殊字串 `-s3snap-`。快照庫位名稱格式化為 `<base_bucket_name>-s3snap-<snapshot_name>`。

  例如，執行下列命令在上 `bucket-a`**建立** `snap1`**快照儲存區時，會建立名稱為的快照儲存區** `bucket-a-s3snap-snap1`，如果您有權存取基本儲存區，則可透過 S3 用戶端存取該儲存區。

```
vserver object-store-server bucket snapshot create -bucket bucket-a
-snapshot snap1
```

- 您無法建立快照，以產生超過 63 個字元的快照儲存區名稱。
- 自動快照名稱包含原則排程名稱和時間戳記，類似於傳統 Volume 快照的命名慣例。例如，排程的快照名稱可以是 `daily-2024-01-01-0015`**和** `hourly-2024-05-22-1105`。

手動建立 S3 快照

您可以使用 ONTAP CLI 手動建立 S3 快照。此程序僅會在本機叢集上建立快照。

步驟

1. 建立 S3 快照：

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

以下範例建立一個名為 `vs0`儲存 VM 和儲存 `website-data`區的快照 `pre-update`：

```
vserver object-store-server bucket snapshot create -vserver vs0 -bucket
website-data -snapshot pre-update
```

將 S3 快照原則指派給貯體

當您在 S3 儲存區層級設定快照原則時， ONTAP 會自動為您建立排程的 S3 快照。與傳統的快照原則一樣， S3 快照最多可設定五個排程。

Snapshot 原則通常會指定建立快照的排程，每個排程要保留的複本數，以及排程前置碼。例如，策略可以每天中午 12:10 創建一個 S3 快照，保留兩個最新的副本，並將其命名 `daily-<timestamp>`。

預設的快照原則可保留：

- 每小時六個快照
- 每日兩個快照
- 每週兩次快照

開始之前

- 將快照原則指派給 S3 儲存區之前，必須先建立快照原則。

> S3 快照原則遵循與其他 ONTAP 快照原則相同的規則。不過，任何快照排程中設定了保留期間的快照原則，無法指派給 S3 儲存區。

有關爲自動生成快照創建快照策略的詳細信息，請參閱"設定自訂快照原則總覽"。

步驟

1. 在您的貯體上指派快照原則：

```
vserver object-store-server bucket create -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

或

```
vserver object-store-server bucket modify -vserver <svm_name> -bucket
<bucket_name> -snapshot-policy <policy_name>
```

如果您需要將叢集還原為早於 ONTAP 9 。 16.1 的 ONTAP 版本，請確定所有貯體的值 `snapshot-policy`**都設定為** `none（或 -）。

相關資訊

"瞭解 ONTAP S3 快照"

檢視及還原 **ONTAP S3** 快照

從ONTAP 9.16.1 開始，您可以從 S3 用戶端查看和瀏覽儲存桶的 S3 快照資料。從ONTAP 9.18.1 開始，可以使用ONTAP CLI 直接存取 S3 快照儲存桶。此外，您還可以從 S3 快照在 S3 用戶端上還原單一物件、一組物件或整個儲存桶。

開始之前

- 叢集中的所有節點必須執行ONTAP 9.18.1 或更高版本，才能在ONTAP CLI 中以原生方式執行儲存桶快照復原作業。從ONTAP 9.18,1 開始，不再需要 S3 瀏覽器，但操作仍支援。
- 在給定的儲存桶上，一次只允許執行一次快照復原操作。

關於這項工作

從ONTAP 9.16.1 開始， ONTAP S3 快照功能為ONTAP S3 儲存桶提供基本的快照功能，包括手動和規劃快照的建立和刪除、S3 儲存桶的快照策略以及基於 S3 用戶端的快照瀏覽。

從ONTAP 9.18.1 開始， ONTAP增加了對原生快照復原的支持，使ONTAP管理員無需使用 S3 瀏覽器即可實現時間點復原功能。快照中僅擷取目前儲存桶版本。版本歷史記錄不會被捕獲，也不會透過 S3 快照還原作業進行還原。

列出並檢視 **S3** 快照

您可以檢視 S3 快照詳細資料，進行比較，並識別錯誤。使用 ONTAP CLI ，您可以列出在 S3 儲存區上建立的所有快照。

步驟

1. 列出 S3 快照：

```
vserver object-store-server bucket snapshot show
```

   您可以查看叢集上所有儲存桶建立的 S3 快照的快照名稱、儲存虛擬機器、儲存桶、建立時間和實例 UUID。

2. 您也可以指定儲存桶名稱，以查看為該特定儲存桶建立的所有 S3 快照的名稱、建立時間和實例 UUID。

```
vserver object-store-server bucket snapshot show -vserver <svm_name>
-bucket <bucket_name>
```

瀏覽 S3 快照內容

如果您發現環境中有任何故障或問題，您可以瀏覽 S3 儲存區快照的內容以識別錯誤。您也可以瀏覽 S3 快照，判斷要還原的無錯誤內容。

S3 快照以快照儲存桶的形式呈現給 S3 用戶端。快照儲存桶名稱的格式為： `<base_bucket_name>-s3snap-<snapshot_name>` 。您可以使用以下方法查看儲存虛擬機器中的所有快照儲存桶： `ListBuckets` S3 API 操作。

S3 快照儲存桶繼承了基礎儲存桶的存取策略，並且僅支援唯讀操作。禁止執行刪除和寫入操作。如果您擁有存取基礎儲存桶的權限，您也可以對 S3 快照儲存桶執行唯讀的 S3 API 操作，例如： `HeadObject` ， `GetObject` ， `GetObjectTagging` ， `ListObjects` ， `ListObjectVersions` ， `GetObjectAcl` ，和 `CopyObject` 。

> 只有當 S3 快照儲存區是來源儲存區的快照時，此 `CopyObject`作業才會受到支援，而非當它是快照的儲存目的地時。

有關這些操作的詳細信息，請"支援的動作ONTAP"參閱。

使用ONTAP從 S3 快照還原儲存桶

從ONTAP 9.18.1 開始，您可以使用ONTAP CLI 透過ONTAP S3 快照還原整個儲存桶。您只能還原在建立所選快照時存在的儲存桶版本。

步驟

1. 決定要用於還原儲存桶的快照：

```
vserver object-store-server bucket snapshot show
```

2. 恢復儲存桶：

```
vserver object-store-server bucket snapshot restore start -vserver
<storage VM name> -bucket <bucket name> -snapshot <snapshot name>
```

使用 S3 用戶端從 S3 儲存桶快照恢復數據

除了在ONTAP中還原整個儲存桶之外，您還可以使用 S3 用戶端（如 S3cmd 或 S3 Browser）從 S3 快照還原單一物件、一組物件或整個儲存桶。

"了解更多關於版本化快照和非版本化快照的資訊。"

您可以使用以下方法還原整個儲存桶、具有特定前綴的物件或單一物件： `aws s3 cp`命令。

步驟

1. 拍攝基礎 S3 儲存區的快照。

```
vserver object-store-server bucket snapshot create -vserver <svm_name>
-bucket <base_bucket_name> -snapshot <snapshot_name>
```

2. 使用快照還原基本貯體：
   - 還原整個貯體。請使用格式的 Snapshot 儲存區名稱 `<base_bucket_name>-s3snap-<snapshot_name>`。

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>
     s3://<base-bucket>  --recursive
     ```

   - 使用前置碼還原目錄中的物件 `dir1`：

     ```
     aws --endpoint http://<IP> s3 cp s3://<snapshot-bucket-name>/dir1
     s3://<base_bucket_name>/dir1 --recursive
     ```

   - 還原一個名爲的對象 `web.py`：

     ```
     aws --endpoint http://<IP> s3 cp s3:// <snapshot-bucket-name>/web.py
     s3://<base_bucket_name>/web.py
     ```

刪除 **ONTAP S3** 快照

您可以刪除不再需要的 S3 快照，並釋放儲存空間。您可以手動移除 S3 快照，或修改 S3 儲存區附加的快照原則，以變更排程中要保留的快照數量。

S3 貯體的 Snapshot 原則遵循與傳統 ONTAP 快照原則相同的刪除規則。有關創建快照策略的詳細信息，請參閱"建立快照原則"。

關於這項工作

- 如果在多個快照中擷取物件版本（在版本化儲存庫中）或物件（在非版本化儲存庫中），則只有在刪除保護物件的最後一個快照之後，物件才會從檔案系統中移除。
- 如果您需要刪除包含快照物件的 S3 儲存區，請確定已刪除該儲存區中所有物件的所有快照。
- 如果您需要將叢集還原為早於 ONTAP 9 。 16.1 的 ONTAP 版本，請確定您已刪除所有儲存區的所有 S3 快照。您可能也需要執行 `vserver object-store-server bucket clear-snapshot-metadata`命令，以移除 S3 儲存區的快照中繼資料。如需相關資訊、請 "清除 S3 快照中繼資料"參閱。
- 當您分批刪除快照時，可以移除多個快照中擷取的大量物件，有效釋放的空間比個別快照刪除所造成的空間更多。因此，您可以為儲存物件回收更多空間。

步驟

1. 若要刪除特定 S3 快照，請執行下列命令：

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot <snapshot_name>
```

2. 若要移除貯體中的所有 S3 快照，請執行下列命令：

```
vserver object-store-server bucket snapshot delete -vserver <svm_name>
-bucket <bucket_name> -snapshot *
```

清除 **S3** 快照中繼資料

使用 S3 快照時，也會在貯體中產生快照中繼資料。即使從貯體移除所有快照，快照中繼資料仍會繼續存在。快照中繼資料的存在會封鎖下列作業：

- 叢集還原為 ONTAP 9 之前的 ONTAP 版本
- 在貯體上組態 SnapMirror S3

在執行這些作業之前，您應該清除貯體中的所有快照中繼資料。

開始之前

在開始清除中繼資料之前，請確定已從儲存區移除所有 S3 快照。

步驟

1. 若要清除貯體中的快照中繼資料，請執行下列命令：

```
vserver object-store-server bucket clear-snapshot-metadata -vserver
<svm_name> -bucket <bucket_name>
```

稽核**S3**事件

瞭解如何稽核 **ONTAP S3** 事件

從功能完善的S59.10.1開始ONTAP 、您可以在ONTAP 支援功能完善的支援環境中稽核資料與管理事件。S3稽核功能類似於現有的NAS稽核功能、S3和NAS稽核可共存於叢集內。

當您在SVM上建立及啟用S3稽核組態時、S3事件會記錄在記錄檔中。您可以指定要記錄的下列事件：

物件存取（資料）事件（依版本）

9.11.1 ：

- listBucketVerions
- ListBucket （ 9.10.1 的 ListObjects 已重新命名為此項目）

- ListAllMyb鏟 斗（已將 9.10.1 的清單鏟斗重新命名為此）

9.10.1 ：

- 標題物件
- GetObject
- PuttObject
- 刪除物件
- 列表桶
- 清單物件
- MPUpload
- MPUploadPart
- MPComplete
- MPAbort
- GetObjectTagging
- 刪除ObjectTagging
- PuttObjectTagging
- ListUploads
- 清單零件

依版本管理事件

9.15.1 ：

- GetBucketCORS
- PuttBucketCORS
- DeleteBucketCORS

9.14.1 ：

- GetObjectRetention
- PutObjectRetention
- PutBucketObjectLockConfiguration
- GetBucketObjectLockConfiguration

9.13.1 ：

- PutBucketLifecycle
- 刪除 BucketLifecycle
- GetBucketLifecycle

9.12.1 ：

- GetBucketPolicy
- CopyObject
- 上傳PartCopy
- PuttBucketPolicy
- 刪除BucketPolicy

9.11.1 ：

- GetBucketVersion
- PuttBucketVersion

9.10.1 ：

- 標題庫
- GetBucketAcl
- GetObjectAcl
- 推桿
- 刪除Bucket
- ModifyObjectTagging
- GetBucketLocation

記錄格式為JavaScript物件標記法（Json）。

S3和NFS稽核組態的總限制為每個叢集400個SVM。

需要下列授權：

- ONTAP One （原為核心產品組合的一部分）、適用於 ONTAP S3 傳輸協定和儲存設備

如需詳細資訊、請參閱 "如何執行不稽核程序ONTAP"。

保證稽核

根據預設、S3和NAS稽核是保證的。即使節點無法使用、也能保證記錄所有可稽核的儲存貯體存取事件。ONTAP在將該作業的稽核記錄儲存至持續儲存設備上的接移磁碟區之前、無法完成要求的儲存區作業。如果因為空間不足或其他問題而無法在暫存檔案中提交稽核記錄、則會拒絕用戶端作業。

稽核所需的空間

在不稽核系統中ONTAP 、稽核記錄一開始會儲存在個別節點的二進位暫存檔案中。這些記錄會定期整合並轉換成使用者可讀取的事件記錄、這些記錄會儲存在SVM的稽核事件記錄目錄中。

暫存檔案儲存在專屬的暫存磁碟區中、ONTAP 此磁碟區是由建立稽核組態時由支援所建立。每個Aggregate有一個接移磁碟區。

您必須在稽核組態中規劃足夠的可用空間：

- 適用於集合體中包含稽核桶的暫存磁碟區。

- 用於儲存已轉換事件記錄之目錄的磁碟區。

建立S3稽核組態時、您可以使用下列兩種方法之一來控制事件記錄的數量、以及磁碟區中的可用空間：

- 數值限制 `-rotate-limit` 參數控制必須保留的稽核檔案數量下限。
- 時間限制 `-retention-duration` 參數控制檔案可保留的最長期間。

在這兩個參數中、一旦超過設定、就能刪除較舊的稽核檔案、為較新的稽核檔案留出空間。這兩個參數的值都是0、表示必須維護所有檔案。因此、為了確保有足夠空間、最佳做法是將其中一個參數設定為非零值。

由於稽核保證、如果稽核資料的可用空間在旋轉限制之前用盡、就無法建立較新的稽核資料、導致用戶端無法存取資料。因此、您必須謹慎選擇此值及分配給稽核的空間、而且必須回應稽核系統中有關可用空間的警告。

如需詳細資訊、請參閱 "基本稽核概念"。

規劃 ONTAP S3 稽核組態

您必須為S3稽核組態指定多個參數、或接受預設值。特別是、您應該考慮哪些記錄旋轉參數有助於確保有足夠的可用空間。

如"指令參考資料ONTAP"需詳細 `vserver object-store-server audit create`資訊，請參閱。

一般參數

建立稽核組態時、必須指定兩個必要參數。您也可以指定三個選用參數。

資訊類型	選項	必要
*SVM*名稱 要在其中建立稽核組態的SVM名稱。 SVM必須已經存在、且已啟用S3。	`-vserver` *`svm_name`*	是的
記錄目的地路徑 指定轉換後的稽核記錄儲存位置。路徑必須已存在於SVM上。 路徑長度最多可達864個字元、且必須具有讀寫權限。 如果路徑無效、稽核組態命令就會失敗。	`-destination` *`text`*	是的

要稽核的事件類別_ 您可以稽核下列事件類別： • 資料 GetObject 、 PutObject 和 DeleteObject 事件 • 管理 PutBucket 和 DeleteBucket 活動 預設為僅稽核資料事件。	`-events {data|management}, …`	否

您可以輸入下列其中一個參數、以控制稽核記錄檔的數量。如果未輸入任何值、則會保留所有記錄檔。

資訊類型	選項	必要
記錄檔案旋轉限制 決定要保留多少稽核記錄檔、然後再將最舊的記錄檔轉出。例如、如果您輸入值5、則會保留最後五個記錄檔。 值0表示保留所有記錄檔。預設值為 0 。	`-rotate-limit` *`integer`*	否
記錄檔案持續時間限制 決定在刪除記錄檔之前可以保留多久。例如、如果您輸入5d0h0m的值、超過5天的記錄就會刪除。 值0表示保留所有記錄檔。預設值為 0 。	`-retention duration` *`integer_time`*	否

稽核記錄輪調的參數

您可以根據大小或排程來旋轉稽核記錄。預設值是根據大小來旋轉稽核記錄。

根據記錄大小來旋轉記錄

如果您要使用預設的記錄檔旋轉方法和預設的記錄檔大小、則不需要設定任何特定的記錄檔旋轉參數。預設記錄大小為100 MB。

如果您不想使用預設記錄大小、可以設定 `-rotate-size` 指定自訂記錄大小的參數。

如果您想要僅根據記錄大小重設旋轉、請使用下列命令取消設定 `-rotate-schedule-minute` 參數：

`vserver audit modify -vserver` *`svm_name`* `-destination / -rotate-schedule-minute -`

根據排程來旋轉記錄

如果您選擇根據排程來旋轉稽核記錄、您可以使用任何組合的時間型旋轉參數來排程記錄輪調。

- 如果您使用時間型旋轉、則會使用 `-rotate-schedule-minute` 參數為必填。

- 所有其他的時間型旋轉參數都是選用的。
  - `-rotate-schedule-month`
  - `-rotate-schedule-dayofweek`
  - `-rotate-schedule-day`
  - `-rotate-schedule-hour`
- 旋轉排程是使用所有與時間相關的值來計算。
  例如、如果您只指定 `-rotate-schedule-minute` 參數時、稽核記錄檔會根據一週中所有天所指定的分鐘數、在一年中所有月份的所有小時內進行旋轉。
- 如果只指定一或兩個時間型旋轉參數（例如、 `-rotate-schedule-month` 和 `-rotate-schedule-minutes`）、記錄檔會根據您在一週的所有天、所有時間、但僅在指定的月份內所指定的分鐘值來旋轉。

  例如、您可以指定稽核日誌在一月、三月和八月的所有週一、週三和週六上午10：30進行輪調
- 如果您同時指定兩者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`的問題。

  例如、如果您指定 `-rotate-schedule-dayofweek` 星期五和 `-rotate-schedule-day` 截至 13 日、稽核記錄將會在每週五和指定月份的第 13 天、而不只是在每週五的第 13 天輪調。
- 如果您想要僅根據排程重設旋轉、請使用下列命令取消設定 `-rotate-size parameter`：

  `vserver audit modify -vserver` *`svm_name`* `-destination / -rotate-size -`

根據記錄大小和排程來旋轉記錄

您可以選擇根據記錄大小和排程來旋轉記錄檔、方法是在任何組合中設定-rote-size參數和時間型旋轉參數。例如： IF `-rotate-size` 設為 10 MB 、且 `-rotate-schedule-minute` 設為 15 、當記錄檔大小達到 10 MB 或每小時 15 分鐘（以先發生的事件為準）時、記錄檔會旋轉。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立並啟用 **ONTAP S3** 稽核組態

若要實作S3稽核、您必須先在啟用S3的SVM上建立持續性物件存放區稽核組態、然後啟用該組態。

開始之前

- 您有啟用 S3 的 SVM 。
- 確認您有足夠的空間在本端層中暫存磁碟區。

關於這項工作

每個包含您要稽核之S3儲存區的SVM都需要稽核組態。您可以在新的或現有的S3伺服器上啟用S3稽核。稽核組態會保留在S3環境中、直到* vserver object-store-server稽核DELETE *命令移除為止。

S3稽核組態會套用至您選取進行稽核的SVM中的所有儲存區。啟用稽核的SVM可包含稽核和未稽核的儲存區。

建議您設定S3稽核以自動進行記錄輪調、視記錄大小或排程而定。如果您未設定自動記錄旋轉，則預設會保留所有記錄檔。您也可以使用* vserver object-store-server稽核rote-log*命令手動旋轉S3記錄檔。

如果SVM是SVM災難恢復來源、則目的地路徑無法位於根磁碟區上。

步驟

1. 建立稽核組態、根據記錄大小或排程來旋轉稽核記錄。

如果您想要以下列方式來旋轉稽核記錄...	輸入...
記錄檔大小	`vserver object-store-server audit create -vserver` *svm_name* `-destination` *path* `[[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integer_d*`][`*integer_h*`][`*integer_m*`][`*integers*`]]} [-rotate-size {`*integer*`[KB|MB|GB|TB|PB]}]`
排程	`vserver object-store-server audit create -vserver` *svm_name* `-destination path [[-events] {data|management}, …] {[-rotate-limit` *integer*`] | [-retention-duration [`*integerd*`][`*integerh*`] [`*integerm*`][`*integers*`]] } [-rotate-schedule-month` *chron_month*`] [-rotate-schedule-dayofweek` *chron_dayofweek*`] [-rotate-schedule-day` *chron_dayofmonth*`] [-rotate-schedule-hour` *chron_hour*`] -rotate-schedule-minute` *chron_minute* 。 `-rotate-schedule-minute` 如果您正在設定時間型稽核記錄輪調、則需要參數。

2. 啟用S3稽核：

   `vserver object-store-server audit enable -vserver` *svm_name*

範例

下列範例會建立稽核組態、使用大小型旋轉功能來稽核所有S3事件（預設值）。記錄儲存在/Audit記錄目錄中。記錄檔大小上限為200 MB。當記錄大小達到200 MB時、就會進行旋轉。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -rotate
-size 200MB
```

下列範例會建立稽核組態、使用大小型旋轉功能來稽核所有S3事件（預設值）。記錄檔大小上限為100 MB（預設值）、而且記錄會保留5天、之後才會刪除。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -retention
-duration 5d0h0m
```

下列範例會建立稽核組態、以稽核S3管理事件、以及使用時間型輪調的集中存取原則暫存事件。稽核記錄會每月於下午12：30循環一次一週中的所有天。記錄旋轉限制為5。

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log -events
management -rotate-schedule-month all -rotate-schedule-dayofweek all -rotate
-schedule-hour 12 -rotate-schedule-minute 30 -rotate-limit 5
```

選擇 ONTAP S3 稽核的儲存區

您必須在啟用稽核的SVM中指定要稽核的儲存區。

開始之前

- 您已啟用 SVM 進行 S3 稽核。

關於這項工作

S3 稽核組態是以每個 SVM 為基礎啟用、但您必須在 SVMS 中選取已啟用稽核的儲存區。如果您將儲存區新增至SVM、而且想要稽核新的儲存區、則必須使用此程序來選取這些儲存區。您也可以在SVM中啟用未稽核的儲存區以進行S3稽核。

在命令移除之前，貯體的稽核組態會持續保留 `vserver object-store-server audit event-selector delete`。

步驟

1. 選取S3稽核的儲存庫：

```
vserver object-store-server audit event-selector create -vserver
<svm_name> -bucket <bucket_name> [[-access] {read-only|write-only|all}]
[[-permission] {allow-only|deny-only|all}]
```

   - `-access`：指定要稽核的事件存取類型： `read-only`，`write-only`或 `all`（預設為 `all`）。
   - `-permission`：指定要稽核的事件權限類型： `allow-only`，`deny-only`或 `all`（預設為 `all`）。

範例

下列範例會建立只記錄允許唯讀存取的事件的庫區稽核組態：

```
cluster1::> vserver object-store-server audit event-selector create -vserver vs1
-bucket test-bucket -access read-only -permission allow-only
```

修改 ONTAP S3 稽核組態

您可以修改個別儲存區的稽核參數、或是在SVM中選取要稽核的所有儲存區的稽核組態。

如果您想要修改稽核組態...	輸入...
個別庫存箱	`vserver object-store-server audit event-selector modify -vserver` *`svm_name`* `[-bucket` *`bucket_name`*`] [`*`parameters to modify`*`]`
SVM中的所有儲存區	`vserver object-store-server audit modify -vserver` *`svm_name`* `[`*`parameters to modify`*`]`

範例

下列範例會修改個別的儲存區稽核組態、以僅稽核純寫入的存取事件：

```
cluster1::> vserver object-store-server audit event-selector modify
-vserver vs1 -bucket test-bucket -access write-only
```

以下範例修改 SVM 中所有貯體的稽核組態、將記錄大小限制變更為 10MB 、並在旋轉前保留 3 個記錄檔。

```
cluster1::> vserver object-store-server audit modify -vserver vs1 -rotate
-size 10MB -rotate-limit 3
```

顯示 ONTAP S3 稽核組態

完成稽核組態之後、您可以確認稽核設定正確且已啟用。您也可以顯示叢集中所有物件存放區稽核組態的相關資訊。

關於這項工作

您可以顯示關於儲存區和SVM稽核組態的資訊。

- 貯體：使用 `vserver object-store-server audit event-selector show`命令

  如果沒有任何參數、命令會在叢集中的所有SVM中、以物件存放區稽核組態顯示下列關於貯體的資訊：

  - SVM名稱
  - 儲存區名稱
  - 存取和權限值
- SVM ：使用 `vserver object-store-server audit show`命令

  如果沒有任何參數、命令會顯示叢集中所有具有物件存放區稽核組態之SVM的下列資訊：

  - SVM名稱
  - 稽核狀態
  - 目標目錄

您可以指定 `-fields` 用於指定要顯示哪些稽核組態資訊的參數。

步驟

顯示S3稽核組態的相關資訊：

如果您要修改下列項目的組態...	輸入...
桶	`vserver object-store-server audit event-selector show [-vserver` *`svm_name`*`] [`*`parameters`*`]`
SVM	`vserver object-store-server audit show [-vserver` *`svm_name`*`] [`*`parameters`*`]`

範例

下列範例顯示單一儲存區的資訊：

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1 -bucket test-bucket
     Vserver     Bucket     Access          Permission
     ----------- ---------- --------------- ----------
     vs1         bucket1    read-only       allow-only
```

下列範例顯示SVM上所有儲存區的資訊：

```
cluster1::> vserver object-store-server audit event-selector show -vserver
vs1

     Vserver           :vs1
     Bucket            :test-bucket
     Access            :all
     Permission        :all
```

下列範例顯示所有SVM的名稱、稽核狀態、事件類型、記錄格式及目標目錄。

```
cluster1::> vserver object-store-server audit show

Vserver     State  Event Types Log Format Target Directory
----------- ------ ----------- ---------- --------------------
vs1         false  data        json       /audit_log
```

下列範例顯示所有SVM稽核記錄的SVM名稱和詳細資料。

```
cluster1::> vserver object-store-server audit show -log-save-details

                Rotation                            Rotation
      Vserver   File Size Rotation Schedule         Limit
      ----------- --------- ------------------------ --------
      vs1         100MB     -                        0
```

下列範例會以清單形式顯示所有SVM的所有稽核組態資訊。

```
cluster1::> vserver object-store-server audit show -instance

                              Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: data
                          Log Format: json
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 0
                  Log Retention Time: 0s
```

驗證與存取控制

驗證與存取控制總覽

您可以管理 ONTAP 叢集驗證、以及對 ONTAP Web 服務的存取控制。

使用 System Manager 或 CLI 、您可以控制並保護用戶端和管理員對叢集和儲存設備的存取。

如果您使用的是傳統系統管理員（僅適用於 ONTAP 9.7 及更早版本）、請參閱 "System Manager Classic（ONTAP 版本9.0至9.7）"

用戶端驗證與授權

利用信任的來源驗證用戶端機器和使用者的身分、藉此驗證其身分。ONTAP利用比較使用者的認證資料與檔案或目錄上設定的權限、即可授權使用者存取檔案或目錄。ONTAP

系統管理員驗證與**RBAC**

系統管理員使用本機或遠端登入帳戶、驗證自己是否已進入叢集和儲存VM。角色型存取控制（RBAC）決定系統管理員可以存取的命令。

管理系統管理員驗證和 **RBAC**

瞭解 **ONTAP** 中的系統管理員驗證和 **RBAC**

您可以為ONTAP 叢集管理員和儲存虛擬機器（SVM）管理員啟用登入帳戶。您也可以使用角色型存取控制（RBAC）來定義系統管理員的功能。

您可以使用下列驗證類型、讓本機系統管理員帳戶存取管理儲存虛擬機器（SVM）或資料SVM：

- "密碼"
- "SSH公開金鑰"
- "SSL 憑證"
- "SSH多因素驗證（MFA）"

  從支援使用密碼和公開金鑰的驗證功能、從ONTAP 功能表9.3開始。

您可以使用下列驗證類型、讓遠端系統管理員帳戶存取管理SVM或資料SVM：

- "Active Directory"

  從 ONTAP 9.13.1 開始，您可以使用 SSH 公開金鑰做為 Active Directory 使用者的主要或次要驗證方法。

- "SAML驗證（僅適用於管理SVM）"

  從ONTAP Sf9.3開始、安全聲明標記語言（SAML）驗證可用於使用下列任一Web服務存取管理SVM：服務

處理器基礎架構、ONTAP Sf0 API或系統管理員。

- "LDAP 或 NIS"

  從ONTAP 版本9.4開始、SSH MFA可用於LDAP或NIS伺服器上的遠端使用者。支援使用nsswitch和公開金鑰進行驗證。

ONTAP 系統管理員驗證和 RBAC 工作流程

您可以啟用本機系統管理員帳戶或遠端系統管理員帳戶的驗證。本機帳戶的帳戶資訊位於儲存系統上、遠端帳戶的帳戶資訊則位於其他位置。每個帳戶都可以擁有預先定義的角色或自訂角色。

1 完成組態工作表

在建立登入帳戶及設定角色型存取控制 (RBAC) 之前，您應該先收集中每個項目的資訊"組態工作表"。

2 判斷系統管理員帳戶是本機帳戶還是遠端帳戶

- * 如果為本機： * 啟用"密碼"，，"SSH" "SSH MFA"或"SSL"存取。
- * 如果是遠端： * 判斷遠端存取的類型。取決於存取類型，"啟用 Active Directory 存取"，"啟用 LDAP 或 NIS 存取"或"設定 SAML 驗證（僅適用於管理 SVM ）"。

3 設定角色型存取

指派給系統管理員的角色會決定系統管理員可以存取的命令。角色會在您建立系統管理員帳戶時指派，稍後也可以指派"已修改"。您可以為和"SVM"管理員或"定義自訂角色"視需要使用預先定義的角色"叢集"。

4 管理系統管理員帳戶

根據您啟用帳戶存取權限的方式，您可能需要關聯"具有本機帳戶的公開金鑰" ， 管理"公開金鑰和 X.509 憑證"，配置"適用於 SSH 登入的 Cisco 雙核心 2FA" ，安裝一個"CA簽署的伺服器數位憑證"或配置"Active Directory" ， "LDAP 或 NIS"訪問。您可以在啟用帳戶存取權限之前或之後執行任何這些任務。

5 設定其他安全功能

- "管理多管理員驗證"如果您想確保某些作業需要指定的系統管理員核准。
- "管理動態授權"如果您想根據使用者的信任層級動態套用其他授權檢查，
- "設定即時 (JIT) 權限提升"如果您想要允許使用者暫時存取提升的權限來執行某些任務。

ONTAP 系統管理員驗證和 RBAC 設定工作表

在建立登入帳戶及設定角色型存取控制（RBAC）之前、您應該先收集組態工作表中每個項目的資訊。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

建立或修改登入帳戶

當您啟用登入帳戶以存取儲存 VM 時，您可以使用命令提供這些值 `security login create`。如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

修改帳戶存取儲存 VM 的方式時，您可以使用命令提供相同的值 `security login modify`。如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	帳戶存取的儲存 VM 名稱。預設值為叢集的管理儲存 VM 名稱。	
`-user-or-group-name`	帳戶的使用者名稱或群組名稱。指定群組名稱可讓您存取群組中的每個使用者。您可以將使用者名稱或群組名稱與多個應用程式建立關聯。	
`-application`	用於存取儲存 VM 的應用程式： • `http` • `ontapi` • `snmp` • `ssh`	
`-authmethod`	用於驗證帳戶的方法： • `cert` 用於 SSL 憑證驗證 • `domain` 用於 Active Directory 驗證 • `nsswitch` 用於 LDAP 或 NIS 驗證 • `password` 用於使用者密碼驗證 • `publickey` 用於公開金鑰驗證 • `community` 適用於 SNMP 社群字串 • `usm` 適用於 SNMP 使用者安全模式 • `saml` 用於安全聲明標記語言（SAML）驗證	

`-remote-switch-ipaddress`	遠端交換器的IP位址。遠端交換器可以是由叢集交換器健全狀況監控器（CSHM）監控的叢集交換器、或MetroCluster 是由不健全狀況監控器（MCC-HM）監控的光纖通道（FC）交換器。此選項僅適用於應用程式 `snmp` 驗證方法是 `usm`。	
`-role`	指派給帳戶的存取控制角色： • 對於叢集（管理儲存 VM ）、預設值為 `admin`。 • 對於資料儲存 VM 、預設值為 `vsadmin`。	
`-comment`	（選用）帳戶的說明文字。您應該以雙引號（"）括住文字。	
`-is-ns-switch-group`	帳戶是 LDAP 群組帳戶還是 NIS 群組帳戶 (`yes` 或 `no`）。	
`-second-authentication-method`	多因素驗證的第二種驗證方法： • `none` 如果不使用多因素驗證、則為預設值 • `publickey` 用於公開金鑰驗證 `authmethod` 為密碼或 nsswitch • `password` 用於使用者密碼驗證 `authmethod` 為公開金鑰 • `nsswitch` 驗證方法為 publickey 時用於使用者密碼驗證 驗證順序一律是公開金鑰、然後是密碼。	
`-is-ldap-fastbind`	從「支援支援支援」9.11.1開始ONTAP 、設定為「真」時、會啟用LDAP快速連結以進行Nsswitch驗證；預設值為「假」。要使用 LDAP 快速綁定，必須將該 `-authentication-method`值設置爲 `nsswitch`。"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。	

設定 **Cisco** 雙核心安全性資訊

當您為儲存 VM 啟用 Cisco 雙核心雙因素驗證並登入 SSH 時，您可以使用命令提供這些值 `security login duo create`。如"指令參考資料ONTAP"需詳細 `security login duo create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	套用雙核心驗證設定的儲存 VM （在 ONTAP CLI 中稱為 vserver ）。	
`-integration-key`	您的整合金鑰是在向 DuoTM 註冊 SSH 應用程式時取得的。	
`-secret-key`	您的秘密金鑰是在向 DuoTM 註冊 SSH 應用程式時取得的。	
`-api-host`	API 主機名稱、是在使用 DuoTM 登錄 SSH 應用程式時取得的。例如： `api-<HOSTNAME>.duosecurity.com`	
`-fail-mode`	若發生服務或組態錯誤而無法進行雙核心驗證、則會失敗 `safe` （允許存取）或 `secure` （拒絕存取）。預設值為 `safe`這表示如果由於無法存取雙核心 API 伺服器等錯誤而失敗、就會略過雙核心驗證。	
`-http-proxy`	使用指定的 HTTP Proxy 。如果 HTTP Proxy 需要驗證、請在 Proxy URL 中加入認證。例如： `http-proxy=http://username:password@proxy.example.org:8080`	

`-autopush`	也可以 `true` 或 `false`。預設為 `false`。如果 `true`，雙核會自動將推入登錄請求發送至用戶的電話，如果推入不可用，則會恢復至電話呼叫。請注意、這會有效停用密碼驗證。如果 `false`，系統會提示使用者選擇驗證方法。 當設定為時 `autopush = true`、建議您進行設定 `max-prompts = 1`。	
`-max-prompts`	如果使用者無法以第二個因素驗證、則 DUO 會提示使用者再次驗證。此選項可設定在拒絕存取之前、 DUO 顯示的提示數量上限。必須是 `1`、 `2`或 `3`。預設值為 `1`。 例如、何時 `max-prompts = 1`，使用者必須在第一個提示字元上成功驗證，如果是的話 `max-prompts = 2`如果使用者在初始提示時輸入不正確的資訊、系統會提示使用者再次驗證。 當設定為時 `autopush = true`、建議您進行設定 `max-prompts = 1`。 為了獲得最佳體驗、只有公共金鑰驗證的使用者將永遠擁有 `max-prompts` 設定為 `1`。	
`-enabled`	啟用雙核心雙因素驗證。設定為 `true` 依預設。啟用時、會根據設定的參數、在 SSH 登入期間強制執行雙核心雙因素驗證。當雙核心停用時（設為 `false`）、會忽略雙核心驗證。	
`-pushinfo`	此選項會在推播通知中提供其他資訊、例如正在存取的應用程式或服務名稱。這有助於使用者驗證登入的服務是否正確、並提供額外的安全層。	

定義自訂角色

您可以在定義自訂角色時，使用命令提供這些值 `security login role create`。如"指令參考資料ONTAP"需詳細 `security login role create`資訊，請參閱。

欄位	說明	您的價值
-vserver	（選用）與角色相關聯的儲存 VM 名稱（在 ONTAP CLI 中稱為 vserver ）。	
-role	角色名稱。	
-cmddirname	角色提供存取權的命令或命令目錄。您應該以雙引號（"）括住命令子目錄名稱。例如、 "volume snapshot"。您必須輸入 DEFAULT 指定所有命令目錄。	
-access	（選用）角色的存取層級。對於命令目錄： • none （自訂角色的預設值）會拒絕存取命令目錄中的命令 • readonly 授予存取權 show 命令目錄及其子目錄中的命令 • all 授予對命令目錄及其子目錄中所有命令的存取權 用於 _nonnonnalin 命令 _ （不以結尾的命令） create、 modify、 delete`或 `show）： • none （自訂角色的預設值）拒絕存取命令 • readonly 不適用 • all 授予對命令的存取權 若要授與或拒絕內部命令的存取權、您必須指定命令目錄。	
-query	（選用）用於篩選存取層級的查詢物件、其格式為命令的有效選項或命令目錄中的命令的有效選項。您應該以雙引號（"）括住查詢物件。例如、如果命令目錄為 volume，查詢物件 "-aggr aggr0" 將啟用的存取 aggr0 僅 Aggregate 。	

將公開金鑰與使用者帳戶建立關聯

當您將 SSH 公開金鑰與使用者帳戶建立關聯時，您可以使用命令提供這些值 security login publickey create。如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	（選用）帳戶存取的儲存 VM 名稱。	
`-username`	帳戶的使用者名稱。預設值、`admin`，這是叢集管理員的預設名稱。	
`-index`	公開金鑰的索引編號。如果金鑰是為帳戶建立的第一個金鑰、則預設值為0；否則、預設值大於該帳戶現有的最高索引編號。	
`-publickey`	OpenSSH公開金鑰。您應該以雙引號（"）括住金鑰。	
`-role`	指派給帳戶的存取控制角色。	
`-comment`	（選用）公開金鑰的說明文字。您應該以雙引號（"）括住文字。	
`-x509-certificate`	（選用）從 ONTAP 9.13.1 開始、可讓您管理與 SSH 公開金鑰的 X.509 憑證關聯。 當您將 X.509 憑證與 SSH 公開金鑰建立關聯時、 ONTAP 會在 SSH 登入時檢查此憑證是否有效。如果已過期或遭撤銷、則不允許登入、並停用相關的 SSH 公開金鑰。可能值： • `install`：安裝指定的 PEM 編碼的 X.509 憑證、並將其與 SSH 公開金鑰建立關聯。包含您要安裝之憑證的完整文字。 • `modify`：使用指定的證書更新現有的 PEM 編碼的 X.509 證書，並將其與 SSH 公共密鑰相關聯。包含新憑證的完整文字。 • `delete`：移除現有的 X.509 憑證與 SSH 公開金鑰的關聯。	

設定動態授權全域設定

從 ONTAP 9.15.1 開始，您可以使用命令提供這些值 `security dynamic-authorization modify`。如"指令參考資料ONTAP"需詳細 `security dynamic-authorization modify`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	應修改其信任分數設定的儲存 VM 名稱。如果省略此參數、則會使用叢集層級的設定。	
`-state`	動態授權模式。可能值： • `disabled`：（預設）停用動態授權。 • `visibility`：此模式可用於測試動態授權。在此模式中、信任分數會針對每個受限活動進行檢查、但不會強制執行。但是、任何會被拒絕或受到其他驗證挑戰的活動都會記錄下來。 • `enforced`：在您完成測試之後、請使用 `visibility` 模式。在此模式中、每個受限活動都會檢查信任分數、如果符合限制條件、則會強制執行活動限制。也會強制執行抑制間隔、以防止在指定時間間隔內發生其他驗證挑戰。	
`-suppression-interval`	防止在指定時間間隔內發生其他驗證挑戰。時間間隔為 ISO-8601 格式、可接受 1 分鐘至 1 小時的值（含 1 小時）。如果設為 0 、則會停用抑制時間間隔、並在需要驗證挑戰時一律提示使用者。	
`-lower-challenge-boundary`	較低的多因素驗證（ MFA ）挑戰百分比界限。有效範圍為 0 到 99 。值 100 無效、因為這會導致拒絕所有要求。預設值為 0 。	
`-upper-challenge-boundary`	MFA 上限挑戰百分比界限。有效範圍為 0 至 100 。此值必須等於或大於下限值。值為 100 表示每個要求都會遭到拒絕或受到額外的驗證挑戰；沒有任何要求會在沒有挑戰的情況下被允許。預設值為 90 。	

安裝**CA**簽署的伺服器數位憑證

當您產生數位憑證簽署要求（ CSR ）以將儲存 VM 驗證為 SSL 伺服器時，您可以使用命令提供這些值 `security certificate generate-csr`。如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

欄位	說明	您的價值
-common-name	憑證的名稱、可以是完整網域名稱（FQDN）或自訂通用名稱。	
-size	私密金鑰中的位元數。價值越高、金鑰就越安全。預設值為 2048。可能的值包括 512、 1024、 1536`和 `2048。	
-country	儲存 VM 的國家 / 地區、以兩個字母的代碼表示。預設值為 US。如需代碼清單，請參閱"指令參考資料ONTAP"。	
-state	儲存 VM 的州或省。	
-locality	儲存 VM 的位置。	
-organization	儲存 VM 的組織。	
-unit	儲存 VM 組織中的單位。	
-email-addr	儲存 VM 連絡管理員的電子郵件地址。	
-hash-function	用於簽署憑證的密碼編譯雜湊功能。預設值為 SHA256。可能的值包括 SHA1、 SHA256`和 `MD5。	

當您安裝 CA 簽署的數位憑證以將叢集或儲存 VM 驗證為 SSL 伺服器時，您可以使用命令提供這些值 security certificate install。下表僅顯示與帳戶組態相關的選項。如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

欄位	說明	您的價值
-vserver	要安裝憑證的儲存 VM 名稱。	

`-type`	憑證類型： • `server` 適用於伺服器憑證和中繼憑證 • `client-ca` 用於 SSL 用戶端根 CA 的公開金鑰憑證 • `server-ca` 用於 ONTAP 為用戶端之 SSL 伺服器根 CA 的公開金鑰憑證 • `client` 適用於自我簽署或 CA 簽署的數位憑證、以及 ONTAP 做為 SSL 用戶端的私密金鑰	

設定**Active Directory**網域控制器存取

當您已為資料儲存 VM 設定 SMB 伺服器，並且想要將儲存 VM 設定為閘道或 *tunnel* ，以便 Active Directory 網域控制器存取叢集時，您可以使用命令提供這些值 `security login domain-tunnel create`。如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	已設定 SMB 伺服器的儲存 VM 名稱。	

當您尚未設定 SMB 伺服器，且想要在 Active Directory 網域上建立儲存 VM 電腦帳戶時，您可以使用命令提供這些值 `vserver active-directory create`。如"指令參考資料ONTAP"需詳細 `vserver active-directory create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要為其建立 Active Directory 電腦帳戶的儲存 VM 名稱。	
`-account-name`	電腦帳戶的NetBios名稱。	
`-domain`	完整網域名稱（FQDN）。	
`-ou`	網域中的組織單位。預設值為 `CN=Computers`。將此值附加到網域名稱、以產生Active Directory辨別名稱。ONTAP	

設定**LDAP**或**NIS**伺服器存取

當您為儲存 VM 建立 LDAP 用戶端組態時，可以使用命令提供這些值 `vserver services name-service ldap client create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

下表僅顯示與帳戶組態相關的選項：

欄位	說明	您的價值
`-vserver`	用戶端組態的儲存 VM 名稱。	
`-client-config`	用戶端組態的名稱。	
`-ldap-servers`	以逗號分隔的 IP 位址清單、以及用戶端所連線之 LDAP 伺服器的主機名稱。	
`-schema`	用戶端用來進行LDAP查詢的架構。	
`-use-start-tls`	用戶端是否使用 Start TLS 來加密與 LDAP 伺服器的通訊 (`true` 或 `false`) 。 支援 Start TLS 、僅能存取資料儲存 VM 。不支援存取管理儲存 VM 。	

當您將 LDAP 用戶端組態與儲存 VM 建立關聯時，可以使用命令提供這些值 `vserver services name-service ldap create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要與用戶端組態建立關聯的儲存 VM 名稱。	
`-client-config`	用戶端組態的名稱。	
`-client-enabled`	儲存 VM 是否可以使用 LDAP 用戶端組態 (`true` 或 `false`) 。	

當您在儲存 VM 上建立 NIS 網域組態時，可以使用命令提供這些值 `vserver services name-service nis-domain create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要在其中建立網域組態的儲存 VM 名稱。	

`-domain`	網域名稱。	
`-nis-servers`	網域組態所使用之 NIS 伺服器的 IP 位址和主機名稱的逗號分隔清單。	

當您指定名稱服務來源的查詢順序時，您可以使用命令來提供這些值 `vserver services name-service ns-switch create`。如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch create`資訊，請參閱。

欄位	說明	您的價值
`-vserver`	要設定名稱服務查詢順序的儲存 VM 名稱。	
`-database`	名稱服務資料庫： • `hosts` 適用於檔案和 DNS 名稱服務 • `group` 適用於檔案、 LDAP 和 NIS 名稱服務 • `passwd` 適用於檔案、 LDAP 和 NIS 名稱服務 • `netgroup` 適用於檔案、 LDAP 和 NIS 名稱服務 • `namemap` 適用於檔案和 LDAP 名稱服務	
`-sources`	查詢名稱服務來源的順序（在以逗號分隔的清單中）： • `files` • `dns` • `ldap` • `nis`	

設定**SAML**存取

從 ONTAP 9.3 開始，您可以使用 `security saml-sp create`命令來設定 SAML 驗證。如"指令參考資料ONTAP"需詳細 `security saml-sp create`資訊，請參閱。

欄位	說明	您的價值

`-idp-uri`	身分識別供應商（IDP）主機的FTP位址或HTTP位址、可從該主機下載IDP中繼資料。	
`-sp-host`	SAML服務供應商主機ONTAP （亦即系統）的主機名稱或IP位址。根據預設、會使用叢集管理LIF的IP位址。	
`-cert-ca` 和 `-cert-serial`或 `-cert-common-name`	服務供應商主機ONTAP 的伺服器認證詳細資料（不知系統如何）。您可以輸入服務供應商的憑證發行憑證授權單位（CA）和憑證序號、或是伺服器憑證一般名稱。	
`-verify-metadata-server`	IDP 中繼資料伺服器的身分識別是否必須驗證 `true` 或 `false`）。最佳實務做法是永遠將此值設為 `true`。	

建立登入帳戶

瞭解如何建立 **ONTAP** 登入帳戶

您可以啟用本機或遠端叢集和SVM系統管理員帳戶。本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。AD帳戶資訊儲存在網域控制器上。LDAP和NIS帳戶位於LDAP和NIS伺服器上。

叢集與**SVM**管理員

_叢集管理員_存取叢集的管理SVM。管理員 SVM 和具有保留名稱的叢集管理員 `admin` 會在叢集設定時自動建立。

具有預設值的叢集管理員 `admin` 角色可以管理整個叢集及其資源。叢集管理員可視需要建立其他具有不同角色的叢集管理員。

_SVM系統管理員_存取資料SVM。叢集管理員會視需要建立資料SVM和SVM管理員。

SVM 系統管理員會被指派 `vsadmin` 依預設、角色。叢集管理員可視需要指派不同的角色給SVM管理員。

命名慣例

下列一般名稱無法用於遠端叢集和 SVM 系統管理員帳戶：

- "ADM"
- " 垃圾桶 "
- "CL1"
- " 常駐程式 "

- "FTP"
- " 遊戲 "
- " 停止 "
- "LP"
- " 郵件 "
- " 男性 "
- " 拍攝範圍 "
- 「 NetApp 」
- " 新聞 "
- " 無人 "
- " 營運者 "
- " 根目錄 "
- " 關機 "
- "sshd"
- " 同步 "
- " 系統 "
- "uucp"
- "www"

合併的角色

如果您為同一位使用者啟用多個遠端帳戶、則會將為該帳戶指定的所有角色指派給該使用者。也就是說、如果已指派 LDAP 或 NIS 帳戶 `vsadmin` 角色、以及指派給相同使用者的 AD 群組帳戶 `vsadmin-volume` 角色、 AD 使用者以更具包容性的方式登入 `vsadmin` 功能。這些角色據說是_合併_。

啟用本機帳戶存取

瞭解如何啟用本機 **ONTAP** 帳戶存取

本機帳戶是指帳戶資訊、公開金鑰或安全性憑證位於儲存系統上的帳戶。您可以使用 `security login create`命令啟用本機帳戶來存取管理或資料 SVM 。

相關資訊

- "建立安全登入"

啟用 **ONTAP** 帳戶密碼存取

您可以使用 `security login create`命令來啟用系統管理員帳戶，以密碼存取管理員或資料 SVM 。輸入命令後、系統會提示您輸入密碼。

關於這項工作

如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 讓本機系統管理員帳戶使用密碼存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用叢集管理員帳戶 `admin1` 使用預先定義的 `backup` 存取管理 SVM 的角色`engCluster` 使用密碼。輸入命令後、系統會提示您輸入密碼。

   ```
   cluster1::>security login create -vserver engCluster -user-or-group-name
   admin1 -application ssh -authmethod password -role backup
   ```

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

啟用 **ONTAP** 帳戶 **SSH** 公開金鑰存取

您可以使用 `security login create`命令，讓系統管理員帳戶使用 SSH 公開金鑰存取管理或資料 SVM 。

關於這項工作

- 您必須先將公開金鑰與帳戶建立關聯、帳戶才能存取SVM。

  將公開金鑰與使用者帳戶建立關聯

  您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

如果您想在叢集上啟用FIPS模式、則必須使用支援的金鑰類型來重新設定現有SSH公開金鑰帳戶、而不需要支援的金鑰演算法。 在您啟用FIPS之前、應先重新設定帳戶、否則系統管理員驗證將會失敗。

下表指出ONTAP 支援哪些主機金鑰類型演算法來進行支援以利執行支援的SSH連線。 這些金鑰類型不適用於設定SSH公用驗證。

發行版ONTAP	FIPS模式支援的金鑰類型	非FIPS模式支援的金鑰類型

9.11.1 及更新版本	ECDSA-SHA2-nistp256	ECDSA-SHA2-nistp256 RSA-SHA2-512 RSA-SHA2-256 SSH-ed25519 SSH-DSS SSH-RSA
9.10.1及更早版本	ECDSA-SHA2-nistp256 SSH-ed25519.	ECDSA-SHA2-nistp256 SSH-ed25519 SSH-DSS SSH-RSA

從 ONTAP 9.11.1 開始、移除對 ssh-ed25519 主機金鑰演算法的支援。

如需更多資訊、請參閱 "使用FIPS設定網路安全性"。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 允許本機系統管理員帳戶使用SSH公開金鑰存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用 SVM 管理員帳戶 `svmadmin1` 使用預先定義的 `vsadmin-volume` 存取 SVM 的角色`engData1` 使用 SSH 公開金鑰：

   ```
   cluster1::>security login create -vserver engData1 -user-or-group-name
   svmadmin1 -application ssh -authmethod publickey -role vsadmin-volume
   ```

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

完成後

如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

將公開金鑰與使用者帳戶建立關聯

啟用多因素驗證（ **MFA** ）帳戶

瞭解 **ONTAP** 多因素驗證

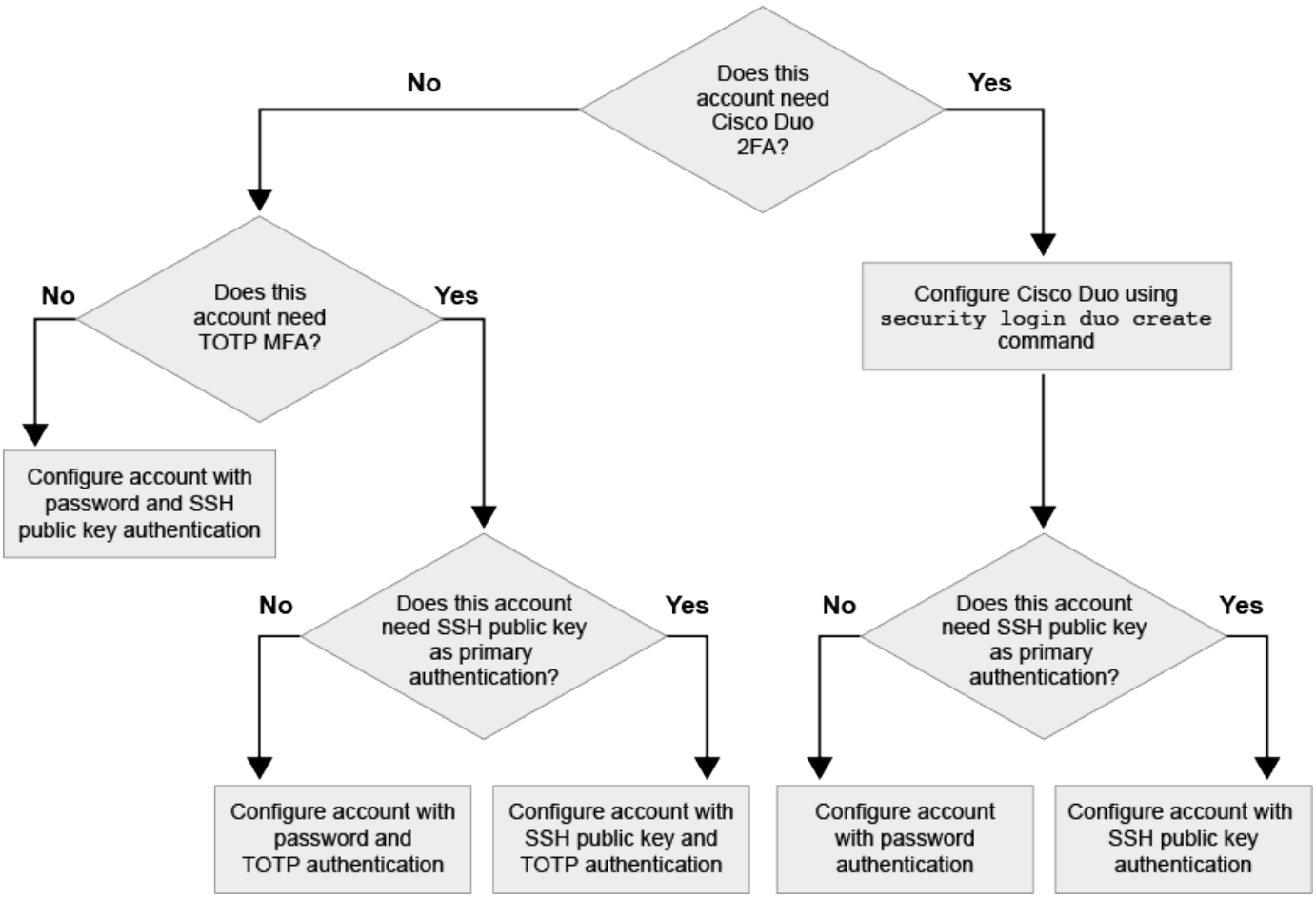
多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料儲存 VM 、以增強安全性。

視您的 ONTAP 版本而定、您可以結合使用 SSH 公開金鑰、使用者密碼和時間型一次性密碼（ TOTP ）進行多

因素驗證。當您啟用和設定 Cisco Duo （ ONTAP 9.14.1 及更新版本）時、它會作為額外的驗證方法、以補充所有使用者的現有方法。

可從 ... 開始使用。	第一種驗證方法	第二種驗證方法
ONTAP 9.14.1.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
	SSH公開金鑰	Cisco DuoTM
	使用者密碼	Cisco DuoTM
ONTAP 9.13.1.12.9.11.9.11.	SSH公開金鑰	TOTP
	使用者密碼	TOTP
ONTAP 9.3	SSH公開金鑰	使用者密碼

如果已設定 MFA 、叢集管理員必須先啟用本機使用者帳戶、則該帳戶必須由本機使用者設定。



使用 **SSH** 和 **TOTP** 啟用 **ONTAP** 多因素驗證

多因素驗證（ MFA ）可讓您要求使用者提供兩種驗證方法來登入管理或資料 SVM 、以增強安全性。

關於這項工作

- 您必須是叢集管理員才能執行此工作。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  "修改指派給系統管理員的角色"

- 如果您使用公開金鑰進行驗證、則必須先將公開金鑰與帳戶建立關聯、帳戶才能存取 SVM 。

  "將公開金鑰與使用者帳戶建立關聯"

  您可以在啟用帳戶存取之前或之後執行此工作。

- 從S廳9.12.1開始ONTAP 、您可以使用FIDO2（Fast Identity Online）或個人身分驗證（PIV）驗證標準、將Yobikey硬體驗證裝置用於SSH用戶端MFA。

使用 **SSH** 公開金鑰和使用者密碼來啟用 **MFA**

從 ONTAP 9.3 開始、叢集管理員可以設定本機使用者帳戶、使用 SSH 公開金鑰和使用者密碼登入 MFA 。

1. 使用 SSH 公開金鑰和使用者密碼、在本機使用者帳戶上啟用 MFA ：

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_name> -application ssh -authentication-method <password|publickey>
   -role admin -second-authentication-method <password|publickey>
   ```

   下列命令需要 SVM 系統管理員帳戶 `admin2` 使用預先定義的 `admin` 登入 SVM 的角色`engData1` 使用 SSH 公開金鑰和使用者密碼：

   ```
   cluster-1::> security login create -vserver engData1 -user-or-group-name
   admin2 -application ssh -authentication-method publickey -role admin
   -second-authentication-method password

   Please enter a password for user 'admin2':
   Please enter it again:
   Warning: To use public-key authentication, you must create a public key
   for user "admin2".
   ```

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

使用 **TOTP** 啟用 **MFA**

從 ONTAP 9.13.1 開始、您可以要求本機使用者同時使用 SSH 公開金鑰或使用者密碼和時間型一次性密碼（ TOTP ）登入管理或資料 SVM 、以增強安全性。啟用 MFA 與 TOTP 的帳戶後、本機使用者必須登入 "完成組態設定"。

TOTP 是一種電腦演算法、使用目前時間來產生一次性密碼。 如果使用 TOTP 、它永遠是 SSH 公開金鑰或使用

者密碼之後的第二種驗證形式。

開始之前

您必須是儲存管理員才能執行這些工作。

步驟

您可以將 MFA 設為使用者密碼或 SSH 公開金鑰做為第一種驗證方法、並將 TOTP 設為第二種驗證方法。

使用使用者密碼和 **TOTP** 啟用 **MFA**

1. 使用使用者密碼和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   password -second-authentication-method totp -role <role> -comment
   <comment>
   ```

2. 確認 MFA 已啟用 TOTP ：

   ```
   security login show
   ```

使用 **SSH** 公開金鑰和 **TOTP** 啟用 **MFA**

1. 使用 SSH 公開金鑰和 TOTP 啟用多因素驗證的使用者帳戶。

   ◦ 適用於新使用者帳戶 *

   ```
   security login create -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role>
   -comment <comment>
   ```

   ◦ 適用於現有使用者帳戶 *

   ```
   security login modify -vserver <svm_name> -user-or-group-name
   <user_or_group_name> -application ssh -authentication-method
   publickey -second-authentication-method totp -role <role> -comment
   <comment>
   ```

   +
   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

2. 確認 MFA 已啟用 TOTP ：

```
security login show
```

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

完成後

- 如果您尚未將公開金鑰與系統管理員帳戶建立關聯、則必須先建立公開金鑰、帳戶才能存取SVM。

  "將公開金鑰與使用者帳戶建立關聯"

- 本機使用者必須登入才能使用 TOTP 完成 MFA 組態。

  "使用 TOTP 設定 MFA 的本機使用者帳戶"

相關資訊

- "支援多因素驗證ONTAP 功能（TR-4647）"
- "指令參考資料ONTAP"

使用 **TOTP** 設定 **MFA** 的本機 **ONTAP** 使用者帳戶

從 ONTAP 9.13.1 開始，使用者帳戶可以使用時間型一次性密碼（ TOTP ）來設定多因素驗證（ MFA ）。

開始之前

- 儲存管理員必須 "使用 TOTP 啟用 MFA" 作為使用者帳戶的第二種驗證方法。
- 您的主要使用者帳戶驗證方法應為使用者密碼或公開 SSH 金鑰。
- 您必須將 TOTP 應用程式設定為與智慧型手機搭配使用、並建立 TOTP 秘密金鑰。

  支援 Microsoft Authenticator 、 Google Authenticator 、 Authy 及任何其他 TOTP 相容驗證器。

步驟

1. 使用目前的驗證方法登入您的使用者帳戶。

   您目前的驗證方法應該是使用者密碼或 SSH 公開金鑰。

2. 在您的帳戶上建立 TOTP 組態：

```
security login totp create -vserver "<svm_name>" -username
"<account_username >"
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver "<svm_name>" -username
"<account_username>"
```

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 顯示"

重設 **ONTAP** 使用者帳戶的 **TOTP** 秘密金鑰

為了保護您的帳戶安全、如果 TOTP 秘密金鑰遭到洩漏或遺失、您應該停用該金鑰並建立新的金鑰。

如果金鑰遭到入侵、請重設 **TOTP**

如果您的 TOTP 秘密金鑰已洩漏、但您仍有權存取、您可以移除洩漏的金鑰並建立新的金鑰。

1. 使用您的使用者密碼或 SSH 公開金鑰、以及您遭入侵的 TOTP 秘密金鑰、登入您的使用者帳戶。
2. 移除遭入侵的 TOTP 秘密金鑰：

```
security login totp delete -vserver <svm_name> -username
<account_username>
```

3. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username
<account_username>
```

4. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

如果金鑰遺失、請重設 **TOTP**

如果 TOTP 秘密金鑰遺失、請聯絡您的儲存管理員 "停用金鑰"。停用金鑰後、您可以使用第一種驗證方法登入並設定新的 TOTP 。

開始之前

TOTP 秘密金鑰必須由儲存管理員停用。
如果您沒有儲存管理員帳戶、請聯絡您的儲存管理員以停用金鑰。

步驟

1. 儲存管理員停用 TOTP 密碼後、請使用主要驗證方法登入您的本機帳戶。
2. 建立新的 TOTP 秘密金鑰：

```
security login totp create -vserver <svm_name> -username
<account_username >
```

3. 確認您的帳戶已啟用 TOTP 組態：

```
security login totp show -vserver <svm_name> -username
<account_username>
```

相關資訊

- "安全登入 totp 創建"
- "安全登入 totp 刪除"
- "安全登入 totp 顯示"

停用 **ONTAP** 使用者帳戶的 **TOTP** 秘密金鑰

如果本機使用者的時間型一次性密碼（ TOTP ）秘密金鑰遺失、則儲存管理員必須先停用遺失的金鑰、使用者才能建立新的 TOTP 秘密金鑰。

關於這項工作

此工作只能從叢集管理員帳戶執行。

步驟

1. 停用 TOTP 秘密金鑰：

```
security login totp modify -vserver <svm_name> -username
<account_username> -enabled false
```

如"指令參考資料ONTAP"需詳細 `security login totp modify`資訊，請參閱。

啟用 **SSL** 憑證 **ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用系統管理員帳戶，以 SSL 憑證存取管理或資料 SVM 。

關於這項工作

- 您必須先安裝CA簽署的伺服器數位憑證、帳戶才能存取SVM。

  產生及安裝CA簽署的伺服器憑證

您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色、可以稍後再使用新增該角色 `security login modify` 命令。

  修改指派給系統管理員的角色

  對於叢集管理員帳戶、支援憑證驗證 `http`、 `ontapi`和 `rest` 應用程式：對於 SVM 系統管理員帳戶、僅支援憑證驗證 `ontapi` 和 `rest` 應用程式：

步驟

1. 啟用本機系統管理員帳戶、以使用SSL憑證存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_or_group_name
   -application application -authmethod authentication_method -role role -comment
   comment
   ```

   下列命令可啟用 SVM 管理員帳戶 `svmadmin2` 使用預設值 `vsadmin` 存取 SVM 的角色`engData2` 使用 SSL 數位憑證。

   ```
   cluster1::>security login create -vserver engData2 -user-or-group-name
   svmadmin2 -application ontapi -authmethod cert
   ```

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

完成後

如果您尚未安裝CA簽署的伺服器數位憑證、則必須先安裝該憑證、帳戶才能存取SVM。

產生及安裝CA簽署的伺服器憑證

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

啟用 **Active Directory ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用 Active Directory （ AD ）使用者或群組帳戶，以存取管理員或資料 SVM 。AD群組中的任何使用者都可以使用指派給群組的角色來存取SVM。

關於這項工作

- 您必須先設定AD網域控制器存取叢集或SVM、帳戶才能存取SVM。

  設定Active Directory網域控制器存取

  您可以在啟用帳戶存取之前或之後執行此工作。

- 從 ONTAP 9.13.1 開始、您可以使用 SSH 公開金鑰做為主要或次要驗證方法、並提供 AD 使用者密碼。

  如果您選擇使用 SSH 公開金鑰做為主要驗證、則不會進行 AD 驗證。

- 從 ONTAP 9.11.1 開始，如果 AD LDAP 伺服器支援，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。
- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  修改指派給系統管理員的角色

僅支援 AD 群組帳戶存取 `SSH`、 `ontapi`和 `rest` 應用程式：SSH 公開金鑰驗證通常用於多因素驗證、因此不支援 AD 群組。

開始之前

- 叢集時間必須在AD網域控制器上的時間後五分鐘內同步處理。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 啟用AD使用者或群組管理員帳戶以存取SVM：

   ◦ 針對 AD 使用者： *

版本**ONTAP**	主要驗證	次要驗證	命令
9.13.1 及更新版本	公開金鑰	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method publickey -role <role>`

版本**ONTAP**	主要驗證	次要驗證	命令

9.13.1 及更新版本	網域	公開金鑰	• 適用於新使用者 *
			`security login create -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`
			• 適用於現有使用者 *
			`security login modify -vserver <svm_name> -user-or-group-name <user_name> -application ssh -authentication-method domain -second -authentication-method publickey -role <role>`

9.0 及更新版本	網域	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

◦ 對於 AD 群組： *

版本**ONTAP**	主要驗證	次要驗證	命令
9.0 及更新版本	網域	無	`security login create -vserver <svm_name> -user-or-group-name <user_name> -application <application> -authentication-method domain -role <role> -comment <comment> [-is-ldap-fastbind true]`

完成後

如果您尚未設定AD網域控制器對叢集或SVM的存取、則必須先設定、帳戶才能存取SVM。

設定Active Directory網域控制器存取

相關資訊

- "建立安全登入"

啟用 **LDAP** 或 **NIS ONTAP** 帳戶存取

您可以使用 `security login create`命令來啟用 LDAP 或 NIS 使用者帳戶，以存取管理或資料 SVM 。如果您尚未設定LDAP或NIS伺服器存取SVM、則必須先設定、帳戶才能存取SVM。

關於這項工作

- 不支援群組帳戶。
- 您必須先設定LDAP或NIS伺服器存取SVM、帳戶才能存取SVM。

  設定LDAP或NIS伺服器存取

  您可以在啟用帳戶存取之前或之後執行此工作。

- 如果您不確定要指派給登入帳戶的存取控制角色，可以使用 `security login modify`命令稍後再新增該角色。

  如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

  修改指派給系統管理員的角色

- 從ONTAP 功能支援的版本為2、9.4開始、透過LDAP或NIS伺服器、遠端使用者可支援多因素驗證（MFA）。
- 從 ONTAP 9.11.1 開始，如果 LDAP 伺服器支援，您可以使用"使用 LDAP 快速綁定對 ONTAP NFS SVM 進行 nsswitch 驗證"。
- 由於已知的 LDAP 問題、您不應使用 `':'` （結腸） LDAP 使用者帳戶資訊任何欄位中的字元（例如、 `gecos`、 `userPassword`等）。否則、該使用者的查詢作業將會失敗。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 啟用LDAP或NIS使用者或群組帳戶以存取SVM：

   ```
   security login create -vserver SVM_name -user-or-group-name user_name
   -application application -authmethod nsswitch -role role -comment comment -is
   -ns-switch-group yes|no [-is-ldap-fastbind true]
   ```

   "建立或修改登入帳戶"

   下列命令可啟用 LDAP 或 NIS 叢集管理員帳戶 `guest2` 使用預先定義的 `backup` 存取管理 SVM 的角色`engCluster`。

```
cluster1::>security login create -vserver engCluster -user-or-group-name
guest2 -application ssh -authmethod nsswitch -role backup
```

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

2. 為LDAP或NIS使用者啟用MFA登入：

```
security login modify -user-or-group-name rem_usr1 -application ssh
-authentication-method nsswitch -role admin -is-ns-switch-group no -second
-authentication-method publickey
```

驗證方法可以指定為 `publickey` 和第二種驗證方法 `nsswitch`。

下列範例顯示正在啟用MFA驗證：

```
cluster-1::*> security login modify -user-or-group-name rem_usr2
-application ssh -authentication-method nsswitch -vserver
cluster-1 -second-authentication-method publickey"
```

完成後

如果您尚未設定LDAP或NIS伺服器存取SVM、則必須先設定、帳戶才能存取SVM。

設定LDAP或NIS伺服器存取

相關資訊

- "安全登入"

管理存取控制角色

瞭解如何管理 **ONTAP** 存取控制角色

指派給系統管理員的角色會決定系統管理員可以存取的命令。當您為系統管理員建立帳戶時、可以指派角色。您可以指派不同的角色、或視需要定義自訂角色。

修改指派給 **ONTAP** 管理員的角色

您可以使用 `security login modify`命令來變更叢集或 SVM 管理員帳戶的角色。您可以指派預先定義或自訂的角色。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 變更叢集或SVM管理員的角色：

```
security login modify -vserver SVM_name -user-or-group-name user_or_group_name
-application application -authmethod authentication_method -role role -comment
comment
```

"建立或修改登入帳戶"

下列命令會變更 AD 叢集管理員帳戶的角色 `DOMAIN1\guest1` 至預先定義的 `readonly` 角色：

```
cluster1::>security login modify -vserver engCluster -user-or-group-name
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

下列命令會變更 AD 群組帳戶中 SVM 管理員帳戶的角色 `DOMAIN1\adgroup` 自訂 `vol_role` 角色：

```
cluster1::>security login modify -vserver engData -user-or-group-name
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

為 ONTAP 管理員定義自訂角色

您可以使用 `security login role create`命令來定義自訂角色。您可以視需要多次執行命令、以取得想要與角色建立關聯的確切功能組合。

關於這項工作

- 無論是預先定義或自訂的角色、都會授予或拒絕ONTAP 存取各種指令或命令目錄。

  命令目錄 (`volume`（例如）是一組相關命令和命令子目錄。除非如本程序所述、否則授與或拒絕存取命令目錄會授與或拒絕存取目錄及其子目錄中的每個命令。

- 特定命令存取或子目錄存取會覆寫父目錄存取。

  如果某個角色是以命令目錄定義、然後以不同的存取層級再次定義、以用於特定命令或父目錄的子目錄、則為該命令或子目錄指定的存取層級會覆寫父目錄的存取層級。

> ⓘ 您無法為 SVM 管理員指派一個角色、讓其存取僅供使用的命令或命令目錄 `admin` 叢集管理員、例如 `security` 命令目錄。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 定義自訂角色：

   ```
   security login role create -vserver SVM_name -role role -cmddirname
   command_or_directory_name -access access_level -query query
   ```

下列命令會授與 `vol_role` 角色完整存取中的命令 `volume` 命令目錄及中命令的唯讀存取權 `volume snapshot` 子目錄。

```
cluster1::>security login role create -role vol_role -cmddirname
"volume" -access all

cluster1::>security login role create -role vol_role -cmddirname "volume
snapshot" -access readonly
```

下列命令會授與 `SVM_storage` 角色對中命令的唯讀存取權 `storage` 命令目錄、無法存取中的命令 `storage encryption` 子目錄、以及對的完整存取權 `storage aggregate plex offline` 非固有命令。

```
cluster1::>security login role create -role SVM_storage -cmddirname
"storage" -access readonly

cluster1::>security login role create -role SVM_storage -cmddirname
"storage encryption" -access none

cluster1::>security login role create -role SVM_storage -cmddirname
"storage aggregate plex offline" -access all
```

如"指令參考資料ONTAP"需詳細 `security login role create`資訊，請參閱。

相關資訊

- "建立安全登入角色"
- "離線儲存Aggregate叢"
- "儲存加密"

預先定義的 **ONTAP** 叢集管理員角色

叢集管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。依預設、會指派預先定義的叢集管理員 `admin` 角色：

下表列出叢集管理員的預先定義角色：

此角色...	具有此存取層級...	至下列命令或命令目錄
管理	全部	所有命令目錄 (`DEFAULT`)

Admin-NO FSA （從 ONTAP 9.12.1 開始提供）	讀取/寫入	• 所有命令目錄 (DEFAULT) • security login rest-role • security login role
唯讀	• security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics	無
volume file show-disk-usage	AutoSupport	全部
• set • system node autosupport	無	所有其他命令目錄 (DEFAULT)
備份	全部	vserver services ndmp
唯讀	volume	無
所有其他命令目錄 (DEFAULT)	唯讀	全部

• `security login password` 僅用於管理自己的使用者帳戶本機密碼和金鑰資訊 • `set`	• 從 ONTAP 9.8 開始，只讀 • ONTAP 9.8 之前，無	`security`
唯讀	所有其他命令目錄 (`DEFAULT`)	SnapLock
全部	• `set` • `volume create` • `volume modify` • `volume move` • `volume show`	無
• `volume move governor` • `volume move recommend`	無	所有其他命令目錄 (`DEFAULT`)
無	無	所有命令目錄 (`DEFAULT`)

。 `autosupport` 角色會指派給預先定義的 `autosupport` 帳戶、由 AutoSupport OnDemand 使用。ONTAP 可防止您修改或刪除 `autosupport` 帳戶。ONTAP 也會防止您指派 `autosupport` 其他使用者帳戶的角色。

相關資訊

- "安全登入"
- "設定"
- "Volume"
- "Vserver 服務 NDMP"

預先定義的 **ONTAP SVM** 管理員角色

SVM系統管理員的預先定義角色應能滿足您大部分的需求。您可以視需要建立自訂角色。根據預設、系統會指派預先定義的 SVM 管理員 `vsadmin` 角色：

下表列出SVM系統管理員的預先定義角色：

角色名稱	功能

vsadmin	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 執行SnapLock 不含權限刪除的功能 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控工作 • 監控網路連線和網路介面 • 監控SVM的健全狀況
vsadmin-volume	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 管理LUN • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 監控網路介面 • 監控SVM的健全狀況
vsadmin-Protocol	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 設定通訊協定： NFS 、 SMB 、 iSCSI 、 FC 、 FCoE 、 NVMe / FC 和 NVMe / TCP • 設定服務：DNS、LDAP及NIS • 管理LUN • 監控網路介面 • 監控SVM的健全狀況
vsadmin-Backup	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理NDMP作業 • 使還原的Volume能夠讀取/寫入 • 管理 SnapMirror 關係和快照 • 檢視磁碟區和網路資訊

vsadmin-SnapLock	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 管理磁碟區、磁碟區移動除外 • 管理配額， qtree ，快照和檔案 • 執行SnapLock 包含特權刪除在內的功能 • 設定傳輸協定：NFS和SMB • 設定服務：DNS、LDAP及NIS • 監控工作 • 監控網路連線和網路介面
vsadmin-readonly	• 管理自己的使用者帳戶本機密碼和金鑰資訊 • 監控SVM的健全狀況 • 監控網路介面 • 檢視磁碟區和LUN • 檢視服務與傳輸協定

使用系統管理員管理 **ONTAP** 管理員存取

指派給系統管理員的角色會決定系統管理員可以使用System Manager執行哪些功能。叢集管理員和儲存VM管理員的預先定義角色由System Manager提供。 您可以在建立系統管理員帳戶時指派角色、也可以稍後指派不同的角色。

視啟用帳戶存取的方式而定、您可能需要執行下列任一項：

- 將公開金鑰與本機帳戶建立關聯。
- 安裝CA簽署的伺服器數位憑證。
- 設定AD、LDAP或NIS存取。

您可以在啟用帳戶存取之前或之後執行這些工作。

指派角色給系統管理員

指派角色給系統管理員、如下所示：

步驟

1. 選擇*叢集>設定*。
2. 選取 → * 使用者與角色 * 旁的。
3. 在 * 使用者 * 下選取 + Add 。
4. 指定使用者名稱、然後在下拉式功能表中選取*角色*的角色。
5. 指定使用者的登入方法和密碼。

變更系統管理員的角色

變更系統管理員的角色、如下所示：

步驟

1. 按一下*叢集>設定*。
2. 選取您要變更其角色的使用者名稱、然後按一下 ⋮ 出現在使用者名稱旁的。
3. 按一下 * 編輯 * 。
4. 在下拉式功能表中選取*角色*的角色。

在**ONTAP**中存取 **JIT** 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以"配置即時（JIT）權限提升"允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者設定 JIT 後，使用者可以將其權限暫時提升到具有執行任務所需權限的角色。會話到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，叢集管理員可以將使用者存取 JIT 提升的權限配置為每次會話 30 分鐘（會話有效期），為期 30 天（JIT 有效期）。在 30 天的期限內，使用者可以根據需要多次提升權限，但每次會話的時長限制為 30 分鐘。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在目前 SSH 會話中可用，但您可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。
- 如果設定的會話或 JIT 有效期到期，或叢集管理員撤銷使用者的 JIT 存取權限，則使用者的 JIT 會話將會終止。

開始之前

- 若要存取 JIT 權限提升，叢集管理員必須為您的帳戶設定 JIT 存取權限。叢集管理員將確定您可以提升權限的角色，以及您可以存取提升權限的時間長度。

步驟

1. 暫時將您的權限提升至配置的角色：

```
security jit-privilege elevate
```

輸入此指令後，系統會提示您輸入登入密碼。如果您的帳戶配置了 JIT 存取權限，您將在配置的會話時間長度內獲得提升的存取權限。會話時長到期後，您將恢復到原始存取等級。您可以在設定的 JIT 有效期內根據需要多次提升權限。

2. 查看 JIT 會話中的剩餘時間：

```
security jit-privilege show-remaining-time
```

如果您目前處於 JIT 會話中，此命令將顯示剩餘時間。

3. 如果需要，請提前結束 JIT 會話：

```
security jit-privilege reset
```

如果您目前處於 JIT 會話中，此命令將結束 JIT 會話並恢復您的原始存取等級。

在**ONTAP**中設定 **JIT** 權限提升

從ONTAP 9.17.1 開始，叢集管理員可以設定即時 (JIT) 權限提升，以允許ONTAP使用者暫時提升其權限以執行某些任務。為使用者配置 JIT 後，他們可以臨時"提升他們的特權"賦予具有執行任務所需權限的角色。會話持續時間到期後，使用者將恢復其原始存取等級。

叢集管理員可以設定使用者存取 JIT 提升的時長。例如，您可以設定使用者存取 JIT 提升的時長，在 30 天的時間內（即「JIT 有效期」），每次會話的時長限制為 30 分鐘（即「會話有效期限」）。在這 30 天的時間段內，使用者可以根據需要多次提升權限，但每次會話的時間限制為 30 分鐘。

JIT 權限提升支援最小權限原則，讓使用者執行需要提升權限的任務，而無需永久授予這些權限。這有助於降低未經授權的存取或意外更改系統的風險。以下範例描述了 JIT 權限提升的一些常見用例：

- 允許臨時訪問 `security login create`和 `security login delete`命令來啟用使用者的入職和離職。
- 允許臨時訪問 `system node image update`和 `system node upgrade-revert`在更新視窗期間。更新完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `cluster add-node`， `cluster remove-node`， 和 `cluster modify`以啟用叢集擴充或重新配置。叢集變更完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `volume snapshot restore`啟用還原作業和備份目標管理。還原或設定完成後，命令存取權限將被撤銷。
- 允許臨時訪問 `security audit log show`在合規性檢查期間啟用稽核日誌審查和匯出。

如需查看更詳細的常見 JIT 用例列表，請參閱常見的 JIT 用例 。

叢集管理員可以為ONTAP使用者設定 JIT 存取權限，並在整個叢集範圍內或為特定 SVM 配置預設 JIT 有效期。

關於這項工作

- JIT 權限提升僅適用於使用 SSH 存取ONTAP的使用者。提升的權限僅在使用者目前的 SSH 會話中可用，但使用者可以根據需要在任意數量的並發 SSH 會話中提升權限。
- JIT 權限提升僅支援使用密碼、nsswitch 或網域驗證登入的使用者。 JIT 權限提升不支援多重身分驗證 (MFA)。

開始之前

- 您必須是ONTAP叢集管理員 `admin`權限等級來執行下列任務。

修改全域 **JIT** 設定

您可以修改ONTAP叢集全域或特定 SVM 的預設 JIT 設定。這些設定決定了已配置 JIT 存取的使用者的預設會話有效期和最大 JIT 有效期。

關於這項工作

- 預設 `default-session-validity-period`值為一小時。此設定決定使用者在 JIT 會話中可以存取提升權限的時間，之後需要重新提升權限。
- 預設 `max-jit-validity-period`值為 90 天。此設定決定了使用者在配置的開始日期之後可以存取 JIT 提升權限的最長期限。您可以為單一使用者設定 JIT 有效期，但不能超過最長 JIT 有效期。

步驟

1. 檢查目前 JIT 設定：

```
security jit-privilege show -vserver <svm_name>
```

`-vserver`是可選的。如果您未指定 SVM，則命令將顯示全域 JIT 設定。

2. 全域或針對 SVM 修改 JIT 設定：

```
security jit-privilege modify -vserver <svm_name> -default-session
-validity-period <period> -max-jit-validity-period <period>
```

如果您未指定 SVM，則命令將修改全域 JIT 設定。以下範例將 SVM 的預設 JIT 會話時長設定為 45 分鐘，最大 JIT 長度設定為 30 天 `svm1` ：+
`security jit-privilege modify -vserver svm1 -default-session-validity-period 45m -max-jit-validity-period 30d`

在此範例中，使用者將能夠一次存取 45 分鐘的 JIT 提升，並且可以在配置的開始日期之後最多 30 天內啟動 JIT 工作階段。

為使用者配置 **JIT** 權限提升存取權限

您可以為ONTAP使用者指派 JIT 權限提升存取權限。

步驟

1. 檢查使用者目前的 JIT 存取權限：

```
security jit-privilege user show -username <username>
```

`-username`是可選的。如果您未指定使用者名，該命令將顯示所有使用者的 JIT 存取權限。

2. 為使用者指派新的 JIT 存取權限：

```
security jit-privilege create -username <username> -vserver <svm_name>
-role <rbac_role> -session-validity-period <period> -jit-validity-period
<period> -start-time <date>
```

- 如果 `-vserver`未指定，則在叢集層級分配 JIT 存取。
- `-role`是使用者將被提升到的 RBAC 角色。如果未指定， `-role`預設為 `admin`。
- `-session-validity-period`是使用者在需要啟動新的 JIT 會話之前可以存取提升角色的時間長度。如果未指定，則全域或 SVM `default-session-validity-period`被使用。
- `-jit-validity-period`是使用者在配置的開始日期之後可以發起 JIT 會話的最長持續時間。如果未指定，則 `session-validity-period`被使用。此參數不能超過全域或 SVM `max-jit-validity-period`。
- `-start-time`是使用者可以啟動 JIT 會話的日期和時間。如果未指定，則使用目前日期和時間。

  下面的例子將允許 `ontap_user`訪問 `admin`角色運行 1 小時後才需要開始新的 JIT 會話。 `ontap_user`將能夠從 2025 年 7 月 1 日下午 1 點開始啟動為期 60 天的 JIT 會話：+
  `security jit-privilege user create -username ontap_user -role admin -session-validity-period 1h -jit-validity-period 60d -start-time "7/1/25 13:00:00"`

3. 如果需要，撤銷使用者的 JIT 存取權限：

```
security jit-privilege user delete -username <username> -vserver
<svm_name>
```

此命令將撤銷使用者的 JIT 存取權限，即使其存取權限尚未過期。如果 `-vserver`如果未指定，則 JIT 存取權限將在叢集層級撤銷。如果使用者處於活動的 JIT 會話中，則該會話將被終止。

常見的 **JIT** 用例

下表包含 JIT 權限提升的常見用例。對於每個用例，都需要配置一個 RBAC 角色來提供對相關命令的存取權限。每個命令都連結到ONTAP命令參考，其中包含有關該命令及其參數的更多資訊。

使用案例	命令	細節
使用者和角色管理	• `security login create` • `security login delete`	在入職或離職期間暫時提升新增/刪除使用者或變更角色的權限。
證書管理	• `security certificate create` • `security certificate install`	授予證書安裝或更新的短期存取權限。
SSH/CLI 存取控制	• `security login create -application ssh`	暫時授予 SSH 存取權限以進行故障排除或供應商支援。
授權管理	• `system license add` • `system license delete`	授予在功能啟動或停用期間新增或刪除許可證的權限。

使用案例	命令	細節
系統升級和修補	• `system node image update` • `system node upgrade-revert`	提升升級窗口，然後撤銷。
網路安全設定	• `security login role create` • `security login role modify`	允許對網路相關的安全角色進行臨時更改。
叢集管理	• `cluster add-node` • `cluster remove-node` • `cluster modify`	提升叢集擴充或重新配置。
SVM 管理	• `vserver create` • `vserver delete` • `vserver modify`	暫時授予 SVM 管理員權限以進行設定或停用。
磁碟區管理	• `volume create` • `volume delete` • `volume modify`	提升磁碟區配置、調整大小或刪除的權限。
快照管理	• `volume snapshot create` • `volume snapshot delete` • `volume snapshot restore`	提升快照刪除或在復原期間復原的權限。
網路組態	• `network interface create` • `network port vlan create`	授予在維護時段內進行網路變更的權利。
磁碟/聚合管理	• `storage disk assign` • `storage aggregate create` • `storage aggregate add-disks`	提升新增或刪除磁碟或管理聚合的能力。

使用案例	命令	細節
資料保護	• `snapmirror create` • `snapmirror modify` • `snapmirror restore`	暫時提升以配置或恢復SnapMirror關係。
效能調優	• `qos policy-group create` • `qos policy-group modify`	提升性能故障排除或調整。
審計日誌訪問	• `security audit log show`	在合規性檢查期間暫時提升稽核日誌審查或匯出權限。
事件和警報管理	• `event notification create` • `event notification modify`	提升設定或測試事件通知或 SNMP 陷阱的權限。
合規性驅動的數據訪問	• `volume show` • `security audit log show`	授予審計員臨時唯讀存取權限以審查敏感資料或日誌。
特權訪問審查	• `security login show` • `security login role show`	暫時提升權限以審查和報告特權存取權限。在限定時間內授予唯讀權限。

相關資訊

- "叢集"
- "事件通知"
- "網路"
- "QoS策略組"
- "安全性"
- "SnapMirror"
- "貯存"
- "系統"
- "Volume"
- "Vserver"

管理系統管理員帳戶

瞭解如何管理 **ONTAP** 系統管理員帳戶

視啟用帳戶存取的方式而定、您可能需要將公開金鑰與本機帳戶建立關聯、安裝CA簽署的

伺服器數位憑證、或設定AD、LDAP或NIS存取。您可以在啟用帳戶存取之前或之後執行所有這些工作。

將公開金鑰與 ONTAP 系統管理員帳戶建立關聯

若要進行SSH公開金鑰驗證、您必須先將公開金鑰與系統管理員帳戶建立關聯、帳戶才能存取SVM。您可以使用 `security login publickey create`命令將金鑰與系統管理員帳戶建立關聯。

關於這項工作

如果您同時使用密碼和SSH公開金鑰透過SSH驗證帳戶、則會先使用公開金鑰驗證帳戶。

開始之前

- 您必須已產生SSH金鑰。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 將公開金鑰與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -comment comment
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey show`資訊，請參閱。

範例

下列命令會將公開金鑰與 SVM 管理員帳戶建立關聯 `svmadmin1` 適用於 SVM `engData1`。公開金鑰已指派索引編號5。

```
cluster1::> security login publickey create -vserver engData1 -username
svmadmin1 -index 5 -publickey
"<key text>"
```

管理 ONTAP 系統管理員的 SSH 公開金鑰和 X.509 憑證

為了提高使用系統管理員帳戶的 SSH 驗證安全性，您可以使用 `security login publickey` 一組命令來管理 SSH 公開金鑰及其與 X.509 憑證的關聯性。

從 ONTAP 9.13.1 開始、您可以將 X.509 憑證與您與系統管理員帳戶相關聯的公開金鑰建立關聯。這可讓您在登入該帳戶的 SSH 時、更安全地進行憑證過期或撤銷檢查。

關於這項工作

如果您透過 SSH 同時使用 SSH 公開金鑰和 X.509 憑證來驗證帳戶、 ONTAP 會在使用 SSH 公開金鑰進行驗證之前、先檢查 X.509 憑證的有效性。如果該憑證過期或撤銷、 SSH 登入將會被拒絕、而且會自動停用公開金鑰。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 您必須已產生SSH金鑰。
- 如果您只需要檢查 X.509 憑證是否過期、您可以使用自我簽署的憑證。
- 如果您需要檢查 X.509 憑證是否過期及撤銷：
  - 您必須已從憑證授權單位（ CA ）收到憑證。
  - 您必須使用命令來安裝憑證鏈結（中繼和根 CA 憑證） `security certificate install`。如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。
  - 您需要啟用 SSH 的 OCSP 。請參閱 "使用OCSP驗證數位憑證是否有效" 以取得相關指示。

步驟

1. 將公開金鑰和 X.509 憑證與系統管理員帳戶建立關聯：

   ```
   security login publickey create -vserver SVM_name -username user_name -index
   index -publickey certificate -x509-certificate install
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey create`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey show`資訊，請參閱。

範例

下列命令會將公開金鑰和 X.509 憑證與 SVM 系統管理員帳戶建立關聯 `svmadmin2` 適用於 SVM `engData2`。公開金鑰會被指派索引編號 6 。

```
cluster1::> security login publickey create -vserver engData2 -username
svmadmin2 -index 6 -publickey
"<key text>" -x509-certificate install
Please enter Certificate: Press <Enter> when done
<certificate text>
```

從系統管理員帳戶的 SSH 公開金鑰中移除憑證關聯

您可以從帳戶的 SSH 公開金鑰中移除目前的憑證關聯、同時保留公開金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除 X.509 憑證關聯、並保留現有的 SSH 公開金鑰：

   ```
   security login publickey modify -vserver SVM_name -username user_name -index
   index -x509-certificate delete
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey modify`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

範例

下列命令會從 SVM 系統管理員帳戶移除 X.509 憑證關聯 `svmadmin2` 適用於 SVM `engData2` 索引編號 6 。

```
cluster1::> security login publickey modify -vserver engData2 -username
svmadmin2 -index 6 -x509-certificate delete
```

從系統管理員帳戶移除公開金鑰和憑證關聯

您可以從帳戶移除目前的公開金鑰和憑證組態。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 從系統管理員帳戶移除公開金鑰和 X.509 憑證關聯：

   ```
   security login publickey delete -vserver SVM_name -username user_name -index
   index
   ```

   如"指令參考資料ONTAP"需詳細 `security login publickey delete`資訊，請參閱。

2. 檢視公開金鑰以驗證變更：

   ```
   security login publickey show -vserver SVM_name -username user_name -index
   index
   ```

範例

下列命令會從 SVM 系統管理員帳戶移除公開金鑰和 X.509 憑證 `svmadmin3` 適用於 SVM `engData3` 索引編號

7 。

```
cluster1::> security login publickey delete -vserver engData3 -username
svmadmin3 -index 7
```

相關資訊

- "安全登入公鑰"

為 ONTAP SSH 登入設定 Cisco 雙核心 2FA

從 ONTAP 9.14.1 開始、您可以將 ONTAP 設定為在登入 SSH 期間使用 Cisco 雙核心進行雙重驗證（ 2FA ）。您可以在叢集層級設定雙核心、而且預設會套用至所有使用者帳戶。或者、您也可以在儲存 VM 層級（之前稱為 vserver ）設定雙核心、在這種情況下、它只適用於該儲存 VM 的使用者。如果您啟用和設定雙核心、它會作為額外的驗證方法、以補充所有使用者的現有方法。

如果您為 SSH 登入啟用雙核心驗證、使用者下次使用 SSH 登入時、將需要註冊裝置。如需報名資訊、請參閱 Cisco Duo "註冊文件"。

您可以使用 ONTAP 命令列介面來執行 Cisco 雙核心的下列工作：

- 設定 Cisco Duo
- 變更 Cisco Duo 組態
- 移除 Cisco Duo 組態
- 查看 Cisco Duo 組態
- 移除 " 雙核心 " 群組
- [檢視雙核心群組]
- [略過使用者的雙核心驗證]

設定 Cisco Duo

您可以使用命令為整個叢集或特定儲存 VM （在 ONTAP CLI 中稱為 Vserver ）建立 Cisco 雙核心組態 `security login duo create`。當您這麼做時、 Cisco Duo 會啟用此叢集或儲存 VM 的 SSH 登入。如"指令參考資料ONTAP"需詳細 `security login duo create`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。
2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 啟用此儲存 VM 的 Cisco Duo 驗證、以環境中的資訊取代方括號中的值：

```
security login duo create \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME>
```

變更 **Cisco Duo** 組態

您可以變更 Cisco Duo 驗證使用者的方式（例如、提供多少驗證提示、或使用什麼 HTTP Proxy ）。如果您需要變更儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo modify`命令。如"指令參考資料ONTAP"需詳細 `security login duo modify`資訊，請參閱。

步驟

1. 登入 Cisco Duo 管理面板。
2. 前往 * 應用程式 > UNIX 應用程式 * 。
3. 記錄您的整合金鑰、秘密金鑰和 API 主機名稱。
4. 使用 SSH 登入您的 ONTAP 帳戶。
5. 變更此儲存 VM 的 Cisco Duo 組態、以您環境中的更新資訊取代方括號中的值：

```
security login duo modify \
-vserver <STORAGE_VM_NAME> \
-integration-key <INTEGRATION_KEY> \
-secret-key <SECRET_KEY> \
-apihost <API_HOSTNAME> \
-pushinfo true|false \
-http-proxy <HTTP_PROXY_URL> \
-autopush true|false \
-max-prompts 1|2|3 \
-is-enabled true|false \
-fail-mode safe|secure
```

移除 **Cisco Duo** 組態

您可以移除 Cisco Duo 組態、這樣就不需要 SSH 使用者在登入時使用 DuoTM 進行驗證。若要移除儲存 VM 的 Cisco 雙核心組態（在 ONTAP CLI 中稱為 vserver ），您可以使用 `security login duo delete`命令。如"指令參考資料ONTAP"需詳細 `security login duo delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除此儲存 VM 的 Cisco Duo 組態、以您的儲存 VM 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo delete  -vserver <STORAGE_VM_NAME>
```

這會永久刪除此儲存 VM 的 Cisco Duo 組態。

查看 Cisco Duo 組態

您可以使用命令檢視儲存 VM （在 ONTAP CLI 中稱為 vserver ）的現有 Cisco 雙核心組態 `security login duo show`。如"指令參考資料ONTAP"需詳細 `security login duo show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示此儲存 VM 的 Cisco Duo 組態。您也可以選擇使用 `vserver` 用於指定儲存 VM 的參數、請將儲存 VM 名稱取代為 `<STORAGE_VM_NAME>`：

```
security login duo show -vserver <STORAGE_VM_NAME>
```

您應該會看到類似下列的輸出：

```
Vserver: testcluster
Enabled: true

Status: ok
INTEGRATION-KEY: DI89811J9JWMJCCO7IOH
SKEY SHA Fingerprint:
b79ffa4b1c50b1c747fbacdb34g671d4814
API Host: api-host.duosecurity.com
Autopush: true
Push info: true
Failmode: safe
Http-proxy: 192.168.0.1:3128
Prompts: 1
Comments: -
```

建立雙核心群組

您可以指示 Cisco DuoTM 僅在特定 Active Directory 、 LDAP 或本機使用者群組中加入使用者、以進行 DuoTM 驗證程序。如果您建立雙核心群組、系統只會提示該群組中的使用者進行雙核心驗證。您可以使用命令建立雙核心群組 `security login duo group create`。建立群組時、您可以選擇性地將該群組中的特定使用者排除在雙核心驗證程序之外。如"指令參考資料ONTAP"需詳細 `security login duo group create`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 建立 DuoTM 群組、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級建

立：

```
security login duo group create -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會納入雙核心驗證程序。

檢視雙核心群組

您可以使用命令來檢視現有的 Cisco 雙核心群組項目 `security login duo group show`。如"指令參考資料ONTAP"需詳細 `security login duo group show`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 顯示 DUO 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會顯示在叢集層級：

```
security login duo group show -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME> -excluded-users <USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用選用參數指定的使用者 `-excluded-users`將不會顯示。

移除 " 雙核心 " 群組

您可以使用命令移除雙核心群組項目 `security login duo group delete`。如果您移除群組、該群組中的使用者將不再包含在雙核心驗證程序中。如"指令參考資料ONTAP"需詳細 `security login duo group delete`資訊，請參閱。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 移除 DuoTM 群組項目、以環境中的資訊取代方括號中的值。如果您省略 `-vserver` 參數、群組會在叢集層級移除：

```
security login duo group delete -vserver <STORAGE_VM_NAME> -group-name
<GROUP_NAME>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。

略過使用者的雙核心驗證

您可以將所有使用者或特定使用者排除在雙核心 SSH 驗證程序之外。

排除所有雙核心使用者

您可以為所有使用者停用 Cisco 雙核心 SSH 驗證。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 停用 SSH 使用者的 Cisco Duo 驗證、以 vserver 名稱取代 `<STORAGE_VM_NAME>`：

```
security login duo modify -vserver <STORAGE_VM_NAME> -is-enabled false
```

不包括雙核心群組使用者

您可以從雙核心 SSH 驗證程序中排除屬於雙核心群組的特定使用者。

步驟

1. 使用 SSH 登入您的 ONTAP 帳戶。
2. 針對群組中的特定使用者停用 Cisco Duo 驗證。以群組名稱和使用者清單取代方括號中的值：

```
security login duo group modify -group-name <GROUP_NAME> -excluded-users
<USER1, USER2>
```

雙核心群組的名稱必須符合 Active Directory 、 LDAP 或本機群組。您使用參數指定的使用者 `-excluded-users`將不會包含在雙核心驗證程序中。

如"指令參考資料ONTAP"需詳細 `security login duo group modify`資訊，請參閱。

排除本機雙核心使用者

您可以使用 Cisco 雙核心管理面板、排除特定的本機使用者使用雙核心驗證。如需相關指示、請參閱 "Cisco Duo 文件"。

在 **ONTAP** 中產生並安裝 **CA** 簽署的伺服器憑證

在正式作業系統上、最佳做法是安裝CA簽署的數位憑證、以用於將叢集或SVM驗證為SSL伺服器。您可以使用命令來產生憑證簽署要求（ CSR ），並 `security certificate install`使用 `security certificate generate-csr`命令來安裝從憑證授權單位收到的憑證。深入瞭解 `security certificate generate-csr`及 `security certificate install` "指令參考資料ONTAP"。

產生憑證簽署要求

您可以使用 `security certificate generate-csr` 產生憑證簽署要求（ CSR ）的命令。在處理您的要求之後、憑證授權單位（CA）會傳送簽署的數位憑證給您。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 產生CSR：

```
security certificate generate-csr -common-name FQDN_or_common_name -size
512|1024|1536|2048 -country country -state state -locality locality
-organization organization -unit unit -email-addr email_of_contact -hash
-function SHA1|SHA256|MD5
```

下列命令會建立 CSR ，其中包含由雜湊函數產生的 2048 位元私密金鑰 `SHA256`，供自訂一般名稱為的公司部門 `server1.companyname.com`中的群組 `IT`使用 `Software`，位於美國加州森尼維爾。SVM 連絡人管理員的電子郵件地址為 `web@example.com`。系統會在輸出中顯示CSR和私密金鑰。

建立 **CSR** 的範例

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California
-locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256

Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----


Private Key :
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

NOTE: Keep a copy of your certificate request and private key for
future reference.
```

2. 從CSR輸出複製憑證要求、然後以電子形式（例如電子郵件）將其傳送至信任的協力廠商CA進行簽署。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。您應該保留一份私密金鑰和CA簽署的數位憑證複本。

安裝**CA**簽署的伺服器憑證

您可以使用 `security certificate install`命令在 SVM 上安裝 CA 簽署的伺服器憑證。系統會提示您輸入憑證授權單位（CA）根憑證和中繼憑證、以構成伺服器憑證的憑證鏈結。ONTAP如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 安裝 CA 簽署的伺服器憑證：

```
security certificate install -vserver SVM_name -type certificate_type
```

> 系統會提示您輸入CA根憑證和中繼憑證、這些憑證構成伺服器憑證的憑證鏈結。ONTAP鏈結從發行伺服器憑證的CA憑證開始、範圍最多可達CA的根憑證。任何遺失的中繼憑證都會導致伺服器憑證安裝失敗。

以下命令可在 SVM 上安裝 CA 簽署的伺服器憑證和中繼憑證 `engData2`。

安裝 **CA** 簽署的伺服器憑證中繼憑證的範例

```
cluster1::>security certificate install -vserver engData2 -type
server
Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: y

Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


Do you want to continue entering root and/or intermediate
certificates {y|n}: n

You should keep a copy of the private key and the CA-signed digital
certificate for future reference.
```

相關資訊

- "產生安全性憑證-CSR"

從ONTAP 版本號《21：10.1》開始、您可以使用System Manager來管理信任的憑證授權單位、用戶端/伺服器憑證、以及本機（內建）憑證授權單位。

有了System Manager、您可以管理從其他應用程式接收到的憑證、以便驗證這些應用程式的通訊。 您也可以管理自己的憑證、以便將系統識別給其他應用程式。

檢視憑證資訊

使用System Manager、您可以檢視儲存在叢集上的信任憑證授權單位、用戶端/伺服器憑證和本機憑證授權單位。

步驟

1. 在System Manager中、選取*叢集>設定*。
2. 捲動至* Security（安全性）區域。
   在「*憑證」區段中、會顯示下列詳細資料：
   - 儲存的信任憑證授權單位數目。
   - 儲存的用戶端/伺服器憑證數目。
   - 儲存的本機憑證授權單位數目。
3. 選取任何數字以檢視有關某一類別憑證的詳細資料、或選取 → 以開啟包含所有類別資訊的 * 憑證 * 頁面。
   清單會顯示整個叢集的資訊。如果您只想顯示特定儲存VM的資訊、請執行下列步驟：
   a. 選取 * 儲存 > 儲存 VM* 。
   b. 選取儲存VM。
   c. 切換至 * 設定 * 索引標籤。
   d. 選取 * 憑證 * 區段中顯示的數字。

接下來該怎麼做

- 您可以從*憑證*頁面 [產生憑證簽署要求]。
- 憑證資訊分成三個索引標籤、每個類別各一個。 您可以從每個索引標籤執行下列工作：

在此索引標籤上…	您可以執行下列程序…
受信任的憑證授權單位	• [install-trusted-cert] • [刪除信任的憑證授權單位] • [續約信任的憑證授權單位]
用戶端/伺服器憑證	• [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]

當地證書管理機構	• [建立新的本機憑證授權單位] • [使用本機憑證授權單位簽署憑證] • [刪除本機憑證授權單位] • [更新本機憑證授權單位]

產生憑證簽署要求

您可以從「憑證」頁面的任何索引標籤、使用System Manager產生憑證簽署要求（CSR）。系統會產生私密金鑰和對應的CSR、您可以使用憑證授權單位來簽署以產生公開憑證。

步驟

1. 查看*憑證*頁面。 請參閱 [檢視憑證資訊]。
2. 選取 **+** 產生 **CSR** 。
3. 填寫主旨名稱的資訊：
   a. 輸入*通用名稱*。
   b. 選擇*國家/地區*。
   c. 輸入*組織*。
   d. 輸入*組織單位*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

安裝（新增）信任的憑證授權單位

您可以在System Manager中安裝其他信任的憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。

3. 在「新增信任的憑證授權單位」面板上、執行下列步驟：
   ◦ 輸入*名稱*。
   ◦ 對於*範圍*、請選取儲存VM。
   ◦ 輸入*通用名稱*。
   ◦ 選擇*類型*。
   ◦ 輸入或匯入*憑證詳細資料*。

刪除信任的憑證授權單位

使用System Manager、您可以刪除信任的憑證授權單位。

您無法刪除預先安裝 ONTAP 的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 名稱旁邊的，然後選取 * 刪除 * 。

續約信任的憑證授權單位

有了System Manager、您可以續約已過期或即將過期的信任憑證授權單位。

步驟

1. 檢視*信任的憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取信任的憑證授權單位名稱。
3. 選取 ⋮ 憑證名稱旁邊的 * 更新 * 。

安裝（新增）用戶端/伺服器憑證

有了System Manager、您可以安裝其他用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選擇。 + Add
3. 在「新增用戶端/伺服器憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
   - 選擇*類型*。
   - 輸入或匯入*憑證詳細資料*。
     您可以從文字檔寫入或複製及貼上憑證詳細資料、也可以按一下*匯入*從憑證檔案匯入文字。
   - 輸入 * 私密金鑰 * 。
     您可以從文字檔中寫入或複製及貼上私密金鑰、也可以按一下*匯入*從私密金鑰檔匯入文字。

產生（新增）自我簽署的用戶端/伺服器憑證

有了System Manager、您可以產生額外的自我簽署用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取 *+ 產生自我簽署的憑證 * 。
3. 在「產生自我簽署的憑證」面板上、執行下列步驟：
   - 輸入*憑證名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。

- 選擇*類型*。
- 選取*雜湊函數*。
- 選取*金鑰大小*。
- 選擇*儲存VM*。

刪除用戶端/伺服器憑證

使用System Manager、您可以刪除用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的，然後按一下 * 刪除 * 。

續約用戶端/伺服器憑證

有了System Manager、您可以續約已過期或即將過期的用戶端/伺服器憑證。

步驟

1. 檢視*用戶端/伺服器憑證*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取用戶端 / 伺服器憑證的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

建立新的本機憑證授權單位

有了System Manager、您就能建立新的本機憑證授權單位。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選擇。

3. 在「新增本機憑證授權單位」面板上、執行下列步驟：
   - 輸入*名稱*。
   - 對於*範圍*、請選取儲存VM。
   - 輸入*通用名稱*。
4. 如果您要置換預設值、請選取*更多選項*並提供其他資訊。

使用本機憑證授權單位簽署憑證

在System Manager中、您可以使用本機憑證授權單位來簽署憑證。

步驟

1. 查看*本地證書頒發機構*選項卡。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。

3. 選擇 ⋮ 名稱旁邊的，然後 * 簽署證書 * 。
4. 填寫*簽署憑證簽署要求*表單。
    - 您可以貼上憑證簽署內容、或按一下*匯入*以匯入憑證簽署要求檔案。
    - 指定憑證有效的天數。

刪除本機憑證授權單位

使用System Manager、您可以刪除本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。 請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選擇 ⋮ 名稱旁邊的 * 刪除 * 。

更新本機憑證授權單位

有了System Manager、您可以續約已過期或即將過期的本機憑證授權單位。

步驟

1. 檢視*本機憑證授權單位*索引標籤。請參閱 [檢視憑證資訊]。
2. 選取本機憑證授權單位的名稱。
3. 選取 ⋮ 名稱旁邊的、然後按一下 * 更新 * 。

在 **ONTAP** 中設定 **Active Directory** 網域控制站存取

您必須先設定AD網域控制器存取叢集或SVM、AD帳戶才能存取SVM。如果您已為資料SVM設定SMB伺服器、則可將SVM設定為閘道、或將_tunnel_設定為用於AD存取叢集的閘道。如果您尚未設定SMB伺服器、可以在AD網域上建立SVM的電腦帳戶。

支援下列網域控制器驗證服務：ONTAP

- Kerberos
- LDAP
- Netlogon
- 本機安全性授權（LSA）

支援下列工作階段金鑰演算法以確保Netlogon連線安全：ONTAP

工作階段金鑰演算法	可從 … 開始使用。

HMA-SHA256、以進階加密標準（AES）為基礎 如果您的叢集執行的是 ONTAP 9.9.1 或更早版本、而且您的網域控制器會強制執行 AES 來提供安全的 Netlogon 服務、則連線會失敗。在這種情況下、您需要重新設定網域控制器、改為接受與 ONTAP 的強大金鑰連線。	零點9.10.1 ONTAP
DE和HMC-MD5（設定強式金鑰時）	所有ONTAP 的版本

如果您想要在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰、則需要驗證 SVM 上是否已啟用 AES 。

- 從 ONTAP 9.14.1 開始、在建立 SVM 時、預設會啟用 AES 、而且您不需要修改 SVM 的安全設定、即可在 Netlogon 安全通道建立期間使用 AES 工作階段金鑰。
- 在 ONTAP 9.10.1 至 9.13.1 中、建立 SVM 時、預設會停用 AES 。您需要使用下列命令來啟用 AES ：

```
cifs security modify -vserver vs1 -aes-enabled-for-netlogon-channel true
```

當您升級至 ONTAP 9.14.1 或更新版本時、以舊版 ONTAP 建立的現有 SVM 的 AES 設定將不會自動變更。您仍需要更新此設定的值、才能在這些 SVM 上啟用 AES 。

設定驗證通道

如果您已為資料 SVM 設定 SMB 伺服器、則可以使用 `security login domain-tunnel create` 命令將 SVM 設定為閘道或 *tunnel* 、以便 AD 存取叢集。

在 ONTAP 9.16.1 之前，您必須使用驗證通道來管理具有 AD 的叢集管理員帳戶。

開始之前

- 您必須為資料SVM設定SMB伺服器。
- 您必須啟用AD網域使用者帳戶、才能存取叢集的管理SVM。
- 您必須是叢集管理員才能執行此工作。

從ONTAP 《S209.10.1》開始、如果您有SVM閘道（網域通道）可供AD存取、則如果您在AD網域中停用了NTLM、就可以使用Kerberos進行系統管理驗證。在舊版中、不支援Kerberos搭配SVM閘道的管理驗證。此功能預設為可用、不需設定。

一律會先嘗試Kerberos驗證。一旦失敗、就會嘗試執行NTLM驗證。

步驟

1. 將啟用SMB的資料SVM設定為驗證通道、以便AD網域控制器存取叢集：

```
security login domain-tunnel create -vserver <svm_name>
```

如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

SVM必須執行、使用者才能通過驗證。

下列命令會將啟用 SMB 的資料 SVM 設定 `engData`為驗證通道。

```
cluster1::>security login domain-tunnel create -vserver engData
```

在網域上建立**SVM**電腦帳戶

如果您尚未設定資料 SVM 的 SMB 伺服器、則可以使用 `vserver active-directory create` 命令、為網域上的 SVM 建立電腦帳戶。

關於這項工作

輸入之後 `vserver active-directory create` 命令時、系統會提示您提供 AD 使用者帳戶的認證、並提供足夠的權限、以便將電腦新增至網域中指定的組織單位。帳戶密碼不可空白。

從 ONTAP 9.16.1 開始，您可以使用此程序來管理具有 AD 的叢集管理員帳戶。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在AD網域上建立SVM的電腦帳戶：

```
vserver active-directory create -vserver <SVM_name> -account-name
<NetBIOS_account_name> -domain <domain> -ou <organizational_unit>
```

從 ONTAP 9.16.1 開始，此 `-vserver`參數會接受管理 SVM 。如"指令參考資料ONTAP"需詳細 `vserver active-directory create`資訊，請參閱。

以下命令將在 SVM 的域上 `example.com`創建一個名爲的 `engData`計算機帳戶 `ADSERVER1`。輸入命令後、系統會提示您輸入AD使用者帳戶認證。

```
cluster1::>vserver active-directory create -vserver engData -account
-name ADSERVER1 -domain example.com

In order to create an Active Directory machine account, you must supply
the name and password of a Windows account with sufficient privileges to
add computers to the "CN=Computers" container within the "example.com"
domain.

Enter the user name: Administrator

Enter the password:
```

在 **ONTAP** 中設定 **LDAP** 或 **NIS** 伺服器存取

您必須先設定LDAP或NIS伺服器存取SVM、LDAP或NIS帳戶才能存取SVM。交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。

設定**LDAP**伺服器存取

您必須先設定LDAP伺服器存取SVM、LDAP帳戶才能存取SVM。您可以使用 `vserver services name-service ldap client create` 在 SVM 上建立 LDAP 用戶端組態的命令。然後您就可以使用 `vserver services name-service ldap create` 用於將 LDAP 用戶端組態與 SVM 建立關聯的命令。

關於這項工作

大多數LDAP伺服器都可以使用ONTAP 由下列功能提供的預設架構：

- ms-AD-BIS（大多數Windows 2012及更新版本AD伺服器的偏好架構）
- AD-IDMU （ Windows 2008 、 Windows 2016 及更新版本的 AD 伺服器）
- AD-SFU（Windows 2003和舊版AD伺服器）
- RFC-2307（UNIX LDAP伺服器）

除非有其他需求、否則最好使用預設架構。如果是、您可以複製預設架構並修改複本、以建立自己的架構。如需詳細資訊、請參閱：

- "NFS 組態"
- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"

開始之前

- 您必須已在 SVM 上安裝"CA簽署的伺服器數位憑證"。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 LDAP 用戶端組態：

   ```
   vserver services name-service ldap client create -vserver <SVM_name> -client
   -config <client_configuration> -servers <LDAP_server_IPs> -schema <schema>
   -use-start-tls <true|false>
   ```

   只有資料SVM存取才支援Start TLS。不支援存取管理SVM。

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap client create`資訊，請參閱。

   以下命令用於創建名爲 SVM `engData` 的 LDAP 客戶端配置 `corp`。用戶端會匿名連結至 IP 位址為 172.0.0.100 和 172.16.0.101 的 LDAP 伺服器。用戶端使用 RFC-2307 架構進行 LDAP 查詢。用戶端與伺服器之間的通訊會使用Start TLS加密。

```
cluster1::> vserver services name-service ldap client create
-vserver engData -client-config corp -servers 172.16.0.100,172.16.0.101
-schema RFC-2307 -use-start-tls true
```

這 `-ldap-servers`字段替換 `-servers`字段。您可以使用 `-ldap-servers`欄位指定 LDAP 伺服器的主機名稱或 IP 位址。

2. 將 LDAP 用戶端組態與 SVM 建立關聯： `vserver services name-service ldap create -vserver <SVM_name> -client-config <client_configuration> -client-enabled <true|false>`

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ldap create`資訊，請參閱。

   下列命令會關聯 LDAP 用戶端組態 `corp` 使用 SVM `engData`，並在 SVM 上啟用 LDAP 用戶端。

```
cluster1::>vserver services name-service ldap create -vserver engData
-client-config corp -client-enabled true
```

這 `vserver services name-service ldap create`如果ONTAP無法聯繫名稱伺服器，則該命令將執行自動設定驗證並報告錯誤訊息。

3. 使用vserver services name-service LDAP檢查命令來驗證名稱伺服器的狀態。

   下列命令會驗證SVM vs0上的LDAP伺服器。

```
cluster1::> vserver services name-service ldap check -vserver vs0

| Vserver: vs0                                                  |
| Client Configuration Name: c1                                 |
| LDAP Status: up                                               |
| LDAP Status Details: Successfully connected to LDAP server
"10.11.12.13".                                                |
```

   您可以使用 `name service check``命令來驗證名稱伺服器的狀態。

設定 **NIS** 伺服器存取

您必須先設定NIS伺服器對SVM的存取權、NIS帳戶才能存取SVM。您可以使用 `vserver services name-service nis-domain create` 在 SVM 上建立 NIS 網域組態的命令。

開始之前

- 在SVM上設定NIS網域之前、所有已設定的伺服器都必須可供使用和存取。
- 您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 在 SVM 上建立 NIS 網域組態：

   ```
   vserver services name-service nis-domain create -vserver <SVM_name> -domain
   <client_configuration> -nis-servers <NIS_server_IPs>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service nis-domain create`資訊，請參閱。

   這 `-nis-servers`字段替換 `-servers`字段。您可以使用 `-nis-servers`欄位指定 NIS 伺服器的主機名稱或 IP 位址。

   以下命令在 SVM 上創建 NIS 域配置 `engData`。NIS 網域 `nisdomain`會與 `IP` 位址為的 `NIS` 伺服器進行通訊 `192.0.2.180`。

   ```
   cluster1::>vserver services name-service nis-domain create
   -vserver engData -domain nisdomain -nis-servers 192.0.2.180
   ```

建立名稱服務交換器

名稱服務交換器功能可讓您使用LDAP或NIS做為替代名稱服務來源。您可以使用 `vserver services name-service ns-switch modify` 命令以指定名稱服務來源的查詢順序。

開始之前

- 您必須已設定LDAP和NIS伺服器存取。
- 您必須是叢集管理員或SVM管理員、才能執行此工作。

步驟

1. 指定名稱服務來源的查詢順序：

   ```
   vserver services name-service ns-switch modify -vserver <SVM_name> -database
   <name_service_switch_database> -sources <name_service_source_order>
   ```

   如"指令參考資料ONTAP"需詳細 `vserver services name-service ns-switch modify`資訊，請參閱。

   以下命令指定 SVM 上資料庫 `engData`的 `LDAP` 和 `NIS` 名稱服務來源的查詢順序 `passwd`。

   ```
   cluster1::>vserver services name-service ns-switch
   modify -vserver engData -database passwd -source files ldap,nis
   ```

變更 **ONTAP** 管理員密碼

首次登入系統後、您應該立即變更初始密碼。如果您是 SVM 管理員、可以使用 `security login password` 命令以變更您自己的密碼。如果您是叢集管理員、可以使用 `security login password` 命令以變更任何系統管理員的密碼。

關於這項工作

新密碼必須遵守下列規則：

- 它不能包含使用者名稱
- 長度必須至少八個字元
- 它必須包含至少一個字母和一個數字
- 不能與最後六個密碼相同

您可以使用 `security login role config modify`命令來修改與指定角色相關聯之帳戶的密碼規則。

開始之前

- 您必須是叢集或SVM管理員、才能變更自己的密碼。
- 您必須是叢集管理員、才能變更其他管理員的密碼。

步驟

1. 變更管理員密碼： `security login password -vserver svm_name -username user_name`

   下列命令會變更系統管理員的密碼 `admin1` 適用於 SVM`vs1.example.com`。系統會提示您輸入目前密碼、然後輸入並重新輸入新密碼。

```
vs1.example.com::>security login password -vserver engData -username
admin1
Please enter your current password:
Please enter a new password:
Please enter it again:
```

相關資訊

- "安全登入角色組態修改"
- "安全登入密碼"

鎖定及解除鎖定 **ONTAP** 系統管理員帳戶

您可以使用 `security login lock` 用於鎖定系統管理員帳戶的命令、以及 `security login unlock` 解除鎖定帳戶的命令。

開始之前

您必須是叢集管理員才能執行這些工作。

步驟

1. 鎖定系統管理員帳戶：

   ```
   security login lock -vserver SVM_name -username user_name
   ```

   下列命令會鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

```
cluster1::>security login lock -vserver engData -username admin1
```

如"指令參考資料ONTAP"需詳細 `security login lock`資訊，請參閱。

2. 解除鎖定系統管理員帳戶：

   `security login unlock -vserver SVM_name -username user_name`

   下列命令會解除鎖定系統管理員帳戶 `admin1` 適用於 SVM `vs1.example.com`：

```
cluster1::>security login unlock -vserver engData -username admin1
```

如"指令參考資料ONTAP"需詳細 `security login unlock`資訊，請參閱。

相關資訊

- "安全登入"

在 **ONTAP** 中管理失敗的登入嘗試

重複失敗的登入嘗試有時表示入侵者正在嘗試存取儲存系統。您可以採取許多步驟來確保不會發生入侵。

如何得知登入嘗試失敗

事件管理系統（EMS）每小時都會通知您登入失敗的嘗試。您可以在中找到登入嘗試失敗的記錄 `audit.log` 檔案：

重複登入嘗試失敗時該怎麼辦

從短期來看、您可以採取許多步驟來預防入侵：

- 密碼必須由最少的大寫字元、小寫字元、特殊字元和/或數字組成
- 在登入嘗試失敗後強制延遲
- 限制允許的失敗登入嘗試次數、並在指定的失敗嘗試次數後鎖定使用者
- 過期並封鎖在指定天數內處於非使用中狀態的帳戶

您可以使用 `security login role config modify`命令來執行這些工作。如"指令參考資料ONTAP"需詳細 `security login role config modify`資訊，請參閱。

長期而言、您可以採取下列額外步驟：

- 使用 `security ssh modify`命令可限制所有新建立的 SVM 失敗登入嘗試次數。如"指令參考資料ONTAP"需詳細 `security ssh modify`資訊，請參閱。
- 要求使用者變更密碼、將現有的MD5-演算 法帳戶移轉至更安全的SHA-512演算法。

對 ONTAP 系統管理員帳戶密碼強制執行 SHA-2

在升級之後、ONTAP 在更新之前建立的管理員帳戶會繼續使用md5密碼、直到手動變更密碼為止。與SHA-2相比、MD5的安全性較低。因此、在升級之後、您應該提示使用者將密碼變更為使用預設的SHA-512雜湊功能。

關於這項工作

密碼雜湊功能可讓您執行下列動作：

- 顯示符合指定雜湊功能的使用者帳戶。
- 使使用指定雜湊功能的帳戶過期（例如、md5）、強制使用者在下次登入時變更密碼。
- 鎖定密碼使用指定雜湊功能的帳戶。
- 還原至ONTAP 版本早於發揮作用9的版本時、請重設叢集管理員自己的密碼、使其與舊版支援的雜湊功能（md5）相容。

ONTAP 只接受預先散列的 SHA-2 密碼、只能使用 NetApp Manageability SDK (`security-login-create` 和 `security-login-modify-password`) 。

步驟

1. 將md5系統管理員帳戶移轉至SHA-512密碼雜湊功能：
   a. 使所有 MD5 系統管理員帳戶過期： `security login expire-password -vserver * -username * -hash-function md5`

      如此一來、會強制md5帳戶使用者在下次登入時變更密碼。

   b. 要求具有MD5帳戶的使用者透過主控台或SSH工作階段登入。

      系統偵測到帳戶已過期、並提示使用者變更密碼。SHA-512預設用於變更的密碼。

2. 若使用者未在一段時間內登入以變更密碼的MD5帳戶、請強制進行帳戶移轉：
   a. 鎖定仍使用 MD5 雜湊功能的帳戶（進階權限層級）： `security login expire-password -vserver * -username * -hash-function md5 -lock-after integer`

      在指定的天數之後 `-lock-after`、使用者無法存取其 MD5 帳戶。

   b. 當使用者準備好變更密碼時、請解除鎖定帳戶： `security login unlock -vserver svm_name -username user_name`
   c. 請使用者透過主控台或SSH工作階段登入帳戶、並在系統提示使用者時變更密碼。

相關資訊

- "安全登入過期密碼"
- "安全登入解除鎖定"

使用系統管理員診斷並修正 ONTAP 檔案存取問題

從功能不全的9.8開始ONTAP 、您可以追蹤及檢視檔案存取問題。

步驟

1. 在System Manager中、選取* Storage > Storage VM*。
2. 選取您要在其中執行追蹤的儲存VM。
3. 按一下 * 更多 * 。
4. 按一下*追蹤檔案存取*。
5. 提供使用者名稱和用戶端IP位址、然後按一下*開始追蹤*。

   追蹤結果會顯示在表格中。 「理由」欄提供無法存取檔案的原因。

6. 按一下 結果表左欄、即可檢視檔案存取權限。

管理多管理員驗證

瞭解 **ONTAP** 多管理驗證

從 ONTAP 9.11.1 開始，您可以使用多管理驗證（ MAV ）來確保某些作業（例如刪除磁碟區或快照）只能在指定管理員核准後執行。如此可防止遭到入侵、惡意或缺乏經驗的系統管理員進行不必要的變更或刪除資料。

設定多管理員驗證包括：

- "建立一個或多個系統管理員核准群組。"
- "啟用多管理員驗證功能。"
- "新增或修改規則。"

初始設定之後、這些元素只能由MAV核准群組（MAV系統管理員）中的系統管理員修改。

啟用多重管理驗證時、完成每項受保護的作業都需要下列步驟：

1. 當使用者啟動作業時 "已產生要求。"
2. 在執行作業之前，請至少先執行一個"MAV管理員必須核准。"
3. 核准後，系統會提示使用者並完成作業。

如果您需要在未經 MAV 管理員批准的情況下停用多管理員驗證功能，請聯絡NetApp支援並提及以下內容"NetApp知識庫：如果 MAV 管理員不可用，如何停用多管理員驗證"。

多管理員驗證不適用於涉及大量自動化的磁碟區或工作流程、因為每項自動化工作都需要核准才能完成作業。如果您想要同時使用自動化和 MAV ，建議您針對特定的 MAV 作業使用查詢。例如，您只能將 MAV 規則套用 `volume delete`至不涉及自動化的磁碟區，而且可以使用特定的命名方案來指定這些磁碟區。

Cloud Volumes ONTAP 無法使用多重管理驗證。

多管理員驗證的運作方式

多管理員驗證包括：

- 一或多位系統管理員的群組、擁有核准和否決的權限。
- _規則表_中的一組受保護作業或命令。
- _規則engine _以識別及控制受保護作業的執行。

根據角色型存取控制（RBAC）規則、評估MAV規則。因此、執行或核准受保護作業的系統管理員必須已擁有這些作業的最低RBAC權限。 "深入瞭解RBAC"。

系統定義的規則

啟用多管理員驗證時、系統定義的規則（也稱為_guard rail _規則）會建立一組MAV作業、以控制規避MAV程序本身的風險。這些作業無法從規則表格中移除。啟用MAV之後、以星號（）指定的作業在執行之前、必須先經過一或多位管理員的核准、 show*命令除外。

- `security multi-admin-verify modify` 營運 *

  控制多管理員驗證功能的組態。

- `security multi-admin-verify approval-group` 營運 *

  以多管理員驗證認證身分證明來控制系統管理員群組的成員資格。

- `security multi-admin-verify rule` 營運 *

  控制需要多管理員驗證的命令集。

- `security multi-admin-verify request` 營運

  控制核准程序。

受規則保護的命令

除了系統定義的操作外，啟用多管理員驗證時，以下命令預設受到保護，但您可以修改規則以刪除對這些命令的保護：

- "安全登入密碼"
- "安全登入解除鎖定"
- "設定"

每個 ONTAP 版本都提供更多命令、讓您可以選擇使用多重管理驗證規則來保護這些命令。請選擇您的 ONTAP 版本、以取得可保護的命令完整清單。

9.17.1

- `cluster date modify` [3]
- `cluster log-forwarding create` [3]
- `cluster log-forwarding delete` [3]
- `cluster log-forwarding modify` [3]
- `cluster peer delete`
- `cluster time-service ntp server create` [3]
- `cluster time-service ntp server delete` [3]
- `cluster time-service ntp key create`[3]
- `cluster time-service ntp key delete`[3]
- `cluster time-service ntp key modify`[3]
- `cluster time-service ntp server modify` [3]
- `event config modify`
- `event config set-mail-server-password` [3]
- `lun delete` [3]
- `security anti-ransomware volume attack clear-suspect` [1]
- `security anti-ransomware volume disable` [1]
- `security anti-ransomware volume event-log modify`[2]
- `security anti-ransomware volume pause` [1]
- `security anti-ransomware vserver event-log modify`[2]
- `security audit modify` [3]
- `security ipsec config modify` [3]
- `security ipsec policy create` [3]
- `security ipsec policy delete` [3]
- `security ipsec policy modify` [3]
- `security login create`
- `security login delete`
- `security login modify`
- `security login publickey create`
- `security login publickey delete`
- `security login publickey modify`
- `security key-manager onboard update-passphrase`[3]
- `security saml-sp create` [3]

- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete[4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline[4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start[4]
- volume encryption rekey start[4]

- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume rename [5]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]

- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create[4]
- vserver object-store-server bucket cors-rule delete[4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop[4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.16.1.

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create[3]
- cluster time-service ntp key delete[3]
- cluster time-service ntp key modify[3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]

- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- security webauthn credentials delete[4]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage aggregate offline[4]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]

- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume encryption conversion start [4]
- volume encryption rekey start [4]
- volume file privileged-delete [3]
- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver consistency-group create[4]
- vserver consistency-group delete[4]
- vserver consistency-group modify[4]
- vserver consistency-group snapshot create[4]
- vserver consistency-group snapshot delete[4]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver object-store-server bucket cors-rule create[4]
- vserver object-store-server bucket cors-rule delete[4]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]
- vserver security file-directory remove-slag [3]
- vserver stop[4]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]

- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.15.1..

- cluster date modify [3]
- cluster log-forwarding create [3]
- cluster log-forwarding delete [3]
- cluster log-forwarding modify [3]
- cluster peer delete
- cluster time-service ntp server create [3]
- cluster time-service ntp server delete [3]
- cluster time-service ntp key create[3]
- cluster time-service ntp key delete[3]
- cluster time-service ntp key modify[3]
- cluster time-service ntp server modify [3]
- event config modify
- event config set-mail-server-password [3]
- lun delete [3]
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security audit modify [3]
- security ipsec config modify [3]
- security ipsec policy create [3]
- security ipsec policy delete [3]
- security ipsec policy modify [3]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete

- security login publickey modify
- security key-manager onboard update-passphrase[3]
- security saml-sp create [3]
- security saml-sp delete [3]
- security saml-sp modify [3]
- snaplock legal-hold end [3]
- storage aggregate delete [3]
- storage encryption disk destroy [3]
- storage encryption disk modify [3]
- storage encryption disk revert-to-original-state [3]
- storage encryption disk sanitize [3]
- system bridge run-cli [3]
- system controller flash-cache secure-erase run [3]
- system controller service-event delete [3]
- system health alert delete [3]
- system health alert modify [3]
- system health policy definition modify [3]
- system node autosupport modify [3]
- system node autosupport trigger modify [3]
- system node coredump delete [3]
- system node coredump delete-all [3]
- system node hardware nvram-encryption modify [3]
- system node run
- system node systemshell
- system script delete [3]
- system service-processor ssh add-allowed-addresses [3]
- system service-processor ssh remove-allowed-addresses [3]
- system smtape restore [3]
- system switch ethernet log disable-collection [3]
- system switch ethernet log modify [3]
- timezone [3]
- volume create [3]
- volume delete
- volume file privileged-delete [3]

- volume flexcache delete
- volume modify [3]
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot create [3]
- volume snapshot delete
- volume snapshot modify [3]
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot rename [3]
- volume snapshot restore
- vserver audit create [3]
- vserver audit delete [3]
- vserver audit disable [3]
- vserver audit modify [3]
- vserver audit rotate-log [3]
- vserver create[2]
- vserver delete [3]
- vserver modify [2]
- vserver object-store-server audit create [3]
- vserver object-store-server audit delete [3]
- vserver object-store-server audit disable [3]
- vserver object-store-server audit modify [3]
- vserver object-store-server audit rotate-log [3]
- vserver options [3]
- vserver peer delete
- vserver security file-directory apply [3]

- vserver security file-directory remove-slag [3]
- vserver vscan disable [3]
- vserver vscan on-access-policy create [3]
- vserver vscan on-access-policy delete [3]
- vserver vscan on-access-policy disable [3]
- vserver vscan on-access-policy modify [3]
- vserver vscan scanner-pool create [3]
- vserver vscan scanner-pool delete [3]
- vserver vscan scanner-pool modify [3]

9.14.1.

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect [1]
- security anti-ransomware volume disable [1]
- security anti-ransomware volume event-log modify[2]
- security anti-ransomware volume pause [1]
- security anti-ransomware vserver event-log modify[2]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume recovery-queue modify [2]
- volume recovery-queue purge [2]
- volume recovery-queue purge-all [2]
- volume snaplock modify [1]
- volume snapshot autodelete modify
- volume snapshot delete

- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver create[2]
- vserver modify[2]
- vserver peer delete

9.13.1.12.9.12.9.

- cluster peer delete
- event config modify
- security anti-ransomware volume attack clear-suspect[1]
- security anti-ransomware volume disable[1]
- security anti-ransomware volume pause[1]
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snaplock modify[1]
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify

- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

9.12.1/9.11.1

- cluster peer delete
- event config modify
- security login create
- security login delete
- security login modify
- security login publickey create
- security login publickey delete
- security login publickey modify
- system node run
- system node systemshell
- volume delete
- volume flexcache delete
- volume snapshot autodelete modify
- volume snapshot delete
- volume snapshot policy add-schedule
- volume snapshot policy create
- volume snapshot policy delete *
- volume snapshot policy modify
- volume snapshot policy modify-schedule
- volume snapshot policy remove-schedule
- volume snapshot restore
- vserver peer delete

1. 9.13.1 全新的規則保護命令
2. 適用於 9.14.1 的全新規則保護命令
3. 9.15.1 的新規則保護命令
4. 9.16.1 的新規則保護命令
5. 9.17.1 的新規則保護命令
    - 此命令僅適用於 CLI ，在某些版本中不適用於 System Manager 。

只要在受MAV保護的叢集上輸入受保護的作業、就會將作業執行要求傳送至指定的MAV系統管理員群組。

您可以設定：

- MAV群組中的系統管理員名稱、聯絡資訊和數量。

  MAV管理員應具備具備叢集管理員權限的RBAC角色。

- MAV系統管理員群組的數目。
  - 每個受保護的作業規則都會指派一個MAV群組。
  - 對於多個MAV群組、您可以設定哪個MAV群組核准特定規則。
- 執行受保護作業所需的MAV核准數。
- MAV管理員必須在_核准到期_期間內回應核准要求。
- 執行過期_期間、要求的系統管理員必須在此期間內完成作業。

設定這些參數後、必須取得MAV核准才能加以修改。

MAV系統管理員無法核准自己執行受保護作業的要求。因此：

- 不應在只有一位系統管理員的叢集上啟用MAV。
- 如果 MAV 群組中只有一個人、則 MAV 管理員無法啟動受保護的作業；一般管理員必須啟動受保護的作業、且 MAV 管理員只能核准。
- 如果您想讓MAV管理員能夠執行受保護的作業、則MAV管理員人數必須大於所需的核准人數。
  例如、如果受保護的作業需要兩次核准、而您希望MAV系統管理員執行這些核准、則MAV系統管理員群組中必須有三位人員。

MAV系統管理員可以接收電子郵件警示中的核准要求（使用EMS）、也可以查詢要求佇列。 當他們收到要求時、可以採取下列三種行動之一：

- 核准
- 拒絕（否決）
- 忽略（無行動）

在下列情況下、電子郵件通知會傳送給與MAV規則相關的所有核准者：

- 隨即建立要求。
- 申請已核准或遭否決。
- 系統會執行核准的申請。

如果申請者在該作業的同一個核准群組中、他們會在申請獲得核准時收到一封電子郵件。

申請者即使在核准群組中，也無法核准自己的申請（雖然他們可以針對自己的申請取得電子郵件通知）。不在核准群組中的申請者（即非MAV系統管理員）不會收到電子郵件通知。

受保護的作業執行方式

如果已核准執行受保護的作業、則要求的使用者會在收到提示時繼續執行該作業。如果作業遭否決、申請使用者必須先刪除申請、然後再繼續。

MAV規則會在RBAC權限之後評估。因此、沒有足夠RBAC權限執行作業的使用者無法啟動MAV要求程序。

在執行受保護的操作之前，MAV 規則會被評估。這意味著規則會根據系統的目前狀態執行。例如，如果為以下物件建立了 MAV 規則： `volume modify`查詢 `-size 5GB` ，使用 `volume modify`將 5GB 磁碟區大小調整為 2GB 需要 MAV 批准，但將 2GB 磁碟區大小調整為 5GB 則不需要。

相關資訊

- "叢集"
- "LUN"
- "安全性"
- "終止合法持有SnapLock"
- "儲存聚合"
- "儲存加密"
- "系統"

管理 **MAV** 的 **ONTAP** 管理員核准群組

在啟用多管理員驗證（MAV）之前、您必須先建立管理員核准群組、其中包含一或多位系統管理員、以便獲得核准或否決權限。啟用多管理員驗證之後、任何對核准群組成員資格的修改都必須取得現有合格管理員的核准。

關於這項工作

您可以將現有的系統管理員新增至MAV群組、或建立新的系統管理員。

MAV功能可執行現有的角色型存取控制（RBAC）設定。潛在的MAV系統管理員必須擁有足夠的權限、才能執行受保護的作業、才能將其新增至MAV系統管理員群組。 "深入瞭解RBAC。"

您可以設定MAV來警示MAV系統管理員核准要求已擱置。若要這麼做、您必須設定電子郵件通知、尤其是 `Mail From` 和 `Mail Server` 參數 — 或者您可以清除這些參數以停用通知。沒有電子郵件警示、MAV管理員必須手動檢查核准佇列。

從ONTAP 9.15.1 開始，您可以將 Active Directory (AD) 使用者設定為 MAV 管理員。 AD 使用者必須是"配置為ONTAP管理員"。

System Manager程序

如果您想第一次建立MAV核准群組、請參閱的系統管理員程序 "啟用多管理員驗證。"

若要修改現有的核准群組或建立其他核准群組：

1. 識別要接收多管理員驗證的系統管理員。
   a. 按一下*叢集>設定。*

b. 按一下 → * 使用者和角色旁邊的。 *

c. 按一下 + Add * 使用者 * 。 *

d. 視需要修改名單。

如需詳細資訊、請參閱 "控制系統管理員存取權。"

2. 建立或修改MAV核准群組：

a. 按一下*叢集>設定。*

b. 按一下 → * 安全性 * 區段中 * 多重管理核准 * 旁的。（如果尚未設定 MAV 、您會看到 ⚙ 圖示。）

- 名稱：輸入群組名稱。
- 核准者：從使用者清單中選取核准者。
- 電子郵件地址：輸入電子郵件地址。
- 預設群組：選取群組。

啟用MAV後、必須取得MAV核准才能編輯現有的組態。

CLI程序

1. 確認已為設定值 `Mail From` 和 `Mail Server` 參數。輸入：

```
event config show
```

顯示器應類似於下列內容：

```
cluster01::> event config show
                            Mail From:  admin@localhost
                          Mail Server:  localhost
                            Proxy URL:  -
                           Proxy User:  -
 Publish/Subscribe Messaging Enabled:  true
```

若要設定這些參數、請輸入：

```
event config modify -mail-from email_address -mail-server server_name
```

深入瞭解 `event config show`及 `event config modify` "指令參考資料ONTAP"。

2. 識別要接收多管理員驗證的系統管理員

如果您想...	輸入此命令
顯示目前的系統管理員	`security login show`
修改目前系統管理員的認證資料	`security login modify <parameters>`

如果您想...	輸入此命令
建立新的系統管理員帳戶	`security login create -user-or-group -name admin_name -application ssh -authentication-method password`

深入瞭解 `security login show`，`security login modify`和 `security login create` "指令參考資料ONTAP"。

3. 建立MAV核准群組：

   `security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1[,approver2…] [[-email address1], address1…]`

   - `-vserver` - 此版本僅支援管理 SVM 。
   - `-name` - MAV 群組名稱、最多 64 個字元。
   - `-approvers`- 一個或多個審核者的清單。對於 AD 用戶，使用格式 `domain\user`。例如，`mydomain\pavan` 。
   - `-email` ：一或多個電子郵件地址、在建立、核准、遭否決或執行要求時收到通知。

     *範例：*下列命令會建立一個MAV群組、其中包含兩個成員及相關的電子郵件地址。

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. 驗證群組建立與成員資格：

   `security multi-admin-verify approval-group show`

   範例：

```
cluster-1::> security multi-admin-verify approval-group show
Vserver  Name        Approvers        Email
-------  ----------------- ------------------
------------------------------------------------------------
svm-1    mav-grp1   pavan,julia      email
pavan@myfirm.com,julia@myfirm.com
```

使用這些命令來修改初始MAV群組組態。

*附註：*所有項目都需要MAV系統管理員核准才能執行。

如果您想...	輸入此命令
修改群組特性或修改現有的成員資訊	`security multi-admin-verify approval-group modify [parameters]`
新增或移除成員	`security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2…]][-approvers-to-remove approver1[,approver2…]]`
刪除群組	`security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name`

相關資訊

- "安全多管理員驗證"

在 **ONTAP** 中啟用或停用多管理驗證

必須明確啟用多管理員驗證（MAV）。啟用多管理員驗證後、必須取得MAV核准群組（MAV系統管理員）的系統管理員核准、才能將其刪除。

關於這項工作

啟用MAV之後、修改或停用MAV需要MAV管理員核准。

如果您需要在未經 MAV 管理員批准的情況下停用多管理員驗證功能，請聯絡NetApp支援並提及以下內容"NetApp知識庫：如果 MAV 管理員不可用，如何停用多管理員驗證"。

啟用MAV時、您可以全域指定下列參數。

核准群組

全域核准群組清單。至少需要一個群組才能啟用MAV功能。

如果您使用 MAV 搭配自主勒索軟體保護（ ARP ）、請定義一個新的或現有的核准群組、負責核准 ARP 暫停、停用及清除可疑的要求。

必要的核准者

執行受保護作業所需的核准者數量。預設和最小數字為1。

必要的核准者數量必須小於預設核准群組中唯一核准者的總數。

核准過期（小時、分鐘、秒）

MAV管理員必須回應核准要求的期間。預設值為1小時（1小時）、支援的最小值為1秒、支援的最大值為14天（14d）。

執行過期（小時、分鐘、秒）

要求系統管理員必須完成以下作業的期間：預設值為1小時（1小時）、支援的最小值為1秒、支援的最大值為14天（14d）。

您也可以針對特定項目覆寫任何這些參數 "營運規則。"

System Manager程序

1. 識別要接收多管理員驗證的系統管理員。
   a. 按一下*叢集>設定。*
   b. 按一下 → * 使用者和角色旁邊的。 *
   c. 按一下 + Add * 使用者 * 。 *
   d. 視需要修改名單。

      如需詳細資訊、請參閱 "控制系統管理員存取權。"

2. 建立至少一個核准群組並新增至少一個規則、以啟用多管理員驗證。
   a. 按一下*叢集>設定。*
   b. 按一下 ⚙ * 安全性 * 區段中 * 多重管理核准 * 旁的。
   c. 按一下 + Add 以新增至少一個核准群組。
      - 名稱–輸入群組名稱。
      - 核准者：從使用者清單中選取核准者。
      - 電子郵件地址–輸入電子郵件地址。
      - 預設群組–選取群組。
   d. 至少新增一個規則。
      - 作業–從清單中選取支援的命令。
      - 查詢–輸入任何所需的命令選項和值。
      - 選用參數；保留空白以套用全域設定、或為特定規則指派不同的值以覆寫全域設定。
        - 必要的核准人數
        - 核准群組
   e. 按一下*進階設定*以檢視或修改預設值。
      - 必要的核准人數（預設：1）
      - 執行要求過期（預設：1小時）
      - 核准要求過期（預設：1小時）
      - 郵件伺服器*
      - 寄件者電子郵件地址*

        *這些更新在「通知管理」下管理的電子郵件設定。如果尚未設定、系統會提示您進行設定。
   f. 按一下「啟用」以完成MAV初始組態。

初始組態之後、目前的MAV狀態會顯示在*多管理員核准*方塊中。

- 狀態（已啟用或未啟用）
- 需要核准的作用中作業
- 處於擱置狀態的未處理要求數

您可以按一下以顯示現有的組態 → 。需要MAV核准才能編輯現有的組態。

若要停用多管理員驗證：

1. 按一下*叢集>設定。*
2. 按一下 ⚙ * 安全性 * 區段中 * 多重管理核准 * 旁的。
3. 按一下「已啟用」切換按鈕。

   必須取得MAV核准才能完成此作業。

CLI程序

在CLI中啟用MAV功能之前、請先至少啟用一項 "MAV系統管理員群組" 必須已建立。

如果您想...	輸入此命令

啟用MAV功能	`security multi-admin-verify modify -approval-groups group1[,group2…] [-required-approvers nn ] -enabled true [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`
	
	範例：下列命令可啟用具有1個核准群組、2個必要核准者及預設到期期間的MAV。
	
	`cluster-1::> security multi-admin-verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true`
	
	至少新增一組、以完成初始組態 "營運規則："

修改MAV組態（需要MAV核准）	`security multi-admin-verify approval-group modify [-approval-groups group1[,group2…]] [-required-approvers nn ] [-execution-expiry [nnh][nnm][nns]] [-approval-expiry [nnh][nnm][nns]]`

如果您想...	輸入此命令

驗證MAV功能	`security multi-admin-verify show`
	
	範例：
	
	`cluster-1::> security multi-admin-verify show`
	`Is Required Execution`
	`Approval Approval`
	`Enabled Approvers Expiry Expiry`
	`Groups`
	`------- --------- ---------`
	`-------- ----------`
	`true 2 1h 1h`
	`mav-grp1`

停用MAV功能（需要MAV核准）	`security multi-admin-verify modify -enabled false`

相關資訊

- "安全多管理員驗證"

管理 **ONTAP** 中受保護作業的多重管理驗證規則

您可以建立多管理員驗證（MAV）規則、以指定需要核准的作業。只要啟動作業、就會攔截受保護的作業、並產生核准要求。

任何具備適當RBAC功能的系統管理員都可以在啟用MAV之前建立規則、但一旦啟用MAV、對規則集的任何修改都需要MAV核准。

每個作業只能建立一個 MAV 規則、例如、您無法建立多個 `volume-snapshot-delete` 規則。任何所需的規則限制都必須包含在單一規則中。

您可以建立規則來保護 "這些命令"。您可以從 ONTAP 版本開始保護每個命令、在此版本中、命令的保護功能會先開始提供。

MAV 系統預設命令的規則 `security multi-admin-verify` "命令"、不可變更。

除了系統定義的操作外，啟用多管理員驗證時，以下命令預設受到保護，但您可以修改規則以刪除對這些命令的保護：

- "安全登入密碼"
- "安全登入解除鎖定"
- "設定"

規則限制

建立規則時，您可以選擇性地指定 `-query`選項，將要求限制為命令功能的子集。此 `-query`選項也可用於限制組態元素，例如 SVM ， Volume 和 Snapshot 名稱。

例如，在命令 `-query`中 `volume snapshot delete`，可以設定為 `-snapshot !hourly*,!daily*,!weekly*`，表示以每小時，每天或每週屬性為前置的 Volume 快照不受 MAV 保護。

```
smci-vsim20::> security multi-admin-verify rule show
                                                 Required  Approval
Vserver Operation                                Approvers Groups
------- ---------------------------------------- --------- -------------
vs01    volume snapshot delete                   -         -
          Query: -snapshot !hourly*,!daily*,!weekly*
```

任何排除的組態元素都不會受到 MAV 保護、任何管理員都可以刪除或重新命名。

根據預設，規則會指定在輸入受保護的作業時自動產生對應的 `security multi-admin-verify request create *"protected_operation"*`命令。您可以修改此預設值，要求 `request create`分別輸入命令。

根據預設、規則會繼承下列全域MAV設定、不過您可以指定規則特定的例外狀況：

- 所需核准者人數
- 核准群組
- 核准到期日
- 執行到期期間

System Manager程序

如果您想要第一次新增受保護的作業規則、請參閱的系統管理員程序 "啟用多管理員驗證。"

若要修改現有的規則集：

1. 選擇*叢集>設定*。
2. 在 * 安全性 * 區段中、選取 * 多重管理核准 * 旁的。
3. 選取 Add 以新增至少一個規則；您也可以修改或刪除現有規則。
   - 作業–從清單中選取支援的命令。
   - 查詢–輸入任何所需的命令選項和值。
   - 選用參數–保留空白以套用全域設定、或為特定規則指派不同的值以覆寫全域設定。
     - 必要的核准人數
     - 核准群組

CLI程序

全部 `security multi-admin-verify rule` 命令必須先獲得 MAV 管理員核准、才能執行 `security multi-admin-verify rule show`。

如果您想...	輸入此命令
建立規則	`security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]`

修改目前系統管理員的認證資料	`security login modify <parameters>`
	
	範例：下列規則需要核准才能刪除根Volume。
	
	`security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"`

修改規則	`security multi-admin-verify rule modify -operation "protected_operation" [parameters]`
刪除規則	`security multi-admin-verify rule delete -operation "protected_operation"`
顯示規則	`security multi-admin-verify rule show`

相關資訊

- "安全多管理員驗證規則"
- "修改安全登入"

要求在 **ONTAP** 中執行受 **MAV** 保護的作業

當您在啟用多管理員驗證（MAV）的叢集上啟動受保護的作業或命令時ONTAP 、多方面的操作或命令都會自動攔截、並要求產生要求、而該要求必須獲得一或多位MAV核准群組（MAV系統管理員）中的系統管理員核准。或者、您也可以建立不含對話方塊的MAV要求。

如果核准、您必須回應查詢、才能在申請到期期間內完成作業。如果被否決、或是超過申請或過期期間、您必須刪除申請並重新提交。

MAV功能會遵守現有的RBAC設定。也就是您的系統管理員角色必須擁有足夠的權限、才能在不考慮MAV設定的情況下執行受保護的作業。"深入瞭解RBAC"。

如果您是MAV管理員、則執行受保護作業的要求也必須獲得MAV管理員核准。

System Manager程序

當使用者按一下功能表項目以啟動作業且作業受到保護時、系統會產生核准要求、且使用者會收到類似下列內容的通知：

```
Approval request to delete the volume was sent.
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

啟用MAV時、可使用*多管理員要求*視窗、顯示根據使用者登入ID和MAV角色（核准者或非核准者）而擱置的要求。針對每個擱置的要求、會顯示下列欄位：

- 營運
- 索引（數字）
- 狀態（「Pending（擱置）」、「Approved（已核准）」、「Rejected（已拒絕）

  如果某個申請被一位核准者拒絕、則不可能採取進一步行動。

- 查詢（所要求作業的任何參數或值）
- 正在申請使用者
- 申請截止日期
- （數量）待核准者
- （數量）潛在核准者

申請核准後、申請使用者可在到期期間內重試該作業。

如果使用者在未經核准的情況下重試作業、則會顯示類似下列的通知：

```
Request to perform delete operation is pending approval.
Retry the operation after request is approved.
```

CLI程序

1. 直接輸入受保護的作業、或使用MAV REQUEST命令輸入。

   範例：若要刪除磁碟區、請輸入下列其中一個命令：

   ◦ `volume delete`

```
cluster-1::*> volume delete -volume vol1 -vserver vs0

Warning: This operation requires multi-admin verification. To create
a
         verification request use "security multi-admin-verify
request
         create".

         Would you like to create a request for this operation?
          {y|n}: y

Error: command failed: The security multi-admin-verify request (index
3) is
       auto-generated and requires approval.
```

- `security multi-admin-verify request create "volume delete"`

```
Error: command failed: The security multi-admin-verify request (index
3)
       requires approval.
```

2. 檢查申請狀態、並回應MAV通知。
   a. 如果申請獲得核准、請回應CLI訊息以完成作業。

      範例：

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: approved
Required Approvers: 1
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Info: Volume "vol1" in Vserver "vs0" will be marked as deleted and
placed in the volume recovery queue. The space used by the volume
will be recovered only after the retention period of 12 hours has
completed. To recover the space immediately, get the volume name
using (privilege:advanced) "volume recovery-queue show vol1_*" and
then "volume recovery-queue purge -vserver vs0 -volume <volume_name>"
command. To recover the volume use the (privilege:advanced) "volume
recovery-queue recover -vserver vs0       -volume <volume_name>"
command.

Warning: Are you sure you want to delete volume "vol1" in Vserver
"vs0" ?
{y|n}: y
```

b. 如果申請遭否決或過期、請刪除申請、然後重新提交或聯絡MAV管理員。

   範例：

```
cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -vserver vs0 -volume vol1
             State: vetoed
Required Approvers: 1
 Pending Approvers: 1
   Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
         Approvals: -
       User Vetoed: admin2
           Vserver: cluster-1
    User Requested: admin
      Time Created: 2/25/2022 13:38:47
     Time Approved: -
           Comment: -
   Users Permitted: -

cluster-1::*> volume delete -volume vol1 -vserver vs0

Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

相關資訊

- "安全多管理員驗證"

在 ONTAP 中管理受 MAV 保護的作業要求

當 MAV 審批組中的管理員（MAV 管理員）收到待處理的操作執行請求通知時，他們必須在固定時間內（審批到期）回覆批准或否決訊息。如果沒有收到足夠數量的批准，請求者必須刪除該請求並提出另一個請求。

關於這項工作

核准要求會以索引編號來識別、這些索引編號會包含在電子郵件訊息中、並顯示要求佇列。

> `multi-admin-verify`處於終端狀態的請求可能會自動覆寫或刪除。使用"審計日誌"審查先前的請求。

可顯示來自要求佇列的下列資訊：

營運

建立要求的受保護作業。

查詢

使用者想要套用作業的物件（或物件）。

州/省

申請的目前狀態；擱置、核准、拒絕、過期、 已執行。如果某個申請被一位核准者拒絕、則不可能採取進一步行動。

必要的核准者

核准申請所需的MAV系統管理員人數。使用者可以為作業規則設定必要的核准者參數。如果使用者未將必要的核准者設定為規則、則會套用全域設定的必要核准者。

待核准者

仍需核准申請並將申請標記為「已核准」的MAV系統管理員人數。

核准過期

MAV管理員必須回應核准要求的期間。任何獲授權的使用者都可以設定作業規則的核准過期時間。如果未針對規則設定核准到期、則會套用全域設定的核准到期日。

執行過期

要求系統管理員必須完成作業的期間。任何授權使用者都可以設定作業規則的執行到期時間。如果未針對規則設定執行過期、則會套用全域設定的執行過期。

使用者已核准

已核准申請的MAV系統管理員。

使用者遭否決

已否決要求的MAV系統管理員。

儲存**VM**（**Vserver**）

與要求相關聯的SVM。此版本僅支援管理SVM。

使用者要求

建立要求之使用者的使用者名稱。

建立時間

建立要求的時間。

核准時間

申請狀態變更為「已核准」的時間。

留言

與申請相關的任何意見。

允許的使用者

允許執行已核准要求之受保護作業的使用者清單。如果 `users-permitted` 為空白、則任何具有適當權限的

使用者都可以執行此作業。

系統管理員

MAV 管理員會收到一封電子郵件，其中包含批准請求的詳細資訊、請求到期期限以及批准或拒絕請求的連結。他們可以透過點擊電子郵件中的連結存取批准對話框，或導航至系統管理員中的*事件和作業>請求*。

啟用多管理員驗證時，*請求*視窗可用，根據使用者的登入 ID 和 MAV 角色（是否為批准者）顯示待處理的請求。

- 營運
- 索引（數字）
- 狀態（「Pending（擱置）」、「Approved（已核准）」、「Rejected（已拒絕）

  如果某個申請被一位核准者拒絕、則不可能採取進一步行動。
- 查詢（所要求作業的任何參數或值）
- 正在申請使用者
- 申請截止日期
- （數量）待核准者
- （數量）潛在核准者

MAV系統管理員在此視窗中有其他控制項、他們可以核准、拒絕或刪除個別作業、或是選取的作業群組。但是、如果MAV管理員是申請使用者、則他們無法核准、拒絕或刪除自己的申請。

CLI

1. 當透過電子郵件收到待處理請求的通知時，請記下請求的索引號和核准有效期限。索引號碼也可以使用下面提到的 **show** 或 **show-pending** 選項顯示。
2. 核准或否決要求。

如果您想...	輸入此命令
核准申請	`security multi-admin-verify request approve` *nn*
否決要求	`security multi-admin-verify request veto` *nn*
顯示所有要求、擱置中的要求或單一要求	`security multi-admin-verify request { show
show-pending } [*nn*] { -fields *field1*[,*field2*…]	[-instance] }`  您可以顯示佇列中的所有要求、或只顯示擱置中的要求。如果您輸入索引編號、則只會顯示該索引編號的資訊。您可以顯示特定欄位的相關資訊（使用 `-fields` 參數）或關於所有欄位（使用 `-instance` 參數）。

如果您想...	輸入此命令
刪除要求	`security multi-admin-verify request delete nn`

範例：

下列順序會在MAV管理員收到索引編號為3的要求電子郵件後核准申請、該電子郵件已獲得一次核准。

```
          cluster1::> security multi-admin-verify request show-pending
                                      Pending
Index Operation      Query State   Approvers Requestor
----- -------------- ----- ------- --------- ---------
    3 volume delete  -     pending 1         julia


cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: approved
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin2
       User Vetoed: -
           Vserver: cluster-1
    User Requested: julia
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

範例：

下列順序會在MAV管理員收到索引編號為3的要求電子郵件後、將要求覆寫、該電子郵件已獲得一次核准。

```
      cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State    Approvers Requestor
----- -------------- ----- -------- --------- ---------
    3 volume delete  -     pending 1         pavan


cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

     Request Index: 3
         Operation: volume delete
             Query: -
             State: vetoed
Required Approvers: 2
 Pending Approvers: 0
   Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
         Approvals: mav-admin1
       User Vetoed: mav-admin2
           Vserver: cluster-1
    User Requested: pavan
      Time Created: 2/25/2022 13:32:03
     Time Approved: 2/25/2022 13:35:36
           Comment: -
   Users Permitted: -
```

相關資訊

- "安全多管理員驗證"

管理動態授權

瞭解 ONTAP 動態授權

從 ONTAP 9.15.1 開始、系統管理員可以設定並啟用動態授權、以提高遠端存取 ONTAP 的安全性、同時降低惡意攻擊者可能造成的潛在損害。有了 ONTAP 9.15.1 、動態授權提供了一個初始架構、可將安全分數指派給使用者、如果他們的活動看起來可疑、則可透過額外的授權檢查來挑戰他們、或是完全拒絕作業。系統管理員可以建立規則、指派信任分數、以及限制命令、以決定何時允許或拒絕使用者的特定活動。系統管理員可以在整個叢集範圍內啟用動態授權、或是為個別的儲存 VM 啟用授權。

動態授權的運作方式

動態授權使用信任評分系統、根據授權原則、將不同的信任等級指派給使用者。根據使用者的信任層級、可以允許或拒絕他們執行的活動、也可以提示使用者進行進一步驗證。

請參閱"自訂動態授權"以深入瞭解如何設定準則分數權重和其他動態授權屬性。

信任的裝置

使用動態授權時、受信任裝置的定義是使用者使用公開金鑰驗證作為驗證方法之一來登入 ONTAP 的裝置。裝置受信任、因為只有該使用者擁有對應的私密金鑰。

動態授權範例

以嘗試刪除磁碟區的三個不同使用者為例。當他們嘗試執行作業時、會檢查每位使用者的風險等級：

- 第一位使用者從信任的裝置登入時、先前的驗證失敗次數極少、這使得她的風險等級偏低；無需額外驗證即可執行此作業。
- 第二位使用者從信任的裝置登入時、其先前的驗證失敗百分比適中、因此風險等級較為溫和；在允許操作之前、系統會提示她進行額外驗證。
- 第三位使用者從不受信任的裝置登入時、其先前的驗證失敗率很高、因此風險等級很高；不允許此作業。

下一步

- "啟用或停用動態授權"
- "自訂動態授權"

在 **ONTAP** 中啟用或停用動態授權

從 ONTAP 9.15.1 開始、系統管理員可以在中設定及啟用動態授權 `visibility` 測試組態的模式、或在中 `enforced` 模式、可啟動透過 SSH 連線的 CLI 使用者組態。如果您不再需要動態授權、可以停用它。當您停用動態授權時、組態設定會保持可用狀態、如果您決定重新啟用、您可以稍後再使用。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization modify`資訊，請參閱。

啟用動態授權以進行測試

您可以在可見度模式中啟用動態授權、藉此測試功能、並確保使用者不會被意外鎖定。在此模式中、信任分數會針對每個受限活動進行檢查、但不會強制執行。但是、任何會被拒絕或受到其他驗證挑戰的活動都會記錄下來。最佳實務做法是先在此模式中測試您想要的設定、然後再執行設定。

即使您尚未設定任何其他動態授權設定、也可以依照此步驟第一次啟用動態授權。"自訂動態授權"如需設定其他動態授權設定的步驟、請參閱以根據您的環境進行自訂。

步驟

1. 設定全域設定並將功能狀態變更為、即可在可見度模式中啟用動態授權 `visibility`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state visibility</strong> \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

在強制模式中啟用動態授權

您可以在強制模式中啟用動態授權。一般而言、在使用可見度模式完成測試之後、您會使用此模式。在此模式中、每個受限活動都會檢查信任分數、如果符合限制條件、則會強制執行活動限制。也會強制執行抑制間隔、以防止在指定時間間隔內發生其他驗證挑戰。

此步驟假設您先前已在中設定並啟用動態授權 `visibility` 強烈建議使用模式。

步驟

1. 在中啟用動態授權 `enforced` 模式、將其狀態變更為 `enforced`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state enforced</strong> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

停用動態授權

如果不再需要新增的驗證安全性、您可以停用動態授權。

步驟

1. 將動態授權狀態變更為、以停用動態授權 `disabled`。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境。必須使用粗體參數：

```
security dynamic-authorization modify \
<strong>-state disabled</strong> \
-vserver <storage_VM_name>
```

2. 使用檢查結果 `show` 顯示全域組態的命令：

```
security dynamic-authorization show
```

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization show`資訊，請參閱。

下一步

（選用）視您的環境而定"自訂動態授權"、請參閱以設定其他動態授權設定。

在 **ONTAP** 中自訂動態授權

身為管理員、您可以自訂動態授權組態的不同層面、以提高遠端系統管理員 SSH 連線至 ONTAP 叢集的安全性。

您可以根據安全需求自訂下列動態授權設定：

- [設定動態授權全域設定]
- [設定動態授權信任分數元件]
- [設定自訂信任分數提供者]
- [設定受限命令]
- [設定動態授權群組]

設定動態授權全域設定

您可以設定動態授權的全域設定、包括要保護的儲存 VM 、驗證挑戰的抑制時間間隔、以及信任分數設定。

如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

步驟

1. 設定動態授權的全域設定。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。更新括弧 <> 中的值以符合您的環境：

```
security dynamic-authorization modify \
-lower-challenge-boundary <percent> \
-upper-challenge-boundary <percent> \
-suppression-interval <interval> \
-vserver <storage_VM_name>
```

2. 檢視產生的組態：

```
security dynamic-authorization show
```

設定受限命令

啟用動態授權時、此功能會包含一組預設的限制命令。您可以修改此清單以符合您的需求。請參閱 "多重管理驗證（ MAV ）文件" 以取得受限命令的預設清單資訊。

新增受限制的命令

您可以將命令新增至受限於動態授權的命令清單。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization rule create`資訊，請參閱。

步驟

1. 新增命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization rule create \
-query <query> \
<strong>-operation <text></strong> \
-index <integer> \
-vserver <storage_VM_name>
```

2. 檢視所產生的限制命令清單：

```
security dynamic-authorization rule show
```

移除受限制的命令

您可以從受限於動態授權的命令清單中移除命令。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization rule delete`資訊，請參閱。

步驟

1. 移除命令。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization rule delete \
<strong>-operation <text></strong> \
-vserver <storage_VM_name>
```

2. 檢視所產生的限制命令清單：

```
security dynamic-authorization rule show
```

設定動態授權群組

根據預設、動態授權會在您啟用後立即套用至所有使用者和群組。不過、您可以使用建立群組 `security dynamic-authorization group create` 因此動態授權僅適用於這些特定使用者。

新增動態授權群組

您可以新增動態授權群組。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization group create`資訊，請參閱。

步驟

1. 建立群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization group create \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name> \
-excluded-usernames <user1,user2,user3...>
```

2. 檢視產生的動態授權群組：

```
security dynamic-authorization group show
```

移除動態授權群組

您可以移除動態授權群組。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization group delete`資訊，請參閱。

步驟

1. 刪除群組。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization group delete \
<strong>-name <group-name></strong> \
-vserver <storage_VM_name>
```

2. 檢視產生的動態授權群組：

```
security dynamic-authorization group show
```

設定動態授權信任分數元件

您可以設定最大分數權重、以變更評分準則的優先順序、或移除風險評分的特定準則。

最佳做法是保留預設分數權重值、並在需要時才進行調整。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component modify`資訊，請參閱。

以下是您可以修改的元件、以及其預設分數和百分比權重：

準則	元件名稱	預設原始分數權重	預設百分比權重
信任的裝置	`trusted-device`	20.	50
使用者登入驗證記錄	`authentication-history`	20.	50

步驟

1. 修改信任分數元件。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component modify \
<strong>-component <component-name></strong> \
<strong>-weight <integer></strong> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數元件設定：

```
security dynamic-authorization trust-score-component show
```

重設使用者的信任分數

如果使用者因系統原則而遭拒存取、且能夠證明其身分識別、則系統管理員可以重設使用者的信任分數。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization user-trust-score reset`資訊，請參閱。

步驟

1. 新增命令。請參閱 [設定動態授權信任分數元件] 取得您可以重設的信任分數元件清單。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization user-trust-score reset \
<strong>-username <username></strong> \
<strong>-component <component-name></strong> \
-vserver <storage_VM_name>
```

顯示您的信任分數

使用者可以顯示自己的登入工作階段信任分數。

步驟

1. 顯示您的信任分數：

   ```
   security login whoami
   ```

   您應該會看到類似下列的輸出：

   ```
   User: admin
   Role: admin
   Trust Score: 50
   ```

   如"指令參考資料ONTAP"需詳細 `security login whoami`資訊，請參閱。

設定自訂信任分數提供者

如果您已經收到外部信任分數提供者的評分方法、可以將自訂提供者新增至動態授權組態。

開始之前

- 自訂信任分數提供者必須傳回 JSON 回應。必須符合下列語法需求：
  - 傳回信任分數的欄位必須是純量欄位、而非陣列的元素。
  - 傳回信任分數的欄位可以是巢狀欄位、例如 `trust_score.value`。
  - JSON 回應中必須有一個欄位可傳回數值信任分數。如果無法原生使用、您可以撰寫包裝函式指令碼來傳回此值。
- 提供的值可以是信任分數或風險分數。差異在於信任分數以遞增順序排列、分數較高則代表較高的信任層級、而風險分數則以遞減順序排列。例如、分數範圍為 0 至 100 的信任分數為 90 、表示分數非常值得信賴、可能會導致「允許」而不需要其他挑戰、 雖然分數範圍為 0 到 100 的風險分數為 90 、表示風險高、可能導致「拒絕」、而不會有額外的挑戰。
- 自訂信任分數提供者必須透過 ONTAP REST API 存取。
- 自訂信任分數提供者必須使用其中一個支援的參數進行設定。不支援需要不在支援參數清單中的組態的自訂信任分數提供者。

  如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component create`資訊，請參閱。

步驟

1. 新增自訂信任分數提供者。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component create \
-component <text> \
<strong>-provider-uri <text></strong> \
-score-field <text> \
-min-score <integer> \
<strong>-max-score <integer></strong> \
<strong>-weight <integer></strong> \
-secret-access-key "<key_text>" \
-provider-http-headers <list<header,header,header>> \
-vserver <storage_VM_name>
```

2. 檢視產生的信任分數提供者設定：

```
security dynamic-authorization trust-score-component show
```

設定自訂信任分數提供者標記

您可以使用標記與外部信任分數提供者通訊。這可讓您將 URL 中的資訊傳送給信任分數提供者、而不會洩漏敏感資訊。

如"指令參考資料ONTAP"需詳細 `security dynamic-authorization trust-score-component create`資訊，請參閱。

步驟

1. 啟用信任分數提供者標記。更新括弧 <> 中的值以符合您的環境。如果您不使用 `-vserver` 參數、命令會在叢集層級執行。必須使用粗體參數：

```
security dynamic-authorization trust-score-component create \
<strong>-component <component_name></strong> \
-weight <initial_score_weight> \
-max-score <max_score_for_provider> \
<strong>-provider-uri <provider_URI></strong> \
-score-field <REST_API_score_field> \
<strong>-secret-access-key "<key_text>"</strong>
```

例如：

```
security dynamic-authorization trust-score-component create -component
comp1 -weight 20 -max-score 100 -provider-uri https://<url>/trust-
scores/users/<user>/<ip>/component1.html?api-key=<access-key> -score
-field score -access-key "MIIBBjCBrAIBArqyTHFvYdWiOpLkLKHGjUYUNSwfzX"
```

使用 OAuth 2.0 進行驗證與授權

ONTAP OAuth 2.0 實作總覽

從 ONTAP 9.14 開始、您可以選擇使用開放授權（ OAuth 2.0 ）架構來控制對 ONTAP 叢集的存取。您可以使用任何 ONTAP 管理介面（包括 ONTAP CLI 、系統管理員和 REST API ）來設定此功能。不過、 OAuth 2.0 授權和存取控制決策只能在用戶端使用 REST API 存取 ONTAP 時套用。

OAuth 2.0 支援是 ONTAP 9.14.0 首次推出、因此可用度取決於您使用的 ONTAP 版本。請參閱 "發行說明ONTAP" 以取得更多資訊。

功能與優勢

以下說明搭配 ONTAP 使用 OAuth 2.0 的主要功能與優點。

支援 **OAuth 2.0** 標準

OAuth 2.0 是業界標準授權架構。它可用來限制及控制使用簽署存取權杖來存取受保護資源的權限。使用 OAuth 2.0 有幾個好處：

- 授權組態有許多選項
- 切勿洩漏用戶端認證、包括密碼
- 您可以根據組態將權杖設定為過期
- 非常適合與 REST API 搭配使用

使用熱門授權伺服器進行測試

ONTAP OAuth 2.0 實作已針對數個熱門伺服器或服務進行測試，其依據為 ONTAP 版本，如下所示：

- ONTAP 9 。 16.1 （支援群組 UUID 至名稱對應和外部角色）：
  - Microsoft Entra ID
- ONTAP 9 。 14.1 （支援標準 OAuth 2.0 功能）
  - 驗證0
  - Active Directory Federation Service （ ADFS ）
  - Keycloak

如需每個 ONTAP 版本可用功能的詳細資訊，請參閱"授權伺服器和存取權杖"。

支援多個並行授權伺服器

您最多可以為單一 ONTAP 叢集定義八個授權伺服器。如此一來、您就能靈活地滿足各種安全環境的需求。

與 **REST** 角色整合

ONTAP 授權決策最終取決於指派給使用者或群組的其餘角色。這些角色可在存取權杖中作為獨立範圍、或是根據本機 ONTAP 定義以及 Active Directory 或 LDAP 群組來執行。

使用寄件者限制存取權杖的選項

您可以將 ONTAP 和授權伺服器設定為使用相互傳輸層安全性（ MTLS ）、以強化用戶端驗證。它保證 OAuth 2.0 存取權杖只能由最初核發的用戶端使用。此功能支援並符合數項常用的安全性建議、包括由 FAPI 和斜接建立的建議。

實作與組態

在較高層級、 OAuth 2.0 實作和組態有幾個層面、您應該在開始使用時考慮。

ONTAP 內的 **OAuth 2.0** 實體

OAuth 2.0 授權架構定義了數個實體、可對應至資料中心或網路中的實際或虛擬元素。下表列出 OAuth 2.0 實體及其對 ONTAP 的調適。

OAuth 2.0 實體	說明
資源	REST API 端點、可透過內部 ONTAP 命令存取 ONTAP 資源。
資源擁有者	建立受保護資源或依預設擁有資源的 ONTAP 叢集使用者。
資源伺服器	受保護資源的主機、即 ONTAP 叢集。
用戶端	代表或取得資源擁有者權限、要求存取 REST API 端點的應用程式。
授權伺服器	通常是負責發行存取權杖和強制執行管理原則的專用伺服器。

核心 **ONTAP** 組態

您需要設定 ONTAP 叢集以啟用和使用 OAuth 2.0 。這包括建立與授權伺服器的連線、以及定義所需的 ONTAP 授權組態。您可以使用任何管理介面來執行此組態、包括：

- 指令行介面ONTAP
- 系統管理員
- 靜態API ONTAP

環境與支援服務

除了 ONTAP 定義之外、您也需要設定授權伺服器。如果您使用群組對角色對應、也需要設定 Active Directory 群組或 LDAP 等量。

支援的 **ONTAP** 用戶端

從 ONTAP 9.14 開始、 REST API 用戶端可以使用 OAuth 2.0 存取 ONTAP 。在發出 REST API 呼叫之前、您需要從授權伺服器取得存取權杖。然後、用戶端使用 HTTP 授權要求標頭、將此權杖以 _bon承載 權杖的形式傳送至 ONTAP 叢集。視所需的安全性層級而定、您也可以在用戶端建立及安裝憑證、以使用以 MTLS 為基礎的寄件者限制權杖。

選定的術語

當您開始使用 ONTAP 探索 OAuth 2.0 部署時、熟悉其中一些詞彙是很有幫助的。請參閱 "其他資源" 取得有關 OAuth 2.0 的詳細資訊連結。

存取權杖

由授權伺服器發出的權杖、由 OAuth 2.0 用戶端應用程式用來發出存取受保護資源的要求。

JSON Web Token

用於格式化存取權杖的標準。JSON 用於以精簡格式呈現 OAuth 2.0 宣告、並將宣告分為三個主要區段。

寄件者限制的存取權杖

以相互傳輸層安全性（ MTLS ）傳輸協定為基礎的選用功能。藉由在權杖中使用額外的確認宣告、這可確保存取權杖僅供最初核發的用戶端使用。

JSON Web 金鑰集

JWKS 是 ONTAP 用來驗證用戶端所呈現 JWT Token 的公開金鑰集合。金鑰集通常可透過專用 URI 在授權伺服器上使用。

範圍

範圍提供一種方法來限制或控制應用程式對受保護資源（例如 ONTAP REST API ）的存取。它們在存取權杖中以字串表示。

ONTAP REST 角色

REST 角色是 ONTAP 9.6 引進的、是 ONTAP RBAC 架構的核心部分。這些角色與 ONTAP 仍支援的舊版傳統角色不同。ONTAP 中的 OAuth 2.0 實作僅支援 REST 角色。

HTTP 授權標頭

HTTP 要求中包含的標頭、用於在進行 REST API 呼叫時識別用戶端及相關權限。視驗證和授權的執行方式而定、有多種類型或實作可供選擇。將 OAuth 2.0 存取權杖呈現給 ONTAP 時、該權杖會識別為 _stoning 權杖 _ 。

HTTP 基本驗證

ONTAP 仍支援早期的 HTTP 驗證技術。純文字認證（使用者名稱和密碼）會與冒號串連、並以 base64 編碼。字串會放在授權要求標頭中、並傳送至伺服器。

FAPI

OpenID Foundation 的工作群組、為金融產業提供通訊協定、資料架構及安全建議。API 原本稱為財務等級 API 。

斜接

一家私人非營利公司、為美國空軍和美國政府提供技術與安全指引。

其他資源

以下提供幾項額外資源。您應該檢閱這些網站、以取得有關 OAuth 2.0 及相關標準的更多資訊。

通訊協定與標準

- "RFC 6749 ： OAuth 2.0 授權架構"

- "RFC 7519 ： JSON Web Token （ JWT ）"
- "RFC 7523 ：適用於 OAuth 2.0 用戶端驗證和授權授與的 JSON Web Token （ JWT ）設定檔"
- "RFC 7662 ： OAUTH 2.0 Token 反思"
- "RFC 7800 ： JWTs 的持有證明金鑰"
- "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖"

組織

- "OpenID Foundation"
- "FAPI 工作組"
- "斜接"
- "IANA - JWT"

產品與服務

- "驗證0"
- "entra ID"
- "ADFS 總覽"
- "Keycloak"

其他工具與公用程式

- "JWT by Auth0"
- "Openssl"

NetApp 文件與資源

- "ONTAP 自動化文件"

概念

ONTAP中的 **OAuth 2.0** 授權伺服器和存取令牌

授權伺服器會在 OAuth 2.0 授權架構中執行多項重要功能、做為中央元件。

OAuth 2.0 授權伺服器

授權伺服器主要負責建立和簽署存取權杖。這些權杖包含身分識別與授權資訊、可讓用戶端應用程式選擇性地存取受保護的資源。這些伺服器通常彼此隔離、可透過多種不同方式實作、包括獨立的專用伺服器、或是作為較大型的身分識別與存取管理產品的一部分。

> 授權伺服器有時會使用不同的術語、尤其是 OAuth 2.0 功能會封裝在較大的身分識別與存取管理產品或解決方案中。例如，術語 * 身分識別提供者（ IDP ） * 經常與 * 授權伺服器 * 互換使用。

系統管理

除了發行存取權杖之外、授權伺服器也會提供相關的管理服務、通常是透過 Web 使用者介面。例如、您可以定義和管理：

- 使用者和使用者驗證
- 範圍
- 透過租戶和領域進行管理隔離
- 原則強制執行
- 連線至各種外部服務
- 支援其他身分識別傳輸協定（例如 SAML ）

ONTAP 與符合 OAuth 2.0 標準的授權伺服器相容。

定義至 **ONTAP**

您需要定義一或多個 ONTAP 授權伺服器。ONTAP 會安全地與每部伺服器通訊、以驗證權杖、並執行其他相關工作來支援用戶端應用程式。

ONTAP 組態的主要層面如下所示。另請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

存取權杖的驗證方式與位置

驗證存取權杖有兩個選項。

- 本機驗證

  ONTAP 可以根據發行權杖的授權伺服器所提供的資訊、在本機驗證存取權杖。從授權伺服器擷取的資訊會由 ONTAP 快取、並定期重新整理。

- 遠端自我反思

  您也可以使用遠端自我反思來驗證授權伺服器上的權杖。introspection 是一種允許授權方查詢授權伺服器有關存取權杖的通訊協定。它提供 ONTAP 從存取權杖擷取特定中繼資料並驗證權杖的方法。由於效能原因、ONTAP 會快取部分資料。

網路位置

ONTAP 可能位於防火牆後方。在這種情況下、您需要將 Proxy 識別為組態的一部分。

授權伺服器的定義方式

您可以使用任何管理介面（包括 CLI 、系統管理員或 REST API ）來定義 ONTAP 的授權伺服器。例如、您可以使用 CLI 使用命令 `security oauth2 client create`。

如"指令參考資料ONTAP"需詳細 `security oauth2 client create`資訊，請參閱。

授權伺服器數量

您最多可以定義八個授權伺服器到單一 ONTAP 叢集。只要發卡行或發卡行 / 受眾聲明是唯一的、同一授權伺服器就可以多次定義到同一個 ONTAP 叢集。例如、使用 Keycloak 時、使用不同領域時、這種情況永遠都會發生。

ONTAP 支援的 **OAuth 2.0** 功能

OAUTH 2.0 的支援最初隨 ONTAP 9 提供。 14.1 之後的版本將持續增強。ONTAP 支援的 OAuth 2.0 功能如下所述。

隨特定 ONTAP 版本推出的功能將會持續到未來的版本。

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 功能，以納入原生 Entra ID 群組的 Entra ID 專屬副檔名。這涉及在存取權杖中使用 GUID ，而非名稱。此外，此版本還新增外部角色對應支援，可利用存取權杖中的「角色」欄位，將原生身分識別提供者角色對應至 ONTAP 角色。

ONTAP 9.14.1.

從 ONTAP 9 。 14.1 開始，授權伺服器可透過下列標準 OAuth 2.0 功能來支援使用的應用程式：

- OAuth 2.0 標準欄位包括「 iss 」，「 aud 」和「 exp 」，如和 "RFC 7519 ： JSON Web Token （ JWT ）"中所述 "RFC6749 ： OAuth 2.0 授權架構"。這也支援透過存取權杖中的欄位來唯一識別使用者，例如「 UPN 」，「 AppID 」，「 Sub" ，「使用者名稱」或「 Preferred _UserName 」。
- 針對具有「群組」欄位的群組名稱，針對特定於供應商的 ADFS 副檔名。
- Azure 廠商專屬的群組 UUID 延伸功能，並具有「群組」欄位。
- 使用 OAuth 2.0 存取權杖範圍內的獨立角色和具名角色來提供授權支援的 ONTAP 延伸功能。其中包括「範圍」和「 scp 」欄位，以及範圍內的群組名稱。

使用 **OAuth 2.0** 存取權杖

由授權伺服器發出的 OAuth 2.0 存取權杖是由 ONTAP 驗證、用於為 REST API 用戶端要求做出角色型存取決策。

取得存取權杖

您需要從定義至 ONTAP 叢集的授權伺服器取得存取權杖、以便在其中使用 REST API 。若要取得權杖、您必須直接聯絡授權伺服器。

ONTAP 不會核發存取權杖、也不會將用戶端的要求重新導向至授權伺服器。

您要求權杖的方式取決於多項因素、包括：

- 授權伺服器及其組態選項
- OAuth 2.0 授與類型
- 用於發出要求的用戶端或軟體工具

授與類型

_Grant 是定義完善的程序、包括一組網路流量、用於要求及接收 OAuth 2.0 存取權杖。視用戶端、環境和安全性需求而定、可使用多種不同的授與類型。下表列出熱門的補助類型清單。

授與類型	說明
用戶端認證	一種僅使用認證（例如 ID 和共用密碼）的常用授與類型。假設用戶端與資源擁有者有密切的信任關係。

授與類型	說明
密碼	資源擁有者密碼認證授與類型可用於資源擁有者與用戶端建立信任關係的情況。將舊版 HTTP 用戶端移轉至 OAuth 2.0 時、這項功能也很實用。
授權代碼	這是機密用戶端的理想授與類型、是以重新導向為基礎的流程為基礎。它可用於取得存取權杖和重新整理權杖。

JWT 內容

OAuth 2.0 存取權杖格式化為 JWT 。內容是由授權伺服器根據您的組態建立。不過、這些 Token 對用戶端應用程式來說是不透明的。用戶端沒有理由檢查權杖或是知道其內容。

每個 JWT 存取權杖都包含一組宣告。聲明說明發卡行的特性、以及根據授權伺服器的管理定義進行的授權。下表說明部分已登錄於標準的索賠。所有字串都區分大小寫。

請款	關鍵字	說明
發卡行	ISS	識別發出權杖的主體。請款處理是針對特定應用程式。
主旨	子	權杖的主旨或使用者。名稱的範圍是全域或本機唯一的。
目標對象	AUD	權杖的目標收件者。以字串陣列形式實作。
過期	到期	權杖過期且必須拒絕的時間。

請參閱 "RFC 7519 ： JSON Web Token" 以取得更多資訊。

用戶端授權

ONTAP 用戶端授權的總覽與選項

ONTAP OAUTH 2.0 實作的設計既靈活又穩健，提供您保護 ONTAP 環境所需的功能。有多種互斥的組態選項可供選擇。授權決策最終取決於 OAuth 2.0 存取權杖中包含或衍生的 ONTAP REST 角色。

> 您只能使用 "ONTAP REST 角色" 設定 OAuth 2.0 授權時。不支援舊版 ONTAP 傳統角色。

ONTAP 會根據您的組態，套用最適當的單一授權選項。如需 ONTAP 如何做出用戶端存取決策的詳細資訊，請參閱"ONTAP 如何決定存取"。

OAuth 2.0 獨立範圍

這些範圍包含一或多個自訂 REST 角色，每個角色都封裝在存取權杖中的單一字串內。它們不受 ONTAP 角色定義的影響。您需要在授權伺服器上設定範圍字串。如需詳細資訊、請參閱 "獨立 OAuth 2.0 範圍" 。

本機 ONTAP REST 角色

可以使用單一命名 REST 角色，無論是內建或自訂。命名角色的範圍語法是 *ONTAP 角色 <URL-encoded-ONTAP-role-name> 。例如，如果 ONTAP 角色是範圍字串，則 `admin`為 `ontap-role-admin`。

使用者

您可以使用存取權杖中定義的使用者名稱，以存取應用程式「 http 」。根據定義的驗證方法，以下列順序測試使用者：密碼，網域（ Active Directory ）， nsswitch （ LDAP ）。

群組

授權伺服器可設定為使用 ONTAP 群組進行授權。如果檢查本機 ONTAP 定義、但無法做出存取決定、則會使用 Active Directory （「網域」）或 LDAP （「 nsswitch 」）群組。群組資訊可透過下列兩種方式之一來指定：

- OAuth 2.0 範圍字串

  支援使用用戶端認證流程的機密應用程式、而該流程沒有使用者擁有群組成員資格。範圍應命名為 *ONTAP 群組 <URL-encoded-ONTAP-group-name> 。例如、如果群組為「開發」、範圍字串將為「 ontap 群組開發」。

- 在「群組」請款中

  這是針對使用資源擁有者（密碼授予）流程的 ADFS 所發行的存取權杖。

看"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組"了解更多。

ONTAP中的獨立 OAuth 2.0 範圍

自我包含的範圍是存取權杖中攜帶的字串。每個角色都是完整的自訂角色定義、包括 ONTAP 做出存取決策所需的一切。範圍與 ONTAP 本身定義的任何其他角色是分開的。

範圍字串的格式

在基礎層級、範圍會以連續字串表示、並由六個以冒號分隔的值組成。範圍字串中使用的參數如下所述。

ONTAP 文字

範圍必須以文字值開頭 `ontap` 以小寫形式顯示。這會將範圍識別為 ONTAP 特有的範圍。

叢集

這會定義範圍所適用的 ONTAP 叢集。這些值可以包括：

- 叢集 UUID

  識別單一叢集。

- 星號（ * ）

  表示範圍適用於所有叢集。

您可以使用 ONTAP CLI 命令 `cluster identity show`來顯示叢集的 UUID 。如果未指定、範圍會套用至所有叢集。如"指令參考資料ONTAP"需詳細 `cluster identity show`資訊，請參閱。

角色

包含在獨立範圍中的 REST 角色名稱。ONTAP 不會檢查此值、也不會與任何定義給 ONTAP 的現有 REST 角色相符。名稱用於記錄。

存取層級

此值表示在範圍內使用 API 端點時、套用至用戶端應用程式的存取層級。下表說明了六個可能的值。

存取層級	說明
無	拒絕對指定端點的所有存取。
唯讀	僅允許使用 GET 進行讀取存取。
read_create	允許讀取存取、以及使用 POST 建立新的資源執行個體。
Read_modify	允許讀取存取權、以及使用修補程式更新現有資源的能力。
read_create_modify	允許刪除以外的所有存取。允許的作業包括 GET （讀取）、 POST （建立）和修補程式（更新）。
全部	允許完整存取。

SVM

適用範圍之叢集內的 SVM 名稱。使用 * 值（星號）表示所有 SVM 。

ONTAP 9.14.1 不完全支援此功能。您可以忽略 SVM 參數、並使用星號做為預留位置。檢閱 "發行說明ONTAP" 檢查將來的 SVM 支援。

REST API URI

資源或一組相關資源的完整或部分路徑。字串必須以開頭 `/api`。如果您未指定值、範圍會套用至 ONTAP 叢集上的所有 API 端點。

範圍範例

以下是一些自我包含範圍的範例。

ONTAP ： * ： jjoes-role ： read_create_modify ： * ： /API/cluster
提供指派此角色的使用者讀取、建立及修改對的存取權 `/cluster` 端點：

CLI 管理工具

為了讓自我包含範圍的管理更容易且更容易出錯、 ONTAP 提供了 CLI 命令 `security oauth2 scope` 根據輸入參數產生範圍字串。

命令 `security oauth2 scope` 根據您的意見、有兩種使用案例：

- 範圍字串的 CLI 參數

  您可以使用此版本的命令來根據輸入參數產生範圍字串。

- 範圍字串至 CLI 參數

  您可以使用此版本的命令、根據輸入範圍字串產生命令參數。

範例

下列範例會產生範圍字串、並在下列命令範例之後包含輸出。此定義適用於所有叢集。

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap:*:joes-role:readonly:*:/api/cluster
```

如"指令參考資料ONTAP"需詳細 `security oauth2 scope`資訊，請參閱。

ONTAP中的 OAuth 2.0 外部角色映射

外部角色是在設定供 ONTAP 使用的識別供應商處定義。您可以使用 ONTAP CLI 建立及管理這些外部角色與 ONTAP 角色之間的對應關係。

您也可以使用 ONTAP REST API 來設定外部角色對應功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

存取權杖中的外部角色

以下是包含兩個外部角色的 JSON 存取權杖片段。

```
...
"appidacr": "1",
"family_name": "User",
"name": "Test User 1",
"oid": "4c2215c7-6d52-40a7-ce71-096fa41379ba",
"roles": [
  "Global Administrator",
  "Application Administrator"
],
"ver": "1.0",
...
```

組態

您可以使用 ONTAP 命令列介面來管理外部角色對應功能。

建立

您可以使用命令定義角色對應組態 `security login external-role-mapping create`。您必須處於 ONTAP * 管理 * 權限層級，才能發出此命令及相關選項。

參數

用於建立群組對應的參數如下所述。

參數	說明
`external-role`	在外部身分識別提供者定義的角色名稱。
`provider`	身分識別提供者的名稱。這應該是系統的識別碼。
`ontap-role`	表示外部角色對應的現有 ONTAP 角色。

範例

```
security login external-role-mapping create -external-role "Global
Administrator" -provider entra -ontap-role admin
```

如"指令參考資料ONTAP"需詳細 `security login external-role-mapping create`資訊，請參閱。

其他 **CLI** 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改
- 刪除

相關資訊

- "指令參考資料ONTAP"

ONTAP 如何決定用戶端存取

若要正確設計及實作 OAuth 2.0 、您必須瞭解 ONTAP 如何使用您的授權組態來為用戶端做出存取決策。根據 ONTAP 版本，決定存取權限的主要步驟如下所示。

ONTAP 9 · 15.1 沒有重大的 OAuth 2.0 更新。如果您使用的是 9.15.1 版，請參閱 ONTAP 9 。14.1 的說明。

相關資訊

- "ONTAP 支援的 OAuth 2.0 功能"

ONTAP 9.16.1.

ONTAP 9 。 16.1 擴充標準 OAuth 2.0 支援，以納入適用於原生 Entra ID 群組的 Microsoft Entra ID 特定副檔名，以及外部角色對應。

判斷 **ONTAP 9** 的用戶端存取權。 **16.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`，或是宣告， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，則檢查其格式。如果群組以 UUID 表示，則搜尋內部群組對應表。如果存在符合的群組和關聯的角色，ONTAP將使用為該群組定義的角色做出存取決策。這始終會導致“允許”或“拒絕”決策，處理結束。有關更多信息，請參閱"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組" 。

如果群組是以名稱表示，並已設定網域或 nsswitch 授權，則 ONTAP 會分別嘗試將其與 Active Directory 或 LDAP 群組進行比對。如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

ONTAP 9.14.1.

支援的初始 OAUTH 2.0 是根據標準 OAUTH 2.0 功能而在 ONTAP 9 中推出的。

決定 **ONTAP 9** 的用戶端存取權。 **14.1**

步驟 **1** ：自我包含的範圍

如果存取權杖包含任何獨立的範圍， ONTAP 會先檢查這些範圍。如果沒有獨立的範圍、請前往步驟 2 。

如果存在一個或多個獨立的範圍、 ONTAP 會套用每個範圍、直到可以做出明確的 * 允許 * 或 * 拒絕 * 決策為止。如果做出明確的決定、處理程序就會結束。

如果 ONTAP 無法做出明確的存取決策、請繼續執行步驟 2 。

步驟 **2** ：檢查本機角色旗標

ONTAP 檢查布爾參數 `use-local-roles-if-present`。此旗標的值會針對定義為 ONTAP 的每個授權伺服器分別設定。

- 如果值為 `true` 繼續進行步驟 3 。
- 如果值為 `false` 處理結束、存取遭拒。

步驟 **3** ：具名的 **ONTAP REST** 角色

如果存取權杖在 OR `scp` 欄位中包含具名的 REST 角色 `scope`， ONTAP 會使用該角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有指定的 REST 角色或找不到角色、請繼續執行步驟 4 。

步驟 **4** ：使用者

從存取權杖擷取使用者名稱，並嘗試將其與有權存取應用程式「 http 」的使用者配對。根據驗證方法，依下列順序檢查使用者：

- 密碼
- 網域（ Active Directory ）
- NSWITCH （ LDAP ）

如果找到相符的使用者， ONTAP 會使用為使用者定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果使用者不相符，或存取權杖中沒有使用者名稱，請繼續執行步驟 5 。

步驟 **5** ：群組

如果包含一個或多個群組，並設定了網域或 nsswitch 授權， ONTAP 會分別嘗試將它們與 Active Directory 或 LDAP 群組配對。

如果有群組相符項目、 ONTAP 會使用為群組定義的角色來做出存取決策。這總是導致 * 允許 * 或 * 拒絕 * 決策和處理結束。

如果沒有符合的群組、或存取權杖中沒有群組、則會拒絕存取並結束處理。

使用**ONTAP** 的**OAuth 2.0** 部署場景

將授權伺服器定義為 ONTAP 時、有幾個組態選項可供使用。根據這些選項，您可以使用多種部署案例之一，定義適合您環境的授權伺服器。

組態參數摘要

將授權伺服器定義為 ONTAP 時、有幾個組態參數可供使用。這些參數通常在所有管理介面中都受到支援。

個別參數或欄位使用的名稱可能會因 ONTAP 管理介面而異。為了因應管理介面的差異，表格中的每個參數都會使用單一通用名稱。根據上下文，與特定介面搭配使用的確切名稱應該是顯而易見的。

參數	說明
名稱	ONTAP 已知的授權伺服器名稱。
應用程式	定義所適用的 ONTAP 內部應用程式。這必須是 * http * 。
發卡行 URI	具有路徑的 FQDN 、可識別發出權杖的站台或組織。
提供者 JWKS URI	ONTAP 取得用於驗證存取權杖之 JSON 網頁金鑰集的路徑和檔案名稱 FQDN 。
JWKS 重新整理時間間隔	決定 ONTAP 從提供者 JWKS URI 重新整理憑證資訊的頻率的時間間隔。此值以 ISO-8601 格式指定。
introspection 端點	ONTAP 透過自我介紹來執行遠端權杖驗證所使用的路徑 FQDN 。
用戶端ID	授權伺服器上定義的用戶端名稱。包含此值時、您也需要根據介面提供相關的用戶端機密。
傳出 Proxy	這是為了在 ONTAP 位於防火牆後方時提供對授權伺服器的存取。URI 必須為 cURL 格式。
如果存在、請使用本機角色	判斷是否使用本機 ONTAP 定義的布林旗標、包括具名 REST 角色和本機使用者。
遠端使用者請款	ONTAP 用來比對本機使用者的替代名稱。使用 `sub` 存取權杖中的欄位、以符合本機使用者名稱。
目標對象	此欄位定義可使用存取權杖的端點。

部署案例

以下提供幾種常見的部署案例。它們是根據權杖驗證是由 ONTAP 在本機執行、還是由授權伺服器遠端執行來組織。每個案例都包含所需組態選項的清單。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得組態命令的範例。

定義授權伺服器之後、您可以透過 ONTAP 管理介面顯示其組態。例如、使用命令 `security oauth2 client show` 使用 ONTAP CLI 。

本機驗證

下列部署案例是以 ONTAP 在本機執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是僅使用 OAuth 2.0 獨立範圍的最簡單部署。不會使用任何本機 ONTAP 身分識別定義。您需要包含下列參數

：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 發卡行 URI

您也需要在授權伺服器上新增範圍。

在 **Proxy** 中使用自我包含的範圍

此部署案例使用 OAuth 2.0 獨立範圍。不會使用任何本機 ONTAP 身分識別定義。但是授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您也需要在授權伺服器上新增範圍。

使用本機使用者角色和預設使用者名稱對應搭配 **Proxy**

此部署案例使用具有預設名稱對應的本機使用者角色。遠端使用者宣告使用的預設值 `sub` 因此、存取權杖中的這個欄位是用來比對本機使用者名稱。使用者名稱必須少於 40 個字元。授權伺服器位於防火牆後方、因此您也需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI
- 如果存在、請使用本機角色 (`true`)
- 傳出 Proxy
- 發卡行

您必須確定本機使用者已定義為 ONTAP 。

使用本機使用者角色和替代使用者名稱對應搭配 **Proxy**

此部署案例使用具有替代使用者名稱的本機使用者角色、用於與本機 ONTAP 使用者配對。授權伺服器位於防火牆後方、因此您需要設定 Proxy 。您需要包含下列參數：

- 名稱
- 應用程式（ http ）
- 提供者 JWKS URI

- 如果存在、請使用本機角色 (`true`)
- 遠端使用者請款
- 傳出 Proxy
- 發卡行 URI
- 目標對象

您必須確定本機使用者已定義為 ONTAP 。

遠端自我反思

下列部署組態是以 ONTAP 透過自我反思遠端執行權杖驗證為基礎。

使用不含 **Proxy** 的自我控制範圍

這是以 OAuth 2.0 獨立範圍為基礎的簡單部署。不會使用任何 ONTAP 身分識別定義。您必須包含下列參數：

- 名稱
- 應用程式（ http ）
- introspection 端點
- 用戶端ID
- 發卡行 URI

您需要在授權伺服器上定義範圍以及用戶端和用戶端機密。

相關資訊

- "安全 oauth2 用戶端展示"

使用 **OAuth 2.0 Mutual TLS** 進行**ONTAP**客戶端身份驗證

視您的安全需求而定、您可以選擇性地設定相互 TLS （ MTLS ）來實作強式用戶端驗證。搭配 ONTAP 搭配 OAuth 2.0 部署使用時、 MTLS 保證存取權杖只能由最初核發的用戶端使用。

與 **OAuth 2.0** 共同使用 **TLS**

傳輸層安全性（ TLS ）用於在兩個應用程式（通常是用戶端瀏覽器和 Web 伺服器）之間建立安全的通訊通道。相互 TLS 可透過用戶端憑證提供用戶端的強大識別功能、藉此延伸此功能。在具有 OAuth 2.0 的 ONTAP 叢集中使用時、可透過建立和使用寄件者限制的存取權杖來擴充基礎 MTLS 功能。

傳送者限制的存取權杖只能由最初核發的用戶端使用。若要支援此功能、請提出新的確認聲明 (`cnf`）插入令牌中。欄位包含內容 `x5t#S256` 其中包含要求存取權杖時所使用的用戶端憑證摘要。此值由 ONTAP 驗證、作為驗證權杖的一部分。未受寄件者限制的授權伺服器所核發的存取權杖、不包含額外的確認宣告。

您需要將 ONTAP 設定為針對每個授權伺服器分別使用 MTLS 。例如、 CLI 命令 `security oauth2 client` 包含參數 `use-mutual-tls` 根據下表所示的三個值來控制 MTLS 處理。

在每個組態中、 ONTAP 所採取的結果和行動、都要視組態參數值、以及存取權杖和用戶端憑證的內容而定。表格中的參數是從最少組織到最嚴格的組織。

參數	說明
無	授權伺服器的 OAuth 2.0 相互 TLS 驗證已完全停用。ONTAP 不會執行 MTLS 用戶端憑證驗證、即使憑證中有確認宣告、或是用戶端憑證隨附 TLS 連線。
要求	如果用戶端提供寄件者限制的存取權杖、則會強制執行 OAuth 2.0 相互 TLS 驗證。也就是說、只有在確認宣告（含屬性）時、才會強制執行 MTLS `x5t#S256`）存在於存取權杖中。這是預設設定。
必要	對於由授權伺服器發出的所有存取權杖、都會強制執行 OAuth 2.0 相互 TLS 驗證。因此、所有存取權杖都必須受寄件者限制。如果存取權杖中沒有確認宣告、或是用戶端憑證無效、驗證和 REST API 要求就會失敗。

高階實作流程

在 ONTAP 環境中搭配 OAuth 2.0 使用 MTLS 時所涉及的一般步驟如下所示。請參閱 "RFC 8705 ： OAuth 2.0 雙向 TLS 用戶端驗證和憑證繫結存取權杖" 以取得更多詳細資料。

步驟 **1** ：建立及安裝用戶端憑證

建立用戶端身分識別的基礎、是證明客戶端私密金鑰的知識。對應的公開金鑰會放置在用戶端提供的簽署 X.509 憑證中。在較高層級、建立用戶端憑證所涉及的步驟包括：

1. 產生公開金鑰與私密金鑰配對
2. 建立憑證簽署要求
3. 將 CSR 檔案傳送至知名的 CA
4. CA 會驗證要求並核發簽署的憑證

您通常可以在本機作業系統中安裝用戶端憑證、或直接搭配一般公用程式（例如 Curl ）使用。

步驟 **2** ：將 **ONTAP** 設定為使用 **MTLS**

您需要設定 ONTAP 以使用 MTLS 。每個授權伺服器都會分別完成此組態設定。例如、使用 CLI 命令 `security oauth2 client` 與選用參數搭配使用 `use-mutual-tls`。請參閱 "在 ONTAP 中部署 OAuth 2.0" 以取得更多資訊。

步驟 **3** ：用戶端要求存取權杖

用戶端需要從設定為 ONTAP 的授權伺服器要求存取權杖。用戶端應用程式必須在步驟 1 中建立並安裝憑證時使用 MTLS 。

步驟 **4** ：授權伺服器會產生存取權杖

授權伺服器會驗證用戶端要求並產生存取權杖。在此過程中、它會建立用戶端憑證的訊息摘要、並將其作為確認宣告（欄位 `cnf`）。

步驟 **5** ：用戶端應用程式會將存取權杖呈現給 **ONTAP**

用戶端應用程式會對 ONTAP 叢集進行 REST API 呼叫、並在授權要求標頭中以 * 承載權杖 * 的形式包含存取權杖。用戶端必須使用 MTLS 搭配用於要求存取權杖的相同憑證。

步驟 **6** ： **ONTAP** 會驗證用戶端和權杖。

ONTAP 會在 HTTP 要求中接收存取權杖、以及作為 MTLS 處理一部分的用戶端憑證。ONTAP 會先驗證存取權杖中的簽章。根據組態、 ONTAP 會產生用戶端憑證的訊息摘要、並將其與權杖中的確認宣告 **cnf** 進行比較。如果這兩個值相符、 ONTAP 已確認發出 API 要求的用戶端與最初發出存取權杖的用戶端相同。

相關資訊

- "安全oauth2客戶端"

設定與部署

準備使用 **ONTAP** 部署 **OAuth 2.0**

在 ONTAP 環境中設定 OAuth 2.0 之前、您應該先準備部署。主要任務和決定摘要如下。各節的排列方式通常與您應遵循的順序一致。不過、雖然它適用於大多數的部署、但您應該視需要調整以符合您的環境。您也應該考慮建立正式的部署計畫。

根據您的環境、您可以為定義為 ONTAP 的授權伺服器選取組態。這包括您需要針對每種部署類型指定的參數值。請參閱 "OAuth 2.0 部署案例" 以取得更多資訊。

受保護的資源和用戶端應用程式

OAuth 2.0 是一個授權架構、用於控制受保護資源的存取。有鑑於此、任何部署的重要第一步、就是判斷可用資源為何、以及哪些用戶端需要存取這些資源。

識別用戶端應用程式

您需要決定在發出 REST API 呼叫時、哪些用戶端會使用 OAuth 2.0 、以及哪些 API 端點需要存取。

檢閱現有的 **ONTAP REST** 角色和本機使用者

您應該檢閱現有的 ONTAP 身分識別定義、包括其餘角色和本機使用者。視您設定 OAuth 2.0 的方式而定、這些定義可用於做出存取決策。

全域移轉至 **OAuth 2.0**

雖然您可以逐步實作 OAuth 2.0 授權、但也可以為每個授權伺服器設定全域旗標、立即將所有其餘 API 用戶端移至 OAuth 2.0 。如此一來、就能根據現有的 ONTAP 組態來做出存取決策、而無需建立獨立的範圍。

授權伺服器

授權伺服器在 OAuth 2.0 部署中扮演重要角色、方法是核發存取權杖並強制執行管理原則。

選取並安裝授權伺服器

您需要選取並安裝一或多個授權伺服器。請務必熟悉身分識別供應商的組態選項和程序、包括如何定義範圍。請注意，某些授權伺服器（包括 Microsoft Entra ID ）代表使用 UUID 而非名稱的群組。

判斷是否需要安裝授權根 **CA** 憑證

ONTAP 使用授權伺服器的憑證來驗證用戶端所提供的已簽署存取權杖。為達此目的、 ONTAP 需要根 CA 憑證和任何中繼憑證。這些可能已預先安裝在 ONTAP 中。如果沒有、您需要安裝它們。

評估網路位置和組態

如果授權伺服器位於防火牆之後、則需要將 ONTAP 設定為使用 Proxy 伺服器。

用戶端驗證與授權

您需要考量用戶端驗證和授權的幾個層面。

獨立範圍或本機 **ONTAP** 身分識別定義

在高層級、您可以定義在授權伺服器上定義的自我包含範圍、或是仰賴現有的本機 ONTAP 身分識別定義、包括角色和使用者。

具有本機 **ONTAP** 處理功能的選項

如果您使用 ONTAP 身分識別定義、則必須決定要套用的項目、包括：

- 具名 REST 角色
- 符合本機使用者
- Active Directory 或 LDAP 群組

本機驗證或遠端自我反省

您需要決定存取權杖是由 ONTAP 在本機驗證、還是透過自我反省在授權伺服器驗證。也有幾個相關的值需要考量、例如重新整理時間間隔。

寄件者限制的存取權杖

對於需要高安全性的環境、您可以使用以 MTLS 為基礎的傳送限制存取權杖。這需要每個用戶端的憑證。

群組為 **UUID** 和身分識別對應

如果您使用的授權伺服器代表使用 UUID 的群組，則需要規劃如何將這些群組對應至群組名稱，並可能對應至相關角色。

管理介面

您可以透過任何 ONTAP 介面執行 OAuth 2.0 管理、包括：

- 命令列介面
- 系統管理員
- REST API

用戶端如何要求存取權杖

用戶端應用程式必須直接從授權伺服器要求存取權杖。您需要決定如何執行、包括授與類型。

設定**ONTAP** 功能

您需要執行幾項 ONTAP 組態工作。

定義 **REST** 角色和本機使用者

根據您的授權組態、可使用本機 ONTAP 識別處理。在這種情況下、您需要檢閱並定義其餘角色和使用者定義。此外，視您的授權伺服器而定，這也可能包括根據 UUID 值管理群組。

核心組態

執行核心 ONTAP 組態需要三個主要步驟、包括：

- 您也可以為簽署授權伺服器憑證的 CA 安裝根憑證（及任何中繼憑證）。

- 定義授權伺服器。
- 啟用叢集的 OAuth 2.0 處理。

在 **ONTAP** 中部署 **OAuth 2.0**

部署核心 OAuth 2.0 功能需要三個主要步驟。

開始之前

您必須準備 OAuth 2.0 部署、才能設定 ONTAP 。例如、您需要評估授權伺服器、包括其憑證的簽署方式、以及它是否位於防火牆的後方。請參閱 "準備使用 ONTAP 部署 OAuth 2.0" 以取得更多資訊。

步驟 **1** ：安裝授權伺服器根 **CA** 憑證

ONTAP 包含大量預先安裝的根 CA 憑證。因此、在許多情況下、 ONTAP 會立即辨識您的授權伺服器憑證、而無需額外設定。但視授權伺服器憑證的簽署方式而定、您可能需要安裝根 CA 憑證和任何中繼憑證。

如有需要、請依照下列指示安裝憑證。您應該在叢集層級安裝所有必要的憑證。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **26.** 步驟

系統管理員

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

CLI

1. 開始安裝：

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

2. 查看下列主控台訊息：

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

3. 使用文字編輯器開啟憑證檔案。
4. 複製整個憑證、包括下列幾行：

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

5. 在命令提示字元之後、將憑證貼到終端機。
6. 按 **Enter** 鍵完成安裝。
7. 使用下列其中一項來確認已安裝憑證：

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

   ```
   security certificate show
   ```

步驟 **2** ：設定授權伺服器

您需要定義至少一個 ONTAP 授權伺服器。您應該根據組態和部署計畫來選擇參數值。檢閱 "OAuth2 部署案例" 以判斷您的組態所需的確切參數。

若要修改授權伺服器定義、您可以刪除現有定義並建立新定義。

以下提供的範例是根據第一個簡單部署案例、網址為： "本機驗證"。不使用 Proxy 就能使用獨立的範圍。

根據您存取 ONTAP 的方式、選擇正確的程序。CLI 程序會使用您在發出命令之前需要置換的符號變數。

範例 **27.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性 * 區段。
3. 按一下 * oAuth 2.0 授權 * 旁的 * + * 。
4. 選擇 * 更多選項 * 。
5. 提供部署所需的值、例如：
   - 名稱
   - 應用程式（ http ）
   - 提供者 JWKS URI
   - 發卡行 URI
6. 按一下「 * 新增 * 」。

CLI

1. 再次建立定義：

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

例如：

```
security oauth2 client create \
-config-name auth0 \
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-
realm/protocol/openid-connect/certs \
-application http \
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

如"指令參考資料ONTAP"需詳細 `security oauth2 client create`資訊，請參閱。

步驟 **3** ：啟用 **OAuth 2.0**

最後一步是啟用 OAuth 2.0 。這是 ONTAP 叢集的全域設定。

在您確認 ONTAP 、授權伺服器及任何支援服務均已正確設定之前、請勿啟用 OAuth 2.0 處理。

根據您存取 ONTAP 的方式、選擇正確的程序。

範例 **28.** 步驟

系統管理員

1. 在 System Manager 中，選擇 **Cluster** >* Settings* 。
2. 向下捲動至 * 安全性區段 * 。
3. 按一下 **OAuth 2.0** 授權 * 旁邊的 *→ 。
4. 啟用 * oAuth 2.0 授權 * 。

CLI

1. 啟用 OAuth 2.0 ：

```
security oauth2 modify -enabled true
```

2. 確認 OAuth 2.0 已啟用：

```
security oauth2 show
Is OAuth 2.0 Enabled: true
```

相關資訊

- "安全性憑證安裝"
- "安全證書展示"
- "安全oauth2修改"
- "安全 oauth2 顯示"

使用 **OAuth 2.0** 發出**ONTAP REST API** 呼叫

ONTAP 中的 OAuth 2.0 實作支援 REST API 用戶端應用程式。您可以使用 Curl 發出簡單的 REST API 呼叫、開始使用 OAuth 2.0 。以下範例擷取 ONTAP 叢集版本。

開始之前

您必須為 ONTAP 叢集設定並啟用 OAuth 2.0 功能。這包括定義授權伺服器。

步驟 **1** ：取得存取權杖

您必須取得存取權杖、才能與 REST API 呼叫搭配使用。權杖要求是在 ONTAP 之外執行、具體程序取決於授權伺服器及其組態。您可以透過網頁瀏覽器、使用 cURL 命令或使用程式設計語言來要求權杖。

以下是使用捲曲向 Keycloak 申請存取權杖的範例。

Keycloak 範例

```
curl --request POST \
--location
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-
connect/token' \
--header 'Content-Type: application/x-www-form-urlencoded' \
--data-urlencode 'client_id=dp-client-1' \
--data-urlencode 'grant_type=client_credentials' \
--data-urlencode 'client_secret=5iTUf9QKLGxAoYa1iR33vlD5A2xq09V7'
```

您應該複製並儲存傳回的權杖。

步驟 **2** ：發出 **REST API** 呼叫

擁有有效的存取權杖之後、您可以使用具有存取權杖的 cURL 命令來發出 REST API 呼叫。

參數與變數

下表說明了捲髮範例中的兩個變數。

變動	說明
$FQDN_IP	ONTAP 管理 LIF 的完整網域名稱或 IP 位址。
$access_token	由授權伺服器發出的 OAuth 2.0 存取權杖。

您應該先在 Bash Shell 環境中設定這些變數、然後再發佈 Curl 範例。例如、在 Linux CLI 中、輸入下列命令以設定及顯示 FQDN 變數：

```
FQDN_IP=172.14.31.224
echo $FQDN_IP
172.14.31.224
```

在本機 Bash Shell 中定義兩個變數之後、您可以複製 curl 命令並將其貼到 CLI 中。按 **Enter** 以替換變數並發出命令。

Curl範例

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=version" \
--include \
--header "Accept: */*" \
--header "Authorization: Bearer $ACCESS_TOKEN"
```

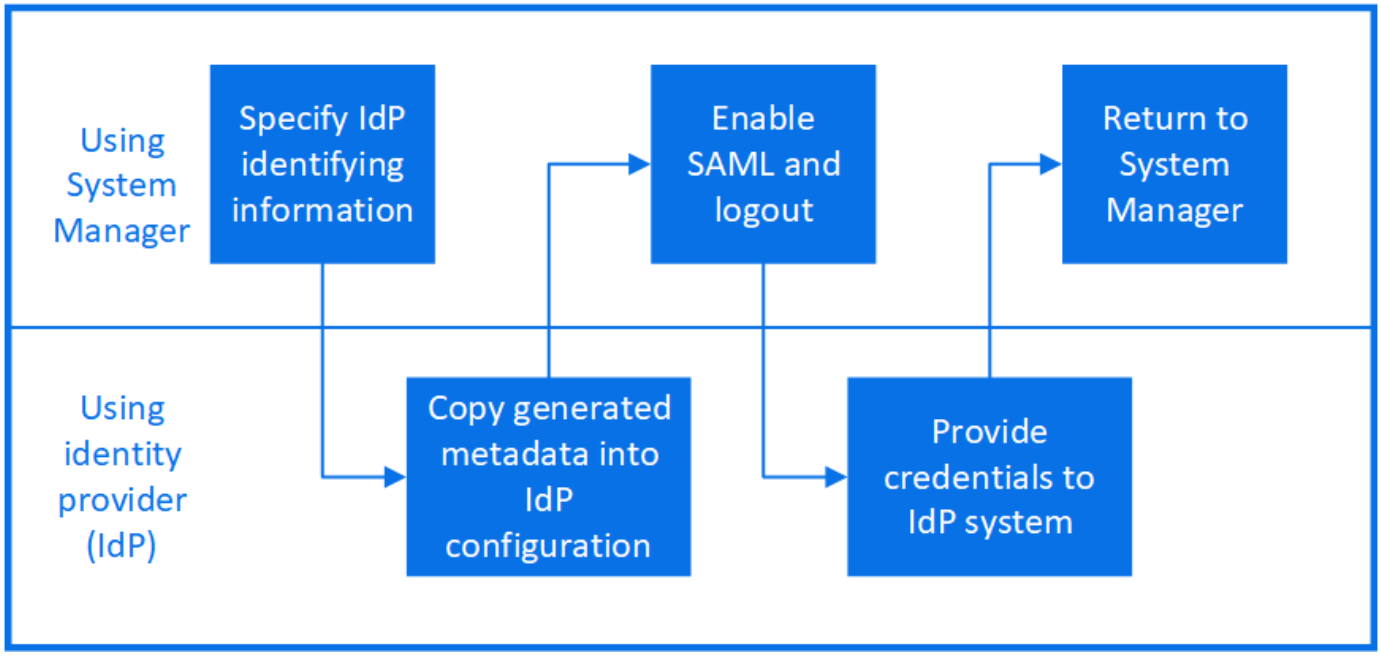
為遠端ONTAP用戶設定 SAML 身份驗證

從ONTAP 9.3 開始，您可以為 Web 服務設定安全性斷言標記語言 (SAML) 驗證。設定並啟用 SAML 驗證後，使用者將透過外部身分提供者 (IdP) 進行身份驗證，而不是透過 Active Directory 和 LDAP 等目錄服務提供者進行驗證。停用 SAML 驗證後，將使用已設定的目錄服務提供者（例如 Active Directory 和 LDAP）進行驗證。

啟用SAML驗證

若要使用 System Manager 或 CLI 啟用 SAML 驗證、請執行下列步驟。如果您的叢集執行的是 ONTAP 9.7 或更早版本、則您需要遵循的系統管理員步驟會有所不同。請參閱系統上的 System Manager 線上說明。

啟用 SAML 身份驗證後，只有已配置了 SAML 身份驗證的遠端使用者才能存取系統管理員 GUI。啟用 SAML 身份驗證後，本機使用者將無法存取系統管理員 GUI。



關於這項工作

- SAML 驗證僅適用於ONTAP `http`和 `ontapi`應用程式.

  這 `http`和 `ontapi`應用程式由下列 Web 服務使用：服務處理器基礎架構、 ONTAP API 和系統管理員。

- SAML驗證僅適用於存取管理SVM。
- 從ONTAP 9.17.1 開始，IdP 提供的群組資訊可以對應到ONTAP角色。這樣，您就可以根據 IdP 中定義的群組為使用者指派角色。有關更多信息，請參閱"在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組" 。

下列 IDP 已通過 System Manager 驗證：

- Microsoft Entra ID（已通過ONTAP 9.17.1 及更高版本驗證）
- Active Directory Federation Services
- Cisco Duo（已通過以下ONTAP版本驗證：）

- 9.7P21 及更新版本 9.7 版本（請參閱 "System Manager Classic 文件"）
- 9.8P17 及更高版本的 9.8 補丁版本
- 9.9.1P13 及更高版本的 9.9.1 補丁版本
- 9.10.1P9 及更高版本的 9.10.1 補丁版本
- 9.11.1P4 及更高版本的 9.11.1 補丁版本
- 9.12.1 及更新版本

- Shibboleth

開始之前

- 您計劃用於遠端驗證的 IdP 必須是 配置.您必須擁有 IdP 的 URI。 IdPURI 是ONTAP向其發送身份驗證請求並接收回應的 Web 位址
- ONTAP叢集和 IdP 之間必須開啟連接埠 443。
- ONTAP叢集和 IdP 必須能夠 ping 通對方的完全限定域名。確保 DNS 配置正確，且叢集憑證未過期。
- 如果需要，請將 IdP 的受信任憑證授權單位 (CA) 新增至ONTAP。您可以"使用系統管理員管理ONTAP證書"。您可能需要在 IdP 中設定ONTAP叢集憑證。
- 您必須能夠存取ONTAP叢集的"服務處理器（SP）"控制台。如果 SAML 設定錯誤，則需要從SP控制台將其停用。
- 如果您使用的是 Entra ID（從ONTAP 9.17.1 開始已驗證），則必須在建立ONTAP SAML 設定之前使用ONTAP元資料配置 Entra ID。 EntraID 只有在配置了ONTAP元資料後才會提供 IdP URI。建立ONTAP SAML 配置需要 IdP URI。

  - 如果您使用 System Manager 設定 SAML，請將 IdP URI 欄位留空，直到 System Manager 提供ONTAP元資料。使用ONTAP元資料配置 Entra ID，然後將 IdP URI 複製到 System Manager 中，然後再啟用 SAML 設定。
  - 如果您使用ONTAP CLI 設定 SAML，則必須先生成ONTAP元數據，然後才能啟用ONTAP SAML 設定。您可以使用以下命令產生ONTAP元資料檔：

    ```
    security saml-sp default-metadata create -sp-host <ontap_host_name>
    ```

    `ontap_host_name`是 SAML 服務提供者主機（在本例中為ONTAP系統）的主機名稱或 IP 位址。預設情況下，使用叢集管理 IP 位址。您可以選擇提供ONTAP伺服器憑證資訊。預設情況下，使用ONTAP Web 伺服器憑證資訊。

  使用提供的元資料配置 Entra ID。您必須在建立ONTAP SAML 設定之前設定 Entra ID。配置 Entra 後，繼續執行下列 CLI 程序。

  - 在叢集中的所有節點都達到版本 9.17.1 之前，您無法產生 Entra ID 的ONTAP元資料。

步驟

視您的環境而定、請執行下列步驟：

系統管理員

1. 按一下*叢集>設定*。
2. 在 * SAML 驗證 * 旁邊、按一下 ⚙ 。
3. 請確認「啟用**SAML**驗證」核取方塊已勾選。
4. 輸入 IdP URI 的 URL（包括"https://" ）。如果您使用Entra ID，請跳過此步驟。
5. 如果需要，請修改主機系統位址。這是 IdP 在身份驗證後將定向到的地址。預設值為群集管理 IP 位址。
6. 確保使用正確的憑證：
   - 如果您的系統只對應一個類型為「server」的憑證、則該憑證會被視為預設憑證、不會顯示出來。
   - 如果您的系統已對應多個憑證做為「server」類型、則會顯示其中一個憑證。 若要選取不同的憑證、請按一下*變更*。
7. 按一下「 * 儲存 * 」。確認視窗會顯示已自動複製到剪貼簿的中繼資料資訊。
8. 前往您指定的 IdP 系統，並從剪貼簿複製元資料以更新系統元資料。如果您使用的是 Entra ID，請在使用系統元資料配置 Entra ID 後，將 IdP URI 複製到ONTAP中。
9. 返回確認視窗（在System Manager中）、然後勾選「I have configured the IDP with the host URI or medetid*（我已使用主機URI或中繼資料*設定IDP）」核取方塊。
10. 按一下*登出*以啟用SAML型驗證。 IDP系統會顯示驗證畫面。
11. 在 IdP 登入頁面，輸入您的基於 SAML 的憑證。憑證驗證完成後，您將被導向到系統管理器主頁。

CLI

1. 建立SAML組態、ONTAP 以便讓整個程序能夠存取IDP中繼資料：

   ```
   security saml-sp create -idp-uri <idp_uri> -sp-host <ontap_host_name>
   ```

   `idp_uri` 是 IDP 主機的 FTP 或 HTTP 位址、可從其中下載 IDP 中繼資料。

   > ⓘ 某些 URL 包含問號 (?)。問號用於啟動ONTAP命令列活動幫助。要輸入帶有問號的URL，您需要先使用以下命令停用活動協助 `set -active-help false` 。稍後可以使用以下命令重新啟用主動協助 `set -active-help true`了解更多信息"指令參考資料ONTAP" 。

   `ontap_host_name` 是 SAML 服務供應商主機的主機名稱或 IP 位址、在此情況下為 ONTAP 系統。根據預設、會使用叢集管理LIF的IP位址。

   您可以選擇性地提供ONTAP 伺服器的驗證資訊。根據預設ONTAP 、會使用「驗證」Web伺服器憑證資訊。

```
cluster_12::> security saml-sp create -idp-uri
https://example.url.net/idp/shibboleth

Warning: This restarts the web server. Any HTTP/S connections that
are active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and ONTAP users for the same directory server
domain to ensure that users are the same for different
authentication methods. See the "security login show" command for
the ONTAP user configuration.
```

畫面ONTAP 會顯示存取主機中繼資料的URL。

2. 從 IdP 主機， 配置 IdP使用ONTAP主機元資料。如果您使用的是 Entra ID，則已完成此步驟。
3. 配置 IdP 後，啟用 SAML 設定：

   ```
   security saml-sp modify -is-enabled true
   ```

   存取的任何現有使用者 `http` 或 `ontapi` 應用程式會自動設定以進行 SAML 驗證。

4. 如果你想為 `http`或者 `ontapi`設定 SAML 後，請將 SAML 指定為新使用者的驗證方法。在ONTAP 9.17.1 之前的版本中，系統會自動為現有使用者建立 SAML 登入名 `http`或者 `ontapi`啟用 SAML 時，使用者必須設定新使用者。從ONTAP 9.17.1 開始，所有使用 `password ， domain ， 或者 `nsswitch`當啟用 SAML 時，身份驗證方法會自動針對 IdP 進行身份驗證。

   a. 為新使用者建立使用 SAML 驗證的登入方法。 `user_name`必須與 IdP 中配置的使用者名稱相符：

      該 `user_name`值區分大小寫。除非您使用 Entra ID ，否則請僅包含使用者名稱，不要包含網域的任何部分。如果您使用 Entra ID ，則可以建立包含網域的使用者名稱，例如 *user_name@domain.com* 。

      ```
      security login create -user-or-group-name <user_name> -application [http
      | ontapi] -authentication-method saml -vserver <svm_name>
      ```

      範例：

      ```
      cluster_12::> security login create -user-or-group-name admin1
      -application http -authentication-method saml -vserver cluster_12
      ```

   b. 確認已建立使用者項目：

security login show

範例：

```
cluster_12::> security login show

Vserver: cluster_12

Second
User/Group                  Authentication                 Acct
Authentication
Name            Application Method        Role Name        Locked
Method
--------------- ----------- ------------- ---------------- ------
--------------
admin           console     password      admin            no
none
admin           http        password      admin            no
none
admin           http        saml          admin            -
none
admin           ontapi      password      admin            no
none
admin           ontapi      saml          admin            -
none
admin           service-processor
                            password      admin            no
none
admin           ssh         password      admin            no
none
admin1          http        password      backup           no
none
admin1          http        saml          backup           -
none
```

+
如"指令參考資料ONTAP"需詳細 `security login show`資訊，請參閱。

停用SAML驗證

當您想要停止使用外部身分提供者 (IdP) 對遠端系統管理員使用者進行驗證時，可以停用 SAML 驗證。停用 SAML 驗證後，系統將使用本機使用者驗證或已設定的目錄服務提供者（例如 Active Directory 和 LDAP）對使用者進行驗證。

視您的環境而定、請執行下列步驟：

範例 **29.** 步驟

系統管理員

1. 按一下*叢集>設定*。
2. 在「* SAML驗證*」下、按一下「已啟用」切換按鈕。
3. *Optional* ：您也可以按一下 * SAML 驗證 * 旁的、然後取消勾選 * 啟用 SAML 驗證 * 核取方塊。

CLI

1. 停用SAML驗證：

   ```
   security saml-sp modify -is-enabled false
   ```

2. 如果您不想再使用SAML驗證、或想要修改IDP、請刪除SAML組態：

   ```
   security saml-sp delete
   ```

配置第三方 IdP

關於這項工作

為了使用ONTAP進行身份驗證，您可能需要變更 IdP 的設定。以下部分提供了受支援的 IdP 的配置資訊。

entra ID

配置 Entra ID 時，建立一個新的應用程序，並使用ONTAP提供的元資料配置 SAML 登入。建立應用程式後，編輯應用程式 SAML 設定的「屬性和聲明」部分，以符合以下內容：

設定	價值
名稱	urn：oid：0.9.2342.19200300.100.1.1
命名空間	留空
名稱格式	URI
來源	屬性
來源屬性	使用者.使用者主體名稱

如果您想使用具有 Entra ID 的群組，請使用下列設定新增群組聲明：

設定	價值
名稱	urn：oid：1.3.6.1.4.1.5923.1.5.1.1
命名空間	留空
來源屬性	群組ID

Entra ID 以 UUID 格式提供群組資訊。有關使用 Entra ID 群組的更多信息，請參閱"使用 UUID 管理群組"。

應用程式 SAML 設定的「SAML 憑證」部分中提供的「應用程式聯合元資料 URL」是您將在ONTAP中輸入的 IdP URI。

有關配置 Entra ID 多因素身份驗證的信息，請參閱"規劃 Microsoft Entra 多重驗證部署"。

欲了解更多信息，請參閱"Entra ID 文件"。

Active Directory Federation Services

設定 Active Directory 聯合驗證服務 (AD FS) 時，必須使用ONTAP提供的服務提供者元資料新增的可感知聲明的依賴方信任。建立依賴方信任後，使用「將 LDAP 屬性作為聲明傳送」範本將下列聲明規則新增至依賴方信任的聲明頒發策略：

屬性儲存	**LDAP** 屬性	傳出索賠類型
Active Directory	SAM 帳戶名稱	姓名 ID
Active Directory	SAM 帳戶名稱	urn：oid：0.9.2342.19200300.100.1.1
Active Directory	名稱格式	urn:oasis:names:tc:SAML:2.0:attrname-format:uri
Active Directory	令牌組 - 按網域限定	urn：oid：1.3.6.1.4.1.5923.1.5.1.1
Active Directory	sAM帳戶名稱	urn:oid:1.2.840.113556.1.4.221

AD FS 以名稱格式提供群組資訊。有關在 AD FS 中使用群組的更多信息，請參閱"使用名稱管理群組"。

欲了解更多信息，請參閱"AD FS 文檔" 。

Cisco DuoTM

請參閱"Cisco Duo 文件"取得配置資訊。

Shibboleth

在設定 Shibboleth IdP 之前，您必須已經設定了 LDAP 伺服器。

在ONTAP上啟用 SAML 時，請儲存提供的主機元資料 XML。在安裝了 Shibboleth 的主機上，將以下內容替換為 `metadata/sp-metadata.xml`使用 Shibboleth IdP 主目錄中的主機元資料 XML。

有關詳細信息，請參閱"Shibboleth" 。

疑難排解SAML組態問題

如果設定安全性聲明標記語言（SAML）驗證失敗、您可以手動修復SAML組態失敗的每個節點、並從故障中恢復。在修復程序期間、會重新啟動Web伺服器、並中斷任何作用中的HTTP連線或HTTPS連線。

關於這項工作

設定SAML驗證時ONTAP 、將會以每個節點為基礎來套用SAML組態。啟用SAML驗證時ONTAP 、如果發生組態問題、則會自動嘗試修復每個節點。如果任何節點上的SAML組態發生問題、您可以停用SAML驗證、然後重新啟用SAML驗證。在重新啟用SAML驗證後、SAML組態仍無法套用至一或多個節點的情況下、可能會發生。您可以識別SAML組態失敗的節點、然後手動修復該節點。

步驟

1. 登入進階權限層級：

   ```
   set -privilege advanced
   ```

2. 識別SAML組態失敗的節點：

   ```
   security saml-sp status show -instance
   ```

   範例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                 Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                 Update Status: config-failed
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `security saml-sp status show`資訊，請參閱。

3. 修復故障節點上的SAML組態：

   `security saml-sp repair -node <node_name>`

   範例：

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
         will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

   Web伺服器會重新啟動、且任何作用中的HTTP連線或HTTPS連線都會中斷。

   如"指令參考資料ONTAP"需詳細 `security saml-sp repair`資訊，請參閱。

4. 確認已在所有節點上成功設定SAML：

   `security saml-sp status show -instance`

   範例：

```
cluster_12::*> security saml-sp status show -instance

                          Node: node1
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                          Node: node2
                Update Status: config-success
               Database Epoch: 9
   Database Transaction Count: 997
                   Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

如"指令參考資料ONTAP"需詳細 `security saml-sp status show`資訊，請參閱。

相關資訊

- "指令參考資料ONTAP"
- "安全性 SAML SP"
- "建立安全登入"

在ONTAP中使用 OAuth 2.0 或 SAML IdP 群組

ONTAP提供了多種基於 OAuth 2.0 授權伺服器或 SAML 身分提供者 (IdP) 設定群組的選項。然後，可以將這些群組對應到ONTAP用於確定存取權限的角色。

從ONTAP 9.17.1 開始，SAML IdP 提供的群組資訊可以對應到ONTAP角色。這樣，您就可以根據 IdP 中定義的群組為使用者指派角色。如需詳細資訊，請參閱"設定SAML驗證"。從ONTAP 9.14.1 開始， ONTAP支援 OAuth 2.0 的群組名稱驗證。從ONTAP 9.16.1 開始， ONTAP支援 OAuth 2.0 群組 UUID 驗證和角色對應。"ONTAP OAuth 2.0 實作總覽" 。

如何識別群組

在授權伺服器或 SAML IdP 上設定群組時，系統會使用名稱或 UUID 在 OAuth 2.0 存取權杖或 SAML 斷言中識別並攜帶該群組。在設定ONTAP之前，您需要了解授權伺服器或 SAML IdP 如何處理群組。

如果存取權杖中包含多個群組， ONTAP 會嘗試使用每個群組，直到有相符項目為止。

群組名稱

許多授權伺服器和 SAML IdP（例如 Active Directory Federation Service (ADFS)）都使用名稱來識別和表示群組。以下是 ADFS 產生的包含多個群組的 JSON OAuth 2.0 存取權杖片段。請參閱[使用名稱管理群組]了解更多。

```
...
"sub": "User1_TestDev@NICAD5.COM",
"group": [
  "NICAD5\\Domain Users",
  "NICAD5\\Development Group",
  "NICAD5\\Production Group"
],
"apptype": "Confidential",
"appid": "3bff3b2b-8e40-44ba-7c11-d73c3b76e3e8",
...
```

群組 **UUID**

一些授權伺服器和 SAML IdP（例如 Microsoft Entra ID）使用 UUID 來識別和表示群組。以下是 Entra ID 產生的包含多個群組的 OAuth 2.0 存取權杖片段。請參閱使用 UUID 管理群組了解更多。

```
...
"appid": "4aff4b4b-8e40-44ba-7c11-d73c3b76e3d7",
"appidacr": "1",
"groups": [
  "8ea4c5b0-bcad-4e66-8f1e-cd395474a448",
  "a8558fc2-a1b2-4cb7-cc41-59bd831840cc"],
"name": "admin007 with group membership",
...
```

使用名稱管理群組

如果您的授權伺服器或 SAML IdP 使用名稱來識別群組，則需要確保已為ONTAP叢集定義了每個群組。根據您的安全環境，您可能已經定義了相應的群組。

以下是定義ONTAP組的 CLI 指令範例。請注意，它使用範例存取令牌中的命名組。您需要具有ONTAP 管理員權限等級才能發出該指令。

範例

```
security login create -user-or-group-name "NICAD5\\Domain Users"
-application http -authentication-method domain -role admin
```

使用 `-authentication-method` `domain`或者 `nsswitch`用於 SAML IdP 和 OAuth 2.0 授權伺服器群組。

您也可以使用ONTAP REST API 來設定此功能。了解更多信息，請參閱 "ONTAP 自動化文件" 。

使用 UUID 管理群組

如果您的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則在使用群組之前需要執行兩步驟設定。從ONTAP 9.16.1 開始，提供了兩種映射功能，並且已使用 Entra ID 進行測試。從ONTAP 9.16.1 開始支援 OAuth 2.0 的 Entra ID，從ONTAP 9.17.1 開始支援 SAML 的 Entra ID。您需要具有ONTAP 管理員 權限等級才能發出 CLI 命令。

您也可以使用 ONTAP REST API 來設定這些功能。如需詳細資訊，請參閱 "ONTAP 自動化文件"。

將群組 UUID 對應至群組名稱

如果您使用的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則需要將群組 UUID 對應到群組名稱。主要的ONTAP CLI 操作如下所述。

建立

您可以使用以下方式定義新的群組映射配置 `security login group create`命令。群組 UUID 和名稱應與授權伺服器或 SAML IdP 上的設定相符。詳細了解 `security login group create`在"指令參考資料ONTAP" 。

參數

用於建立群組對應的參數如下所述。

參數	說明
`vserver`	選擇性地指定群組所關聯的 SVM （ Vserver ）名稱。如果省略，群組就會與 ONTAP 叢集相關聯。
`name`	ONTAP 將使用的群組唯一名稱。
`type`	此值表示群組來源的身分識別提供者。
`uuid`	指定授權伺服器或 SAML IdP 提供的群組的通用唯一識別碼。

以下是為ONTAP定義群組的範例 CLI 指令。請注意，它使用範例存取令牌中的 UUID 群組。

範例

```
security login group create -vserver ontap-cls-1 -name IAM_Dev -type entra
-uuid 8ea4c5b0-bcad-4e66-8f1e-cd395474a448
```

建立群組之後，會為群組產生唯一的唯讀整數識別碼。

其他 CLI 作業

此命令支援多項額外作業，包括：

- 顯示

- 修改
- 刪除

您可以使用 `show`選項來擷取為群組所產生的唯一群組 ID 。如"指令參考資料ONTAP"需詳細 `show`資訊，請參閱。

將群組 **UUID** 對應至角色

如果您使用的授權伺服器或 SAML IdP 使用 UUID 值來表示群組，則可以將群組對應到角色。如需 ONTAP 中基於角色的存取控制的詳細資訊，請參閱 "瞭解如何管理 ONTAP 存取控制角色"。主要的ONTAP CLI 操作如下所述。需要具有ONTAP **admin** 權限等級才能發出這些命令。

> 你需要先將群組 UUID 對應到群組名並檢索為該組產生的唯一整數 ID。您需要該 ID 來將群組對應到角色。

建立

您可以使用 `security login group role-mapping create`命令。詳細了解 `security login group role-mapping create`在"指令參考資料ONTAP" 。

參數

用於將群組對應至角色的參數如下所述。

參數	說明
`group-id`	指定使用命令為群組產生的唯一 ID `security login group create` 。
`role`	群組對應的 ONTAP 角色名稱。

範例

```
security login group role-mapping create -group-id 1 -role admin
```

其他 **CLI** 作業

此命令支援多項額外作業，包括：

- 顯示
- 修改
- 刪除

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

相關資訊

- "外部角色對應"

使用 **WebAuthn MFA** 進行驗證與授權

了解 **ONTAP System Manager** 使用者的 **WebAuthn** 多因素驗證

從 ONTAP 9 。 16.1 開始，系統管理員可以為登入系統管理員的使用者啟用 WebAuthn 多因素驗證（ MFA ）。這可讓系統管理員以 FIDO2 金鑰（例如 YibiKey ）作為第二種驗證形式登入。根據預設，新的和現有的 ONTAP 使用者會停用 WebAuthn MFA 。

第一種驗證方法使用下列驗證類型的使用者和群組可支援 WebAuthn MFA ：

- 使用者：密碼，網域或 nsswitch
- 群組：網域或 nsswitch

當您將 WebAuthn MFA 啟用為使用者的第二種驗證方法之後，系統會要求使用者在登入 System Manager 時登錄硬體驗證者。註冊後，私密金鑰會儲存在驗證者中，而公開金鑰則儲存在 ONTAP 中。

ONTAP 支援每位使用者一個 WebAuthn 認證。如果使用者遺失驗證者，需要更換驗證者，則 ONTAP 管理員需要刪除使用者的 WebAuthn 認證，以便使用者在下次登入時註冊新的驗證者。

> 啟用 WebAuthn MFA 做為第二種驗證方法的使用者"https://192.168.100.200"，必須使用 FQDN （例如"https://myontap.example.com"）而非 IP 位址（例如）來存取 System Manager 。對於啟用 WebAuthn MFA 的使用者，會拒絕使用 IP 位址登入 System Manager 的嘗試。

為 **ONTAP** 系統管理員使用者或群組啟用 **WebAuthn MFA**

身為 ONTAP 管理員，您可以新增已啟用 WebAuthn MFA 選項的新使用者或群組，或是啟用現有使用者或群組的選項，為系統管理員使用者或群組啟用 WebAuthn MFA 。

> 將 WebAuthn MFA 啟用為使用者或群組的第二種驗證方法之後，下次登入 System Manager 時，系統會要求使用者（或該群組中的所有使用者）登錄硬體 FIDO2 裝置。此登錄由使用者的本機作業系統處理，通常包括插入安全金鑰，建立金鑰，以及輕觸安全金鑰（如果支援）。

建立新使用者或群組時，請啟用 **WebAuthn MFA**

您可以使用系統管理員或 ONTAP CLI ，建立啟用 WebAuthn MFA 的新使用者或群組。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在 * 使用者 * 下選取 * 新增 * 。
4. 指定使用者或群組名稱，然後在 * 角色 * 的下拉式功能表中選取角色。
5. 指定使用者或群組的登入方法和密碼。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

6. 在 **MFA for HTTP** 欄中，選取 * Enabled* 。
7. 選擇*保存*。

CLI

1. 啟用 WebAuthn MFA ，建立新的使用者或群組。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

   ```
   security login create -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

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

為現有的使用者或群組啟用 **WebAuthn MFA**

您可以為現有的使用者或群組啟用 WebAuthn MFA 。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯之使用者或群組的選項功能表。

   WebAuthn MFA 支援使用者的「密碼」，「網域」或「 nsswitch 」登入方法，以及群組的「網域」或「 nsswitch 」登入方法。

4. 在該使用者的 * MFA for HTTP* 欄中，選取 * Enabled* 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，為該使用者或群組啟用 WebAuthn MFA 。

   在下列範例中，選擇第二種驗證方法的「 publickey 」即可啟用 WebAuthn MFA ：

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method publickey \
                         -application http \
                         -role admin
   ```

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

停用 **ONTAP System Manager** 使用者的 **WebAuthn MFA**

身為 ONTAP 管理員，您可以使用系統管理員或 ONTAP CLI 編輯使用者或群組，為使用者或群組停用 WebAuthn MFA 。

停用現有使用者或群組的 **WebAuthn MFA**

您可以隨時停用現有使用者或群組的 WebAuthn MFA 。

> 如果停用已登錄的認證，則會保留認證。如果您在未來再次啟用認證，則會使用相同的認證，因此使用者在登入時不需要重新登錄。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，選取您要編輯的使用者或群組。
4. 在該使用者的 * MFA for HTTP* 欄中，選取 * 停用 * 。
5. 選擇*保存*。

CLI

1. 修改現有的使用者或群組，以停用該使用者或群組的 WebAuthn MFA 。

   在下列範例中，選擇「無」作為第二種驗證方法，即可停用 WebAuthn MFA 。

   ```
   security login modify -user-or-group-name <user_or_group_name> \
                         -authentication-method domain \
                         -second-authentication-method none \
                         -application http \
                         -role admin
   ```

   如"指令參考資料ONTAP"需詳細 `security login modify`資訊，請參閱。

檢視 **ONTAP WebAuthn MFA** 設定並管理認證

身為 ONTAP 管理員，您可以檢視整個叢集的 WebAuthn MFA 設定，並管理 WebAuthn MFA 的使用者和群組認證。

檢視 **WebAuthn MFA** 的叢集設定

您可以使用 ONTAP CLI 檢視 WebAuthn MFA 的叢集設定。

步驟

1. 檢視 WebAuthn MFA 的叢集設定。您可以選擇使用下列引數指定儲存 VM `vserver` ：

   ```
   security webauthn show -vserver <storage_vm_name>
   ```

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

檢視支援的公開金鑰 **WebAuthn MFA** 演算法

您可以檢視儲存 VM 或叢集所支援的 WebAuthn MFA 公開金鑰演算法。

步驟

1. 列出支援的公開金鑰 WebAuthn MFA 演算法。您可以選擇使用下列引數指定儲存 VM `vserver` ：

```
security webauthn supported-algorithms show -vserver <storage_vm_name>
```

如"指令參考資料ONTAP"需詳細 `security webauthn supported-algorithms show`資訊，請參閱。

檢視已註冊的 **WebAuthn MFA** 認證

身為 ONTAP 管理員，您可以檢視所有使用者的註冊 WebAuthn 認證。使用此程序的非系統管理員使用者只能檢視自己已註冊的 WebAuthn 認證。

步驟

1. 檢視已註冊的 WebAuthn MFA 認證：

```
security webauthn credentials show
```

如"指令參考資料ONTAP"需詳細 `security webauthn credentials show`資訊，請參閱。

移除已註冊的 **WebAuthn MFA** 認證

您可以移除已註冊的 WebAuthn MFA 認證。當使用者的硬體金鑰遺失，遭竊或不再使用時，此功能非常實用。當使用者仍擁有原始硬體驗證者，但想要以新的驗證者來取代時，您也可以移除已登錄的認證。移除認證之後，系統會提示使用者註冊替換驗證者。

移除使用者的登錄認證並不會停用使用者的 WebAuthn MFA 。如果使用者遺失硬體驗證者，需要先登入再進行更換，您需要使用這些步驟移除認證，也需要針對使用者移除認證"停用 WebAuthn MFA"。

系統管理員

1. 選擇*叢集>設定*。
2. 選取 * 使用者和角色 * 旁邊的箭頭圖示。
3. 在使用者和群組清單中，針對您要移除其認證的使用者或群組，選取選項功能表。
4. 選取 * 移除 MFA 以取得 HTTP 認證 * 。
5. 選擇*移除*。

CLI

1. 刪除已註冊的認證。請注意下列事項：
   - 您可以選擇性地指定使用者的儲存 VM 。如果省略，則會在叢集層級移除認證。
   - 您可以選擇性地指定要刪除認證的使用者名稱。如果省略，則會移除目前使用者的認證。

   ```
   security webauthn credentials delete -vserver <storage_vm_name>
   -username <username>
   ```

   如"指令參考資料ONTAP"需詳細 `security webauthn credentials delete`資訊，請參閱。

管理Web服務

管理網路服務總覽

您可以啟用或停用叢集或儲存虛擬機器（SVM）的Web服務、顯示Web服務的設定、以及控制角色使用者是否可以存取Web服務。

您可以使用下列方式來管理叢集或SVM的Web服務：

- 啟用或停用特定的Web服務
- 指定是否僅限加密的HTTP（SSL）存取Web服務
- 顯示Web服務的可用度
- 允許或禁止角色使用者存取Web服務
- 顯示允許存取Web服務的角色

若要讓使用者存取Web服務、必須符合下列所有條件：

- 使用者必須通過驗證。

  例如、Web服務可能會提示輸入使用者名稱和密碼。使用者的回應必須符合有效的帳戶。

- 使用者必須使用正確的存取方法來設定。

  驗證只會針對使用者成功、並針對指定的Web服務提供正確的存取方法。適用於 ONTAP API Web 服務

ontapi）、使用者必須擁有 ontapi 存取方法。對於所有其他 Web 服務、使用者必須擁有 http 存取方法。

> 您可以使用 security login 管理使用者存取方法和驗證方法的命令。

- Web服務必須設定為允許使用者的存取控制角色。

> 您可以使用 vserver services web access 控制角色存取 Web 服務的命令。

如果啟用防火牆、則必須設定用於Web服務的LIF防火牆原則、以允許HTTP或HTTPS。

如果您使用HTTPS進行Web服務存取、也必須啟用提供Web服務之叢集或SVM的SSL、而且必須提供叢集或SVM的數位憑證。

管理對ONTAP Web 服務的訪問

Web服務是使用者可以使用HTTP或HTTPS存取的應用程式。叢集管理員可以設定Web傳輸協定引擎、設定SSL、啟用Web服務、以及讓角色的使用者存取Web服務。

從支援下列Web服務的支援範圍ONTAP 起、從功能支援的9.6開始：

- 服務處理器基礎架構 (spi)

  此服務可透過叢集管理LIF或節點管理LIF、讓節點的記錄檔、核心傾印檔和MIBA檔案可供HTTP或HTTPS存取。預設設定為 enabled。

  當請求存取節點的日誌檔案或核心轉儲檔案時， spi Web 服務會自動建立一個從一個節點到另一個節點的根磁碟區（檔案所在的根磁碟區）的掛載點。您無需手動建立掛載點。

- ONTAP API (ontapi)

  這項服務可讓您執行ONTAP IsyAPI、以遠端程式執行管理功能。預設設定為 enabled。

  某些外部管理工具可能需要此服務。例如、如果您使用System Manager、則應保持啟用此服務。

- Data ONTAP 探索 (disco)

  此服務可讓隨裝即用的管理應用程式在網路中探索叢集。預設設定為 enabled。

- 支援診斷 (supdiag)

  此服務可控制系統上的權限環境存取、以協助進行問題分析和解決問題。預設設定為 disabled。您只能在技術支援人員的指示下啟用此服務。

- 系統管理員 (sysmgr)

  此服務可控制系統管理員的可用度、ONTAP 而此功能隨附於本服務。預設設定為 enabled。此服務僅在叢集上受支援。

- 韌體基礎板管理控制器（ BMC ）更新 (FW_BMC)

此服務可讓您下載BMC韌體檔案。預設設定為 `enabled`。

- 資訊文件ONTAP (`docs`)

  此服務可讓您存取ONTAP 有關的資料。預設設定為 `enabled`。

- ONTAP RESTful API (`docs_api`)

  此服務可讓您存取ONTAP 「REST風格的API」文件。預設設定為 `enabled`。

- 檔案上傳與下載 (`fud`)

  此服務提供檔案上傳與下載。預設設定為 `enabled`。

- ONTAP 訊息 (`ontapmsg`)

  此服務支援發佈及訂閱介面、可讓您訂閱活動。預設設定為 `enabled`。

- ONTAP 入口網站 (`portal`)

  此服務會將閘道實作至虛擬伺服器。預設設定為 `enabled`。

- ONTAP REST 風格的介面 (`rest`)

  此服務支援RESTful介面、可用於遠端管理叢集基礎架構的所有元素。預設設定為 `enabled`。

- 安全聲明標記語言（ SAML ）服務供應商支援 (`saml`)

  此服務提供資源來支援SAML服務供應商。預設設定為 `enabled`。

- SAML 服務供應商 (`saml-sp`)

  此服務可為服務供應商提供SP中繼資料和聲明使用者服務等服務。預設設定為 `enabled`。

從支援下列附加服務的支援範圍ONTAP 起、從支援使用者支援的範圍開始：

- 組態備份檔案 (`backups`)

  此服務可讓您下載組態備份檔案。預設設定為 `enabled`。

- ONTAP 安全性 (`security`)

  此服務支援CSRF權杖管理、以加強驗證。預設設定為 `enabled`。

在 **ONTAP** 中管理網路傳輸協定引擎

您可以在叢集上設定Web傳輸協定引擎、以控制是否允許Web存取、以及可以使用哪些SSL版本。您也可以顯示Web傳輸協定引擎的組態設定。

您可以透過下列方式、在叢集層級管理Web傳輸協定引擎：

- 您可以使用指定遠端用戶端是否可以使用 HTTP 或 HTTPS 來存取 Web 服務內容 `system services web modify` 命令 `-external` 參數。
- 您可以使用來指定是否應使用 SSLv3 來進行安全的 Web 存取 `security config modify` 命令 `-supported-protocol` 參數。
  根據預設、SSLv3會停用。傳輸層安全性1.0（TLSv1.0）已啟用、可視需要停用。

  如"指令參考資料ONTAP"需詳細 `security config modify`資訊，請參閱。

- 您可以針對整個叢集的控制面板Web服務介面、啟用聯邦資訊處理標準（FIPS）140-2法規遵循模式。

  預設會停用FIPS 140-2相容模式。

  - 當**FIPS 140-2**相容模式停用時
    您可以透過設定來啟用 FIPS 140-2 規範模式 `is-fips-enabled` 參數至 `true` 適用於 `security config modify` 命令、然後使用 `security config show` 確認線上狀態的命令。
  - 啟用**FIPS 140-2**規範模式時
    - 從 ONTAP 9.11.1 開始， TLSv1 ， TLSv1.1 和 SSLv3 都會停用，只有 TSLv1.2 和 TSLv1.3 會保持啟用狀態。它會影響ONTAP 到其他內部和外部的系統和通訊、而這些系統和通訊則是來自於19。如果您啟用FIPS 140-2規範模式、然後停用、則TLSv1、TLSv1.1及SSLv3會維持停用狀態。視先前的組態而定、TLSv1.2或TLSSv1.3仍會保持啟用狀態。
    - 對於9.11.1之前的ONTAP 版本、TLSv1和SSLv3都會停用、只有TLSv1.1和TLSv1.2會維持啟用狀態。啟用FIPS 140-2相容模式時、無法同時啟用TLSv1和SSLv3。ONTAP如果您啟用FIPS 140-2規範模式、然後停用該模式、則TLSv1和SSLv3仍會維持停用狀態、但根據先前的組態、TLSv1.2或同時啟用TLSv1.1和TLSv1.2。
- 您可以使用顯示叢集整體安全性的組態 `system security config show` 命令。

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

如果啟用防火牆、則必須設定用於Web服務的邏輯介面（LIF）防火牆原則、以允許HTTP或HTTPS存取。

如果您使用HTTPS進行Web服務存取、則提供Web服務的叢集或儲存虛擬機器（SVM）的SSL也必須啟用、而且您必須提供叢集或SVM的數位憑證。

在「樣」組態中、您對叢集上的Web傳輸協定引擎所做的設定變更不會複寫到合作夥伴叢集上。MetroCluster

用於管理 **Web** 協定引擎的**ONTAP**指令

您可以使用 `system services web` 用於管理網路傳輸協定引擎的命令。您可以使用 `system services firewall policy create` 和 `network interface modify` 允許 Web 存取要求通過防火牆的命令。

如果您想要...	使用此命令...
在叢集層級設定Web傳輸協定引擎： • 啟用或停用叢集的Web傳輸協定引擎 • 啟用或停用叢集的SSLv3 • 啟用或停用安全網路服務（HTTPS）的FIPS 140-2法規遵循	`system services web modify`
在叢集層級顯示Web傳輸協定引擎的組態、判斷Web傳輸協定是否在整個叢集內正常運作、並顯示FIPS 140-2相容性是否已啟用且處於線上狀態	`system services web show`
顯示節點層級的Web傳輸協定引擎組態、以及叢集中節點的Web服務處理活動	`system services web node show`
建立防火牆原則、或將HTTP或HTTPS傳輸協定服務新增至現有的防火牆原則、以允許Web存取要求通過防火牆	`system services firewall policy create` 設定 `-service` 參數至 `http` 或 `https` 允許 Web 存取要求通過防火牆。
將防火牆原則與LIF建立關聯	`network interface modify` 您可以使用 `-firewall-policy` 修改 LIF 防火牆原則的參數。

相關資訊

- "修改網路介面"

配置對ONTAP Web 服務的存取

設定Web服務存取權可讓授權使用者使用HTTP或HTTPS存取叢集或儲存虛擬機器（SVM）上的服務內容。

步驟

1. 如果已啟用防火牆、請確定將用於Web服務的LIF防火牆原則中已設定HTTP或HTTPS存取：

   您可以使用檢查是否啟用防火牆 `system services firewall show` 命令。

   a. 若要確認已在防火牆原則中設定 HTTP 或 HTTPS 、請使用 `system services firewall policy show` 命令。

      您可以設定 `-service` 的參數 `system services firewall policy create` 命令至 `http` 或 `https` 啟用原則以支援網路存取。

   b. 若要驗證支援 HTTP 或 HTTPS 的防火牆原則是否與提供 Web 服務的 LIF 相關聯、請使用 `network interface show` 命令 `-firewall-policy` 參數。

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

您可以使用 `network interface modify` 命令 `-firewall-policy` 將防火牆原則對 LIF 生效的參數。

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

2. 若要設定叢集層級的 Web 傳輸協定引擎、並讓 Web 服務內容可供存取、請使用 `system services web modify` 命令。
3. 如果您打算使用安全 Web 服務（ HTTPS ）、請啟用 SSL 、並使用為叢集或 SVM 提供數位憑證資訊 `security ssl modify` 命令。

   如"指令參考資料ONTAP"需詳細 `security ssl modify`資訊，請參閱。

4. 若要啟用叢集或 SVM 的 Web 服務、請使用 `vserver services web modify` 命令。

   您必須針對要為叢集或SVM啟用的每個服務重複此步驟。

5. 若要授權角色存取叢集或 SVM 上的 Web 服務、請使用 `vserver services web access create` 命令。

   您授予存取權的角色必須已經存在。您可以使用顯示現有角色 `security login role show` 使用命令或建立新角色 `security login role create` 命令。

   深入瞭解 `security login role show`及 `security login role create` "指令參考資料ONTAP"。

6. 對於已獲授權存取 Web 服務的角色、請檢查的輸出、以確保其使用者也使用正確的存取方法進行設定 `security login show` 命令。

   存取 ONTAP API Web 服務 `ontapi`）、使用者必須使用設定 `ontapi` 存取方法。若要存取所有其他 Web 服務、必須使用設定使用者 `http` 存取方法。

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

   > ⓘ 您可以使用 `security login create`命令來新增使用者的存取方法。如"指令參考資料ONTAP"需詳細 `security login create`資訊，請參閱。

用於管理 **Web** 服務的**ONTAP**命令

您可以使用 `vserver services web` 用於管理叢集或儲存虛擬機器（ SVM ） Web 服務可用度的命令。您可以使用 `vserver services web access` 控制角色存取 Web 服務的命令。

如果您想要...	使用此命令...
設定叢集或AnSVM的Web服務： • 啟用或停用Web服務 • 指定是否只能使用HTTPS存取Web服務	`vserver services web modify`
顯示叢集或anSVM的Web服務組態和可用度	`vserver services web show`
授權角色存取叢集或anSVM上的Web服務	`vserver services web access create`
顯示授權存取叢集或anSVM上Web服務的角色	`vserver services web access show`
防止角色存取叢集或anSVM上的Web服務	`vserver services web access delete`

相關資訊

"指令參考資料ONTAP"

用於管理**ONTAP**節點上的掛載點的命令

。 `spi` Web 服務會在要求存取節點的記錄檔或核心檔案時、自動從一個節點建立掛載點到另一個節點的根磁碟區。雖然您不需要手動管理掛載點、但可以使用來進行 `system node root-mount` 命令。

如果您想要...	使用此命令...
手動從一個節點建立掛載點到另一個節點的根磁碟區	`system node root-mount create` 只有一個掛載點可以從一個節點存在到另一個節點。
在叢集中的節點上顯示現有的掛載點、包括建立掛載點的時間及其目前狀態	`system node root-mount show`
從一個節點刪除掛載點到另一個節點的根磁碟區、並強制關閉與掛載點的連線	`system node root-mount delete`

相關資訊

"指令參考資料ONTAP"

在**ONTAP**中管理 **SSL**

使用 `security ssl` 用於管理叢集或儲存虛擬機器（ SVM ） SSL 傳輸協定的命令。SSL 通訊協定可利用數位憑證在 Web 伺服器與瀏覽器之間建立加密連線、進而改善網路存取的安全性。

您可以透過下列方式管理叢集或儲存虛擬機器（SVM）的SSL：

- 啟用SSL
- 產生及安裝數位憑證、並將其與叢集或SVM建立關聯
- 顯示SSL組態以查看是否已啟用SSL、以及SSL憑證名稱（如果有）
- 設定叢集或SVM的防火牆原則、以便Web存取要求能夠通過
- 定義可以使用的SSL版本
- 限制僅存取Web服務的HTTPS要求

管理 **SSL** 的命令

您可以使用 `security ssl` 用於管理叢集或儲存虛擬機器（ SVM ） SSL 傳輸協定的命令。

如果您想要...	使用此命令...
為叢集或 SVM 啟用 SSL 、並將數位憑證與其建立關聯	`security ssl modify`
顯示叢集或 SVM 的 SSL 組態和憑證名稱	`security ssl show`

深入瞭解 `security ssl modify`及 `security ssl show` "指令參考資料ONTAP"。

將 **HSTS** 用於**ONTAP Web** 服務

HTTP 嚴格傳輸安全性 (HSTS) 是一種 Web 安全性原則機制，可協助保護網站免受中間人攻擊，例如協定降級攻擊和 Cookie 劫持。透過強制使用 HTTPS，HSTS 可確保使用者瀏覽器與伺服器之間的所有通訊都經過加密。從ONTAP 9.17.1 開始， ONTAP可以為ONTAP Web 服務強制使用 HTTPS 連線。

只有在與ONTAP建立初始安全 HTTPS 連線後，Web 瀏覽器才會強制執行 HSTS。如果瀏覽器未建立初始安全連接，則不會強制執行 HSTS。有關 HSTS 管理的信息，請參閱您的瀏覽器文件。

關於這項工作

- 對於 9.17.1 及更高版本，新安裝的ONTAP叢集預設為啟用 HSTS。升級到 9.17.1 後，HSTS 預設不啟用。您必須在升級後啟用 HSTS。
- 所有產品均支援 HSTS "ONTAP Web 服務" 。

開始之前

- 以下任務需要進階權限。

顯示 **HSTS** 配置

您可以顯示目前的 HSTS 配置以檢查它是否已啟用並查看最大年齡設定。

步驟

1. 使用 `system services web show`指令顯示目前的 Web 服務配置，包括 HSTS 設定：

```
cluster-1::system services web*> show

                    External Web Services: true
                                HTTP Port: 80
                               HTTPS Port: 443
                          Protocol Status: online
                       Per Address Limit: 80
                     Wait Queue Capacity: 192
                            HTTP Enabled: true
                  CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                            HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

啟用 **HSTS** 並設定最大使用期限

從ONTAP 9.17.1 開始，新的ONTAP叢集預設啟用 HSTS。如果您將現有叢集升級至 9.17.1 或更高版本，則需要在叢集上手動啟用 HSTS 以強制使用 HTTPS。您可以啟用 HSTS 並設定最長使用期限。如果已啟用 HSTS，您可以隨時變更最長使用期限。啟用 HSTS 後，瀏覽器僅在建立初始安全連線後才會開始強制執行安全連線。

步驟

1. 使用 `system services web modify`啟用 HSTS 或修改最大年齡的命令：

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age`指定瀏覽器記住強制執行 HTTPS 的時長（以秒為單位）。預設值為 63072000 秒（兩年）。

禁用 **HSTS**

瀏覽器會在每次連接時保存 HSTS 最長使用期限設置，即使在ONTAP上停用 HSTS，它們也會在整個連接期間繼續強制執行 HSTS。停用 HSTS 後，瀏覽器需要等待配置的最長使用期限才能停止強制執行 HSTS。如果在此期間無法建立安全連接，則強制執行 HSTS 的瀏覽器將不允許存取ONTAP Web 服務，直到問題解決或瀏覽器的最長使用期限到期。

步驟

1. 使用 `system services web modify`命令：

```
system services web modify -hsts-enabled false
```

相關資訊

"RFC 6797 - HTTP 嚴格傳輸安全性 (HSTS)"

解決ONTAP Web 服務存取問題

組態錯誤會導致網路服務存取問題。您可以確保LIF、防火牆原則、Web傳輸協定引擎、Web服務、數位憑證、 而且使用者存取授權均設定正確。

下表可協助您識別及解決Web服務組態錯誤：

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
您的 Web 瀏覽器會傳回 `unable to connect` 或 `failure to establish a connection` 嘗試存取 Web 服務時發生錯誤。	您的LIF設定可能不正確。	請確定您可以ping提供Web服務的LIF。 您可以使用 `network ping`命令 ping LIF 。
您的防火牆可能設定不正確。	請確定防火牆原則已設定為支援HTTP或HTTPS、而且原則已指派給提供Web服務的LIF。 您可以使用 `system services firewall policy` 管理防火牆原則的命令。您可以使用 `network interface modify` 命令 `-firewall -policy` 將原則與 LIF 建立關聯的參數。	您的網路傳輸協定引擎可能已停用。
確保已啟用Web傳輸協定引擎、以便存取Web服務。 您可以使用 `system services web` 用於管理叢集 Web 傳輸協定引擎的命令。	您的網路瀏覽器會傳回 A `not found` 嘗試存取 Web 服務時發生錯誤。	Web服務可能已停用。

此存取問題...	發生原因是此組態錯誤...	若要解決錯誤...
確保您要允許存取的每個Web服務都已個別啟用。 您可以使用 `vserver services web modify` 命令以啟用 Web 服務進行存取。	Web瀏覽器無法以使用者的帳戶名稱和密碼登入Web服務。	無法驗證使用者、存取方法不正確、或使用者無權存取Web服務。
請確定使用者帳戶存在、並使用正確的存取方法和驗證方法進行設定。此外、請確認使用者的角色已獲授權可存取Web服務。 您可以使用 `security login` 管理使用者帳戶及其存取方法和驗證方法的命令。存取 ONTAP API Web 服務需要 `ontapi` 存取方法。存取所有其他 Web 服務需要 `http` 存取方法。您可以使用 `vserver services web access` 用於管理角色存取 Web 服務的命令。	您使用HTTPS連線至Web服務、而您的Web瀏覽器則表示連線中斷。	您可能未在提供Web服務的叢集或儲存虛擬機器（SVM）上啟用SSL。
確認叢集或SVM已啟用SSL、且數位憑證有效。 您可以使用 `security ssl` 用於管理 HTTP 伺服器和的 SSL 組態的命令 `security certificate show` 顯示數位憑證資訊的命令。	您使用HTTPS連線至Web服務、Web瀏覽器則表示該連線不受信任。	您可能使用自我簽署的數位憑證。

相關資訊

- "ONTAP網路配置的最佳實務是什麼？"
- "網路ping"
- "修改網路介面"

- "產生安全性憑證-CSR"
- "安全性憑證安裝"
- "安全證書展示"
- "安全 SSL"

使用憑證驗證遠端伺服器的身分

了解如何在**ONTAP**中使用憑證驗證遠端伺服器的身份

支援安全認證功能、可驗證遠端伺服器的身分。ONTAP

利用下列數位憑證功能與傳輸協定、支援安全連線：ONTAP

- 線上憑證狀態傳輸協定（OCSP）會使用ONTAP SSL和傳輸層安全（TLS）連線、驗證來自支援服務的數位憑證要求狀態。此功能預設為停用。
- 預設的一組信任根憑證會隨ONTAP 附於整套的軟體中。
- 金鑰管理互通性傳輸協定（KMIP）憑證可讓叢集和KMIP伺服器相互驗證。

使用**ONTAP**中的 **OCSP** 驗證數位憑證是否有效

線上憑證狀態協定 (OCSP) 可讓使用傳輸層安全性 (TLS) 通訊的ONTAP應用程式能夠在啟用 OCSP 時接收數位憑證狀態。您可以隨時啟用或停用特定應用程式的OCSP憑證狀態檢查。根據預設、OCSP憑證狀態檢查會停用。

開始之前

您需要進階權限層級存取權限才能執行此工作。

關於這項工作

OCSP支援下列應用程式：

- AutoSupport
- 事件管理系統（EMS）
- LDAP over TLS
- 金鑰管理互通性傳輸協定（KMIP）
- 稽核記錄
- FabricPool
- SSH （從 ONTAP 9.13.1 開始）

步驟

1. 將權限層級設為進階： `set -privilege advanced`。
2. 若要啟用或停用OCSP憑證狀態檢查以檢查特定ONTAP 的功能、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查某些應用程式...	使用命令...
已啟用	`security config ocsp enable -app app name`
已停用	`security config ocsp disable -app app name`

下列命令可支援AutoSupport OCSP for the flexf及EMS。

```
cluster::*> security config ocsp enable -app asup,ems
```

啟用OCSP時、應用程式會收到下列其中一個回應：

- 好-憑證有效且通訊繼續進行。
- 已撤銷：憑證由其核發的憑證授權單位永久視為不信任、且無法繼續通訊。
- 不明：伺服器沒有任何關於憑證的狀態資訊、而且無法繼續通訊。
- 憑證中缺少OCSP伺服器資訊-伺服器的運作方式如同OCSP已停用、並繼續進行TLS通訊、但不會進行狀態檢查。
- OCSP伺服器無回應-應用程式無法繼續。

3. 若要啟用或停用使用TLS通訊之所有應用程式的OCSP憑證狀態檢查、請使用適當的命令。

如果您希望**OCSP**憑證狀態檢查所有應用程式...	使用命令...
已啟用	`security config ocsp enable -app all`
已停用	`security config ocsp disable -app all`

啟用時、所有應用程式都會收到已簽署的回應、表示指定的憑證良好、已撤銷或不明。若憑證遭撤銷、應用程式將無法繼續進行。如果應用程式無法從OCSP伺服器接收回應、或伺服器無法連線、則應用程式將無法繼續進行。

4. 使用 `security config ocsp show` 顯示所有支援 OCSP 的應用程式及其支援狀態的命令。

```
cluster::*> security config ocsp show
         Application                         OCSP Enabled?
         --------------------                ---------------------
         autosupport                         false
         audit_log                           false
         fabricpool                          false
         ems                                 false
         kmip                                false
         ldap_ad                             true
         ldap_nis_namemap                    true
         ssh                                 true

         8 entries were displayed.
```

相關資訊

- "啟用安全性組態OCSP"
- "安全性組態OCSP停用"
- "安全組態OCSP顯示"

查看ONTAP中基於 TLS 的應用程式的預設證書

ONTAP使用傳輸層安全性 (TLS) 為ONTAP應用程式提供了一組預設的受信任根憑證。

開始之前

預設憑證僅在管理 SVM 建立期間或升級期間安裝在管理 SVM 上。

關於這項工作

目前做為用戶端且需要驗證憑證的應用程式包括AutoSupport ：FabricPool 和KMIP。

當憑證過期時、系統會呼叫一則EMS訊息、要求使用者刪除憑證。預設憑證只能在進階權限層級刪除。

> 刪除預設憑證可能會導致部分ONTAP 功能不正常的應用程式（例如AutoSupport 、「可靠性記錄」和「稽核記錄」）。

步驟

1. 您可以使用安全性憑證show命令來檢視安裝在管理SVM上的預設憑證：

   security certificate show -vserver –type server-ca

```
cluster1::> security certificate show

Vserver    Serial Number   Certificate Name
Type
---------- -------------- ----------------------------------------
---------
vs0        4F4E4D7B         www.example.com
server
    Certificate Authority:  www.example.com
          Expiration Date: Thu Feb 28 16:08:28 2013
```

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

相互驗證叢集和 KMIP 伺服器

相互驗證ONTAP叢集和 KMIP 伺服器概述

相互驗證叢集和外部金鑰管理程式（例如金鑰管理互通性傳輸協定（KMIP）伺服器）、可讓金鑰管理程式使用KMIP over SSL與叢集進行通訊。當應用程式或特定功能（例如儲存加密功能）需要安全金鑰來提供安全的資料存取時、您就會這麼做。

在 ONTAP 中為叢集產生憑證簽署要求

您可以使用安全性憑證 `generate-csr` 產生憑證簽署要求（ CSR ）的命令。在處理您的要求之後、憑證授權單位（CA）會傳送簽署的數位憑證給您。

開始之前

您必須是叢集管理員或SVM管理員、才能執行此工作。

步驟

1. 產生CSR：

```
security certificate generate-csr -common-name <FQDN_or_common_name>
-size 512|1024|1536|2048 -country <country> -state <state> -locality
<locality> -organization <organization> -unit <unit> -email-addr
<email_of_contact> -hash-function SHA1|SHA256|MD5
```

如"指令參考資料ONTAP"需詳細 `security certificate generate-csr`資訊，請參閱。

下列命令會建立CSR、其中包含由SHA256雜湊功能所產生的2、048位元私密金鑰、供公司IT部門的軟體群組使用、其自訂通用名稱為server1.companyname.com、位於美國加州桑尼維爾。SVM聯絡人管理員的電子郵件地址為web@example.com。系統會在輸出中顯示CSR和私密金鑰。

```
cluster1::>security certificate generate-csr -common-name
server1.companyname.com -size 2048 -country US -state California -
locality Sunnyvale -organization IT -unit Software -email-addr
web@example.com -hash-function SHA256
Certificate Signing Request :
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
Private Key :
24 | Administrator Authentication and RBAC
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
Note: Please keep a copy of your certificate request and private key
for future reference.
```

2. 從CSR輸出複製憑證要求、然後以電子形式（例如電子郵件）將其傳送至信任的協力廠商CA進行簽署。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。您應該保留一份私密金鑰和CA簽署的數位憑證複本。

為**ONTAP**叢集安裝 **CA** 簽署的伺服器憑證

若要讓SSL伺服器將叢集或儲存虛擬機器（SVM）驗證為SSL用戶端、請在叢集或SVM上安裝具有用戶端類型的數位憑證。然後將用戶端CA憑證提供給SSL伺服器管理員、以便在伺服器上安裝。

開始之前

您必須已在叢集上安裝 SSL 伺服器的根憑證、或是在上安裝 SVM `server-ca` 憑證類型。

步驟

1. 若要使用自我簽署的數位憑證進行用戶端驗證、請使用 `security certificate create` 命令 `type client` 參數。

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

2. 若要使用CA簽署的數位憑證進行用戶端驗證、請完成下列步驟：

   a. 使用安全性憑證產生數位憑證簽署要求（ CSR ） `generate-csr` 命令。

      包含憑證要求和私密金鑰的CSR輸出會顯示出來、並提醒您將輸出複製到檔案、以供日後參考。ONTAP

   b. 將CSR輸出的憑證要求以電子形式（例如電子郵件）傳送至信任的CA進行簽署。

      您應該保留一份私密金鑰和CA簽署憑證的複本、以供日後參考。

   在處理您的要求之後、CA會將簽署的數位憑證傳送給您。

a. 使用安裝 CA 簽署的憑證 `security certificate install` 命令 `-type client` 參數。

b. 在系統提示時輸入憑證和私密金鑰、然後按* Enter *。

c. 在出現提示時輸入任何其他根或中繼憑證、然後按* Enter *。

如果從信任的根CA開始且以核發給您的SSL憑證結束的憑證鏈結遺失中繼憑證、您可以在叢集或SVM上安裝中繼憑證。中繼憑證是由信任的根所核發的次要憑證、專門用於發行終端實體伺服器憑證。結果是憑證鏈結從信任的根CA開始、經過中繼憑證、最後以核發給您的SSL憑證結束。

3. 提供 `client-ca` 將叢集或 SVM 的憑證交給 SSL 伺服器的管理員、以便在伺服器上安裝。

的安全性憑證 show 命令 `-instance` 和 `-type client-ca` 參數會顯示 `client-ca` 憑證資訊。

相關資訊

- "安全性憑證安裝"
- "安全證書展示"

在ONTAP中為 KMIP 伺服器安裝 CA 簽署的客戶端憑證

金鑰管理互通性傳輸協定（KMIP）的憑證子類型（-subtype kmip-cert參數）、以及用戶端和伺服器-ca類型、都會指定該憑證用於互動驗證叢集和外部金鑰管理程式、例如KMIP伺服器。

關於這項工作

安裝KMIP憑證、將KMIP伺服器驗證為叢集的SSL伺服器。

步驟

1. 使用 `security certificate install` 命令 `-type server-ca` 和 `-subtype kmip-cert` 用於為 KMIP 伺服器安裝 KMIP 憑證的參數。
2. 出現提示時、請輸入憑證、然後按Enter。

提醒您保留一份憑證複本、以供日後參考。ONTAP

```
cluster1::> security certificate install -type server-ca -subtype kmip-
cert
-vserver cluster1

Please enter Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----


You should keep a copy of the CA-signed digital certificate for future
reference.

cluster1::>
```

相關資訊

- "安全性憑證安裝"

安全性與資料加密

自主勒索軟體保護

瞭解 **ONTAP** 自主勒索軟體保護

從ONTAP 9.10.1 開始， ONTAP管理員可以啟用自主勒索軟體防護 (ARP) 功能，在 NAS（NFS 和 SMB）環境中執行工作負載分析，從而主動偵測並警告可能預示勒索軟體攻擊的異常活動。從ONTAP 9.17.1 開始，ARP 也支援區塊設備卷，包括包含 LUN 或 NVMe 命名空間的 SAN 卷，或包含來自 VMware 等虛擬機器管理程式的虛擬磁碟的 NAS 卷。

ARP 直接內建於 ONTAP 中，確保與 ONTAP 的其他功能實現整合控制和協調。 ARP即時運行，在檔案系統中寫入或讀取資料時進行處理，並快速偵測和回應潛在的勒索軟體攻擊。

ARP 除了按計畫建立快照外，還會定期建立鎖定快照，以增加保護。它可以智慧地管理快照的保存時長。如果沒有偵測到異常活動，快照將迅速回收。但是，如果偵測到攻擊，則會將攻擊開始前建立的快照保留較長時間。有關更多信息，包括ONTAP版本添加的更改，請參閱 ARP快照。

授權與能力

您需要取得授權才能使用 ARP。請決定是預設在新磁碟區上啟用 ARP，還是手動為每個磁碟區啟用 ARP。

ARP 的授權選項

ARP 支援包含在內"ONTAP One 許可證"。如果您沒有ONTAP One 許可證，則可以使用其他許可證來用於 ARP，具體取決於您的ONTAP版本。

發行版**ONTAP**	授權
更新版本ONTAP	`Anti_ransomware`
零點9.10.1 ONTAP	`MT_EK_MGMT` （多租戶密鑰管理）

- 如果您要從ONTAP 9.10.1 升級到ONTAP 9.11.1 或更高版本，且系統上已設定 ARP，則無需安裝新的 `Anti-ransomware`許可證。對於新的 ARP 配置，需要新的許可證。
- 如果您從ONTAP 9.11.1 或更高版本還原到ONTAP 9.10.1，並且已使用 Anti_ransomware 授權啟用 ARP，您將看到警告訊息，可能需要重新設定 ARP。"瞭解如何還原Arp" 。

ARP 啟用選項

ARP 在叢集、SVM 和磁碟區層級提供靈活的啟用選項，可讓您為新磁碟區設定自動預設啟用，或根據需要在現有磁碟區上手動啟用 ARP。

新磁碟區上的自動預設啟用

從 ONTAP 9.18.1 開始，對於 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統，所有新建磁碟區預設會自動啟用 ARP。此預設會自動啟用 ARP 的功能不適用於 "不支援的磁碟區或組態"。

升級後，新磁碟區上的 ARP 預設啟用將在 12 小時寬限期後生效；對於新 ONTAP 9.18.1 安裝，則 ARP 預設啟

用將立即生效，前提是已安裝 ARP 授權。您必須手動啟用 ARP在現有磁碟區上。

在寬限期內，您可以"使用 System Manager 或 ONTAP CLI 在叢集層級選擇退出新磁碟區的預設啟用"。如果您未選擇退出，則寬限期結束後建立的所有新磁碟區都會自動啟用 ARP。如果寬限期結束後需求發生變化，您也可以隨時靈活地啟用或停用預設啟用功能。

在新磁碟區上手動啟用預設功能

如果您在叢集層級停用了 ARP 的自動預設啟用，也可以選擇"手動在所有新磁碟區上預設啟用 ARP"在 SVM 層級進行設定。對於 ONTAP 9.17.1 及更早版本，這是將 ARP 設定為在新磁碟區上預設啟用的唯一方法。

在所有或特定現有磁碟區上啟用 **ARP**

從 9.18.1 版本開始，您可以從叢集層級手動在所有現有磁碟區上啟用 ARP（選擇 叢集 **>** 安全性，然後在 **Anti-ransomware** 區段中按一下 ⋮，接著選擇 在所有現有磁碟區上啟用）。

如果您希望將 ARP 啟用限制在特定磁碟區上，您可以"以每個磁碟區為基礎啟用 ARP"。

勒索軟體保護策略**ONTAP**

有效的勒索軟體防護需要多層防護協同運作。

雖然 ONTAP 包含 FPolicy、快照、SnapLock 和 Active IQ Digital Advisor（也稱為 Digital Advisor）等功能來幫助抵禦勒索軟體，但 ARP 提供了一層額外的防禦。

若要深入瞭解 NetApp 產品組合中可防範勒索軟體的其他功能，請參閱：

- "勒索軟體和 NetApp 的保護產品組合"
- "使用 PowerShell 進行 ONTAP 網路保險庫加固"

ARP 偵測到什麼

ONTAP ARP 旨在防禦拒絕服務攻擊，即攻擊者扣留資料直至支付贖金。 ARP基於以下方式提供即時勒索軟體偵測：

- 將傳入資料識別為加密或純文字。
- 可偵測下列項目的分析：
  - 熵：（用於 NAS 和 SAN）對文件中資料隨機性的評估
  - 檔案副檔名類型：（僅在 NAS 中使用）不符合預期副檔名類型的檔案副檔名
  - 檔案 **IOPS**：（僅在ONTAP 9.11.1 開始的 NAS 中使用）資料加密時異常卷活動激增

ARP 只需少量檔案被加密即可偵測到大多數勒索軟體攻擊的傳播，自動回應以保護數據，並提醒您疑似攻擊正在發生。

沒有任何勒索軟體偵測系統可以保證完全的安全。如果防毒軟體無法偵測到入侵，ARP 可提供額外的防禦層。

了解 **ARP** 模式

在為磁碟區啟用 ARP 後，它將進入學習期以建立基線。 ARP 在轉換到主動偵測模式之前會分析系統指標以建立警報設定檔。在主動模式下，ARP 監控異常活動，如果偵測到異常行為，則採取保護措施並產生警報。

對於 ARP，學習模式和主動模式行為因ONTAP版本、磁碟區類型和協定（NAS 或 SAN）而異。

NAS 環境和模式類型

下表總結了ONTAP 9.10.1 與 NAS 環境的更高版本之間的差異。

對於採用早期 ARP 模型的版本，建議在開始主動監控之前先進行一段時間的學習。對於支援 NAS 的環境ARP/AI沒有學習期，立即開始主動監控。

模式	說明	卷類型和版本
學習	對於某些版本的ONTAP和某些磁碟區類型，啟用 ARP 時，ARP 會自動設定為學習模式。在學習模式下， ONTAP系統會根據以下分析領域（熵、檔案副檔名類型和檔案 IOPS）制定警報設定檔。 建議您將 ARP 保持在學習模式 30 天。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習間隔並自動切換，切換可能在 30 天之前完成。對於ONTAP 9.13.1 之前的版本，您可以手動進行切換。 從ONTAP 9.16.1 開始， FlexVol磁碟區僅存在活動模式，任何升級到此版本或更高版本的FlexVol磁碟區都會自動從學習模式過渡到活動模式。 對於ONTAP 9.16.1 到 9.17.1，ARP/AI 尚不支援FlexGroup卷，並繼續運行較舊的 ARP 模型。因此，對於這些帶有FlexGroup卷的版本，仍然建議留出一段學習期。 從ONTAP 9.18.1 開始， FlexVol和FlexGroup磁碟區都只有活動模式。任何升級後的捲都會自動切換到活動模式。 "了解有關從學習模式切換到主動模式的更多信息" 。 命令 `security anti-ransomware volume workload-behavior show`會顯示已在磁碟區中偵測到的副檔名。如果您在學習模式早期執行此命令，並顯示正確的檔案類型呈現，則不應將該資料當作移至作用中模式的基礎，因為 ONTAP 仍在收集其他計量。如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume workload-behavior show`資訊，請參閱。	• FlexVol卷（採用ONTAP 9.10.1 至 9.15.1） • FlexGroup卷，版本從ONTAP 9.13.1 到ONTAP 9.17.1
積極的	在主動模式下，如果檔案副檔名被標記為異常，您應該評估該警報。您可以根據警報採取行動來保護數據，也可以將警報標記為誤報。將警報標記為誤報會更新警報設定檔。例如，如果警報是由新的檔案副檔名觸發的，並且您將警報標記為誤報，則下次觀察到該檔案副檔名時，您將不會收到警報。	所有支援的ONTAP版本以及FlexVol和FlexGroup卷

SAN 環境和模式類型

SAN 環境會使用評估期（類似 NAS 環境中的學習模式），然後自動過渡到主動偵測。下表總結了評估模式和主動模式。

模式	說明	卷類型和版本
評估	進行為期兩到四週的評估期，以確定基線加密行為，同時 ARP/AI 在評估期內為 SAN 磁碟區提供即時主動保護。在建立基線閾值期間，可以進行偵測並發出警報。您可以透過執行以下命令來確定評估期間是否結束： `security anti-ransomware volume show`命令和檢查 `Block device detection status`。 "了解有關 SAN 捲和熵評估期的更多信息" 。	• 帶有ONTAP 9.17.1 及更高版本的FlexVol 卷
積極的	評估期結束後，您可以透過運行 `security anti-ransomware volume show`指揮和檢查 `Block device detection status`.的狀態 `Active_suitable_workload`表示可以成功監測到評估的熵值。 ARP會根據評估過程中審查的數據自動調整自適應閾值。	• 帶有ONTAP 9.17.1 及更高版本的FlexVol 卷

威脅評估和 **ARP** 快照

ARP 根據接收到的數據，並結合現有的分析數據來評估威脅機率。當 ARP 偵測到異常情況時，會指派一個度量值。ARP 可能會在偵測到異常時分配一個快照，也可能定期分配一個快照。

ARP 閾值

- * 低 * ：磁碟區最早偵測到異常（例如，在磁碟區中觀察到新的副檔名）。此偵測層級僅適用於 ONTAP 9 。16.1 之前的版本，但沒有 ARP/AI 。
  - 從ONTAP 9.11.1 開始，您可以"自訂ARP檢測參數" 。
  - 在 ONTAP 9.10.1 中、向上提報至中度的臨界值為 100 個以上的檔案。
- 中：偵測到高熵，或觀察到多個具有相同前所未見檔案副檔名的檔案。這是ONTAP 9.16.1 及更高版本中帶有 ARP/AI 的基準檢測等級。

當ONTAP運行分析報告確定異常是否與勒索軟體設定檔匹配時，威脅會升級為中等。當攻擊機率為中等時，ONTAP會產生 EMS 通知，提示您評估威脅。 ONTAPONTAP 不會傳送關於低威脅的警示；但是，從 ONTAP 9.14.1 開始，您可以 "修改預設警報設定"。"回應異常活動" 。

您可以在 System Manager 的 * 事件 * 區段或命令中檢視中度威脅的相關資訊 `security anti-ransomware volume show`。在 ONTAP 9.16.1 之前的版本中，如果沒有 ARP/AI ，也可以使用命令來檢視低威脅事件 `security anti-ransomware volume show`。如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

ARP快照

當偵測到攻擊的早期跡象時，ARP 會建立快照。然後進行詳細分析，以確認或排除潛在攻擊。由於 ARP 快照是在攻擊得到完全確認之前主動創建的，因此它們也可能會定期為某些合法應用程式產生。這些快照的存在不應被視為異常。如果確認發生攻擊，則攻擊機率將升級為 `Moderate`並產生攻擊通知。

從ONTAP 9.17.1 開始，會定期為 NAS 和 SAN 磁碟區產生 ARP 快照，並回應偵測到的異常。ONTAP在 ARP 快照前新增一個名稱，以便於識別。

從ONTAP 9.11.1 開始，您可以修改保留設定。有關更多信息，請參閱"修改快照選項" 。

下表總結了不同版本的 ARP 快照差異。

功能	**ONTAP 9.17.1** 及更高版本	**ONTAP 9.16.1** 及更早版本
建立觸發器	• 快照以固定的 4 小時間隔創建，無論任何特定觸發器如何 • 確認攻擊 根據觸發類型建立“定期”或“攻擊”快照。	• 偵測到高熵 • 偵測到新的檔案副檔名（9.15.1 及更早版本） • 偵測到文件操作激增（9.15.1 及更早版本） 快照建立間隔基於觸發器類型。
前綴名稱約定	“反勒索軟體定期備份” “反勒索軟體攻擊備份”	“反勒索軟體備份”
刪除行為	ARP快照被鎖定，管理員無法刪除	ARP快照被鎖定，管理員無法刪除
最大快照數	"六個快照可配置限制"	"六個快照可配置限制"
保留期	快照通常保留 12 小時。 • NAS 卷：如果透過檔案分析確認了攻擊，則攻擊前建立的快照將保留，直到管理員將攻擊標記為真或誤報（明確懷疑）。 • SAN 磁碟區或 VM 資料儲存：如果透過區塊熵分析確認了攻擊，則攻擊前建立的快照將保留 10 天（可設定）。	• 根據觸發條件確定（不固定） • 攻擊先前建立的快照將保留，直到管理員將攻擊標記為真或誤報（明確嫌疑）。
明確嫌疑行動	管理員可以執行清除嫌疑的操作，該操作根據確認設定保留： • 誤報保留時間為 24 小時 • 真實陽性保留時間為 7 天	管理員可以執行清除嫌疑的操作，該操作根據確認設定保留： • 誤報保留時間為 24 小時 • 真實陽性保留時間為 7 天 此預防性保留行為在ONTAP 9.16.1 之前不存在
到期時間	所有快照均設定了到期時間	無

如何在**ONTAP** 勒索軟體攻擊後恢復資料

ARP 基於成熟的ONTAP資料保護和災難復原技術，可有效應對勒索軟體攻擊。當偵測到攻擊的早期跡象時，ARP 會建立鎖定快照。您需要先確認攻擊是真實攻擊還是誤報。如果您確認有攻擊，則可以使用 ARP 快照復原磁碟區。

鎖定的快照無法透過正常方式刪除。但是，如果您稍後決定將攻擊標記為誤報， ONTAP會刪除鎖定的副本。

您可以從選定的快照中恢復受影響的文件，而不必恢復整個磁碟區。

有關應對攻擊和恢復資料的更多信息，請參閱以下主題：

- "回應異常活動"

- "從 ARP 快照恢復數據"
- "從ONTAP快照恢復"
- "智慧型勒索軟體還原"

ARP 的多管理驗證保護

從 ONTAP 9.13.1 開始，我們建議您啟用多重管理驗證（ MAV ），以便在進行自主勒索軟體保護（ ARP ）組態時，需要兩個或更多已驗證的使用者管理員。如需更多資訊、請參閱 "啟用多重管理驗證"。

人工智慧的自主勒索軟體保護（ **ARP/AI** ）

從ONTAP 9.16.1 開始，ARP 採用機器學習模型進行反勒索軟體分析，從而提升了網路彈性。該模型能夠在 NAS 環境中以 99% 的準確率檢測不斷演變的勒索軟體形式。的機器學習模型在模擬勒索軟體攻擊前後都基於大量文件資料集進行了預訓練。這種資源密集的訓練是在ONTAP之外進行的，使用開源取證研究資料集來訓練模型。整個建模流程不會使用客戶數據，因此不存在隱私問題。此訓練產生的預訓練模型隨ONTAP一起提供。但無法透過ONTAP CLI 或ONTAP API 存取或修改此模型。

立即過渡到主動防禦**ARP/AI**

使用ARP/AI，就沒有學習週期。對於以下受支援的磁碟區類型，ARP/AI 在安裝或升級後立即啟動：

- NAS FlexVol卷，支援ONTAP 9.16.1 及更高版本
- NAS FlexGroup卷， ONTAP9.18.1 及更高版本
- 使用ONTAP 9.17.1 及更高版本的 SAN 磁碟區（立即激活，即使在期間）"評估期" ）

對於已啟用 ARP 功能的現有捲和新磁碟區，將叢集升級至支援 ARP/AI 的ONTAP版本後，ARP/AI 保護將自動啟動。

ARP/AI 自動更新

為了持續提供對最新勒索軟體威脅的最新保護，ARP/AI 提供頻繁的自動更新，這些更新在ONTAP常規升級和發布週期之外進行。如果您"已啟用自動更新"在您選擇安全檔案自動更新後，您也將能夠開始接收 ARP/AI 的自動安全性更新。您也可以選擇"手動進行這些更新"並控制更新發生的時間。

從 ONTAP 9 。 16.1 開始，除了系統和韌體更新之外，還可使用系統管理員來提供 ARP/AI 的安全性更新。

"深入瞭解 ARP/AI 更新"

ARP/AI 與 **ARP** 模型之間的差異概覽

功能	**ARP**	**ARP/AI**
ONTAP 版本	ONTAP 9.10.1-9.15.1	ONTAP 9.16.1 及更新版本；9.15.1（技術預覽）
偵測方法	分析檔案活動、資料熵和檔案副檔名類型	基於大型取證資料集訓練的 AI / 機器學習模型；分析熵和檔案行為
學習期	NAS FlexVol Volume 需要 30 天學習模式（9.13.1 及更高版本支援自動切換）	無需學習期；啟用後立即生效

功能	ARP	ARP/AI
磁碟區類型支援	• FlexVol：9.10.1 及更高版本 • FlexGroup：9.13.1 及更高版本 • SAN:不支援	• FlexVol：9.16.1 及更高版本 • FlexGroup：9.18.1 及更高版本 • SAN：9.17.1 及更新版本（含評估期間）
Snapshot 建立	由高熵、新的檔案副檔名或檔案操作激增所觸發	以固定 4 小時間隔建立，並在確認攻擊時建立
Snapshot 保留	保留直到管理員清除可疑活動	預設時間為 12 小時；依攻擊確認情況延長（誤報為 24 小時，確認為正確為 7 天）
更新	靜態偵測邏輯（僅在 ONTAP 升級時更新）	自動安全性更新，與 ONTAP 版本無關
部署	手動啟用（按磁碟區）或 SVM 層級預設設定	可手動按磁碟區啟用或設定 SVM 等級的預設設定；對於 9.18.1 及更高版本中支援的系統，所有新磁碟區均預設在叢集層級啟用
評估期	不適用	SAN 磁碟區需要（2-4 週）來建立基線加密閾值

相關資訊

- "指令參考資料ONTAP"

ONTAP 自主勒索軟體保護使用案例與考量

自主勒索軟體防護 (ARP) 適用於從ONTAP 9.10.1 開始的 NAS 工作負載和從ONTAP 9.17.1 開始的 SAN 工作負載。在部署 ARP 之前，您應該了解其建議用途、支援的配置以及效能影響。

支援和不支援的組態

在決定使用 ARP 時、請務必確保您的磁碟區工作負載適合 ARP 、並且符合所需的系統組態。

合適的工作負載

ARP 適用於以下類型的工作負載：

- NFS 或 SAN 儲存上的資料庫
- Windows或Linux主目錄

  對於沒有 ARP/AI 的環境，使用者可能會建立一些在學習期間無法偵測到的副檔名的檔案。因此，此類工作負載中出現誤報的可能性較大。

- 影像與影片

  例如、醫療記錄和電子設計自動化（ EDA ）資料

不適當的工作負載

ARP 不適合以下類型的工作負載：

- 具有高頻率檔案建立或刪除操作的工作負載（幾秒鐘內數十萬個檔案；例如，測試/開發工作負載）。
- ARP 的威脅偵測依賴於其識別檔案建立、重新命名或刪除操作異常激增的能力。如果應用程式本身是文件活動的來源，則無法有效區分勒索軟體活動。
- 應用程式或主機加密資料的工作負載。

  ARP 依賴區分傳入資料是加密的還是未加密的。如果應用程式本身正在加密數據，則該功能的有效性會降低。但是，ARP 仍然可以根據檔案活動（刪除、覆蓋、創建，或建立檔案或使用新的檔案副檔名重新命名）和檔案類型進行工作。

支援的組態

從ONTAP 9.10.1 開始，ARP 可用於 NAS NFS 和 SMB FlexVol磁碟區。從 9.17.1 開始，ARP 可用於 iSCSI、FC 和具有 SAN 儲存的 NVMe 的 SAN FlexVol磁碟區。

從 ONTAP 9.10.1 開始，MetroCluster 組態支援 ARP。

下列 ONTAP 版本支援其他組態和磁碟區類型：

	ONTAP 9.18.1	**ONTAP 9.17.1**	**ONTAP 9.16.1.**	**ONTAP 9.15.1.1**	**ONTAP 9.14.1.**	**ONTAP 9.13.1.12 .9.11.9.1 1.**	**ONTAP 9.12.1**	**零點9.11.1. ONTAP**	**零點9.10.1 ONTAP**
使用SnapMirror 非同步保護的磁碟區	✓	✓	✓	✓	✓	✓	✓		
受SnapMirror 非同步（SVM災難恢復）保護的SVM	✓	✓	✓	✓	✓	✓	✓		
SVM資料移動性（`vserver migrate`）	✓	✓	✓	✓	✓	✓	✓		
FlexGroup卷[1]	✓	✓	✓	✓	✓	✓			
多管理員驗證	✓	✓	✓	✓	✓				

	ONTAP 9.18.1	ONTAP 9.17.1	ONTAP 9.16.1.	ONTAP 9.15.1.1	ONTAP 9.14.1.	ONTAP 9.13.1.12 .9.11.9.1 1.	ONTAP 9.12.1	零點9.11. 1. ONTAP	零點9.10. 1 ONTAP
ARP/AI 提供自動更新	✓	✓							
ARP/AI 預設啟用[2]	✓								

[1] ONTAP 9.16.1 和 9.17.1 不提供FlexGroup卷的 ARP/AI 支援。升級到這些版本後，啟用 ARP 的FlexGroup磁碟區將繼續使用 ARP/AI 之前使用的相同 ARP 模型運行。從ONTAP 9.18.1 開始， FlexGroup磁碟區使用 ARP/AI 模型。

[2] 從 ONTAP 9.18.1 開始，AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統均支援 ARP/AI 預設為啟用。此行為會在升級後 12 小時寬限期後自動為所有新磁碟區啟用 ARP/AI,或新 ONTAP 9.18.1 安裝的系統則立即啟用。您需要手動啟用 ARP "現有磁碟區"。

SnapMirror與ARP互通性

從ONTAP 9.12.1 開始， SnapMirror非同步目標磁碟區支援 ARP。 SnapMirrorSnapMirror同步或SnapMirror主動同步不支援 ARP。

如果SnapMirror來源磁碟區啟用了 ARP，則SnapMirror目標磁碟區會自動取得 ARP 設定狀態（例如 `dry-run` 或者 `enabled`）、ARP 訓練資料以及 ARP 建立的來源磁碟區快照。無需明確啟用。

儘管目標磁碟區包含唯讀 (RO) 快照，但其資料不會進行任何 ARP 處理。但是，當SnapMirror目標磁碟區轉換為讀寫 (RW) 時，ARP 會在已轉換為 RW 的目標磁碟區上自動啟用。除了來源磁碟區上已記錄的內容外，目標磁碟區不需要任何其他學習過程。

在ONTAP 9.10.1 和 9.11.1 中， SnapMirror不會將 ARP 設定狀態、訓練資料和快照從來源磁碟區傳送到目標磁碟區。因此，當SnapMirror目標磁碟區轉換為 RW 時，必須在轉換後在學習模式下明確啟用目標磁碟區上的 ARP。

ARP 和虛擬機器

VMware 上的虛擬機器 (VM) 支援 ARP。檢測對於虛擬機器內部和外部的變更有不同的行為。對於虛擬機器中涉及大量高度壓縮檔案（例如 7z 和 ZIP）或加密檔案（例如受密碼保護的 PDF、DOC 或 ZIP）的工作負載，不建議使用 ARP。

VM 以外的變更

如果新副檔名以加密狀態進入磁碟區或檔案副檔名發生變化，ARP 可以偵測到 VM 外部 NFS 磁碟區上的檔案副檔名變化。

VM 內部的變更

如果勒索軟體攻擊更改了虛擬機器內部的文件，而沒有更改虛擬機器外部的文件，且虛擬機器的預設熵較低（例如 .txt、.docx 或 .mp4 文件），ARP 就會偵測到威脅。對於ONTAP 9.16.1 及更早版本，ARP 會在這種情況下建立保護性快照，但不會產生威脅警報，因為虛擬機器外部的檔案副檔名未被竄改。從ONTAP 9.17.1 中的 SAN 支援開始，如果 ARP 偵測到虛擬機器內部的熵異常，也會產生威脅警報。

如果檔案預設為高熵檔案（例如 .gzip 檔案或受密碼保護的檔案），ARP 的偵測能力就會受到限制。在這種情況下，ARP 仍然可以主動拍攝快照；但是，如果檔案副檔名未被外部篡改，則不會觸發警報。

對於 SAN，ARP 在磁碟區層級分析熵統計數據，並在發現熵異常時觸發檢測。

> 在ONTAP 9.18.1 及更高版本中，僅FlexVol磁碟區可偵測 VM 內發生的攻擊，如果 VM 資料儲存配置在FlexGroup磁碟區上，則無法偵測 VM 內發生的攻擊。

不支援的組態

ONTAP S3 環境不支援 ARP。

ARP 不支援下列 Volume 組態：

- FlexGroup磁碟區（在ONTAP 9.10.1 至 9.12.1 中）。

> 從ONTAP 9.13.1 到ONTAP 9.17.1，支援FlexGroup卷，但僅限於 ARP/AI 之前使用的 ARP 模型。 ONTAP 9.18.1 開始支援 ARP/AI 的FlexGroup磁碟區。

- FlexCache Volume （原始 FlexVol 磁碟區支援 ARP 、快取磁碟區則不支援）
- 離線磁碟區
- 資料量SnapLock
- SnapMirror 主動同步
- SnapMirror 同步
- SnapMirror非同步（在ONTAP 9.10.1 和 9.11.1 中）。從ONTAP 9.12.1 開始支援SnapMirror非同步。有關更多信息，請參閱SnapMirror 。
- 受限磁碟區
- 儲存VM的根磁碟區
- 已停止儲存VM的磁碟區

ARP效能和頻率考量

ARP 對系統效能（以吞吐量和峰值 IOPS 衡量）的影響極小。 ARP功能的影響取決於特定的捲工作負載。對於常見工作負載，建議採用以下配置限制：

工作負載特性	每個節點的建議**Volume**限制	當每個節點的磁碟區限制超過上限時，效能會下降[1]
讀取密集型或資料可以壓縮	150	最高IOPS的4%
寫入密集且資料無法壓縮	60	• NAS： ONTAP 9.15.1 及更早版本的最大 IOPS 的 10% • NAS：ONTAP 9.16.1 及更高版本最大 IOPS 的 5% • SAN： ONTAP 9.17.1 及更高版本的最大 IOPS 的 5%

[1] 無論添加的捲數量超過建議的限制多少，系統效能都不會下降超過這些百分比。

由於 ARP 分析按優先順序運行，因此隨著受保護磁碟區數量的增加，每個磁碟區上運行的分析頻率會降低。

預設在大量新磁碟區上啟用 ARP 可能會增加系統資源使用量。在磁碟區上啟用 ARP 時，請考慮快照等競爭程序的空間需求。

依平台的 **ARP** 磁碟區限制

從 ONTAP 9.18.1 開始、ARP 支援根據平台類型和 CPU 核心數增加磁碟區限制。

平台類型	每個節點啟用 **ARP** 的最大磁碟區數
低階（最多 20 個 CPU 核心的系統）	250
中等配置（最多 64 個 CPU 核心的系統）	500
高階（擁有超過 64 個 CPU 核心的系統）	1000

CPU 核心數適用於 2 節點 HA 對中的每個單獨節點。

使用 **ARP** 保護的磁碟區進行多重管理驗證

從 ONTAP 9.13.1 開始、您可以啟用多重管理驗證（ MAV ）、以提高 ARP 的安全性。MAV 可確保至少有兩位或多位通過驗證的系統管理員必須關閉 ARP 、暫停 ARP 、或將可疑攻擊標示為受保護磁碟區上的誤報。瞭解如何"為受 ARP 保護的磁碟區啟用 MAV"。

您需要為 MAV 群組定義系統管理員，並為您要保護的， `security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect` ARP 命令建立 MAV 規則 `security anti-ransomware volume disable`。MAV 群組中的每位管理員都必須核准每個新規則要求，並"再次新增 MAV 規則"在 MAV 設定內進行。

深入瞭解 `security anti-ransomware volume disable`， `security anti-ransomware volume pause`和 `security anti-ransomware volume attack clear-suspect` "指令參考資料ONTAP"。

從ONTAP 9.14.1 開始，ARP 會在建立 ARP 快照和發現新檔案副檔名時發出警報。這些事件的警報預設為禁用狀態。警報可以在磁碟區或 SVM 層級設定。您可以使用以下命令啟用警報 `security anti-ransomware vserver event-log modify`或使用 `security anti-ransomware volume event-log modify`。

深入瞭解 `security anti-ransomware vserver event-log modify`及 `security anti-ransomware volume event-log modify` "指令參考資料ONTAP"。

後續步驟

- "啟用自發勒索軟體保護"
- "為受 ARP 保護的磁碟區啟用 MAV"

啟用 **ARP**

在磁碟區上啟用 **ONTAP Autonomous Ransomware Protection**

從 ONTAP 9 。 10.1 開始，您可以在現有的磁碟區上啟用「自主勒索軟體保護」（ ARP ），或是建立新的磁碟區，從頭開始啟用 ARP 。

關於這項工作

若要啟用 ARP，請按照與您的環境相符的步驟操作。您確保您的環境符合某些要求 ：

- 帶有FlexVol磁碟區的 NAS
- 帶有FlexGroup磁碟區的 NAS
- SAN 磁碟區

啟用 ARP 後，ARP 可能會進入過渡期，具體取決於您的環境和ONTAP版本：

Volume類型	版本**ONTAP**	啟用後的行為
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP啟動後將進入學習模式，持續30天。
NAS FlexVol	ONTAP 9.16.1 及更新版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP啟動後將進入學習模式，持續30天。
SAN 磁碟區	ONTAP 9.17.1 及更高版本	ARP/AI 立即啟動，啟動評估期，以確定合適的警報閾值，然後再從初始的保守閾值過渡。

開始之前

啟用 ARP 之前，請確保您的環境具備以下條件：

NAS 特定要求

- 啟用了 NFS 或 SMB（或兩者）協定的儲存虛擬機器 (SVM)。
- 已配置客戶端的 NAS 工作負載。
- 積極"交會路徑"就音量而言。

SAN 特定要求

- 啟用了 iSCSI、FC 或 NVMe 協定的儲存虛擬機器 (SVM)。
- 已配置客戶端的 SAN 工作負載。

一般要求

- 這"正確授權"適用於您的ONTAP版本。
- （建議）啟用多管理員驗證 (MAV)（ONTAP 9.13.1 及更高版本）。看"啟用多重管理驗證"。

在 **NAS FlexVol**磁碟區上啟用 **ARP**

您可以使用系統管理員或ONTAP CLI 在 NAS FlexVol磁碟區上啟用 ARP。具體流程會根據您的ONTAP版本而有所不同。

ONTAP 9.16.1 及更新版本

從ONTAP 9.16.1 開始，ARP/AI 可立即激活，無需學習期。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要保護的磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled -junction-path
</path_name>
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

ONTAP 9.10.1 至 **9.15.1**

對於ONTAP 9.10.1 至 9.15.1 版本，您應該先啟用 ARP。"學習模式" （或“試運轉”狀態）。該系統透過分析工作負載來描述正常行為。以主動模式啟動可能會導致過多的誤報。

建議讓 ARP 以學習模式運作至少 30 天。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習間隔並自動切換，切換可能在 30 天之前完成。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要保護的磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中選擇「在學習模式下啟用」。

你可以"停用關聯儲存虛擬機器上的自動學習活動模式轉換"如果您想手動控制學習模式到主動模式的轉換。

在現有的磁碟區中、學習和作用中模式僅適用於新寫入的資料、而不適用於磁碟區中現有的資料。不會掃描和分析現有資料、因為在啟用Volume以進行Arp之後、會根據新資料來假設先前一般資料流量的特性。

4. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有磁碟區上啟用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume dry-run`資訊，請參閱。

建立啟用 **ARP** 的新磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state dry-run -junction-path
</path_name>
```

停用自動切換（可選）：

如果您已將ONTAP升級至 ONTAP 9.13.1 至ONTAP 9.15.1，並且想要手動控制所有關聯磁碟區從學習模式切換到活動模式，則可以從 SVM 執行此操作：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

在 **NAS FlexGroup**磁碟區上啟用 **ARP**

您可以使用系統管理員或ONTAP CLI 在 NAS FlexGroup磁碟區上啟用 ARP。具體流程會根據您的ONTAP版本而有所不同。

ONTAP 9.18.1 及更高版本

從ONTAP 9.18.1 開始，ARP/AI 對FlexGroup卷立即生效，無需學習期。

系統管理員

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的FlexGroup區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有**FlexGroup**磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新**FlexGroup**區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state enabled -junction-path </path_name>
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

ONTAP 9.13.1 至 **9.17.1**

對於ONTAP 9.13.1 至 9.17.1 版本， FlexGroup磁碟區的起始版本為：“學習模式” 。該系統透過分析工作負載來描述正常行為。

建議讓 ARP 以學習模式運作至少 30 天。ARP 會自動確定最佳學習週期間隔並自動切換，切換可能在 30 天之前發生。

系統管理員

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的FlexGroup區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. 在「反勒索軟體」方塊中選擇「在學習模式下啟用」。

你可以"停用自動學習到活動模式的轉換"如果您想手動控制學習模式到主動模式的轉換。

4. 在「反勒索軟體」方塊中驗證磁碟區的 ARP 狀態。

CLI

在現有**FlexGroup**磁碟區上啟用 **ARP**：

```
security anti-ransomware volume dry-run -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新**FlexGroup**區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggr-list
<aggregate name> -aggr-list-multiplier <integer> -size <nn> -anti
-ransomware-state dry-run -junction-path </path_name>
```

停用自動切換（可選）：

如果您想手動控制從學習模式到活動模式的切換：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證**ARP**狀態：

```
security anti-ransomware volume show
```

在**SAN**磁碟區上啟用**ARP**

從ONTAP 9.17.1 開始，您可以在 SAN 磁碟區上啟用 ARP。 ARP/AI 功能會自動啟用，並在 SAN 磁碟區維護期間立即開始主動監控和保護 SAN 磁碟區。"評估期"同時確定工作負載是否適合 ARP，並設定最佳加密偵測閾值。

您可以使用系統管理員或ONTAP CLI 在 SAN 磁碟區上啟用 ARP。

系統管理員

步驟

1. 選擇“儲存 > 磁碟區”，然後選擇要保護的 SAN 磁碟區。
2. 在 * Volumes （卷） * 概述的 * Security （安全） * 選項卡中，選擇 * Status （狀態） * 以從 Disabled （已禁用）切換到 Enabled （已啓用）。
3. ARP/AI自動進入評估期。
4. 在「反勒索軟體」方塊中驗證 ARP 狀態和評估狀態。

   若要顯示所有磁碟區的 ARP 狀態：在 * Volumes （磁碟區） * 窗格中，選取 * Show （顯示） / Hide （隱藏） * ，然後確定已勾選 * Anti-勒索 ware* 狀態。

CLI

在現有 **SAN** 磁碟區上啟用 **ARP**：

```
security anti-ransomware volume enable -volume <vol_name> -vserver
<svm_name>
```

建立啟用 **ARP** 的新 **SAN** 磁碟區：

```
volume create -volume <vol_name> -vserver <svm_name> -aggregate
<aggr_name> -size <nn> -anti-ransomware-state enabled
```

驗證**ARP**狀態和評估狀態：

```
security anti-ransomware volume show
```

檢查 `Block device detection status`現場監測評估期進展。

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume show`資訊，請參閱。

相關資訊

- "在學習期間後切換至使用中模式"

在新磁碟區中，預設啟用 **ONTAP** 自主勒索軟體保護

從 ONTAP 9.10.1 開始，您可以設定儲存虛擬機器（SVM），以便預設為新磁碟區啟用自主勒索軟體防護（ARP）。您可以使用 System Manager 或 ONTAP CLI 修改此設定。

從 ONTAP 9.18.1 開始，在叢集升級或全新安裝後經過 12 小時的寬限期後，"支援的系統" 的所有新磁碟區預設會在叢集層級啟用 ARP。如果您在叢集層級停用 ARP 的自動預設啟用，仍可選擇在 SVM 層級手動為所有新磁碟區預設啟用 ARP。

對於 ONTAP 9.17.1 及更早版本，在 SVM 層級進行設定是預設在新磁碟區上啟用 ARP 的唯一方法。

關於這項工作

預設情況下，新建磁碟區的 ARP 功能是停用的。您需要啟用 ARP 功能，並將其設定為在 SVM 中建立的新磁碟區上預設為啟用。

當您變更 SVM 的預設值時，未啟用 ARP 的現有磁碟區不會自動變更 ARP 啟用狀態。本程式中所述的 SVM 設定變更僅影響新產生的磁碟區。學習如何"為現有磁碟區啟用 ARP"。

啟用 ARP 後，ARP 可能會進入過渡期，具體取決於您的環境和ONTAP版本：

Volume類型	版本**ONTAP**	啟用後的行為
NAS FlexGroup	ONTAP 9.18.1 及更高版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.13.1 至 9.17.1	ARP啟動後將進入學習模式，持續30天。
NAS FlexVol	ONTAP 9.16.1 及更新版本	ARP/AI 無需學習期即可立即生效
	ONTAP 9.10.1 至 9.15.1	ARP啟動後將進入學習模式，持續30天。
SAN 磁碟區	ONTAP 9.17.1 及更高版本	ARP/AI 立即啟動，啟動評估期，以確定合適的警報閾值，然後再從初始的保守閾值過渡。

開始之前

啟用 ARP 之前，請確保您的環境具備以下條件：

NAS 特定要求

- 啟用了 NFS 或 SMB（或兩者）協定的儲存虛擬機器 (SVM)。
- 積極"交會路徑"就音量而言。

SAN 特定要求

- 啟用了 iSCSI、FC 或 NVMe 協定的儲存虛擬機器 (SVM)。

一般要求

- 這"正確授權"適用於您的ONTAP版本。
- （建議）啟用多管理員驗證（MAV）（ONTAP 9.13.1+）。看"啟用多重管理驗證"。

步驟

您可以使用系統管理員或 ONTAP CLI 在新磁碟區上預設啟用 ARP 。

系統管理員

1. 選擇“儲存”或“叢集”（取決於您的環境），選擇“儲存虛擬機器”，然後選擇將包含要使用 ARP 保護的磁碟區的儲存虛擬機器。
2. 導航至“設定”標籤。在「安全性」下，找到「反勒索軟體」磁貼，然後選擇 。
3. 勾選此方塊以啟用反勒索軟體 (ARP)。勾選附加方塊可在儲存虛擬機器中所有符合條件的磁碟區上啟用 ARP。
4. 對於有建議學習期的ONTAP版本，請選擇「學習足夠時間後自動從學習模式切換到活動模式」。這允許 ARP 確定最佳學習間隔並自動切換到主動模式。

CLI

修改現有**SVM**，使其在新磁碟區中預設啟用**ARP**。

選擇 `dry-run`如果您的 `ARP` 版本需要學習週期。否則，請選擇 `enabled`。

```
vserver modify -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

建立一個新的**SVM**，並預設為新磁碟區啟用**ARP**。

選擇 `dry-run`如果您的 `ARP` 版本需要學習週期。否則，請選擇 `enabled`。

```
vserver create -vserver <svm_name> -anti-ransomware-default-volume
-state <dry-run|enabled>
```

修改現有**SVM**，停用自動學習到主動模式的轉換

如果您已從ONTAP 9.13.1 升級到ONTAP 9.15.1，並且預設狀態為 `dry-run`（學習模式），啟用自適應學習，以便進行更改 `enabled`狀態（活動模式）是自動完成的。您可以停用此自動切換功能，以便手動控制所有關聯音量從學習模式切換到活動模式：

```
vserver modify <svm_name> -anti-ransomware-auto-switch-from-learning-to
-enabled false
```

驗證 **ARP** 狀態

```
security anti-ransomware volume show
```

相關資訊

- "在學習期間後切換至使用中模式"
- "安全反勒索軟體卷顯示"

選擇退出 **ONTAP Autonomous Ransomware Protection** 預設啟用狀態

從 ONTAP 9.18.1 開始，對於 AFF A 系列和 AFF C 系列、ASA 和 ASA r2 系統，在升級或全新安裝後的 12 小時預熱期結束後，所有新磁碟區預設自動啟用 Autonomous Ransomware Protection（ARP），前提是已安裝 ARP 授權。您可以在 12 小時寬限期內或之後使用 System Manager 或 ONTAP CLI 選擇停用此預設功能。

現有磁碟區必須"手動啟用"用於 ARP。

關於這項工作

您可以稍後變更此程序所選擇的設定。寬限期過後，您可以隨時靈活地開啟或關閉預設啟用功能：

```
security anti-ransomware auto-enable modify -new-volume-auto-enable
false|true
```

步驟

您可以使用 System Manager 或 ONTAP CLI 來管理 ARP 預設啟用選項。

系統管理員

1. 選擇*叢集>設定*。
2. 執行下列其中一項：
   - 在作用中寬限期內停用：
     i. 在「反勒索軟體」部分，您會看到一則訊息，指示啟用 ARP 前剩餘的小時數。選取「不啟用」。
     ii. 在下一個對話方塊中選取 **Disable**，以確認已為新磁碟區關閉預設 ARP 啟用功能。
   - 寬限期過後停用：
     i. 在 **Anti-ransomware** 部分中，選取 。
     ii. 選取核取方塊，然後按一下 **Save** 以停用新磁碟區的預設 ARP 啟用功能。

CLI

1. 檢查預設啟用狀態：

   ```
   security anti-ransomware auto-enable show
   ```

2. 停用新磁碟區的預設啟用：

   ```
   security anti-ransomware auto-enable modify -new-volume-auto-enable
   false
   ```

相關資訊

- "在單一磁碟區啟用 ONTAP 自主勒索軟體防護"

在學習期間之後，在 **ONTAP ARP** 中切換至作用中模式

對於 NAS 環境，手動或自動將啟用 ARP 的磁碟區從學習模式切換到活動模式。如果您在ONTAP 9.15.1 及更早版本中使用 ARP，或在ONTAP 9.17.1 及更早版本的FlexGroup區上執行 ARP，則需要切換模式。

ARP 完成建議至少 30 天的學習模式運作後，您可以手動切換到活動模式。從ONTAP 9.13.1 開始，ARP 會自動確定最佳學習週期間隔並自動切換，切換可能在 30 天之前發生。

如果您將 ARP 與 ARP/AI 保護結合使用，則 ARP 會自動啟動。無需學習期。

> 在現有的磁碟區中、學習和作用中模式僅適用於新寫入的資料、而不適用於磁碟區中現有的資料。不會掃描和分析現有資料、因為在啟用Volume以進行Arp之後、會根據新資料來假設先前一般資料流量的特性。

在學習期間後手動切換至使用中模式

對於ONTAP 9.10.1 至 9.15.1（ONTAP 9.17.1 及更早版本，帶FlexGroup卷），學習期結束後，您可以使用系統管理器或ONTAP CLI 手動將 ARP 學習模式轉換為活動模式。

關於這項工作

本過程中所描述的學習期後手動過渡到主動模式特定於 NAS 環境。

步驟

您可以使用系統管理員或ONTAP CLI 從學習模式切換到主動模式。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取已準備好用於作用中模式的磁碟區。
2. 在 * Volumes * （卷）總覽的 * Security （安全性） * 標籤中，在 Anti-勒索 軟體方塊中選取 * Switch to active mode* （切換至作用中模式）。
3. 您可以在 * 反勒索軟體 * 方塊中驗證磁碟區的 ARP 狀態。

CLI

1. 如果尚未自動完成，則修改受保護的磁碟區以切換到活動模式：

   ```
   security anti-ransomware volume enable -volume <vol_name> -vserver
   <svm_name>
   ```

   您也可以使用modify volume命令切換至作用中模式：

   ```
   volume modify -volume <vol_name> -vserver <svm_name> -anti
   -ransomware-state enabled
   ```

2. 驗證磁碟區的ARP狀態。

   ```
   security anti-ransomware volume show
   ```

自動從學習模式切換至使用中模式

從ONTAP 9.13.1 開始，自適應學習已新增至 ARP 分析中，並且可以自動從學習模式切換到主動模式。 ARP自動從學習模式切換到主動模式的自主決策基於以下選項的配置設定：

```
-anti-ransomware-auto-switch-minimum-incoming-data-percent
-anti-ransomware-auto-switch-duration-without-new-file-extension
-anti-ransomware-auto-switch-minimum-learning-period
-anti-ransomware-auto-switch-minimum-file-count
-anti-ransomware-auto-switch-minimum-file-extension
```

如果啟用自動切換功能，即使未滿足所有條件，磁碟區也會在最多 30 天後自動切換到活動模式。此 30 天的限制是固定的，無法更改。

如需 ARP 組態選項（包括預設值）的詳細資訊、請參閱 "指令參考資料ONTAP"。

相關資訊

- "安全反勒索軟體量"

了解 SAN 磁碟區的ONTAP ARP 評估期

從ONTAP 9.17.1 開始，ARP 需要一段評估期來確定 SAN 磁碟區工作負載的熵等級是否適合勒索軟體防護。在 SAN 磁碟區上啟用 ARP 後，ARP/AI 會在評估期間主動監控並保護該磁碟區，同時確定最佳加密閾值。在評估期間，可以使用保守閾值進行檢測和發出警報，同時建立基線閾值。會區分評估後的 SAN 磁碟區中適用和不適用的工作負載，如果確定工作負載適合防護，則會根據評估期統計資料自動設定加密閾值。

理解熵評估

系統每隔 10 分鐘收集一次連續的加密統計資料。在評估期間，也會每四小時持續建立一次 ARP 定期快照。如果某個時間間隔內的加密百分比超過了為該磁碟區確定的最佳加密閾值，則會觸發警報，`Anti_ransomware_attack_backup`建立快照，並且任何定期 ARP 快照的快照保留時間都會增加。

確認評估期間有效

您可以執行下列指令，確認評估已啟動，並確認狀態為 `evaluation_period`。如果磁碟區不符合評估條件，則不會顯示評估狀態。

```
security anti-ransomware volume show -vserver <svm_name> -volume
<volume_name>
```

回應範例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : evaluation_period
```

監測評估期資料收集

您可以透過執行以下命令來即時監控加密偵測。該命令將傳回一個直方圖，顯示每個加密百分比範圍內的資料量。此直方圖每 10 分鐘更新一次。

```
security anti-ransomware volume entropy-stat show-encryption-percentage-
histogram -vserver <svm_name> -name <lun_name> -duration real_time
```

回應範例：

```
Vserver     Name              Entropy Range   Seen N Time     Data Written
----------  ----------------  --------------- --------------
-------------
vs0         lun1              0-5%            4               100MB
vs0         lun1              6-10%           10              900MB
vs0         lun1              11-15%          20              40MB
vs0         lun1              16-20%          10              70MB
vs0         lun1              21-25%          60              450MB
vs0         lun1              26-30%          4               100MB
vs0         lun1              31-35%          10              900MB
vs0         lun1              36-40%          20              40MB
vs0         lun1              41-45%          0               0
vs0         lun1              46-50%          0               0
vs0         lun1              51-55%          0               0
vs0         lun1              56-60%          0               0
vs0         lun1              61-65%          0               0
vs0         lun1              66-70%          0               0
vs0         lun1              71-75%          0               0
vs0         lun1              76-80%          0               0
vs0         lun1              81-85%          0               0
vs0         lun1              86-90%          0               0
vs0         lun1              91-95%          0               0
vs0         lun1              96-100%         0               0

20 entries were displayed.
```

合適的工作負荷和自適應閾值

評估以下列結果之一作結：

- 此工作負載適用於 **ARP**。 ARP會自動將自適應閾值設定為高於評估期間最大加密百分比的 10%。 ARP也會持續收集統計資料並定期建立 ARP 快照。
- 該工作負載不適合 **ARP**。 ARP會自動將自適應閾值設定為評估期間內可見的最大加密百分比。 ARP也會繼續收集統計資料並定期建立 ARP 快照，但係統最終會建議在該磁碟區上停用 ARP。

確定評估結果

評估期結束後，ARP會根據評估結果自動設定自適應閾值。

您可以透過執行以下命令來確定評估結果。卷適用性顯示在 `Block device detection status`場地：

```
security anti-ransomware volume show  -vserver <svm_name> -volume
<volume_name>
```

回應範例：

```
Vserver Name                                : vs1
Volume Name                                 : v1
State                                       : enabled
Attack Probability                          : none
Attack Timeline                             : -
Number of Attacks                           : -
Attack Detected By                          : -
Block device detection status               : Active_suitable_workload

Block device evaluation start time :  5/16/2025 01:49:01
```

您也可以顯示評估結果所採用的值閾值：

```
security anti-ransomware volume attack-detection-parameters show -vserver
<svm_name> -volume <volume_name>
```

回應範例：

```
                                  Vserver Name : vs_1

                                   Volume Name : vm_2

Block Device Auto Learned Encryption Threshold : 10
...
```

暫停 ONTAP 自主勒索軟體保護，將工作負載事件排除在分析之外

如果您預期會發生異常的工作負載事件、可以隨時暫停並恢復自發勒索軟體保護（Arp）分析。

從 ONTAP 9.13.1 開始，您可以啟用多重管理驗證（ MAV ），以便需要兩個或多個已驗證的使用者管理員才能暫停 ARP 。

"深入瞭解MAV"。

關於這項工作

在 ARP 暫停期間， ONTAP不會記錄新寫入的事件或操作；但是，對早期日誌的分析會在背景繼續進行。

> 請勿使用 ARP 停用功能來暫停分析。這樣做會停用磁碟區上的Arp、並會遺失所有有關已學習工作負載行為的現有資訊。這需要重新啟動學習期間。

步驟

您可以使用系統管理員或 ONTAP CLI 來暫停 ARP 。

系統管理員

1. 選取 * 儲存 > 磁碟區 * 、然後選取您要暫停 ARP 的磁碟區。
2. 在卷概覽的「安全性」標籤中，選擇「反勒索軟體」方塊中的「暫停反勒索軟體」。

> 從ONTAP 9.13.1 開始，如果您使用 MAV 來保護 ARP 設置，暫停操作會提示您獲得一個或多個其他管理員的批准。"必須收到所有管理員的核准"與 MAV 審批小組相關，否則操作將會失敗。

3. 若要恢復監控，請選擇*恢復反勒索軟體*。

CLI

1. 在磁碟區上暫停ARP：

```
security anti-ransomware volume pause -vserver <svm_name> -volume
<vol_name>
```

2. 若要繼續處理、請使用 `resume` 命令：

```
security anti-ransomware volume resume -vserver <svm_name> -volume
<vol_name>
```

如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume`資訊，請參閱。

3. 如果您使用 MAV（從ONTAP 9.13.1 開始與 ARP 一起使用）來保護 ARP 設置，則暫停操作會提示您獲得一個或多個其他管理員的批准。必須獲得與 MAV 審批組相關的所有管理員的批准，否則操作將失敗。

   如果您使用的是 MAV 、而預期的暫停作業需要額外核准、則每位 MAV 群組核准者都會執行下列動作：

   a. 顯示要求：

   ```
   security multi-admin-verify request show
   ```

   b. 核准申請：

   ```
   security multi-admin-verify request approve -index[<number
   returned from show request>]
   ```

   最後一個群組核准者的回應表示該磁碟區已修改、而且 ARP 狀態已暫停。

   如果您使用的是 MAV 、而且您是 MAV 群組核准者、您可以拒絕暫停作業要求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

+
如"指令參考資料ONTAP"需詳細 `security multi-admin-verify request`資訊，請參閱。

管理 ONTAP 自主勒索軟體保護攻擊偵測參數

從 ONTAP 9.11.1 開始，您可以在啟用自動勒索軟體保護的特定磁碟區上修改勒索軟體偵測的參數，並將已知的激增報告為正常檔案活動。調整偵測參數有助於根據您的特定 Volume 工作負載、提高報告的準確度。

攻擊偵測的運作方式

當自主勒索軟體防護 (ARP) 處於學習或評估模式時，它會為卷宗行為制定基準值。這些基準值包括熵、檔案副檔名以及（從ONTAP 9.11.1 開始的）IOPS。這些基準用於評估勒索軟體威脅。有關這些標準的更多信息，請參閱"ARP 偵測到什麼" 。

不同的資料量和工作負載需要不同的偵測參數。例如，啟用 ARP 的磁碟區可能託管多種類型的檔案副檔名，在這種情況下，您可能需要將從未見過的檔案副檔名的閾值計數修改為大於預設值 20 的數字，或停用基於從未見過的檔案副檔名的警告。從ONTAP 9.11.1 開始，您可以修改攻擊偵測參數，使其更適應您的特定工作負載。

從 ONTAP 9.14.1 開始，您可以在 ARP 觀察到新的副檔名，以及 ARP 建立快照時，設定警示。如需更多資訊、請參閱 [modify-alerts]。

NAS 環境中的攻擊偵測

在 ONTAP 9.10.1 中、如果 ARP 偵測到下列兩種情況、就會發出警告：

- 超過 20 個檔案的副檔名先前未在磁碟區中觀察到
- 高 Entropy 資料

從 ONTAP 9.11.1 開始，如果符合 _ 僅 _ 一個條件， ARP 就會發出威脅警告。例如，如果在 24 小時內觀察到超過 20 個檔案的副檔名，而這些副檔名先前未在磁碟區中觀察到，則 ARP 會將此歸類為威脅（無論觀察到的 Entropy 為何）。24 小時和 20 個檔案值為預設值，可加以修改。

> 若要減少大量誤報，請前往“儲存”>“磁碟區”>“安全性”>“設定工作負載特性”，並停用“監控新檔案類型”。此設定在ONTAP 9.14.1 P7、9.15.1 P1、9.16.1 及更高版本中預設為停用。

SAN 環境中的攻擊偵測

從ONTAP 9.17.1 開始，如果 ARP 偵測到超過自動學習閾值的高加密速率，則會發出警告。此閾值是在"評估期"但可以修改。

修改攻擊偵測參數

根據啟用 ARP 的磁碟區的預期行為，您可能需要修改攻擊偵測參數。

步驟

1. 檢視現有的攻擊偵測參數：

```
security anti-ransomware volume attack-detection-parameters show
-vserver <svm_name> -volume <volume_name>
```

```
security anti-ransomware volume attack-detection-parameters show
-vserver vs1 -volume vol1
                                              Vserver Name : vs1
                                               Volume Name : vol1
           Block Device Auto Learned Encryption Threshold : 10
            Is Detection Based on High Entropy Data Rate? : true
  Is Detection Based on Never Seen before File Extension? : true
                 Is Detection Based on File Create Rate? : true
                 Is Detection Based on File Rename Rate? : true
                 Is Detection Based on File Delete Rate? : true
           Is Detection Relaxing Popular File Extensions? : true
                High Entropy Data Surge Notify Percentage : 100
                 File Create Rate Surge Notify Percentage : 100
                 File Rename Rate Surge Notify Percentage : 100
                 File Delete Rate Surge Notify Percentage : 100
 Never Seen before File Extensions Count Notify Threshold : 5
       Never Seen before File Extensions Duration in Hour : 48
```

2. 所有顯示的欄位均可使用布林值或整數值進行修改。若要修改字段，請使用 `security anti-ransomware volume attack-detection-parameters modify`命令。

   如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume attack-detection-parameters modify`資訊，請參閱。

回報已知的突波

即使在作用中， ARP 仍會繼續修改偵測參數的基準值。如果您知道 Volume 活動的突波，一次性突波或是屬於新常態特徵的突波，您應該將它們回報為安全的。手動回報這些突波的安全性、有助於提高 ARP 威脅評估的準確度。

回報一次性突波

1. 如果已知情況下發生一次性喘振、而您希望 ARP 在未來的情況下回報類似的喘振、請清除工作負載行為中的喘振：

```
security anti-ransomware volume workload-behavior clear-surge -vserver
<svm_name> -volume <volume_name>
```

   如"指令參考資料ONTAP"需詳細 `security anti-ransomware volume workload-behavior clear-surge`資訊，請參閱。

修改基準突波

1. 如果回報的喘振應視為正常應用程式行為、請回報喘振、以修改基準喘振值。

```
security anti-ransomware volume workload-behavior update-baseline-from-
surge -vserver <svm_name> -volume <volume_name>
```

詳細了解 `security anti-ransomware volume workload-behavior update-baseline-from-surge`在"指令參考資料ONTAP" 。

設定 **ARP** 警示

從 ONTAP 9.14.1 開始， ARP 可讓您指定兩個 ARP 事件的警示：

- 觀察磁碟區上的新副檔名
- 建立 ARP 快照

這兩個事件的警示可在個別磁碟區或整個 SVM 上設定。如果您啟用 SVM 的警示、則警示設定只會由啟用警示後建立的磁碟區繼承。根據預設、警示不會在任何磁碟區上啟用。

事件警報可透過多管理員驗證進行控制。有關更多信息，請參閱"使用 ARP 保護的磁碟區進行多重管理驗證" 。

步驟

您可以使用系統管理員或ONTAP CLI 設定 ARP 事件警報。

系統管理員

設定磁碟區的警示

1. 導航到“卷”。選擇要修改設定的單一磁碟區。
2. 選擇“安全”選項卡，然後選擇“事件嚴重性設定”。
3. 若要接收「偵測到新檔案副檔名」和「已建立勒索軟體快照」的警報，請選擇「嚴重性」標題下的下拉式功能表。將設定從「不產生事件」修改為「通知」。
4. 選擇*保存*。

設定 **SVM** 的警示

1. 導覽至 儲存虛擬機器，然後選擇要啟用設定的 SVM。
2. 在「安全性」標題下，找到「反勒索軟體」標籤。選擇然後*編輯勒索軟體事件嚴重性*。
3. 若要接收「偵測到新檔案副檔名」和「已建立勒索軟體快照」的警報，請選擇「嚴重性」標題下的下拉式功能表。將設定從「不產生事件」修改為「通知」。
4. 選擇*保存*。

CLI

設定磁碟區的警示

- 若要設定新副檔名的警示：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-new-file-extension-seen true`
```

- 若要設定建立 ARP 快照的警示：

```
security anti-ransomware volume event-log modify -vserver <svm_name>
-volume <volume_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用確認您的設定 `anti-ransomware volume event-log show` 命令。

設定 **SVM** 的警示

- 若要設定新副檔名的警示：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-new-file-extension-seen true
```

- 若要設定建立 ARP 快照的警示：

```
security anti-ransomware vserver event-log modify -vserver
<svm_name> -is-enabled-on-snapshot-copy-creation true
```

- 使用確認您的設定 `security anti-ransomware vserver event-log show` 命令。

詳細了解 `security anti-ransomware vserver event-log`命令"指令參考資料ONTAP" 。

相關資訊

- "瞭解自主勒索軟體保護攻擊和自主勒索軟體保護快照"。
- "指令參考資料ONTAP"

回應 ONTAP ARP 偵測到的異常活動

當自發勒索軟體保護（Arp）偵測到受保護磁碟區中的異常活動時、就會發出警告。您應該評估通知、以判斷該活動是否可接受（誤判）、或攻擊是否看起來惡意。將攻擊分類後，您可以清除可疑檔案的警告和注意事項。

對攻擊進行分類時，ARP 快照要麼在分類作業啟動後保留一段較短的時間（ONTAP 9.16.1 及更高版本），要麼立即刪除（ONTAP 9.15.1 及更早版本）。

從ONTAP 9.11.1 開始，您可以修改"保留設定"用於 ARP 快照。

關於這項工作

當 ARP 偵測到高資料熵、包含資料加密的異常磁碟區活動以及異常檔案副檔名的任意組合時，它會顯示可疑檔案清單。從適用於 NAS 和 SAN 環境的ONTAP 9.17.1 開始，系統管理員中的「反勒索軟體」頁面也會報告熵峰值的詳細資訊。

當發出 ARP 警告通知時，透過以下兩種方式之一指定活動進行回應：

- * 誤判 *

  已識別的文件類型或熵峰值是您的工作負載中預期會出現的，可以忽略。

- * 可能的勒索軟體攻擊 *

  所識別的文件類型或熵峰值在您的工作負載中是意外的，應被視為潛在攻擊。

在您更新您的決定並清除 ARP 通知後，系統將恢復正常監控。 ARP會將您的評估記錄到威脅評估設定檔中，並使用您的選擇來監控後續的檔案活動。

如果是可疑的攻擊、您必須判斷它是否為攻擊、如果是攻擊、請回應、並在清除通知之前還原受保護的資料。 "深入瞭解如何從勒索軟體攻擊中恢復"。

如果您還原整個磁碟區、則沒有要清除的通知。

開始之前

ARP 必須主動保護卷，而不是處於學習或評估模式。

步驟

您可以使用系統管理員或 ONTAP CLI 來回應異常活動。

系統管理員

1. 當您收到「異常活動」通知時，請點擊連結。或者，導覽至「磁碟區」概覽的「安全性」標籤。

   警告會顯示在 * 事件 * 功能表的 * 總覽 * 窗格中。

2. 在「安全」標籤中，查看可疑檔案類型或熵峰值報告。
   - 對於可疑文件，請檢查「可疑文件類型」對話方塊中的每種文件類型，並分別標記。
   - 對於熵峰值，請檢查熵報告。
3. 記錄你的答案：

如果選擇此值…	請採取此行動…
誤判	a. 執行下列其中一項： ◦ 對於文件類型警告，選擇*更新並清除可疑文件類型*。 ◦ 對於熵尖峰，選擇*標記為假陽性*。 這些操作可清除有關可疑文件或活動的警告通知。 ARP隨後將恢復對磁碟區的正常監控。對於ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，清除可疑檔案類型後，相關的 ARP 快照會自動刪除。 ⓘ 從ONTAP 9.13.1 開始，如果您使用 MAV 來保護 ARP 設置，清除可疑項目操作會提示您獲得一個或多個其他管理員的批准。"必須收到所有管理員的核准"與 MAV 審批小組相關，否則操作將會失敗。
可能的勒索軟體攻擊	a. 回應攻擊： ◦ 對於文件類型警告，將選定的文件標記為*潛在勒索軟體攻擊*，並"還原受保護的資料" 。 ◦ 對於表示攻擊的熵峰值，選擇「標記為潛在勒索軟體攻擊」並"還原受保護的資料" 。 b. 資料恢復完成後，記錄您的決定並恢復正常的ARP監控： ◦ 對於文件類型警告，選擇*更新並清除可疑文件類型*。 ◦ 對於熵峰值，選擇*標記為潛在勒索軟體攻擊*並選擇*儲存並關閉*。 ⓘ 如果您已還原整個磁碟區，則無需清除任何可疑文件類型通知。 記錄您的決定將清除攻擊報告。對於ONTAP 9.16.1 及更高版本中的 ARP/AI ，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，還原磁碟區後，ARP 快照將自動刪除。

CLI

驗證攻擊

1. 當您收到可疑勒索軟體攻擊的通知時、請確認攻擊的時間和嚴重性：

```
security anti-ransomware volume show -vserver <svm_name> -volume
<vol_name>
```

範例輸出：

```
Vserver Name: vs0
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 5/12/2025 01:03:23
Number of Attacks: 1
Attack Detected By: encryption_percentage_analysis
```

您也可以檢查EMS訊息：

```
event log show -message-name callhome.arw.activity.seen
```

2. 產生攻擊報告並指定儲存位置：

```
security anti-ransomware volume attack generate-report -vserver
<svm_name> -volume <vol_name> -dest-path
<[svm_name]:[junction_path/sub_dir_name]>
```

命令範例：

```
security anti-ransomware volume attack generate-report -vserver vs0
-volume vol1 -dest-path vs0:vol1
```

範例輸出：

```
Report "report_file_vs0_vol1_14-09-2021_01-21-08" available at path
"vs0:vol1/"
```

3. 在管理用戶端系統上檢視報告。例如：

```
cat report_file_vs0_vol1_14-09-2021_01-21-08
```

採取行動

1. 根據您對檔案副檔名或熵峰值的評估，請執行以下操作之一：

   - 誤判

     執行以下命令之一來記錄您的決定並恢復正常的自主勒索軟體防護監控：

     - 對於檔案副檔名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension_identifiers>] -false
       -positive true
       ```

       使用下列選用參數，僅將特定副檔名識別為誤報：

       - `[-extension <text>, … ]`：檔案副檔名

     - 對於熵尖峰：

       ```
       security anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
       HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive true
       ```

   - 可能的勒索軟體攻擊

     回應攻擊和 "從 ARP 建立的備份快照中恢復資料"。執行以下命令之一記錄您的決定並恢復正常的 ARP 監控：

     - 對於檔案副檔名：

       ```
       anti-ransomware volume attack clear-suspect -vserver
       <svm_name> -volume <vol_name> [<extension identifiers>] -false
       -positive false
       ```

       請使用下列選用參數，僅將特定的擴充功能識別為可能的勒索軟體：

       - `[-extension <text>, … ]`：檔案副檔名

     - 對於熵尖峰：

```
security anti-ransomware volume attack clear-suspect -vserver
<svm_name> -volume <vol_name> -start-time <MM/DD/YYYY
HH:MM:SS> -end-time <MM/DD/YYYY HH:MM:SS> -false-positive
false
```

這 `clear-suspect`操作會清除攻擊報告。如果您還原了整個磁碟區，則無需清除任何可疑檔案類型通知。對於ONTAP 9.16.1 及更高版本中的 ARP/AI，ARP 快照會在分類操作觸發的縮短保留期後自動刪除。對於ONTAP 9.15.1 及更早版本，還原磁碟區或清除可疑事件後，ARP 快照會自動刪除。

2. 從 9.18.1 版本開始，您可以確定以下狀態： `clear-suspect`手術：

```
security anti-ransomware volume show -clear-suspect-status -volume
<vol_name> -vserver <svm_name>
```

MAV選項

1. 如果您使用的是 MAV 、而且是預期的 `clear-suspect` 作業需要額外核准、每位 MAV 群組核准者必須：

   a. 顯示要求：

   ```
   security multi-admin-verify request show
   ```

   b. 核准恢復正常反勒索軟體監控的要求：

   ```
   security multi-admin-verify request approve -index[<number
   returned from show request>]
   ```

   最後一個群組核准者的回應表示已修改磁碟區、並記錄誤報。

2. 如果您使用的是 MAV 、而您是 MAV 群組核准者、您也可以拒絕明確可疑的要求：

```
security multi-admin-verify request veto -index[<number returned
from show request>]
```

相關資訊

- "NetApp知識庫：了解自主勒索軟體防護攻擊與自主勒索軟體防護快照"
- "修改自動快照選項"
- "安全反勒索軟體量"
- "安全多管理員驗證請求"

在勒索軟體攻擊之後，從 **ONTAP ARP** 快照還原資料

自主勒索軟體防護 (ARP) 會建立快照來防禦潛在的勒索軟體威脅。您可以使用其中一個 ARP 快照或磁碟區的其他快照來還原資料。

關於這項工作

ARP 使用以下前綴名稱之一建立快照：

- `Anti_ransomware_periodic_backup` ：在ONTAP 9.17.1 及更高版本中用於定期建立的快照。例如，`Anti_ransomware_periodic_backup.2025-06-01_1248` 。
- `Anti_ransomware_attack_backup`：在ONTAP 9.17.1 及更高版本中用於回應異常而建立的快照。例如，`Anti_ransomware_attack_backup.2025-08-25_1248` 。
- `Anti_ransomware_backup` ：在ONTAP 9.16.1 及更早版本中，用於為應對異常而建立的快照。例如，`Anti_ransomware_backup.2022-12-20_1248` 。

要從快照中恢復， `Anti_ransomware`快照 辨識出系統攻擊後，必須先釋放ARP快照。

如果沒有報告系統攻擊，您必須先從 `Anti_ransomware`快照，然後從您選擇的快照完成磁碟區的後續還原。

如果受 ARP 保護的磁碟區屬於SnapMirror關係，則從快照還原磁碟區後，您需要手動更新該磁碟區的所有映像副本。如果跳過此步驟，鏡像副本可能會變得不可用，需要刪除並重新建立。

開始之前

"您必須將攻擊標記為潛在的勒索軟體攻擊"從快照恢復資料之前。

步驟

您可以使用System Manager或ONTAP NetApp CLI來還原資料。

系統管理員

系統攻擊後還原

1. 若要從 ARP 快照還原，請跳至步驟二。若要從較早的快照還原，您必須先釋放 ARP 快照的鎖定。
   a. 選擇*儲存>磁碟區*。
   b. 選擇 * 安全 * ，然後 * 檢視可疑的檔案類型 * 。
   c. 將檔案標記為「可能的勒索軟體攻擊」。
   d. 選擇 * 更新 * 和 * 清除可疑檔案類型 * 。
2. 在磁碟區中顯示快照：

   選擇 * 儲存 > Volumes （磁碟區） * 、然後選擇 Volume （磁碟區）和 * Snapshot Copies （ * 快照複本） * 。
3. 選取：您要還原的快照旁的 * 還原 * 。

如果未識別出系統攻擊、請進行還原

1. 在磁碟區中顯示快照：

   選擇 * 儲存 > Volumes （磁碟區） * 、然後選擇 Volume （磁碟區）和 * Snapshot Copies （ * 快照複本） * 。
2. 選擇：然後選擇 `Anti_ransomware`快照。
3. 選擇*還原*。
4. 返回 * Snapshot Copies （快照複本） * 功能表，然後選擇您要使用的快照。選擇*還原*。

CLI

系統攻擊後還原

若要從 ARP 快照還原，請跳至步驟二。若要還原舊版快照的資料，您必須釋放 ARP 快照的鎖定。

> 如果您使用的命令如下所述，則只有在從先前的快照還原之前，才需要先釋放反勒索軟體 SnapLock `volume snapshot restore` 。如果您使用 FlexClone ，單一檔案貼齊還原或其他方法還原資料，則不需要這麼做。

1. 將攻擊標記為潛在的勒索軟體攻擊(`-false-positive false` ）並清除可疑文件(`clear-suspect`):

   ```
   anti-ransomware volume attack clear-suspect -vserver <svm_name>
   -volume <vol_name> [<extension identifiers>] -false-positive false
   ```

   使用以下參數之一來識別擴充：

   - `[-seq-no integer]` ：可疑清單中文件的序號。
   - `[-extension text, … ]` ：檔案副檔名
   - `[-start-time date_time -end-time date_time]` ：需要清除的檔案範圍的開始和結束時

間，格式為「MM/DD/YYYY HH:MM:SS」。

2. 列出磁碟區中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下範例顯示中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

3. 從快照還原磁碟區的內容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

下列範例還原的內容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

如果未識別出系統攻擊、請進行還原

1. 列出磁碟區中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下範例顯示中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 從快照還原磁碟區的內容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

下列範例還原的內容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

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

相關資訊

- "NetApp知識庫： ONTAP中的勒索軟體預防與恢復"
- "指令參考資料ONTAP"

調整自動產生的 ARP 快照的設置

從 ONTAP 9 · 11.1 開始，您可以使用 CLI 來控制自動產生的勒索軟體保護（ ARP ）快照保留設定，以因應可疑的勒索軟體攻擊。

開始之前

您只能修改"節點SVM"而不適用於其他類型的 SVM。

步驟

1. 顯示所有目前的 ARP 快照設定：

```
options -option-name arw*
```

2. 顯示選取的目前 ARP 快照設定：

```
options -option-name <arw_setting_name>
```

3. 修改 ARP 快照設定：

```
options -option-name <arw_setting_name> -option-value
<arw_setting_value>
```

您可以修改以下設定：

> 從ONTAP 9.17.1 開始，部分所述命令已棄用。 ONTAPONTAP中引入的指令同時支援 NAS 和 SAN 環境。

設定	說明	支援的版本
`arw.snap.max.count`	指定任意給定時間卷中可存在的 ARP 快照的最大數量。系統會刪除較舊的副本，以確保 ARP 快照的總數不會超過此指定限制。	更新版本ONTAP
`arw.snap.create.interval.hours`	指定 ARP 快照之間的間隔（以小時為單位）。當懷疑存在基於資料熵的攻擊且最近建立的 ARP 快照早於指定間隔時，將建立新的 ARP 快照。	更新版本ONTAP
`arw.snap.normal.retain.interval.hours`	指定 ARP 快照的保留時長（以小時為單位）。當 ARP 快照達到保留閾值時，將被刪除。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.max.retain.interval.days`	指定可以保留 ARP 快照的最長持續時間（以天為單位）。如果磁碟區未回報任何攻擊，則會刪除任何早於此持續時間的 ARP 快照。 > 如果偵測到中度威脅，就會忽略 ARP 快照的最大保留時間間隔。針對威脅所建立的 ARP 快照會保留，直到您回應威脅為止。當您將威脅標示為誤判時， ONTAP 會刪除該磁碟區的 ARP 快照。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用

設定	說明	支援的版本
`arw.snap.create.interval.hours.post.max.count`	當磁碟區已包含最大數量的 ARP 快照時，指定 ARP 快照之間的間隔（以小時為單位）。達到最大數量時，將刪除一個 ARP 快照，為新副本騰出空間。使用此選項可以降低新 ARP 快照的建立速度，以保留舊副本。如果磁碟區已包含最大數量的 ARP 快照，則下次建立 ARP 快照時將使用此選項中指定的間隔，而不是 `arw.snap.create.interval.hours` 。	• ONTAP 9.11.1 至 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.low.encryption.retain.duration.hours`	指定在加密活動較少期間建立的 ARP 快照的保留時間（以小時為單位）。	• ONTAP 9.17.1 及更高版本
`arw.snap.new.extns.interval.hours`	指定偵測到新檔案副檔名時建立 ARP 快照的間隔（以小時為單位）。偵測到新檔案副檔名時會建立一個新的 ARP 快照；上一個在偵測到新檔案副檔名時所建立的快照早於此指定的間隔。在頻繁建立新檔案副檔名的工作負載上，此間隔有助於控制 ARP 快照的頻率。此選項獨立於 `arw.snap.create.interval.hours` ，指定基於資料熵的 ARP 快照的間隔。	• ONTAP 9.11.1 升級至ONTAP 9.16.1 • 在ONTAP 9.17.1 及更高版本中已棄用
`arw.snap.retain.hours.after.clear.suspect.false.alert`	指定在管理員將攻擊事件標記為誤報後，ARP 快照作為預防措施保留的時間間隔（以小時為單位）。在此預防性保留期到期後，可能會根據選項定義的標準保留期限刪除快照 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更新版本
`arw.snap.retain.hours.after.clear.suspect.real.attack`	指定管理員將攻擊事件標記為真實攻擊後，ARP 快照作為預防措施保留的時間間隔（以小時為單位）。在此預防性保留期到期後，可能會根據選項定義的標準保留期限刪除快照。 `arw.snap.normal.retain.interval.hours`和 `arw.snap.max.retain.interval.days` 。	• ONTAP 9.16.1 及更新版本
`arw.snap.surge.interval.days`	指定為回應 IO 突波而建立的 ARP 快照之間的間隔（以天為單位）。當 IO 流量激增且上次建立的 ARP 快照快照比此指定時間間隔還早時， ONTAP 會建立 ARP 快照突波複本。此選項也會指定 ARP 喘振快照的保留期間（以天為單位）。	更新版本ONTAP
`arw.high.encryption.alert.enabled`	啟用高級別加密警報。當此選項設定為 `on` （預設），當ONTAP百分比超過 `arw.high.encryption.percentage.threshold` 。	ONTAP 9.17.1 及更高版本
`arw.high.encryption.percentage.threshold`	指定卷的最大加密百分比。如果加密百分比超過此閾值，則ONTAP會將加密百分比的增加視為攻擊，並建立 ARP 快照。 `arw.high.encryption.alert.enabled`必須設定為 `on`以使此選項生效。	ONTAP 9.17.1 及更高版本

設定	說明	支援的版本
`arw.snap.high.encryption.retain.duration.hours`	指定在高加密閾值事件期間建立的快照的保留持續時間間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本

4. 如果您在 SAN 環境中使用 ARP，您也可以修改以下評估期設定：

設定	說明	支援的版本
`arw.block_device.auto.learn.threshold.min_value`	指定區塊設備評估的自動學習階段的最小加密閾值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.auto.learn.threshold.max_value`	指定區塊設備評估的自動學習階段的最大加密閾值百分比值。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_hours`	指定在設定加密閾值之前評估階段必須運行的最小間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.max_hours`	指定在設定加密閾值之前評估階段必須運行的最大間隔（以小時為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.min_data_ingest_size_GB`	指定在設定加密閾值之前評估階段必須提取的最小資料量（以 GB 為單位）。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.enabled`	指定是否在區塊設備上啟用 ARP 評估階段的警報。預設值為 `True` 。	ONTAP 9.17.1 及更高版本
`arw.block_device.evaluation.phase.alert.threshold`	指定區塊設備上 ARP 評估階段的閾值百分比。如果加密百分比超過此閾值，則會觸發警報。	ONTAP 9.17.1 及更高版本

相關資訊

- "威脅評估和 ARP 快照"
- "SAN熵評估期"

使用 **AI** （ **ARP/AI** ）更新 **ONTAP** 自主勒索軟體保護

為了隨時掌握最新的勒索軟體威脅防護， ARP/AI 提供在一般 ONTAP 發行時程之外自動更新。

從ONTAP 9.16.1 開始，除系統和韌體更新外，系統管理器軟體下載中還提供 ARP/AI 安全性更新。如果您的ONTAP叢集已註冊"自動系統與韌體更新" ，當 ARP/AI 安全性更新可用時，系統會自動通知您。您也可以更改您的更新偏好以便ONTAP自動安裝安全性更新。

如果您想要手動更新 ARP/AI，可以從 NetApp 支援網站下載更新，然後使用系統管理員進行安裝。

關於這項工作

您只能使用系統管理員更新 ARP/AI。

選取 **ARP/AI** 的更新偏好選項

在系統管理員中，安全文件的啟用自動更新頁面上的設定被設定為 `Show notifications`如果您已註冊自動韌體和系統更新，您可以變更更新設定以 `Automatically update`如果您希望ONTAP自動套用最新更新。如果您使用暗網或希望手動執行更新，您可以選擇顯示通知或自動關閉安全性更新。

開始之前

如需自動安全性更新，請參閱"應啟用 AutoSupport 和 AutoSupport OnDemand ，傳輸傳輸協定應設定為 HTTPS"。

步驟

1. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
2. 在 * 軟體更新 * 區段中，選擇 → 。
3. 從 * 軟體更新 * 頁面，選取 * 所有其他更新 * 索引標籤。
4. 選取 * 所有其他更新 * 索引標籤，然後按一下 * 更多 * 。
5. 選取 * 編輯自動更新設定 * 。
6. 從「自動更新設定」頁面，選取 * 安全檔案 * 。
7. 指定要對安全檔案採取的行動（ ARP/AI 更新）。

   您可以選擇自動更新，顯示通知或自動關閉更新。

   ⓘ 若要自動更新安全性更新，應啟用 AutoSupport 和 AutoSupport OnDemand ，並將傳輸通訊協定設定為 HTTPS 。

8. 接受條款與條件、然後選取 * 儲存 * 。

使用最新的安全套件手動更新 **ARP/AI**

視您是否已向 Active IQ Unified Manager 註冊而定，請遵循適當的程序。

ⓘ 請務必僅安裝比目前版本更新的 ARP 更新，以免任何非預期的 ARP 降級。

ONTAP 9 。 16.1 及更新版本，搭配數位顧問

1. 在 System Manager 中、前往 * 儀表板 * 。

   在 * 狀況 * 區段中，如果叢集有任何建議的安全性更新，則會顯示一則訊息。

2. 按一下警示訊息。
3. 在建議更新清單中的安全性更新旁，選取 * 動作 * 。
4. 按一下 * 更新 * 立即安裝更新、或按 * 排程 * 排程稍後更新。

   如果已排程更新、您可以 * 編輯 * 或 * 取消 * 。

ONTAP 9 。 16.1 及更新版本，不含數位顧問

1. 瀏覽"NetApp 支援網站"並登入。
2. 完成提示並下載您要用來更新叢集 ARP/AI 的安全套件。
3. 將檔案複製到網路上的 HTTP 或 FTP 伺服器，或複製到可使用 ARP/AI 的叢集可存取的本機資料夾。
4. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
5. 在 * 軟體更新 * 中，選取 * 所有其他更新 * 索引標籤。
6. 在 * 手動更新 * 窗格中，按一下 * 新增安全檔案 * ，然後使用下列其中一個偏好設定來新增檔案：
   - * 從伺服器下載 * ：輸入安全檔案套件的 URL 。
   - * 從本機用戶端上傳 * ：瀏覽至下載的 TGZ 檔案。

   請確定檔案名稱以開頭，並具有 `.tgz`副檔名 `ontap_security_file_arpai_`。
7. 按一下 * 新增 * 以套用更新。

驗證 **ARP/AI** 更新

若要檢視已關閉或安裝失敗的自動更新歷程記錄，請執行下列步驟：

1. 在 System Manager 中，按一下 * 叢集 > 設定 > 軟體更新 * 。
2. 在 * 軟體更新 * 區段中，選擇→。
3. 在 * 軟體更新 * 頁面中，選取 * 所有其他更新 * 索引標籤，然後按一下 * 更多 * 。
4. 選取 * 檢視所有自動更新 * 。

相關資訊

- "了解ARP/AI"
- "軟體更新的電子郵件訂閱"

使用 VScan 保護病毒

了解 ONTAP Vscan 的防毒配置

VScan 是由 NetApp 開發的防毒掃描解決方案、可讓客戶保護資料免於受到病毒或其他惡意程式碼的侵害。

當用戶端透過 SMB 存取檔案時、 VScan 會執行病毒掃描。您可以將 VScan 設定為隨需或依排程進行掃描。您

可以使用 ONTAP 命令列介面（ CLI ）或 ONTAP 應用程式設計介面（ API ）與 VScan 互動。

相關資訊

"VScan 合作夥伴解決方案"

關於NetApp防毒保護

了解 **NetApp** 使用 **ONTAP Vscan** 進行病毒掃描

VScan 是由 NetApp 開發的防毒掃描解決方案、可讓客戶保護資料免於受到病毒或其他惡意程式碼的侵害。它結合了合作夥伴提供的防毒軟體與 ONTAP 功能、讓客戶能夠靈活地管理檔案掃描。

掃毒的運作方式

儲存系統會將掃描作業卸載至裝載協力廠商防毒軟體的外部伺服器。

根據使用中的掃描模式、當用戶端透過 SMB （存取時）存取檔案或存取特定位置、排程或立即（隨需）的檔案時、 ONTAP 會傳送掃描要求。

- 當用戶端透過SMB開啟、讀取、重新命名或關閉檔案時、您可以使用「存取時掃描」來檢查是否有病毒。檔案作業會暫停、直到外部伺服器回報檔案的掃描狀態為止。如果檔案已掃描完畢、ONTAP 則支援檔案操作。否則、它會要求伺服器進行掃描。

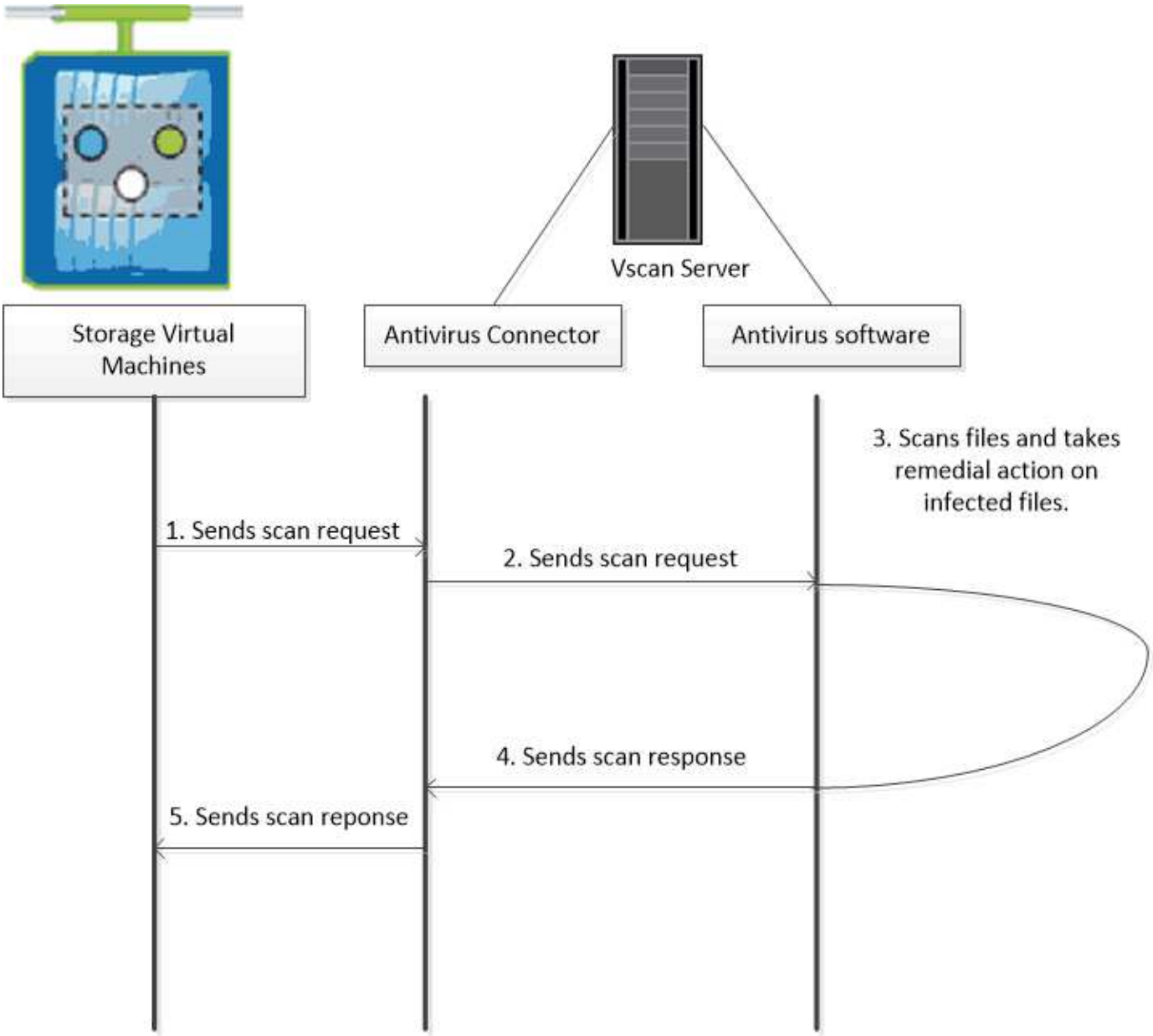
  NFS不支援存取時掃描。

- 您可以使用隨需掃描_來立即或排程檢查檔案是否有病毒。我們建議隨選掃描只在非尖峰時間執行、以避免現有的 AV 基礎架構過載、而這種基礎架構通常會設定為存取掃描的大小。外部伺服器會更新已核取檔案的掃描狀態、以便透過 SMB 降低檔案存取延遲。如果有檔案修改或軟體版本更新、它會要求從外部伺服器進行新的檔案掃描。

  您可以針對SVM命名空間中的任何路徑使用隨需掃描、即使是僅透過NFS匯出的磁碟區也一樣。

您通常可以在 SVM 上同時啟用存取和隨選掃描模式。在任一模式中、防毒軟體都會根據您的軟體設定、針對受感染的檔案採取補救行動。

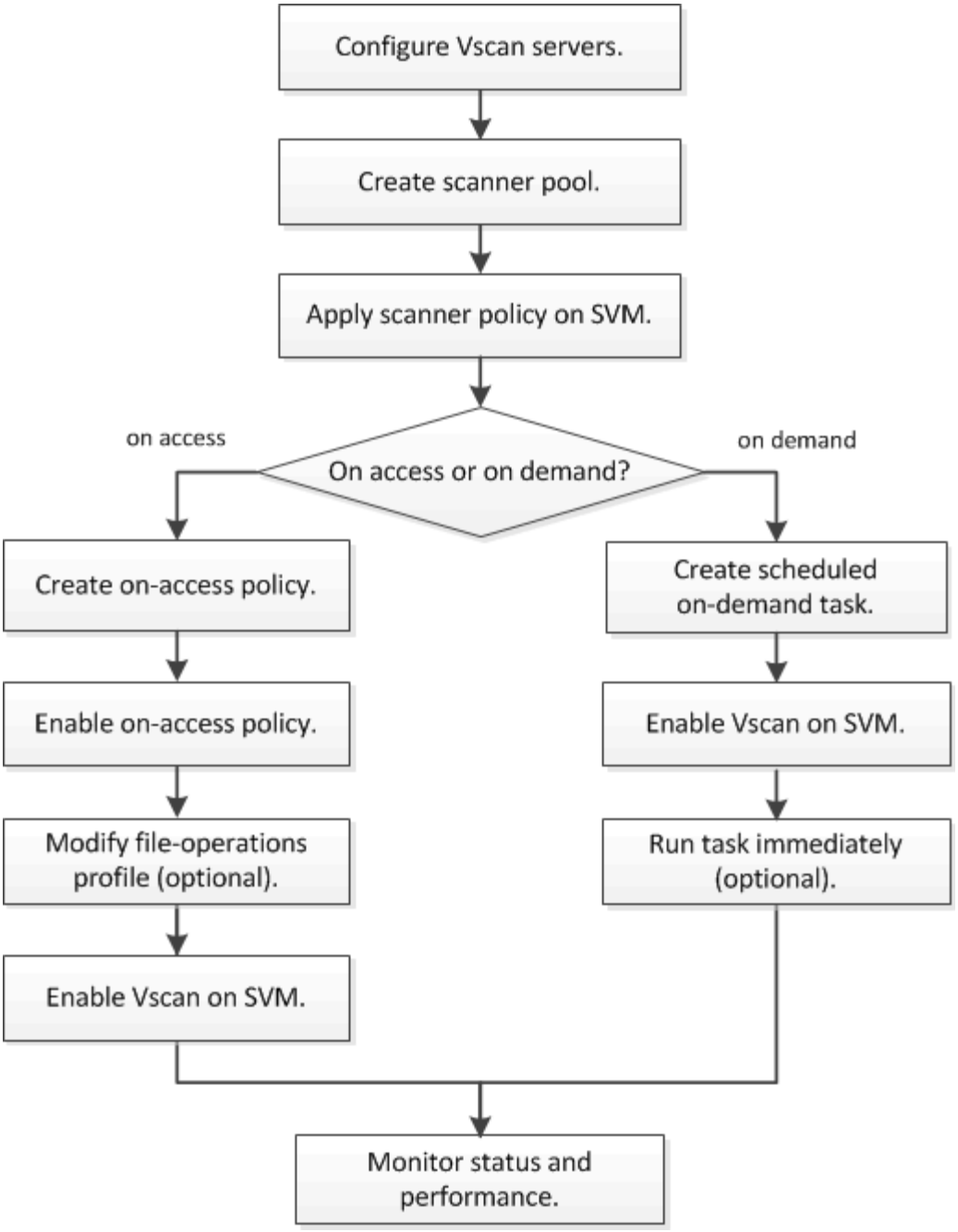
由NetApp提供並安裝在外部伺服器上的《The停止防毒連接器：處理儲存系統與防毒軟體之間的通訊。ONTAP



使用 **ONTAP Vscan** 進行病毒掃描工作流程

您必須先建立掃描器資源池並套用掃描器原則、才能啟用掃描。您通常可以在 SVM 上同時啟用存取和隨選掃描模式。

您必須已完成CIFS組態。



若要建立隨選工作、必須至少啟用一個存取原則。它可以是預設原則、也可以是使用者建立的存取原則。

後續步驟

- 在單一叢集上建立掃描器集區
- 在單一叢集上套用掃描器原則
- 建立存取時原則

採用 **ONTAP Vscan** 的防毒架構

NetApp 防毒架構包含 VScan 伺服器軟體和相關設定。

VScan 伺服器軟體

您必須在 VScan 伺服器上安裝此軟體。

- 《防毒連接器》 ONTAP

  這是 NetApp 提供的軟體、可處理 SVM 與防毒軟體之間的掃描要求與回應通訊。它可以在虛擬機器上執行、但為了達到最佳效能、請使用實體機器。您可以從 NetApp 支援網站 下載此軟體（需要登入）。

- 防毒軟體

  這是合作夥伴提供的軟體、可掃描檔案中是否有病毒或其他惡意程式碼。您可以指定在設定軟體時、對受感染檔案採取的補救行動。

VScan 軟體設定

您必須在 VScan 伺服器上設定這些軟體設定。

- 掃描器資源池

  此設定定義可連線至 SVM 的 VScan 伺服器和授權使用者。它也定義掃描要求逾時期間、之後若有可用的VScan伺服器、掃描要求會傳送至替代的VScan伺服器。

  > ⓘ 您應該將 VScan 伺服器上防毒軟體的逾時時間設定為比掃描器集區掃描要求逾時時間少五秒。這可避免因為軟體的逾時時間超過掃描要求的逾時時間、導致檔案存取延遲或完全遭拒的情況。

- 貴賓使用者

  此設定是 VScan 伺服器用來連線至 SVM 的網域使用者帳戶。帳戶必須存在於掃描器集區中的授權使用者清單中。

- 掃描程式原則

  此設定決定掃描器集區是否為作用中。掃描器原則是系統定義的、因此您無法建立自訂的掃描器原則。只有這三個原則可供使用：

  - `Primary` 指定掃描儀池處於活動狀態。
  - `Secondary` 指定掃瞄器集區為作用中、只有在沒有連接主要掃瞄器集區中的 VScan 伺服器時。
  - `Idle` 指定掃描器集區為非作用中。

- 存取原則

  此設定定義存取掃描的範圍。您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。

  依預設、只會掃描讀寫磁碟區。您可以指定篩選條件、以允許掃描唯讀磁碟區、或限制掃描以執行存取開啟的檔案：

  - `scan-ro-volume` 可掃描唯讀磁碟區。
  - `scan-execute-access` 限制掃描至以執行存取權限開啟的檔案。

「執行存取」與「執行權限」不同。 只有在以「執行目的」開啟檔案時、指定的用戶端才能在執行檔上擁有「執行存取」。

您可以設定 `scan-mandatory` 選項為「關閉」、可指定在沒有 VScan 伺服器可供病毒掃描時、允許檔案存取。在存取模式中、您可以從這兩個互斥的選項中選擇：

- 必要：使用此選項、 VScan 會嘗試將掃描要求傳送至伺服器、直到逾時期間過期為止。如果伺服器不接受掃描要求、則用戶端存取要求會遭到拒絕。
- 非必要：無論 VScan 伺服器是否可用於掃毒、 VScan 都一律允許用戶端存取。

- 隨需工作

此設定定義隨選掃描的範圍。您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。依預設會掃描子目錄中的檔案。

您可以使用cron排程來指定工作執行的時間。您可以使用 `vserver vscan on-demand-task run`命令立即執行工作。如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task run`資訊，請參閱。

- * VScan檔案作業設定檔（僅限存取掃描）*

。 `vscan-fileop-profile` 的參數 `vserver cifs share create` 命令定義哪些 SMB 檔案作業會觸發病毒掃描。依預設、參數會設為 `standard`，這是 NetApp 最佳實務做法。您可以在建立或修改 SMB 共用時視需要調整此參數：

- `no-scan` 指定從不觸發共享區的病毒掃描。
- `standard` 指定透過開啟、關閉及重新命名作業觸發病毒掃描。
- `strict` 指定透過開啟、讀取、關閉及重新命名作業來觸發病毒掃描。

  。 `strict` 設定檔可針對多個用戶端同時存取檔案的情況、提供增強的安全性。如果某個用戶端在寫入病毒後關閉檔案、而同一個檔案仍會在第二個用戶端上開啟、 `strict` 確保第二個用戶端上的讀取作業會在檔案關閉之前觸發掃描。

  您應該小心將 `strict`設定檔限制為包含預期將同時存取的檔案的共用。由於此設定檔會產生更多掃描要求、因此可能會影響效能。

- `writes-only` 指定只有在關閉修改過的檔案時才觸發病毒掃描。

  自 `writes-only` 產生較少的掃描要求、通常會改善效能。

如果您使用此設定檔、掃描器必須設定為刪除或隔離無法修復的受感染檔案、因此無法存取這些檔案。例如、如果用戶端在寫入病毒後關閉檔案、而且檔案未被修復、刪除或隔離、則任何用戶端都會存取該檔案 `without` 寫信給 IT 的人會受到感染。

如果用戶端應用程式執行重新命名作業、檔案會以新名稱關閉、不會掃描。如果此類作業在您的環境中造成安全性考量、您應該使用 `standard` 或 `strict` 設定檔。

如"指令參考資料ONTAP"需詳細 `vserver cifs share create`資訊，請參閱。

NetApp 與 Trelix ， Symantec ， Trend Micro ， Sentinel One ， Deep Instinct 及 OPSWAT 合作，提供以 ONTAP VScan 技術為基礎的領先業界的惡意軟體防護與防毒解決方案。這些解決方案可協助您掃描檔案中的惡意軟體、並修正任何受影響的檔案。

如下表所示， Trellix ， Symantec 和 Trend Micro 的互通性詳細資料會保留在 NetApp 互通性對照表上。您也可以在合作夥伴網站上找到 Trelix ， Symantec ， Deep Instinct 和 OPSWAT 的互通性詳細資料。合作夥伴將在其網站上維護 Sentinel One ， Deep Instinct ， OPSWAT 及其他新合作夥伴的互通性詳細資料。

合作夥伴	解決方案文件	互通性詳細資料
Trelix （原 McAfee ）	"Trellix 產品文件"	• "NetApp 互通性對照表工具" • "端點安全儲存保護支援平台（ trellix.com ）"
Symantec	"Symantec Protection Engine 9.0.0"	• "NetApp 互通性對照表工具" • "支援對照表：通過 Symantec Protection Engine （ SPE ）認證的合作夥伴裝置、適用於網路附加儲存（ NAS ） 9.x.x"
Trend Micro	"Trend Micro ServerProtect for Storage 6.0 入門指南"	"NetApp 互通性對照表工具"
Sentinel One	• "SentinelOne 奇異性雲端資料安全性" • "SentinelOne 支援" 此連結需要使用者登入。您可以從 Sentinel One 要求存取。	不適用
深直覺	適用於 NAS 的深度直覺 DSX • "文件與互通性" 此連結需要使用者登入。您可以從深切本能要求存取。 • "資料表"	不適用
OPSWAT	OPSWAT MetaDefender 儲存安全性 • "MetaDefender 儲存安全性與 NetApp 整合" • "OPSWAT 合作夥伴頁面" • "整合解決方案簡介"	不適用

VScan伺服器安裝與組態

ONTAP Vscan 伺服器安裝與設定

設定一或多個 VScan 伺服器、以確保系統上的檔案已掃描到病毒。請依照廠商提供的指示、在伺服器上安裝及設定防毒軟體。

請依照 NetApp 提供的 README 檔案中的指示來安裝及設定 ONTAP 防毒連接器。或者、請遵循上的指示 "安裝 ONTAP 防毒連接器頁面"。

> 對於災難恢復和 MetroCluster 組態、您必須為主要 / 本機和次要 / 合作夥伴 ONTAP 叢集分別設定和設定 VScan 伺服器。

防毒軟體需求

- 如需防毒軟體需求的相關資訊、請參閱廠商文件。
- 如需 VScan 支援的廠商、軟體和版本資訊、請參閱"VScan 合作夥伴解決方案"頁面。

防毒連接器需求ONTAP

- 您可以從 NetApp 支援網站 的 * 軟體下載 * 頁面下載 ONTAP 防毒連接器。 "NetApp下載：軟體"
- 如需 ONTAP 防毒連接器支援的 Windows 版本和互通性需求的相關資訊，請參閱"VScan 合作夥伴解決方案"。

> 您可以為叢集中的不同VScan伺服器安裝不同版本的Windows伺服器。

- Windows伺服器上必須安裝.NET 3.0或更新版本。
- 必須在Windows伺服器上啟用SMB 2.0。

安裝 ONTAP Vscan 防毒連接器

在 VScan 伺服器上安裝 ONTAP 防毒連接器、以啟用執行 ONTAP 的系統與 VScan 伺服器之間的通訊。安裝 ONTAP 防毒連接器後、防毒軟體就能與一或多個儲存虛擬機器（ SVM ）通訊。

關於這項工作

- 如"VScan 合作夥伴解決方案"需支援的通訊協定、防毒廠商軟體版本、 ONTAP 版本、互通性需求和 Windows 伺服器的相關資訊、請參閱頁面。
- 必須安裝 .NET 4.5.1 或更新版本。
- ONTAP 防毒連接器可以在虛擬機器上執行。不過、為了獲得最佳效能、 NetApp 建議使用專用實體機器進行防毒掃描。
- 您必須在安裝及執行 ONTAP 防毒連接器的 Windows 伺服器上啟用 SMB 2.0 。

開始之前

- 從支援網站下載 ONTAP 防毒連接器設定檔、並將其儲存至硬碟上的目錄。
- 確認您符合安裝 ONTAP 防毒連接器的要求。

- 請確認您擁有安裝防毒 Connector 的系統管理員權限。

步驟

1. 執行適當的安裝檔案來啟動防毒連接器安裝精靈。
2. 選取 *Next* 。「目的地資料夾」對話方塊隨即開啟。
3. 選取 *Next* 將防毒 Connector 安裝到列出的資料夾、或選取 *Changle* 安裝到不同的資料夾。
4. ONTAP AV Connector Windows 服務認證對話方塊隨即開啟。
5. 輸入您的 Windows 服務認證、或選取 * 新增 * 以選取使用者。對於 ONTAP 系統、此使用者必須是有效的網域使用者、而且必須存在於 SVM 的掃描器集區組態中。
6. 選擇*下一步*。「準備安裝程式」對話方塊隨即開啟。
7. 選擇 * 安裝 * 開始安裝、或選擇 * 上一步 * 來變更設定。
狀態方塊隨即開啟並記錄安裝進度、接著顯示「 Installshield Wizard Completed 」（安裝精靈已完成）對話方塊。
8. 如果您要繼續設定 ONTAP 管理或資料生命、請選取「設定 ONTAP 生命期」核取方塊。
您必須至少設定一個 ONTAP 管理或資料 LIF 、才能使用此 VScan 伺服器。
9. 如果您要檢視安裝記錄、請選取顯示 * Windows Installer 記錄 * 核取方塊。
10. 選擇 * 完成 * 結束安裝並關閉 Installshield 精靈。
桌面上會儲存 **Configure ONTAP Lifs** 圖示、以設定 ONTAP 生命。
11. 將 SVM 新增至防毒 Connector 。
您可以新增 ONTAP 管理 LIF 來將 SVM 新增至防毒連接器、此 LIF 會輪詢以擷取資料生命清單、或直接設定資料 LIF 或生命。
如果已設定 ONTAP 管理 LIF 、您也必須提供意見調查資訊和 ONTAP 管理帳戶認證。
    - 確認已啟用 SVM 的管理 LIF 或 IP 位址 `management-https`。當您只是設定資料生命時、這不是必要的。
    - 確認您已為 HTTP 應用程式建立使用者帳戶，並指派（至少為唯讀）存取 REST API 的角色 `/api/network/ip/interfaces`。
    - 深入瞭解 `security login role create`及 `security login create` "指令參考資料ONTAP"。

> 您也可以新增管理 SVM 的驗證通道 SVM 、將網域使用者當成帳戶使用。如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。
2. 在「設定 ONTAP 生命」對話方塊中、選取偏好的組態類型、然後執行下列動作：

若要建立此類型的 LIF…	執行下列步驟…

資料LIF	a. 將「角色」設為「資料」 b. 將「資料傳輸協定」設定為「 CIFS 」 c. 將「防火牆原則」設定為「資料」 d. 將「服務原則」設定為「 default-data-files 」
管理層 LIF	a. 將「 role * 」設為「 data 」 b. 將「資料傳輸協定」設為「無」 c. 將「防火牆原則」設定為「管理」 d. 將「服務原則」設定為「預設管理」

瞭解更多關於"建立 LIF"的資訊。

建立 LIF 之後、請輸入您要新增之 SVM 的資料或管理 LIF 或 IP 位址。您也可以輸入叢集管理 LIF 。如果您指定叢集管理 LIF 、則該叢集中所有服務 SMB 的 SVM 都可以使用 VScan 伺服器。

當 VScan 伺服器需要 Kerberos 驗證時、每個 SVM 資料 LIF 都必須有唯一的 DNS 名稱、而且您必須在 Windows Active Directory 中將該名稱登錄為伺服器主要名稱（ SPN ）。當每個資料 LIF 無法使用唯一的 DNS 名稱或登錄為 SPN 時、 VScan 伺服器會使用 NT LAN Manager 機制進行驗證。如果您在連線 VScan 伺服器後新增或修改 DNS 名稱和 SPN 、則必須重新啟動 VScan 伺服器上的防毒連接器服務、才能套用變更。

3. 若要設定管理 LIF 、請以秒為單位輸入輪詢持續時間。輪詢持續時間是防毒 Connector 檢查 SVM 或叢集 LIF 組態變更的頻率。預設的輪詢時間間隔為 60 秒。
4. 輸入 ONTAP 管理帳戶名稱和密碼以設定管理 LIF 。
5. 按一下 * 測試 * 以檢查連線能力並驗證驗證。驗證僅適用於管理 LIF 組態。
6. 按一下 * 更新 * 將 LIF 新增至要輪詢或連線的生命清單。
7. 按一下 * 儲存 * 以儲存登錄的連線。
8. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

請參閱 "設定 ONTAP 防毒連接器頁面" 以取得組態選項。

設定 **ONTAP Vscan** 防毒連接器

設定 ONTAP 防毒連接器、輸入 ONTAP 管理 LIF 、輪詢資訊、 ONTAP 管理帳戶認證、或只輸入資料 LIF 、以指定您要連線的一或多個儲存虛擬機器（ SVM ）。您也可以修改 SVM 連線的詳細資料、或移除 SVM 連線。根據預設、如果已設定 ONTAP 管理 LIF 、 ONTAP 防毒連接器會使用 REST API 來擷取資料生命體清單。

修改 **SVM** 連線的詳細資料

您可以修改 ONTAP 管理 LIF 和輪詢資訊、以更新已新增至防毒 Connector 的儲存虛擬機器（ SVM ）連線的詳細資料。新增資料生命後、您無法更新這些資料生命。若要更新資料生命期、您必須先移除資料生命期、然後再以新的 LIF 或 IP 位址重新新增資料生命期。

開始之前

確認您已為 HTTP 應用程式建立使用者帳戶，並指派（至少為唯讀）存取 REST API 的角色 `/api/network/ip/interfaces`。

深入瞭解 `security login role create`及 `security login create` "指令參考資料ONTAP"。

您也可以新增管理 SVM 的驗證通道 SVM 、將網域使用者當成帳戶使用。如"指令參考資料ONTAP"需詳細 `security login domain-tunnel create`資訊，請參閱。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。此時將打開 Configure Lifs （配置 ONTAP 生命）對話框。
2. 選取 SVM IP 位址、然後按一下 * 更新 * 。
3. 視需要更新資訊。
4. 按一下 * 儲存 * 以更新登錄中的連線詳細資料。
5. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。
   如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

從防毒 **Connector** 移除 **SVM** 連線

如果不再需要 SVM 連線、您可以將其移除。

步驟

1. 在 * 設定 ONTAP Lifs* 圖示上按一下滑鼠右鍵、此圖示會在您完成防毒連接器安裝時儲存在桌面上、然後選取 * 以系統管理員身分執行 * 。此時將打開 Configure Lifs （配置 ONTAP 生命）對話框。
2. 選取一或多個 SVM IP 位址、然後按一下 * 移除 * 。
3. 按一下 * 儲存 * 以更新登錄中的連線詳細資料。
4. 如果您要將連線清單匯出至登錄匯入或登錄匯出檔案、請按一下 * 匯出 * 。
   如果多部 VScan 伺服器使用相同的管理或資料生命負載、這項功能就很實用。

疑難排解

開始之前

當您在此程序中建立登錄值時、請使用右側窗格。

您可以啟用或停用防毒連接器記錄以供診斷之用。根據預設、這些記錄會停用。為了提升效能、您應該停用防毒 Connector 記錄檔、並僅在發生重大事件時啟用記錄檔。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、找到 ONTAP 防毒連接器的下列子機碼：
   `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 提供下表所示的類型、名稱和值來建立登錄值：

類型	名稱	價值

字串	追蹤路徑	C ： \avshim.log

此登錄值可以是任何其他有效路徑。

4. 提供下表所示的類型、名稱、值及記錄資訊、以建立另一個登錄值：

類型	名稱	關鍵記錄	中繼記錄	詳細記錄
雙字節	Tracelight	1.	2 或 3	4.

這會啟用儲存在步驟 3 追蹤路徑中所提供路徑值的防毒 Connector 記錄檔。

5. 刪除您在步驟 3 和 4 中建立的登錄值、以停用防毒 Connector 記錄。
6. 使用「 LogRotation 」（記錄旋轉）名稱（不含引號）、建立另一個「 multy_SZ 」類型的登錄值。在「 LogRotation 」中、
提供 "logFileSize:1 " 做為旋轉大小的項目（其中 1 代表 1MB ）、在下一行提供 "logFileCount:5" 做為進入旋轉限制（上限為 5 ）。

這些值是選用的。如果未提供、預設值 20MB 和 10 個檔案會分別用於旋轉大小和旋轉限制。提供的整數值不提供十進位或分數值。如果您提供的值高於預設值、則會改用預設值。

7. 若要停用使用者設定的記錄輪替功能、請刪除您在步驟 6 中建立的登錄值。

可自訂橫幅

自訂橫幅可讓您在 *Configure ONTAP LIF API* 視窗中放置具法律約束力的聲明和系統存取免責聲明。

步驟

1. 透過更新中的內容來修改預設橫幅 `banner.txt` 將檔案儲存在安裝目錄中、然後儲存變更。
您必須重新開啟 Configure LIF API （設定 ONTAP LIF API ）視窗、才能查看橫幅中反映的變更。

啟用延伸條例（ **EO** ）模式

您可以啟用和停用「延伸條例」（ EOO ）模式、以確保操作安全。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、找到下列 ONTAP 防毒連接器子機碼：
`HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0`
3. 在右側窗格中、建立名稱為「 EO_Mode 」（不含引號）且值為「 1 」（不含引號）的新登錄值（不含引號）、以啟用「 EO Mode 」（ EO 模式）或值「 0 」（不含引號）來停用「 EO Mode 」（ EO 模式）。

依預設、如果是 `EO_Mode` 登錄項目不存在、會停用 EO 模式。啟用「 EOO 」模式時、您必須同時設定外部 Syslog 伺服器和相互憑證驗證。

開始之前

請注意、在本程序中建立登錄值時、請使用右側窗格。

步驟

1. 選取 * 開始 * 、在搜尋方塊中輸入「 regedit" 、然後選取 `regedit.exe` 在「程式集」清單中。
2. 在 * 登錄編輯程式 * 中、針對 ONTAP 防毒連接器的系統記錄組態建立下列子機碼： `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Data ONTAP\Clustered Data ONTAP Antivirus Connector\v1.0\syslog`
3. 請提供下表所示的類型、名稱和值來建立登錄值：

類型	名稱	價值
雙字節	啟用 SysLog	1 或 0

請注意，「 1 」值會啟用 Syslog ，而「 0 」值則會停用。

4. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_host

提供系統記錄主機 IP 位址或網域名稱作為值欄位。

5. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_port

在值欄位中提供 Syslog 伺服器執行的連接埠編號。

6. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱
Reg_SZ	syslog_protocol

在值欄位中輸入 Syslog 伺服器上使用的傳輸協定（「 TCP 」或「 UDP 」）。

7. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱	log_crt	log_notice	log_info	log_debug
雙字節	syslog_level	2.	5.	6.	7.

8. 提供下表所示的資訊、建立另一個登錄值：

類型	名稱	價值
雙字節	syslog_tls	1 或 0

請注意，「 1 」值會啟用含傳輸層安全性（ TLS ）的 Syslog ，而「 0 」值則會停用含 TLS 的 Syslog 。

確保已設定的外部 **Syslog** 伺服器能順暢運作

- 如果金鑰不存在或具有 null 值：
  - 傳輸協定預設為「 TCP 」。
  - 對於純「 TCP/UDP 」、連接埠預設為「 514 」、而 TLS 預設為「 6514 」。
  - 系統記錄層級預設為 5 （ log_notice ）。
- 您可以驗證是否已啟用 Syslog `syslog_enabled` 值為「 1 」。當 `syslog_enabled` 值為「 1 」、無論是否啟用「 EO 」模式、您都應該能夠登入設定的遠端伺服器。
- 如果將 EO 模式設定為「 1 」、則您可以變更 `syslog_enabled` 值從「 1 」到「 0 」、適用下列條件：
  - 如果系統記錄未在 EO 模式中啟用、則無法啟動服務。
  - 如果系統以穩定狀態執行、系統會顯示一則警告訊息、表示無法在 EO 模式中停用 Syslog 、且系統記錄會強制設定為「 1 」、您可以在登錄中看到。如果發生這種情況、您應該先停用 EO 模式、然後停用 Syslog 。
- 如果在啟用 EO 模式和 Syslog 時、系統記錄伺服器無法成功執行、則服務會停止執行。這可能是因為下列其中一項原因所致：
  - 未設定無效或不設定任何 syslog_host 。
  - 設定的傳輸協定無效、除了 UDP 或 TCP 之外。
  - 連接埠號碼無效。
- 對於 TCP 或 TLS over TCP 組態、如果伺服器未接聽 IP 連接埠、則連線會失敗、且服務會關閉。

設定 **X.509** 相互憑證驗證

管理路徑中的防毒連接器和 ONTAP 之間的安全通訊端層 (SSL) 通訊可以使用基於 X.509 憑證的相互驗證。如果啟用了 EO 模式、但找不到憑證、 AV Connector 就會終止。在防毒連接器上執行下列程序：

步驟

1. 防毒連接器會在防毒連接器執行安裝目錄的目錄路徑中搜尋防毒連接器用戶端憑證和 NetApp 伺服器的憑證授權單位（ CA ）憑證。將憑證複製到此固定目錄路徑。
2. 以 PKCS12 格式內嵌用戶端憑證及其私密金鑰、並將其命名為「 AV_CLIent.p12 」。
3. 確保用於簽署NetApp伺服器憑證的 CA 憑證（以及直至根 CA 的任何中間簽章機構）採用 Privacy Enhanced Mail (PEM) 格式，並命名為「Ontap_CA.pem」。將其放置在防毒軟體連接器的安裝目錄中。在ONTAP系統上，將用於在「ONTAP」上為防毒連接器簽署用戶端憑證的 CA 憑證（以及任何中間簽章機構，直到根 CA）安裝為「client-ca」類型的憑證。

設定掃描器資源池

了解如何設定 ONTAP Vscan 掃描器池

掃描器集區會定義VScan伺服器和可連線至SVM的授權使用者。掃描器原則會決定掃描器集區是否處於作用中狀態。

如果您在 SMB 伺服器上使用匯出原則、則必須將每個 VScan 伺服器新增至匯出原則。

在單一叢集上建立 ONTAP Vscan 掃描器池

掃描器集區會定義VScan伺服器和可連線至SVM的授權使用者。

開始之前

- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 使用叢集管理 LIF 設定 ONTAP 防毒連接器。
- 授權使用者清單必須包含 VScan 伺服器用來連線至 SVM 的網域和使用者名稱。
- 設定掃描器集區後、請檢查伺服器的連線狀態。

步驟

1. 建立掃描器集區：

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 指定叢集管理 SVM 。
   - 為每個VScan伺服器主機名稱指定IP位址或FQDN。
   - 指定每個授權使用者的網域和使用者名稱。

   如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool create`資訊，請參閱。

2. 確認已建立掃描器集區：

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   下列命令會顯示的詳細資料 `SP` 掃描器集區：

```
cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
-scanner-pool SP

                                    Vserver: cluster_admin_SVM
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: cluster
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

您也可以使用 `vserver vscan scanner-pool show`命令來檢視叢集上的所有掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

在 **MetroCluster** 配置中建立 **ONTAP Vscan** 掃描器池

您必須在MetroCluster 每個叢集上建立一個適用於整個叢集的主和次掃描儀資源池、以對應於叢集上的主要和次要SVM。

開始之前

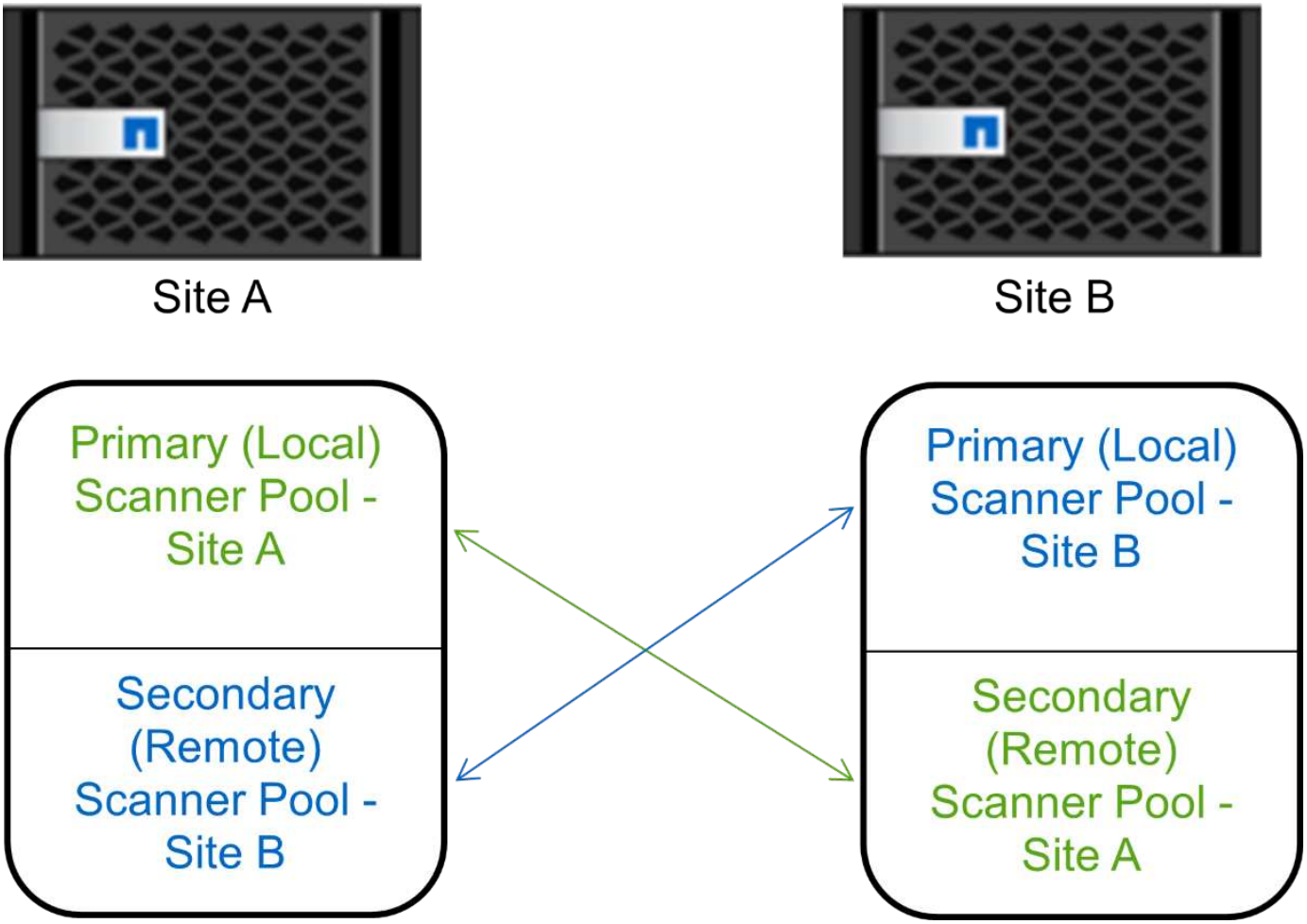
- SVM和VScan伺服器必須位於同一個網域或信任的網域中。
- 針對為個別 SVM 定義的掃描器集區、您必須使用 SVM 管理 LIF 或 SVM 資料 LIF 來設定 ONTAP 防毒連接器。
- 針對叢集中所有 SVM 定義的掃描器集區、您必須使用叢集管理 LIF 來設定 ONTAP 防毒連接器。
- 授權使用者清單必須包含VScan伺服器用來連線至SVM的網域使用者帳戶。
- 設定掃描器集區後、請檢查伺服器的連線狀態。

關於這項工作

透過實作兩個實體獨立的鏡射叢集、可利用各種組態來保護資料。MetroCluster每個叢集都會同步複寫另一個叢集的資料和SVM組態。當叢集上線時、本機叢集上的主要SVM會提供資料。當遠端叢集離線時、本機叢集上的次要SVM會提供資料。

這表示您必須在 MetroCluster 組態中的每個叢集上建立主要和次要掃描器集區、當叢集開始從次要 SVM 服務資料時、次要集區就會變成作用中。災難恢復（ DR ）的組態與 MetroCluster 類似。

此圖顯示典型的 MetroCluster / DR 組態。



步驟

1. 建立掃描器集區：

   ```
   vserver vscan scanner-pool create -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - 為個別SVM定義的資源池指定資料SVM、並為叢集中所有SVM定義的資源池指定叢集管理SVM。
   - 為每個VScan伺服器主機名稱指定IP位址或FQDN。
   - 指定每個授權使用者的網域和使用者名稱。

   > 您必須從包含主要SVM的叢集建立所有掃描器集區。

   如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool create`資訊，請參閱。

   下列命令會在MetroCluster 每個叢集上建立一個以功能為基礎的基本和次要掃描器集區：

```
cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site1 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_site2 -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site1 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

cluster1::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_site2 -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. 確認已建立掃描器集區：

   `vserver vscan scanner-pool show -vserver` *`data_SVM|cluster_admin_SVM`* `-scanner -pool` *`scanner_pool`*

   下列命令會顯示掃描器集區的詳細資料 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                              Scanner Pool: pool1_for_site1
                            Applied Policy: idle
                            Current Status: off
        Cluster on Which Policy Is Applied: -
                  Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                   List of Privileged Users: cifs\u1,cifs\u2
```

   您也可以使用 `vserver vscan scanner-pool show`命令來檢視 SVM 上的所有掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

使用 **ONTAP Vscan** 在單一叢集上套用掃描器策略

掃描器原則會決定掃描器集區是否處於作用中狀態。您必須先啟動掃瞄器集區、其定義的 VScan 伺服器才能連線至 SVM 。

關於這項工作

- 您只能將一個掃描器原則套用至掃描器集區。
- 如果您為叢集中的所有 SVM 建立了掃瞄器集區、則必須個別在每個 SVM 上套用掃瞄器原則。

步驟

1. 套用掃描器原則：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   掃描器原則可以具有下列其中一個值：

   - `Primary` 指定掃描儀池處於活動狀態。
   - `Secondary` 指定只有在沒有連接主要掃描器集區中的 VScan 伺服器時、掃描器集區才為作用中。
   - `Idle` 指定掃描器集區為非作用中。

   以下範例顯示掃描器集區的名稱 `SP` 在上 `vs1` SVM 處於作用中狀態：

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. 確認掃描器集區處於作用中狀態：

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

   下列命令會顯示的詳細資料 `SP` 掃描器集區：

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
           Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
         List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
   27.fsct.nb
                     List of Privileged Users: cifs\u1, cifs\u2
   ```

   您可以使用 `vserver vscan scanner-pool show-active`命令來檢視 SVM 上的作用中掃描器集區。如"指令參

考資料ONTAP"需詳細 `vserver vscan scanner-pool show-active`資訊，請參閱。

在 **MetroCluster ONTAP Vscan** 設定中套用掃描器策略

掃描器原則會決定掃描器集區是否處於作用中狀態。您必須將掃描儀原則套用至MetroCluster 每個叢集上的主掃描儀資源池和次掃描儀資源池、以供選擇。

關於這項工作

- 您只能將一個掃描器原則套用至掃描器集區。
- 如果您為叢集中的所有 SVM 建立了掃瞄器集區、則必須個別在每個 SVM 上套用掃瞄器原則。
- 對於災難恢復和 MetroCluster 組態、您必須將掃描器原則套用至本機叢集和遠端叢集中的每個掃描器集區。
- 在您為本機叢集建立的原則中、您必須在中指定本機叢集 `cluster` 參數。在您為遠端叢集建立的原則中、您必須在中指定遠端叢集 `cluster` 參數。接著、遠端叢集便可在發生災難時接管病毒掃描作業。

步驟

1. 套用掃描器原則：

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool apply-policy`資訊，請參閱。

   掃描器原則可以具有下列其中一個值：

   - `Primary` 指定掃描儀池處於活動狀態。
   - `Secondary` 指定只有在沒有連接主要掃描器集區中的 VScan 伺服器時、掃描器集區才為作用中。
   - `Idle` 指定掃描器集區為非作用中。

     您必須套用包含主要SVM之叢集的所有掃描器原則。

   下列命令會將掃描儀原則套用至MetroCluster 每個叢集上的主掃描儀集區和次掃描儀集區、以供選擇：

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. 確認掃描器集區處於作用中狀態：

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show`資訊，請參閱。

   下列命令會顯示掃描器集區的詳細資料 `pool1`：

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                     List of Privileged Users: cifs\u1,cifs\u2
```

   您可以使用 `vserver vscan scanner-pool show-active`命令來檢視 SVM 上的作用中掃描器集區。如"指令參考資料ONTAP"需詳細 `vserver vscan scanner-pool show-active`資訊，請參閱。

用於管理 **Vscan** 中的掃描器池的 **ONTAP** 指令

您可以修改及刪除掃描器資源池、以及管理掃描器資源池的授權使用者和VScan伺服器。您也可以檢視掃描器集區的摘要資訊。

如果您想要...	輸入下列命令...
修改掃描器資源池	`vserver vscan scanner-pool modify`
刪除掃描器資源池	`vserver vscan scanner-pool delete`
新增授權使用者至掃描器集區	`vserver vscan scanner-pool privileged-users add`
從掃描器集區刪除具有權限的使用者	`vserver vscan scanner-pool privileged-users remove`
將VScan伺服器新增至掃描器集區	`vserver vscan scanner-pool servers add`
從掃描器集區刪除VScan伺服器	`vserver vscan scanner-pool servers remove`
檢視掃描器集區的摘要與詳細資料	`vserver vscan scanner-pool show`
檢視掃描器集區的授權使用者	`vserver vscan scanner-pool privileged-users show`
檢視所有掃描器集區的VScan伺服器	`vserver vscan scanner-pool servers show`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定存取時掃描

建立 **ONTAP Vscan** 依存取策略

存取時原則定義存取時掃描的範圍。您可以為個別SVM或叢集中的所有SVM建立存取原則。如果您為叢集中的所有SVM建立了存取原則、則必須個別在每個SVM上啟用原則。

關於這項工作

- 您可以指定要掃描的檔案大小上限、掃描中要包含的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。
- 您可以設定 `scan-mandatory` 選項為「關閉」、可指定在沒有 VScan 伺服器可供病毒掃描時、允許檔案存取。
- 根據預設、 ONTAP 會建立名為「 Default_CIFS 」的存取上原則、並為叢集中的所有 SVM 啟用該原則。
- 符合掃描排除條件的任何檔案、根據 `paths-to-exclude`、 `file-ext-to-exclude`或 `max-file-size` 即使是、也不會考慮掃描參數 `scan-mandatory` 選項設為「開啟」。（請勾選此項 "疑難排解" 有關連線問題的章節 `scan-mandatory` 選項。）
- 依預設、只會掃描讀寫磁碟區。您可以指定篩選條件、以允許掃描唯讀磁碟區、或限制掃描以執行存取開啟的檔案。

- 不會在 SMB 共用上執行病毒掃描、而持續可用的參數會設為是。
- 請參閱 "防毒架構" 節以取得關於 _VScan 檔案作業設定檔的詳細資料。
- 每個 SVM 最多可建立十（ 10 ）個存取原則。不過、您一次只能啟用一個存取原則。
  - 在存取原則中、您最多可以排除一百（ 100 ）個路徑和檔案副檔名、使其無法進行病毒掃描。
- 一些檔案排除建議：
  - 請考慮將大型檔案（可以指定檔案大小）排除在病毒掃描之外、因為這些檔案可能會導致 CIFS 使用者回應緩慢或掃描要求逾時。排除的預設檔案大小為 2GB 。
  - 請考慮排除檔案副檔名、例如 `.vhd` 和 `.tmp` 因為具有這些副檔名的檔案可能不適合掃描。
  - 請考慮排除檔案路徑、例如僅儲存虛擬硬碟或資料庫的隔離目錄或路徑。
  - 請確認所有排除項目都是在同一個原則中指定、因為一次只能啟用一個原則。NetApp 強烈建議您在防毒引擎中指定相同的排除項目集。
  - 從 ONTAP 9.14.1 開始、您可以使用萬用字元來指定要排除的存取路徑。
- 必須有存取上的原則才能使用 隨需掃描。為了避免進行存取掃描、您應該設定 `-scan-files-with-no-ext` 為假、且 `-file-ext-to-exclude` 至 * 以排除所有副檔名。

步驟

1. 建立存取時原則：

   ```
   vserver vscan on-access-policy create -vserver data_SVM|cluster_admin_SVM
   -policy-name policy_name -protocol CIFS -max-file-size
   max_size_of_files_to_scan -filters [scan-ro-volume,][scan-execute-access]
   -file-ext-to-include extensions_of_files_to_include -file-ext-to-exclude
   extensions_of_files_to_exclude -scan-files-with-no-ext true|false -paths-to
   -exclude paths_of_files_to_exclude -scan-mandatory on|off
   ```

   - 為個別SVM定義的原則指定資料SVM、為叢集中所有SVM定義的原則指定叢集管理SVM。
   - 。 `-file-ext-to-exclude` 設定會覆寫 `-file-ext-to-include` 設定：
   - 設定 `-scan-files-with-no-ext` 至 true 可掃描不含副檔名的檔案。
     下列命令會建立名為的存取上原則 `Policy1` 在上 `vs1` SVM ：

   ```
   cluster1::> vserver vscan on-access-policy create -vserver vs1 -policy
   -name Policy1 -protocol CIFS -filters scan-ro-volume -max-file-size 3GB
   -file-ext-to-include "mp*","tx*" -file-ext-to-exclude "mp3","txt" -scan
   -files-with-no-ext false -paths-to-exclude "\vol\a b\","\vol\a,b\"
   ```

2. 確認已建立存取原則： `vserver vscan on-access-policy show -instance data_SVM|cluster_admin_SVM -policy-name name`

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-access-policy`資訊，請參閱。

   下列命令會顯示的詳細資料 `Policy1` 原則：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: off
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

啟用 **ONTAP Vscan** 依存取策略

存取時原則定義存取時掃描的範圍。您必須在SVM上啟用存取原則、才能掃描其檔案。

如果您為叢集中的所有SVM建立了存取原則、則必須個別在每個SVM上啟用原則。您一次只能在SVM上啟用一個存取原則。

步驟

1. 啟用存取原則：

   `vserver vscan on-access-policy enable -vserver data_SVM -policy-name policy_name`

   下列命令會啟用名為的存取原則 `Policy1` 在上 `vs1` SVM ：

   ```
   cluster1::> vserver vscan on-access-policy enable -vserver vs1 -policy
   -name Policy1
   ```

2. 確認已啟用存取原則：

   `vserver vscan on-access-policy show -instance *data_SVM* -policy-name *policy_name*`

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-access-policy show`資訊，請參閱。

   下列命令會顯示的詳細資料 `Policy1` 存取原則：

```
cluster1::> vserver vscan on-access-policy show -instance vs1 -policy
-name Policy1

                            Vserver: vs1
                             Policy: Policy1
                      Policy Status: on
                Policy Config Owner: vserver
               File-Access Protocol: CIFS
                            Filters: scan-ro-volume
                     Mandatory Scan: on
Max File Size Allowed for Scanning: 3GB
             File Paths Not to Scan: \vol\a b\, \vol\a,b\
       File Extensions Not to Scan: mp3, txt
           File Extensions to Scan: mp*, tx*
      Scan Files with No Extension: false
```

修改 **SMB** 共享的 **ONTAP Vscan** 檔案操作設定文件

SMB 共用的 _VScan 檔案作業設定檔 _ 會定義可觸發掃描的共用作業。依預設、參數會設為 `standard`。您可以在建立或修改SMB共用時、視需要調整參數。

請參閱 "防毒架構" 節以取得關於 _VScan 檔案作業設定檔的詳細資料。

在具有的 SMB 共用上不會執行病毒掃描 `continuously-available` 參數設為 `Yes`。

步驟

1. 修改 SMB 共用的 VScan 檔案作業設定檔值：

   ```
   vserver cifs share modify -vserver data_SVM -share-name share -path share_path
   -vscan-fileop-profile no-scan|standard|strict|writes-only
   ```

   如"指令參考資料ONTAP"需詳細 `vserver cifs share modify`資訊，請參閱。

   下列命令會將 SMB 共用的 VScan 檔案作業設定檔變更為 `strict`：

   ```
   cluster1::> vserver cifs share modify -vserver vs1 -share-name
   SALES_SHARE -path /sales -vscan-fileop-profile strict
   ```

用於管理按存取原則的 **ONTAP Vscan** 命令

您可以修改、停用或刪除存取時原則。您可以檢視原則的摘要和詳細資料。

如果您想要…	輸入下列命令…

建立存取時原則	`vserver vscan on-access-policy create`
修改存取時原則	`vserver vscan on-access-policy modify`
啟用存取原則	`vserver vscan on-access-policy enable`
停用存取原則	`vserver vscan on-access-policy disable`
刪除存取時原則	`vserver vscan on-access-policy delete`
檢視存取原則的摘要和詳細資料	`vserver vscan on-access-policy show`
新增至要排除的路徑清單	`vserver vscan on-access-policy paths-to-exclude add`
從要排除的路徑清單中刪除	`vserver vscan on-access-policy paths-to-exclude remove`
檢視要排除的路徑清單	`vserver vscan on-access-policy paths-to-exclude show`
新增至要排除的副檔名清單	`vserver vscan on-access-policy file-ext-to-exclude add`
從要排除的副檔名清單中刪除	`vserver vscan on-access-policy file-ext-to-exclude remove`
檢視要排除的副檔名清單	`vserver vscan on-access-policy file-ext-to-exclude show`
新增至要包含的副檔名清單	`vserver vscan on-access-policy file-ext-to-include add`
從要包含的副檔名清單中刪除	`vserver vscan on-access-policy file-ext-to-include remove`
檢視要包含的副檔名清單	`vserver vscan on-access-policy file-ext-to-include show`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

設定隨需掃描

了解如何設定 **ONTAP Vscan** 按需掃描

您可以使用隨需掃描功能、立即或排程檢查檔案是否有病毒。

例如、您可能只想在非尖峰時間執行掃描、或者您可能想要掃描在存取時掃描中排除的超大型檔案。您可以使用 cron 排程來指定工作執行時間。

若要建立隨選工作、必須至少啟用一個存取原則。它可以是預設原則、也可以是使用者建立的存取原則。

關於本主題

- 您可以在建立工作時指派排程。
- 在SVM上一次只能排程一項工作。
- 隨需掃描不支援掃描符號連結或串流檔案。

隨需掃描不支援掃描符號連結或串流檔案。

若要建立隨選工作、必須至少啟用一個存取原則。它可以是預設原則、也可以是使用者建立的存取原則。

使用 **ONTAP Vscan** 建立按需任務

隨選工作會定義隨選病毒掃描的範圍。您可以指定要掃描的檔案大小上限、要包含在掃描中的檔案副檔名和路徑、以及要從掃描中排除的檔案副檔名和路徑。依預設會掃描子目錄中的檔案。

關於這項工作

- 每個 SVM 最多可有十（ 10 ）個隨選工作、但只有一個可以使用中。
- 隨選工作會建立報告、其中包含與掃描相關的統計資料資訊。您可以使用命令或下載工作在定義位置所建立的報告檔案、來存取此報告。
- 從 ONTAP 9.14.1 開始，您可以使用萬用字元來指定要排除的隨選路徑。

開始之前

- 您必須擁有 已建立存取原則。原則可以是預設原則或使用者建立的原則。如果沒有存取原則、就無法啟用掃描。

步驟

1. 建立隨需工作：

```
vserver vscan on-demand-task create -vserver data_SVM -task-name task_name
-scan-paths paths_of_files_to_scan -report-directory report_directory_path
-report-expiry-time expiration_time_for_report -schedule cron_schedule -max
-file-size max_size_of_files_to_scan -paths-to-exclude paths -file-ext-to
-exclude file_extensions -file-ext-to-include file_extensions -scan-files-with
-no-ext true|false -directory-recursion true|false
```

  - 。 `-file-ext-to-exclude` 設定會覆寫 `-file-ext-to-include` 設定：

- 設定 `-scan-files-with-no-ext` 至 true 可掃描不含副檔名的檔案。

  如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task create`資訊，請參閱。

  下列命令會建立名為的隨選工作 `Task1` 在「 VS1 ' shVM ：

```
cluster1::> vserver vscan on-demand-task create -vserver vs1 -task-name
Task1 -scan-paths "/vol1/","/vol2/cifs/" -report-directory "/report"
-schedule daily -max-file-size 5GB -paths-to-exclude "/vol1/cold-files/"
-file-ext-to-include "vmdk?","mp*" -file-ext-to-exclude "mp3","mp4"
-scan-files-with-no-ext false
[Job 126]: Vscan On-Demand job is queued. Use the "job show -id 126"
command to view the status.
```

+

> 您可以使用 `job show`命令來檢視工作的狀態。您可以使用 `job pause`和 `job resume`命令暫停和重新啟動工作，或使用 `job stop`命令結束工作。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

2. 確認已建立隨選工作：

   `vserver vscan on-demand-task show -instance data_SVM -task-name task_name`

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task show`資訊，請參閱。

   下列命令會顯示的詳細資料 `Task1` 工作：

```
cluster1::> vserver vscan on-demand-task show -instance vs1 -task-name
Task1

                            Vserver: vs1
                          Task Name: Task1
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
       File Extensions Not to Scan: mp3, mp4
           File Extensions to Scan: vmdk?, mp*
      Scan Files with No Extension: false
           Request Service Timeout: 5m
                    Cross Junction: true
               Directory Recursion: true
                     Scan Priority: low
                  Report Log Level: info
        Expiration Time for Report: -
```

完成後

您必須先在SVM上啟用掃描、工作才會排程執行。

使用 **ONTAP Vscan** 安排按需任務

您可以建立工作、而無需指派排程和使用 `vserver vscan on-demand-task schedule` 命令來指派排程、或在建立工作時新增排程。

關於這項工作

指派給的排程 `vserver vscan on-demand-task schedule` 命令會覆寫已指派給的排程 `vserver vscan on-demand-task create` 命令。

步驟

1. 排程隨需工作：

   `vserver vscan on-demand-task schedule -vserver` *`data_SVM`* `-task-name` *`task_name`* `-schedule cron_schedule`

   下列命令會排程名為的存取上工作 `Task2` 在上 `vs2` SVM ：

```
cluster1::> vserver vscan on-demand-task schedule -vserver vs2 -task
-name Task2 -schedule daily
[Job 142]: Vscan On-Demand job is queued. Use the "job show -id 142"
command to view the status.
```

如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task schedule`資訊，請參閱。

若要檢視工作狀態，請使用 `job show`命令。 `job pause`和 `job resume`命令分別暫停和重新啟動工作；命令會終止工作 `job stop`。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

2. 確認隨選工作已排程：

   `vserver vscan on-demand-task show -instance` *`data_SVM`* `-task-name` *`task_name`*

   如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task show`資訊，請參閱。

   下列命令會顯示的詳細資料 `Task 2` 工作：

```
cluster1::> vserver vscan on-demand-task show -instance vs2 -task-name
Task2

                            Vserver: vs2
                          Task Name: Task2
                List of Scan Paths: /vol1/, /vol2/cifs/
              Report Directory Path: /report
                       Job Schedule: daily
Max File Size Allowed for Scanning: 5GB
             File Paths Not to Scan: /vol1/cold-files/
        File Extensions Not to Scan: mp3, mp4
            File Extensions to Scan: vmdk, mp*
      Scan Files with No Extension: false
            Request Service Timeout: 5m
                     Cross Junction: true
                Directory Recursion: true
                      Scan Priority: low
                   Report Log Level: info
```

完成後

您必須先在SVM上啟用掃描、工作才會排程執行。

立即執行 ONTAP Vscan 按需任務

無論您是否已指派排程、您都可以立即執行隨需工作。

開始之前

您必須已在SVM上啟用掃描。

步驟

1. 立即執行隨需工作：

`vserver vscan on-demand-task run -vserver data_SVM -task-name task_name`

下列命令會執行名為的存取上工作 `Task1` 在上 `vs1` SVM ：

```
cluster1::> vserver vscan on-demand-task run -vserver vs1 -task-name
Task1
[Job 161]: Vscan On-Demand job is queued. Use the "job show -id 161"
command to view the status.
```

如"指令參考資料ONTAP"需詳細 `vserver vscan on-demand-task run`資訊，請參閱。

> 您可以使用 `job show`命令來檢視工作的狀態。您可以使用 `job pause`和 `job resume`命令暫停和重新啟動工作，或使用 `job stop`命令結束工作。如"指令參考資料ONTAP"需詳細 `job`資訊，請參閱。

用於管理按需任務的 **ONTAP Vscan** 命令

您可以修改、刪除或取消排程隨需工作。您可以檢視工作的摘要和詳細資料、以及管理工作的報告。

如果您想要...	輸入下列命令...
建立隨需工作	`vserver vscan on-demand-task create`
修改隨需工作	`vserver vscan on-demand-task modify`
刪除隨需工作	`vserver vscan on-demand-task delete`
執行隨選工作	`vserver vscan on-demand-task run`
排程隨需工作	`vserver vscan on-demand-task schedule`
取消排程隨需工作	`vserver vscan on-demand-task unschedule`
檢視隨需工作的摘要和詳細資料	`vserver vscan on-demand-task show`
檢視隨需報告	`vserver vscan on-demand-task report show`
刪除隨需報告	`vserver vscan on-demand-task report delete`

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

在 **ONTAP Vscan** 中配置機外防毒功能的最佳實踐

請考量下列在 ONTAP 中設定隨裝即用功能的建議。

- 限制授權使用者執行掃毒作業。一般使用者不應使用授權使用者認證。若要達到此限制、請在 Active Directory 上關閉授權使用者的登入權限。
- 權限使用者不一定要是網域中擁有大量權限的任何使用者群組成員、例如系統管理員群組或備份操作員群組。授權使用者必須僅由儲存系統驗證、才能建立 VScan 伺服器連線並存取檔案進行病毒掃描。
- 請僅將執行 VScan 伺服器的電腦用於病毒掃描。若要阻止一般使用、請停用這些機器上的 Windows 終端機服務和其他遠端存取條款、並授予僅在這些機器上安裝新軟體的權限給系統管理員。
- 將 VScan 伺服器專用於病毒掃描、而不要將其用於其他作業、例如備份。您可以決定將 VScan 伺服器當作虛擬機器（ VM ）來執行。如果您將 VScan 伺服器當作 VM 執行、請確定分配給 VM 的資源並未共用、而且足以執行病毒掃描。
- 為 VScan 伺服器提供足夠的 CPU 、記憶體和磁碟容量、以避免資源過度分配。大多數 VScan 伺服器都是專為使用多個 CPU 核心伺服器而設計、並可在 CPU 之間分配負載。
- NetApp 建議使用專用網路搭配私有 VLAN 、以便從 SVM 連線至 VScan 伺服器、使掃描流量不會受到其他用戶端網路流量的影響。建立獨立的網路介面卡（ NIC ）、專用於 VScan 伺服器上的防毒 VLAN 、以及 SVM 上的資料 LIF 。如果發生網路問題、此步驟可簡化管理和疑難排解。防毒流量應使用私有網路隔離。防毒伺服器應設定為以下列其中一種方式與網域控制站（ DC ）和 ONTAP 通訊：
  - DC 應透過用於隔離流量的私有網路與防毒伺服器通訊。
  - DC 和防毒伺服器應透過不同的網路（而非先前提到的私有網路）進行通訊、這與 CIFS 用戶端網路不同。
  - 若要啟用 Kerberos 驗證以進行防毒通訊、請在 DC 上建立私人生命體的 DNS 項目、並在 DC 上建立對應於為私有 LIF 建立的 DNS 項目的服務主體名稱。將 LIF 新增至防毒連接器時、請使用此名稱。DNS 應能為每個連線至防毒 Connector 的私有 LIF 傳回唯一名稱。

如果 VScan 流量的 LIF 設定在與用戶端流量的 LIF 不同的連接埠上、則 VScan LIF 可能會在連接埠故障時容錯移轉至另一個節點。此變更會使 VScan 伺服器無法從新節點存取、且在節點上執行檔案作業的掃描通知失敗。驗證 VScan 伺服器是否可透過節點上至少一個 LIF 來存取、以便處理掃描要求、以便在該節點上執行檔案作業。

- 使用至少 1GbE 網路連接 NetApp 儲存系統和 VScan 伺服器。
- 對於具有多個 VScan 伺服器的環境、請連接所有具有類似高效能網路連線的伺服器。連接 VScan 伺服器可允許負載共用、進而改善效能。
- 對於遠端站台和分公司、 NetApp 建議使用本機 VScan 伺服器、而非遠端 VScan 伺服器、因為前者是高延遲的最佳選擇。如果成本是因素、請使用筆記型電腦或電腦來提供適度的防毒保護。您可以透過共用磁碟區或 qtree 、並從遠端站台的任何系統掃描、來排程定期完成的檔案系統掃描。
- 使用多部 VScan 伺服器來掃描 SVM 上的資料、以達到負載平衡和備援目的。CIFS 工作負載量和產生的防毒流量會因 SVM 而異。監控儲存控制器上的 CIFS 和病毒掃描延遲。持續監控結果趨勢。如果由於 VScan 伺服器上的 CPU 或應用程式佇列超過趨勢臨界值而導致 CIFS 延遲和病毒掃描延遲增加、則 CIFS 用戶端可能會經歷長時間的等待。新增其他 VScan 伺服器
以分散負載。
- 安裝最新版本的 ONTAP 防毒連接器。
- 將防毒引擎和定義保持在最新狀態。請諮詢合作夥伴、瞭解您應該多久更新一次的建議。
- 在多租戶環境中、只要 VScan 伺服器和 SVM 屬於同一個網域或信任的網域、即可與多個 SVM 共用掃描程

式集區（ VScan 伺服器集區）。

- 受感染檔案的防毒軟體原則應設為「刪除」或「隔離」、這是大多數防毒廠商設定的預設值。如果「 vscan 檔案 op-profile 」設定為「 write_only 」、而且發現受感染的檔案、檔案會保留在共用區中、而且可以開啟、因為開啟檔案不會觸發掃描。防毒掃描只會在檔案關閉後觸發。
- 。 `scan-engine timeout` 值應小於 `scanner-pool request-timeout` 價值。
  如果設定為較高的值、可能會延遲存取檔案、最終可能會逾時。
  若要避免這種情況、請設定 `scan-engine timeout` 少於 5 秒 `scanner-pool request-timeout` 價值。請參閱掃描引擎廠商的文件、以取得如何變更的指示 `scan-engine timeout` 設定：。 `scanner-pool timeout` 您可以在進階模式中使用下列命令、並提供適當的值來變更 `request-timeout` 參數：`vserver vscan scanner-pool modify`。
- 對於規模適合存取掃描工作負載、且需要使用隨選掃描的環境、 NetApp 建議將隨選掃描工作排程在非尖峰時間、以避免現有防毒基礎架構增加負載。

如需更多關於合作夥伴"VScan 合作夥伴解決方案"的最佳實務做法、請參閱。

在 SVM ONTAP Vscan 上啟用病毒掃描

您必須在SVM上啟用掃毒、才能執行隨需存取或隨需掃描。

步驟

1. 在SVM上啟用掃毒：

   ```
   vserver vscan enable -vserver data_SVM
   ```

   如"指令參考資料ONTAP"需詳細 `vserver vscan enable`資訊，請參閱。

   > 如有必要，您可以使用 `vserver vscan disable`命令來停用病毒掃描。如"指令參考資料ONTAP"需詳細 `vserver vscan disable`資訊，請參閱。

   下列命令可在上啟用病毒掃描 `vs1` SVM ：

   ```
   cluster1::> vserver vscan enable -vserver vs1
   ```

2. 確認SVM上已啟用掃毒：

   ```
   vserver vscan show -vserver data_SVM
   ```

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

   下列命令會顯示的 VScan 狀態 `vs1` SVM ：

   ```
   cluster1::> vserver vscan show -vserver vs1

                               Vserver: vs1
                          Vscan Status: on
   ```

重設 ONTAP Vscan 掃描檔的狀態

有時候，您可能會想要重設 SVM 上已成功掃描檔案的掃描狀態，方法是使用 `vserver vscan reset`命令捨棄檔案的快取資訊。例如、您可能想要使用此命令、在錯誤設定的掃描時重新啟動掃毒掃描處理。如"指令參考資料ONTAP"需詳細 `vserver vscan reset`資訊，請參閱。

關於這項工作

執行之後 `vserver vscan reset` 命令、所有符合資格的檔案都會在下次存取時掃描。

視要重新掃描的檔案數量和大小而定、此命令可能會對效能造成不良影響。

開始之前

此工作需要進階權限。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

   如"指令參考資料ONTAP"需詳細 `set -privilege advanced`資訊，請參閱。

2. 重設掃描檔案的狀態：

   ```
   vserver vscan reset -vserver data_SVM
   ```

   下列命令會重設上掃描檔案的狀態 `vs1` SVM ：

   ```
   cluster1::> vserver vscan reset -vserver vs1
   ```

使用 ONTAP 檢視 VScan 事件記錄資訊

您可以使用 `vserver vscan show-events` 命令可檢視受感染檔案、 VScan 伺服器更新等相關事件記錄資訊。您可以檢視叢集或特定節點、SVM或VScan伺服器的事件資訊。

開始之前

檢視 VScan 事件記錄需要進階權限。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

   如"指令參考資料ONTAP"需詳細 `set`資訊，請參閱。

2. 檢視VScan事件記錄資訊：

```
vserver vscan show-events
```

如"指令參考資料ONTAP"需詳細 `vserver vscan show-events`資訊，請參閱。

下列命令會顯示叢集的事件記錄資訊 `cluster1`：

```
cluster1::*> vserver vscan show-events

Vserver     Node            Server          Event Type         Event Time
----------- --------------- --------------- -----------------
-----------------
vs1         Cluster-01      192.168.1.1     file-infected      9/5/2014
11:37:38
vs1         Cluster-01      192.168.1.1     scanner-updated    9/5/2014
11:37:08
vs1         Cluster-01      192.168.1.1     scanner-connected 9/5/2014
11:34:55
3 entries were displayed.
```

監控並疑難排解連線問題

涉及掃描強制選項的潛在 **ONTAP Vscan** 連線問題

您可以使用 `vserver vscan connection-status show` 檢視 VScan 伺服器連線相關資訊的命令、可能有助於疑難排解連線問題。

依預設 `scan-mandatory` 當無法掃描 VScan 伺服器連線時、存取掃描選項會拒絕檔案存取。雖然此選項提供重要的安全功能、但在少數情況下可能會導致問題。

- 在啟用用戶端存取之前、您必須確保至少有一部VScan伺服器連線至每個具有LIF的節點上的SVM。如果您需要在啟用用戶端存取後、將伺服器連線至 SVM 、則必須關閉 `scan-mandatory` SVM 上的選項、可確保檔案存取不會因無法使用 VScan 伺服器連線而遭到拒絕。您可以在伺服器連線後重新開啟選項。
- 如果目標LIF主控SVM的所有VScan伺服器連線、則移轉LIF時、伺服器與SVM之間的連線將會中斷。為了確保檔案存取不會因為無法使用 VScan 伺服器連線而遭到拒絕、您必須關閉 `scan-mandatory` 移轉 LIF 之前的選項。您可以在LIF移轉後重新開啟選項。

每個SVM應至少指派兩部VScan伺服器給它。最佳實務做法是透過不同網路、將VScan伺服器連接至儲存系統、而不使用用於用戶端存取的網路。

如"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

用於查看 **Vscan** 伺服器連線狀態的 **ONTAP** 命令

您可以使用 `vserver vscan connection-status show` 用於檢視 VScan 伺服器連線狀態摘要和詳細資訊的命令。

如果您想要...	輸入下列命令...
檢視VScan伺服器連線的摘要	`vserver vscan connection-status show`
檢視VScan伺服器連線的詳細資料	`vserver vscan connection-status show-all`
檢視連線VScan伺服器的詳細資料	`vserver vscan connection-status show-connected`
檢視未連線之可用VScan伺服器的詳細資料	`vserver vscan connection-status show-not-connected`

如"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

排除病毒 **ONTAP Vscan** 掃描故障

對於常見的病毒掃描問題、有可能的原因和解決方法。病毒掃描也稱為 VScan 。

問題	如何解決此問題
VScan 伺服器無法連線至叢集式 ONTAP 儲存系統。	檢查掃描器集區組態是否指定 VScan 伺服器 IP 位址。也請檢查掃描器集區清單中允許的權限使用者是否為作用中。若要檢查掃描器集區、請執行 `vserver vscan scanner-pool show` 儲存系統命令提示字元上的命令。如果 VScan 伺服器仍無法連線、則網路可能有問題。
用戶端觀察到高延遲。	現在可能是時候將更多 VScan 伺服器新增到掃描器集區了。
觸發的掃描過多。	修改的值 `vscan-fileop-profile` 限制監控進行病毒掃描的檔案作業數的參數。
部分檔案未被掃描。	檢查存取原則。這些檔案的路徑可能已新增至路徑排除清單、或其大小超過設定的排除值。若要檢查存取原則、請執行 `vserver vscan on-access-policy show` 儲存系統命令提示字元上的命令。
檔案存取遭拒。	檢查原則組態中是否指定了 _scan 強制設定。如果沒有連接 VScan 伺服器、此設定會拒絕資料存取。視需要修改設定。

相關資訊

- "Vserver vscan掃描程式集區顯示"
- "Vserver vscan存取時原則顯示"

監控 ONTAP Vscan 狀態和效能活動

您可以監控 VScan 模組的關鍵層面、例如 VScan 伺服器連線狀態、VScan 伺服器的健全狀況、以及已掃描的檔案數量。此資訊有助於您達成目標您可以診斷與 VScan 伺服器相關的問題。

檢視 VScan 伺服器連線資訊

您可以檢視 VScan 伺服器的連線狀態、以管理已在使用中的連線以及可供使用的連線。各種命令會顯示資訊關於 VScan 伺服器的連線狀態。

命令 ...	顯示的資訊 ...
`vserver vscan connection-status show`	連線狀態摘要
`vserver vscan connection-status show-all`	連線狀態的詳細資訊
`vserver vscan connection-status show-not-connected`	可用但未連線的連線狀態
`vserver vscan connection-status show-connected`	有關連線 VScan 伺服器的資訊

如"指令參考資料ONTAP"需詳細 `vserver vscan connection-status show`資訊，請參閱。

檢視 VScan 伺服器統計資料

您可以查看 Vscan 伺服器特定的統計信息，以監控效能並診斷與病毒掃描相關的問題。您必須先收集資料樣本，然後才能使用 `statistics show`命令顯示 Vscan 伺服器統計資料。

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

若要完成資料範例、請完成下列步驟：

步驟

1. 執行 `statistics start`命令和選用命令 `statistics stop`。

   詳細了解 `statistics start`和 `statistics stop`在"指令參考資料ONTAP" 。

檢視 VScan 伺服器要求和延遲的統計資料

您可以使用 ONTAP `offbox_vscan` 以每個 SVM 為基礎的計數器來監控 VScan 的速率每秒發送和接收的伺服器要求、以及所有 VScan 的伺服器延遲伺服器。若要檢視這些統計資料、請完成下列步驟：

步驟

1. 使用下列計數器執行 `statistics show -object offbox_vscan –instance SVM`命令：

計數器 ...	顯示的資訊 ...
scan_request_dispatched_rate	每秒從 ONTAP 傳送至 VScan 伺服器的掃毒要求數
scan_noti_received_rate	ONTAP 每秒從 VScan 伺服器收到的掃毒要求數
dispatch_latency	ONTAP 內的延遲、可識別可用的 VScan 伺服器、並將要求傳送至該 VScan 伺服器
scan_latency	從 ONTAP 到 VScan 伺服器的往返延遲、包括掃描的執行時間

從 **ONTAP offbox vscan** 計數器產生的統計資料範例

```
Object: offbox_vscan
Instance: SVM
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 2 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_noti_received_rate 292
dispatch_latency 43986us
scan_latency 3433501us
-------------------------------------------------------------------
```

檢視個別 **VScan** 伺服器要求和延遲的統計資料

您可以使用 ONTAP `offbox_vscan_server` 每個 SVM 上的計數器、每個隨裝即用 VScan 伺服器、以每個節點為基礎、監控已派遣 VScan 伺服器要求的速度和上的伺服器延遲
每個 VScan 伺服器。若要收集此資訊、請完成下列步驟：

步驟

1. 執行 `statistics show -object offbox_vscan -instance SVM:servername:nodename` 具有下列計數器的命令：

計數器 ...	顯示的資訊 ...
scan_request_dispatched_rate	從 ONTAP 傳送的掃毒要求數
scan_latency	從 ONTAP 到 VScan 伺服器的往返延遲、包括掃描的執行時間 每秒至 VScan 伺服器

從 **ONTAP offbox_vscan** 伺服器計數器產生的統計資料範例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scan_request_dispatched_rate 291
scan_latency 3433830us
-----------------------------------------------------------------
```

檢視 **VScan** 伺服器使用率的統計資料

您也可以使用 ONTAP `offbox_vscan_server` 收集 VScan 伺服器端使用率的計數器
統計資料。這些統計資料會以每個 SVM 、每個隨裝即用 VScan 伺服器和每個節點為基礎進行追蹤。他們
包括 VScan 伺服器上的 CPU 使用率、 VScan 伺服器上掃描作業的佇列深度
（目前和最大）、已用記憶體和已用網路。
防毒連接器會將這些統計資料轉送到 ONTAP 中的統計資料計數器。他們
以每 20 秒輪詢一次的資料為基礎、必須收集多次以確保準確度；
否則、統計資料中所顯示的值只會反映上次輪詢。CPU 使用率和佇列為
監控與分析尤其重要。平均佇列的高值可能表示
VScan 伺服器有瓶頸。
收集每個 SVM 、每個隨裝即用 VScan 伺服器和每個節點上的 VScan 伺服器使用率統計資料
請完成下列步驟：

步驟

1. 收集 VScan 伺服器的使用率統計資料

   執行 `statistics show -object offbox_vscan_server -instance SVM:servername:nodename` 命令 `offbox_vscan_server` 計數器：

計數器 ...	顯示的資訊 ...
`scanner_stats_pct_cpu_used`	VScan 伺服器上的 CPU 使用率
`scanner_stats_pct_input_queue_avg`	VScan 伺服器上掃描要求的平均佇列
`scanner_stats_pct_input_queue_hiwatermark`	VScan 伺服器上掃描要求的尖峰佇列
`scanner_stats_pct_mem_used`	VScan 伺服器上使用的記憶體
`scanner_stats_pct_network_used`	在 VScan 伺服器上使用的網路

VScan 伺服器的使用率統計資料範例

```
Object: offbox_vscan_server
Instance: SVM:vscan_server:node
Start-time: 10/16/2013 10:13:25
End-time: 10/16/2013 10:25:11
Cluster: cluster01
Number of Constituents: 1 (complete_aggregation)
Counter Value
-------------------------------- --------------------------------
scanner_stats_pct_cpu_used 51
scanner_stats_pct_dropped_requests 0
scanner_stats_pct_input_queue_avg 91
scanner_stats_pct_input_queue_hiwatermark 100
scanner_stats_pct_mem_used 95
scanner_stats_pct_network_used 4
---------------------------------------------------------------
```

相關資訊

- "指令參考資料ONTAP"

稽核SVM上的NAS事件

瞭解如何針對 SMB 和 NFS 傳輸協定使用 ONTAP 來稽核檔案存取

您可以搭配ONTAP 使用適用於SMB和NFS傳輸協定的檔案存取稽核功能、例如使用FPolicy進行原生稽核和檔案原則管理。

在下列情況下、您應該設計及實作SMB與NFS檔案存取事件的稽核：

- 已設定基本的SMB和NFS傳輸協定檔案存取。
- 您想要使用下列其中一種方法來建立及維護稽核組態：
  - 原生ONTAP 的功能
  - 外部FPolicy伺服器

稽核SVM上的NAS事件

稽核NAS事件是一項安全性措施、可讓您追蹤及記錄儲存虛擬機器（SVM）上的特定SMB和NFS事件。這有助於您追蹤潛在的安全問題、並提供任何安全漏洞的證據。您也可以登錄及稽核Active Directory集中存取原則、以瞭解實作原則的結果。

SMB 活動

您可以稽核下列事件：

- SMB檔案與資料夾存取事件

  您可以稽核儲存在FlexVol 包含啟用稽核功能之SVM的物件上的SMB檔案和資料夾存取事件。

- SMB登入和登出事件

  您可以稽核SVM上SMB伺服器的SMB登入和登出事件。

- 集中存取原則執行事件

  您可以使用透過建議的集中存取原則套用的權限、來稽核SMB伺服器上物件的有效存取。透過集中存取原則的暫存進行稽核、可讓您在部署中央存取原則之前、先瞭解其影響。

  使用Active Directory GPO設定集中存取原則暫存稽核；不過、SVM稽核組態必須設定為稽核集中存取原則暫存事件。

  雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

NFS 事件

您可以利用NFSv4 ACL來稽核儲存在SVM上的物件、以稽核檔案和目錄事件。

稽核的運作方式

瞭解 ONTAP 的基本稽核概念

若要瞭解ONTAP 功能性稽核、您應該瞭解一些基本的稽核概念。

- 暫存檔案

  在合併與轉換之前、會儲存稽核記錄的個別節點上的中間二進位檔案。暫存檔案包含在暫存磁碟區中。

- 暫存磁碟區

  由支援儲存暫存檔案的功能所建立的專屬Volume ONTAP 。每個Aggregate有一個接移磁碟區。執行磁碟區由所有啟用稽核的儲存虛擬機器（SVM）共享、以儲存資料磁碟區在該特定集合體中的資料存取稽核記錄。每個SVM的稽核記錄都儲存在暫存磁碟區內的個別目錄中。

  叢集管理員可以檢視暫存磁碟區的相關資訊、但不允許執行其他大部分的Volume作業。只ONTAP 有能夠建立暫存磁碟區。自動為暫存磁碟區指派名稱。ONTAP所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID （例如： `MDV_aud_1d0131843d4811e296fc123478563412`）

- 系統磁碟區

  包含特殊中繼資料（例如檔案服務稽核記錄的中繼資料）的Some Volume。FlexVol管理SVM擁有整個叢集可見的系統磁碟區。接移磁碟區是一種系統磁碟區。

- 整合工作

  啟用稽核時建立的工作。這項在每個SVM上長期執行的工作、會將稽核記錄從SVM成員節點上的暫存檔案中

移出。此工作會依照時間順序合併稽核記錄、然後將其轉換成稽核組態中指定的使用者可讀取事件記錄格式（無論是evtx或XML檔案格式）。轉換後的事件記錄會儲存在SVM稽核組態中指定的稽核事件記錄目錄中。

瞭解 **ONTAP** 稽核程序的功能

這個不一樣的稽核程序與Microsoft稽核程序不同。ONTAP在您設定稽核之前、您應該先瞭解ONTAP 不稽核程序的運作方式。

稽核記錄一開始會儲存在個別節點上的二進位暫存檔案中。如果在SVM上啟用稽核、則每個成員節點都會維護該SVM的暫存檔案。這些記錄會定期整合並轉換成使用者可讀取的事件記錄、這些記錄會儲存在SVM的稽核事件記錄目錄中。

在**SVM**上啟用稽核的程序

稽核只能在SVM上啟用。當儲存管理員在SVM上啟用稽核時、稽核子系統會檢查暫存磁碟區是否存在。每個包含SVM擁有之資料磁碟區的Aggregate都必須存在暫存Volume。稽核子系統會建立任何必要的暫存磁碟區（如果不存在）。

稽核子系統也會在啟用稽核之前完成其他必要工作：

- 稽核子系統會驗證記錄目錄路徑是否可用、而且不包含symlink。

  記錄目錄必須已存在於SVM命名空間內的路徑中。建議您建立新的Volume或qtree來保存稽核記錄檔。稽核子系統不會指派預設的記錄檔位置。如果稽核組態中指定的記錄目錄路徑不是有效路徑、則稽核組態建立會失敗 `The specified path "/path" does not exist in the namespace belonging to Vserver "Vserver_name"` 錯誤。

  如果目錄存在但包含symlink、則組態建立會失敗。

- 稽核會排程整合工作。

  排程此工作之後、就會啟用稽核。SVM稽核組態和記錄檔會在重新開機時持續存在、或者NFS或SMB伺服器會停止或重新啟動。

事件記錄整合

記錄整合是一項排程工作、會在停用稽核之前、定期執行。停用稽核時、整合工作會驗證是否已合併所有剩餘的記錄。

保證稽核

依預設、稽核是保證的。此功能可確保記錄所有可稽核的檔案存取事件（如設定的稽核原則ACL所指定）、即使節點無法使用亦然。ONTAP在將該作業的稽核記錄儲存至持續儲存設備上的暫存磁碟區之前、無法完成要求的檔案作業。如果稽核記錄無法提交至暫存檔案中的磁碟、無論是因為空間不足或其他問題、用戶端作業都會遭到拒絕。

系統管理員或具有權限層級存取權的帳戶使用者、可以使用NetApp Manageability SDK或REST API來略過檔案稽核記錄作業。您可以檢閱儲存在中的命令記錄檔、判斷是否已使用 NetApp Manageability SDK 或 REST API 執行任何檔案動作 `audit.log` 檔案：

如需命令歷程記錄稽核記錄的詳細資訊、請參閱中的「管理管理管理活動的稽核記錄」一節 "系統管理"。

節點無法使用時的整合程序

如果包含屬於已啟用稽核之SVM的磁碟區的節點無法使用、則稽核整合工作的行為取決於節點的儲存容錯移轉（SFO）合作夥伴（或是雙節點叢集的HA合作夥伴）是否可用：

- 如果接移磁碟區可透過SFO合作夥伴取得、則會掃描上次從節點回報的接移磁碟區、並正常進行整合。
- 如果無法取得SFO合作夥伴、工作會建立部分記錄檔。

  當節點無法連線時、整合工作會整合該SVM其他可用節點的稽核記錄。為了識別尚未完成、工作會新增後置字元 `.partial` 合併的檔案名稱。

- 當無法使用的節點可用之後、該節點中的稽核記錄會與當時來自其他節點的稽核記錄合併。
- 所有稽核記錄都會保留下來。

事件記錄檔循環

稽核事件記錄檔會在達到設定的臨界值記錄大小或已設定的排程時進行旋轉。當事件記錄檔旋轉時、排程的整合工作會先將作用中的轉換檔重新命名為具有時間戳記的歸檔檔檔、然後建立新的作用中轉換事件記錄檔。

在**SVM**上停用稽核的程序

在SVM上停用稽核時、整合工作會最後觸發一次。所有未處理、記錄的稽核記錄都會以使用者可讀取的格式記錄。在SVM上停用稽核且可供檢視時、不會刪除儲存在事件記錄目錄中的現有事件記錄。

合併該SVM的所有現有暫存檔案之後、整合工作就會從排程中移除。停用SVM的稽核組態不會移除稽核組態。儲存管理員可以隨時重新啟用稽核。

稽核整合工作會在啟用稽核時建立、可監控整合工作、並在整合工作因錯誤而結束時重新建立。使用者無法刪除稽核整合工作。

ONTAP 稽核的必要條件

在儲存虛擬機器（SVM）上設定及啟用稽核之前、您必須瞭解特定的需求和考量。

- NFS 和 S3 稽核啟用 SVM 的合併限制取決於您的 ONTAP 版本：

版本ONTAP	最大值
9.8 及更早版本	50
9.9.1及更新版本	400

- 稽核不受限於SMB或NFS授權。

即使叢集上未安裝SMB與NFS授權、您仍可設定及啟用稽核。

- NFS稽核支援安全性ACE（類型U）。
- 對於NFS稽核、模式位元與稽核ACE之間沒有對應關係。

  將ACL轉換為模式位元時、會跳過稽核ACE。將模式位元轉換為ACL時、不會產生稽核ACE。

- 稽核組態中指定的目錄必須存在。

  如果不存在、建立稽核組態的命令就會失敗。

- 稽核組態中指定的目錄必須符合下列需求：
  - 目錄不得包含符號連結。

    如果稽核組態中指定的目錄包含符號連結、建立稽核組態的命令就會失敗。

  - 您必須使用絕對路徑來指定目錄。

    您不應指定相對路徑、例如 `/vs1/../`。

- 稽核取決於暫存磁碟區中是否有可用空間。

  您必須瞭解並制定計畫、確保集合體中含有稽核磁碟區的暫存磁碟區有足夠的空間。

- 稽核取決於磁碟區中是否有可用空間、其中包含儲存轉換事件記錄的目錄。

  您必須注意並制定計畫、確保用於儲存事件記錄的磁碟區有足夠的空間。您可以使用指定要保留在稽核目錄中的事件記錄數目 `-rotate-limit` 建立稽核組態時的參數、有助於確保磁碟區中有足夠的可用空間用於事件記錄。

- 雖然您可以在稽核組態中啟用集中存取原則接移、而不需在SMB伺服器上啟用動態存取控制、但必須啟用動態存取控制、才能產生集中存取原則接移事件。

  預設不會啟用動態存取控制。

啟用稽核時的**Aggregate space**考量

建立稽核組態並在叢集中至少一個儲存虛擬機器（SVM）上啟用稽核時、稽核子系統會在所有現有的集合體和所有建立的新集合體上建立暫存磁碟區。在叢集上啟用稽核時、您必須注意特定的Aggregate空間考量。

由於Aggregate中的空間不可用、所以暫存磁碟區建立可能會失敗。如果您建立稽核組態、而現有的Aggregate沒有足夠的空間來容納接移磁碟區、就可能發生這種情況。

在SVM上啟用稽核之前、您應該先確定現有集合體上有足夠的空間可用於暫存磁碟區。

限制 **ONTAP** 稽核記錄的暫存檔案大小

暫存檔案上的稽核記錄大小不得大於32 KB。

發生大型稽核記錄時

在下列其中一種情況下、在管理稽核期間可能會發生大量的稽核記錄：

- 新增或刪除具有大量使用者之群組的使用者。
- 新增或刪除檔案共用區上的檔案共用存取控制清單（ACL）、以供大量的檔案共用使用者使用。
- 其他案例。

停用管理稽核以避免此問題。若要這麼做、請修改稽核組態、並從稽核事件類型清單中移除下列項目：

- 檔案共用
- 使用者帳戶
- 安全性群組
- 授權原則變更

  移除之後、檔案服務稽核子系統不會稽核這些檔案。

稽核記錄過大的影響

- 如果稽核記錄的大小過大（超過32 KB）、則不會建立稽核記錄、稽核子系統會產生類似下列的事件管理系統（EMS）訊息：

  ```
  File Services Auditing subsystem failed the operation or truncated an audit
  record because it was greater than max_audit_record_size value. Vserver
  UUID=%s, event_id=%u, size=%u
  ```

  如果保證稽核、則檔案作業會因為無法建立稽核記錄而失敗。

- 如果稽核記錄的大小超過9、999個位元組、則會顯示與上述相同的EMS訊息。系統會建立部分稽核記錄、但缺少較大的金鑰值。
- 如果稽核記錄超過2、000個字元、則會顯示下列錯誤訊息、而非實際值：

  ```
  The value of this field was too long to display.
  ```

瞭解 ONTAP 稽核事件記錄的支援格式

已轉換的稽核事件記錄檔支援的檔案格式為 EVTX 和 XML 檔案格式。

您可以在建立稽核組態時指定檔案格式的類型。根據預設、 ONTAP 會將二進位記錄轉換成 EVTX 檔案格式。

檢視及處理 ONTAP 稽核事件記錄

您可以使用稽核事件記錄來判斷是否有足夠的檔案安全性、以及是否有不當的檔案和資料夾存取嘗試。您可以檢視及處理儲存在中的稽核事件記錄 EVTX 或 XML 檔案格式。

- EVTX 檔案格式

您可以開啟已轉換的 EVTX 使用 Microsoft 事件檢視器將事件記錄稽核為儲存的檔案。

使用「事件檢視器」檢視事件記錄時、您可以使用兩種選項：

- 一般檢視

  所有事件的通用資訊都會顯示在事件記錄中。在此版本ONTAP 的資訊不顯示事件記錄的事件特定資料。您可以使用詳細檢視來顯示特定事件的資料。

- 詳細檢視

  提供友善的檢視和XML檢視。易記檢視和XML檢視會同時顯示所有事件通用的資訊、以及事件記錄的事件特定資料。

- XML 檔案格式

  您可以檢視及處理 XML 稽核支援的協力廠商應用程式上的事件記錄 XML 檔案格式。XML檢視工具可用於檢視稽核記錄、前提是您必須具備XML架構和XML欄位定義的相關資訊。如需XML架構和定義的詳細資訊、請參閱 "《稽核架構參考》ONTAP"。

使用事件檢視器檢視作用中稽核記錄的方式

如果稽核整合程序正在叢集上執行、則整合程序會將新記錄附加到啟用稽核的儲存虛擬機器（SVM）作用中稽核記錄檔。此作用中稽核記錄可透過Microsoft事件檢視器中的SMB共用區存取及開啟。

除了檢視現有的稽核記錄之外、「事件檢視器」還提供重新整理選項、可讓您重新整理主控台視窗中的內容。新附加的記錄是否可在事件檢視器中檢視、取決於是否在用來存取作用中稽核記錄的共用區上啟用oplocks。

共享區上的oplocks設定	行為
已啟用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業不會以合併程序附加的新事件來重新整理記錄。
已停用	「事件檢視器」會開啟記錄、其中包含寫入到該時間點的事件。重新整理作業會以合併程序附加的新事件來重新整理記錄。

此資訊僅適用於 EVTX 事件記錄。 XML 事件記錄可以透過 SMB 瀏覽器或 NFS 、使用任何 XML 編輯器或檢視器來檢視。

可稽核的SMB事件

瞭解 **ONTAP** 可稽核以解讀結果的 **SMB** 事件

可稽核特定的SMB事件、包括特定檔案和資料夾存取事件、特定登入和登出事件、以及集中存取原則暫存事件。ONTAP瞭解哪些存取事件可以稽核、有助於解讀事件記錄的結果。

可以審核以下附加 SMB 事件：

事件ID（EVT/evtx）	活動	說明	類別

4670	物件權限已變更	物件存取：權限已變更。	檔案存取
4907	物件稽核設定已變更	物件存取：稽核設定已變更。	檔案存取
4913.	物件中心存取原則已變更	物件存取：CAP已變更。	檔案存取

下列SMB事件ONTAP 可在下列版本中透過下列功能進行稽核：

事件ID（EVT/evtx）	活動	說明	類別
540/4624	帳戶已成功登入	登入/登出：網路（SMB）登入。	登入與登出
598/4625	帳戶無法登入	登入/登出：不明的使用者名稱或錯誤的密碼。	登入與登出
530/4625	帳戶無法登入	登入/登出：帳戶登入時間限制。	登入與登出
531/4625	帳戶無法登入	登入/登出：帳戶目前已停用。	登入與登出
532/4625	帳戶無法登入	登入/登出：使用者帳戶已過期。	登入與登出
533/4625	帳戶無法登入	登入/登出：使用者無法登入此電腦。	登入與登出
534/4625	帳戶無法登入	登入/登出：使用者未在此授予登入類型。	登入與登出
535/4625	帳戶無法登入	登入/登出：使用者密碼已過期。	登入與登出
537-4625	帳戶無法登入	登入/登出：登入失敗的原因並非上述原因。	登入與登出
5310/4625	帳戶無法登入	登入/登出：帳戶已鎖定。	登入與登出
538/4634	帳戶已登出	登入/登出：本機或網路使用者登出。	登入與登出
560/ 4656	開啟物件/建立物件	物件存取：物件（檔案或目錄）開啟。	檔案存取
563/4659	開啟要刪除的物件	物件存取：要求物件（檔案或目錄）的控點、目的是刪除。	檔案存取

564/4660	刪除物件	物件存取：刪除物件（檔案或目錄）。當Windows用戶端嘗試刪除物件（檔案或目錄）時、會產生此事件。ONTAP	檔案存取
567/4663	讀取物件/寫入物件/取得物件屬性/設定物件屬性	物件存取：物件存取嘗試（讀取、寫入、取得屬性、設定屬性）。 附註： ONTAP 針對此活動、僅針對物件上的第一個SMB讀取和第一個SMB寫入作業（成功或失敗）進行不稽核。這可防止ONTAP 在單一用戶端開啟物件並對同一個物件執行多次連續的讀取或寫入作業時、造成過多的記錄項目。	檔案存取
NA/4664	硬式連結	物件存取：嘗試建立硬式連結。	檔案存取
NA/4818	建議的集中存取原則並未授予與目前集中存取原則相同的存取權限	物件存取：集中存取原則Staging。	檔案存取
NA/ NA Data ONTAP 不適用事件ID 9999	重新命名物件	物件存取：物件已重新命名。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取
NA/ NA Data ONTAP 不景事件ID 9998	取消連結物件	物件存取：物件未連結。這是一個不確定的事件。ONTAPWindows目前不支援將它當成單一事件。	檔案存取

活動**4656**的其他相關資訊

。 `HandleID` 稽核中的標記 `XML` 事件包含所存取物件（檔案或目錄）的處理方式。。 `HandleID` evtx 4656 事件的標記包含不同的資訊、取決於開啟的事件是用於建立新物件或開啟現有物件：

- 如果開啟的事件是建立新物件（檔案或目錄）的開放式要求、則 `HandleID` 稽核 XML 事件中的標記顯示為空白 `HandleID` （例如： `<Data Name="HandleID">00000000000000;00;00000000;00000000</Data>` ）。

  。 `HandleID` 為空白、因為在實際物件建立之前和處理代碼存在之前、會先稽核開啟（用於建立新物件）的要求。相同物件的後續稽核事件在中具有適當的物件控點 `HandleID` 標記。

- 如果開啟的事件是開啟現有物件的開放式要求、則稽核事件會在中指派該物件的處理代碼 `HandleID` 標記（例如： `<Data Name="HandleID">00000000000401;00;000000ea;00123ed4</Data>` ）。

決定 **ONTAP** 稽核物件的完整路徑

列印在中的物件路徑 `<ObjectName>` 稽核記錄的標記包含磁碟區名稱（以括弧括住）、以及包含磁碟區根目錄的相對路徑。如果您想要判斷稽核物件的完整路徑（包括交會路徑

）、您必須採取某些步驟。

步驟

1. 請查看、判斷哪些磁碟區名稱和受稽核物件的相對路徑 `<ObjectName>` 稽核事件中的標記。

   在此範例中、磁碟區名稱為「 data1 」、檔案的相對路徑為 `/dir1/file.txt`：

   ```
   <Data Name="ObjectName"> (data1);/dir1/file.txt </Data>
   ```

2. 使用上一步驟所決定的磁碟區名稱、判斷包含稽核物件之磁碟區的交會路徑：

   在此範例中、磁碟區名稱為「 data1 」、而包含稽核物件之磁碟區的交會路徑為 `/data/data1`：

   ```
   volume show -junction -volume data1
   ```

   ```
                                  Junction                       Junction
   Vserver   Volume       Language Active    Junction Path      Path Source
   --------- ------------ -------- --------  ------------------ -----------
   vs1       data1        en_US.UTF-8
                                  true      /data/data1        RW_volume
   ```

3. 附加在中找到的相對路徑、以決定稽核物件的完整路徑 `<ObjectName>` 標記為磁碟區的交會路徑。

   在此範例中、磁碟區的交會路徑為：

   ```
   /data/data1/dir1/file.text
   ```

瞭解 **ONTAP** 對符號連結和硬式連結的稽核

稽核symlink和硬式連結時、必須謹記某些考量事項。

稽核記錄包含所稽核物件的相關資訊、包括中所識別的已稽核物件路徑 `ObjectName` 標記。您應該瞭解 symlinks 和硬式連結的路徑如何記錄在中 `ObjectName` 標記。

symlinks

symlink是一個具有獨立inode的檔案、其中包含指向目的地物件（稱為目標）位置的指標。透過symlink存取物件時ONTAP 、流通會自動解譯symlink、並遵循實際規範的非規範傳輸協定路徑、前往磁碟區中的目標物件。

在下列範例輸出中、有兩個 symlink 、兩者都指向一個名為的檔案 `target.txt`。其中一個symlink是相對symlink、一個是絕對symlink。如果稽核其中任一符號連結、則為 `ObjectName` 稽核事件中的標記包含檔案路徑 `target.txt`：

```
[root@host1 audit]# ls -l
total 0
lrwxrwxrwx 1 user1 group1 37 Apr  2 10:09 softlink_fullpath.txt ->
/data/audit/target.txt
lrwxrwxrwx 1 user1 group1 10 Apr  2 09:54 softlink.txt -> target.txt
-rwxrwxrwx 1 user1 group1 16 Apr  2 10:05 target.txt
```

硬式連結

硬式連結是指將名稱與檔案系統上現有檔案相關聯的目錄項目。硬式連結指向原始檔案的inode位置。如同用什麼方式解譯symlinks、它會解譯硬式連結、並遵循實際規範路徑前往Volume中的目標物件。ONTAP ONTAP稽核硬式連結物件的存取時、稽核事件會在中記錄這條絕對規範路徑 `ObjectName` 標記而非硬連結路徑。

瞭解替代 **NTFS** 資料串流的 **ONTAP** 稽核

在使用NTFS替代資料流稽核檔案時、您必須謹記某些考量事項。

要稽核的物件位置會使用兩個標籤（即）記錄在事件記錄中 `ObjectName` 標記（路徑）和 `HandleID` 標記（控點）。若要正確識別正在記錄的串流要求、您必須知道ONTAP 這些欄位中有哪些資料流是NTFS替代資料串流的佐證記錄：

- evtxID：4656個事件（開啟並建立稽核事件）
  - 替代資料串流的路徑會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。
- evtxID：4663個事件（所有其他稽核事件、例如讀取、寫入、getattr等）
  - 基礎檔案的路徑、而非替代資料串流、會記錄在中 `ObjectName` 標記。
  - 替代資料串流的處理方式會記錄在中 `HandleID` 標記。

範例

下列範例說明如何使用識別 evtx ID ： 4663 個事件以用於替代資料串流 `HandleID` 標記。即使是 `ObjectName` 在讀取稽核事件中記錄的標記（路徑）位於基礎檔案路徑 `HandleID` 標記可用於將事件識別為替代資料串流的稽核記錄。

串流檔案名稱採用格式 `base_file_name:stream_name`。在此範例中 `dir1` 目錄包含基礎檔案、具有下列路徑的替代資料串流：

```
/dir1/file1.txt
/dir1/file1.txt:stream1
```

下列事件範例中的輸出會如所示被刪減；輸出不會顯示事件的所有可用輸出標記。

對於 evtx ID 4656 （開放式稽核事件）、替代資料串流的稽核記錄輸出會在中記錄替代資料串流名稱 `ObjectName` 標記：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4656</EventID>
  <EventName>Open Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt:stream1</Data\>
**
  [...]
  </EventData>
  </Event>
- <Event>
```

對於 evtx ID 4663 （讀取稽核事件）、相同替代資料串流的稽核記錄輸出會在中記錄基礎檔案名稱 `ObjectName` 標記；不過、中的控點 `HandleID` 標記是替代資料串流的處理方式、可用於將此事件與替代資料串流建立關聯：

```
- <Event>
- <System>
  <Provider Name="Netapp-Security-Auditing" />
  <EventID>4663</EventID>
  <EventName>Read Object</EventName>
  [...]
  </System>
- <EventData>
  [...]
  **<Data Name="ObjectType"\>Stream</Data\>
  <Data Name="HandleID"\>00000000000401;00;000001e4;00176767</Data\>
  <Data Name="ObjectName"\>\(data1\);/dir1/file1.txt</Data\> **
  [...]
  </EventData>
  </Event>
- <Event>
```

瞭解 **ONTAP** 對 **NFS** 檔案和目錄存取事件的稽核

可以稽核某些NFS檔案和目錄存取事件。ONTAP瞭解哪些存取事件可稽核、有助於解讀轉換後的稽核事件記錄結果。

您可以稽核下列NFS檔案和目錄存取事件：

- 讀取
- 開啟
- 關閉
- readdir
- 寫入
- 設定
- 建立
- 連結
- OPENATTR
- 移除
- GetAttr
- 驗證
- n驗證
- 重新命名

若要可靠地稽核NFS重新命名事件、您應該在目錄上設定稽核ACE、而不要在檔案上設定、因為如果目錄權限足夠、就不會檢查檔案權限來執行重新命名作業。

規劃 **ONTAP VM** 上的稽核組態

在儲存虛擬機器（SVM）上設定稽核之前、您必須先瞭解可用的組態選項、並針對每個選項規劃您要設定的值。此資訊可協助您設定稽核組態、以滿足您的業務需求。

所有稽核組態都有一些通用的組態參數。

此外、您也可以使用某些參數來指定在旋轉合併和轉換的稽核記錄時使用哪些方法。您可以在設定稽核時指定下列三種方法之一：

- 根據記錄大小來旋轉記錄

  這是用來旋轉記錄的預設方法。

- 根據排程來旋轉記錄
- 根據記錄大小和排程來旋轉記錄（以先發生的事件為準）

至少應設定一種記錄輪調方法。

所有稽核組態的通用參數

建立稽核組態時、必須指定兩個必要參數。您也可以指定三個選用參數：

資訊類型	選項	必要	包括	您的價值

*SVM*名稱 要在其中建立稽核組態的SVM名稱。SVM必須已經存在。	`-vserver vserver_name`	是的	是的	
記錄目的地路徑 指定儲存已轉換稽核記錄的目錄、通常是專屬磁碟區或qtree。路徑必須已存在於SVM命名空間中。 路徑長度最多可達864個字元、且必須具有讀寫權限。 如果路徑無效、稽核組態命令就會失敗。 如果SVM是SVM災難恢復來源、則記錄目的地路徑無法位於根磁碟區上。這是因為根磁碟區內容並未複寫到災難恢復目的地。 您無法將FlexCache 無法使用的功能區當成記錄目的地ONTAP （例如、更新版本的更新版本）。	`-destination text`	是的	是的	

要稽核的事件類別_ 指定要稽核的事件類別。您可以稽核下列事件類別： • 檔案存取事件（SMB和NFSv4） • SMB登入和登出事件 • 集中存取原則執行事件 從 Windows 2012 Active Directory 網域開始、就可以使用中央存取原則的移位事件。 • 非同步刪除 • 檔案共用類別事件 • 稽核原則變更事件 • 本機使用者帳戶管理事件 • 安全性群組管理事件 • 授權原則變更事件 預設為稽核檔案存取和SMB登入及登出事件。 • 備註： * 您可以先指定 `cap-staging` 在事件類別中、 SVM 上必須存在 SMB 伺服器。雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。	`-events{file-ops`	`cifs-logon-logoff`	`cap-staging`	`file-share`
`audit-policy-change`	`user-account`	`security-group`	`authorization-policy-change`	`async-delete}`

否			記錄檔案輸出格式 決定稽核記錄的輸出格式。輸出格式可以是 ONTAP 專用格式 `XML` 或 Microsoft Windows `EVTX` 記錄格式。依預設、輸出格式為 `EVTX`。	`-format {xml`
`evtx}`	否			記錄檔案旋轉限制 決定要保留多少稽核記錄檔、然後再將最舊的記錄檔轉出。例如、如果您輸入的值 `5`，最後五個記錄檔會保留。 的值 `0` 表示保留所有記錄檔。預設值為 0 。

用於判斷何時旋轉稽核事件記錄的參數

根據記錄大小旋轉記錄

預設值是根據大小來旋轉稽核記錄。

- 預設記錄大小為100 MB
- 如果您要使用預設的記錄檔旋轉方法和預設的記錄檔大小、則不需要設定任何特定的記錄檔旋轉參數。

- 如果您想要根據記錄檔大小來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-schedule-minute` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-schedule-minute -`

如果您不想使用預設記錄大小、可以設定 `-rotate-size` 指定自訂記錄大小的參數：

資訊類型	選項	必要	包括	您的價值
記錄檔案大小限制 決定稽核記錄檔大小限制。	`-rotate-size {integer[kb`	MB	GB	TB

根據排程旋轉記錄

如果您選擇根據排程來旋轉稽核記錄、您可以使用任何組合的時間型旋轉參數來排程記錄輪調。

- 如果您使用時間型旋轉、則會使用 `-rotate-schedule-minute` 參數為必填。
- 所有其他的時間型旋轉參數都是選用的。
- 旋轉排程是使用所有與時間相關的值來計算。

  例如、如果您只指定 `-rotate-schedule-minute` 參數時、稽核記錄檔會根據一週中所有天所指定的分鐘數、在一年中所有月份的所有小時內進行旋轉。

- 如果只指定一或兩個時間型旋轉參數（例如、 `-rotate-schedule-month` 和 `-rotate-schedule -minutes`）、記錄檔會根據您在一週的所有天、所有時間、但僅在指定的月份內所指定的分鐘值來旋轉。

  例如、您可以指定稽核日誌在一月、三月和八月的所有週一、週三和週六上午10：30進行輪調

- 如果您同時指定兩者的值 `-rotate-schedule-dayofweek` 和 `-rotate-schedule-day`的問題。

  例如、如果您指定 `-rotate-schedule-dayofweek` 星期五和 `-rotate-schedule-day` 截至 13 日、稽核記錄將會在每週五和指定月份的第 13 天、而不只是在每週五的第 13 天輪調。

- 如果您想要根據排程來旋轉稽核記錄檔、請使用下列命令來取消設定 `-rotate-size` 參數： `vserver audit modify -vserver vs0 -destination / -rotate-size -`

您可以使用下列可用稽核參數清單、來決定要使用哪些值來設定稽核事件記錄輪調的排程：

資訊類型	選項	必要	包括	您的價值
記錄輪調排程：月 決定每月循環稽核記錄的排程。 有效值為 `January` 透過 `December`和 `all`。例如、您可以指定稽核日誌在1月、3月和8月期間輪調。	`-rotate-schedule-month chron_month`	否		

記錄輪調排程：週中日 決定每日（一週中的某天）排程以循環稽核記錄。 有效值為 `Sunday` 透過 `Saturday`和 `all`。例如、您可以指定稽核日誌在週二和週五、或一週中的所有日子循環顯示。	`-rotate-schedule -dayofweek chron_dayofweek`	否		
記錄輪調排程：天 決定每月的日期排程、以循環稽核記錄。 有效值範圍從 `1` 透過 `31`。例如、您可以指定稽核日誌在每月的第10天和第20天、或每月的所有天進行旋轉。	`-rotate-schedule-day chron_dayofmonth`	否		
_記錄輪調排程：hour _ 決定每小時循環稽核記錄的排程。 有效值範圍從 `0` （午夜）至 `23` （下午 11 ： 00 ）。指定 `all` 每小時輪換稽核記錄。例如、您可以指定稽核日誌的旋轉時間為6（上午6點）和18（下午6點）。	`-rotate-schedule-hour chron_hour`	否		
記錄輪調排程：分 決定稽核日誌的分鐘排程。 有效值範圍從 `0` 至 `59`。例如、您可以指定稽核日誌在30分鐘內旋轉。	`-rotate-schedule-minute chron_minute`	是、如果設定排程型記錄輪調、則為否		

根據記錄大小和排程來旋轉記錄

您可以選擇根據記錄大小和排程來旋轉記錄檔、方法是同時設定 `-rotate-size` 參數和時間型旋轉參數。例如：IF `-rotate-size` 設為 10 MB 、且 `-rotate-schedule-minute` 設為 15 、當記錄檔大小達到 10 MB 或每小時 15 分鐘（以先發生的事件為準）時、記錄檔會旋轉。

在**SVM**上建立檔案和目錄稽核組態

在 **ONTAP VM** 上建立檔案和目錄稽核組態

在儲存虛擬機器（SVM）上建立檔案和目錄稽核組態、包括瞭解可用的組態選項、規劃組態、然後設定和啟用組態。然後您可以顯示稽核組態的相關資訊、以確認所產生的組態為所需的組態。

在開始稽核檔案和目錄事件之前、您必須先在儲存虛擬機器（SVM）上建立稽核組態。

開始之前

如果您打算建立稽核組態以進行集中存取原則暫存、則SVM上必須有SMB伺服器。

- 雖然您可以在稽核組態中啟用集中存取原則接移功能、但不會在SMB伺服器上啟用動態存取控制、但只有啟用動態存取控制時、才會產生集中存取原則接移事件。

  動態存取控制是透過SMB伺服器選項來啟用。預設不會啟用此功能。

- 如果命令中某個欄位的引數無效、例如欄位的輸入無效、項目重複、以及項目不存在、則命令會在稽核階段之前失敗。

  此類失敗不會產生稽核記錄。

關於這項工作

如果SVM是SVM災難恢復來源、則目的地路徑無法位於根磁碟區上。

步驟

1. 使用規劃工作表中的資訊、建立稽核組態、根據記錄大小或排程來旋轉稽核記錄：

如果您想要以下列方式來旋轉稽核記錄…	輸入…
記錄檔大小	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging
file-share	authorization-policy-change
user-account	security-group
authorization-policy-change}] [-format {xml	evtx}] [-rotate-limit integer] [-rotate-size {integer[KB
MB	GB
TB	PB]}]`
排程	`vserver audit create -vserver vserver_name -destination path -events [{file-ops
cifs-logon-logoff	cap-staging}] [-format {xml

範例

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/audit_log` 目錄。記錄檔大小限制為 `200 MB`。當記錄大小達到200 MB時、就會進行旋轉：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-rotate-size 200MB
```

下列範例會建立稽核組態、以大小為基礎的旋轉方式來稽核檔案作業和SMB登入及登出事件（預設值）。記錄格式為 `EVTX` （預設）。記錄會儲存在中 `/cifs_event_logs` 目錄。記錄檔大小限制為 `100 MB` （預設值）、且記錄輪調限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination
/cifs_event_logs -rotate-limit 5
```

下列範例建立稽核組態、以稽核檔案作業、CIFS登入和登出事件、以及使用時間型輪調的集中存取原則暫存事件。記錄格式為 `EVTX` （預設）。稽核記錄會每月於下午12：30循環一次一週中的所有天。日誌輪轉限制為 `5`：

```
cluster1::> vserver audit create -vserver vs1 -destination /audit_log
-events file-ops,cifs-logon-logoff,file-share,audit-policy-change,user-
account,security-group,authorization-policy-change,cap-staging -rotate
-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour
12 -rotate-schedule-minute 30 -rotate-limit 5
```

相關資訊

- "在SVM上啟用稽核"
- "驗證稽核組態"

在設定稽核組態之後，啟用 **ONTAP SVM** 的稽核

完成稽核組態的設定之後、您必須在儲存虛擬機器（SVM）上啟用稽核。

開始之前

SVM稽核組態必須已經存在。

關於這項工作

當SVM災難恢復ID捨棄組態第一次啟動（完成SnapMirror初始化之後）且SVM具有稽核組態時ONTAP 、無法自動停用稽核組態。在唯讀SVM上停用稽核、以防止執行磁碟區填滿。只有在SnapMirror關係中斷且SVM為讀寫時、才能啟用稽核。

步驟

1. 在SVM上啟用稽核：

   ```
   vserver audit enable -vserver vserver_name

   vserver audit enable -vserver vs1
   ```

相關資訊

- "建立稽核組態"
- "驗證稽核組態"

驗證 ONTAP 稽核組態

完成稽核組態之後、您應該確認稽核設定正確且已啟用。

步驟

1. 驗證稽核組態：

   ```
   vserver audit show -instance -vserver vserver_name
   ```

   下列命令會以清單形式顯示儲存虛擬機器（SVM）VS1的所有稽核組態資訊：

   ```
   vserver audit show -instance -vserver vs1
   ```

   ```
                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                           Log Format: evtx
                  Log File Size Limit: 200MB
        Log Rotation Schedule: Month: -
   Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
   ```

相關資訊

- "建立稽核組態"
- "在SVM上啟用稽核"

設定檔案和資料夾稽核原則

啟用 ONTAP SVM 上的稽核組態，並設定檔案和資料夾稽核原則

在檔案和資料夾存取事件上實作稽核是兩步驟的程序。首先、您必須在儲存虛擬機器（SVM）上建立並啟用稽核組態。其次、您必須在要監控的檔案和資料夾上設定稽核原則。您可以設定稽核原則、以監控成功和失敗的存取嘗試。

您可以設定SMB和NFS稽核原則。SMB與NFS稽核原則具有不同的組態需求與稽核功能。

如果已設定適當的稽核原則、ONTAP 僅當SMB或NFS伺服器正在執行時、才會監控稽核原則中指定的SMB和NFS存取事件。

在 **NTFS** 安全性樣式的檔案和目錄上設定 **ONTAP** 稽核原則

在稽核檔案和目錄作業之前、您必須先在要收集稽核資訊的檔案和目錄上設定稽核原則。這是設定及啟用稽核組態的附加功能。您可以使用Windows安全性索引標籤或ONTAP 使用CLI來設定NTFS稽核原則。

使用**Windows**安全性索引標籤設定**NTFS**稽核原則

您可以使用「Windows內容」視窗中的「* Windows安全性*」索引標籤、在檔案和目錄上設定NTFS稽核原則。這是在Windows用戶端上設定資料稽核原則時所使用的相同方法、讓您能夠使用慣用的GUI介面。

開始之前

稽核必須在儲存虛擬機器（SVM）上設定、其中包含您要套用系統存取控制清單（SACL）的資料。

關於這項工作

若要設定NTFS稽核原則、請將項目新增至與NTFS安全性描述元相關聯的NTFS SACL。然後將安全性描述元套用至NTFS檔案和目錄。這些工作會由Windows GUI自動處理。安全性描述元可包含用於套用檔案和資料夾存取權限的判別存取控制清單（DACL）、用於檔案和資料夾稽核的SACL、或同時套用SACL和DACL。

若要使用Windows安全性索引標籤設定NTFS稽核原則、請在Windows主機上完成下列步驟：

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 填寫*對應網路磁碟機*方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入包含共用區的SMB伺服器名稱、其中包含您要稽核的資料及共用區名稱。

      您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

      如果您的 SMB 伺服器名稱為「 ShMB_Server 」、而您的共用名稱為「 shahre1 」、則您應該輸入 `\\SMB_SERVER\share1`。

   c. 單擊*完成*。

   您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要啟用稽核存取的檔案或目錄。
4. 以滑鼠右鍵按一下檔案或目錄、然後選取*內容*。
5. 選取*安全性*索引標籤。
6. 按一下*進階*。
7. 選取*稽核*索引標籤。
8. 執行所需的動作：

如果你想…	請執行下列動作

設定新使用者或群組的稽核	a. 按一下「 * 新增 * 」。 b. 在「輸入要選取的物件名稱」方塊中、輸入您要新增的使用者或群組名稱。 c. 按一下「確定」。
移除使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要移除的使用者或群組。 b. 按一下「移除」。 c. 按一下「確定」。 d. 跳過此程序的其餘部分。
變更使用者或群組的稽核	a. 在「輸入要選取的物件名稱」方塊中、選取您要變更的使用者或群組。 b. 按一下 * 編輯 * 。 c. 按一下「確定」。

如果您要在使用者或群組上設定稽核、或是變更現有使用者或群組的稽核、就會開啟「<object>的稽核項目」方塊。

9. 在「套用至」方塊中、選取您要套用此稽核項目的方式。

   您可以選擇下列其中一項：

   - 此資料夾、子資料夾及檔案
   - 此資料夾及子資料夾
   - 僅此資料夾
   - 此資料夾與檔案
   - 僅限子資料夾與檔案
   - 僅子資料夾
   - * 僅檔案 *
     如果您要在單一檔案上設定稽核、則「 * 套用至 * 」方塊不會啟用。「套用至」方塊設定預設為*僅此物件*。

   由於稽核需要SVM資源、因此請僅選取提供稽核事件的最低層級、以符合您的安全需求。

10. 在「存取」方塊中、選取您要稽核的項目、以及是否要稽核成功的事件、失敗事件或兩者。
    - 若要稽核成功的事件、請選取「成功」方塊。
    - 若要稽核失敗事件、請選取「失敗」方塊。

      只選取您需要監控的動作、以符合安全性需求。如需這些可稽核事件的詳細資訊、請參閱Windows文件。您可以稽核下列事件：

- 完全控制
- 周遊資料夾/執行檔案
- 列出資料夾/讀取資料
- 讀取屬性
- 讀取延伸屬性
- 建立檔案/寫入資料
- 建立資料夾/附加資料
- 寫入屬性
- 寫入延伸屬性
- 刪除子資料夾與檔案
- 刪除
- 讀取權限
- 變更權限
- 取得所有權

11. 如果不希望稽核設定傳播到原始容器的後續檔案和資料夾、請選取「僅將這些稽核項目套用至此容器內的物件和（或）容器*」方塊。
12. 按一下「 * 套用 * 」。
13. 完成新增、移除或編輯稽核項目之後、請按一下*確定*。

    「<object>的稽核項目」方塊隨即關閉。

14. 在「稽核」方塊中、選取此資料夾的繼承設定。

    只選取提供稽核事件的最低層級、以符合您的安全需求。您可以選擇下列其中一項：

    - 選取[包含來自此物件父物件的可繼承稽核項目]方塊。
    - 選取「使用此物件的可繼承稽核項目來取代所有子系上所有現有的可繼承稽核項目」方塊。
    - 選取兩個方塊。
    - 請選取兩個方塊。
      如果您要在單一檔案上設定SACL，則[稽核]方塊中不會出現[以這個物件的可繼承稽核項目取代所有子系上所有現有的可繼承稽核項目]方塊。

15. 按一下「確定」。

    稽核方塊隨即關閉。

使用**ONTAP CLI**設定**NTFS**稽核原則

您可以使用ONTAP CLI在檔案和資料夾上設定稽核原則。這可讓您設定NTFS稽核原則、而不需要使用Windows用戶端上的SMB共用區連線至資料。

您可以使用設定 NTFS 稽核原則 `vserver security file-directory` 命令系列。

您只能使用CLI設定NTFS SACL。此支援的不支援NFSv4 SACL系列。ONTAP深入瞭解如何使用這些命令來設定 NTFS SACL "指令參考資料ONTAP"，並將其新增至中的檔案和資料夾。

設定 **UNIX** 安全性樣式檔案和目錄的 **ONTAP** 稽核

您可以將稽核ACE新增至NFSv4.x ACL、以設定UNIX安全樣式檔案和目錄的稽核。這可讓您監控特定NFS檔案和目錄存取事件、以確保安全。

關於這項工作

對於NFSv4.x、可自由判斷的ACE和系統的ACE都儲存在相同的ACL中。它們不會儲存在個別的DACL和SACL中。因此、在將稽核ACE新增至現有ACL時、您必須謹慎小心、以免覆寫及遺失現有ACL。將稽核ACE新增至現有ACL的順序並不重要。

步驟

1. 使用擷取檔案或目錄的現有 ACL `nfs4_getfacl` 或等效命令。

   如"指令參考資料ONTAP"需有關操作 ACL 的詳細資訊，請參閱。

2. 附加所需的稽核ACE。
3. 使用將更新的 ACL 套用至檔案或目錄 `nfs4_setfacl` 或等效命令。

顯示套用至檔案和目錄的稽核原則相關資訊

存取 **Windows** 安全性索引標籤，即可檢視 **ONTAP** 稽核原則資訊

您可以使用「Windows內容」視窗中的「安全性」索引標籤、顯示已套用至檔案和目錄的稽核原則相關資訊。這種方法與存放在Windows伺服器上的資料相同、可讓客戶使用慣用的GUI介面。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

若要顯示已套用至NTFS檔案和資料夾的SACL相關資訊、請在Windows主機上完成下列步驟。

步驟

1. 從Windows檔案總管的*工具*功能表中、選取*對應網路磁碟機*。
2. 完成*對應網路磁碟機*對話方塊：

   a. 選取*磁碟機*字母。

   b. 在「資料夾」方塊中、輸入儲存虛擬機器（SVM）的IP位址或SMB伺服器名稱、其中包含要稽核的資料及共用名稱。

      如果您的 SMB 伺服器名稱為「 ShMB_Server 」、而您的共用名稱為「 shahre1 」、則您應該輸入 `\\SMB_SERVER\share1`。

      您可以指定 SMB 伺服器的資料介面 IP 位址、而非 SMB 伺服器名稱。

c. 單擊*完成*。

您選取的磁碟機會掛載、並在Windows檔案總管視窗中顯示共用區中包含的檔案和資料夾、做好準備。

3. 選取您要顯示稽核資訊的檔案或目錄。
4. 在檔案或目錄上按一下滑鼠右鍵、然後選取*內容*。
5. 選取*安全性*索引標籤。
6. 按一下*進階*。
7. 選取*稽核*索引標籤。
8. 按一下 * 繼續 * 。

稽核方塊隨即開啟。「稽核項目」方塊會顯示套用SACL的使用者和群組摘要。

9. 在「稽核項目」方塊中、選取您要顯示其SACL項目的使用者或群組。
10. 按一下 * 編輯 * 。

隨即開啟<object>的稽核項目方塊。

11. 在「存取」方塊中、檢視套用至所選物件的目前SACL。
12. 按一下*取消*以關閉*稽核項目*方塊。
13. 單擊*取消*關閉*稽核*方塊。

顯示 **ONTAP FlexVol** 磁碟區上 **NTFS** 稽核原則的相關資訊

您可以在FlexVol 功能區上顯示NTFS稽核原則的相關資訊、包括安全樣式和有效的安全樣式、套用的權限、以及系統存取控制清單的相關資訊。您可以使用這些資訊來驗證安全性組態或疑難排解稽核問題。

關於這項工作

顯示套用至檔案和目錄的稽核原則相關資訊、可讓您驗證是否已在指定的檔案和資料夾上設定適當的系統存取控制清單（SACL）。

您必須提供儲存虛擬機器（SVM）的名稱、以及要顯示其稽核資訊的檔案或資料夾路徑。您可以以摘要形式或詳細清單來顯示輸出。

- NTFS安全型磁碟區和qtree僅使用NTFS系統存取控制清單（SACL）來執行稽核原則。
- 在具有NTFS有效安全性的混合式安全型磁碟區中、檔案和資料夾可以套用NTFS稽核原則。

  混合式安全型磁碟區和qtree可包含使用UNIX檔案權限的部分檔案和目錄、包括模式位元或NFSv4 ACL、以及使用NTFS檔案權限的部分檔案和目錄。

- 混合式安全型磁碟區的最上層可能具有UNIX或NTFS有效安全性、而且可能包含或不包含NTFS SACL。
- 因為即使Volume root或qtree的有效安全樣式為UNIX、也可以在混合式安全型Volume或qtree上設定儲存層級的存取保護安全性、 已設定儲存層級存取保護的Volume或qtree路徑輸出、可能會同時顯示一般檔案和資料夾NFSv4 SACL、以及儲存層級存取保護NTFS SACL。
- 如果在命令中輸入的路徑是使用NTFS有效安全性的資料、則輸出也會顯示動態存取控制ACE的相關資訊（

如果已針對指定的檔案或目錄路徑設定動態存取控制）。

- 在顯示具有NTFS有效安全性的檔案和資料夾的安全性資訊時、UNIX相關的輸出欄位會包含僅供顯示的UNIX檔案權限資訊。

  NTFS安全型檔案和資料夾在決定檔案存取權限時、僅使用NTFS檔案權限、Windows使用者和群組。

- ACL輸出只會針對具有NTFS或NFSv4安全性的檔案和資料夾顯示。

  對於使用UNIX安全性的檔案和資料夾而言、此欄位為空白、只套用模式位元權限（無NFSv4 ACL）。

- ACL輸出中的擁有者和群組輸出欄位僅適用於NTFS安全性描述元。

步驟

1. 以所需的詳細資料層級顯示檔案和目錄稽核原則設定：

如果您想要顯示資訊...	輸入下列命令...
以摘要形式提供	`vserver security file-directory show -vserver vserver_name -path path`
詳細清單	`vserver security file-directory show -vserver vserver_name -path path -expand-mask true`

範例

下列範例顯示路徑的稽核原則資訊 `/corp` 在 SVM VS1 中。路徑具有NTFS有效安全性。NTFS安全性描述元包含成功和成功/失敗SACL項目。

```
cluster::> vserver security file-directory show -vserver vs1 -path /corp
                Vserver: vs1
              File Path: /corp
      File Inode Number: 357
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0x8014
                         Owner:DOMAIN\Administrator
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           ALL-DOMAIN\Administrator-0x100081-OI|CI|SA|FA
                           SUCCESSFUL-DOMAIN\user1-0x100116-OI|CI|SA
                         DACL - ACEs
                           ALLOW-BUILTIN\Administrators-0x1f01ff-OI|CI
                           ALLOW-BUILTIN\Users-0x1f01ff-OI|CI
                           ALLOW-CREATOR OWNER-0x1f01ff-OI|CI
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff-OI|CI
```

下列範例顯示路徑的稽核原則資訊 `/datavol1` 在 SVM VS1 中。路徑包含一般檔案和資料夾SACL、以及儲存層級存取保護SACL。

```
cluster::> vserver security file-directory show -vserver vs1 -path
/datavol1

                Vserver: vs1
              File Path: /datavol1
        File Inode Number: 77
         Security Style: ntfs
        Effective Style: ntfs
         DOS Attributes: 10
 DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
           Unix User Id: 0
          Unix Group Id: 0
         Unix Mode Bits: 777
 Unix Mode Bits in Text: rwxrwxrwx
                   ACLs: NTFS Security Descriptor
                         Control:0xaa14
                         Owner:BUILTIN\Administrators
                         Group:BUILTIN\Administrators
                         SACL - ACEs
                           AUDIT-EXAMPLE\marketing-0xf01ff-OI|CI|FA
                         DACL - ACEs
                           ALLOW-EXAMPLE\Domain Admins-0x1f01ff-OI|CI
                           ALLOW-EXAMPLE\marketing-0x1200a9-OI|CI

                         Storage-Level Access Guard security
                         SACL (Applies to Directories):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Directories):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
                         SACL (Applies to Files):
                           AUDIT-EXAMPLE\Domain Users-0x120089-FA
                           AUDIT-EXAMPLE\engineering-0x1f01ff-SA
                         DACL (Applies to Files):
                           ALLOW-EXAMPLE\Domain Users-0x120089
                           ALLOW-EXAMPLE\engineering-0x1f01ff
                           ALLOW-NT AUTHORITY\SYSTEM-0x1f01ff
```

使用萬用字元顯示 **ONTAP** 檔案安全性和稽核原則的相關資訊

您可以使用萬用字元（*）來顯示特定路徑或根磁碟區下所有檔案和目錄的檔案安全性和稽核原則相關資訊。

萬用字元（*）可做為指定目錄路徑的最後一個子元件、您可以在該子元件下方顯示所有檔案和目錄的資訊。

如果您想要顯示名為「*」的特定檔案或目錄資訊、則必須在雙引號（「」）內提供完整路徑。

範例

下列含有萬用字元的命令會顯示路徑下方所有檔案和目錄的相關資訊 `/1/` SVM VS1 ：

```
cluster::> vserver security file-directory show -vserver vs1 –path /1/*

                    Vserver: vs1
                  File Path: /1/1
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8514
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
                    Vserver: vs1
                  File Path: /1/1/abc
            Security Style: mixed
           Effective Style: ntfs
            DOS Attributes: 10
     DOS Attributes in Text: ----D---
    Expanded Dos Attributes: -
              Unix User Id: 0
             Unix Group Id: 0
            Unix Mode Bits: 777
     Unix Mode Bits in Text: rwxrwxrwx
                       ACLs: NTFS Security Descriptor
                             Control:0x8404
                             Owner:BUILTIN\Administrators
                             Group:BUILTIN\Administrators
                             DACL - ACEs
                             ALLOW-Everyone-0x1f01ff-OI|CI (Inherited)
```

下列命令會顯示路徑下名為「 * 」的檔案資訊 `/vol1/a` SVM VS1 的路徑會以雙引號（""）括住。

```
cluster::> vserver security file-directory show -vserver vs1 -path
"/vol1/a/*"

                Vserver: vs1
              File Path: "/vol1/a/*"
      Security Style: mixed
     Effective Style: unix
      DOS Attributes: 10
  DOS Attributes in Text: ----D---
Expanded Dos Attributes: -
         Unix User Id: 1002
        Unix Group Id: 65533
       Unix Mode Bits: 755
  Unix Mode Bits in Text: rwxr-xr-x
                  ACLs: NFSV4 Security Descriptor
                        Control:0x8014
                        SACL - ACEs
                          AUDIT-EVERYONE@-0x1f01bf-FI|DI|SA|FA
                        DACL - ACEs
                          ALLOW-EVERYONE@-0x1f00a9-FI|DI
                          ALLOW-OWNER@-0x1f01ff-FI|DI
                          ALLOW-GROUP@-0x1200a9-IG
```

可稽核的CLI變更事件

瞭解可稽核的 **ONTAP CLI** 變更事件

可稽核某些CLI變更事件、包括特定SMB共用事件、特定稽核原則事件、特定本機安全性群組事件、本機使用者群組事件、以及授權原則事件。ONTAP瞭解哪些變更事件可稽核、有助於解讀事件記錄的結果。

您可以手動旋轉稽核記錄、啟用或停用稽核、顯示稽核變更事件的相關資訊、修改稽核變更事件、以及刪除稽核變更事件、藉此管理儲存虛擬機器（SVM）稽核CLI變更事件。

身為系統管理員、如果您執行任何命令來變更SMB共用區、本機使用者群組、本機安全性群組、授權原則及稽核原則事件的相關組態、 產生記錄並稽核相應的事件：

稽核類別	活動	事件ID	執行此命令…
主機稽核	原則變更	[4719]稽核組態已變更	`vserver audit disable
enable	modify`	檔案共用	已新增[5142]網路共用

vserver cifs share create	[5143]網路共用區已修改	vserver cifs share modify `vserver cifs share create	modify
delete` `vserver cifs share add	remove`	[5144]網路共用區已刪除	vserver cifs share delete
稽核	使用者帳戶	[4720]本機使用者已建立	vserver cifs users-and-groups local-user create vserver services name-service unix-user create
[4722]本機使用者已啟用	`vserver cifs users-and-groups local-user create	modify`	[4724]本機使用者密碼重設
vserver cifs users-and-groups local-user set-password	[4725]本機使用者已停用	`vserver cifs users-and-groups local-user create	modify`
[4726]本機使用者已刪除	vserver cifs users-and-groups local-user delete vserver services name-service unix-user delete	[4738]本機使用者變更	vserver cifs users-and-groups local-user modify vserver services name-service unix-user modify
[4781]本機使用者重新命名	vserver cifs users-and-groups local-user rename	安全性群組	[4731]已建立本機安全性群組
vserver cifs users-and-groups local-group create vserver services name-service unix-group create	[4734]本機安全性群組已刪除	vserver cifs users-and-groups local-group delete vserver services name-service unix-group delete	[4735]本機安全性群組已修改
`vserver cifs users-and-groups local-group rename	modify` vserver services name-service unix-group modify	[4732]使用者已新增至本機群組	vserver cifs users-and-groups local-group add-members vserver services name-service unix-group adduser

[4733]使用者已從本機群組中移除	`vserver cifs users-and-groups local-group remove-members vserver services name-service unix-group deluser`	授權原則變更	[4704]已指派使用者權限
`vserver cifs users-and-groups privilege add-privilege`	[4705]使用者權限已移除	`vserver cifs users-and-groups privilege remove-privilege`	reset-privilege`

相關資訊

- "Vserver"

管理檔案共用 **ONTAP** 事件

為儲存虛擬機器（SVM）設定檔案共用事件並啟用稽核時、就會產生稽核事件。使用修改 SMB 網路共用時、會產生檔案共用事件 `vserver cifs share` 相關命令。

新增、修改或刪除SVM的SMB網路共用時、會產生事件ID為5142、5143和5144的檔案共用事件。SMB 網路共用組態是使用修改的 `cifs share access control create|modify|delete` 命令。

下列範例顯示建立名為「稽核目的地」的共用物件時、會產生ID為5143的檔案共用事件：

```
netapp-clus1::*> cifs share create -share-name audit_dest -path
/audit_dest
- System
  - Provider
    [ Name]  NetApp-Security-Auditing
    [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 5142
   EventName Share Object Added
   ...
   ...
  ShareName audit_dest
  SharePath /audit_dest
  ShareProperties oplocks;browsable;changenotify;show-previous-versions;
  SD O:BAG:S-1-5-21-2447422786-1297661003-4197201688-513D:(A;;FA;;;WD)
```

管理稽核原則變更 **ONTAP** 事件

當為儲存虛擬機器（SVM）設定稽核原則變更事件並啟用稽核時、就會產生稽核事件。使用修改稽核原則時、會產生稽核原則變更事件 `vserver audit` 相關命令。

每當停用、啟用或修改稽核原則時、就會產生事件ID 4719的稽核原則變更事件、並有助於識別使用者嘗試停用稽核以涵蓋追蹤的時間。此設定預設為設定、需要診斷權限才能停用。

下列範例顯示稽核原則變更事件、並在停用稽核時產生ID 4719：

```
netapp-clus1::*> vserver audit disable -vserver vserver_1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4719
   EventName Audit Disabled
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
```

管理使用者帳戶 **ONTAP** 事件

當儲存虛擬機器（SVM）的使用者帳戶事件設定為啟用稽核時、就會產生稽核事件。

事件ID為4720、4722、4724、4725、4726、 當本機SMB或NFS使用者從系統建立或刪除、本機使用者帳戶啟用、停用或修改、以及本機SMB使用者密碼重設或變更時、就會產生4738和4781。使用修改使用者帳戶時、會產生使用者帳戶事件 `vserver cifs users-and-groups <local user>` 和 `vserver services name-service <unix user>` 命令。

下列範例顯示建立本機SMB使用者時產生ID 4720的使用者帳戶事件：

```
netapp-clus1::*> vserver cifs users-and-groups local-user create -user
-name testuser -is-account-disabled false -vserver vserver_1
Enter the password:
Confirm the password:

- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4720
   EventName Local Cifs User Created
   ...
   ...
  TargetUserName testuser
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1003
  TargetType CIFS
  DisplayName testuser
  PasswordLastSet 1472662216
  AccountExpires NO
  PrimaryGroupId 513
  UserAccountControl %%0200
  SidHistory ~
  PrivilegeList ~
```

下列範例顯示在先前範例中建立的本機SMB使用者重新命名時、產生ID為4781的使用者帳戶事件：

```
 netapp-clus1::*> vserver cifs users-and-groups local-user rename -user
-name testuser -new-user-name testuser1
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4781
   EventName Local Cifs User Renamed
   ...
   ...
  OldTargetUserName testuser
  NewTargetUserName testuser1
  TargetDomainName NETAPP-CLUS1
  TargetSid S-1-5-21-2447422786-1297661003-4197201688-1000
  TargetType CIFS
  SidHistory ~
  PrivilegeList ~
```

管理安全性群組 **ONTAP** 事件

當儲存虛擬機器（SVM）的安全性群組事件設定為啟用稽核時、就會產生稽核事件。

從系統建立或刪除本機SMB或NFS群組、並從群組新增或移除本機使用者時、會產生事件ID為4731、4732、4733、4734和4735的安全性群組事件。當使用修改使用者帳戶時、就會產生安全性群組事件 `vserver cifs users-and-groups <local-group>` 和 `vserver services name-service <unix-group>` 命令。

下列範例顯示建立本機UNIX安全性群組時、產生ID 4731的安全性群組事件：

```
netapp-clus1::*> vserver services name-service unix-group create -name
testunixgroup -id 20
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4731
   EventName Local Unix Security Group Created
   ...
   ...
  SubjectUserName admin
  SubjectUserSid 65533-1001
  SubjectDomainName ~
  SubjectIP console
  SubjectPort
  TargetUserName testunixgroup
  TargetDomainName
  TargetGid 20
  TargetType NFS
  PrivilegeList ~
  GidHistory ~
```

管理授權原則變更 **ONTAP** 事件

當儲存虛擬機器（SVM）的授權原則變更事件設定為啟用稽核時、就會產生稽核事件。

每當SMB使用者和SMB群組的授權權限被授予或撤銷時、就會產生事件ID為4704和4705的授權原則變更事件。當使用指派或撤銷授權權限時、就會產生授權原則變更事件 `vserver cifs users-and-groups privilege` 相關命令。

下列範例顯示指派SMB使用者群組授權權限時、產生ID 4704的授權原則事件：

```
netapp-clus1::*> vserver cifs users-and-groups privilege add-privilege
-user-or-group-name testcifslocalgroup -privileges *
- System
  - Provider
   [ Name]  NetApp-Security-Auditing
   [ Guid]  {3CB2A168-FE19-4A4E-BDAD-DCF422F13473}
   EventID 4704
   EventName User Right Assigned
   ...
   ...
  TargetUserOrGroupName testcifslocalgroup
  TargetUserOrGroupDomainName NETAPP-CLUS1
  TargetUserOrGroupSid S-1-5-21-2447422786-1297661003-4197201688-1004;
  PrivilegeList
SeTcbPrivilege;SeBackupPrivilege;SeRestorePrivilege;SeTakeOwnershipPrivile
ge;SeSecurityPrivilege;SeChangeNotifyPrivilege;
  TargetType CIFS
```

管理稽核組態

手動旋轉稽核事件記錄檔，以檢視特定的 ONTAP SVM 事件記錄

您必須先將記錄轉換成使用者可讀取的格式、才能檢視稽核事件記錄。如果您想要先檢視特定儲存虛擬機器（SVM）的事件記錄、再ONTAP 由SVM自動旋轉記錄、您可以手動旋轉SVM上的稽核事件記錄。

步驟

1. 使用旋轉稽核事件記錄 `vserver audit rotate-log` 命令。

   ```
   vserver audit rotate-log -vserver vs1
   ```

   稽核事件記錄會以稽核組態指定的格式儲存在 SVM 稽核事件記錄目錄中 (`XML` 或 `EVTX`）、並可使用適當的應用程式來檢視。

啟用或停用 ONTAP SVM 上的稽核

您可以在儲存虛擬機器（SVM）上啟用或停用稽核。您可能想要停用稽核功能、暫時停止檔案和目錄稽核。您可以隨時啟用稽核（如果存在稽核組態）。

開始之前

在SVM上啟用稽核之前、SVM的稽核組態必須已經存在。

"建立稽核組態"

關於這項工作

停用稽核不會刪除稽核組態。

步驟

1. 執行適當的命令：

如果您想要稽核...	輸入命令...
已啟用	`vserver audit enable -vserver vserver_name`
已停用	`vserver audit disable -vserver vserver_name`

2. 確認稽核處於所需狀態：

   `vserver audit show -vserver vserver_name`

範例

下列範例可啟用SVM VS1的稽核：

```
cluster1::> vserver audit enable -vserver vs1

cluster1::> vserver audit show -vserver vs1

                               Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
      Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

下列範例停用SVM VS1的稽核：

```
cluster1::> vserver audit disable -vserver vs1

                                Vserver: vs1
                      Auditing state: false
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops, cifs-logon-logoff
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
         Log Rotation Schedule: Day: -
        Log Rotation Schedule: Hour: -
      Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
            Log Files Rotation Limit: 10
```

顯示 **ONTAP** 稽核組態的相關資訊

您可以顯示稽核組態的相關資訊。這些資訊可協助您判斷每個SVM的組態是否符合您的需求。顯示的資訊也可讓您驗證是否已啟用稽核組態。

關於這項工作

您可以在所有SVM上顯示稽核組態的詳細資訊、也可以指定選用參數來自訂輸出中顯示的資訊。如果您未指定任何選用參數、則會顯示下列項目：

- 稽核組態套用至的SVM名稱
- 稽核狀態、可以是 `true` 或 `false`

  如果稽核狀態為 `true`，已啟用稽核。如果稽核狀態為 `false`，稽核已停用。

- 要稽核的事件類別
- 稽核記錄格式
- 稽核子系統儲存合併及轉換稽核記錄的目標目錄

步驟

1. 使用顯示稽核組態的相關資訊 `vserver audit show` 命令。

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

範例

下列範例顯示所有SVM稽核組態的摘要：

```
cluster1::> vserver audit show

 Vserver     State  Event Types Log Format Target Directory
 ----------- ------ ----------- ---------- --------------------
 vs1         false  file-ops    evtx       /audit_log
```

下列範例以清單形式顯示所有SVM的所有稽核組態資訊：

```
cluster1::> vserver audit show -instance

                            Vserver: vs1
                     Auditing state: true
                Log Destination Path: /audit_log
       Categories of Events to Audit: file-ops
                          Log Format: evtx
                 Log File Size Limit: 100MB
        Log Rotation Schedule: Month: -
  Log Rotation Schedule: Day of Week: -
          Log Rotation Schedule: Day: -
         Log Rotation Schedule: Hour: -
       Log Rotation Schedule: Minute: -
                  Rotation Schedules: -
             Log Files Rotation Limit: 0
```

用於修改稽核組態的 **ONTAP** 命令

如果您想要變更稽核設定、可以隨時修改目前的組態、包括修改記錄路徑目的地和記錄格式、修改要稽核的事件類別、如何自動儲存記錄檔、以及指定要儲存的記錄檔數目上限。

如果您想要...	使用此命令...
修改記錄目的地路徑	`vserver audit modify` 使用 `-destination` 參數
修改要稽核的事件類別	`vserver audit modify` 使用 `-events` 參數 若要稽核集中存取原則暫存事件、必須在儲存虛擬機器（SVM）上啟用動態存取控制（DAC）SMB伺服器選項。
修改記錄格式	`vserver audit modify` 使用 `-format` 參數
根據內部記錄檔大小啟用自動儲存	`vserver audit modify` 使用 `-rotate-size` 參數

根據時間間隔啟用自動儲存	`vserver audit modify` 使用 `-rotate-schedule-month`、`-rotate-schedule-dayofweek`、`-rotate-schedule-day`、`-rotate-schedule-hour`和 `-rotate-schedule-minute` 參數
指定儲存的記錄檔數目上限	`vserver audit modify` 使用 `-rotate-limit` 參數

刪除 ONTAP SVM 上的稽核組態

如果您不想再稽核儲存虛擬機器（SVM）上的檔案和目錄事件、也不想在SVM上維護稽核組態、可以刪除稽核組態。

步驟

1. 停用稽核組態：

```
vserver audit disable -vserver vserver_name

vserver audit disable -vserver vs1
```

2. 刪除稽核組態：

```
vserver audit delete -vserver vserver_name

vserver audit delete -vserver vs1
```

瞭解還原稽核 ONTAP 叢集的影響

如果您打算還原叢集、ONTAP 當叢集中有啟用稽核的儲存虛擬機器（SVM）時、您應該注意下列還原程序。您必須先採取特定行動、才能恢復。

還原ONTAP 至不支援SMB登入和登出事件稽核、以及集中存取原則執行事件的版本

支援SMB登入和登出事件的稽核、以及集中存取原則執行事件、從叢集Data ONTAP 式的版本資訊8.3開始。如果您要回復ONTAP 到不支援這些事件類型的版本、而且您有監控這些事件類型的稽核組態、則必須在還原之前變更這些啟用稽核的SVM的稽核組態。您必須修改組態、以便只稽核檔案作業事件。

疑難排解 ONTAP 稽核和暫存磁碟區空間問題

當暫存磁碟區或包含稽核事件記錄的磁碟區空間不足時、可能會發生問題。如果空間不足、就無法建立新的稽核記錄、這會使用戶端無法存取資料、而且存取要求也會失敗。您應該知道如何疑難排解及解決這些磁碟區空間問題。

疑難排解與事件記錄磁碟區相關的空間問題

如果包含事件記錄檔的磁碟區空間不足、稽核將無法將記錄轉換成記錄檔。這會導致用戶端存取失敗。您必須知道如何疑難排解與事件記錄磁碟區相關的空間問題。

- 儲存虛擬機器（ SVM ）和叢集管理員可以顯示有關 Volume 和 Aggregate 使用率和組態的資訊、藉此判斷是否有足夠的磁碟區空間。
- 如果包含事件記錄的磁碟區空間不足、SVM和叢集管理員可以移除部分事件記錄檔、或是增加磁碟區的大小、來解決空間問題。

> ⓘ 如果包含事件記錄磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有叢集管理員可以增加集合體的大小。

- 事件記錄檔的目的地路徑可透過修改稽核組態、變更為另一個磁碟區上的目錄。

> ⓘ 在下列情況下、資料存取遭拒：
>
> ◦ 目的地目錄即會刪除。
>
> ◦ 主控目的地目錄的磁碟區上的檔案限制達到其最大層級。

深入瞭解：

- "如何檢視磁碟區的相關資訊、以及增加磁碟區大小"。
- "如何檢視有關集合體與管理集合體的資訊"。

疑難排解與接移磁碟區相關的空間問題

如果任何包含儲存虛擬機器（SVM）暫存檔案的磁碟區空間不足、稽核將無法將記錄寫入暫存檔案。這會導致用戶端存取失敗。若要疑難排解此問題、您必須顯示磁碟區使用量的相關資訊、以判斷SVM中使用的任何暫存磁碟區是否已滿。

如果包含合併事件記錄檔的磁碟區有足夠空間、但由於空間不足、仍有用戶端存取失敗、則暫存磁碟區可能空間不足。SVM管理員必須聯絡您、以判斷內含SVM暫存檔案的暫存磁碟區是否空間不足。如果因暫存磁碟區空間不足而無法產生稽核事件、則稽核子系統會產生EMS事件。畫面會顯示下列訊息： `No space left on device`。只有您可以檢視暫存磁碟區的相關資訊、SVM管理員無法檢視。

所有暫存磁碟區名稱都以開頭 `MDV_aud_` 接著是包含該暫存磁碟區的集合的 UUID 。以下範例顯示管理SVM上的四個系統磁碟區、這些磁碟區是在為叢集中的資料SVM建立檔案服務稽核組態時自動建立的：

```
cluster1::> volume show -vserver cluster1
Vserver   Volume       Aggregate    State      Type       Size  Available
Used%
--------- ------------ ------------ ---------- ---- ---------- ----------
-----
cluster1  MDV_aud_1d0131843d4811e296fc123478563412
                       aggr0        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_8be27f813d7311e296fc123478563412
                       root_vs0     online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_9dc4ad503d7311e296fc123478563412
                       aggr1        online     RW          5GB     4.75GB
5%
cluster1  MDV_aud_a4b887ac3d7311e296fc123478563412
                       aggr2        online     RW          5GB     4.75GB
5%
4 entries were displayed.
```

如果暫存磁碟區空間不足、您可以增加磁碟區的大小來解決空間問題。

如果包含暫存磁碟區的Aggregate已滿、則必須先增加Aggregate的大小、才能增加磁碟區的大小。只有您可以增加Aggregate的大小、SVM管理員才能增加。

如果一個或多個集合體的可用空間小於 2GB （在 ONTAP 9.14.1 及更早版本中）或 5GB （從 ONTAP 9.15.1 開始）、則 SVM 稽核建立會失敗。當SVM稽核建立失敗時、所建立的暫存磁碟區會被刪除。

在SVM上使用FPolicy進行檔案監控與管理

瞭解 FPolicy

了解ONTAP FPolicy 解決方案

FPolicy 是檔案存取通知架構、可用來透過合作夥伴解決方案監控及管理儲存虛擬機器（ SVM ）上的檔案存取事件。合作夥伴解決方案可協助您處理各種使用案例、例如資料治理與法規遵循、勒索軟體保護及資料移動性。

合作夥伴解決方案包括 NetApp 支援的第三方解決方案，以及 NetApp 產品工作負載安全性和雲端資料感測。

FPolicy解決方案有兩個部分。ONTAP FPolicy 架構可管理叢集上的活動、並傳送通知給合作夥伴應用程式（也稱為外部 FPolicy 伺服器）。外部 FPolicy 伺服器會處理 ONTAP FPolicy 傳送的通知、以履行客戶使用案例。

此解決方案可建立及維護FPolicy組態、監控檔案事件、並將通知傳送至外部FPolicy伺服器。ONTAP支援內部基礎架構、可在外部FPolicy伺服器與儲存虛擬機器（SVM）節點之間進行通訊。ONTAP

FPolicy架構會連線至外部FPolicy伺服器、並在用戶端存取導致這些事件發生時、將特定檔案系統事件的通知傳

送至FPolicy伺服器。外部FPolicy伺服器會處理通知、並將回應傳回節點。通知處理的結果取決於應用程式、以及節點與外部伺服器之間的通訊是否為非同步或同步。

ONTAP FPolicy 同步與非同步通知

FPolicy會透過FPolicy介面將通知傳送至外部FPolicy伺服器。通知會以同步或非同步模式傳送。通知模式會決定ONTAP 將通知傳送至FPolicy伺服器後的功能。

- 非同步通知

  藉由非同步通知、節點不會等待FPolicy伺服器的回應、進而提升系統的整體處理量。這類通知適用於FPolicy伺服器不需要在通知評估後採取任何行動的應用程式。例如、當儲存虛擬機器（SVM）管理員想要監控和稽核檔案存取活動時、就會使用非同步通知。

  如果以非同步模式運作的FPolicy伺服器發生網路中斷、則中斷期間產生的FPolicy通知會儲存在儲存節點上。當FPolicy伺服器重新連線時、系統會警示已儲存的通知、並從儲存節點擷取通知。在停機期間可儲存通知的時間長度可設定為10分鐘。

  從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步（強制或非強制）和非同步強制組態。

- 同步通知

  設定為以同步模式執行時、FPolicy伺服器必須先確認每個通知、才能繼續執行用戶端作業。此類型的通知會在根據通知評估結果需要採取行動時使用。例如、當SVM管理員想要根據外部FPolicy伺服器上指定的條件來允許或拒絕要求時、就會使用同步通知。

同步與非同步應用程式

FPolicy應用程式有許多可能的用途、包括非同步和同步。

非同步應用程式是指外部FPolicy伺服器不會改變存取儲存虛擬機器（SVM）上檔案或目錄或修改資料的方式。例如：

- 檔案存取與稽核記錄
- 儲存資源管理

同步應用程式是指資料存取遭竄改或資料遭外部FPolicy伺服器修改的應用程式。例如：

- 配額管理
- 檔案存取封鎖
- 檔案歸檔與階層式儲存管理
- 加密與解密服務
- 壓縮與解壓縮服務

ONTAP FPolicy 持久存儲

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。從

ONTAP 9.14.1 開始、您可以設定 FPolicy 持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

此功能僅適用於 FPolicy 外部模式。您使用的合作夥伴應用程式需要支援此功能。您應與合作夥伴合作、確保支援此 FPolicy 組態。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store create` 命令可自動建立 SVM 的 Volume 、並使用持續儲存區最佳實務做法來設定 Volume 。

如需持續儲存最佳實務做法的詳細資訊、請參閱 "設定FPolicy的需求、考量及最佳實務做法"。

如需新增持續儲存區的相關資訊、請參閱 "建立持續儲存區"。

ONTAP FPolicy 配置類型

有兩種基本的FPolicy組態類型。其中一個組態使用外部FPolicy伺服器來處理通知並根據通知採取行動。另一個組態不使用外部FPolicy伺服器、而是使用ONTAP 內部的、原生的FPolicy伺服器、根據副檔名來進行簡單的檔案封鎖。

- 外部**FPolicy**伺服器組態

  通知會傳送至FPolicy伺服器、該伺服器會篩選要求並套用規則、以判斷節點是否應允許要求的檔案操作。對於同步原則、FPolicy伺服器接著會傳送回應給節點、以允許或封鎖要求的檔案作業。

- 原生**FPolicy**伺服器組態

  通知會在內部篩選。根據在FPolicy範圍中設定的副檔名設定、允許或拒絕要求。

  附註：不記錄被拒絕的副檔名要求。

何時建立原生**FPolicy**組態

原生FPolicy組態使用ONTAP 內部的FPolicy引擎、根據檔案副檔名來監控及封鎖檔案作業。此解決方案不需要外部FPolicy伺服器（FPolicy伺服器）。當這個簡單的解決方案只是需要的時候、使用原生檔案封鎖組態是適當的做法。

原生檔案封鎖功能可讓您監控符合設定作業和篩選事件的任何檔案作業、然後拒絕存取具有特定副檔名的檔案。這是預設組態。

此組態可讓您僅根據檔案副檔名來封鎖檔案存取。例如、封鎖包含的檔案 `mp3` 副檔名時、您可以設定原則、為目標副檔名為的特定作業提供通知 `mp3`。原則設定為拒絕 `mp3` 產生通知之作業的檔案要求。

下列項目適用於原生FPolicy組態：

- FPolicy伺服器型檔案篩選所支援的相同篩選器和傳輸協定集、也支援原生檔案封鎖。
- 您可以同時設定原生檔案封鎖和FPolicy伺服器型檔案篩選應用程式。

  若要這麼做、您可以針對儲存虛擬機器（SVM）設定兩個獨立的FPolicy原則、其中一個設定為原生檔案封鎖、另一個設定為FPolicy伺服器型檔案篩選。

- 原生檔案封鎖功能只會根據副檔名而非檔案內容來篩選檔案。

- 在符號連結的情況下、原生檔案封鎖會使用根檔案的副檔名。

深入瞭解 "FPolicy：原生檔案封鎖"。

何時建立使用外部**FPolicy**伺服器的組態

使用外部FPolicy伺服器來處理及管理通知的FPolicy組態、可針對需要根據副檔名進行簡單檔案封鎖的使用案例、提供健全的解決方案。

當您想要執行監控及記錄檔案存取事件、提供配額服務、根據簡單副檔名以外的條件執行檔案封鎖、使用階層式儲存管理應用程式提供資料移轉服務等作業時、應建立使用外部FPolicy伺服器的組態、 或是提供一組精細的原則、僅監控儲存虛擬機器（SVM）中的資料子集。

ONTAP FPolicy 實作中的叢集元件角色

叢集、內含的儲存虛擬機器（SVM）和資料生命量、都在FPolicy實作中扮演著重要角色。

- 叢集

  叢集包含FPolicy管理架構、並維護及管理叢集中所有FPolicy組態的相關資訊。

- * SVM*

  FPolicy組態是在SVM層級定義。組態的範圍是SVM、它只能在SVM資源上運作。某個SVM組態無法監控及傳送針對位於另一個SVM上的資料所提出的檔案存取要求通知。

  可在管理SVM上定義FPolicy組態。在管理SVM上定義組態之後、即可在所有SVM中看到及使用這些組態。

- 資料生命量

  連接至FPolicy伺服器的方式是透過屬於SVM的資料LIF與FPolicy組態。這些連線所使用的資料生命量、可能會像一般用戶端存取所使用的資料生命量一樣進行容錯移轉。

ONTAP FPolicy 如何與外部 **FPolicy** 伺服器搭配使用

在儲存虛擬機器（SVM）上設定並啟用FPolicy之後、FPolicy會在SVM所參與的每個節點上執行。FPolicy負責建立及維護與外部FPolicy伺服器（FPolicy伺服器）的連線、通知處理、以及管理與FPolicy伺服器之間的通知訊息。

此外、在連線管理中、FPolicy有下列責任：

- 確保檔案通知會透過正確的LIF傳送到FPolicy伺服器。
- 確保當多個FPolicy伺服器與某個原則相關聯時、會在傳送通知給FPolicy伺服器時完成負載平衡。
- 當與FPolicy伺服器的連線中斷時、嘗試重新建立連線。
- 透過驗證的工作階段將通知傳送至FPolicy伺服器。
- 管理FPolicy伺服器所建立的Passthrough-read資料連線、以便在啟用passe-read時、為用戶端要求提供服務。

控制通道如何用於**FPolicy**通訊

FPolicy會從儲存虛擬機器（SVM）上每個節點的資料生命期、啟動與外部FPolicy伺服器的控制通道連線。FPolicy使用控制通道來傳輸檔案通知、因此FPolicy伺服器可能會根據SVM拓撲看到多個控制通道連線。

特殊權限資料存取通道如何用於同步通訊

在同步使用案例中、FPolicy伺服器會透過特殊權限的資料存取路徑、存取儲存虛擬機器（SVM）上的資料。透過權限路徑存取時、會將完整的檔案系統公開給FPolicy伺服器。它可以存取資料檔案來收集資訊、掃描檔案、讀取檔案或寫入檔案。

由於外部FPolicy伺服器可透過特殊權限的資料通道、從SVM的根目錄存取整個檔案系統、因此具有特殊權限的資料通道連線必須安全無虞。

如何將**FPolicy**連線認證用於特殊權限的資料存取通道

FPolicy伺服器會使用與FPolicy組態一起儲存的特定Windows使用者認證、建立與叢集節點的授權資料存取連線。SMB是唯一支援的傳輸協定、可用來建立特殊權限資料存取通道連線。

如果FPolicy伺服器需要存取授權資料、則必須符合下列條件：

- 必須在叢集上啟用SMB授權。
- FPolicy伺服器必須在FPolicy組態中設定的認證下執行。

建立資料通道連線時、FPolicy會使用指定Windows使用者名稱的認證資料。資料存取是透過管理共用ONTAP_admin$進行。

授與超級使用者認證以進行授權資料存取的意義

使用FPolicy組態中設定的IP位址和使用者認證組合、將超級使用者認證授予FPolicy伺服器。ONTAP

當FPolicy伺服器存取資料時、超級使用者狀態會授予下列權限：

- 避免進行權限檢查

  使用者無需檢查檔案和目錄存取。

- 特殊鎖定權限

  支援讀取、寫入或修改任何檔案的存取權限、無論現有的鎖定為何。ONTAP如果FPolicy伺服器對檔案進行位元組範圍鎖定、則會立即移除檔案上現有的鎖定。

- 略過任何FPolicy檢查

  存取不會產生任何FPolicy通知。

FPolicy如何管理原則處理

可能有多個FPolicy原則指派給您的儲存虛擬機器（SVM）、每個原則的優先順序各不相同。若要在SVM上建立適當的FPolicy組態、請務必瞭解FPolicy如何管理原則處理。

每個檔案存取要求都會經過初始評估、以判斷哪些原則正在監控此事件。如果是受監控的事件、則監控事件的相

關資訊以及相關的原則都會傳送到FPolicy、並在FPolicy中進行評估。每個原則都會依照指派的優先順序進行評估。

在設定原則時、您應考慮下列建議：

- 當您想要在其他原則之前一律先評估原則時、請以較高的優先順序設定該原則。
- 如果所要求的檔案存取作業在受監控事件上成功、是根據其他原則評估檔案要求的先決條件、請將控制第一個檔案作業成功或失敗的原則設定為較高的優先順序。

  例如、如果一個原則管理FPolicy檔案歸檔與還原功能、而另一個原則管理線上檔案的檔案存取作業、 管理檔案還原的原則必須具有較高的優先順序、才能在第二個原則所管理的作業之前還原檔案。

- 如果您想要評估所有可能套用至檔案存取作業的原則、請將同步原則的優先順序降低。

您可以修改原則順序編號、重新排列現有原則的原則優先順序。不過、若要讓FPolicy根據修改後的優先順序來評估原則、您必須停用並重新啟用具有修改順序編號的原則。

節點到外部 **ONTAP FPolicy** 伺服器通訊過程

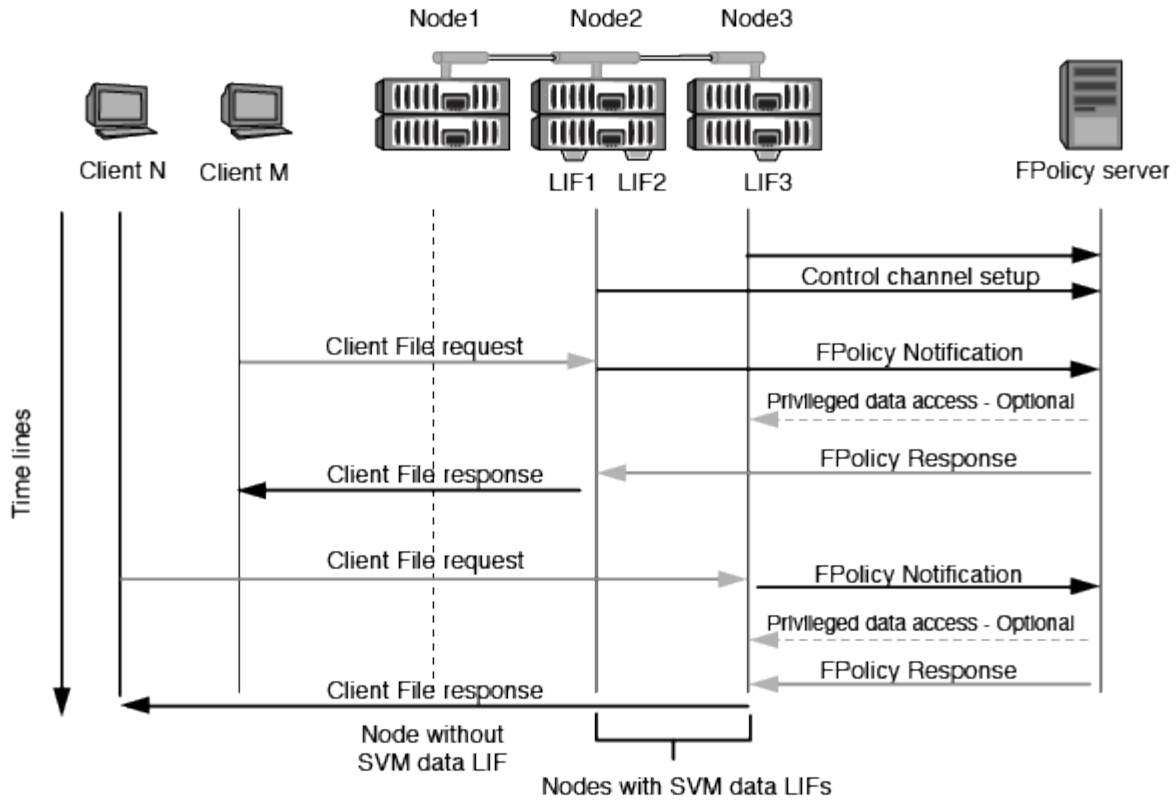
若要正確規劃FPolicy組態、您應該瞭解節點對外部FPolicy伺服器的通訊程序為何。

每個參與每個儲存虛擬機器（SVM）的節點、都會使用TCP/IP來啟動與外部FPolicy伺服器（FPolicy伺服器）的連線。與FPolicy伺服器的連線是使用節點資料LIF設定、因此只有當節點具有SVM的作業資料LIF時、參與的節點才能設定連線。

啟用原則時、參與節點上的每個FPolicy程序都會嘗試建立與FPolicy伺服器的連線。它使用原則組態中指定的FPolicy外部引擎IP位址和連接埠。

此連線會透過資料LIF、從每個SVM上的每個節點建立一個控制通道、以連接至FPolicy伺服器。此外、如果同一個參與節點上有IPV4和IPV6資料LIF位址、FPolicy會嘗試建立連線、以便同時連線至IPV4和IPV6。因此、在SVM延伸到多個節點上的案例中、或是同時存在IPV4和IPV6位址時、FPolicy伺服器必須在SVM上啟用FPolicy原則之後、為叢集的多個控制通道設定要求做好準備。

例如、如果叢集有三個節點（節點1、節點2和節點3）、而SVM資料LIF僅散佈於節點2和節點3、則控制通道只會從節點2和節點3啟動、無論資料磁碟區的分佈為何。說明Node2有兩個屬於SVM的資料生命期、分別是LIF1和LIF2、而且初始連線來自於LIF1。如果LIF1失敗、FPolicy會嘗試從LIF2建立控制通道。



FPolicy如何在**LIF**移轉或容錯移轉期間管理外部通訊

資料生命期可移轉至同一個節點的資料連接埠、或移轉至遠端節點的資料連接埠。

當資料LIF容錯移轉或移轉時、會建立新的控制通道連線至FPolicy伺服器。然後FPolicy可以重試逾時的SMB和NFS用戶端要求、並將新通知傳送至外部FPolicy伺服器。節點會拒絕FPolicy伺服器對原始、逾時SMB和NFS要求的回應。

FPolicy如何在節點容錯移轉期間管理外部通訊

如果裝載用於FPolicy通訊之資料連接埠的叢集節點故障、ONTAP 則無法中斷FPolicy伺服器與節點之間的連線。

透過設定容錯移轉原則、將 FPolicy 通訊中使用的資料連接埠移轉至另一個作用中節點、可減輕叢集容錯移轉至 FPolicy 伺服器的影響。移轉完成後、會使用新的資料連接埠建立新的連線。

如果未將容錯移轉原則設定為移轉資料連接埠、 FPolicy 伺服器必須等待故障節點啟動。節點啟動後、會使用新的工作階段ID從該節點啟動新的連線。

FPolicy伺服器會使用「保持作用中」傳輸協定訊息來偵測中斷的連線。清除工作階段ID的逾時是在設定FPolicy時決定。預設的「保持作用中」逾時為兩分鐘。

了解跨 **SVM** 命名空間的 **ONTAP FPolicy** 服務

提供統一化儲存虛擬機器（SVM）命名空間。ONTAP叢集內的磁碟區會透過連接點連接在一起、以提供單一的邏輯檔案系統。FPolicy伺服器知道命名空間拓撲、並在命名空間中提供FPolicy服務。

命名空間是特定於SVM並包含在SVM中、因此您只能從SVM內容中查看命名空間。命名空間具有下列特性：

- 每個SVM中都有一個命名空間、命名空間的根目錄為根磁碟區、在命名空間中以斜槓（/）表示。
- 所有其他磁碟區的交會點均低於根（/）。
- Volume交會對用戶端而言是透明的。
- 單一NFS匯出可提供完整命名空間的存取權、否則匯出原則可匯出特定磁碟區。
- SMB共用可在磁碟區或磁碟區內的qtree上建立、或是在命名空間內的任何目錄上建立。
- 命名空間架構具有彈性。

  典型命名空間架構的範例如下：

  - 具有根目錄外單一分支的命名空間
  - 具有多個根目錄分支的命名空間
  - 一個命名空間、其根部有多個未分支的磁碟區

ONTAP FPolicy 直通讀取如何增強分層儲存管理的可用性

Passthsthro-read可讓FPolicy伺服器（做為階層式儲存管理（HSM）伺服器）提供離線檔案的讀取存取權限、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。

當FPolicy伺服器設定為提供HSM給SMB伺服器上的檔案時、會發生原則型檔案移轉、檔案會離線儲存在次要儲存設備上、而且只有存根檔案保留在主要儲存設備上。雖然存根檔案對用戶端而言是正常檔案、但實際上是與原始檔案大小相同的稀疏檔案。該檔案設有SMB離線位元、並指向已移轉至次要儲存設備的實際檔案。

一般而言、當收到離線檔案的讀取要求時、必須將要求的內容重新叫用回主要儲存設備、然後再透過主要儲存設備存取。需要將資料重新叫用回主儲存設備、會產生幾種不良影響。其中不良的影響包括：回應要求前必須回收內容、導致用戶端要求延遲增加、以及主儲存設備上已回收檔案所需的空間使用量增加。

FPolicy Passthrough-read可讓HSM伺服器（FPolicy伺服器）提供移轉離線檔案的讀取存取權、而不需要從次要儲存系統將檔案重新叫用至主要儲存系統。讀取要求可直接從次要儲存設備處理、而非將檔案重新叫用回主要儲存設備。

FPolicy pass-read作業不支援複本卸載（ODX）。

Passthsther-read提供下列優點、可增強使用性：

- 即使主儲存設備沒有足夠空間可將要求的資料回收回主儲存設備、仍可處理讀取要求。
- 當發生大量的資料回收時（例如指令碼或備份解決方案需要存取許多離線檔案）、容量和效能管理會更好。
- 您可以處理快照中離線檔案的讀取要求。

  由於快照是唯讀的，因此如果存根檔案位於快照中， FPolicy 伺服器就無法還原原始檔案。使用Passthrough-read可消除此問題。

- 您可以設定原則、以控制何時透過存取次要儲存設備上的檔案來處理讀取要求、以及何時應將離線檔案重新叫用至主要儲存設備。

  例如、您可以在HSM伺服器上建立原則、指定在檔案移轉回主要儲存設備之前、於指定時間段內存取離線檔

案的次數。這類原則可避免重呼很少存取的檔案。

啟用**FPolicy Passthrough-read**時、如何管理讀取要求

您應該瞭解啟用FPolicy pass-read時如何管理讀取要求、以便最佳設定儲存虛擬機器（SVM）與FPolicy伺服器之間的連線。

啟用FPolicy Passthrough-read且SVM收到離線檔案的要求時、FPolicy會透過標準連線通道傳送通知給FPolicy伺服器（HSM伺服器）。

收到通知後、FPolicy伺服器會從通知中傳送的檔案路徑讀取資料、並透過SVM與FPolicy伺服器之間建立的Passthrough-read權限資料連線、將要求的資料傳送至SVM。

傳送資料後、FPolicy伺服器會以允許或拒絕的形式回應讀取要求。根據讀取要求是允許還是拒絕、ONTAP 所以無法傳送要求的資訊或傳送錯誤訊息給用戶端。

規劃**FPolicy**組態

配置 **ONTAP FPolicy** 的要求、注意事項和最佳實踐

在儲存虛擬機器（SVM）上建立及設定FPolicy組態之前、您必須瞭解設定FPolicy的特定需求、考量事項及最佳實務做法。

FPolicy 功能可透過命令列介面（ CLI ）或 REST API 進行設定。

設定**FPolicy**的需求

在儲存虛擬機器（SVM）上設定及啟用FPolicy之前、您必須先瞭解特定需求。

- 叢集中的所有節點都必須執行ONTAP 支援FPolicy的版本的功能。
- 如果您不使用ONTAP 本機的FPolicy引擎、則必須安裝外部FPolicy伺服器（FPolicy伺服器）。
- FPolicy伺服器必須安裝在可從啟用FPolicy原則的SVM資料生命區存取的伺服器上。

> 從 ONTAP 9 8 開始、 ONTAP 提供用戶端 LIF 服務 `data-fpolicy-client`、用於外傳 FPolicy 連線、並新增服務。"深入瞭解生命與服務原則"。

- FPolicy伺服器的IP位址必須在FPolicy原則外部引擎組態中設定為主要或次要伺服器。
- 如果FPolicy伺服器透過特殊權限的資料通道存取資料、則必須滿足下列額外需求：
  - SMB必須在叢集上獲得授權。

    特殊權限資料存取是使用SMB連線來完成。
  - 必須設定使用者認證、才能透過權限資料通道存取檔案。
  - FPolicy伺服器必須在FPolicy組態中設定的認證下執行。
  - 用於與 FPolicy 伺服器通訊的所有資料生命都必須設定為具有 `cifs` 作為其中一種允許的通訊協定。

    這包括用於傳遞讀取連線的lifs。

在儲存虛擬機器（ SVM ）上設定 FPolicy 時、請熟悉一般組態最佳實務做法和建議、以確保 FPolicy 組態能提供強大的監控效能和符合您需求的結果。

如需效能、規模調整及組態的特定準則、請與 FPolicy 合作夥伴應用程式合作。

持續儲存區

從 ONTAP 9.14.1 開始、 FPolicy 可讓您設定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。不支援同步（強制或非強制）和非同步強制組態。

- 在使用持續儲存功能之前、請確保您的合作夥伴應用程式支援此組態。
- 每個啟用 FPolicy 的 SVM 都需要一個持續儲存區。
  - 每個 SVM 只能設定一個持續儲存區。此單一持續儲存區必須用於該 SVM 上的所有 FPolicy 組態、即使這些原則來自不同的合作夥伴。
- ONTAP 9.15.1 或更新版本：
  - 當您建立持續儲存區時、會自動處理持續儲存區、其磁碟區及其磁碟區組態。
- ONTAP 9.14.1 ：
  - 持續儲存區、其磁碟區及其磁碟區組態是手動處理的。
- 在節點上建立持續儲存區磁碟區、其中包含預期由 FPolicy 監控的最大流量。
  - ONTAP 9.15.1 或更新版本：磁碟區會在持續儲存區建立期間自動建立及設定。
  - ONTAP 9.14.1 ：叢集管理員必須在啟用 FPolicy 的每個 SVM 上建立及設定持續儲存區的磁碟區。
- 如果持續儲存區中累積的通知超過已配置的磁碟區大小、 FPolicy 就會開始以適當的 EMS 訊息來丟棄傳入通知。
  - ONTAP 9.15.1 或更新版本：除了 `size` 參數 `autosize-mode` 參數可協助磁碟區隨使用空間量而增加或縮小。
  - ONTAP 9.14.1 `size` 在磁碟區建立期間設定參數、以提供最大限制。
- 將 Snapshot 原則設為 `none` 用於永久儲存區 Volume 、而非 `default`。這是為了確保不會意外還原快照而導致目前事件遺失、並防止可能的重複事件處理。
  - ONTAP 9.15.1 或更新版本 `snapshot-policy` 在持續儲存區建立期間、參數會自動設定為無。
  - ONTAP 9.14.1 `snapshot-policy` 參數設定為 `none` 在磁碟區建立期間。
- 讓外部使用者傳輸協定存取（ CIFS/NFS ）無法存取持續儲存區磁碟區、以避免意外毀損或刪除持續存在的事件記錄。
  - ONTAP 9.15.1 或更新版本： ONTAP 會在持續儲存區建立期間、自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。
  - ONTAP 9.14.1 ：啟用 FPolicy 之後、請在 ONTAP 中卸載 Volume 以移除連接路徑。這使得外部使用者傳輸協定存取（ CIFS/NFS ）無法存取。

如需詳細資訊、請參閱 "FPolicy 永續性儲存區" 和 "建立持續儲存區"。

持續儲存區容錯移轉和恢復

持續儲存區會維持上次收到事件、發生非預期的重新開機、或是停用 FPolicy 並再次啟用時的狀態。在接管作業之後、新事件會由合作夥伴節點儲存和處理。恢復作業完成後、持續儲存區會繼續處理任何未處理的事件、這些事件可能會在節點接管發生時保留。即時事件將優先於未處理的事件。

如果持久性儲存磁碟區從同一 SVM 中的一個節點移至另一個節點，則尚未處理的通知也會移至新節點。您需要重新運行 `fpolicy persistent-store create`移動磁碟區後，在任一節點上執行指令，以確保待處理的通知傳遞到外部伺服器。

詳細了解 `fpolicy persistent-store create`在"指令參考資料ONTAP" 。

原則組態

設定 FPolicy 外部引擎、事件和 SVM 範圍、可改善您的整體體驗和安全性。

- 設定 SVM 的 FPolicy 外部引擎：
  - 提供額外的安全性需要付出效能成本。啟用安全通訊端層（ SSL ）通訊對存取共用具有效能影響。
  - FPolicy 外部引擎應設定多個 FPolicy 伺服器、以提供 FPolicy 伺服器通知處理的恢復能力和高可用度。
- 設定 SVM 的 FPolicy 事件：

  監控檔案作業會影響您的整體體驗。例如、在儲存端篩選不想要的檔案作業、可改善您的使用體驗。NetApp 建議設定下列組態：

  - 監控檔案作業的最小類型、並在不中斷使用案例的情況下啟用最大篩選器數量。
  - 使用篩選器執行 getattr 、讀取、寫入、開啟及關閉作業。SMB 和 NFS 主目錄環境在這些作業中所佔的比例很高。
- SVM 的 FPolicy 範圍組態：

  將原則的範圍限制在相關的儲存物件上、例如共用、磁碟區和匯出、而非在整個 SVM 中啟用這些物件。NetApp 建議您檢查目錄副檔名。如果是 `is-file-extension-check-on-directories-enabled` 參數設定為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。

網路組態

FPolicy 伺服器與控制器之間的網路連線應為低延遲。NetApp 建議使用私有網路來分隔 FPolicy 流量與用戶端流量。

此外、您應該將外部 FPolicy 伺服器（ FPolicy 伺服器）放置在離具有高頻寬連線能力的叢集近的位置、以提供最小的延遲和高頻寬連線能力。

> 如果將 FPolicy 流量的 LIF 設定在與 LIF 不同的連接埠上、以進行用戶端流量、則 FPolicy LIF 可能會因為連接埠故障而容錯移轉至其他節點。因此、 FPolicy 伺服器無法從節點連線、導致 FPolicy 通知節點上的檔案作業失敗。若要避免此問題、請確認可透過節點上至少一個 LIF 來連線 FPolicy 伺服器、以處理在該節點上執行檔案作業的 FPolicy 要求。

硬體組態

您可以在實體伺服器或虛擬伺服器上使用 FPolicy 伺服器。如果 FPolicy 伺服器位於虛擬環境中、您應該將專用

資源（ CPU 、網路和記憶體）分配給虛擬伺服器。

叢集節點對FPolicy伺服器比率應最佳化、以確保FPolicy伺服器不會過載、這可能會在SVM回應用戶端要求時產生延遲。最佳比率取決於使用 FPolicy 伺服器的合作夥伴應用程式。NetApp 建議與合作夥伴合作、以確定適當的價值。

多原則組態

無論序號為何、原生封鎖的 FPolicy 原則都具有最高優先順序、而變更決策原則的優先順序比其他原則高。原則優先順序取決於使用案例。NetApp 建議與合作夥伴合作、以決定適當的優先順序。

規模考量

FPolicy 會執行 SMB 和 NFS 作業的即時監控、傳送通知給外部伺服器、並根據外部引擎通訊模式（同步或非同步）等待回應。此程序會影響 SMB 和 NFS 存取和 CPU 資源的效能。

為了減輕任何問題、 NetApp 建議您在啟用 FPolicy 之前、先與合作夥伴合作、評估環境並調整其規模。效能受到多種因素影響、包括使用者數量、工作負載特性、例如每位使用者的作業次數和資料大小、網路延遲、故障或伺服器速度緩慢。

監控效能

FPolicy 是以通知為基礎的系統。通知會傳送至外部伺服器以進行處理、並產生回覆 ONTAP 的回應。此往返程序會增加用戶端存取的延遲。

監控 FPolicy 伺服器和 ONTAP 中的效能計數器、可讓您識別解決方案中的瓶頸、並視需要調整參數、以獲得最佳解決方案。例如、 FPolicy 延遲增加會對 SMB 和 NFS 存取延遲造成串聯影響。因此、您應該同時監控工作負載（ SMB 和 NFS ）和 FPolicy 延遲。此外、您可以在 ONTAP 中使用服務品質原則、為每個啟用 FPolicy 的 Volume 或 SVM 設定工作負載。

NetApp 建議您執行 `statistics show -object workload` 顯示工作負載統計資料的命令。此外、您應該監控下列參數：

- 平均、讀取和寫入延遲
- 作業總數
- 讀寫計數器

您可以使用下列 FPolicy 計數器來監控 FPolicy 子系統的效能。

您必須處於診斷模式、才能收集與 FPolicy 相關的統計資料。

步驟

1. 收集 FPolicy 計數器：
   a. `statistics start -object fpolicy -instance <instance_name> -sample-id <ID>`
   b. `statistics start -object fpolicy_policy -instance <instance_name> -sample-id <ID>`
2. 顯示 FPolicy 計數器：
   a. `statistics show -object fpolicy -instance <instance_name> -sample-id <ID>`

b. `statistics show -object fpolicy_server -instance <instance_name> -sample-id <ID>`

   ◦ `fpolicy` 和 `fpolicy_server` Counters 提供下表所述數種效能參數的相關資訊。

計數器	說明
*fpolicy 計數器 *	aborted_requests
在 SVM 上中止處理的畫面要求數	event_count
導致通知的事件清單	max_requent_l滯
最大螢幕要求延遲時間	未處理的要求
處理中的畫面要求總數	Processed_requests
在 SVM 上執行 fpolicy 處理的畫面要求總數	requy_histure_hist
畫面要求延遲長條圖	Requests_Dispatched_Rate
每秒發出的畫面要求數	Requests_receiped_rate
每秒接收的畫面要求數	*fpolicy_server counters *
max_requent_l滯	畫面要求的最大延遲
未處理的要求	等待回應的畫面要求總數
requy_l滯	畫面要求的平均延遲
requy_histure_hist	畫面要求延遲長條圖
requy_sent_rate	每秒傳送至 FPolicy 伺服器的畫面要求數
RESPONY_REATE_RATE	每秒從 FPolicy 伺服器收到的畫面回應數

深入瞭解 `statistics start`及 `statistics show` "指令參考資料ONTAP"。

管理 **FPolicy** 工作流程、並仰賴其他技術

NetApp 建議您先停用 FPolicy 原則、再進行任何組態變更。例如、如果您想要新增或修改為啟用原則設定的外部引擎中的 IP 位址、請先停用原則。

如果您將 FPolicy 設定為監控 NetApp FlexCache 磁碟區、 NetApp 建議您不要設定 FPolicy 來監控讀取和 getattr 檔案作業。在 ONTAP 中監控這些作業需要擷取 inode 到路徑（ I2P ）資料。由於 I2P 資料無法從 FlexCache 磁碟區擷取、因此必須從原始磁碟區擷取。因此、監控這些作業可免除 FlexCache 所能提供的效能效益。

當同時部署 FPolicy 和隨裝即用的防毒解決方案時、防毒解決方案會先收到通知。FPolicy 處理只會在防毒掃描完成後才會開始。請務必正確設定防毒解決方案的大小、因為慢速防毒掃描程式可能會影響整體效能。

Passthsther-read升級與還原考量

在升級ONTAP 至支援Passthrough-read的版本之前、或在回復至不支援passe-read的版本之前、您必須瞭解某些升級與還原考量事項。

升級

將所有節點升級至ONTAP 支援FPolicy Passthrough-read的版本後、叢集就能使用Passthrough-read功能；不過、在現有的FPolicy組態上、依預設會停用pass-read。若要在現有的FPolicy組態上使用passThrough讀取、您必須停用FPolicy原則並修改組態、然後重新啟用組態。

還原

還原至不支援 FPolicy Passthrough-read 的 ONTAP 版本之前、您必須符合下列條件：

- 使用 Passthrough-read 停用所有原則、然後修改受影響的組態、使其不使用 passthrough Read 。
- 停用叢集上的每個 FPolicy 原則、以停用叢集上的 FPolicy 功能。

在還原至不支援持續儲存區的 ONTAP 版本之前、請確定 FPolicy 原則中沒有任何一個具有設定的持續儲存區。如果設定持續儲存區、還原將會失敗。

相關資訊

- "統計數據顯示"
- "統計開始"

設定 **ONTAP FPolicy** 配置

在FPolicy能夠監控檔案存取之前、必須先在需要FPolicy服務的儲存虛擬機器（SVM）上建立並啟用FPolicy組態。

在SVM上設定及啟用FPolicy組態的步驟如下：

1. 建立FPolicy外部引擎。

   FPolicy外部引擎可識別與特定FPolicy組態相關聯的外部FPolicy伺服器（FPolicy伺服器）。如果使用內部的「原生」FPolicy引擎來建立原生檔案封鎖組態、則不需要建立FPolicy外部引擎。

   從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。如需詳細資訊、請參閱 "規劃FPolicy外部引擎組態"

2. 建立FPolicy事件。

   FPolicy事件說明FPolicy原則應監控的項目。事件包括要監控的傳輸協定和檔案作業、並可包含篩選器清單。事件使用篩選器來縮小FPolicy外部引擎必須傳送通知的受監控事件清單。事件也會指定原則是否監控Volume作業。

3. 建立 FPolicy 持續儲存區（選用）。

   從 ONTAP 9.14.1 開始、 FPolicy 可讓您進行設定 "持續儲存區" 擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store-create` 命令可自動建立 SVM 的 Volume 、並設定持續儲存區的 Volume 。

4. 建立FPolicy原則。

   FPolicy原則負責將需要監控的一組事件與適當範圍相關聯、以及哪些受監控的事件通知必須傳送至指定的FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。該原則也定義是否允許FPolicy伺服器以權限存取其接收通知的資料。如果伺服器需要存取資料、FPolicy伺服器就需要存取權限。需要存取權限的典型使用案例包括檔案封鎖、配額管理及階層式儲存管理。您可以在原則中指定此原則的組態是使用FPolicy伺服器、還是使用內部的「原生」FPolicy伺服器。

   原則會指定是否必須篩選。如果篩選是強制性的、且所有FPolicy伺服器都關閉、或在定義的逾時期間內、未從FPolicy伺服器收到任何回應、則檔案存取將遭拒。

   原則的界限是SVM。原則無法套用至多個SVM。不過、特定SVM可以有多個FPolicy原則、每個原則的範圍、事件和外部伺服器組態組合相同或不同。

5. 設定原則範圍。

   FPolicy範圍決定原則在哪些磁碟區、共享區或匯出原則上執行、或排除在監控範圍之外。範圍也會決定哪些副檔名應納入或排除在FPolicy監控範圍之外。

   排除清單優先於包含清單。

6. 啟用FPolicy原則。

   啟用原則時、會連接控制通道和（可選）特殊權限資料通道。SVM參與之節點上的FPolicy程序會開始監控檔案和資料夾存取、若事件符合設定的條件、則會將通知傳送至FPolicy伺服器（若未設定FPolicy伺服器、則會傳送至原生引擎）。

如果原則使用原生檔案封鎖、則不會設定外部引擎、也不會與原則建立關聯。

規劃**FPolicy**外部引擎組態

規劃 **ONTAP FPolicy** 外部引擎配置

設定 FPolicy 外部引擎之前、您必須先瞭解建立外部引擎的意義、以及哪些組態參數可供使用。此資訊可協助您判斷要為每個參數設定哪些值。

建立**FPolicy**外部引擎時所定義的資訊

外部引擎組態定義 FPolicy 需要建立及管理外部 FPolicy 伺服器連線的資訊、包括：

- SVM名稱
- 引擎名稱
- 主要和次要FPolicy伺服器的IP位址、以及連接至FPolicy伺服器時要使用的TCP連接埠號碼
- 引擎類型為非同步或同步

- 引擎格式是否為 `xml` 或 `protobuf`

  從 ONTAP 9.15.1 開始、您可以使用 `protobuf` 引擎格式。設定為時 `protobuf`、通知訊息會使用Google Prototbuf以二進位格式編碼。將引擎格式設定為之前 `protobuf`，請確保 FPolicy 伺服器也支援 `protobuf` 反序列化。

  由於支援的 probuf 格式從 ONTAP 9.15.1 開始、因此您必須先考慮外部引擎格式、才能還原至舊版 ONTAP 。如果您恢復為 ONTAP 9.15.1 之前的版本、請與 FPolicy 合作夥伴合作、以：

  - 從變更每個引擎格式 `protobuf` 至 `xml`
  - 刪除引擎格式為的引擎 `protobuf`

- 如何驗證節點與FPolicy伺服器之間的連線

  如果您選擇設定相互SSL驗證、則也必須設定提供SSL憑證資訊的參數。

- 如何使用各種進階權限設定來管理連線

  這包括定義逾時值、重試值、保持活動值、最大要求值、傳送和接收緩衝區大小值、以及工作階段逾時值等項目的參數。

。 `vserver fpolicy policy external-engine create` 命令用於建立 FPolicy 外部引擎。

基本的外部引擎參數是什麼

您可以使用下表的基本FPolicy組態參數來協助規劃組態：

資訊類型	選項
SVM 指定您要與此外部引擎建立關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`

引擎名稱_ 指定要指派給外部引擎組態的名稱。之後建立FPolicy原則時、您必須指定外部引擎名稱。這會將外部引擎與原則建立關聯。 名稱最長可達256個字元。 如果在MetroCluster 一個還原或SVM災難恢復組態中設定外部引擎名稱、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-engine-name engine_name`
主要*FPolicy*伺服器 指定節點傳送特定FPolicy原則通知的主要FPolicy伺服器。此值會指定為以逗號分隔的IP位址清單。 如果指定多個主要伺服器IP位址、則SVM參與的每個節點都會在原則啟用時、建立每個指定主要FPolicy伺服器的控制連線。如果您設定多個主要FPolicy伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。 如果外部引擎用於MetroCluster SVM災難恢復組態、您應該將來源站台FPolicy伺服器的IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。	`-primary-servers IP_address、 ...`
連接埠號碼_ 指定FPolicy服務的連接埠號碼。	`-port integer`
次要FPolicy伺服器_ 指定次要FPolicy伺服器、以便針對指定的FPolicy原則傳送檔案存取事件。此值會指定為以逗號分隔的IP位址清單。 次要伺服器只會在無法連線到任何一部主要伺服器時使用。當原則啟用時、就會建立次要伺服器的連線、但只有在所有主要伺服器都無法連線時、才會將通知傳送到次要伺服器。如果您設定多個次要伺服器、通知會以循環配置資源的方式傳送至FPolicy伺服器。	`-secondary-servers IP_address、 ...`

外部引擎類型_ 指定外部引擎是以同步或非同步模式運作。根據預設、FPolicy會以同步模式運作。 設定為時 `synchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、但在收到 FPolicy 伺服器的回應之後才會繼續。此時、視FPolicy伺服器的回應是否允許要求的動作而定、要求流程會繼續或處理會導致拒絕。 設定為時 `asynchronous`、檔案要求處理會傳送通知給 FPolicy 伺服器、然後繼續。	`-extern-engine-type external_engine_type` 此參數的值可以是下列其中一項： • `synchronous` • `asynchronous`
外部引擎格式_ 指定外部引擎格式是 XML 還是 protobuf 。 從 ONTAP 9.15.1 開始、您可以使用原型引擎格式。設為 probuf 時、通知訊息會使用 Google Prototbuf 以二進位格式編碼。在將引擎格式設定為 protobuf 之前、請確定 FPolicy 伺服器也支援 protobuf 反序列化。	`- extern-engine-format {protobuf 或 xml}`
與FPolicy server_通訊的_SSL選項 指定與FPolicy伺服器通訊的SSL選項。這是必要的參數。您可以根據下列資訊選擇其中一個選項： • 設定為時 `no-auth`、不進行驗證。 通訊連結是透過TCP建立。 • 設定為時 `server-auth`， SVM 使用 SSL 伺服器驗證來驗證 FPolicy 伺服器。 • 設定為時 `mutual-auth`、在 SVM 和 FPolicy 伺服器之間進行相互驗證；SVM 驗證 FPolicy 伺服器、 FPolicy 伺服器驗證 SVM 。 如果您選擇設定相互 SSL 驗證、則也必須設定 `-certificate -common-name`、 `-certificate-serial`和 `-certifcate-ca` 參數。	`-ssl-option {no-auth`
`server-auth`	`mutual-auth}`
憑證*FQDN*或自訂通用名稱 指定在SVM與FPolicy伺服器之間設定SSL驗證時所使用的憑證名稱。您可以將憑證名稱指定為FQDN或自訂通用名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-common-name` 參數。	`-certificate-common -name text`

憑證序號 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證序號。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-serial` 參數。	`-certificate-serial text`
憑證授權單位 指定在SVM與FPolicy伺服器之間設定SSL驗證時、用於驗證的憑證CA名稱。 如果您指定 `mutual-auth` 適用於 `-ssl-option` 參數、您必須指定的值 `-certificate-ca` 參數。	`-certificate-ca text`

進階的外部引擎選項是什麼

您可以在規劃是否使用進階參數自訂組態時、使用下表的進階FPolicy組態參數。您可以使用這些參數來修改叢集節點與FPolicy伺服器之間的通訊行為：

資訊類型	選項
取消要求的逾時_ 指定時間間隔（小時） (`h`）、分鐘 (`m`）或秒 (`s`）節點等待 FPolicy 伺服器的回應。 如果逾時時間間隔超過、節點會將取消要求傳送至FPolicy伺服器。然後、節點會將通知傳送至替代的FPolicy伺服器。此逾時有助於處理無回應的FPolicy伺服器、進而改善SMB/NFS用戶端回應。此外、在逾時期間之後取消要求、也有助於釋出系統資源、因為通知要求會從停機/不良的FPolicy伺服器移至替代的FPolicy伺服器。 此值的範圍為 `0` 透過 `100`。如果值設為 `0`，此選項已停用，取消要求訊息不會傳送至 FPolicy 伺服器。預設值為 `20s`。	`-reqs-cancel-timeout integer`[h
m	s]
中止要求的逾時_ 指定逾時（以小時為單位） (`h`）、分鐘 (`m`）或秒 (`s`）以中止要求。 此值的範圍為 `0` 透過 `200`。	`-reqs-abort-timeout ` `integer`[h
m	s]

傳送狀態要求的時間間隔 指定以小時為單位的時間間隔 (h）、分鐘 (m）或秒 (s）之後、狀態要求會傳送至 FPolicy 伺服器。 此值的範圍為 0 透過 50。如果值設為 0、選項已停用、狀態要求訊息不會傳送至 FPolicy 伺服器。預設值為 10s。	`-status-req-interval integer`[h
m	s]
*FPolicy*伺服器上未處理的要求上限 指定可在FPolicy伺服器上排入佇列的未處理要求數目上限。 此值的範圍為 1 透過 10000。預設值為 500。	`-max-server-reqs integer`
中斷無回應的*FPolicy*伺服器連線逾時 指定時間間隔（小時）(h）、分鐘 (m）或秒 (s）之後、會終止與 FPolicy 伺服器的連線。 只有FPolicy伺服器的佇列包含允許的最大要求數、且在逾時期間內未收到任何回應時、才會在逾時期間之後終止連線。允許的最大要求數為其中之一 50（預設）或指定的號碼 `max-server-reqs-` 參數。 此值的範圍為 1 透過 100。預設值為 60s。	`-server-progress -timeout integer`[h
m	s]
_將保持活動訊息傳送至FPolicy server_的時間間隔 指定時間間隔（小時）(h）、分鐘 (m）或秒 (s）將保持活動的訊息傳送到 FPolicy 伺服器。 「保持連線」訊息會偵測半開啟的連線。 此值的範圍為 10 透過 600。如果值設為 0，此選項會停用，並防止將持續作用的訊息傳送至 FPolicy 伺服器。預設值為 120s。	`-keep-alive-interval- integer`[h
m	s]
最大重新連線嘗試次數_ 指定SVM在連線中斷後嘗試重新連線至FPolicy伺服器的最大次數。 此值的範圍為 0 透過 20。預設值為 5。	`-max-connection-retries integer`

接收緩衝區大小_ 指定FPolicy伺服器之連接插槽的接收緩衝區大小。 預設值設為256 KB。當值設定為0時、接收緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設接收緩衝區大小為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定接收緩衝區的大小（以位元組為單位）。	`-recv-buffer-size integer`
傳送緩衝區大小 指定FPolicy伺服器之連線通訊端的傳送緩衝區大小。 預設值設為256 KB。當值設定為0時、傳送緩衝區的大小會設定為系統定義的值。 例如、如果套接字的預設傳送緩衝區大小設為65536位元組、將可調值設為0、則套接字緩衝區大小會設為65536位元組。您可以使用任何非預設值來設定傳送緩衝區的大小（以位元組為單位）。	`-send-buffer-size integer`
重新連線期間清除工作階段*ID*逾時 指定以小時為單位的時間間隔 (`h`）、分鐘 (`m`）或秒 (`s`）之後、新的工作階段 ID 會在重新連線嘗試期間傳送至 FPolicy 伺服器。 如果儲存控制器與FPolicy伺服器之間的連線終止、並在中進行重新連線 `-session-timeout` 時間間隔時、舊的工作階段ID會傳送至FPolicy伺服器、以便傳送舊通知的回應。 預設值設為 10 秒。	`-session-timeout [integerh][integerM][integers]`

有關配置 **ONTAP FPolicy** 外部引擎以使用 **SSL** 身份驗證連接的其他信息

如果您想要設定FPolicy外部引擎、以便在連線至FPolicy伺服器時使用SSL、您需要知道一些其他資訊。

SSL伺服器驗證

如果您選擇將FPolicy外部引擎設定為SSL伺服器驗證、則在建立外部引擎之前、必須先安裝簽署FPolicy伺服器憑證的憑證授權單位（CA）的公開憑證。

相互驗證

如果您將FPolicy外部引擎設定為在將儲存虛擬機器（SVM）資料LIF連線至外部FPolicy伺服器時使用SSL相互驗證、則在建立外部引擎之前、 您必須安裝簽署FPolicy伺服器憑證的CA公開憑證、以及用於驗證SVM的公開憑證和金鑰檔。當任何 FPolicy 原則使用已安裝的憑證時，請勿刪除此憑證。

如果在FPolicy連線至外部FPolicy伺服器時、憑證被刪除、則無法重新啟用使用該憑證的停用FPolicy原則。在這

種情況下、即使在SVM上建立並安裝了具有相同設定的新憑證、也無法重新啟用FPolicy原則。

如果憑證已刪除、您需要安裝新的憑證、建立使用新憑證的新FPolicy外部引擎、並透過修改FPolicy原則、將新的外部引擎與您要重新啟用的FPolicy原則建立關聯。

安裝**SSL**憑證

用來簽署 FPolicy 伺服器憑證的 CA 公用憑證是使用安裝 `security certificate install` 命令 `-type` 參數設為 `client-ca`。使用安裝驗證 SVM 所需的私密金鑰和公開憑證 `security certificate install` 命令 `-type` 參數設為 `server`。

相關資訊

- "安全性憑證安裝"

ONTAP FPolicy 憑證不會在具有非 **ID** 保留配置的 **SVM** 災難復原關係中複製

連線至FPolicy伺服器時用於SSL驗證的安全性憑證、不會以非ID-preserve組態複寫至SVM災難恢復目的地。雖然已複寫SVM上的FPolicy外部引擎組態、但不會複寫安全性憑證。您必須在目的地上手動安裝安全性憑證。

當您設定 SVM 災難恢復關係時、您為選取的值 `-identity-preserve` 的選項 `snapmirror create` 命令可決定在目的地 SVM 中複寫的組態詳細資料。

如果您設定 `-identity-preserve` 選項 `true` （ ID-preserve ）、所有 FPolicy 組態詳細資料都會複寫、包括安全性憑證資訊。只有當您將選項設定為時、才必須在目的地上安裝安全性憑證 `false` （非 ID-Preserve ）。

相關資訊

- "SnapMirror建立"

具有 **MetroCluster** 和 **SVM** 災難復原配置的叢集範圍 **ONTAP FPolicy** 外部引擎的限制

您可以將叢集儲存虛擬機器（SVM）指派給外部引擎、藉此建立叢集範圍內的FPolicy外部引擎。然而、在MetroCluster 使用叢集或SVM災難恢復組態建立以叢集為範圍的外部引擎時、選擇SVM用於與FPolicy伺服器進行外部通訊的驗證方法時、會有某些限制。

建立外部FPolicy伺服器時、您可以選擇三種驗證選項：無驗證、SSL伺服器驗證和SSL相互驗證。雖然在選擇驗證選項時沒有任何限制、但如果將外部FPolicy伺服器指派給資料SVM、則在建立叢集範圍的FPolicy外部引擎時仍有限制：

組態	是否允許？
不含驗證的SVM災難恢復和叢集範圍的FPolicy外部引擎（未設定SSL）MetroCluster	是的
包含SSL伺服器或SSL相互驗證的SVM災難恢復、以及叢集範圍的FPolicy外部引擎MetroCluster	否

- 如果存在具有SSL驗證的叢集範圍FPolicy外部引擎、而您想要建立MetroCluster 一套支援還原或SVM災難恢復的組態、您必須先修改此外部引擎、使其不使用驗證、或是移除外部引擎、才能建立MetroCluster 還原

或SVM災難恢復組態。

- 如果MetroCluster 已存在支援功能的不支援功能或SVM災難恢復組態、ONTAP 則無法使用SSL驗證來建立叢集範圍的FPolicy外部引擎。

完成 **ONTAP FPolicy** 外部引擎設定工作表

您可以使用這份工作表來記錄FPolicy外部引擎組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、再設定外部引擎。

基本外部引擎組態資訊

您應該記錄是否要在外部引擎組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
引擎名稱	是的	是的	
主要FPolicy伺服器	是的	是的	
連接埠號碼	是的	是的	
次要FPolicy伺服器	否		
外部引擎類型	否		
用於與外部FPolicy伺服器通訊的SSL選項	是的	是的	
憑證FQDN或自訂通用名稱	否		
憑證序號	否		
憑證授權單位	否		

進階外部引擎參數資訊

若要使用進階參數設定外部引擎、您必須在進階權限模式下輸入組態命令。

資訊類型	必要	包括	您的價值
取消要求逾時	否		
中止要求的逾時	否		

傳送狀態要求的時間間隔	否		
FPolicy伺服器上未處理的要求上限	否		
中斷無回應的FPolicy伺服器連線逾時	否		
將「保持作用中」訊息傳送至FPolicy伺服器的時間間隔	否		
最大重新連線嘗試次數	否		
接收緩衝區大小	否		
傳送緩衝區大小	否		
重新連線期間清除工作階段ID的逾時	否		

規劃**FPolicy**事件組態

瞭解 **ONTAP FPolicy** 事件組態

在設定FPolicy事件之前、您必須先瞭解建立FPolicy事件的意義。您必須決定要監控事件的傳輸協定、要監控的事件、以及要使用的事件篩選器。此資訊可協助您規劃要設定的值。

建立**FPolicy**事件的意義

建立FPolicy事件是指定義FPolicy程序所需的資訊、以決定要監控的檔案存取作業、以及應將哪些受監控事件通知傳送至外部FPolicy伺服器。FPolicy事件組態定義下列組態資訊：

- 儲存虛擬機器（SVM）名稱
- 事件名稱
- 要監控的傳輸協定

  FPolicy 可監控 SMB ， NFSv3 ， NFSv4 ，以及從 ONTAP 9.15.1 開始的 NFSv4.1 檔案存取作業。

- 要監控的檔案作業

  並非所有檔案作業都適用於每個傳輸協定。

- 要設定哪些檔案篩選器

  只有特定的檔案作業與篩選組合有效。每個傳輸協定都有自己的一組支援組合。

- 是否要監控磁碟區掛載和卸載作業

其中三個參數有相依性 (`-protocol`、 `-file-operations`、 `-filters`）。下列組合對三個參數有效：

- 您可以指定 `-protocol` 和 `-file-operations` 參數。
- 您可以指定全部三個參數。
- 您不能指定任何參數。

FPolicy事件組態包含的內容

您可以使用下列可用的FPolicy事件組態參數清單來協助規劃組態：

資訊類型	選項
SVM 指定您要與此FPolicy事件相關聯的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
事件名稱_ 指定要指派給FPolicy事件的名稱。當您建立FPolicy原則時、會使用事件名稱將FPolicy事件與原則建立關聯。 名稱最長可達256個字元。 如果在MetroCluster 還原或SVM災難恢復組態中設定事件、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • "_"、"-`", and “.”	`-event-name event_name`

傳輸協定 指定要為FPolicy事件設定的傳輸協定。的清單 `-protocol` 可以包含下列其中一個值： • `cifs` • `nfsv3` • `nfsv4` 如果您指定 `-protocol`、然後您必須在中指定有效值 `-file-operations` 參數。隨著傳輸協定版本變更、有效值可能會變更。 從 ONTAP 9.15.1 開始， NFSv4 可讓您擷取 NFSv4.0 和 NFSv4.1 事件。	`-protocol protocol`

_File operations _ 指定FPolicy事件的檔案作業清單。 事件會使用中指定的通訊協定、從所有用戶端要求檢查此清單中指定的作業 `-protocol` 參數。您可以使用以逗號分隔的清單來列出一或多個檔案作業。的清單 `-file-operations` 可以包含下列一或多個值： • `close` 用於檔案關閉作業 • `create` 用於檔案建立作業 • `create-dir` 用於目錄建立作業 • `delete` 用於檔案刪除作業 • `delete_dir` 用於目錄刪除作業 • `getattr` 以取得屬性作業 • `link` 用於連結作業 • `lookup` 用於查詢作業 • `open` 適用於檔案開啟作業 • `read` 檔案讀取作業 • `write` 適用於檔案寫入作業 • `rename` 用於檔案重新命名作業 • `rename_dir` 用於目錄重新命名作業 • `setattr` 用於 Set 屬性作業 • `symlink` 用於符號連結作業 如果您指定 `-file-operations`、然後您必須在中指定有效的傳輸協定 `-protocol` 參數。	`-file-operations file_operations、 ...`

篩選 指定指定傳輸協定之特定檔案作業的篩選器清單。中的值 `-filters` 參數用於篩選用戶端要求。清單可包含下列一項或多項內容： 如果您指定 `-filters` 參數、您也必須為指定有效值 `-file-operations` 和 `-protocol` 參數。 • `monitor-ads` 用於篩選用戶端要求的替代資料串流選項。 • `close-with-modification` 篩選用戶端要求以進行修改以關閉的選項。 • `close-without-modification` 篩選用戶端要求以關閉而不修改的選項。 • `first-read` 篩選用戶端要求以進行第一讀取的選項。 • `first-write` 篩選用戶端要求進行第一次寫入的選項。 • `offline-bit` 用於篩選用戶端離線位元集要求的選項。 設定此篩選器後、FPolicy伺服器只會在存取離線檔案時收到通知。 • `open-with-delete-intent` 用於篩選用戶端要求以進行「刪除目的」開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案以刪除檔案時收到通知。檔案系統會在使用時使用此功能 `FILE_DELETE_ON_CLOSE` 已指定旗標。 • `open-with-write-intent` 篩選用戶端要求以進行寫入目的開啟的選項。 設定此篩選器後、FPolicy伺服器只會在嘗試開啟檔案時收到通知、以便在其中寫入內容。 • `write-with-size-change` 選項可篩選用戶端寫入要求、並變更大小。 • `setattr-with-owner-change` 用於篩選用戶端設定檔要求以變更檔案或目錄擁有者的選項。 • `setattr-with-group-change` 用於篩選用戶端集點要求以變更檔案或目錄群組的選項。 • `setattr-with-sacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 SACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 • `setattr-with-dacl-change` 用於篩選用戶端集點要求以變更檔案或目錄上的 DACL 的選項。 此篩選器僅適用於SMB和NFSv4傳輸協定。 `setattr-with-modify-time-change` 用於篩選用戶端 setattr 要求以變更檔案或目錄的修改時間的選項。 `setattr-with-access-time-change` 用於篩選用戶端 setattr 要求	`-filters filter、 ...`

需要磁碟區作業 指定磁碟區掛載和卸載作業是否需要監控。預設值為 `false`。	`-volume-operation {true`

`false}`
 	
`-filters filter、 ...`
	_FPolicy 存取遭拒通知 _
	
	從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。由於缺乏權限、將會產生檔案作業失敗的通知、其中包括：
	
	• NTFS 權限導致的失敗。
	• 因 Unix 模式位元而發生故障。
	• NFSv4 ACL 導致故障。

`-monitor-fileop-failure {true`	`false}`

ONTAP FPolicy 監控 **SMB** 支援的檔案操作和過濾器組合

設定FPolicy事件時、您必須注意、監控SMB檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

下表提供了用於監控SMB檔案存取事件的FPolicy支援檔案操作和篩選器組合清單：

支援的檔案作業	支援的篩選器
關閉	監控廣告、離線位元、近距離修改、近距離不需修改、近距離讀取、 exclude目錄
建立	監控廣告、離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	監控廣告、離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、exclude目錄
開啟	監控廣告、離線位元、開放刪除意圖、開放寫入目的、排除目錄

讀取	監控廣告、離線位元、第一讀取
寫入	監控廣告、離線位元、第一寫入、大小變更寫入
重新命名	監控廣告、離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	監控廣告、離線位元、設定ATtr_with _Owner_change、設定ATr_with _group_change、設定ATtr_with _mode_change、 setattr_with _SACL_change、setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with creation_time_change、 setattr_with _size_change、setattr_with _all撥款_size_change、exclude目錄

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的存取遭拒檔案作業清單、以及 FPolicy 監控 SMB 檔案存取事件的篩選器組合：

支援的存取遭拒檔案作業	支援的篩選器
開啟	不適用

ONTAP FPolicy 為 **NFSv3** 監控的支援的檔案操作和過濾器組合

當您設定 FPolicy 事件時、您必須注意、只有特定的檔案作業和篩選器組合才支援監控 NFSv3 檔案存取作業。

下表提供支援的檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的檔案作業	支援的篩選器
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
連結	離線位元
查詢	離線位元、exclude目錄
讀取	離線位元、第一讀取

寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定attr_with模式變更、設定ATtr_with修改時間變更、 setattr_with存取時間變更、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv3 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用
建立	不適用
create_dir	不適用
刪除	不適用
刪除目錄	不適用
連結	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

ONTAP FPolicy 為 **NFSv4** 監控的支援的檔案操作和過濾器組合

設定FPolicy事件時、您必須注意、監控NFSv4檔案存取作業時、僅支援特定的檔案作業和篩選器組合。

從 ONTAP 9.15.1 開始、 FPolicy 支援 NFSv4.1 傳輸協定。

下表提供 NFSv4 或 NFSv4.1 檔案存取事件的 FPolicy 監控支援檔案作業和篩選器組合清單：

支援的檔案作業	支援的篩選器
關閉	離線位元、排除目錄
建立	離線位元
create_dir	目前此檔案作業不支援篩選器。
刪除	離線位元
刪除目錄	目前此檔案作業不支援篩選器。
GetAttr	離線位元、排除目錄
連結	離線位元
查詢	離線位元、排除目錄
開啟	離線位元、排除目錄
讀取	離線位元、第一讀取
寫入	離線位元、第一寫入、大小變更寫入
重新命名	離線位元
重新命名目錄	目前此檔案作業不支援篩選器。
設定	離線位元、設定attr_with _Owner_change、設定attr_with _group變更、設定ATr_with模式變更、設定ATtr_with _SACL_change、 setattr_with _dacl_change、setattr_with _dmodify_time_change、setattr_with _access_time_change、setattr_with _size_change、exclude目錄
symlink	離線位元

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。下表提供支援的拒絕存取檔案作業清單、以及 FPolicy 監控 NFSv4 或 NFSv4.1 檔案存取事件的篩選組合：

支援的存取遭拒檔案作業	支援的篩選器
存取	不適用

建立	不適用
create_dir	不適用
刪除	不適用
刪除目錄	不適用
連結	不適用
開啟	不適用
讀取	不適用
重新命名	不適用
重新命名目錄	不適用
設定	不適用
寫入	不適用

完成 **ONTAP FPolicy** 事件設定工作表

您可以使用這份工作表單來記錄FPolicy事件組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的值、再設定FPolicy事件。

您應該記錄是否要在FPolicy事件組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
事件名稱	是的	是的	
傳輸協定	否		
檔案作業	否		
篩選器	否		
Volume作業	否		

存取遭拒事件 （從 ONTAP 9.13 開始支援）	否		

規劃FPolicy原則組態

了解 ONTAP FPolicy 策略配置

在設定FPolicy原則之前、您必須先瞭解建立原則時需要哪些參數、以及設定某些選用參數的原因。此資訊可協助您判斷要為每個參數設定哪些值。

建立FPolicy原則時、您會將原則與下列項目建立關聯：

- 儲存虛擬機器（SVM）
- 一或多個FPolicy事件
- FPolicy外部引擎

您也可以設定多個選用的原則設定。

FPolicy原則組態包含的內容

您可以使用下列可用的必要FPolicy原則清單和選用參數來協助規劃組態：

資訊類型	選項	必要	預設
*SVM*名稱 指定您要在其中建立FPolicy原則的SVM名稱。	`-vserver vserver_name`	是的	無

原則名稱 指定FPolicy原則的名稱。 名稱最長可達256個字元。 如果在MetroCluster 還原或SVM災難恢復組態中設定原則、名稱最長應為200個字元。 名稱可以包含下列任何Ascii範圍字元的組合： • `a` 透過 `z` • `A` 透過 `Z` • `0` 透過 `9` • “_” 、 “-”, and “.”	`-policy-name policy_name`	是的	無
事件名稱_ 指定要與FPolicy原則相關聯的以逗號分隔的事件清單。 • 您可以將多個事件與原則建立關聯。 • 事件是特定於傳輸協定的事件。 • 您可以使用單一原則來監控多個傳輸協定的檔案存取事件、方法是針對您要原則監控的每個傳輸協定建立事件、然後將事件與原則建立關聯。 • 事件必須已經存在。	`-events event_name、 ...`	是的	無
Persistent story 從 ONTAP 9.14.1 開始、此參數會指定持續儲存區、以擷取 SVM 中非強制性非非同步原則的檔案存取事件。	`-persistent -store persistent_store_name`	否	無

外部引擎名稱_ 指定要與FPolicy原則關聯的外部引擎名稱。 • 外部引擎包含節點傳送通知至FPolicy伺服器所需的資訊。 • 您可以將FPolicy設定為使用ONTAP 靜態原生外部引擎來進行簡單的檔案封鎖、或是使用外部引擎來設定使用外部FPolicy伺服器（FPolicy伺服器）來進行更精密的檔案封鎖和檔案管理。 • 如果您想要使用原生外部引擎、則無法指定此參數的值、也可以指定 `native` 做為價值。 • 如果您要使用FPolicy伺服器、則外部引擎的組態必須已經存在。	`-engine engine_name`	是（除非原則使用內部ONTAP 的非原生引擎）	`native`
是必填篩選 指定是否需要強制檔案存取篩選。 • 強制篩選設定可決定當所有主要和次要伺服器都當機、或在指定的逾時期間內未收到FPolicy伺服器的回應時、檔案存取事件會採取什麼行動。 • 設定為時 `true`、檔案存取事件遭拒。 • 設定為時 `false`，允許檔案存取事件。	`-is-mandatory {true`	`false}`	否

true	允許權限存取_ 指定您是否要FPolicy伺服器使用權限資料連線、以具有存取受監控檔案和資料夾的權限。 如果設定、FPolicy伺服器可以使用權限資料連線、從SVM的根目錄存取包含受監控資料的檔案。 若要進行特殊權限的資料存取、必須在叢集上授權 SMB 、且必須將用於連線至 FPolicy 伺服器的所有資料生命體設定為具有 `cifs` 作為其中一種允許的通訊協定。 如果您想要設定原則以允許權限存取、也必須為您想要FPolicy伺服器用於權限存取的帳戶指定使用者名稱。	`-allow -privileged -access {yes`	`no}`
否（除非啟用Passthrough-read）	`no`	特殊權限使用者名稱 指定FPolicy伺服器用來存取特殊權限資料的帳戶使用者名稱。 • 此參數的值應使用「'domain\username'」格式。 • 如果 `-allow -privileged -access` 設為 `no`，將忽略爲此參數設置的任何值。	`-privileged -user-name user_name`

否（除非已啟用權限存取）	無	允許Passthrough-read_ 指定FPolicy伺服器是否能為FPolicy伺服器歸檔至次要儲存設備（離線檔案）的檔案提供Passter-Read服務： • Passthsther-read是一種讀取離線檔案資料的方法、無需將資料還原至主要儲存設備。 Passthroh-read可減少回應延遲、因為在回應讀取要求之前、不需要將檔案重新叫用回主要儲存設備。此外、Passthrough-read可免除使用僅為了滿足讀取要求而回收的檔案來耗用主要儲存空間的需求、藉此優化儲存效率。 • 啟用時、FPolicy伺服器會透過專為Passthrough-Reads所開啟的個別特殊權限資料通道、提供檔案的資料。 • 如果您想要設定Passthrough-read、也必須將原則設定為允許權限存取。	`-is-passthrough-read-enabled {true`

如果 **FPolicy** 政策使用本機引擎，則需要 **ONTAP FPolicy** 範圍配置

如果您將FPolicy原則設定為使用原生引擎、則需要針對原則設定的FPolicy範圍進行定義。

FPolicy範圍會定義套用FPolicy原則的界限、例如FPolicy是否套用至指定的磁碟區或共用區。有許多參數會進一步限制FPolicy原則套用的範圍。其中一個參數、 `-is-file-extension-check-on-directories`

`-enabled`，指定是否檢查目錄上的副檔名。預設值為 `false`，這表示不會檢查目錄上的副檔名。

當使用原生引擎的 FPolicy 原則在共用區或磁碟區和上啟用時 `-is-file-extension-check-on-directories-enabled` 參數設定為 `false` 對於原則的範圍、目錄存取會被拒絕。使用此組態時、因為不會檢查目錄的副檔名、所以如果目錄作業屬於原則範圍、則會拒絕任何目錄作業。

若要確保使用原生引擎時目錄存取成功、您必須設定 `-is-file-extension-check-on-directories-enabled parameter` 至 `true` 建立範圍時。

將此參數設為 `true`、會針對目錄作業進行延伸檢查、並根據 FPolicy 範圍組態中所包含或排除的延伸來決定是否允許或拒絕存取。

完成 **ONTAP FPolicy** 策略工作表

您可以使用這份工作表單來記錄FPolicy原則組態程序期間所需的值。您應該記錄是否要在FPolicy原則組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	
原則名稱	是的	
事件名稱	是的	
持續儲存區		
外部引擎名稱		
是否需要強制篩選？		
允許特殊權限存取		
權限使用者名稱		
是否已啟用Passthrough-read？		

規劃**FPolicy**範圍組態

了解 **ONTAP FPolicy** 範圍配置

在設定FPolicy範圍之前、您必須先瞭解建立範圍的意義。您必須瞭解範圍組態包含哪些內容。您也需要瞭解優先順序的範圍規則。此資訊可協助您規劃要設定的值。

建立**FPolicy**範圍的意義

建立FPolicy範圍是指定義套用FPolicy原則的界限。儲存虛擬機器（SVM）是基本邊界。當您建立FPolicy原則的

範圍時、必須定義要套用該原則的FPolicy原則、而且必須指定要套用範圍的SVM。

有許多參數會進一步限制指定SVM內的範圍。您可以指定要納入範圍的內容、或指定要從範圍中排除的項目、來限制範圍。將範圍套用至已啟用的原則之後、原則事件檢查就會套用至此命令所定義的範圍。

系統會針對檔案存取事件產生通知、其中「include'」選項中有相符項目。不會針對檔案存取事件產生通知、其中「exclude」選項中有相符項目。

FPolicy範圍組態定義下列組態資訊：

- SVM名稱
- 原則名稱
- 要納入或排除的共享區
- 匯出原則、以納入或排除受監控的內容
- 要納入或排除的磁碟區
- 要納入或排除的檔案副檔名
- 是否對目錄物件進行檔案副檔名檢查

> 叢集FPolicy原則的範圍有特殊考量。叢集FPolicy原則是叢集管理員為管理SVM所建立的原則。如果叢集管理員也為該叢集FPolicy原則建立範圍、則SVM管理員無法為該相同原則建立範圍。但是、如果叢集管理員未建立叢集FPolicy原則的範圍、則任何SVM管理員都可以建立該叢集原則的範圍。如果SVM管理員為該叢集FPolicy原則建立範圍、叢集管理員便無法隨後為該相同的叢集原則建立叢集範圍。這是因為叢集管理員無法覆寫同一個叢集原則的範圍。

優先順序的範圍規則為何

下列優先規則適用於範圍組態：

- 當共享區包含在中時 `-shares-to-include` 共享區的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-shares-to-include`。
- 當中包含匯出原則時 `-export-policies-to-include` 匯出原則的參數和父Volume會包含在中 `-volumes-to-exclude` 參數、 `-volumes-to-exclude` 優先於 `-export-policies-to-include`。
- 系統管理員可以同時指定兩者 `-file-extensions-to-include` 和 `-file-extensions-to-exclude` 清單。

  。 `-file-extensions-to-exclude` 參數會在之前檢查 `-file-extensions-to-include` 參數已核取。

FPolicy範圍組態包含的內容

您可以使用下列可用的FPolicy範圍組態參數清單來協助規劃組態：

> 當設定要納入或排除範圍的共用、匯出原則、磁碟區及副檔名時、包含和排除參數可以包含像是「」之類的元元符號?" and "*。 不支援使用規則運算式。

資訊類型	選項

SVM 指定您要在其中建立FPolicy範圍的SVM名稱。 每個FPolicy組態都是在單一SVM中定義。為了建立FPolicy原則組態、而將外部引擎、原則事件、原則範圍和原則結合在一起的原則、都必須與相同的SVM建立關聯。	`-vserver vserver_name`
原則名稱 指定要附加範圍的FPolicy原則名稱。FPolicy原則必須已經存在。	`-policy-name policy_name`
要納入的共享_ 指定以逗號分隔的共用清單、以監控套用範圍的FPolicy原則。	`-shares-to-include share_name、...`
要排除的共享_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的共用清單。	`-shares-to-exclude share_name、...`
_要包含的磁碟區_指定以逗號分隔的磁碟區清單、以監控套用範圍的FPolicy原則。	`-volumes-to-include volume_name、...`
要排除的磁碟區_ 指定要從套用範圍之FPolicy原則的監控中排除的以逗號分隔的磁碟區清單。	`-volumes-to-exclude volume_name、...`
匯出要納入的原則_ 指定以逗號分隔的匯出原則清單、以監控套用範圍的FPolicy原則。	`-export-policies-to -include export_policy_name、...`
匯出要排除的原則_ 指定要從套用範圍之FPolicy原則的監控中排除的匯出原則清單（以英文分隔）。	`-export-policies-to -exclude export_policy_name、...`
要包括的副檔名 指定要監控套用範圍之FPolicy原則的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -include file_extensions、...`
要排除的檔案副檔名_ 指定要從套用範圍之FPolicy原則的監控中排除的檔案副檔名以逗號分隔的清單。	`-file-extensions-to -exclude file_extensions、...`

檔案副檔名檢查是否已啟用目錄？ 指定副檔名檢查是否也適用於目錄物件。如果此參數設為 `true`，目錄物件會受到與一般檔案相同的副檔名檢查。如果此參數設為 `false`，目錄名稱不符合副檔名，即使目錄的副檔名不符，也會傳送通知給目錄。 如果將範圍指派給的 FPolicy 原則設定為使用原生引擎、則必須將此參數設定為 `true`。	`-is-file-extension -check-on-directories -enabled {true`
`false`	}

完成 **ONTAP FPolicy** 範圍工作表

您可以使用這份工作表單來記錄FPolicy範圍組態程序期間所需的值。如果需要參數值、您必須先判斷這些參數的使用值、然後再設定FPolicy範圍。

您應該記錄是否要在FPolicy範圍組態中包含每個參數設定、然後記錄您要納入的參數值。

資訊類型	必要	包括	您的價值
儲存虛擬機器（SVM）名稱	是的	是的	
原則名稱	是的	是的	
要納入的共享區	否		
要排除的共享區	否		
要包含的磁碟區	否		
要排除的磁碟區	否		
匯出要納入的原則	否		
匯出要排除的原則	否		
要包含的副檔名	否		
要排除的副檔名	否		
是否已啟用目錄的副檔名檢查？	否		

建立**FPolicy**組態

您必須建立外部引擎、才能開始建立FPolicy組態。外部引擎定義FPolicy如何建立及管理外部FPolicy伺服器的連線。如果您的組態使用內部ONTAP 的靜態引擎（原生外部引擎）來進行簡單的檔案封鎖、則不需要設定個別的FPolicy外部引擎、也不需要執行此步驟。

開始之前

。 "外部引擎" 工作表應填寫完畢。

關於這項工作

如果外部引擎用於MetroCluster 整個功能表組態、您應該將來源站台的FPolicy伺服器IP位址指定為主要伺服器。目的地站台FPolicy伺服器的IP位址應指定為次要伺服器。

步驟

1. 使用建立 FPolicy 外部引擎 `vserver fpolicy policy external-engine create` 命令。

   下列命令會在儲存虛擬機器（SVM）vs1.example.com上建立外部引擎。與FPolicy伺服器的外部通訊不需要驗證。

   ```
   vserver fpolicy policy external-engine create -vserver-name vs1.example.com
   -engine-name engine1 -primary-servers 10.1.1.2,10.1.1.3 -port 6789 -ssl-option
   no-auth
   ```

2. 使用驗證 FPolicy 外部引擎組態 `vserver fpolicy policy external-engine show` 命令。

   下列命令會顯示有關SVM vs1.example.com上設定的所有外部引擎資訊：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com
   ```

   ```
                                Primary         Secondary
   External
   Vserver             Engine   Servers         Servers        Port Engine
   Type
   ---------------     ---------- -------------- ----------- ------
   ----------
   vs1.example.com     engine1  10.1.1.2,       -              6789
   synchronous
                                10.1.1.3
   ```

   下列命令會在SVM vs1.example.com上顯示名為「engin1」的外部引擎詳細資訊：

   ```
   vserver fpolicy policy external-engine show -vserver vs1.example.com -engine
   -name engine1
   ```

```
                                Vserver: vs1.example.com
                                 Engine: engine1
              Primary FPolicy Servers: 10.1.1.2, 10.1.1.3
       Port Number of FPolicy Service: 6789
            Secondary FPolicy Servers: -
                 External Engine Type: synchronous
SSL Option for External Communication: no-auth
           FQDN or Custom Common Name: -
         Serial Number of Certificate: -
               Certificate Authority: -
```

建立 ONTAP FPolicy 事件

在建立FPolicy原則組態時、您需要建立FPolicy事件。您可以在建立事件時、將其與FPolicy原則建立關聯。事件會定義要監控的傳輸協定、以及要監控和篩選的檔案存取事件。

開始之前

您應該完成 FPolicy 事件"工作表"。

建立FPolicy事件

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

   ```
   vserver fpolicy policy event create -vserver vs1.example.com -event-name
   event1 -protocol cifs -file-operations open,close,read,write
   ```

2. 使用驗證 FPolicy 事件組態 `vserver fpolicy policy event show` 命令。

   ```
   vserver fpolicy policy event show -vserver vs1.example.com
   ```

   ```
                     Event                File                       Is Volume
   Vserver           Name      Protocols  Operations     Filters    Operation
   ---------------   --------- ---------  -------------  ---------
   ------------
   vs1.example.com   event1    cifs       open, close,   -          false
                                          read, write
   ```

建立 FPolicy 存取遭拒事件

從 ONTAP 9.13.1 開始、使用者可以收到因權限不足而導致檔案作業失敗的通知。這些通知對於安全性、勒索軟體保護和治理來說非常重要。

1. 使用建立 FPolicy 事件 `vserver fpolicy policy event create` 命令。

```
vserver fpolicy policy event create -vserver vs1.example.com -event-name
event1 -protocol cifs -monitor-fileop-failure true -file-operations open
```

建立 **ONTAP FPolicy** 持久性存儲

持續儲存區可協助將用戶端 I/O 處理與 FPolicy 通知處理分離、以減少用戶端延遲。從 ONTAP 9.14.1 開始、 FPolicy 可讓您進行設定 "持續儲存區" 擷取 SVM 中非強制性非非同步原則的檔案存取事件。不支援同步（強制或非強制）和非同步強制組態。

從 ONTAP 9.15.1 開始、 FPolicy 永續性儲存區組態已簡化。。 `persistent-store create` 命令可自動建立 SVM 的 Volume 、並設定持續儲存區的 Volume 。

根據 ONTAP 版本的不同、有兩種方法可以建立持續儲存區：

- ONTAP 9.15.1 或更新版本：當您建立持續儲存區時、 ONTAP 會自動同時建立及設定其 Volume 。如此可簡化 FPolicy 持續儲存區組態、並實作所有最佳實務做法。
- ONTAP 9.14.1 ：手動建立和設定磁碟區、然後為新建立的磁碟區建立持續儲存區。

每個 SVM 只能設定一個持續儲存區。此單一持續儲存區必須用於該 SVM 上的所有 FPolicy 組態、即使這些原則來自不同的合作夥伴。

建立持續儲存區（ **ONTAP 9.15.1** 或更新版本）

從 ONTAP 9.15.1 開始、請使用 `fpolicy persistent-store create` 命令來建立具有內嵌磁碟區建立和組態的 FPolicy 持續儲存區。ONTAP 會自動封鎖磁碟區、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

開始之前

- 您要建立持續儲存區的 SVM 必須至少有一個集合體。
- 您應該可以存取 SVM 可用的集合體、並擁有足夠的權限來建立 Volume 。

步驟

1. 建立持續儲存區、以自動建立和設定磁碟區：

   ```
   vserver fpolicy persistent-store create -vserver <vserver> -persistent-store
   <name> -volume <volume_name> -size <size> -autosize-mode
   <off|grow|grow_shrink>
   ```

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

     > ⓘ 如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它、並在 Volume 參數中指定它。

   - 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

     例如、如果您想要在每秒有 30K 通知的叢集中保留 30 分鐘的事件容量：

所需 Volume 大小 = 30000 x 30 x 60 x 0.6KB （平均通知記錄大小） = 32400000 KB = ~32 GB

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

> 如果您使用現有的 Volume 、則 Size 參數為選用項目。如果您確實為 size 參數提供值、它會以您指定的大小修改 Volume 。

- 。 `autosize-mode` 參數指定 Volume 的自動調整模式。支援的自動調整大小模式包括：
  - Off （關） - 磁碟區不會因應使用空間量而增加或縮小大小。
  - 擴充 - 當磁碟區中的使用空間超過擴充臨界值時、磁碟區會自動增加。
  - GROW _ 收縮：磁碟區會隨著使用空間的數量而增加或縮小大小。

2. 建立 FPolicy 原則、並將持續儲存區名稱新增至該原則。如需詳細資訊、請參閱 "建立FPolicy原則"。

建立持續儲存區（ **ONTAP 9.14.1** ）

您可以建立磁碟區、然後建立持續儲存區以使用該磁碟區。接著、您可以封鎖新建立的 Volume 、使其無法存取外部使用者傳輸協定（ CIFS/NFS ）。

步驟

1. 在 SVM 上建立一個空的磁碟區、以便為持續儲存區進行資源配置：

```
volume create -vserver <SVM Name> -volume <volume> -state <online> -policy
<default> -unix-permissions <777> -size <value> -aggregate <aggregate name>
-snapshot-policy <none>
```

系統管理員使用者若擁有足夠的 RBAC 權限（以建立 Volume ）、就會建立所需大小的 Volume （使用 Volume CLI 命令或 REST API ）、並提供該 Volume 的名稱做為 `-volume` 在持續儲存區中、建立 CLI 命令或 REST API 。

- 。 `vserver` 參數是 SVM 的名稱。
- 。 `volume` 參數是持續儲存區磁碟區的名稱。
- 。 `state` 參數應設為線上、以便使用 Volume 。
- 。 `policy` 如果您已設定 FPolicy 服務原則、則參數會設為 FPolicy 服務原則。如果沒有、您可以使用 `volume modify` 命令稍後新增原則。
- 。 `unix-permissions` 參數為選用項目。
- 。 `size` 參數是根據您想要保留未傳送至外部伺服器（合作夥伴應用程式）的事件的持續時間。

  例如、如果您想要在每秒有 30K 通知的叢集中保留 30 分鐘的事件容量：

  所需 Volume 大小 = 30000 x 30 x 60 x 0.6KB （平均通知記錄大小） = 32400000 KB = ~32 GB

要查找大致的通知率，您可以聯繫您的 FPolicy 合作伙伴應用程序或使用 FPolicy 計數器 `requests_dispatched_rate`。

- FlexVol Volume 需要 Aggregate 參數、否則不需要。

- 。 `snapshot-policy` 參數必須設定為無。如此可確保不會意外還原快照、導致目前事件遺失、並防止可能的重複事件處理。

  如果您想要使用現有的空白磁碟區、請使用 `volume show` 命令來尋找它和 `volume modify` 命令進行任何必要的變更。確保原則、大小和 `snapshot-policy` 持續儲存區的參數已正確設定。

2. 建立持續儲存區：

```
vserver fpolicy persistent store create -vserver <SVM> -persistent-store
<PS_name> -volume <volume>
```

   - 。 `vserver` 參數是 SVM 的名稱。
   - 。 `persistent-store` 參數是持續儲存區的名稱。
   - 。 `volume` 參數是持續儲存區磁碟區的名稱。

3. 建立 FPolicy 原則、並將持續儲存區名稱新增至該原則。如需詳細資訊、請參閱 "建立FPolicy原則"。

建立 **ONTAP FPolicy** 策略

當您建立FPolicy原則時、會將外部引擎和一或多個事件與原則建立關聯。此原則也會指定是否需要強制篩選、FPolicy伺服器是否具有存取儲存虛擬機器（SVM）上資料的權限、以及是否啟用離線檔案的傳遞讀取。

開始之前

- FPolicy原則工作表應完成。
- 如果您打算設定原則使用FPolicy伺服器、則外部引擎必須存在。
- 您計畫與FPolicy原則建立關聯的FPolicy事件必須至少存在一個。
- 如果您要設定特殊權限資料存取、SVM上必須有SMB伺服器。
- 若要設定原則的持續儲存區、引擎類型必須為 * 非同步 * 、原則必須為 * 非強制 * 。

  如需詳細資訊、請參閱 "建立持續儲存區"。

步驟

1. 建立FPolicy原則：

```
vserver fpolicy policy create -vserver-name vserver_name -policy-name
policy_name -engine engine_name -events event_name, [-persistent-store
PS_name] [-is-mandatory {true|false}] [-allow-privileged-access {yes|no}] [-
privileged-user-name domain\user_name] [-is-passthrough-read-enabled
{true|false}]
```

   - 您可以將一或多個事件新增至FPolicy原則。
   - 預設會啟用強制篩選。
   - 如果您想要透過設定來允許特殊權限存取 `-allow-privileged-access` 參數至 `yes`、您也必須設定權限使用者名稱以進行權限存取。
   - 如果您想要設定 Passthrough-read 、請設定 `-is-passthrough-read-enabled` 參數至 `true`、您也

必須設定特殊權限資料存取。

下列命令會建立名為「policy1'」的原則、其事件名稱為「EVENT1」、外部引擎名稱為「engine 1'」。此原則會在原則組態中使用預設值：
`vserver fpolicy policy create -vserver vs1.example.com -policy-name policy1 -events event1 -engine engine1`

下列命令會建立名為「policy2」的原則、其事件名稱為「'Event2」、外部引擎名稱為「engine 2」。此原則設定為使用指定的使用者名稱來使用權限存取。Passthsthread-read已啟用：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name policy2
-events event2 -engine engine2 -allow-privileged-access yes -privileged-
user-name example\archive_acct -is-passthrough-read-enabled true
```

下列命令會建立名為「native1」的原則、並將事件命名為「事件3」。此原則使用原生引擎、並在原則組態中使用預設值：

```
vserver fpolicy policy create -vserver vs1.example.com -policy-name native1
-events event3 -engine native
```

2. 使用驗證 FPolicy 原則組態 `vserver fpolicy policy show` 命令。

下列命令會顯示有關三個已設定的FPolicy原則的資訊、包括下列資訊：

- 與原則相關聯的SVM
- 與原則相關聯的外部引擎
- 與原則相關的事件
- 是否需要強制篩選
- 是否需要權限存取
  `vserver fpolicy policy show`

```
   Vserver       Policy     Events    Engine    Is Mandatory  Privileged
                 Name                                       Access
--------------   ---------  --------- --------- ------------
-----------
vs1.example.com  policy1    event1    engine1   true          no
vs1.example.com  policy2    event2    engine2   true          yes
vs1.example.com  native1    event3    native    true          no
```

建立 **ONTAP FPolicy** 範圍

建立FPolicy原則之後、您需要建立FPolicy範圍。建立範圍時、您會將範圍與FPolicy原則建立關聯。範圍會定義套用FPolicy原則的界限。範圍可以根據共用、匯出原則、磁碟區和副檔名來包含或排除檔案。

開始之前

必須填寫FPolicy範圍工作表。FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺

服器）、且必須至少有一個關聯的FPolicy事件。

步驟

1. 使用建立 FPolicy 範圍 `vserver fpolicy policy scope create` 命令。

```
vserver fpolicy policy scope create -vserver-name vs1.example.com -policy-name
policy1 -volumes-to-include datavol1,datavol2
```

2. 使用驗證 FPolicy 範圍組態 `vserver fpolicy policy scope show` 命令。

```
vserver fpolicy policy scope show -vserver vs1.example.com -instance
```

```
                    Vserver: vs1.example.com
                     Policy: policy1
          Shares to Include: -
          Shares to Exclude: -
         Volumes to Include: datavol1, datavol2
         Volumes to Exclude: -
 Export Policies to Include: -
 Export Policies to Exclude: -
 File Extensions to Include: -
 File Extensions to Exclude: -
```

啟用 **ONTAP FPolicy** 策略

完成FPolicy原則組態設定之後、您就可以啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。

開始之前

FPolicy原則必須與關聯的外部引擎一起存在（如果原則設定為使用外部FPolicy伺服器）、且必須至少有一個關聯的FPolicy事件。FPolicy原則範圍必須存在、而且必須指派給FPolicy原則。

關於這項工作

當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。

無法在管理SVM上啟用原則。

步驟

1. 使用啟用 FPolicy 原則 `vserver fpolicy enable` 命令。

```
vserver fpolicy enable -vserver-name vs1.example.com -policy-name policy1
-sequence-number 1
```

2. 使用確認 FPolicy 原則已啟用 `vserver fpolicy show` 命令。

```
vserver fpolicy show -vserver vs1.example.com
```

```
                                    Sequence
Vserver          Policy Name          Number  Status   Engine
---------------  ----------------- --------  -------- ---------
vs1.example.com  policy1                   1  on       engine1
```

管理 FPolicy 組態

修改FPolicy組態

在 ONTAP 中修改 FPolicy 配置的命令

您可以修改組成組態的元素、以修改FPolicy組態。您可以修改外部引擎、 FPolicy 事件、 FPolicy 範圍、 FPolicy 持續儲存區和 FPolicy 原則。您也可以啟用或停用FPolicy原則。當您停用FPolicy原則時、該原則的檔案監控將會中斷。

您應該先停用 FPolicy 原則、再修改其組態。

如果您要修改...	使用此命令...
外部引擎	`vserver fpolicy policy external-engine modify`
活動	`vserver fpolicy policy event modify`
範圍	`vserver fpolicy policy scope modify`
持續儲存區	`vserver fpolicy persistent-store modify`
原則	`vserver fpolicy policy modify`

如"指令參考資料ONTAP"需詳細 `vserver fpolicy policy`資訊，請參閱。

啟用或停用 ONTAP FPolicy 策略

您可以在組態完成後啟用FPolicy原則。啟用原則會設定其優先順序、並開始監控原則的檔案存取。若要停止原則的檔案存取監控、您可以停用FPolicy原則。

開始之前

在啟用FPolicy原則之前、必須先完成FPolicy組態。

關於這項工作

- 當在儲存虛擬機器（SVM）上啟用多個原則、且有多個原則已訂閱相同的檔案存取事件時、就會使用優先順序。
- 使用原生引擎組態的原則優先順序高於任何其他引擎的原則、無論啟用原則時指派給它們的順序編號為何。
- 若要變更FPolicy原則的優先順序、您必須停用該原則、然後使用新的順序編號重新啟用。

步驟

1. 執行適當的行動：

如果您想要...	輸入下列命令...
啟用FPolicy原則	`vserver fpolicy enable -vserver-name vserver_name -policy-name policy_name -sequence-number integer`
停用FPolicy原則	`vserver fpolicy disable -vserver-name vserver_name -policy-name policy_name`

顯示FPolicy組態的相關資訊

了解 ONTAP FPolicy 顯示命令

在顯示有關 FPolicy 組態的資訊以瞭解的方式時、這很有幫助 `show` 命令運作正常。

答 `show` 不含其他參數的命令會以摘要形式顯示資訊。此外、每個 `show` Command 具有相同的兩個互斥選擇性參數、 `-instance` 和 `-fields`。

當您使用時 `-instance` 參數與 `show` 命令時、命令輸出會以清單格式顯示詳細資訊。在某些情況下、詳細輸出可能會很長、而且包含的資訊比您需要的還多。您可以使用 `-fields fieldname[,fieldname…]` 此參數可自訂輸出、使其僅顯示指定欄位的資訊。您可以輸入來識別您可以指定的欄位 `?` 之後 `-fields` 參數。

的輸出 `show` 命令 `-fields` 參數可能會顯示與所要求欄位相關的其他相關和必要欄位。

每個 `show` 命令具有一個或多個可選參數，用於篩選輸出結果，並使您能夠縮小命令輸出中顯示的信息範圍。您可以輸入、識別命令可使用的選用參數 `?` 之後 `show` 命令。

。 `show` 命令支援 UNIX 樣式的模式和萬用字元、可讓您在命令參數引數中比對多個值。例如、您可以使用萬用字元運算子（*）、非運算子（！）、OR運算子（|）、範圍運算子（integer…integer）、小於運算子（<）、大於運算子（>）、小於或等於運算子（<=）、以及大於或等於運算子（>=）來指定值。

如需使用UNIX樣式模式和萬用字元的詳細資訊、請參閱 使用ONTAP 指令行介面。

用於在 ONTAP 中顯示 FPolicy 組態資訊的命令

您可以使用 `fpolicy show` 顯示 FPolicy 組態相關資訊的命令、包括有關 FPolicy 外部引擎、事件、範圍和原則的資訊。

如果您要顯示FPolicy的相關資訊...	使用此命令...
外部引擎	`vserver fpolicy policy external-engine show`
活動	`vserver fpolicy policy event show`
範圍	`vserver fpolicy policy scope show`

原則	`vserver fpolicy policy show`

如"指令參考資料ONTAP"需詳細 `vserver fpolicy policy`資訊，請參閱。

顯示有關 **ONTAP FPolicy** 策略狀態的信息

您可以顯示FPolicy原則狀態的相關資訊、以判斷原則是否已啟用、原則要使用的外部引擎、原則的順序編號、以及FPolicy原則與哪個儲存虛擬機器（SVM）相關聯。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則順序編號
- 原則狀態

除了顯示叢集或特定SVM上所設定之FPolicy原則的原則狀態資訊、您也可以使用命令參數、依其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 參數、僅顯示命令輸出或中指定的欄位 `-fields ?` 決定您可以使用哪些欄位。

步驟

1. 使用適當的命令顯示FPolicy原則狀態的篩選資訊：

如果您要顯示原則的狀態資訊…	輸入命令…
在叢集上	`vserver fpolicy show`
具有指定狀態的	`vserver fpolicy show -status {on
off}`	在指定的SVM上
`vserver fpolicy show -vserver vserver_name`	使用指定的原則名稱
`vserver fpolicy show -policy-name policy_name`	使用指定的外部引擎

範例

下列範例顯示叢集上FPolicy原則的相關資訊：

```
cluster1::> vserver fpolicy show
                                        Sequence
Vserver              Policy Name          Number  Status      Engine
-------------------- -------------------- --------  ---------   ---------
FPolicy              cserver_policy       -         off         eng1
vs1.example.com      v1p1                 -         off         eng2
vs1.example.com      v1p2                 -         off         native
vs1.example.com      v1p3                 -         off         native
vs1.example.com      cserver_policy       -         off         eng1
vs2.example.com      v1p1                 3         on          native
vs2.example.com      v1p2                 1         on          eng3
vs2.example.com      cserver_policy       2         on          eng1
```

顯示有關已啟用的 **ONTAP FPolicy** 策略的信息

您可以顯示已啟用FPolicy原則的相關資訊、以判斷其設定使用的FPolicy外部引擎、原則的優先順序、以及FPolicy原則關聯的儲存虛擬機器（SVM）。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 原則名稱
- 原則優先順序

您可以使用命令參數、根據指定的條件篩選命令的輸出。

步驟

1. 使用適當的命令顯示已啟用的FPolicy原則相關資訊：

如果您要顯示已啟用原則的相關資訊...	輸入命令...
在叢集上	`vserver fpolicy show-enabled`
在指定的SVM上	`vserver fpolicy show-enabled -vserver vserver_name`
使用指定的原則名稱	`vserver fpolicy show-enabled -policy-name policy_name`
使用指定的序號	`vserver fpolicy show-enabled -priority integer`

範例

下列範例顯示叢集上已啟用FPolicy原則的相關資訊：

```
cluster1::> vserver fpolicy show-enabled
Vserver                 Policy Name               Priority

----------------------- ------------------------- ----------
vs1.example.com         pol_native                native
vs1.example.com         pol_native2               native
vs1.example.com         pol1                      2
vs1.example.com         pol2                      4
```

管理FPolicy伺服器連線

連線至 ONTAP 中的外部 FPolicy 伺服器

若要啟用檔案處理、您可能需要手動連線至外部FPolicy伺服器（如果先前已終止連線）。連線會在伺服器逾時後終止、或因為發生錯誤而終止。或者、系統管理員也可以手動終止連線。

關於這項工作

如果發生嚴重錯誤、則可終止與FPolicy伺服器的連線。解決造成嚴重錯誤的問題之後、您必須手動重新連線至FPolicy伺服器。

步驟

1. 使用連線至外部 FPolicy 伺服器 `vserver fpolicy engine-connect` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy engine-connect`資訊，請參閱。

2. 使用確認外部 FPolicy 伺服器已連線 `vserver fpolicy show-engine` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy show-engine`資訊，請參閱。

中斷與 ONTAP 中外部 FPolicy 伺服器的連線

您可能需要手動中斷與外部FPolicy伺服器的連線。如果FPolicy伺服器在處理通知要求時發生問題、或是您需要在FPolicy伺服器上執行維護、則可能需要這樣做。

步驟

1. 使用中斷與外部 FPolicy 伺服器的連線 `vserver fpolicy engine-disconnect` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy engine-disconnect`資訊，請參閱。

2. 使用確認外部 FPolicy 伺服器已中斷連線 `vserver fpolicy show-engine` 命令。

   如"指令參考資料ONTAP"需詳細 `vserver fpolicy show-engine`資訊，請參閱。

您可以顯示叢集或特定儲存虛擬機器（SVM）與外部FPolicy伺服器（FPolicy伺服器）連線的狀態資訊。此資訊可協助您判斷哪些FPolicy伺服器已連線。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- 節點名稱
- FPolicy原則名稱
- FPolicy伺服器IP位址
- FPolicy伺服器狀態
- FPolicy伺服器類型

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示FPolicy伺服器的連線狀態資訊…	輸入…
您指定的	`vserver fpolicy show-engine -server IP_address`
適用於指定的SVM	`vserver fpolicy show-engine -vserver vserver_name`
隨附於指定原則的	`vserver fpolicy show-engine -policy-name policy_name`
使用您指定的伺服器狀態	`vserver fpolicy show-engine -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected` • `connecting` • `disconnecting`

使用指定類型	`vserver fpolicy show-engine -server-type type` FPolicy伺服器類型可以是下列其中一種： • `primary` • `secondary`
已中斷連線的原因	`vserver fpolicy show-engine -disconnect-reason text` 中斷連線可能有多種原因。以下是中斷連線的常見原因： • `Disconnect command received from CLI.` • `Error encountered while parsing notification response from FPolicy server.` • `FPolicy Handshake failed.` • `SSL handshake failed.` • `TCP Connection to FPolicy server failed.` • `The screen response message received from the FPolicy server is not valid.`

範例

此範例顯示SVM vs1.example.com上的FPolicy伺服器外部引擎連線相關資訊：

```
cluster1::> vserver fpolicy show-engine -vserver vs1.example.com
FPolicy                                              Server-       Server-
Vserver         Policy    Node         Server        status        type
--------------- --------- ------------ ------------- -------------
---------
vs1.example.com policy1   node1        10.1.1.2      connected     primary
vs1.example.com policy1   node1        10.1.1.3      disconnected  primary
vs1.example.com policy1   node2        10.1.1.2      connected     primary
vs1.example.com policy1   node2        10.1.1.3      disconnected  primary
```

此範例僅顯示連線的FPolicy伺服器相關資訊：

```
cluster1::> vserver fpolicy show-engine -fields server -server-status
connected
node       vserver         policy-name server
---------- --------------- ----------- -------
node1      vs1.example.com policy1     10.1.1.2
node2      vs1.example.com policy1     10.1.1.2
```

顯示有關 **ONTAP FPolicy** 直通讀取連線狀態的信息

您可以針對叢集或特定儲存虛擬機器（SVM）、顯示與外部FPolicy伺服器（FPolicy伺服器）的FPolicy Passthrough-read連線狀態相關資訊。此資訊可協助您判斷哪些FPolicy伺服器具有直通讀取資料連線、以及哪些FPolicy伺服器的直通讀取連線中斷。

關於這項工作

如果未指定任何參數、命令會顯示下列資訊：

- SVM名稱
- FPolicy原則名稱
- 節點名稱
- FPolicy伺服器IP位址
- FPolicy Passthrough-read連線狀態

除了顯示叢集或特定SVM上FPolicy連線的相關資訊、您也可以使用命令參數、根據其他條件篩選命令的輸出。

您可以指定 `-instance` 顯示所列原則詳細資訊的參數。或者、您也可以使用 `-fields` 此參數僅顯示命令輸出中指定的欄位。您可以輸入 `?` 之後 `-fields` 參數來找出您可以使用的欄位。

步驟

1. 使用適當的命令、顯示節點與FPolicy伺服器之間連線狀態的篩選資訊：

如果您要顯示有關…的連線狀態資訊	輸入命令…
叢集的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection`
指定SVM的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -vserver vserver_name`
指定原則的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name`
指定原則的詳細FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -instance`

您指定狀態的FPolicy Passthrough-read連線狀態	`vserver fpolicy show-passthrough-read-connection -policy-name policy_name -server-status status` 伺服器狀態可以是下列其中一項： • `connected` • `disconnected`

範例

下列命令會顯示叢集上所有FPolicy伺服器的Passthrough-read連線相關資訊：

```
cluster1::> vserver fpolicy show-passthrough-read-connection
                                          FPolicy           Server
Vserver          Policy Name   Node       Server            Status
---------------  ------------ ----------- -----------------
--------------
vs2.example.com  pol_cifs_2    FPolicy-01  2.2.2.2           disconnected
vs1.example.com  pol_cifs_1    FPolicy-01  1.1.1.1           connected
```

下列命令會顯示「'pol_CIFS _1'」原則中所設定之FPolicy伺服器的Passthrough-read連線詳細資訊：

```
cluster1::> vserver fpolicy show-passthrough-read-connection -policy-name
pol_cifs_1 -instance

                                       Node: FPolicy-01
                                    Vserver: vs1.example.com
                                     Policy: pol_cifs_1
                                     Server: 1.1.1.1
               Session ID of the Control Channel: 8cef052e-2502-11e3-
88d4-123478563412
                                Server Status: connected
      Time Passthrough Read Channel was Connected: 9/24/2013 10:17:45
   Time Passthrough Read Channel was Disconnected: -
Reason for Passthrough Read Channel Disconnection: none
```

使用安全性追蹤來驗證存取

了解 **ONTAP** 安全追蹤

您可以新增權限追蹤篩選器、以指示ONTAP Sfin記錄儲存虛擬機器（SVM）上SMB和NFS伺服器為何允許或拒絕用戶端或使用者執行作業的要求。當您想要驗證檔案存取安全性配置是否適當、或是想要疑難排解檔案存取問題時、這項功能就很實用。

安全追蹤可讓您設定篩選器、偵測SVM上SMB和NFS上的用戶端作業、並追蹤符合該篩選器的所有存取檢查。然後您可以檢視追蹤結果、以方便的方式摘要說明允許或拒絕存取的原因。

當您想要驗證SVM上檔案和資料夾的SMB或NFS存取安全性設定、或是遇到存取問題時、可以快速新增篩選器來開啟權限追蹤。

下列清單概述安全追蹤運作方式的重要事實：

- 在SVM層級套用安全追蹤。ONTAP
- 每個傳入要求都會經過篩選、以查看是否符合任何已啟用安全追蹤的篩選條件。
- 檔案和資料夾存取要求都會執行追蹤。
- 追蹤可以根據下列準則進行篩選：
  - 用戶端 IP
  - SMB或NFS路徑
  - Windows名稱
  - UNIX 名稱
- 系統會針對「允許_」和「拒絕_」存取回應結果進行篩選。
- 每個符合已啟用追蹤篩選條件的要求、都會記錄在追蹤結果記錄中。
- 儲存管理員可在篩選器上設定逾時、以自動停用篩選器。
- 如果某個要求符合多個篩選器、則會記錄索引編號最高的篩選器結果。
- 儲存管理員可從追蹤結果記錄列印結果、以判斷允許或拒絕存取要求的原因。

ONTAP SVM 上的存取檢查安全追蹤監視器的類型

檔案或資料夾的存取檢查是根據多個準則進行。安全追蹤會監控所有這些準則的作業。

安全追蹤監控的存取檢查類型包括：

- Volume與qtree安全樣式
- 檔案系統的有效安全性、其中包含要求執行作業的檔案和資料夾
- 使用者對應
- 共用層級權限
- 匯出層級權限
- 檔案層級權限
- 儲存層級的存取保護安全性

在 ONTAP SVM 上建立安全追蹤時的注意事項

在儲存虛擬機器（SVM）上建立安全追蹤時、請謹記幾個考量事項。例如、您需要知道可以建立追蹤的通訊協定、支援哪些安全性樣式、以及最大作用中追蹤數量。

- 您只能在SVM上建立安全追蹤。

- 每個安全性追蹤篩選器項目都是SVM專屬項目。

  您必須指定要在其中執行追蹤的SVM。

- 您可以新增SMB和NFS要求的權限追蹤篩選器。
- 您必須在要建立追蹤篩選器的SVM上設定SMB或NFS伺服器。
- 您可以為位於NTFS、UNIX及混合式安全型磁碟區和qtree上的檔案和資料夾建立安全追蹤。
- 每個SVM最多可新增10個權限追蹤篩選器。
- 建立或修改篩選時、必須指定篩選索引編號。

  篩選條件會依索引編號的順序進行考量。索引編號較高的篩選條件、會在索引編號較低的條件之前考量。如果要追蹤的要求符合多個已啟用篩選器中的條件、則只會觸發索引編號最高的篩選器。

- 建立並啟用安全性追蹤篩選器之後、您必須在用戶端系統上執行部分檔案或資料夾要求、以產生追蹤篩選器可擷取並登入追蹤結果記錄的活動。
- 您應該新增權限追蹤篩選器、僅供檔案存取驗證或疑難排解之用。

  新增權限追蹤篩選器對控制器效能的影響不大。

  完成驗證或疑難排解活動後、您應該停用或移除所有權限追蹤篩選器。此外、您選取的篩選條件應盡可能明確、ONTAP 以便不將大量的追蹤結果傳送到記錄檔。

執行安全追蹤

學習執行 **ONTAP** 安全追蹤

執行安全性追蹤包括建立安全性追蹤篩選器、驗證篩選條件、在符合篩選條件的SMB或NFS用戶端上產生存取要求、以及檢視結果。

完成使用安全篩選器擷取追蹤資訊之後、您可以修改篩選器並重複使用、或是在不再需要時停用篩選器。檢視及分析篩選追蹤結果之後、您可以在不再需要時將其刪除。

在 **ONTAP SVM** 中建立安全追蹤過濾器

您可以建立安全追蹤篩選器、以偵測儲存虛擬機器（SVM）上的SMB和NFS用戶端作業、並追蹤符合篩選器的所有存取檢查。您可以使用安全追蹤的結果來驗證組態或疑難排解存取問題。

關於這項工作

Vserver安全追蹤篩選器create命令需要兩個參數：

必要參數	說明
`-vserver vserver_name`	*SVM*名稱 包含您要套用安全性追蹤篩選器之檔案或資料夾的SVM名稱。

`-index index_number`	篩選索引編號_ 要套用至篩選的索引編號。每個SVM最多可有10個追蹤篩選器。此參數允許的值為1到10。

許多選用的篩選參數可讓您自訂安全性追蹤篩選器、以便縮小安全性追蹤所產生的結果：

篩選參數	說明
`-client-ip IP_Address`	此篩選器會指定使用者存取SVM的IP位址。
`-path path`	此篩選器會指定要套用權限追蹤篩選器的路徑。的價值 `-path` 可以使用下列其中一種格式： • 完整路徑、從共用區根目錄或匯出開始 • 部分路徑、相對於共用的根目錄 您必須在路徑值中使用NFS樣式目錄UNIX型目錄分隔符號。
`-windows-name win_user_name` 或 `-unix -name``unix_user_name`	您可以指定要追蹤其存取要求的Windows使用者名稱或UNIX使用者名稱。使用者名稱變數不區分大小寫。您無法在同一個篩選器中同時指定Windows使用者名稱和UNIX使用者名稱。 即使您可以追蹤SMB和NFS存取事件、對應的UNIX使用者和對應的UNIX使用者群組也可以在混合或UNIX安全型資料上執行存取檢查。
`-trace-allow {yes`	`no}`
安全性追蹤篩選器一律會啟用拒絕事件追蹤。您可以選擇追蹤允許事件。若要追蹤允許事件、請將此參數設為 `yes`。	`-enabled {enabled`
`disabled}`	您可以啟用或停用安全性追蹤篩選器。依預設、安全性追蹤篩選器為啟用狀態。
`-time-enabled integer`	您可以指定篩選器的逾時時間、之後篩選器就會停用。

步驟

1. 建立安全追蹤篩選器：

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters` 為選用篩選參數清單。

如"指令參考資料ONTAP"需詳細 `vserver security trace filter create`資訊，請參閱。

2. 驗證安全性追蹤篩選器項目：

```
vserver security trace filter show -vserver vserver_name -index index_number
```

範例

下列命令會為任何使用者建立安全性追蹤篩選器、以存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt` 從 IP 位址 10.10.10.7 。篩選器使用的完整路徑 `-path` 選項。用於存取資料的用戶端IP位址為10.10.10.7.篩選器在30分鐘後逾時：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

下列命令會使用的相對路徑來建立安全性追蹤篩選器 `-path` 選項。篩選器會追蹤名為「'joe'」之Windows使用者的存取權。Joe 正在存取具有共用路徑的檔案 `\\server\share1\dir1\dir2\file.txt`。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                              Vserver: vs1
                         Filter Index: 2
            Client IP Address to Match: -
                                  Path: /dir1/dir2/file.txt
                  Windows User Name: mydomain\joe
                     UNIX User Name: -
                  Trace Allow Events: yes
                      Filter Enabled: enabled
             Minutes Filter is Enabled: 60
```

顯示有關 **ONTAP SVM** 中的安全追蹤過濾器的信息

您可以顯示儲存虛擬機器（SVM）上設定的安全追蹤篩選器相關資訊。這可讓您查看每個篩選器追蹤的存取事件類型。

步驟

1. 使用顯示安全性追蹤篩選項目的相關資訊 `vserver security trace filter show` 命令。

如"指令參考資料ONTAP"需詳細 `vserver security trace filter show`資訊，請參閱。

範例

下列命令會顯示SVM VS1上所有安全追蹤篩選器的相關資訊：

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

在 **ONTAP SVM** 中顯示安全性追蹤結果

您可以顯示針對符合安全性追蹤篩選器的檔案作業所產生的安全性追蹤結果。您可以使用結果來驗證檔案存取安全性組態、或疑難排解SMB和NFS檔案存取問題。

開始之前

啟用的安全性追蹤篩選器必須存在、而且必須從SMB或NFS用戶端執行作業、且該用戶端必須符合安全性追蹤篩選器、才能產生安全性追蹤結果。

關於這項工作

您可以顯示所有安全性追蹤結果的摘要、也可以指定選用參數來自訂輸出中顯示的資訊。當安全性追蹤結果包含大量記錄時、這一點很有幫助。

如果您未指定任何選用參數、則會顯示下列項目：

- 儲存虛擬機器（SVM）名稱
- 節點名稱
- 安全性追蹤索引編號
- 安全風格
- 路徑
- 理由
- 使用者名稱

  使用者名稱會根據追蹤篩選器的設定方式顯示：

如果篩選器已設定…	然後…
使用UNIX使用者名稱	安全性追蹤結果會顯示UNIX使用者名稱。

使用Windows使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。
沒有使用者名稱	安全性追蹤結果會顯示Windows使用者名稱。

您可以使用選用參數來自訂輸出。您可以使用某些選用參數來縮小命令輸出中傳回的結果範圍、其中包括：

選用參數	說明
`-fields field_name、 ...`	在您選擇的欄位上顯示輸出。您可以單獨使用此參數、也可以搭配其他選用參數一起使用。
`-instance`	顯示安全性追蹤事件的詳細資訊。此參數可搭配其他選用參數使用、以顯示特定篩選結果的詳細資訊。
`-node node_name`	僅顯示有關指定節點上事件的資訊。
`-vserver vserver_name`	僅顯示指定SVM上事件的相關資訊。
`-index integer`	顯示與指定索引編號對應之篩選器所產生之事件的相關資訊。
`-client-ip IP_address`	顯示從指定用戶端IP位址存取檔案所發生事件的相關資訊。
`-path path`	顯示因檔案存取指定路徑而發生事件的相關資訊。
`-user-name user_name`	顯示指定Windows或UNIX使用者存取檔案時所發生事件的相關資訊。
`-security-style security_style`	顯示在具有指定安全樣式的檔案系統上發生事件的相關資訊。

如需其他選用參數的詳細"指令參考資料ONTAP"資訊，請參閱。

步驟

1. 使用顯示安全性追蹤篩選結果 `vserver security trace trace-result show` 命令。

```
vserver security trace trace-result show -user-name domain\user
```

```
Vserver: vs1

Node     Index   Filter Details          Reason
-------- ------- ---------------------  ----------------------------
node1    3       User:domain\user       Access denied by explicit ACE
                 Security Style:mixed
                 Path:/dir1/dir2/

node1    5       User:domain\user       Access denied by explicit ACE
                 Security Style:unix
                 Path:/dir1/
```

修改 **ONTAP SVM** 上的安全性追蹤過濾器

如果您想要變更選用的篩選參數、以決定追蹤哪些存取事件、您可以修改現有的安全性追蹤篩選器。

關於這項工作

您必須指定要套用篩選器的儲存虛擬機器（SVM）名稱、以及篩選器的索引編號、以識別要修改的安全性追蹤篩選器。您可以修改所有選用的篩選參數。

步驟

1. 修改安全性追蹤篩選器：

   ```
   vserver security trace filter modify -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   - `vserver_name` 是要套用安全性追蹤篩選器的 SVM 名稱。
   - `index_number` 是您要套用至篩選的索引編號。此參數允許的值為1到10。
   - `filter_parameters` 為選用篩選參數清單。

2. 驗證安全性追蹤篩選器項目：

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

範例

下列命令會修改索引編號為1的安全性追蹤篩選器。篩選器會追蹤任何使用者存取具有共用路徑之檔案的事件 `\\server\share1\dir1\dir2\file.txt` 來自任何 IP 位址。篩選器使用的完整路徑 `-path` 選項。篩選器追蹤會允許及拒絕事件：

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                     Trace Allow Events: yes
                        Filter Enabled: enabled
                Minutes Filter is Enabled: 60
```

刪除 **ONTAP SVM** 上的安全性追蹤過濾器

當您不再需要安全性追蹤篩選器項目時、可以將其刪除。由於每個儲存虛擬機器（SVM）最多可有10個安全追蹤篩選器、因此刪除不需要的篩選器後、您就能在達到上限時建立新的篩選器。

關於這項工作

若要唯一識別您要刪除的安全性追蹤篩選器、您必須指定下列項目：

- 套用追蹤篩選器的SVM名稱
- 追蹤篩選器的篩選索引編號

步驟

1. 識別您要刪除之安全性追蹤篩選器項目的篩選器索引編號：

   ```
   vserver security trace filter show -vserver vserver_name
   ```

   ```
   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. 使用上一個步驟的篩選索引編號資訊、刪除篩選項目：

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number
   ```

```
vserver security trace filter delete -vserver vs1 -index 1
```

3. 確認安全性追蹤篩選器項目已刪除：

```
vserver security trace filter show -vserver vserver_name
```

```
vserver security trace filter show -vserver vs1
```

```
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        2    -            /dir3/dir4/                 no
mydomain\joe
```

刪除 **ONTAP SVM** 上的安全性追蹤記錄

使用篩選器追蹤記錄來驗證檔案存取安全性或疑難排解SMB或NFS用戶端存取問題之後、您可以從安全性追蹤記錄中刪除安全性追蹤記錄。

關於這項工作

在刪除安全性追蹤記錄之前、您必須知道記錄的序號。

> 每個儲存虛擬機器（SVM）最多可儲存128筆追蹤記錄。如果SVM達到上限、則會在新增追蹤記錄時自動刪除最舊的追蹤記錄。如果您不想手動刪除此SVM上的追蹤記錄、ONTAP 可讓SVM在達到最大值後自動刪除最舊的追蹤結果、以便留出新結果的空間。

步驟

1. 識別您要刪除的記錄序號：

```
vserver security trace trace-result show -vserver vserver_name -instance
```

2. 刪除安全性追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name -seqnum integer
```

```
vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
999
```

   - `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。

     這是必要的參數。

   - `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的 SVM 名稱。

     這是必要的參數。

- `-seqnum integer` 為您要刪除的記錄事件序號。

  這是必要的參數。

刪除 **ONTAP SVM** 上的所有安全追蹤記錄

如果您不想保留任何現有的安全性追蹤記錄、可以使用單一命令刪除節點上的所有記錄。

步驟

1. 刪除所有安全追蹤記錄：

```
vserver security trace trace-result delete -node node_name -vserver
vserver_name *
```

   - `-node node_name` 是您要刪除之權限追蹤事件所在的叢集節點名稱。
   - `-vserver vserver_name` 是您要刪除之權限追蹤事件所在的儲存虛擬機器（ SVM ）名稱。

解釋 **ONTAP** 安全追蹤結果

安全性追蹤結果提供允許或拒絕要求的原因。輸出會結合允許或拒絕存取的原因、以及允許或拒絕存取的存取檢查路徑中的位置、來顯示結果。您可以使用結果來隔離及識別為何允許或不允許採取行動。

尋找結果類型清單和篩選詳細資料的相關資訊

您可以在命令的安全性追蹤結果中找到結果類型清單和篩選詳細資料 `vserver security trace trace-result show`。如"指令參考資料ONTAP"需詳細 `vserver security trace trace-result show`資訊，請參閱。

的輸出範例 `Reason` 欄位 `Allow` 結果類型

以下是的輸出範例 `Reason` 出現在追蹤結果中的欄位會登入 `Allow` 結果類型：

```
Access is allowed because SMB implicit permission grants requested
access while opening existing file or directory.
```

```
Access is allowed because NFS implicit permission grants requested
access while opening existing file or directory.
```

的輸出範例 `Reason` 欄位 `Allow` 結果類型

以下是的輸出範例 `Reason` 出現在追蹤結果中的欄位會登入 `Deny` 結果類型：

```
Access is denied. The requested permissions are not granted by the
ACE while checking for child-delete access on the parent.
```

的輸出範例 `Filter details` 欄位

以下是的輸出範例 `Filter details` 追蹤結果記錄中的欄位、其中列出檔案系統的有效安全樣式、其中包含符合篩選條件的檔案和資料夾：

```
Security Style: MIXED and ACL
```

在哪裡可以找到有關 **ONTAP SVM** 的更多信息

成功測試 SMB 用戶端存取之後、您可以執行進階 SMB 組態或新增 SAN 存取。成功測試NFS用戶端存取之後、您可以執行進階NFS組態或新增SAN存取。傳輸協定存取完成時、您應該保護SVM的根Volume。

SMB 組態

您可以使用下列項目來進一步設定SMB存取：

- "中小企業管理"

  說明如何使用 SMB 通訊協定來設定及管理檔案存取。

- "NetApp技術報告4191：叢集Data ONTAP 式更新的最佳實務做法指南8.2 Windows檔案服務"

  提供SMB實作與其他Windows檔案服務功能的簡短概述、並提供ONTAP 有關的建議與基本疑難排解資訊。

- "NetApp技術報告3740：SMB 2 Next-Generation CIFS Protocol in Data ONTAP"

  介紹SMB 2的功能、組態詳細資料、以及ONTAP 其在功能方面的實作。

NFS 組態

您可以使用下列項目進一步設定NFS存取：

- "NFS管理"

  說明如何使用NFS傳輸協定來設定及管理檔案存取。

- "NetApp技術報告4067：NFS最佳實務與實作指南"

  可做為NFSv3和NFSv3作業指南、提供ONTAP 關於以NFSv3為焦點的各種作業系統的概述。

- "NetApp技術報告4668：名稱服務最佳實務做法指南"

  提供完整的最佳實務做法、限制、建議及考量清單、以供設定LDAP、NIS、DNS及本機使用者與群組檔案進行驗證。

- "NetApp技術報告4616：ONTAP NFS Kerberos in Some with Microsoft Active Directory"
- "NetApp技術報告4835：如何在ONTAP 功能方面設定LDAP"
- "NetApp技術報告3580：NFSv4增強功能與最佳實務做法指南Data ONTAP -實作"

說明在掛接到執行ONTAP 此功能的系統上、在AIX、Linux或Solaris用戶端上實作NFSv4元件時應遵循的最佳實務做法。

根**Volume**保護

在SVM上設定傳輸協定之後、您應確保其根Volume受到保護：

- "資料保護"

  說明如何建立負載共用鏡像來保護SVM根磁碟區、這是NetApp啟用NAS的SVM最佳實務做法。同時也說明如何從負載共用鏡像中提升SVM根磁碟區、以快速從磁碟區故障或損失中恢復。

使用System Manager管理加密

使用基於軟體的加密對**ONTAP**叢集中儲存的資料進行加密

使用Volume加密功能、可確保在基礎裝置被重新調整用途、退回、放錯地方或遭竊時、無法讀取Volume資料。Volume加密不需要特殊磁碟、可搭配所有HDD和SSD使用。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"啟用軟體級加密。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

Volume加密需要金鑰管理程式。您可以使用System Manager來設定Onboard Key Manager。您也可以使用外部金鑰管理程式、但必須先使用ONTAP CLI進行設定。

設定金鑰管理程式之後、新的磁碟區預設會加密。

步驟

1. 按一下*叢集>設定*。
2. 在 * 加密 * 下、按一下 以首次設定 Onboard Key Manager 。
3. 若要加密現有磁碟區、請按一下*儲存>磁碟區*。
4. 在所需的磁碟區上、按一下、然後按一下 * 編輯 * 。
5. 選取*啟用加密*。

使用自加密磁碟機加密**ONTAP**叢集中儲存的數據

使用磁碟加密可確保當基礎裝置被重新調整用途、退回、放錯位置或遭竊時、無法讀取本機層級中的所有資料。磁碟加密需要特殊的自我加密HDD或SSD。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"啟用硬體級加密。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

磁碟加密需要金鑰管理程式。您可以使用System Manager設定內建金鑰管理程式。 您也可以使用外部金鑰管理程式、但必須先使用ONTAP CLI進行設定。

如果ONTAP 偵測到自我加密磁碟、當您建立本機層時、系統會提示您設定內建金鑰管理程式。

步驟

1. 在 * 加密 * 下、按一下 以設定內建金鑰管理程式。
2. 如果您看到需要重新輸入磁碟的訊息，請按一下，然後按一下 * 重新輸入磁碟 * 。

使用CLI管理加密

了解ONTAP資料加密

NetApp同時提供軟體與硬體加密技術、確保儲存媒體在重新調整用途、退回、放錯地方或遭竊時、無法讀取閒置的資料。

- 使用NetApp Volume Encryption（NVE）的軟體式加密可一次支援一個磁碟區的資料加密
- 使用NetApp儲存加密（NSE）的硬體式加密可支援寫入資料時的全磁碟加密（FDE）。

配置NetApp捲和聚合加密

了解ONTAP NetApp捲和聚合加密

NetApp Volume Encryption（NVE）是一項軟體技術、可一次加密閒置一個磁碟區的資料。只有儲存系統才能存取的加密金鑰、可確保在基礎裝置重新調整用途、退回、放錯位置或遭竊時、無法讀取Volume資料。

瞭解NVE

使用 NVE 時，中繼資料和資料（包括快照）都會加密。資料的存取權是由唯一的XTS-AES-256金鑰提供、每個磁碟區一個金鑰。外部金鑰管理伺服器或 Onboard Key Manager （ OKM ）可為節點提供金鑰：

- 外部金鑰管理伺服器是儲存環境中的第三方系統、使用金鑰管理互通性傳輸協定（KMIP）為節點提供金鑰。最佳實務做法是在不同的儲存系統上設定外部金鑰管理伺服器與資料。
- 內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供金鑰。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAPVE 授權隨附於"ONTAP One"。設定外部或內建金鑰管理程式時、靜止資料加密的設定方式會改變、以供全新的集合體和全新的磁碟區使用。全新的Aggregate依預設會啟用NetApp Aggregate Encryption（NAE）。非NAE Aggregate一部分的全新磁碟區預設會啟用NetApp Volume Encryption（NVE）。如果資料儲存虛擬機器（SVM）是使用多租戶金鑰管理、以自己的金鑰管理程式進行設定、則為該SVM建立的磁碟區會自動設定NVE。

您可以在新的或現有的磁碟區上啟用加密。NVE支援完整的儲存效率功能、包括重複資料刪除與壓縮。從 ONTAP 9.14.1 開始、您就可以了 在現有 SVM 根磁碟區上啟用 NVE。

> 如果您使用SnapLock 的是功能區、則只能在新的空白SnapLock 版的功能區上啟用加密功能。您無法在現有SnapLock 的流通量上啟用加密功能。

您可以在任何類型的Aggregate（HDD、SSD、混合式、陣列LUN）上使用NVE、搭配任何RAID類型、也可以在ONTAP 任何支援的支援功能中使用、包括ONTAP Select 用作支援的功能、包括用作支援的功能。您也可以使用NVE搭配硬體加密、在自我加密磁碟機上使用「雙重加密」資料。

啟用 NVE 時、核心傾印也會加密。

Aggregate層級加密

通常、每個加密磁碟區都會指派一個唯一的金鑰。刪除磁碟區時、金鑰會隨之刪除。

從ONTAP SURF9.6開始、您可以使用_NetApp Aggregate Encryption（NAE）_將金鑰指派給內含的Aggregate、以便加密磁碟區。刪除加密磁碟區時、會保留該集合體的金鑰。如果刪除整個Aggregate、則會刪除金鑰。

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP

NVE與NAE磁碟區可共存於同一個Aggregate上。根據預設、在Aggregate層級加密下加密的磁碟區為NAE磁碟區。加密磁碟區時、您可以覆寫預設值。

您可以使用 `volume move` 將 NVE Volume 轉換為 NAE Volume 的命令、反之亦然。您可以將NAE磁碟區複寫至NVE磁碟區。

您無法使用 `secure purge` NAE 磁碟區上的命令。

何時使用外部金鑰管理伺服器

雖然使用內建金鑰管理程式的成本較低、而且通常更方便、但如果下列任一項屬實、您應該設定KMIP伺服器：

- 您的加密金鑰管理解決方案必須符合聯邦資訊處理標準（FIPS）140-2或OASIS KMIP標準。
- 您需要一套多叢集解決方案、集中管理加密金鑰。
- 您的企業需要更高的安全性、將驗證金鑰儲存在系統或與資料不同的位置。

外部金鑰管理範圍

外部金鑰管理的範圍決定了金鑰管理伺服器是保護叢集中的所有SVM、還是僅保護選取的SVM：

- 您可以使用_叢集範圍_來設定叢集中所有SVM的外部金鑰管理。叢集管理員可以存取儲存在伺服器上的每個金鑰。
- 從ONTAP S9.6開始、您可以使用_SVM範圍_來設定叢集中命名SVM的外部金鑰管理。這最適合多租戶環境、每個租戶使用不同的SVM（或一組SVM）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。
  - 從ONTAP 9.17.1 開始，您可以使用巴比肯 KMS僅保護資料 SVM 的 NVE 金鑰。
  - 從功能升級到功能升級到ONTAP 功能升級、您可以使用 Azure Key Vault與Google Cloud KMS 僅保護資料 SVM 的 NVE 金鑰。從 9.12.0 開始、 AWS 的 KMS 都可以使用這項功能。

您可以在同一個叢集中使用這兩個範圍。如果SVM已設定金鑰管理伺服器、ONTAP 則僅使用這些伺服器來保護

金鑰。否則ONTAP 、利用為叢集設定的金鑰管理伺服器來保護金鑰。

中提供已驗證的外部金鑰管理程式清單 "NetApp互通性對照表工具IMT （不含）"。您可以在 IMT 的搜尋功能中輸入「關鍵經理」一詞來找到此清單。

Azure Key Vault 和 AWS KMS 等雲端 KMS 供應商不支援 KMIP 。因此，這些項目並未列在 IMT 上。

支援詳細資料

下表顯示NVE支援詳細資料：

資源或功能	支援詳細資料
平台	需要AES-NI卸載功能。請參閱Hardware Universe 《銷售支援》（HWU）、確認您的平台是否支援NVE和NAE。

加密	從推出更新版本時開始ONTAP 、新建立的Aggregate和Volume會在您新增Volume加密（VE）授權、並設定內建或外部金鑰管理程式時、依預設進行加密。如果您需要建立未加密的Aggregate、請使用下列命令：
	
	`storage aggregate create -encrypt-with-aggr-key false`
	
	如果您需要建立純文字Volume、請使用下列命令：
	
	`volume create -encrypt false`
	
	在下列情況下、預設不會啟用加密：
	
	• 未安裝ve授權。
	• 未設定金鑰管理程式。
	• 平台或軟體不支援加密。
	• 硬體加密已啟用。

ONTAP	所有ONTAP實施。 ONTAP9.5 及更高版本支援Cloud Volumes ONTAP 。
裝置	HDD、SSD、混合式陣列LUN。
RAID	RAID0、RAID4、RAID-DP、RAID-TEC
磁碟區	資料磁碟區和現有 SVM 根磁碟區。您無法加密 MetroCluster 中繼資料磁碟區上的資料。在早於 9.14.1 的 ONTAP 版本中、您無法使用 NVE 加密 SVM 根 Volume 上的資料。從 ONTAP 9.14.1 開始、 ONTAP 支援 SVM 根磁碟區上的 NVE。

Aggregate層級加密	從推出支援Aggregate層級加密（NAE）的ONTAP NVE開始： • 如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。 • 您無法重新輸入Aggregate層級加密Volume的金鑰。 • Aggregate層級加密磁碟區不支援安全清除。 • 除了資料磁碟區之外、NAE也支援加密SVM根磁碟區和MetroCluster 元資料Volume。Nae不支援加密根磁碟區。
SVM範圍	從ONTAP 9.8 開始支援MetroCluster 。 從ONTAP 9.6 開始，NVE 僅支援 SVM 範圍的外部金鑰管理，而不支援板載金鑰管理員。
儲存效率	重複資料刪除、壓縮、壓縮、FlexClone。 即使將實體複本從父複本分割出去、複本仍會使用與父複本相同的金鑰。您應該執行 `volume move` 在分割複本上、分割複本之後會有不同的金鑰。
複寫	• 對於 Volume 複寫、來源和目的地磁碟區可以有不同的加密設定。可針對來源設定加密、也可針對目的地設定未設定加密、反之亦然。來源上設定的加密不會複寫到目的地。加密必須在來源和目的地上手動設定。請參閱設定 NVE和使用NVE加密Volume資料。 • 對於SVM複寫、目的地磁碟區會自動加密、除非目的地不包含支援Volume加密的節點、在這種情況下、複寫會成功、但目的地磁碟區不會加密。 • 針對部分組態、每個叢集都會從其設定的金鑰伺服器擷取外部金鑰管理金鑰。MetroCluster組態複寫服務會將OKM金鑰複寫至合作夥伴站台。
法規遵循	合規模式和企業模式均支援SnapLock ，但僅適用於新卷。您無法在現有SnapLock的流通量上啟用加密功能。
資料量FlexGroup	支援FlexGroup磁碟區。目的地Aggregate必須與來源Aggregate的類型相同、無論是Volume層級或Aggregate層級。從功能更新版開始、支援就地重新更新功能、以取代功能。ONTAP FlexGroup
7-Mode轉換	從7-Mode Transition Tool 3.3開始、您可以使用7-Mode Transition Tool CLI、在叢集式系統上執行以複製為基礎的移轉、移轉至啟用NVE的目的地磁碟區。

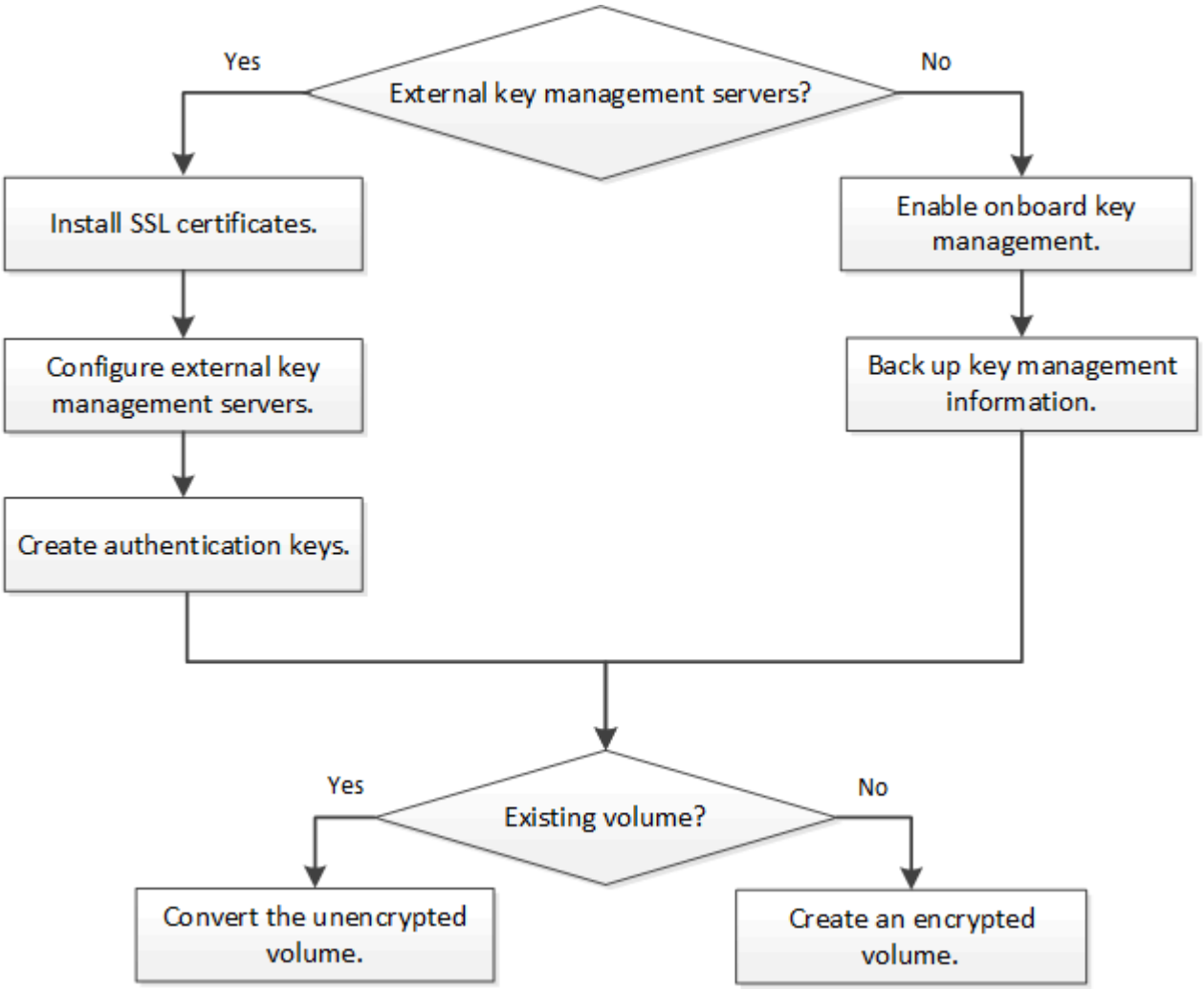
相關資訊

- "常見問題集- NetApp Volume Encryption與NetApp Aggregate Encryption"
- "儲存聚合創建"

ONTAP NetApp磁碟區加密工作流程

您必須先設定金鑰管理服務、才能啟用磁碟區加密。您可以在新磁碟區或現有磁碟區上啟

用加密。



"您必須安裝 VE 授權"並在使用 NVE 加密資料之前、先設定金鑰管理服務。在安裝授權之前"判斷ONTAP 您的版本是否支援NVE"，您應該：

設定 NVE

確定您的ONTAP叢集版本是否支援 NVE

安裝授權之前、您應該先判斷叢集版本是否支援NVE。您可以使用 `version` 判斷叢集版本的命令。

關於這項工作

叢集版本是ONTAP 叢集內任何節點上執行的最低版本的功能。

步驟

1. 判斷叢集版本是否支援NVE：

   ```
   version -v
   ```

   如果命令輸出顯示文字（針對「無靜態資料加密」），或您使用的平台未列於"支援詳細資料"，則不支援

NVE `10no-DARE` 。

在**ONTAP**叢集上安裝磁碟區加密許可證

VE授權可讓您在叢集中的所有節點上使用此功能。使用 NVE 加密資料之前、必須先取得此授權。隨附於"ONTAP One"。

在 ONTAP One 之前、 VE 授權已包含在加密套件中。加密套件已不再提供、但仍然有效。雖然目前並不需要"升級至 ONTAP One"、但現有客戶仍可選擇。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須已從銷售代表處收到 VE 授權金鑰、或已安裝 ONTAP 。

步驟

1. "確認已安裝 VE 授權"。

   VE 授權套件名稱為 `VE`。

2. 如果未安裝授權、"使用系統管理器或 ONTAP CLI 進行安裝"。

設定外部金鑰管理

了解如何使用**ONTAP NetApp**磁碟區加密設定外部金鑰管理

您可以使用一個或多個外部金鑰管理伺服器來保護叢集用於存取加密資料的金鑰。外部金鑰管理伺服器是儲存環境中的第三方系統，它使用金鑰管理互通性協定 (KMIP) 向節點提供金鑰。除了板載金鑰管理器之外， ONTAP還支援多個外部金鑰管理伺服器。

從ONTAP 9.10.1 開始，您可以使用 Azure Key Vault 或 Google Cloud Key Manager 服務 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.11.1 開始，您可以在叢集中設定多個外部金鑰管理員。看配置叢集金鑰伺服器。從ONTAP 9.12.0 開始，您可以使用 "AWS 的 KMS" 保護您的資料 SVM 的 NVE 金鑰。從ONTAP 9.17.1 開始，您可以使用 OpenStack 的 巴比肯 KMS 保護您的資料 SVM 的 NVE 金鑰。

使用**ONTAP**系統管理員管理外部金鑰管理器

從 ONTAP 9.7 開始、您可以使用內建金鑰管理程式來儲存及管理驗證與加密金鑰。從 ONTAP 9.13.1 開始、您也可以使用外部金鑰管理員來儲存及管理這些金鑰。

Onboard Key Manager 會將金鑰儲存並管理在叢集內部的安全資料庫中。其範圍是叢集。外部金鑰管理程式會儲存和管理叢集外部的金鑰。其範圍可以是叢集或儲存 VM 。可以使用一或多個外部金鑰管理員。適用下列條件：

- 如果已啟用 Onboard Key Manager 、則無法在叢集層級啟用外部金鑰管理程式、但可以在儲存 VM 層級啟用外部金鑰管理程式。
- 如果在叢集層級啟用外部金鑰管理程式、則無法啟用 Onboard Key Manager 。

使用外部金鑰管理程式時、每個儲存 VM 和叢集最多可註冊四個主要金鑰伺服器。每個主要金鑰伺服器最多可叢集三個次要金鑰伺服器。

設定外部金鑰管理程式

若要新增儲存 VM 的外部金鑰管理程式、您應該在設定儲存 VM 的網路介面時新增選用閘道。如果儲存 VM 是在沒有網路路由的情況下建立的、您必須為外部金鑰管理程式明確建立路由。請參閱 "建立 LIF （網路介面）"。

步驟

您可以從 System Manager 的不同位置設定外部金鑰管理程式。

1. 若要設定外部金鑰管理程式、請執行下列其中一個啟動步驟。

工作流程	導覽	開始步驟
設定金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⚙。選取 * 外部金鑰管理員 * 。
新增本機層	• 儲存 * > * Tiers*	選取 *+ 新增本機層 * 。核取標有「 Configure Key Manager 」的核取方塊。選取 * 外部金鑰管理員 * 。
準備儲存設備	• 儀表板 *	在 * 容量 * 區段中、選取 * 準備儲存 * 。 然後選取「設定金鑰管理程式」。選取 * 外部金鑰管理員 * 。
設定加密（僅限儲存 VM 範圍的金鑰管理程式）	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全 * 下的 * 加密 * 區段中，選擇 ⚙。

2. 要添加主密鑰服務器，請選擇 ＋ Add ，然後填寫 **IP** 地址或主機名 * 和 ***Port** 字段。
3. 現有安裝的憑證會列在 * KMIP 伺服器 CA 憑證 * 和 * KMIP 用戶端憑證 * 欄位中。 您可以執行下列任一動作：
   - 選取 ⌄ 以選取您要對應至金鑰管理程式的已安裝憑證。（可以選取多個服務 CA 憑證、但只能選取一個用戶端憑證。）
   - 選取 * 新增憑證 * 以新增尚未安裝的憑證、並將其對應至外部金鑰管理員。
   - 選取 × 憑證名稱旁的、以刪除您不想對應至外部金鑰管理程式的已安裝憑證。
4. 若要新增次要金鑰伺服器、請在 * 次要金鑰伺服器 * 欄中選取 * 新增 * 、並提供詳細資料。
5. 選取 * 儲存 * 以完成組態。

編輯現有的外部金鑰管理程式

如果您已設定外部金鑰管理員、則可以修改其設定。

步驟

1. 若要編輯外部金鑰管理程式的組態、請執行下列其中一個開始步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下，選擇 ⋮，然後選擇 * 編輯外部金鑰管理程式 * 。

儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮、然後選取 * 編輯外部金鑰管理員 * 。

2. 現有的主要伺服器會列在 * 金鑰伺服器 * 表中。您可以執行下列作業：
   - 選取以新增金鑰伺服器 + Add 。
   - 選取包含金鑰伺服器名稱的表格儲存格結尾處、以刪除金鑰伺 ⋮ 服器。與該主要金鑰伺服器相關的次要金鑰伺服器也會從組態中移除。

刪除外部金鑰管理程式

如果磁碟區未加密、則可以刪除外部金鑰管理程式。

步驟

1. 若要刪除外部金鑰管理程式、請執行下列其中一個步驟。

範圍	導覽	開始步驟
叢集範圍外部金鑰管理程式	• 叢集 * > * 設定 *	捲動至 * 安全性 * 區段。在 * 加密 * 下、選取 ⋮、然後選取 * 刪除外部金鑰管理員 * 。
儲存 VM 範圍外部金鑰管理程式	• 儲存 * > * 儲存 VM *	選取儲存VM。選取 * 設定 * 索引標籤。在 * 安全性 * 下的 * 加密 * 區段中、選取 ⋮、然後選取 * 刪除外部金鑰管理員 * 。

在關鍵經理之間移轉金鑰

當叢集上啟用多個金鑰管理程式時、金鑰必須從一個金鑰管理程式移轉至另一個金鑰管理程式。系統管理員會自動完成此程序。

- 如果已在叢集層級啟用 Onboard Key Manager 或外部金鑰管理程式、且某些磁碟區已加密、 然後、當您在儲存 VM 層級設定外部金鑰管理程式時、金鑰必須從叢集層級的 Onboard Key Manager 或外部金鑰管理程式移轉至儲存 VM 層級的外部金鑰管理程式。系統管理員會自動完成此程序。
- 如果在儲存 VM 上建立的磁碟區沒有加密、則不需要移轉金鑰。

在**ONTAP**叢集上安裝 **SSL** 憑證

叢集與KMIP伺服器使用KMIP SSL憑證來驗證彼此的身分、並建立SSL連線。在使用KMIP伺服器設定SSL連線之前、您必須先安裝叢集的KMIP用戶端SSL憑證、以及KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。

關於這項工作

在HA配對中、兩個節點必須使用相同的公有和私有KMIP SSL憑證。如果您將多個HA配對連線至相同的KMIP伺服器、HA配對中的所有節點都必須使用相同的公有和私有KMIP SSL憑證。

開始之前

- 建立憑證、KMIP伺服器和叢集的伺服器上、必須同步時間。
- 您必須已取得叢集的公用SSL KMIP用戶端憑證。
- 您必須取得與叢集SSL KMIP用戶端憑證相關的私密金鑰。
- SSL KMIP用戶端憑證不得受密碼保護。
- 您必須已取得KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝用戶端和伺服器憑證。

步驟

1. 安裝叢集的SSL KMIP用戶端憑證：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系統會提示您輸入SSL KMIP公開和私有憑證。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 安裝KMIP伺服器根憑證授權單位（CA）的SSL公開憑證：

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

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

相關資訊

- "安全性憑證安裝"

在**ONTAP 9.6** 及更高版本中為 **NVE** 啟用外部金鑰管理

使用 KMIP 伺服器來保護叢集用於存取加密資料的金鑰。從ONTAP 9.6 開始，您可以選擇配置單獨的外部金鑰管理器來保護資料 SVM 用於存取加密資料的金鑰。

從 ONTAP 9.11.1 開始、每個主要金鑰伺服器最多可新增 3 個次要金鑰伺服器、以建立叢集金鑰伺服器。如需詳細資訊、請參閱 設定叢集式外部金鑰伺服器。

關於這項工作

您最多可以將四個 KMIP 伺服器連接到叢集或 SVM。使用至少兩台伺服器以實現冗餘和災難復原。

外部金鑰管理的範圍決定了金鑰管理伺服器是保護叢集中的所有SVM、還是僅保護選取的SVM：

- 您可以使用_叢集範圍_來設定叢集中所有SVM的外部金鑰管理。叢集管理員可以存取儲存在伺服器上的每個金鑰。
- 從ONTAP 功能表9.6開始、您可以使用_SVM範圍來設定叢集中資料SVM的外部金鑰管理。這最適合多租戶環境、每個租戶使用不同的SVM（或一組SVM）來提供資料。只有特定租戶的SVM管理員可以存取該租戶的金鑰。
- 對於多租戶環境、請使用下列命令安裝_MT_EK-Mgmt_的授權：

```
system license add -license-code <MT_EK_MGMT license code>
```

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

您可以在同一個叢集中使用這兩個範圍。如果SVM已設定金鑰管理伺服器、ONTAP 則僅使用這些伺服器來保護金鑰。否則ONTAP 、利用為叢集設定的金鑰管理伺服器來保護金鑰。

您可以在叢集範圍設定內建金鑰管理、並在SVM範圍設定外部金鑰管理。您可以使用 `security key-manager key migrate` 命令將金鑰從叢集範圍內的機載金鑰管理移轉至 SVM 範圍內的外部金鑰管理程式。

如"指令參考資料ONTAP"需詳細 `security key-manager key migrate`資訊，請參閱。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- KMIP 伺服器必須能夠從每個節點的節點管理 LIF 存取。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 在MetroCluster環境中：
  - 在啟用外部金鑰管理之前，必須完全配置MetroCluster 。
  - 您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。
  - 必須在兩個叢集上配置外部密鑰管理器。

步驟

1. 設定叢集的金鑰管理程式連線：

   ```
   security key-manager external enable -vserver admin_SVM -key-servers
   host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
   server_CA_certificates
   ```

   > ⓘ 這 `security key-manager external enable`命令替換 `security key-manager setup`命令。如果在叢集登入提示字元下執行該命令， `*admin_SVM*`預設為目前叢集的管理 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。

   下列命令可啟用的外部金鑰管理 `cluster1` 使用三個外部金鑰伺服器。第一個金鑰伺服器是使用其主機名稱和連接埠來指定、第二個金鑰伺服器是使用IP位址和預設連接埠來指定、第三個金鑰伺服器則是使用IPv6位址和連接埠來指定：

   ```
   clusterl::> security key-manager external enable -vserver cluster1 -key
   -servers
   ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
   -client-cert AdminVserverClientCert -server-ca-certs
   AdminVserverServerCaCert
   ```

2. 設定SVM的金鑰管理程式：

   ```
   security key-manager external enable -vserver SVM -key-servers
   ```

```
host_name|IP_address:port,… -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

- 如果在 SVM 登入提示字元下執行該命令， `SVM`預設為當前 SVM。您可以運行 `security key-manager external modify`命令來更改外部密鑰管理配置。
- 在支援資料SVM的環境中、如果您要設定外部金鑰管理、就不需要重複執行MetroCluster `security key-manager external enable` 合作夥伴叢集上的命令。

下列命令可啟用的外部金鑰管理 `svm1` 使用單一金鑰伺服器聆聽預設連接埠 5696 ：

```
svm1l::> security key-manager external enable -vserver svm1 -key-servers
keyserver.svm1.com -client-cert SVM1ClientCert -server-ca-certs
SVM1ServerCaCert
```

3. 針對任何其他SVM重複最後一個步驟。

您也可以使用 `security key-manager external add-servers`命令來設定其他 SVM 。命令會 `security key-manager external add-servers`取代 `security key-manager add`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external add-servers`資訊，請參閱。

4. 確認所有已設定的KMIP伺服器均已連線：

```
security key-manager external show-status -node node_name
```

命令會 `security key-manager external show-status`取代 `security key-manager show -status`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external show-status`資訊，請參閱。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  -----------------------------------------
-------------
node1
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available
node2
      svm1
               keyserver.svm1.com:5696                          available
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234     available
               ks1.local:15696                                  available

8 entries were displayed.
```

5. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換磁碟區之前，必須完全設定外部金鑰管理員。

相關資訊

- 設定叢集式外部金鑰伺服器
- "系統許可證添加"
- "安全金鑰管理員金鑰遷移"
- "安全金鑰管理員外部新增伺服器"
- "安全金鑰管理員外部顯示狀態"

在ONTAP 9.5 及更早版本中為 NVE 啟用外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

關於這項工作

可為叢集中的所有節點設定KMIP伺服器連線。ONTAP

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。
- 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集節點的金鑰管理程式連線：

   `security key-manager setup`

   金鑰管理程式設定隨即開始。

   在MetroCluster環境中，您必須在兩個叢集上執行此命令。詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

2. 在每個提示字元輸入適當的回應。
3. 新增KMIP伺服器：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

4. 新增額外的KMIP伺服器以提供備援：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

5. 確認所有已設定的KMIP伺服器均已連線：

   `security key-manager show -status`

   詳細了解此過程中所述的命令"指令參考資料ONTAP"。

```
cluster1::> security key-manager show -status

Node            Port      Registered Key Manager  Status
--------------  ----      ----------------------  ---------------
cluster1-01     5696      20.1.1.1                available
cluster1-01     5696      20.1.1.2                available
cluster1-02     5696      20.1.1.1                available
cluster1-02     5696      20.1.1.2                available
```

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   ```
   volume encryption conversion start
   ```

   在轉換磁碟區之前、必須先完整設定外部金鑰管理程式。在 MetroCluster 環境中、必須在兩個站台上設定外部金鑰管理員。

透過雲端供應商管理**ONTAP**資料 **SVM** 的 **NVE** 金鑰

從 ONTAP 9.10.1 開始，您可以在雲端代管應用程式中使用"Azure Key Vault（AKV）"和"Google Cloud Platform的金鑰管理服務（雲端KMS）"保護 ONTAP 加密金鑰。從 ONTAP 9.12.0 開始，您也可以使用來保護 NVE 金鑰"AWS 的 KMS"。

AWS KMS 、 AKV 和 Cloud KMS 可用於保護 "NetApp Volume Encryption（NVE）金鑰" 僅適用於資料SVM。

關於這項工作

您可以使用 CLI 或 ONTAP REST API 來啟用雲端供應商的金鑰管理。

使用雲端供應商保護金鑰時、請注意、根據預設、資料 SVM LIF 會用於與雲端金鑰管理端點通訊。節點管理網路用於與雲端供應商的驗證服務（login.microsoftonline.com for Azure；oauth2.googleapis.com for Cloud KMS ）進行通訊。如果叢集網路未正確設定，叢集將無法正確使用金鑰管理服務。

使用雲端供應商金鑰管理服務時、您應注意下列限制：

- 雲端供應商金鑰管理不適用於 NetApp 儲存加密（ NSE ）和 NetApp Aggregate Encryption （ NAE ）。"外部KMIP" 可以改用。
- 雲端供應商金鑰管理不適用於 MetroCluster 組態。
- 雲端供應商金鑰管理只能在資料 SVM 上設定。

開始之前

- 您必須在適當的雲端供應商上設定 KMS 。
- ONTAP 叢集的節點必須支援 NVE 。
- "您必須已安裝 Volume Encryption （ VE ）和多租戶加密金鑰管理（ MTEKM ）授權"。這些授權隨附於"ONTAP One"。
- 您必須是叢集或 SVM 管理員。
- 資料 SVM 不得包含任何加密的磁碟區、也不得採用金鑰管理程式。如果資料 SVM 包含加密的磁碟區、您

必須先移轉這些磁碟區、才能設定 KMS 。

啟用外部金鑰管理

啟用外部金鑰管理取決於您使用的特定金鑰管理程式。選擇適當的金鑰管理程式和環境標籤。

AWS

開始之前

- 您必須為 AWS KMS 金鑰建立授權、以便由管理加密的 IAM 角色使用。IAM 角色必須包含允許下列作業的原則：
  - `DescribeKey`
  - `Encrypt`
  - `Decrypt`

    如需詳細資訊、請參閱 AWS 文件 "補助"。

在 **ONTAP SVM** 上啟用 **AWS KMV**

1. 開始之前、請先從 AWS KMS 取得存取金鑰 ID 和秘密金鑰。
2. 將權限層級設為進階：
   `set -priv advanced`
3. 啟用 AWS KMS ：
   `security key-manager external aws enable -vserver` *`svm_name`* `-region` *`AWS_region`* `-key-id` *`key_ID`* `-encryption-context` *`encryption_context`*
4. 出現提示時、請輸入秘密金鑰。
5. 確認 AWS KMS 已正確設定：
   `security key-manager external aws show -vserver` *`svm_name`*

   如"指令參考資料ONTAP"需詳細 `security key-manager external aws`資訊，請參閱。

Azure

在 **ONTAP SVM** 上啟用 **Azure Key Vault**

1. 開始之前、您必須先從Azure帳戶取得適當的驗證認證資料、包括用戶端機密或憑證。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限層級設為進階
   `set -priv advanced`
3. 在 SVM 上啟用 AKV
   `security key-manager external azure enable -client-id` *`client_id`* `-tenant-id` *`tenant_id`* `-name -key-id` *`key_id`* `-authentication-method {certificate|client-secret}`
   出現提示時、請輸入 Azure 帳戶的用戶端憑證或用戶端機密。
4. 確認 AKV 已正確啟用：
   `security key-manager external azure show vserver` *`svm_name`*
   如果服務連線能力不正常、請透過資料 SVM LIF 建立與 AKV 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external azure`資訊，請參閱。

Google Cloud

在 **ONTAP SVM** 上啟用雲端 **KMS**

1. 開始之前、請先以 JSON 格式取得 Google Cloud KMS 帳戶金鑰檔案的私密金鑰。您可以在GCP帳戶中找到這項資訊。您也必須確保叢集中的所有節點都正常運作。您可以使用命令來檢查 `cluster show`。如"指令參考資料ONTAP"需詳細 `cluster show`資訊，請參閱。
2. 將權限等級設為進階：
   `set -priv advanced`
3. 在 SVM 上啟用 Cloud KMS
   `security key-manager external gcp enable -vserver svm_name -project-id project_id-key-ring-name key_ring_name -key-ring-location key_ring_location -key-name key_name`
   出現提示時、請使用服務帳戶私密金鑰輸入 JSON 檔案的內容
4. 驗證 Cloud KMS 是否配置了正確的參數：
   `security key-manager external gcp show vserver svm_name`現狀 `kms_wrapped_key_status`將`"UNKNOWN"`如果沒有建立加密磁碟區。如果服務可達性不正常，則透過資料 SVM LIF 建立與 GCP 金鑰管理服務的連線。

   如"指令參考資料ONTAP"需詳細 `security key-manager external gcp`資訊，請參閱。

如果已為資料SVM設定一或多個加密磁碟區、且對應的NVE金鑰由管理SVM內建金鑰管理程式管理、則這些金鑰應移轉至外部金鑰管理服務。若要使用 CLI 執行此作業、請執行命令：
`security key-manager key migrate -from-Vserver admin_SVM -to-Vserver data_SVM`
在成功移轉資料 SVM 的所有 NVE 金鑰之前、無法為租戶的資料 SVM 建立新的加密磁碟區。

相關資訊

- "使用適用於 Cloud Volumes ONTAP 的 NetApp 加密解決方案來加密磁碟區"
- "安全金鑰管理員外部"

使用 **Barbican KMS** 管理**ONTAP**金鑰

從ONTAP 9.17.1 開始，您可以使用 OpenStack 的"巴比肯 KMS"保護ONTAP加密金鑰。BarbicanKMS 是一項安全儲存和存取金鑰的服務。 BarbicanKMS 可用於保護資料 SVM 的NetApp磁碟區加密 (NVE) 金鑰。 Barbican依賴"OpenStack Keystone" ，OpenStack 的身份服務，用於身份驗證。

關於這項工作

您可以使用 CLI 或ONTAP REST API 使用 Barbican KMS 設定金鑰管理。在 9.17.1 版本中，Barbican KMS 支援有以下限制：

- Barbican KMS 不支援NetApp儲存加密 (NSE) 和NetApp聚合加密 (NAE)。或者，您可以使用"外部 KMIP"或"板載密鑰管理器 (OKM)"用於 NSE 和 NVE 金鑰。
- MetroCluster配置不支援 Barbican KMS。
- Barbican KMS 只能為資料 SVM 配置，不適用於管理 SVM。

除非另有說明，管理員 `admin`特權等級可以執行下列操作程序。

開始之前

- 必須配置 Barbican KMS 和 OpenStack Keystone 。您用於 Barbican 的 SVM 必須能夠透過網路存取

Barbican 和 OpenStack Keystone伺服器。

- 如果您正在為 Barbican 和 OpenStack Keystone伺服器使用自訂憑證授權單位 (CA)，則必須使用 `security certificate install -type server-ca -vserver <admin_svm>` 。

建立並啟動 **Barbican KMS** 配置

您可以為 SVM 建立新的 Barbican KMS 配置並將其啟動。一個 SVM 可以有多個非活動的 Barbican KMS 配置，但一次只能有一個處於活動狀態。

步驟

1. 為 SVM 建立新的非活動 Barbican KMS 配置：

```
security key-manager external barbican create-config -vserver <svm_name>
-config-name <unique_config_name> -key-id <key_id> -keystone-url
<keystone_url> -application-cred-id
<keystone_applications_credentials_id>
```

   - `-key-id`是 `Barbican 密鑰加密密鑰 (KEK) 的密鑰標識符。請輸入完整的 URL，包括 `https://` 。

     某些 URL 包含問號 (?)。問號用於啟動ONTAP命令列活動幫助。要輸入帶有問號的 URL，您需要先使用以下命令停用活動協助 `set -active-help false` 。稍後可以使用以下命令重新啟用主動協助 `set -active-help true`了解更多信息"指令參考資料ONTAP" 。

   - `-keystone-url`是 `OpenStack Keystone授權主機的 URL。請輸入完整的 URL，包括 `https://` 。

   - `-application-cred-id`是應用程式憑證 ID。

     輸入此命令後，系統將提示您輸入應用程式憑證金鑰。此指令將建立一個非活動的 Barbican KMS 配置。

     以下範例建立一個名為的非活動 Barbican KMS 配置 `config1`對於`SVM `svm1` ：

```
cluster1::> security key-manager external barbican create-config
-vserver svm1 -config-name config1 -keystone-url
https://172.21.76.152:5000/v3 -application-cred-id app123 -key-id
https://172.21.76.153:9311/v1/secrets/<id_value>

Enter the Application Credentials Secret for authentication with
Keystone: <key_value>
```

2. 啟動新的 Barbican KMS 配置：

```
security key-manager keystore enable -vserver <svm_name> -config-name
<unique_config_name> -keystore barbican
```

您可以使用此命令在 Barbican KMS 配置之間切換。如果 SVM 上已存在活動的 Barbican KMS 配置，則該配置將處於非活動狀態，並啟動新的配置。

3. 驗證新的 Barbican KMS 配置是否處於活動狀態：

```
security key-manager external barbican check -vserver <svm_name> -node
<node_name>
```

此指令將提供 SVM 或節點上活動的 Barbican KMS 配置的狀態。例如，如果 SVM `svm1`在節點上 `node1` 具有活動的 Barbican KMS 配置，以下命令將傳回該配置的狀態：

```
cluster1::> security key-manager external barbican check -node node1

Vserver: svm1
Node: node1

Category: service_reachability
              Status: OK

Category: kms_wrapped_key_status
              Status: OK
```

更新 **Barbican KMS** 配置的憑證和設置

您可以檢視和更新活動或非活動的 Barbican KMS 配置的目前設定。

步驟

1. 查看 SVM 的目前 Barbican KMS 配置：

```
security key-manager external barbican show -vserver <svm_name>
```

顯示 SVM 上每個 Barbican KMS 配置的金鑰 ID、OpenStack Keystone URL 和應用程式憑證 ID。

2. 更新 Barbican KMS 配置的設定：

```
security key-manager external barbican update-config -vserver <svm_name>
-config-name <unique_config_name> -timeout <timeout> -verify
<true|false> -verify-host <true|false>
```

此指令更新指定 Barbican KMS 設定的逾時和驗證設定。 `timeout`確定ONTAP在連線失敗前等待 Barbican 回應的時間（以秒為單位）。預設 `timeout`是十秒。 `verify`和 `verify-host`確定在連線之前是否應分別驗證 Barbican 主機的身份和主機名稱。預設情況下，這些參數設定為 `true`。這 `vserver`和 `config-name`參數是必需的。其他參數是可選的。

3. 如果需要，請更新活動或非活動的 Barbican KMS 配置的憑證：

```
security key-manager external barbican update-credentials -vserver
<svm_name> -config-name <unique_config_name> -application-cred-id
<keystone_applications_credentials_id>
```

輸入此命令後，系統將提示您輸入新的應用程式憑證金鑰。

4. 如果需要，為活動的 Barbican KMS 設定恢復遺失的 SVM 金鑰加密金鑰 (KEK)：
   a. 使用以下方式恢復遺失的 SVM KEK `security key-manager external barbican restore`：

```
security key-manager external barbican restore -vserver <svm_name>
```

此命令將透過與 Barbican 伺服器通訊來恢復活動 Barbican KMS 配置的 SVM KEK。

5. 如果需要，請為 Barbican KMS 設定重新金鑰 SVM KEK：
   a. 將權限層級設為進階：

```
set -privilege advanced
```

   b. 使用以下方式重新金鑰 SVM KEK `security key-manager external barbican rekey-internal`：

```
security key-manager external barbican rekey-internal -vserver
<svm_name>
```

此指令會為指定的 SVM 產生新的 SVM KEK，並使用新的 SVM KEK 重新封裝磁碟區加密金鑰。新的 SVM KEK 將受到有效的 Barbican KMS 配置的保護。

在 **Barbican KMS** 和 **Onboard Key Manager** 之間遷移金鑰

您可以將密鑰從 Barbican KMS 遷移到板載密鑰管理器 (OKM)，反之亦然。要了解有關 OKM 的更多信息，請參閱"啟用更新版本的更新版本、以利執行內建金鑰管理ONTAP"。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 如果需要，將密鑰從 Barbican KMS 遷移到 OKM：

```
security key-manager key migrate -from-vserver <svm_name> -to-vserver
<admin_svm_name>
```

`svm_name`是具有 Barbican KMS 配置的 SVM 的名稱。

3. 如果需要，將密鑰從 OKM 遷移到 Barbican KMS：

```
security key-manager key migrate -from-vserver <admin_svm_name> -to
-vserver <svm_name>
```

停用並刪除 **Barbican KMS** 配置

您可以停用沒有加密磁碟區的活動 Barbican KMS 配置，並且可以刪除非活動的 Barbican KMS 配置。

步驟

1. 將權限層級設為進階：

```
set -privilege advanced
```

2. 禁用活動的 Barbican KMS 配置：

```
security key-manager keystore disable -vserver <svm_name>
```

如果 SVM 上存在 NVE 加密磁碟區，則必須解密它們，否則遷移金鑰在停用 Barbican KMS 配置之前。啟動新的 Barbican KMS 配置不需要解密 NVE 磁碟區或遷移金鑰，並且會停用目前活動的 Barbican KMS 配置。

3. 刪除不活動的 Barbican KMS 配置：

```
security key-manager keystore delete -vserver <svm_name> -config-name
<unique_config_name> -type barbican
```

在**ONTAP 9.6** 及更高版本中啟用 **NVE** 的板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在存取加密磁碟區或自我加密磁碟的每個叢集上啟用 Onboard Key Manager 。

關於這項工作

您必須執行 `security key-manager onboard sync` 每次將節點新增至叢集時的命令。

如果您有 MetroCluster 組態、則必須執行 `security key-manager onboard enable` 命令先在本機叢集上執行、然後執行 `security key-manager onboard sync` 在遠端叢集上使用相同密碼的命令。當您執行時 `security key-manager onboard enable` 本機叢集的命令、然後在遠端叢集上進行同步處理、您不需要執行 `enable` 從遠端叢集再次執行命令。

詳細了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"指令參考資料ONTAP"。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。您可以使用 `cc-mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `cc-mode-enabled=yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

在設定ONTAP資料加密時，為了滿足商業機密解決方案 (CSfC) 的要求，您必須將 NSE 與 NVE 一起使用，並確保在通用標準模式下啟用板載金鑰管理員。看"CSfC解決方案簡介"。

> 當「內建金鑰管理程式」在「一般條件」模式中啟用時 (`cc-mode-enabled=yes`）、系統行為會以下列方式變更：
>
> - 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。
>
> 如果 5 次輸入叢集密碼失敗，請等待 24 小時或重新啟動節點以重設限制。
>
> - 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。
>
> 升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證成功，系統將繼續進行影像更新過程的下一步；否則，影像更新失敗。詳細了解 `cluster image`在"指令參考資料ONTAP"。

> 板載密鑰管理器將密鑰儲存在揮發性記憶體中。當系統重新啟動或停止時，揮發性記憶體的內容將會被清除。系統停止後 30 秒內清除揮發性記憶體。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定：

```
security key-manager onboard enable -cc-mode-enabled yes|no
```

設定 `cc-mode-enabled=yes` 要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `cc-mode-enabled=yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。。 - `cc-mode-enabled` MetroCluster 組態不支援此選項。 。 `security key-manager onboard enable` 命令會取代 `security key-manager setup` 命令。

2. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“`cc-mode`”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

3. 在通關密碼確認提示下、重新輸入通關密碼。
4. 確認已建立驗證金鑰：

   ```
   security key-manager key query -key-type NSE-AK
   ```

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

5. 您可以選擇將純文字磁碟區轉換為加密磁碟區。

   ```
   volume encryption conversion start
   ```

   在轉換磁碟區之前、必須先完整設定 Onboard Key Manager 。在 MetroCluster 環境中、兩個站台都必須設定內建金鑰管理員。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

配置板載金鑰管理器密碼後，手動將資訊備份到儲存系統外部的安全位置。看"手動備份內建金鑰管理資訊"。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員金鑰查詢"
- "安全金鑰管理員板載啟用"

在**ONTAP 9.5** 及更早版本中為 **NVE** 啟用板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您將 NSE 或 NVE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在配置板載金鑰管理器之前，請先配置MetroCluster環境。

步驟

1. 啟動金鑰管理程式設定：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

   下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「'cc-mode'」（64到256個字元之間的通關密碼）。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。
5. 驗證是否已為所有節點設定金鑰：

   `security key-manager show-key-store`

   ```
   cluster1::> security key-manager show-key-store

   Node: node1
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK

   Node: node2
   Key Store: onboard
   Key ID                                                               Used By
   -------------------------------------------------------------------------
   --------
   <id_value> NSE-AK
   <id_value> NSE-AK
   ```

   詳細了解 `security key-manager show-key-store`在"指令參考資料ONTAP"。

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換卷之前配置板載密鑰管理器。在MetroCluster環境中，在兩個站點上進行配置。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

配置板載金鑰管理器密碼時，請將資訊備份到儲存系統外部的安全位置，以防災難發生。看"手動備份內建金鑰管理資訊"。

相關資訊

- "手動備份內建金鑰管理資訊"

- "從外部金鑰管理移轉至內建金鑰管理"
- "安全金鑰管理員顯示金鑰庫"

在新新增的**ONTAP**節點中啟用板載金鑰管理

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

> 對於ONTAP 9.6 及更高版本，您必須執行 `security key-manager onboard sync` 每次向叢集新增節點時執行此命令。
>
> 若為 ONTAP 9.5 或更早版本、您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。
>
> 如果您將節點新增至具有板載金鑰管理的集群，請執行此命令來刷新遺失的金鑰。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 從 ONTAP 9.6 開始、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。

  深入瞭解 `security key-manager onboard enable`及 `security key-manager onboard sync` "指令參考資料ONTAP"。

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

> 如果密碼嘗試失敗，請重新啟動節點。重新啟動後，您可以再次嘗試輸入密碼。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員板載啟用"

使用 **NVE** 或 **NAE** 加密卷數據

了解如何使用 **NVE** 加密**ONTAP**磁碟區數據

從使用支援功能9.7開始ONTAP 、如果您擁有VE授權、以及內建或外部金鑰管理、則根據

預設會啟用Aggregate和Volume加密。對於支援更新版本的支援、您可以在新磁碟區或現有磁碟區上啟用加密功能。ONTAP您必須先安裝VE授權並啟用金鑰管理、才能啟用Volume加密。NVE符合FIPS-140-2第1級標準。

在 **ONTAP** 中啟用含 **VE** 授權的 **Aggregate** 層級加密

從 ONTAP 9 7 開始"VE 授權"、新建立的集合體和磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。從ONTAP 功能區9.6開始、您可以使用Aggregate層級加密、將金鑰指派給內含的Aggregate、以便加密磁碟區。

關於這項工作

如果您打算執行即時或背景Aggregate層級的重複資料刪除、則必須使用Aggregate層級的加密。NVE不支援Aggregate層級的重複資料刪除。

啟用Aggregate層級加密的Aggregate稱為_NAE Aggregate（適用於NetApp Aggregate Encryption）。NAE Aggregate中的所有磁碟區都必須使用NAE或NVE加密進行加密。使用Aggregate層級加密、您在Aggregate中建立的磁碟區預設會使用NAE加密進行加密。您可以置換預設值、改用NVE加密。

NAE Aggregate不支援純文字磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 啟用或停用Aggregate層級加密：

至…	使用此命令…
使用ONTAP NetApp 9.7或更新版本建立NAE Aggregate	`storage aggregate create -aggregate *aggregate_name* -node *node_name*`
使用ONTAP NetApp 9.6建立NAE Aggregate	`storage aggregate create -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key true`
將非NAE Aggregate轉換為NAE Aggregate	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key true`
將NAE Aggregate轉換為非NAE Aggregate	`storage aggregate modify -aggregate *aggregate_name* -node *node_name* -encrypt-with -aggr-key false`

詳細了解 `storage aggregate modify`在"指令參考資料ONTAP" 。

下列命令可在上啟用彙總層級加密 `aggr1`：

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1
```

- 更新版本：ONTAP

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with
-aggr-key true
```

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

2. 確認已啟用Aggregate進行加密：

`storage aggregate show -fields encrypt-with-aggr-key`

下列命令會驗證是否存在此問題 `aggr1` 已啟用加密：

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate            encrypt-aggr-key
-------------------- ----------------
aggr0_vsim4          false
aggr1                true
2 entries were displayed.
```

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

完成後

執行 `volume create` 建立加密磁碟區的命令。

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

在 **ONTAP** 的新磁碟區上啟用加密

您可以使用 `volume create` 在新磁碟區上啟用加密的命令。

關於這項工作

您可以使用NetApp Volume Encryption（NVE）加密磁碟區、從ONTAP NetApp Aggregate Encryption（NAE）開始加密磁碟區。若要深入瞭解NAE和NVE、請參閱 Volume加密總覽。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

啟用更新版本的加密程序ONTAP 會因ONTAP 您使用的版本和您的特定組態而有所不同：

- 如果ONTAP 啟用、請從支援的問題9.4開始 `cc-mode` 設定Onboard Key Manager時、您可以使用建立的磁碟區 `volume create` 無論您是否指定、命令都會自動加密 `-encrypt true`。

- 在更新版本的版本中、您必須使用ONTAP `-encrypt true` 與 `volume create` 啟用加密的命令（前提是您未啟用 `cc-mode`）。
- 如果您想要在ONTAP 32位址9.6中建立NAE Volume、則必須在Aggregate層級啟用NAE。請參閱 使用VE授權啟用Aggregate層級加密 以取得此工作的詳細資料。
- 從 ONTAP 9 7 開始"VE 授權"、新建立的磁碟區會在您擁有和內建或外部金鑰管理時、依預設進行加密。根據預設、在NAE Aggregate中建立的新磁碟區將為NAE類型、而非NVE。
  - 如有新增、請參閱ONTAP 更新版本的 `-encrypt true` 至 `volume create` 命令若要在NAE Aggregate中建立磁碟區、該磁碟區將採用NVE加密、而非NAE。NAE Aggregate中的所有磁碟區都必須使用NVE或NAE進行加密。

NAE集合體不支援純文字磁碟區。

步驟

1. 建立新磁碟區、並指定是否在磁碟區上啟用加密。如果新磁碟區位於NAE Aggregate中、則根據預設、該磁碟區將是NAE磁碟區：

若要建立...	使用此命令...
NAE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*
NVE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` + 在不支援NAE的情況下、使用支援的版本為ONTAP `-encrypt true` 指定應使用NVE加密磁碟區。在以NAE集合體建立Volume的版本中ONTAP 、 `-encrypt true` 取代預設的NAE加密類型、改為建立NVE Volume。
純文字Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

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

2. 確認已啟用磁碟區進行加密：

   ```
   volume show -is-encrypted true
   ```

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

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

在現有**ONTAP**磁碟區上啟用 **NAE** 或 **NVE**

您可以使用 `volume move start` 或 `volume encryption conversion start` 在

現有磁碟區上啟用加密的命令。

關於這項工作

您可以使用 `volume encryption conversion start`命令可以「就地」啟用現有磁碟區的加密，而無需將磁碟區移動到其他位置。或者，您可以使用 `volume move start`命令。

使用**Volume Encryption Conversion start**命令、在現有磁碟區上啟用加密

您可以使用 `volume encryption conversion start`命令來啟用現有磁碟區的「就地」加密，而無需將磁碟區移動到其他位置。

在您開始轉換作業之後、必須完成此作業。如果您在作業期間遇到效能問題、可以執行 `volume encryption conversion pause` 暫停作業的命令、以及 `volume encryption conversion resume` 命令以恢復作業。

> 您無法使用 `volume encryption conversion start` 轉換 SnapLock Volume 。

步驟

1. 在現有磁碟區上啟用加密：

   ```
   volume encryption conversion start -vserver SVM_name -volume volume_name
   ```

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion start`資訊，請參閱。

   下列命令可在現有磁碟區上啟用加密 `vol1`：

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

   系統會為磁碟區建立加密金鑰。磁碟區上的資料已加密。

2. 確認轉換作業的狀態：

   ```
   volume encryption conversion show
   ```

   如"指令參考資料ONTAP"需詳細 `volume encryption conversion show`資訊，請參閱。

   下列命令會顯示轉換作業的狀態：

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume    Start Time           Status
   -------   ------    ------------------   ----------------------------
   vs1       vol1      9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 轉換作業完成後、請確認磁碟區已啟用加密功能：

   ```
   volume show -is-encrypted true
   ```

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

下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate   State   Type   Size   Available   Used
-------   ------   ---------   -----   ----   -----   ---------  ----
vs1       vol1     aggr2      online     RW   200GB     160.0GB   20%
```

結果

如果您使用KMIP伺服器來儲存節點的加密金鑰、ONTAP 則當您加密磁碟區時、會自動將加密金鑰「推送」至伺服器。

使用**Volume Move start**命令在現有磁碟區上啟用加密

您可以使用 `volume move start`命令來移動現有的磁碟區來啟用加密。您可以使用相同的Aggregate或不同的Aggregate。

關於這項工作

- 從 ONTAP 9.8 開始、您可以使用 `volume move start` 在 SnapLock 或 FlexGroup 磁碟區上啟用加密。
- 從 ONTAP 9.4 開始、如果您在設定內建金鑰管理程式時啟用「 cc 模式」、就會使用建立磁碟區 `volume move start` 命令會自動加密。您不需要指定 `-encrypt-destination true`。
- 從ONTAP 功能區9.6開始、您可以使用Aggregate層級的加密功能、將金鑰指派給內含的Aggregate、以供移動的磁碟區使用。使用唯一金鑰加密的磁碟區稱為 *NVE Volumes* （意指它使用 NetApp Volume Encryption ）。使用Aggregate層級金鑰加密的Volume稱為_NAE Volume（適用於NetApp Aggregate Encryption ）。NAE集合體不支援純文字磁碟區。
- 從 ONTAP 9.14.1 開始、您可以使用 NVE 加密 SVM 根 Volume 。如需詳細資訊、請參閱 在 SVM 根磁碟區上設定 NetApp Volume Encryption。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

"委派權限以執行Volume Move命令"

步驟

1. 移動現有磁碟區、並指定是否在磁碟區上啟用加密：

若要轉換…	使用此命令…
NVE Volume的純文字磁碟區	`volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-encrypt-destination true`

NAE磁碟區的NVE或純文字磁碟區（假設目的地已啟用Aggregate層級加密）	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
NAE Volume至NVE Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`
NAE磁碟區至純文字磁碟區	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
從NVE磁碟區移至純文字磁碟區	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

下列命令會轉換名為的純文字磁碟區 `vol1` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

假設目的地上已啟用 Aggregate 層級加密、下列命令會轉換名為的 NVE 或純文字磁碟區 `vol1` 至 NAE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

下列命令會轉換名為的 NAE Volume `vol2` 至 NVE Volume ：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NAE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

下列命令會轉換名為的 NVE Volume `vol2` 至純文字磁碟區：

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

2. 檢視叢集磁碟區的加密類型：

   `volume show -fields encryption-type none|volume|aggregate`

   ◦ `encryption-type` 欄位可在 ONTAP 9.6 及更新版本中取得。

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

   下列命令會顯示中的磁碟區加密類型 `cluster2`：

```
cluster2::> volume show -fields encryption-type

vserver  volume  encryption-type
-------  ------  ---------------
vs1      vol1    none
vs2      vol2    volume
vs3      vol3    aggregate
```

3. 確認已啟用磁碟區進行加密：

   `volume show -is-encrypted true`

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

   下列命令會顯示上的加密磁碟區 `cluster2`：

```
cluster2::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2     online    RW  200GB    160.0GB  20%
```

結果

如果您使用 KMIP 伺服器來儲存節點的加密金鑰、 ONTAP 會在您加密磁碟區時自動將加密金鑰推送至伺服器。

在**ONTAP SVM** 根磁碟區上設定 **NVE**

從 ONTAP 9.14.1 開始、您可以在儲存 VM （ SVM ）根磁碟區上啟用 NetApp Volume Encryption （ NVE ）。透過 NVE 、根磁碟區會使用唯一金鑰進行加密、以提高 SVM 的安全性。

關於這項工作

只有在建立 SVM 之後、才能在 SVM 根 Volume 上啟用 NVE 。

開始之前

- SVM 根磁碟區不得位於使用 NetApp Aggregate Encryption （ NAE ）加密的 Aggregate 上。
- 您必須已啟用 Onboard Key Manager 或外部金鑰管理程式的加密。
- 您必須執行 ONTAP 9.14.1 或更新版本。
- 若要移轉包含使用 NVE 加密的根 Volume 的 SVM 、您必須在移轉完成後、將 SVM 根 Volume 轉換為純文字 Volume 、然後重新加密 SVM 根 Volume 。
  - 如果 SVM 移轉的目的地集合體使用 NAE 、則根磁碟區預設會繼承 NAE 。
- 如果 SVM 處於 SVM 災難恢復關係中：
  - 鏡射 SVM 上的加密設定不會複製到目的地。如果您在來源或目的地上啟用 NVE 、則必須在鏡射的 SVM 根 Volume 上個別啟用 NVE 。
  - 如果目的地叢集中的所有集合體都使用 NAE 、則 SVM 根 Volume 將使用 NAE 。

步驟

您可以使用 ONTAP CLI 或系統管理員、在 SVM 根磁碟區上啟用 NVE 。

CLI

您可以在 SVM 根磁碟區就地啟用 NVE 、或是在集合體之間移動磁碟區。

將根磁碟區加密到位

1. 將根磁碟區轉換為加密磁碟區：

   ```
   volume encryption conversion start -vserver svm_name -volume volume
   ```

2. 確認加密成功。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

移動 **SVM** 根 **Volume** 來加密它

1. 啟動磁碟區移動：

   ```
   volume move start -vserver svm_name -volume volume -destination-aggregate
   aggregate -encrypt-with-aggr-key false -encrypt-destination true
   ```

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

2. 確認 `volume move` 操作成功 `volume move show` 命令。。 `volume show -encryption-type volume` 顯示使用 NVE 的所有磁碟區清單。

系統管理員

1. 瀏覽至 儲存空間 > 磁碟區 。
2. 在您要加密的 SVM 根 Volume 名稱旁、選取「 編輯 」。
3. 在「 儲存與最佳化 」標題下、選取「 啟用加密 」。
4. 選擇 儲存 。

在**ONTAP**節點根磁碟區上配置 **NVE**

從功能介紹9.8開始ONTAP 、您可以使用NetApp Volume Encryption來保護節點的根磁碟區。

關於這項工作

此程序適用於節點根磁碟區。不適用於SVM根磁碟區。SVM 根磁碟區可透過集合體層級加密來保護、 從 ONTAP 9.14.1 開始、 NVE。

根磁碟區加密一旦開始、就必須完成。您無法暫停作業。加密完成後、您無法將新金鑰指派給根磁碟區、也無法執行安全清除作業。

開始之前

- 您的系統必須使用HA組態。
- 您的節點根磁碟區必須已建立。
- 您的系統必須具有內建金鑰管理程式、或是使用金鑰管理互通性傳輸協定（KMIP）的外部金鑰管理伺服器。

步驟

1. 加密根磁碟區：

   ```
   volume encryption conversion start -vserver SVM_name -volume root_vol_name
   ```

2. 確認轉換作業的狀態：

   ```
   volume encryption conversion show
   ```

3. 完成轉換作業後、請確認磁碟區已加密：

   ```
   volume show -fields
   ```

   以下顯示加密Volume的輸出範例。

   ```
   ::> volume show -vserver xyz  -volume vol0 -fields is-encrypted
   vserver    volume is-encrypted
   ---------- ------ ------------
   xyz        vol0   true
   ```

設定NetApp硬體加密

了解ONTAP基於硬體的加密

NetApp硬體式加密可在寫入資料時支援完整磁碟加密（FDE）。如果沒有儲存在韌體上的加密金鑰、就無法讀取資料。而加密金鑰則只能由驗證的節點存取。

瞭解NetApp硬體型加密

節點會使用從外部金鑰管理伺服器或Onboard Key Manager擷取的驗證金鑰、將自己驗證到自我加密磁碟機：

- 外部金鑰管理伺服器是儲存環境中的第三方系統、使用金鑰管理互通性傳輸協定（KMIP）為節點提供金鑰。最佳實務做法是在不同的儲存系統上設定外部金鑰管理伺服器與資料。
- 內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。

您可以使用NetApp Volume Encryption搭配硬體加密、在自我加密磁碟機上「雙重加密」資料。

啟用自我加密磁碟機時、核心傾印也會加密。

> 如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、您必須遵循主題中的指示 將FIPS磁碟機或SED恢復為無保護模式 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

支援的自我加密磁碟機類型

支援兩種自我加密磁碟機：

- 自我加密FIPS認證SAS或NVMe磁碟機可在FAS 所有的作業系統上支援AFF 。這些磁碟機稱為_FIPS磁碟

機_、符合美國聯邦資訊處理標準出版品1402、Level 2的要求。認證的功能除了提供加密保護之外、還能防止磁碟機遭受拒絕服務攻擊。FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。

- 從ONTAP 推出支援不通過FIPS測試的自我加密NVMe磁碟機開始、AFF 支援在32、320及更新版本系統上執行。這些磁碟機稱為_SED__、提供與FIPS磁碟機相同的加密功能、但可以與同一個節點或HA配對上的非加密磁碟機混合使用。
- 所有FIPS驗證的磁碟機都使用已通過FIPS驗證的韌體密碼編譯模組。 FIPS磁碟機密碼編譯模組不會使用磁碟機外部產生的任何金鑰（磁碟機的韌體密碼編譯模組會使用輸入磁碟機的驗證密碼來取得金鑰加密金鑰）。

非加密磁碟機是不是SED或FIPS磁碟機的磁碟機。

如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

何時使用外部金鑰管理

雖然使用內建金鑰管理程式的成本較低、而且通常更方便、但如果下列任一項屬實、您應該使用外部金鑰管理：

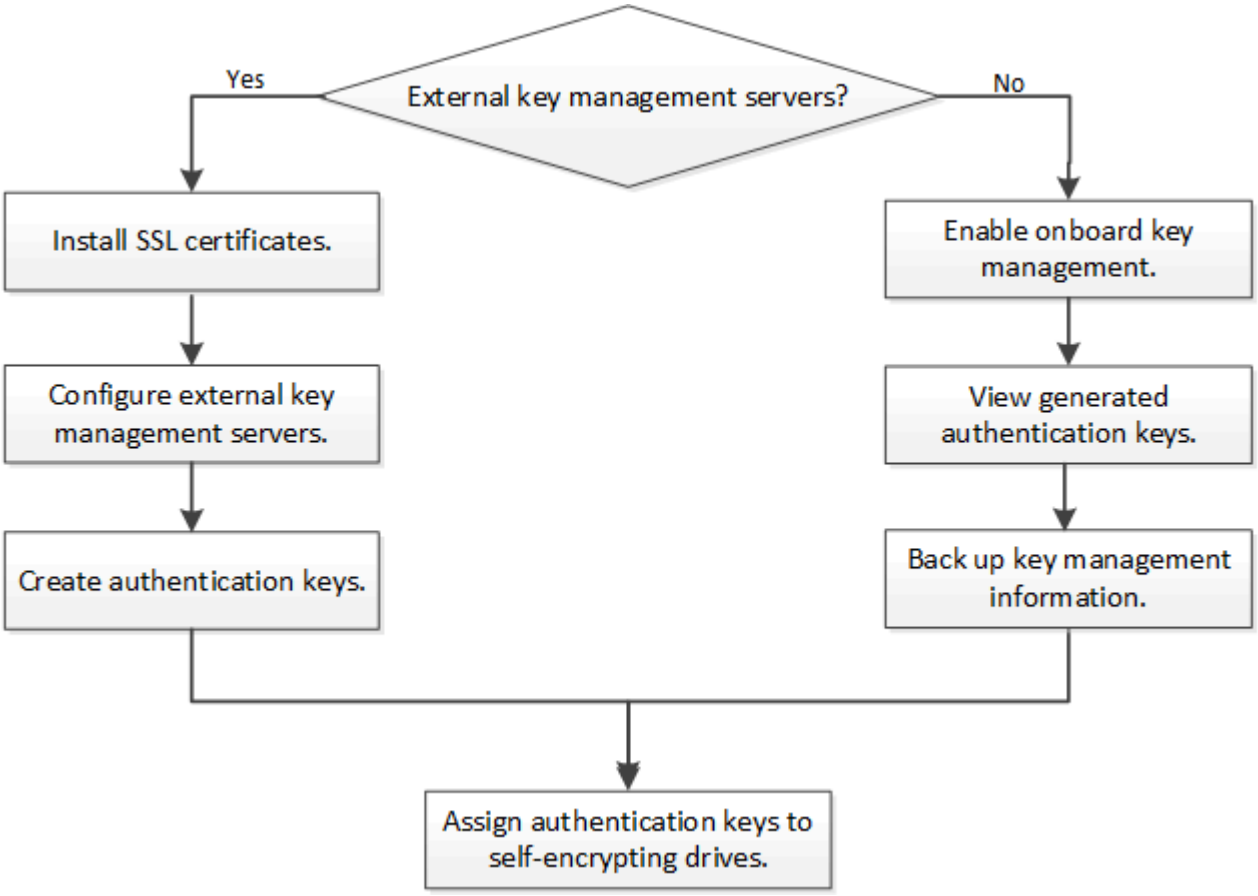
- 貴組織的原則需要使用FIPS 140-2第2級（或更高版本）密碼編譯模組的金鑰管理解決方案。
- 您需要一套多叢集解決方案、集中管理加密金鑰。
- 您的企業需要更高的安全性、將驗證金鑰儲存在系統或與資料不同的位置。

支援詳細資料

下表顯示重要的硬體加密支援詳細資料。如需支援的KMIP伺服器、儲存系統和磁碟櫃的最新資訊、請參閱互通性對照表。

資源或功能	支援詳細資料
非同質磁碟集	• FIPS磁碟機無法與同一個節點或HA配對上的其他類型磁碟機混合使用。符合的HA配對可與同一叢集中不符合要求的HA配對共存。 • SED可與同一節點或HA配對上的非加密磁碟機混合使用。
磁碟機類型	• FIPS磁碟機可以是SAS或NVMe磁碟機。 • SED必須是NVMe磁碟機。
10 Gb網路介面	KMIP金鑰管理組態從ONTAP 支援10 Gb網路介面開始、可與外部金鑰管理伺服器進行通訊。
用於與金鑰管理伺服器通訊的連接埠	從功能介紹9.3開始ONTAP 、您可以使用任何儲存控制器連接埠來與金鑰管理伺服器通訊。否則、您應該使用連接埠 e0M 與金鑰管理伺服器通訊。視儲存控制器機型而定、某些網路介面在開機程序期間可能無法用於與金鑰管理伺服器的通訊。
部分（MCC）MetroCluster	• NVMe磁碟機支援MCC。 • SAS磁碟機不支援MCC。

您必須先設定金鑰管理服務、叢集才能將自己驗證到自我加密磁碟機。您可以使用外部金鑰管理伺服器或內建金鑰管理程式。



相關資訊

- "NetApp Hardware Universe"
- "NetApp Volume Encryption與NetApp Aggregate Encryption"

設定外部金鑰管理

了解如何設定**ONTAP**外部金鑰管理

您可以使用一或多個外部金鑰管理伺服器來保護叢集用來存取加密資料的金鑰。外部金鑰管理伺服器是儲存環境中的第三方系統、使用金鑰管理互通性傳輸協定（KMIP）為節點提供金鑰。

NetApp Volume Encryption （ NVE ）可透過內建金鑰管理程式來實作。在更新版本的支援中、NVE可透過外部金鑰管理（KMIP）和內建金鑰管理程式來實作。ONTAP從 ONTAP 9.11.1 開始，您可以在叢集中設定多個外部金鑰管理員。請參閱 設定叢集式金鑰伺服器。

在**ONTAP**叢集上安裝 **SSL** 憑證

叢集與KMIP伺服器使用KMIP SSL憑證來驗證彼此的身分、並建立SSL連線。在使用KMIP伺服器設定SSL連線之前、您必須先安裝叢集的KMIP用戶端SSL憑證、以及KMIP伺服器

根憑證授權單位（CA）的SSL公開憑證。

關於這項工作

在HA配對中、兩個節點必須使用相同的公有和私有KMIP SSL憑證。如果您將多個HA配對連線至相同的KMIP伺服器、HA配對中的所有節點都必須使用相同的公有和私有KMIP SSL憑證。

開始之前

- 建立憑證、KMIP伺服器和叢集的伺服器上、必須同步時間。
- 您必須已取得叢集的公用SSL KMIP用戶端憑證。
- 您必須取得與叢集SSL KMIP用戶端憑證相關的私密金鑰。
- SSL KMIP用戶端憑證不得受密碼保護。
- 您必須已取得KMIP伺服器根憑證授權單位（CA）的SSL公開憑證。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝用戶端和伺服器憑證。

步驟

1. 安裝叢集的SSL KMIP用戶端憑證：

   ```
   security certificate install -vserver admin_svm_name -type client
   ```

   系統會提示您輸入SSL KMIP公開和私有憑證。

   ```
   cluster1::> security certificate install -vserver cluster1 -type client
   ```

2. 安裝KMIP伺服器根憑證授權單位（CA）的SSL公開憑證：

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

   ```
   cluster1::> security certificate install -vserver cluster1 -type server-ca
   ```

相關資訊

- "安全性憑證安裝"

在**ONTAP 9.6** 及更高版本中啟用基於硬體的加密的外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

從 ONTAP 9.11.1 開始、每個主要金鑰伺服器最多可新增 3 個次要金鑰伺服器、以建立叢集金鑰伺服器。如需詳細資訊、請參閱 設定叢集式外部金鑰伺服器。

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。

- 在MetroCluster環境中：
  - 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
  - 您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集的金鑰管理程式連線：

```
security key-manager external enable -vserver admin_SVM -key-servers
host_name|IP_address:port,... -client-cert client_certificate -server-ca-cert
server_CA_certificates
```

> ◦ 命令會 `security key-manager external enable`取代 `security key-manager setup`命令。您可以執行 `security key-manager external modify`命令來變更外部金鑰管理組態。如"指令參考資料ONTAP"需詳細 `security key-manager external enable`資訊，請參閱。
> ◦ 在支援管理SVM的環境中、如果您要設定外部金鑰管理、則必須重複執行MetroCluster `security key-manager external enable` 合作夥伴叢集上的命令。

下列命令可啟用的外部金鑰管理 `cluster1` 使用三個外部金鑰伺服器。第一個金鑰伺服器是使用其主機名稱和連接埠來指定、第二個金鑰伺服器是使用IP位址和預設連接埠來指定、第三個金鑰伺服器則是使用IPv6位址和連接埠來指定：

```
clusterl::> security key-manager external enable -key-servers
ks1.local:15696,10.0.0.10,[fd20:8b1e:b255:814e:32bd:f35c:832c:5a09]:1234
-client-cert AdminVserverClientCert -server-ca-certs
AdminVserverServerCaCert
```

2. 確認所有已設定的KMIP伺服器均已連線：

```
security key-manager external show-status -node node_name -vserver SVM -key
-server host_name|IP_address:port -key-server-status available|not-
responding|unknown
```

> 命令會 `security key-manager external show-status`取代 `security key-manager show -status`命令。如"指令參考資料ONTAP"需詳細 `security key-manager external show-status`資訊，請參閱。

```
cluster1::> security key-manager external show-status

Node  Vserver  Key Server                                       Status
----  -------  ------------------------------------
-------------
node1
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available
node2
      cluster1
               10.0.0.10:5696                                   available
               fd20:8b1e:b255:814e:32bd:f35c:832c:5a09:1234   available
               ks1.local:15696                                  available

6 entries were displayed.
```

相關資訊

- 設定叢集式外部金鑰伺服器
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員外部顯示狀態"

在**ONTAP 9.5** 及更早版本中啟用基於硬體的加密的外部金鑰管理

您可以使用一或多個KMIP伺服器來保護叢集用來存取加密資料的金鑰。您最多可將四個KMIP伺服器連線至一個節點。建議至少使用兩部伺服器來進行備援和災難恢復。

關於這項工作

可為叢集中的所有節點設定KMIP伺服器連線。ONTAP

開始之前

- KMIP SSL用戶端和伺服器憑證必須已安裝。
- 您必須是叢集管理員才能執行此工作。
- 在設定外部金鑰管理程式之前、您必須先設定MetroCluster 此解決方案。
- 在 MetroCluster 環境中、您必須在兩個叢集上安裝相同的 KMIP SSL 憑證。

步驟

1. 設定叢集節點的金鑰管理程式連線：

   ```
   security key-manager setup
   ```

   金鑰管理程式設定隨即開始。

在MetroCluster環境中，您必須在兩個叢集上執行此命令。詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

2. 在每個提示字元輸入適當的回應。
3. 新增KMIP伺服器：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.1
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

4. 新增額外的KMIP伺服器以提供備援：

   `security key-manager add -address key_management_server_ipaddress`

   ```
   clusterl::> security key-manager add -address 20.1.1.2
   ```

   在這個不支援的環境中、您必須在兩個叢集上執行此命令MetroCluster 。

5. 確認所有已設定的KMIP伺服器均已連線：

   `security key-manager show -status`

   詳細了解此過程中所述的命令"指令參考資料ONTAP"。

   ```
   cluster1::> security key-manager show -status

   Node             Port      Registered Key Manager  Status
   --------------   ----      ----------------------  ---------------
   cluster1-01      5696      20.1.1.1                available
   cluster1-01      5696      20.1.1.2                available
   cluster1-02      5696      20.1.1.1                available
   cluster1-02      5696      20.1.1.2                available
   ```

6. 也可以將純文字磁碟區轉換為加密磁碟區。

   `volume encryption conversion start`

   在轉換磁碟區之前、必須先完整設定外部金鑰管理程式。在 MetroCluster 環境中、必須在兩個站台上設定外部金鑰管理員。

從ONTAP 9.11.1 開始，您可以在 SVM 上設定與叢集外部金鑰管理伺服器的連線。使用叢集金鑰伺服器，您可以在 SVM 上指定主金鑰伺服器和輔助金鑰伺服器。註冊或檢索金鑰時， ONTAP首先嘗試存取主密鑰伺服器，然後依序嘗試存取輔助伺服器，直到操作成功完成。

您可以使用外部金鑰伺服器來取得NetApp儲存加密 (NSE)、 NetApp磁碟區加密 (NVE) 和NetApp聚合加密 (NAE) 金鑰。一個 SVM 最多可以支援四個主外部 KMIP 伺服器。每個主伺服器最多可支援三個輔助密鑰伺服器。

關於這項工作

- 此程序僅支援使用KMIP的主要伺服器。如需支援的金鑰伺服器清單、請查看 "NetApp 互通性對照表工具"。

開始之前

- "必須為 SVM 啟用 KMIP 金鑰管理"。
- 叢集中的所有節點都必須執行ONTAP 版本不符合要求的9.11.1或更新版本。
- 伺服器的排列順序 `-secondary-key-servers`此參數反映了外部金鑰管理（KMIP）伺服器的存取順序。

建立叢集式金鑰伺服器

組態程序取決於您是否已設定主要金鑰伺服器。

將主要和次要金鑰伺服器新增至**SVM**

步驟

1. 確認叢集（admin SVM）未啟用任何金鑰管理功能：

   ```
   security key-manager external show -vserver <svm_name>
   ```

   如果 SVM 已啟用最多四個主金鑰伺服器，則必須先刪除一個現有的主金鑰伺服器，然後再新增新的主金鑰伺服器。

2. 啟用主密鑰管理器：

   ```
   security key-manager external enable -vserver <svm_name> -key-servers
   <primary_key_server_ip> -client-cert <client_cert_name> -server-ca-certs
   <server_ca_cert_names>
   ```

   - 如果您沒有在參數中指定端口， `-key-servers`如果使用參數，則預設使用連接埠 5696。

   > 如果你正在運行 `security key-manager external enable`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

3. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

   > 如果你正在運行 `security key-manager external`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

新增次要金鑰伺服器至現有的主要金鑰伺服器

步驟

1. 修改主密鑰伺服器，新增輔助密鑰伺服器。這 `-secondary-key-servers`此參數接受一個以逗號分隔的列表，最多可包含三個金鑰伺服器：

   ```
   security key-manager external modify-server -vserver <svm_name> -key
   -servers <primary_key_server> -secondary-key-servers <list_of_key_servers>
   ```

   - 請勿在輔助密鑰伺服器中包含連接埠號碼。 `-secondary-key-servers`範圍。它使用與主密鑰伺服器相同的連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。 NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

有關輔助密鑰伺服器的更多信息，請參閱 [mod-secondary]。

修改叢集式金鑰伺服器

您可以透過新增和刪除輔助金鑰伺服器、變更輔助金鑰伺服器的存取順序或變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）來修改叢集外部金鑰伺服器。如果在MetroCluster配置中修改叢集外部金鑰伺服器，NetApp強烈建議在兩個叢集上使用相同的金鑰伺服器。

修改次要金鑰伺服器

使用 `security key-manager external modify-server` 指令的 `-secondary-key-servers` 參數來管理次要金鑰伺服器。這 `-secondary-key-servers` 參數接受以逗號分隔的清單。清單中輔助密鑰伺服器的指定順序決定了輔助密鑰伺服器的存取順序。您可以透過執行指令 `security key-manager external modify-server`，並以不同順序輸入次要金鑰伺服器，來修改存取順序。輔助密鑰伺服器無需提供連接埠號碼。

如果你正在運行 `security key-manager external modify-server`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

若要移除輔助密鑰伺服器，請將要保留的密鑰伺服器新增至清單中。 `-secondary-key-servers`參數，並省略要刪除的參數。若要刪除所有輔助密鑰伺服器，請使用下列參數 `-`表示無。

轉換主要和次要金鑰伺服器

您可以使用下列步驟變更特定金鑰伺服器的指定（主金鑰伺服器或輔助金鑰伺服器）。

將主密鑰伺服器轉換為輔助密鑰伺服器

步驟

1. 從SVM中移除主密鑰伺服器：

```
security key-manager external remove-servers
```

> 如果你正在運行 `security key-manager external remove-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。

2. 執行[建立叢集式金鑰伺服器]使用原主密鑰伺服器作為輔助密鑰伺服器進行此程序。

將輔助金鑰伺服器轉換為主金鑰伺服器

步驟

1. 從現有的主密鑰伺服器移除輔助密鑰伺服器：

```
security key-manager external modify-server -secondary-key-servers
```

- 如果你正在運行 `security key-manager external modify-server -secondary-key-servers`對於MetroCluster配置中的管理 SVM 指令，必須在兩個叢集上執行此命令。如果你要為單一資料 SVM 執行命令，則無需在兩個叢集上執行該命令。
- 如果在刪除現有密鑰伺服器的同時將輔助密鑰伺服器轉換為主密鑰伺服器，則在完成刪除和轉換之前嘗試新增新的密鑰伺服器可能會導緻密鑰重複。

1. 執行[建立叢集式金鑰伺服器]使用原輔助金鑰伺服器作為新叢集金鑰伺服器的主金鑰伺服器進行此程序。

請參閱[mod-secondary]了解更多。

相關資訊

- 了解更多 `security key-manager external`在"指令參考資料ONTAP"

建立**ONTAP** 驗證金鑰、請使用**32**個以上版本

您可以使用 `security key-manager key create` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的 FIPS 法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用Onboard Key Manager時、不支援此命令。不過、啟用Onboard Key Manager時、會自動建立兩個驗證金鑰。您可以使用下列命令來檢視金鑰：

```
security key-manager key query -key-type NSE-AK
```

- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。
- 您可以使用 `security key-manager key delete`命令刪除任何未使用的金鑰。 `security key-manager key delete`如果指定金鑰目前正由 ONTAP 使用，則命令會失敗。（ Privileges 必須大於 `admin`才能使用此命令。）

> 在支援功能環境中、刪除金鑰之前、您必須先確定合作夥伴叢集上沒有使用金鑰MetroCluster。您可以在合作夥伴叢集上使用下列命令、檢查金鑰是否未被使用：
>
> - `storage encryption disk show -data-key-id <key-id>`
> - `storage encryption disk show -fips-key-id <key-id>`

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

```
security key-manager key create -key-tag <passphrase_label> -prompt-for
-key true|false
```

> 此設定 `prompt-for-key=true`會讓系統提示叢集管理員在驗證加密磁碟機時使用複雜密碼。否則、系統會自動產生32位元組的通關密碼。命令會 `security key-manager key create`取代 `security key-manager create-key`命令。如"指令參考資料ONTAP"需詳細 `security key-manager key create`資訊，請參閱。

下列範例會建立的驗證金鑰 `cluster1`，自動產生 32 位元組的複雜密碼：

```
cluster1::> security key-manager key create
Key ID: <id_value>
```

2. 確認已建立驗證金鑰：

```
security key-manager key query -node node
```

> 命令會 `security key-manager key query`取代 `security key-manager query key`命令。
>
> 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

```
cluster1::> security key-manager key query
       Vserver: cluster1
   Key Manager: external
          Node: node1

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node1                                    NSE-AK    yes
    Key ID: <id_value>
node1                                    NSE-AK    yes
    Key ID: <id_value>

       Vserver: cluster1
   Key Manager: external
          Node: node2

Key Tag                                  Key Type  Restored
---------------------------------------  --------  --------
node2                                    NSE-AK    yes
    Key ID: <id_value>
node2                                    NSE-AK    yes
    Key ID: <id_value>
```

如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

相關資訊

- "儲存加密磁碟顯示"

在**ONTAP** 更新版本的版本中建立驗證金鑰

您可以使用 `security key-manager create-key` 命令可建立節點的驗證金鑰、並將其儲存在設定的 KMIP 伺服器上。

關於這項工作

如果您的安全性設定要求您使用不同的金鑰進行資料驗證和FIPS 140-2驗證、您應該為每個金鑰建立個別的金鑰。如果情況並非如此、您可以使用與資料存取相同的FIPS法規遵循驗證金鑰。

此功能可為叢集中的所有節點建立驗證金鑰。ONTAP

- 啟用內建金鑰管理時、不支援此命令。
- 如果設定的金鑰管理伺服器已儲存超過128個驗證金鑰、您會收到警告。

  您可以使用金鑰管理伺服器軟體刪除任何未使用的金鑰、然後再次執行命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 建立叢集節點的驗證金鑰：

   `security key-manager create-key`

   如"指令參考資料ONTAP"需詳細 `security key-manager create-key`資訊，請參閱。

   > 輸出中顯示的金鑰ID是用來參照驗證金鑰的識別碼。它不是實際的驗證金鑰或資料加密金鑰。

   下列範例會建立的驗證金鑰 `cluster1`：

   ```
   cluster1::> security key-manager create-key
      (security key-manager create-key)
   Verifying requirements...

   Node: cluster1-01
   Creating authentication key...
   Authentication key creation successful.
   Key ID: <id_value>

   Node: cluster1-01
   Key manager restore operation initialized.
   Successfully restored key information.

   Node: cluster1-02
   Key manager restore operation initialized.
   Successfully restored key information.
   ```

2. 確認已建立驗證金鑰：

   `security key-manager query`

   如"指令參考資料ONTAP"需詳細 `security key-manager query`資訊，請參閱。

   下列範例會驗證是否已為建立驗證金鑰 `cluster1`：

```
cluster1::> security key-manager query

  (security key-manager query)

          Node: cluster1-01
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-01     NSE-AK    yes
       Key ID: <id_value>


          Node: cluster1-02
   Key Manager: 20.1.1.1
 Server Status: available

Key Tag         Key Type  Restored
--------------  --------  --------
cluster1-02     NSE-AK    yes
       Key ID: <id_value>
```

使用**ONTAP**外部金鑰管理將資料驗證金鑰指派給 **FIPS** 磁碟機或 **SED**

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來鎖定或解除鎖定磁碟機上的加密資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

此程序不會中斷營運。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

   `storage encryption disk modify -disk` *`disk_ID`* `-data-key-id` *`key_ID`*

   如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

   > 您可以使用 `security key-manager query -key-type NSE-AK` 檢視金鑰ID的命令。

```
cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
<id_value>

Info: Starting modify on 14 disks.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

2. 確認已指派驗證金鑰：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
[...]
```

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

設定內建金鑰管理

啟用更新版本的更新版本、以利執行內建金鑰管理**ONTAP**

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用Onboard Key Manager來保護叢集用來存取加密資料的金鑰。您必須在每個存取加密磁碟區或自我加密磁碟的叢集上啟用Onboard Key Manager。

關於這項工作

您必須執行 `security key-manager onboard enable` 每次將節點新增至叢集時的命令。在 MetroCluster 組態中、您必須執行 `security key-manager onboard enable` 先在本機叢集上執行 `security key-manager onboard sync` 在遠端叢集上、使用相同的複雜密碼。

詳細了解 `security key-manager onboard enable`和 `security key-manager onboard sync`在"指令參考資料ONTAP"。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。除了在 MetroCluster 中、您可以使用 `cc-`

`mode-enabled=yes` 選項要求使用者在重新開機後輸入複雜密碼。

> 當「內建金鑰管理程式」在「一般條件」模式中啟用時 (`cc-mode-enabled=yes`）、系統行為會以下列方式變更：
>
> - 系統會監控在「一般準則」模式下運作時、連續嘗試失敗的叢集密碼。
>
> 如果已啟用NetApp儲存加密（NSE）、且您在開機時未輸入正確的叢集密碼、則系統將無法驗證其磁碟機並自動重新開機。若要修正此問題、您必須在開機提示字元中輸入正確的叢集密碼。一旦開機、系統最多可連續5次嘗試在24小時內、針對任何需要叢集密碼作為參數的命令、正確輸入叢集密碼。如果達到限制（例如、您連續5次未正確輸入叢集密碼）、則必須等待24小時逾時期間、或是重新啟動節點、才能重設限制。
>
> - 系統映像更新會使用NetApp RSA-3072程式碼簽署憑證搭配SHA-384程式碼簽署摘要、來檢查映像完整性、而非一般的NetApp RSA-2048程式碼簽署憑證和SHA-256程式碼簽署摘要。
>
> 升級命令透過檢查各種數位簽名來驗證影像內容是否已更改或損壞。如果驗證有效，映像更新將進入下一步。如果驗證無效，則影像更新失敗。詳細了解 `cluster image`在"指令參考資料ONTAP"。

> Onboard Key Manager可將金鑰儲存在揮發性記憶體中。當系統重新開機或停止時、揮發性記憶體內容會被清除。在正常操作條件下、系統停止時、揮發性記憶體內容將在30秒內清除。

開始之前

- 如果您使用NSE搭配外部金鑰管理（KMIP）伺服器、則必須刪除外部金鑰管理程式資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在設定Onboard Key Manager之前、您必須先設定MetroCluster 這個靜態環境。

步驟

1. 啟動金鑰管理程式設定命令：

   ```
   security key-manager onboard enable -cc-mode-enabled yes|no
   ```

   > 設 `cc-mode-enabled=yes`為要求使用者在重新開機後輸入金鑰管理密碼。MetroCluster 組態不支援此 `- cc-mode-enabled`選項。命令會 `security key-manager onboard enable`取代 `security key-manager setup`命令。

   下列範例會在叢集1上啟動金鑰管理程式設定命令、而不要求在每次重新開機後輸入通關密碼：

2. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“`cc-mode`”，輸入一個介於 64 到 256 個字元之間的密碼。

   > 如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

3. 在通關密碼確認提示下、重新輸入通關密碼。

4. 驗證系統是否建立了身份驗證金鑰：

   ```
   security key-manager key query -node node
   ```

   命令會 `security key-manager key query`取代 `security key-manager query key`命令。

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

完成後

將通關密碼複製到儲存系統外部的安全位置、以供未來使用。

系統會自動將關鍵管理資訊備份到叢集的複製資料庫（RDB）。您還應該手動備份此資訊以用於災難復原。

相關資訊

- "叢集影像命令"
- "安全金鑰管理員外部啟用"
- "安全金鑰管理員金鑰查詢"
- "安全金鑰管理員板載啟用"
- "從外部金鑰管理移轉至內建金鑰管理"

啟用更新版本的更新版本**ONTAP**

您可以使用Onboard Key Manager驗證FIPS磁碟機或SED的叢集節點。內建金鑰管理程式是一項內建工具、可從與資料相同的儲存系統、為節點提供驗證金鑰。Onboard Key Manager符合FIPS-140-2第1級標準。

您可以使用板載金鑰管理器來保護叢集用於存取加密資料的金鑰。在存取加密磁碟區或自加密磁碟的每個叢集上啟用板載金鑰管理器。

關於這項工作

您必須執行 `security key-manager setup` 每次將節點新增至叢集時的命令。

如果您使用MetroCluster 的是「不確定」組態、請參閱下列準則：

- 在 ONTAP 9.5 中、您必須執行 `security key-manager setup` 在本機叢集和上 `security key-manager setup -sync-metrocluster-config yes` 在遠端叢集上、使用相同的複雜密碼。
- 在 ONTAP 9.5 之前、您必須執行 `security key-manager setup` 在本機叢集上、等待大約 20 秒、然後執行 `security key-manager setup` 在遠端叢集上、使用相同的複雜密碼。

根據預設、當節點重新開機時、您不需要輸入金鑰管理程式密碼。從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 選項要求使用者在重新開機後輸入複雜密碼。

如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。適用於 `volume create`，您不需要指定 `-encrypt true`。適用於 `volume move start`，您不需要指定 `-encrypt-destination true`。

密碼嘗試失敗後、您必須重新啟動節點。

開始之前

- 如果您將 NSE 與外部金鑰管理 (KMIP) 伺服器一起使用，請刪除外部金鑰管理器資料庫。

  "從外部金鑰管理移轉至內建金鑰管理"

- 您必須是叢集管理員才能執行此工作。
- 在配置板載金鑰管理器之前，請先配置MetroCluster環境。

步驟

1. 啟動金鑰管理程式設定：

   ```
   security key-manager setup -enable-cc-mode yes|no
   ```

   從 ONTAP 9.4 開始、您可以使用 `-enable-cc-mode yes` 此選項可要求使用者在重新開機後輸入金鑰管理密碼。如果您已設定、則適用於 NVE `-enable-cc-mode yes`、您使用建立的磁碟區 `volume create` 和 `volume move start` 命令會自動加密。

   下列範例會在叢集1上開始設定金鑰管理程式、而不要求在每次重新開機後輸入通關密碼：

   ```
   cluster1::> security key-manager setup
   Welcome to the key manager setup wizard, which will lead you through
   the steps to add boot information.

   ...

   Would you like to use onboard key-management? {yes, no} [yes]:
   Enter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   Reenter the cluster-wide passphrase:    <32..256 ASCII characters long
   text>
   ```

2. 輸入 `yes` 在提示下設定內建金鑰管理。
3. 在通關密碼提示字元中、輸入32到256個字元之間的通關密碼、或輸入「'cc-mode'」（64到256個字元之間的通關密碼）。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。
5. 驗證是否已為所有節點設定金鑰：

   ```
   security key-manager show-key-store
   ```

詳細了解 `security key-manager show-key-store`在"指令參考資料ONTAP"。

```
cluster1::> security key-manager show-key-store

Node: node1
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK

Node: node2
Key Store: onboard
Key ID                                                               Used By
-----------------------------------------------------------------------
--------
<id_value> NSE-AK
<id_value> NSE-AK
```

完成後

ONTAP會自動將金鑰管理資訊備份到叢集的複製資料庫 (RDB)。

設定板載金鑰管理器密碼後，請手動將資訊備份到儲存系統外部的安全位置。看"手動備份內建金鑰管理資訊"。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式設定"
- "安全金鑰管理員顯示金鑰庫"
- "從外部金鑰管理移轉至內建金鑰管理"

使用**ONTAP**板載金鑰管理將資料驗證金鑰指派給 **FIPS** 磁碟機或 **SED**

您可以使用 `storage encryption disk modify` 命令將資料驗證金鑰指派給 FIPS 磁碟機或 SED 。叢集節點使用此金鑰來存取磁碟機上的資料。

關於這項工作

自我加密磁碟機只有在驗證金鑰ID設定為非預設值時、才會受到保護、不受未獲授權的存取。製造商安全ID（MSID）具有金鑰ID 0x0、是SAS磁碟機的標準預設值。對於NVMe磁碟機、標準預設值為null金鑰、表示為空白金鑰ID。當您將金鑰ID指派給自我加密磁碟機時、系統會將其驗證金鑰ID變更為非預設值。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 指派資料驗證金鑰給FIPS磁碟機或SED：

   `storage encryption disk modify -disk disk_ID -data-key-id key_ID`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk modify`資訊，請參閱。

   > 您可以使用 `security key-manager key query -key-type NSE-AK` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 0.10.* -data-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

2. 確認已指派驗證金鑰：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   [...]
   ```

相關資訊

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

將 FIPS 140-2 身份驗證金鑰指派給ONTAP FIPS 驅動器

您可以使用 `storage encryption disk modify` 命令 `-fips-key-id` 將 FIPS 140-2 驗證金鑰指派給 FIPS 磁碟機的選項。叢集節點將此金鑰用於資料存取以外的磁碟機作業、例如防止磁碟機遭受拒絕服務攻擊。

關於這項工作

您的安全設定可能需要使用不同的金鑰來進行資料驗證和FIPS 140-2驗證。如果情況並非如此、您可以使用與資料存取相同的FIPS法規遵循驗證金鑰。

此程序不會中斷營運。

開始之前

磁碟機韌體必須支援FIPS 140-2規範。。 "NetApp 互通性對照表工具" 包含支援磁碟機韌體版本的相關資訊。

步驟

1. 您必須先確定已指派資料驗證金鑰。您可以使用來完成這項作業 外部金鑰管理程式 或是 內建金鑰管理程式。確認已使用命令指派金鑰 `storage encryption disk show`。
2. 指派FIPS 140-2驗證金鑰給SED：

   ```
   storage encryption disk modify -disk disk_id -fips-key-id
   fips_authentication_key_id
   ```

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.* -fips-key-id
   <id_value>

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

3. 確認已指派驗證金鑰：

   ```
   storage encryption disk show -fips
   ```

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show -fips
   Disk    Mode FIPS-Compliance Key ID
   ------  ----
   ------------------------------------------------------------------------
   2.10.0  full <id_value>
   2.10.1  full <id_value>
   [...]
   ```

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

在 **ONTAP** 中啟用適用於 **KMIP** 伺服器連線的叢集範圍 **FIPS** 相容模式

您可以使用 `security config modify` 命令 `-is-fips-enabled` 選項可啟用全叢集

FIPS 相容模式、以供傳輸中的資料使用。如此會強制叢集在連接KMIP伺服器時、以FIPS模式使用OpenSSL。

關於這項工作

當您啟用全叢集FIPS相容模式時、叢集將只自動使用TLS1.2和FIPS驗證的密碼套件。預設會停用全叢集FIPS相容模式。

您必須在修改整個叢集的安全性組態之後、手動重新開機叢集節點。

開始之前

- 儲存控制器必須設定為FIPS相容模式。
- 所有KMIP伺服器都必須支援TLSv1.2。啟用叢集範圍FIPS相容模式時、系統需要TLSv1.2才能完成KMIP伺服器的連線。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 驗證是否支援TLSv1.2：

   ```
   security config show -supported-protocols
   ```

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

   ```
   cluster1::> security config show
             Cluster                                                 Cluster
   Security
   Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
   Ready
   --------- ---------- ----------------------- -----------------
   ----------------
   SSL       false      TLSv1.2, TLSv1.1, TLSv1 ALL:!LOW:         yes
                                                !aNULL:!EXP:
                                                !eNULL
   ```

3. 啟用全叢集FIPS相容模式：

   ```
   security config modify -is-fips-enabled true -interface SSL
   ```

   如"指令參考資料ONTAP"需詳細 `security config modify`資訊，請參閱。

4. 手動重新啟動叢集節點。
5. 確認已啟用全叢集FIPS相容模式：

   ```
   security config show
   ```

```
cluster1::> security config show
          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       true       TLSv1.2, TLSv1.1        ALL:!LOW:         yes
                                              !aNULL:!EXP:
                                              !eNULL:!RC4
```

管理NetApp加密

取消 ONTAP 中的 Volume 資料加密

您可以使用 `volume move start` 用於移動和取消加密 Volume 資料的命令。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並取消加密磁碟區上的資料：

   `volume move start -vserver` *`SVM_name`* `-volume volume_name -destination-aggregate` *`aggregate_name`* `-encrypt-destination false`

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並取消加密磁碟區上的資料：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3 -encrypt-destination false
   ```

   系統會刪除磁碟區的加密金鑰。磁碟區上的資料未加密。

2. 確認磁碟區已停用加密：

   `volume show -encryption`

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

   下列命令會顯示磁碟區是否開啟 `cluster1` 已加密：

```
cluster1::> volume show -encryption

Vserver  Volume   Aggregate   State    Encryption State
-------  ------   ---------   -----    ----------------
vs1      vol1     aggr1       online   none
```

在 **ONTAP** 中移動加密磁碟區

您可以使用 `volume move start` 用於移動加密磁碟區的命令。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

如果目的地節點或目的地Volume不支援Volume加密、則移動將會失敗。

。 `-encrypt-destination` 的選項 `volume move start` 加密磁碟區的預設值為 true 。指定您不希望目的地 Volume 加密的要求、可確保您不會不小心將磁碟區上的資料解密。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有的加密磁碟區、並將磁碟區上的資料保持加密狀態：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`*

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume `vol1` 至目的地 Aggregate `aggr3` 並將磁碟區上的資料加密：

   ```
   cluster1::> volume move start -vserver vs1 -volume vol1 -destination
   -aggregate aggr3
   ```

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

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

   下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr3     online    RW  200GB    160.0GB  20%
```

使用 **ONTAP** 中的 **Volume Encryption rekey start** 命令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。從功能介紹9.3開始ONTAP 、您可以使用 `volume encryption rekey start` 變更加密金鑰的命令。

關於這項工作

重新輸入作業一旦開始、就必須完成。不會返回舊金鑰。如果您在作業期間遇到效能問題、可以執行 `volume encryption rekey pause` 暫停作業的命令、以及 `volume encryption rekey resume` 命令以恢復作業。

在重新輸入作業完成之前、磁碟區會有兩個按鍵。新的寫入及其對應的讀取將使用新的金鑰。否則、讀取將使用舊的金鑰。

您無法使用 `volume encryption rekey start` 重新輸入 SnapLock Volume 。

步驟

1. 變更加密金鑰：

   `volume encryption rekey start -vserver SVM_name -volume volume_name`

   下列命令會變更的加密金鑰 `vol1` 在 SVM 上`vs1`：

   ```
   cluster1::> volume encryption rekey start -vserver vs1 -volume vol1
   ```

2. 確認重新輸入作業的狀態：

   `volume encryption rekey show`

   如"指令參考資料ONTAP"需詳細 `volume encryption rekey show`資訊，請參閱。

   下列命令會顯示重新輸入作業的狀態：

   ```
   cluster1::> volume encryption rekey show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   ---------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. 重新輸入作業完成後、請確認磁碟區已啟用加密功能：

   `volume show -is-encrypted true`

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

   下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver   Volume   Aggregate    State    Type     Size  Available  Used
-------   ------   ---------    -----    ----     -----  ---------  ----
vs1       vol1     aggr2      online       RW   200GB     160.0GB   20%
```

使用**ONTAP**磁碟區移動啟動指令變更磁碟區的加密金鑰

定期變更磁碟區的加密金鑰是安全性最佳做法。您可以使用 `volume move start`命令來變更加密金鑰。移動的磁碟區可以位於相同的集合體或不同的集合體上。

關於這項工作

您無法使用 `volume move start` 重新輸入 SnapLock 或 FlexGroup 磁碟區。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 移動現有磁碟區並變更加密金鑰：

   `volume move start -vserver` *`SVM_name`* `-volume` *`volume_name`* `-destination-aggregate` *`aggregate_name`* `-generate-destination-key true`

   如"指令參考資料ONTAP"需詳細 `volume move start`資訊，請參閱。

   下列命令會移動名為的現有 Volume **`vol1`** 至目的地 Aggregate **`aggr2`** 並變更加密金鑰：

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -generate-destination-key true
```

   系統會為磁碟區建立新的加密金鑰。磁碟區上的資料仍保持加密狀態。

2. 確認磁碟區已啟用加密：

   `volume show -is-encrypted true`

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

下列命令會顯示上的加密磁碟區 `cluster1`：

```
cluster1::> volume show -is-encrypted true

Vserver  Volume  Aggregate  State  Type  Size  Available  Used
-------  ------  ---------  -----  ----  -----  ---------  ----
vs1      vol1    aggr2      online    RW  200GB    160.0GB  20%
```

輪換ONTAP NetApp儲存加密的驗證金鑰

使用NetApp儲存加密（NSE）時、您可以旋轉驗證金鑰。

關於這項工作

如果您使用外部金鑰管理程式（KMIP）、則可支援NSE環境中的旋轉驗證金鑰。

Onboard Key Manager（OKM）不支援NSE環境中的旋轉驗證金鑰。

步驟

1. 使用 `security key-manager create-key` 產生新驗證金鑰的命令。

   您必須先產生新的驗證金鑰、才能變更驗證金鑰。

2. 使用 `storage encryption disk modify -disk * -data-key-id` 變更驗證金鑰的命令。

相關資訊

- "儲存加密磁碟修改"

刪除 ONTAP 中的加密磁碟區

您可以使用 `volume delete` 刪除加密磁碟區的命令。

開始之前

- 您必須是叢集管理員才能執行此工作。
- Volume必須離線。

步驟

1. 刪除加密磁碟區：

   `volume delete -vserver` *`SVM_name`* `-volume` *`volume_name`*

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

   下列命令會刪除名為的加密磁碟區 `vol1`：

```
cluster1::> volume delete -vserver vs1 -volume vol1
```

輸入 `yes` 當系統提示您確認刪除時。

系統會在24小時後刪除磁碟區的加密金鑰。

與選項搭配 `-force true`使用 `volume delete`，可立即刪除磁碟區並銷毀對應的加密金鑰。此命令需要進階權限。如"指令參考資料ONTAP"需詳細 `volume delete`資訊，請參閱。

完成後

您可以使用 `volume recovery-queue` 發出後在保留期間內恢復已刪除磁碟區的命令 `volume delete` 命令：

`volume recovery-queue` *SVM_name* `-volume` *volume_name*

"如何使用Volume Recovery功能"

安全地清除加密磁碟區上的資料

了解如何安全地從加密**ONTAP**磁碟區中清除數據

從支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的情況下清除資料。ONTAP加密磁碟區上的資料清理功能可確保資料無法從實體媒體中恢復、例如在「資源回收」的情況下、資料追蹤可能會在區塊遭到覆寫時留下、或是安全地刪除租戶的資料。

安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。您無法清理未加密的Volume。您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

使用安全清除的考量事項

- 在啟用NetApp Aggregate Encryption（NAE）的Aggregate中建立的磁碟區不支援安全清除。
- 安全清除僅適用於已啟用NVE的磁碟區上先前刪除的檔案。
- 您無法清理未加密的Volume。
- 您必須使用KMIP伺服器來提供金鑰、而非內建金鑰管理程式。

視ONTAP 您的版本而定、安全清除功能會有所不同。

更新版本**ONTAP**

- 支援安全清除MetroCluster 功能的不受支援。FlexGroup
- 如果要清除的磁碟區是SnapMirror關係的來源、您就不需要中斷SnapMirror關係、就能執行安全的清除。
- 對於使用SnapMirror資料保護的磁碟區而言、重新加密方法不同於未使用SnapMirror資料保護（DP）或使用SnapMirror延伸資料保護的磁碟區。
  - 根據預設、使用SnapMirror資料保護（DP）模式的磁碟區會使用Volume Move Re-Encryption方法重新加密資料。
  - 根據預設、未使用SnapMirror資料保護的磁碟區或使用SnapMirror延伸資料保護（XDP）模式的磁碟區、會使用就地重新加密方法。
  - 您可以使用變更這些預設值 `secure purge re-encryption-method [volume-move|in-place-rekey]` 命令。
- 根據預設， FlexVol 磁碟區中的所有快照都會在安全清除作業期間自動刪除。根據預設、FlexGroup 在安全清除作業期間、不會自動刪除使用SnapMirror資料保護的所有SnapMirror Volume和Snapshot快照。您可以使用命令變更這些預設值 `secure purge delete-all-snapshots [true|false]`。

更新版本：**ONTAP**

- 安全清除不支援下列項目：
  - FlexClone
  - SnapVault
  - FabricPool
- 如果要清除的磁碟區是SnapMirror關係的來源、您必須先中斷SnapMirror關係、才能清除該磁碟區。

  如果磁碟區中有忙碌的快照，您必須先釋放快照，才能清除磁碟區。例如、您可能需要從其父磁碟區分割FlexClone磁碟區。

- 成功叫用安全清除功能會觸發磁碟區移動、以新金鑰重新加密其餘未清除的資料。

  移動的磁碟區會保留在目前的Aggregate上。舊金鑰會自動銷毀、確保清除的資料無法從儲存媒體中恢復。

從沒有**SnapMirror**關係的加密**ONTAP**磁碟區中清理數據

從使用支援NVE的磁碟區開始、您可以使用安全清除功能、在不中斷營運的「crub」資料中進行安全清除。ONTAP

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
2. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

3. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

4. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   ```

   下列命令可安全地清除上刪除的檔案 `vol1` 在 SVM 上`vs1`：

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

5. 驗證安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

從具有SnapMirror非同步關係的加密ONTAP磁碟區中清理數據

從 ONTAP 9 8 開始、您可以在具有 SnapMirror 非同步關係且啟用 NVE 的磁碟區上、使用安全清除功能、以不中斷營運的「 crub 」資料。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

步驟

1. 在儲存系統上、切換至進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

   ```
   volume encryption secure-purge start -vserver SVM_name -volume volume_name
   -prepare true
   ```

   在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver SVM_name -volume volume_name -snapshot
   ```

5. 如果您要安全清除的檔案位於基礎快照中，請執行下列步驟：
   a. 在 SnapMirror 非同步關係中的目的地磁碟區上建立快照：

      ```
      volume snapshot create -snapshot snapshot_name -vserver SVM_name -volume
      volume_name
      ```

   b. 更新 SnapMirror 以向前移動基礎快照：

      ```
      snapmirror update -source-snapshot snapshot_name -destination-path
      destination_path
      ```

   對 SnapMirror 非同步關係中的每個 Volume 重複此步驟。

   a. 重複步驟（a）和（b），等於基礎快照的數量加上 1 。

      例如，如果您有兩個基礎快照，則應重複步驟（a）和（b）三次。

   b. 確認基礎快照存在：
      `snapshot show -vserver SVM_name -volume volume_name`
   c. 刪除基礎快照：
      `snapshot delete -vserver svm_name -volume volume_name -snapshot snapshot`
6. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver svm_name -volume volume_name
   ```

在 SnapMirror 非同步關係中的每個磁碟區上重複此步驟。

下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案：

```
cluster1::> volume encryption secure-purge start -vserver vs1 -volume
vol1
```

7. 確認安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

相關資訊

- "SnapMirror 更新"

從具有**SnapMirror**同步關係的加密**ONTAP**磁碟區中清理數據

從 ONTAP 9 8 開始、您可以使用安全清除功能、在具有 SnapMirror 同步關係的 NVE 磁碟區上、不中斷地「清理」資料。

關於這項工作

視刪除檔案中的資料量而定、安全清除可能需要數分鐘到數小時才能完成。您可以使用 `volume encryption secure-purge show` 檢視作業狀態的命令。您可以使用 `volume encryption secure-purge abort` 命令以終止作業。

若要在SAN主機上執行安全清除、您必須刪除包含您要清除之檔案的整個LUN、或者您必須能夠在LUN上為屬於您要清除之檔案的區塊鑽孔。如果您無法刪除LUN或主機作業系統不支援在LUN上打孔、則無法執行安全清除。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

步驟

1. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 刪除您要安全清除的檔案或LUN。
   - 在NAS用戶端上、刪除您要安全清除的檔案。
   - 在SAN主機上、針對屬於您要清除之檔案的區塊、刪除您要安全清除LUN上的LUN或在LUN上鑽孔。
3. 在非同步關係中準備好要安全清除的目的地Volume：

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   -prepare true
   ```

   針對 SnapMirror 同步關係中的其他磁碟區重複此步驟。

4. 如果您要安全清除的檔案位於快照中、請刪除快照：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

5. 如果安全清除檔案位於基礎快照或一般快照中，請更新 SnapMirror 以將一般快照向前移：

   ```
   snapmirror update -source-snapshot <snapshot_name> -destination-path
   <destination_path>
   ```

   共有兩個常用快照，因此必須發出兩次此命令。

6. 如果安全清除檔案位於應用程式一致的快照中，請刪除 SnapMirror 同步關係中兩個磁碟區上的快照：

   ```
   snapshot delete -vserver <SVM_name> -volume <volume_name> -snapshot <snapshot>
   ```

   在兩個磁碟區上執行此步驟。

7. 安全地清除刪除的檔案：

   ```
   volume encryption secure-purge start -vserver <SVM_name> -volume <volume_name>
   ```

   在 SnapMirror 同步關係中的每個磁碟區上重複此步驟。

   下列命令可安全清除SVM「'VS1'」上「'vol1'」上的刪除檔案。

   ```
   cluster1::> volume encryption secure-purge start -vserver vs1 -volume
   vol1
   ```

8. 確認安全清除作業的狀態：

   ```
   volume encryption secure-purge show
   ```

相關資訊

- "SnapMirror 更新"

更改ONTAP板載密鑰管理密碼

NetApp建議您定期變更板載金鑰管理密碼。您必須將新密碼短語儲存在儲存系統之外的安全位置。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在MetroCluster環境中，在本地叢集上更新密碼短語後，同步夥伴叢集上的密碼短語更新。

步驟

1. 變更為進階權限層級：

```
set -privilege advanced
```

2. 更改機載密鑰管理密碼。您使用的命令取決於您執行的ONTAP版本。

   更新版本**ONTAP**

   ```
   security key-manager onboard update-passphrase
   ```

   不含更新版本**ONTAP**

   ```
   security key-manager update-passphrase
   ```

3. 輸入一個介於 32 到 256 個字元之間的密碼，或對於“cc-mode”，輸入一個介於 64 到 256 個字元之間的密碼。

   如果指定的"'cc-mode"通關密碼少於64個字元、則在金鑰管理程式設定作業再次顯示通關密碼提示之前、會有五秒鐘的延遲。

4. 在通關密碼確認提示下、重新輸入通關密碼。

5. 如果您使用的是MetroCluster配置，請在夥伴叢集上同步更新後的密碼短語。

   a. 透過選擇適合您ONTAP版本的正確指令，在夥伴叢集上同步密碼短語：

      更新版本**ONTAP**

      ```
      security key-manager onboard sync
      ```

      不含更新版本**ONTAP**

      - 在ONTAP 9.5 中，運行：

        ```
        security key-manager setup -sync-metrocluster-config
        ```

      - 在ONTAP 9.4 及更早版本中，更新本機叢集上的密碼短語後，等待 20 秒，然後在夥伴叢集上執行以下命令：

        ```
        security key-manager setup
        ```

   b. 出現提示時，請輸入新的密碼短語。

      兩個群集必須使用相同的密碼短語。

完成後

將板載金鑰管理密碼短語複製到儲存系統外部的安全位置，以備將來使用。

每次變更機載金鑰管理密碼時，請手動備份金鑰管理資訊。

相關資訊

- "手動備份內建金鑰管理資訊"
- "安全金鑰管理程式內建更新密碼"

設定Onboard Key Manager複雜密碼時、您應該將內建金鑰管理資訊複製到儲存系統外部的安全位置。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 此工作需要進階權限。

關於這項工作

所有的金鑰管理資訊都會自動備份到叢集的複寫資料庫（RDB）。您也應該手動備份金鑰管理資訊、以便在發生災難時使用。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 顯示叢集的金鑰管理備份資訊：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard show-backup`
不含更新版本ONTAP	`security key-manager backup show`

   以下 9.6 指令顯示金鑰管理備份訊息 `cluster1` ：

```
cluster1::> security key-manager onboard show-backup

      -------------------------BEGIN BACKUP-------------------------
      TmV0QXBwIEtleSBCbG9iAAEAAAAEAAAAcAEAAAAAADuD+byAAAAACEAAAAAAAAA
      QAAAAAAAAABvOlH0AAAAAMh7qDLRyH1DBz12piVdy9ATSFMT0C0TlYFss4PDjTaV
      dzRYkLd1PhQLxAWJwOIyqSr8qY1SEBgm1IWgE5DLRqkiAAAAAAAAACgAAAAAAAAA
      3WTh7gAAAAAAAAAAAAAAAAIAAAAAAAgAZJEIWvdeHr5RCAvHGclo+wAAAAAAAAAA
      IgAAAAAAAAoAAAAAAAAAEOTcR0AAAAAAAAAAAAAAACAAAAAAAJAGr3tJA/LRzU
      QRHwv+1aWvAAAAAAAAAACQAAAAAAAAgAAAAAAAACdhTcvAAAAAJ1PXeBfml4N
      BsSyV1B4jc4A7cvWEFY6lLG6hc6tbKLAHZuvfQ4rIbYAAAAAAAAAAAAAAAAAAAAA
      AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

開始之前

- 如果您將 NSE 與外部 KMIP 伺服器一起使用，請刪除外部金鑰管理員資料庫。有關詳細信息，請參閱"從外部金鑰管理過渡到ONTAP板載金鑰管理"。
- 您必須是叢集管理員才能執行此工作。

如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

更新版本**ONTAP**

如果您執行的是 ONTAP 9.8 或更新版本、而且根磁碟區已加密、請遵循的程序 [ontap-9-8]。

1. 確認金鑰需要還原：
   `security key-manager key query -node node`

   如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

2. 還原金鑰：
   `security key-manager onboard sync`

   如"指令參考資料ONTAP"需詳細 `security key-manager onboard sync`資訊，請參閱。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

ONTAP 9.8 或更新版本、含加密的根磁碟區

如果您執行ONTAP 的是更新版本的版本、而且根磁碟區已加密、則必須使用開機功能表設定內建金鑰管理還原密碼。如果您要更換開機媒體、也必須執行此程序。

1. 將節點開機至開機功能表、然後選取選項 `(10) Set onboard key management recovery secrets`。
2. 輸入 `y` 以使用此選項。
3. 出現提示時、輸入叢集的內建金鑰管理通關密碼。
4. 出現提示時、輸入備份金鑰資料。

   輸入備份金鑰資料後，節點返回啟動選單。

5. 從開機功能表中、選取選項 `(1) Normal Boot`。

不含更新版本**ONTAP**

1. 確認金鑰需要還原：
   `security key-manager key show`
2. 還原金鑰：
   `security key-manager setup -node node`

   詳細了解 `security key-manager setup`在"指令參考資料ONTAP"。

3. 在通關密碼提示字元下、輸入叢集的內建金鑰管理通關密碼。

恢復**ONTAP**外部金鑰管理加密金鑰

您可以手動還原外部金鑰管理加密金鑰、並將其推送到不同的節點。如果您重新啟動的節點在建立叢集的金鑰時暫時停機、您可能會想要這麼做。

關於這項工作

在 ONTAP 9.6 及更新版本中、您可以使用 `security key-manager key query -node node_name` 命令以驗證金鑰是否需要還原。

在 ONTAP 9.5 或更早版本中、您可以使用 `security key-manager key show` 命令以驗證金鑰是否需要還原。

如果您在具有 Flash Cache 模組的系統上使用 NSE 、您也應該啟用 NVE 或 NAE 。NSE 不會加密位於 Flash Cache 模組上的資料。

如"指令參考資料ONTAP"需詳細 `security key-manager key query`資訊，請參閱。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 如果您執行ONTAP 的是更新版本的版本、且根磁碟區已加密、請執行下列步驟：

   如果您執行ONTAP 的是更新版本的版本、或是執行ONTAP 的是版本不加密的版本、請跳過此步驟。

   a. 設定 bootargs ：

      ```
      setenv kmip.init.ipaddr <ip-address>

      setenv kmip.init.netmask <netmask>

      setenv kmip.init.gateway <gateway>

      setenv kmip.init.interface e0M

      boot_ontap
      ```

   b. 將節點開機至開機功能表、然後選取選項 `(11) Configure node for external key management`。

   c. 依照提示輸入管理憑證。

      輸入所有管理憑證資訊後、系統會返回開機功能表。

   d. 從開機功能表中、選取選項 `(1) Normal Boot`。

2. 還原金鑰：

此版本… ONTAP	使用此命令…

更新版本ONTAP	`security key-manager external restore -vserver SVM -node node -key-server host_name
IP_address:port -key-id key_id -key -tag key_tag`	不含更新版本ONTAP

`node`預設為所有節點。

啟用內建金鑰管理時、不支援此命令。

下列 ONTAP 9.6 命令可將外部金鑰管理驗證金鑰還原至中的所有節點 `cluster1`：

```
clusterl::> security key-manager external restore
```

相關資訊

- "安全金鑰管理程式外部還原"

替換**ONTAP**叢集上的 **KMIP SSL** 憑證

所有SSL憑證都有到期日。您必須在憑證過期之前更新憑證、以避免喪失驗證金鑰的存取權。

開始之前

- 您必須已取得叢集的替代公開憑證和私密金鑰（KMIP用戶端憑證）。
- 您必須已取得KMIP伺服器（KMIP伺服器- CA憑證）的替代公共憑證。
- 您必須是叢集或SVM管理員、才能執行此工作。
- 如果您要在 MetroCluster 環境中更換 KMIP SSL 憑證、則必須在兩個叢集上安裝相同的置換 KMIP SSL 憑證。

您可以在叢集上安裝憑證之前或之後、在KMIP伺服器上安裝替換用戶端和伺服器憑證。

步驟

1. 安裝新的KMIP伺服器CA憑證：

   ```
   security certificate install -type server-ca -vserver <>
   ```

2. 安裝新的KMIP用戶端憑證：

   ```
   security certificate install -type client -vserver <>
   ```

3. 更新金鑰管理程式組態以使用新安裝的憑證：

   ```
   security key-manager external modify -vserver <> -client-cert <> -server-ca
   -certs <>
   ```

   如果您在ONTAP 支援支援功能的環境中執行的是支援支援功能的版本9.6或更新版本MetroCluster 、而您想

要修改管理SVM上的金鑰管理程式組態、則必須在組態中的兩個叢集上執行命令。

如果新用戶端憑證的公鑰/私鑰與先前安裝的金鑰不同，則更新金鑰管理器設定以使用新安裝的憑證將傳回錯誤。查看"NetApp知識庫：新的用戶端憑證公鑰或私鑰與現有用戶端憑證不同"有關如何覆寫此錯誤的說明。

相關資訊

- "安全性憑證安裝"
- "安全金鑰管理程式外部修改"

更換 **ONTAP** 中的 **FIPS** 磁碟機或 **SED**

更換FIPS磁碟機或SED的方式與更換一般磁碟相同。請務必將新的資料驗證金鑰指派給更換的磁碟機。對於FIPS磁碟機、您可能也想指派新的FIPS 140-2驗證金鑰。

如果HA配對正在使用 "加密SAS或NVMe磁碟機（SED、NSE、FIPS）"、您必須遵循主題中的指示 "將FIPS磁碟機或SED恢復為無保護模式" 在初始化系統之前、HA配對內的所有磁碟機（開機選項4或9）。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

- 您必須知道磁碟機使用的驗證金鑰金鑰ID。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 確定磁碟已標示為故障：

   ```
   storage disk show -broken
   ```

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

   ```
   cluster1::> storage disk show -broken
   Original Owner: cluster1-01
     Checksum Compatibility: block
                                                                      Usable
   Physical
       Disk   Outage Reason HA Shelf Bay Chan   Pool   Type    RPM     Size
   Size
       ------ ---- ------------ ---- --- ---- ------ -----  -----  -------
   -------
       0.0.0  admin  failed  0b    1   0    A  Pool0  FCAL  10000  132.8GB
   133.9GB
       0.0.7  admin  removed 0b    2   6    A  Pool1  FCAL  10000  132.8GB
   134.2GB
   [...]
   ```

2. 請依照磁碟櫃模型硬體指南中的指示、移除故障磁碟、並以新的FIPS磁碟機或SED進行更換。
3. 指派新更換磁碟的擁有權：

   `storage disk assign -disk disk_name -owner node`

   如"指令參考資料ONTAP"需詳細 `storage disk assign`資訊，請參閱。

   ```
   cluster1::> storage disk assign -disk 2.1.1 -owner cluster1-01
   ```

4. 確認已指派新磁碟：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

   ```
   cluster1::> storage encryption disk show
   Disk    Mode Data Key ID
   -----   ----
   ------------------------------------------------------------------------
   0.0.0   data <id_value>
   0.0.1   data <id_value>
   1.10.0  data <id_value>
   1.10.1  data <id_value>
   2.1.1   open 0x0
   [...]
   ```

5. 將資料驗證金鑰指派給FIPS磁碟機或SED。

   "指派資料驗證金鑰給FIPS磁碟機或SED（外部金鑰管理）"

6. 如有必要、請指派FIPS 140-2驗證金鑰給FIPS磁碟機。

   "將FIPS 140-2驗證金鑰指派給FIPS磁碟機"

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存加密磁碟顯示"

使**FIPS**磁碟機或**SED**上的資料無法存取

了解如何使 **FIPS** 驅動器或 **SED** 上的**ONTAP**資料無法存取

如果您想要使FIPS磁碟機或SED上的資料永久無法存取、但要保留磁碟機未使用的空間以供新資料使用、您可以清理磁碟。如果您想要永久無法存取資料、而且不需要重複使用磁

碟機、可以將其銷毀。

- 磁碟資料抹除

  當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

- 磁碟銷毀

  當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟。這樣做會使磁碟永遠無法使用、且上的資料永遠無法存取。

您可以清除或銷毀個別自我加密磁碟機、或是節點的所有自我加密磁碟機。

在 **ONTAP** 中清理 **FIPS** 磁碟機或 **SED**

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、並將磁碟機用於新資料、您可以使用 `storage encryption disk sanitize` 用於清理磁碟機的命令。

關於這項工作

當您清理自我加密磁碟機時、系統會將磁碟加密金鑰變更為新的隨機值、將開機鎖定狀態重設為假、並將金鑰ID設為預設值、例如製造商安全ID 0x0（SAS磁碟機）或null金鑰（NVMe磁碟機）。這樣做會使磁碟上的資料無法存取、而且無法擷取。您可以將已消毒的磁碟重複使用為非零備援磁碟。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要消毒的Aggregate：

   ```
   storage aggregate delete -aggregate aggregate_name
   ```

   ```
   cluster1::> storage aggregate delete -aggregate aggr1
   ```

   如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要消毒的FIPS磁碟機或SED的磁碟ID：

   ```
   storage encryption disk show -fields data-key-id,fips-key-id,owner
   ```

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   `storage encryption disk modify -disk *disk_id* -fips-key-id 0x0`

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

```
cluster1::> storage encryption disk modify -disk 1.10.2 -fips-key-id 0x0

Info: Starting modify on 1 disk.
      View the status of the operation by using the
      storage encryption disk show-status command.
```

5. 為磁碟機消毒：

   `storage encryption disk sanitize -disk *disk_id*`

   您只能使用此命令來清除熱備援磁碟或中斷的磁碟。若要清理所有磁碟，無論其類型為何，請使用 `-force-all-state`選項。如"指令參考資料ONTAP"需詳細 `storage encryption disk sanitize`資訊，請參閱。

   ⓘ ONTAP 會提示您輸入確認片語、然後再繼續。輸入完全如畫面所示的詞彙。

```
cluster1::> storage encryption disk sanitize -disk 1.10.2

Warning: This operation will cryptographically sanitize 1 spare or
broken self-encrypting disk on 1 node.
         To continue, enter sanitize disk: sanitize disk

Info: Starting sanitize on 1 disk.
      View the status of the operation using the
      storage encryption disk show-status command.
```

6. 解除清理磁碟故障：
   `storage disk unfail -spare true -disk *disk_id*`
7. 檢查磁碟是否擁有擁有者：
   `storage disk show -disk *disk_id*`

如果磁碟沒有擁有者、請指派一個擁有者。
`storage disk assign -owner node -disk disk_id`

8. 輸入要清理磁碟的節點節點節點的節點節點節點：

   `system node run -node node_name`

   執行 `disk sanitize release` 命令。

9. 離開 nodesdroand 。再次解除磁碟故障：
   `storage disk unfail -spare true -disk disk_id`
10. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
    `storage disk show -disk disk_id`

相關資訊

- "儲存磁碟分配"
- "儲存磁碟顯示"
- "儲存磁碟未故障"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在 **ONTAP** 中銷毀 **FIPS** 磁碟機或 **SED**

如果您想讓 FIPS 磁碟機或 SED 上的資料永遠無法存取、而且不需要重複使用磁碟機、您可以使用 `storage encryption disk destroy` 破壞磁碟的命令。

關於這項工作

當您銷毀FIPS磁碟機或SED時、系統會將磁碟加密金鑰設為未知的隨機值、並以不可扭轉的方式鎖定磁碟機。這樣做會使磁碟幾乎無法使用、且上的資料永遠無法存取。不過、您可以使用印在磁碟標籤上的實體安全ID（PSID）、將磁碟重設為原廠設定的設定。如需詳細資訊、請參閱 "當驗證金鑰遺失時、將FIPS磁碟機或SED恢復服務"。

除非您擁有不可傳的Disk Plus服務（NRD Plus）、否則請勿銷毀FIPS磁碟機或SED。銷毀磁碟會使其保固失效。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將任何需要保留的資料移轉到另一個不同磁碟上的集合體。
2. 刪除FIPS磁碟機或SED上要銷毀的Aggregate：

   `storage aggregate delete -aggregate aggregate_name`

```
cluster1::> storage aggregate delete -aggregate aggr1
```

如"指令參考資料ONTAP"需詳細 `storage aggregate delete`資訊，請參閱。

3. 識別要銷毀的FIPS磁碟機或SED的磁碟ID：

   `storage encryption disk show`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk show`資訊，請參閱。

```
cluster1::> storage encryption disk show
Disk    Mode Data Key ID
-----   ----
------------------------------------------------------------------------
0.0.0   data <id_value>
0.0.1   data <id_value>
1.10.2  data <id_value>
[...]
```

4. 銷毀磁碟：

   `storage encryption disk destroy -disk disk_id`

   如"指令參考資料ONTAP"需詳細 `storage encryption disk destroy`資訊，請參閱。

   系統會提示您輸入確認短句、然後再繼續。輸入完全如畫面所示的詞彙。

```
cluster1::> storage encryption disk destroy -disk 1.10.2

Warning: This operation will cryptographically destroy 1 spare or broken
         self-encrypting disks on 1 node.
         You cannot reuse destroyed disks unless you revert
         them to their original state using the PSID value.
         To continue, enter
          destroy disk
         :destroy disk

Info: Starting destroy on 1 disk.
      View the status of the operation by using the
      "storage encryption disk show-status" command.
```

相關資訊

- "儲存加密磁碟銷毀"

- "儲存加密磁碟顯示"
- "儲存加密磁碟顯示狀態"

ONTAP 中的 **FIPS** 磁碟機或 **SED** 上的緊急資料會被粉碎

發生安全性緊急情況時、即使儲存系統或KMIP伺服器無法使用電源、您仍可立即防止存取FIPS磁碟機或SED。

開始之前

- 如果您使用的KMIP伺服器沒有可用的電源、則KMIP伺服器必須設定容易銷毀的驗證項目（例如智慧卡或USB磁碟機）。
- 您必須是叢集管理員才能執行此工作。

步驟

1. 緊急銷毀FIPS磁碟機或SED上的資料：

如果…	然後…

儲存系統可提供電力、您也有時間讓儲存系統正常離線	a. 如果儲存系統設定為HA配對、請停用接管功能。
	b. 使所有集合體離線並加以刪除。
	c. 將權限層級設為進階：
	`set -privilege advanced`
	d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：
	`storage encryption disk modify -disk * -fips-key-id 0x0`
	e. 停止儲存系統。
	f. 開機進入維護模式。
	g. 清理或銷毀磁碟：
	◦ 如果您想讓磁碟上的資料無法存取、但仍能重複使用磁碟、請清理磁碟：
	`disk encrypt sanitize -all`
	◦ 如果您想讓磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：
	`disk encrypt destroy disk_id1 disk_id2 …`
	ⓘ ◦ `disk encrypt sanitize` 和 `disk encrypt destroy` 命令僅保留用於維護模式。這些命令必須在每個HA節點上執行、而且無法用於中斷的磁碟。
	h. 針對合作夥伴節點重複這些步驟。
	如此一來、儲存系統就會處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。
		儲存系統可提供電力、您必須立即切斷資料

a. 如果您想要使磁碟上的資料無法存取且仍能重複使用磁碟、請清理磁碟：
b. 如果儲存系統設定為HA配對、請停用接管功能。
c. 將權限層級設為進階：
`set -privilege advanced`
d. 如果磁碟機處於FIPS相容模式、請將節點的FIPS驗證金鑰ID設回預設MSID：
`storage encryption disk modify -disk * -fips-key-id 0x0`
e. 清理磁碟：
`storage encryption disk sanitize -disk * -force-all-states true`
	a. 如果您想要使磁碟上的資料無法存取、而且不需要儲存磁碟、請銷毀磁碟：
	b. 如果儲存系統設定為HA配對、請停用接管功能。
	c. 將權限層級設為進階：
	`set -privilege advanced`
	d. 銷毀磁碟：
	`storage encryption disk destroy -disk * -force-all-states true`
		儲存系統會出現問題、使系統處於永久停用狀態、並清除所有資料。若要再次使用系統、您必須重新設定。

KMIP伺服器可供電、但儲存系統無法供電	a. 登入 KMIP 伺服器。 b. 銷毀與FIPS磁碟機或SED相關的所有金鑰、這些金鑰包含您要防止存取的資料。 如此可防止儲存系統存取磁碟加密金鑰。	KMIP伺服器或儲存系統無法使用電源

相關資訊

- "儲存加密磁碟銷毀"
- "儲存加密磁碟修改"
- "儲存加密磁碟清理"

當**ONTAP**中的驗證金鑰遺失時，將 **FIPS** 磁碟機或 **SED** 還原服務

如果您永久遺失FIPS磁碟機或SED的驗證金鑰、而且無法從KMIP伺服器擷取、系統會將其視為中斷。雖然您無法存取或恢復磁碟上的資料、但您可以採取步驟、讓SED的未使用空間再次可供資料使用。

開始之前

您必須是叢集管理員才能執行此工作。

關於這項工作

只有當您確定FIPS磁碟機或SED的驗證金鑰已永久遺失、而且無法還原時、才應使用此程序。

如果磁碟已分割、則必須先取消磁碟分割、才能開始此程序。

取消磁碟分割的命令僅在診斷層級可用，且只能在NetApp支援監督下執行。強烈建議您在繼續操作之前聯繫**NetApp**支援。 您也可以參考"NetApp知識庫：如何在ONTAP中取消對備用磁碟機的分割區"。

步驟

1. 將FIPS磁碟機或SED送回服務：

如果SED是…	請使用下列步驟…

未處於FIPS相容模式、或處於FIPS相容模式、且FIPS金鑰可供使用	a. 將權限層級設為進階：
	`set -privilege advanced`
	b. 將 FIPS 金鑰重設為預設製造安全 ID 0x0 ：
	`storage encryption disk modify -fips-key-id 0x0 -disk disk_id`
	c. 確認作業成功：
	`storage encryption disk show-status`
	如果作業失敗、請使用本主題中的 PSID 程序。
	d. 清理損壞的磁碟：
	`storage encryption disk sanitize -disk disk_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	e. 解除清理磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	f. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	g. 離開 nodesdroand 。再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	h. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

在FIPS相容模式中、FIPS金鑰無法使用、且SED標籤上印有PSID	a. 從磁碟標籤取得磁碟的PSID。
	b. 將權限層級設為進階：
	`set -privilege advanced`
	c. 將磁碟重設為原廠設定的設定：
	`storage encryption disk revert-to-original-state -disk disk_id -psid disk_physical_secure_id`
	使用命令驗證作業是否成功 `storage encryption disk show-status` 繼續下一步之前。
	d. 如果您執行的是 ONTAP 9.8P5 或更早版本、請跳至下一步。如果您執行的是 ONTAP 9.8P6 或更新版本、請將已清理的磁碟恢復故障。
	`storage disk unfail -disk disk_id`
	e. 檢查磁碟是否擁有擁有者：
	`storage disk show -disk disk_id`
	如果磁碟沒有擁有者、請指派一個擁有者。
	`storage disk assign -owner node -disk disk_id`
	i. 輸入要清理磁碟的節點節點節點的節點節點節點：
	`system node run -node node_name`
	執行 `disk sanitize release` 命令。
	f. 離開 nodesdroe ..再次解除磁碟故障：
	`storage disk unfail -spare true -disk disk_id`
	g. 確認磁碟現在已成為備援磁碟、並可在集合體中重複使用：
	`storage disk show -disk disk_id`

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟恢復到原始狀態"
- "儲存加密磁碟清理"
- "儲存加密磁碟顯示狀態"

在**ONTAP**中將 **FIPS** 驅動器或 **SED** 恢復為不受保護的模式

僅當節點的驗證金鑰ID設為預設值以外的值時、FIPS磁碟機或SED才會受到保護、不受未獲授權的存取。您可以使用命令將金鑰 ID 設為預設值，將 FIPS 磁碟機或 SED 恢復為未受保護模式 `storage encryption disk modify`。未受保護模式下的 FIPS 磁碟機或 SED 使用預設加密金鑰，而受保護模式下的 FIPS 磁碟機或 SED 則使用提供的加密金鑰。如果磁碟機上有加密資料，而且磁碟機重設為未受保護模式，則資料仍會加密，不會公開。

按照此程序確保 FIPS 驅動器或 SED 返回到不受保護的模式後任何加密資料都變得無法存取。一旦重置 FIPS 和資料金鑰 ID，任何現有資料都無法解密，且無法訪問，除非恢復原始金鑰。

如果HA配對使用加密SAS或NVMe磁碟機（SED、NSE、FIPS）、則在初始化系統之前、您必須針對HA配對內的所有磁碟機（開機選項4或9）執行此程序。如果未這麼做、可能會在磁碟機重新調整用途時、導致未來的資料遺失。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 將權限層級設為進階：

   ```
   set -privilege advanced
   ```

2. 如果FIPS磁碟機以FIPS相容模式執行、請將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   ```
   storage encryption disk modify -disk disk_id -fips-key-id 0x0
   ```

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -fips-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用以下命令確認作業成功：

   ```
   storage encryption disk show-status
   ```

   重複 show-status 指令，直到「Disks Begun」和「Disks Done」中的數字相同。

   ```
   cluster1:: storage encryption disk show-status

              FIPS    Latest   Start               Execution   Disks
   Disks Disks
   Node       Support Request  Timestamp           Time (sec)  Begun
   Done  Successful
   -------    ------- -------- ------------------  ---------- ------
   ------  ----------
   cluster1   true    modify   1/18/2022 15:29:38    3           14     5
   5
   1 entry was displayed.
   ```

3. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

   `storage encryption disk modify -disk disk_id -data-key-id 0x0`

   的價值 `-data-key-id` 無論您要將 SAS 或 NVMe 磁碟機恢復為未受保護模式、都應該設定為 0x0 。

   您可以使用 `security key-manager query` 檢視金鑰ID的命令。

   ```
   cluster1::> storage encryption disk modify -disk 2.10.11 -data-key-id
   0x0

   Info: Starting modify on 14 disks.
         View the status of the operation by using the
         storage encryption disk show-status command.
   ```

   使用以下命令確認作業成功：

   `storage encryption disk show-status`

   重複 show-status 指令，直到數字相同。當“disks began”和“disks done”中的數字相同時，操作完成。

維護模式

從支援功能9.7開始ONTAP 、您可以從維護模式重新輸入FIPS磁碟機的金鑰。只有在ONTAP 無法使用上一節中的指令時、才應使用維護模式。

步驟

1. 將節點的FIPS驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey_fips 0x0 disklist`

2. 將節點的資料驗證金鑰ID設回預設的MSID 0x0：

   `disk encrypt rekey 0x0 disklist`

3. 確認FIPS驗證金鑰已成功重新輸入：

   `disk encrypt show_fips`

4. 確認資料驗證金鑰已成功重新輸入：

   `disk encrypt show`

   您的輸出可能會顯示預設的MSID 0x0金鑰ID或金鑰伺服器所保留的64個字元值。。 `Locked?` 欄位是指資料鎖定。

```
Disk        FIPS Key ID                  Locked?
----------- ---------------------------- -------
0a.01.0     0x0                           Yes
```

相關資訊

- "儲存加密磁碟修改"
- "儲存加密磁碟顯示狀態"

移除 **ONTAP** 中的外部金鑰管理程式連線

當不再需要服務器時、您可以從節點中斷KMIP伺服器的連線。例如、當您轉換至Volume加密時、可能會中斷KMIP伺服器的連線。

關於這項工作

當您中斷KMIP伺服器與HA配對中某個節點的連線時、系統會自動中斷伺服器與所有叢集節點的連線。

> 如果您打算在中斷KMIP伺服器連線後繼續使用外部金鑰管理、請確定另一部KMIP伺服器可用於提供驗證金鑰。

開始之前

您必須是叢集或SVM管理員、才能執行此工作。

步驟

1. 中斷KMIP伺服器與目前節點的連線：

此版本… ONTAP	使用此命令…
更新版本ONTAP	`security key-manager external remove-servers -vserver SVM -key -servers host_name
IP_address:port,…`	不含更新版本ONTAP

在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複執行這些命令。

下列 ONTAP 9.6 命令會停用連線至的兩個外部金鑰管理伺服器 `cluster1`，第一個命名的 `ks1`接聽預設連接埠 5696 、第二個連接埠的 IP 位址為 10.0.0.20 、接聽連接埠 24482 ：

```
cluster1::> security key-manager external remove-servers -vserver
cluster-1 -key-servers ks1,10.0.0.20:24482
```

深入瞭解 `security key-manager external remove-servers`及 `security key-manager delete` "指令參考資料ONTAP"。

從 ONTAP 9.6 開始、您可以使用 `security key-manager external modify-server` 變更外部金鑰管理伺服器 I/O 逾時和使用者名稱的命令。

開始之前

- 您必須是叢集或SVM管理員、才能執行此工作。
- 此工作需要進階權限。
- 在這個支援對象環境中MetroCluster 、您必須在兩個叢集上為管理SVM重複這些步驟。

步驟

1. 在儲存系統上、變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 修改叢集的外部金鑰管理程式伺服器內容：

   ```
   security key-manager external modify-server -vserver admin_SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在叢集登入提示字元中執行命令、 *admin_SVM* 預設為目前叢集的管理SVM。您必須是叢集管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會將的逾時值變更為 45 秒 `cluster1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

   ```
   clusterl::> security key-manager external modify-server -vserver
   cluster1 -key-server ks1.local -timeout 45
   ```

3. 修改SVM的外部金鑰管理程式伺服器內容（僅限NVE）：

   ```
   security key-manager external modify-server -vserver SVM -key-server
   host_name|IP_address:port,… -timeout 1…60 -username user_name
   ```

   超時值以秒表示。如果您修改使用者名稱、系統會提示您輸入新密碼。 如果您在 SVM 登入提示字元下執行命令、 *SVM* 預設為目前的 SVM 。您必須是叢集或SVM管理員、才能修改外部金鑰管理程式伺服器內容。

   下列命令會變更的使用者名稱和密碼 `svm1` 偵聽預設連接埠 5696 的外部金鑰管理伺服器：

   ```
   svml::> security key-manager external modify-server -vserver svm11 -key
   -server ks1.local -username svm1user
   Enter the password:
   Reenter the password:
   ```

4. 針對任何其他SVM重複最後一個步驟。

相關資訊

- "安全金鑰管理程式外部修改伺服器"

從 **ONTAP** 的內建金鑰管理移轉至外部金鑰管理

如果您想從內建金鑰管理切換至外部金鑰管理、則必須先刪除內建金鑰管理組態、才能啟用外部金鑰管理。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 對於軟體型加密、您必須取消加密所有磁碟區。

  "取消Volume資料加密"

- 您必須是叢集管理員才能執行此工作。

步驟

1. 刪除叢集的內建金鑰管理組態：

此版本... ONTAP	使用此命令...
更新版本ONTAP	`security key-manager onboard disable -vserver SVM`
不含更新版本ONTAP	`security key-manager delete-key-database`

深入瞭解 `security key-manager onboard disable`及 `security key-manager delete-key-database` "指令參考資料ONTAP"。

從外部金鑰管理切換到**ONTAP**板載金鑰管理

若要切換至板載金鑰管理，請在啟用板載金鑰管理之前刪除外部金鑰管理配置。

開始之前

- 對於硬體型加密、您必須將所有FIPS磁碟機或SED的資料金鑰重設為預設值。

  "將FIPS磁碟機或SED恢復為無保護模式"

- 您必須刪除所有外部金鑰管理程式連線。

  "刪除外部金鑰管理程式連線"

- 您必須是叢集管理員才能執行此工作。

步驟

轉換金鑰管理的步驟取決於您所使用的 ONTAP 版本。

更新版本**ONTAP**

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 使用命令：

   ```
   security key-manager external disable -vserver admin_SVM
   ```

   在支援支援資源的環境中MetroCluster 、您必須在兩個叢集上重複執行命令、才能使用管理SVM。

詳細了解 `security key-manager external disable`在"指令參考資料ONTAP"。

不含更新版本**ONTAP**

使用命令：

```
security key-manager delete-kmip-config
```

詳細了解 `security key-manager delete-kmip-config`在"指令參考資料ONTAP"。

相關資訊

- "安全金鑰管理員外部使用"

如果在**ONTAP**啟動過程中無法存取金鑰管理伺服器，會發生什麼情況

在開機期間、若為NSE設定的儲存系統無法觸及任何指定的金鑰管理伺服器、則執行某些預防措施以避免不必要的行為。ONTAP

如果儲存系統已設定為使用NSE、系統會重新鎖定SED、並開啟SED電源、則儲存系統必須從金鑰管理伺服器擷取所需的驗證金鑰、以驗證自己是否能存取資料。

儲存系統會嘗試聯絡指定的金鑰管理伺服器、最多三小時。如果之後儲存系統仍無法連絡到任何儲存系統、則開機程序會停止、儲存系統也會停止。

如果儲存系統成功連絡任何指定的金鑰管理伺服器、則會嘗試建立長達15分鐘的SSL連線。如果儲存系統無法與任何指定的金鑰管理伺服器建立SSL連線、開機程序會停止、儲存系統也會停止。

當儲存系統嘗試聯絡並連線至主要管理伺服器時、會在CLI中顯示失敗聯絡嘗試的詳細資訊。您可以隨時按Ctrl-C中斷聯絡活動嘗試

為了安全起見、SED僅允許有限數量的未授權存取嘗試、之後會停用對現有資料的存取。如果儲存系統無法連絡任何指定的金鑰管理伺服器以取得適當的驗證金鑰、則只能嘗試使用預設金鑰進行驗證、導致嘗試失敗並造成恐慌。如果儲存系統設定為在發生緊急情況時自動重新開機、則會進入開機迴圈、導致SED持續嘗試驗證失敗。

在這些情況下停止儲存系統的設計、是為了防止儲存系統進入開機迴圈、以及可能因超過某個連續驗證嘗試失敗次數的安全限制而永久鎖定的SED而導致意外的資料遺失。鎖定保護的限制和類型取決於製造規格和SED類型：

SED 類型	導致鎖定的連續驗證嘗試失敗次數	達到安全限制時的鎖定保護類型
HDD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
X440_PHM2800MCTO 800GB NSE SSD搭配韌體版本NA00或NA01	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
具有韌體版本NA00或NA01的X577_PHM2800MCTO 800GB NSE SSD	5.	暫時性。鎖定功能只會在磁碟重新開機之前生效。
X440_PHM2800MCTO 800GB NSE SSD、韌體版本更高	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
具有較高韌體版本的X577_PHM2800MCTO 800GB NSE SSD	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。
所有其他SSD機型	1024	永久。即使適當的驗證金鑰再次可用、也無法還原資料。

對於所有SED類型、成功驗證會將試用數重設為零。

如果您遇到儲存系統因為無法連線至任何指定的金鑰管理伺服器而停止運作的情況、則必須先識別並修正通訊故障的原因、然後再嘗試繼續開機儲存系統。

預設禁用**ONTAP**加密

從支援支援支援的版本起、如果您擁有Volume加密（VE）授權、並使用內建或外部金鑰管理程式、則根據預設會啟用Aggregate和Volume加密。ONTAP如有必要、您可以依預設停用整個叢集的加密功能。

開始之前

您必須是叢集管理員才能執行此工作、或是叢集管理員已委派權限的SVM管理員。

步驟

1. 若要在ONTAP 預設情況下停用對整個叢集的加密功能、請執行下列命令：

```
options -option-name encryption.data_at_rest_encryption.disable_by_default
-option-value on
```

資料保護與災難恢復

叢集與SVM對等關係

瞭解 ONTAP 叢集和 SVM 對等關係

您可以在來源與目的地叢集之間、以及來源與目的地儲存虛擬機器（SVM）之間建立對等關係。您必須先在這些實體之間建立對等關係，才能使用 SnapMirror 複寫快照。

支援的更新功能可簡化叢集與SVM之間的對等關係設定。ONTAP叢集與SVM對等程序適用於ONTAP 所有的版本。您應該使用ONTAP 適用於您的版本的更新程序。

您可以使用命令列介面（CLI）執行程序、而非使用系統管理員或自動化指令碼工具。

準備叢集與SVM對等關係

ONTAP 對等基礎

您必須在來源叢集與目的地叢集之間，以及來源與目的地 SVM 之間建立 _peer 關係，才能使用 SnapMirror 複寫快照。對等關係可定義網路連線、讓叢集和SVM能夠安全地交換資料。

對等關係中的叢集和SVM會使用叢集間邏輯介面（lifs）透過叢集間網路進行通訊。_叢集間LIF是支援「叢集間核心」網路介面服務的LIF、通常是使用「預設叢集間」網路介面服務原則建立。您必須在要處理的叢集中的每個節點上建立叢集間生命體。

叢集間LIF使用屬於其指派之系統SVM的路由。自動建立系統SVM、以便在IPspace內進行叢集層級的通訊。ONTAP

同時支援連出和串聯拓撲。在串聯拓撲中、您只需要在一線和二線叢集之間、以及在二線和三線叢集之間建立叢集間網路。您不需要在主叢集與第三叢集之間建立叢集間網路。

> 系統管理員可以（但不建議）將叢集間核心服務從預設叢集間服務原則中移除。如果發生這種情況、使用「預設叢集間」建立的LIF實際上不會是叢集間LIF。若要確認預設叢集間服務原則是否包含叢集間核心服務、請使用下列命令：
>
> ```
> network interface service-policy show -policy default-intercluster
> ```
>
> 如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。

ONTAP 對等關係先決條件

在設定叢集對等之前、您應該確認連線能力、連接埠、IP位址、子網路、防火牆、 並符合叢集命名需求。

從 ONTAP 9.6 開始、叢集對等關係依預設為資料複寫提供 TLS 1.2 AES-256 GCM 加密支援。即使停用加密、叢集對等關係仍需使用預設的安全性密碼（「 PSK-AES256-GCM-SHA384 」）才能運作。

從 ONTAP 9.11.1 開始、預設會提供 DHE-PSK 安全密碼。

從 ONTAP 9.15.1 開始、叢集對等關係依預設為資料複寫提供 TLS 1.3 加密支援。

連線需求

本機叢集上的每個叢集間LIF都必須能夠與遠端叢集上的每個叢集間LIF通訊。

雖然不需要、但一般而言、設定用於同一子網路中叢集間LIF的IP位址較為簡單。IP位址可以與資料生命體位於同一個子網路中、也可以位於不同的子網路中。每個叢集所使用的子網路必須符合下列需求：

- 子網路必須屬於廣播網域、其中包含用於叢集間通訊的連接埠。
- 子網路必須有足夠的IP位址、才能為每個節點分配一個叢集間LIF。

  例如、在四節點叢集中、用於叢集間通訊的子網路必須有四個可用的IP位址。

每個節點都必須具有叢集間LIF、並在叢集間網路上具有IP位址。

叢集間LIF可以有一個IPv4位址或IPv6位址。

ONTAP 可讓您將對等網路從 IPv4 移轉至 IPv6 、並選擇性地允許兩個通訊協定同時存在於叢集間的生命體上。在早期版本中、整個叢集的所有叢集間關係都是IPV4或IPV6。這表示變更傳輸協定可能會造成中斷。

連接埠需求

您可以使用專用連接埠進行叢集間通訊、或共用資料網路所使用的連接埠。連接埠必須符合下列需求：

- 用於與指定遠端叢集通訊的所有連接埠必須位於相同的IPspace中。

  您可以使用多個IPspace與多個叢集對等。只有在IPspace內才需要配對全網狀網路連線。

- 用於叢集間通訊的廣播網域必須包含每個節點至少兩個連接埠、以便叢集間通訊能夠從一個連接埠容錯移轉到另一個連接埠。

  新增至廣播網域的連接埠可以是實體網路連接埠、VLAN或介面群組（ifgrps）。

- 所有連接埠都必須以纜線連接。
- 所有連接埠都必須處於正常狀態。
- 連接埠的MTU設定必須一致。

防火牆需求

從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需詳細資訊、請參閱 "設定lifs的防火牆原則"。

防火牆和叢集間防火牆原則必須允許下列傳輸協定：

- 雙向 ICMP 流量
- 透過連接埠 11104 和 11105 、雙向起始 TCP 流量至所有叢集間生命體的 IP 位址
- 叢集間LIF之間的雙向HTTPS

  雖然使用CLI設定叢集對等功能時不需要HTTPS、但如果您使用System Manager來設定資料保護、稍後仍需要HTTPS。

預設值 `intercluster` 防火牆原則允許透過 HTTPS 傳輸協定和所有 IP 位址（ 0.0.0/0 ）進行存取。如有必要、您可以修改或取代原則。

叢集需求

叢集必須符合下列需求：

- 叢集不能與超過255個叢集處於對等關係中。

使用共享或專用的 **ONTAP** 連接埠

您可以使用專用連接埠進行叢集間通訊、或共用資料網路所使用的連接埠。在決定是否要共用連接埠時、您需要考量網路頻寬、複寫時間間隔及連接埠可用度。

您可以在一個連接叢集上共用連接埠、同時在另一個連接埠上使用專用連接埠。

網路頻寬

如果您有高速網路（例如10 GbE）、您可能有足夠的本機LAN頻寬來使用用於資料存取的相同10 GbE連接埠來執行複寫。

即使如此、您也應該比較可用的WAN頻寬與LAN頻寬。如果可用的WAN頻寬明顯低於10 GbE、您可能需要使用專用連接埠。

此規則的一個例外是、叢集內的所有或多個節點複寫資料時、頻寬使用率通常會分散於各個節點。

如果您不使用專用連接埠、則複寫網路的最大傳輸單元（MTU）大小通常應與資料網路的MTU大小相同。

複寫時間間隔

如果複寫是在非尖峰時間進行、即使沒有10-GbE LAN連線、也應該能夠使用資料連接埠進行複寫。

如果複寫是在正常上班時間進行、您需要考量要複寫的資料量、以及它是否需要太多頻寬、以致可能導致資料傳輸協定發生爭用。如果資料傳輸協定（SMB、NFS、iSCSI）的網路使用率超過50%、您應該使用專屬的連接埠進行叢集間通訊、以便在發生節點容錯移轉時提供不降級的效能。

連接埠可用度

如果確定複寫流量干擾資料流量、您可以將叢集間的生命體移轉到同一個節點上任何其他具有叢集功能的共用連接埠。

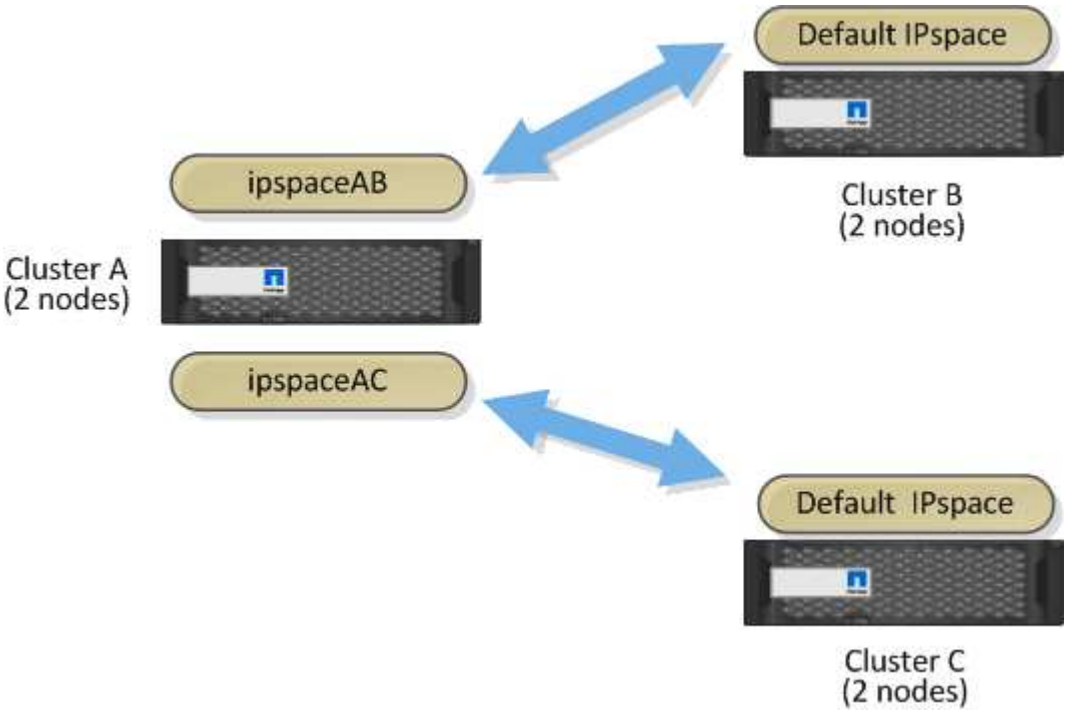
您也可以將VLAN連接埠專用於複寫。連接埠的頻寬會在所有VLAN和基礎連接埠之間共用。

使用自訂 **ONTAP IPspace** 隔離複寫流量

您可以使用自訂IPspaces來分隔叢集與其對等端點之間的互動。此組態稱為_指定叢集間連線_、可讓服務供應商隔離多租戶環境中的複寫流量。

例如、假設您希望叢集A和叢集B之間的複寫流量與叢集A和叢集C之間的複寫流量分開為達成此目標、您可以在叢集A上建立兩個IPspaces

一個IPspace包含用於與叢集B通訊的叢集間LIF另一個包含用於與叢集C通訊的叢集間LIF、如下圖所示。



相關資訊

- "瞭解 ONTAP IPspace 組態"

設定叢集間**LIF**

在共享資料連接埠上設定 **ONTAP** 叢集間的生命

您可以在與資料網路共用的連接埠上設定叢集間的LIF。如此可減少叢集間網路所需的連接埠數量。

步驟

1. 列出叢集中的連接埠：

   ```
   network port show
   ```

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

下列範例顯示中的網路連接埠 `cluster01`：

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
```

2. 在管理 SVM （預設 IPspace ）或系統 SVM （自訂 IPspace ）上建立叢集間的生命體：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port port -address` *`port_IP`* `-netmask` *`netmask`*
• ONTAP 在《S19.5及更早版本》中：*	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

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

以下範例建立叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02`：

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. 驗證是否已建立叢集間的LIF：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster`

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

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01  e0c
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02  e0c
true
```

4. 驗證叢集間的LIF是否為備援：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster -failover`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster -failover`

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

以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在上 `e0c` 連接埠將容錯移轉至 `e0d` 連接埠。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-01:e0c,
                                              cluster01-01:e0d
         cluster01_icl02 cluster01-02:e0c   local-only
192.168.1.201/24
                            Failover Targets: cluster01-02:e0c,
                                              cluster01-02:e0d
```

在專用連接埠上設定 **ONTAP** 叢集間的生命體

您可以在專用連接埠上設定叢集間的LIF。這樣做通常會增加複寫流量的可用頻寬。

步驟

1. 列出叢集中的連接埠：

   ```
   network port show
   ```

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

   下列範例顯示中的網路連接埠 `cluster01`：

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 判斷哪些連接埠可用於叢集間通訊：

   `network interface show -fields home-port,curr-port`

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

   以下範例顯示連接埠 `e0e` 和 `e0f` 尚未指派生命：

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01-01_clus1   e0a       e0a
Cluster cluster01-01_clus2   e0b       e0b
Cluster cluster01-02_clus1   e0a       e0a
Cluster cluster01-02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

3. 為專用連接埠建立容錯移轉群組：

`network interface failover-groups create -vserver system_SVM -failover-group failover_group -targets physical _or_logical_ports`

下列範例指派連接埠 `e0e` 和 `e0f` 移轉至容錯移轉群組 `intercluster01` 在系統 SVM 上 `cluster01`：

```
cluster01::> network interface failover-groups create -vserver cluster01
-failover-group
intercluster01 -targets
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

4. 確認已建立容錯移轉群組：

`network interface failover-groups show`

如"指令參考資料ONTAP"需詳細 `network interface failover-groups show`資訊，請參閱。

```
cluster01::> network interface failover-groups show
                                  Failover
Vserver          Group            Targets
---------------- ----------------
--------------------------------------------
Cluster
                 Cluster
                                  cluster01-01:e0a, cluster01-01:e0b,
                                  cluster01-02:e0a, cluster01-02:e0b
cluster01
                 Default
                                  cluster01-01:e0c, cluster01-01:e0d,
                                  cluster01-02:e0c, cluster01-02:e0d,
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
                 intercluster01
                                  cluster01-01:e0e, cluster01-01:e0f
                                  cluster01-02:e0e, cluster01-02:e0f
```

5. 在系統SVM上建立叢集間LIF、並將它們指派給容錯移轉群組。

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface create -vserver system_SVM -lif LIF_name -service -policy default-intercluster -home -node node -home- port port -address port_IP -netmask netmask -failover -group failover_group`

選項	說明
• ONTAP 在《S19.5及更早版本》中：*	`network interface create -vserver system_SVM -lif LIF_name -role intercluster -home-node node -home -port port -address port_IP -netmask netmask -failover-group failover_group`

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

以下範例建立叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在容錯移轉群組中 `intercluster01`：

```
cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0 -failover-group intercluster01

cluster01::> network interface create -vserver cluster01 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0 -failover-group intercluster01
```

6. 驗證是否已建立叢集間的LIF：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster`

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

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster01
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

7. 驗證叢集間的LIF是否為備援：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster -failover`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster -failover`

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

以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在SVM上`e0e` 連接埠將容錯移轉至 `e0f` 連接埠。

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
cluster01
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

在自訂 **IPspace** 中設定 **ONTAP** 叢集間的生命體

您可以在自訂IPspaces中設定叢集間LIF。如此可讓您隔離多租戶環境中的複寫流量。

建立自訂IPspace時、系統會建立系統儲存虛擬機器（SVM）、做為該IPspace中系統物件的容器。您可以使用新的SVM作為新IPspace中任何叢集間LIF的容器。新的SVM名稱與自訂IPspace名稱相同。

步驟

1. 列出叢集中的連接埠：

   `network port show`

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

   下列範例顯示中的網路連接埠 `cluster01`：

```
cluster01::> network port show
                                                                  Speed
(Mbps)
Node   Port      IPspace      Broadcast Domain Link   MTU    Admin/Oper
------ --------- ------------ ---------------- ----- -------
------------
cluster01-01
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
cluster01-02
       e0a       Cluster      Cluster          up     1500   auto/1000
       e0b       Cluster      Cluster          up     1500   auto/1000
       e0c       Default      Default          up     1500   auto/1000
       e0d       Default      Default          up     1500   auto/1000
       e0e       Default      Default          up     1500   auto/1000
       e0f       Default      Default          up     1500   auto/1000
```

2. 在叢集上建立自訂IPspaces：

   `network ipspace create -ipspace` *`ipspace`*

   以下範例建立自訂 IPspace `ipspace-IC1`：

```
cluster01::> network ipspace create -ipspace ipspace-IC1
```

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

3. 判斷哪些連接埠可用於叢集間通訊：

   `network interface show -fields home-port,curr-port`

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

   以下範例顯示連接埠 `e0e` 和 `e0f` 尚未指派生命：

```
cluster01::> network interface show -fields home-port,curr-port
vserver lif                  home-port curr-port
------- -------------------- --------- ---------
Cluster cluster01_clus1   e0a       e0a
Cluster cluster01_clus2   e0b       e0b
Cluster cluster02_clus1   e0a       e0a
Cluster cluster02_clus2   e0b       e0b
cluster01
        cluster_mgmt         e0c       e0c
cluster01
        cluster01-01_mgmt1   e0c       e0c
cluster01
        cluster01-02_mgmt1   e0c       e0c
```

4. 從預設廣播網域移除可用的連接埠：

   `network port broadcast-domain remove-ports -broadcast-domain Default -ports ports`

   連接埠一次不能位於多個廣播網域中。如"指令參考資料ONTAP"需詳細 `network port broadcast-domain remove-ports`資訊，請參閱。

   下列範例移除連接埠 `e0e` 和 `e0f` 從預設的廣播網域：

```
cluster01::> network port broadcast-domain remove-ports -broadcast
-domain Default -ports
cluster01-01:e0e,cluster01-01:e0f,cluster01-02:e0e,cluster01-02:e0f
```

5. 確認已從預設廣播網域移除連接埠：

   `network port show`

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

   以下範例顯示連接埠 `e0e` 和 `e0f` 已從預設廣播網域中移除：

```
cluster01::> network port show
                                                          Speed (Mbps)
Node   Port    IPspace   Broadcast Domain Link   MTU     Admin/Oper
------ ------- --------- --------------- ----- ------- ------------
cluster01-01
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
cluster01-02
       e0a     Cluster    Cluster          up    9000  auto/1000
       e0b     Cluster    Cluster          up    9000  auto/1000
       e0c     Default    Default          up    1500  auto/1000
       e0d     Default    Default          up    1500  auto/1000
       e0e     Default    -                up    1500  auto/1000
       e0f     Default    -                up    1500  auto/1000
       e0g     Default    Default          up    1500  auto/1000
```

6. 在自訂IPspace中建立廣播網域：

   `network port broadcast-domain create -ipspace` *`ipspace`* `-broadcast-domain` *`broadcast_domain`* `-mtu` *`MTU`* `-ports` *`ports`*

   以下範例建立廣播網域 `ipspace-IC1-bd` 在 IPspace 中 `ipspace-IC1`：

```
cluster01::> network port broadcast-domain create -ipspace ipspace-IC1
-broadcast-domain
ipspace-IC1-bd -mtu 1500 -ports cluster01-01:e0e,cluster01-01:e0f,
cluster01-02:e0e,cluster01-02:e0f
```

7. 確認已建立廣播網域：

   `network port broadcast-domain show`

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

```
cluster01::> network port broadcast-domain show
IPspace Broadcast                                       Update
Name    Domain Name    MTU  Port List                   Status Details
------- ----------- ------  --------------------------- --------------
Cluster Cluster       9000
                            cluster01-01:e0a            complete
                            cluster01-01:e0b            complete
                            cluster01-02:e0a            complete
                            cluster01-02:e0b            complete
Default Default       1500
                            cluster01-01:e0c            complete
                            cluster01-01:e0d            complete
                            cluster01-01:e0f            complete
                            cluster01-01:e0g            complete
                            cluster01-02:e0c            complete
                            cluster01-02:e0d            complete
                            cluster01-02:e0f            complete
                            cluster01-02:e0g            complete
ipspace-IC1
        ipspace-IC1-bd
                      1500
                            cluster01-01:e0e            complete
                            cluster01-01:e0f            complete
                            cluster01-02:e0e            complete
                            cluster01-02:e0f            complete
```

8. 在系統SVM上建立叢集間LIF、並將它們指派給廣播網域：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-service -policy default-intercluster -home -node` *`node`* `-home-port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*
• ONTAP 在《S19.5及更早版本》中：*	`network interface create -vserver` *`system_SVM`* `-lif` *`LIF_name`* `-role intercluster -home-node` *`node`* `-home -port` *`port`* `-address` *`port_IP`* `-netmask` *`netmask`*

LIF是在主連接埠指派給的廣播網域中建立。廣播網域具有預設的容錯移轉群組、其名稱與廣播網域相同。如"指令參考資料ONTAP"需詳細 `network interface create`資訊，請參閱。

以下範例建立叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在廣播網域中 `ipspace-IC1-`

bd：

```
cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0e
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver ipspace-IC1 -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0e
-address 192.168.1.202
-netmask 255.255.255.0
```

9. 驗證是否已建立叢集間的LIF：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster`

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

```
cluster01::> network interface show -service-policy default-intercluster
            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node           Port
Home
----------- ---------- ---------- ------------------ -------------
------- ----
ipspace-IC1
            cluster01_icl01
                       up/up      192.168.1.201/24   cluster01-01   e0e
true
            cluster01_icl02
                       up/up      192.168.1.202/24   cluster01-02   e0f
true
```

10. 驗證叢集間的LIF是否為備援：

選項	說明
• ONTAP 在S69.6及更新版本中：*	`network interface show -service-policy default-intercluster -failover`
• ONTAP 在《S19.5及更早版本》中：*	`network interface show -role intercluster -failover`

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

以下範例顯示叢集間的生命體 `cluster01_icl01` 和 `cluster01_icl02` 在SVM上 `e0e` 連接埠容錯移轉至 'e0f`port:

```
cluster01::> network interface show -service-policy default-intercluster
-failover
         Logical         Home                  Failover        Failover
Vserver  Interface       Node:Port             Policy          Group
-------- --------------- --------------------- --------------- --------
ipspace-IC1
         cluster01_icl01 cluster01-01:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-01:e0e,
                                               cluster01-01:e0f
         cluster01_icl02 cluster01-02:e0e   local-only
intercluster01
                            Failover Targets:  cluster01-02:e0e,
                                               cluster01-02:e0f
```

設定對等關係

建立 ONTAP 叢集對等關係

在您將資料複寫到遠端叢集以進行資料備份和災難恢復之前、您應該先在本機叢集和遠端叢集之間建立叢集對等關係。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"建立設定快照複製。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

有多種預設保護原則可供使用。如果您想要使用自訂原則、必須先建立保護原則。

開始之前

如果您使用 ONTAP CLI 、則必須使用下列其中一種方法、在叢集中的每個節點上建立叢集間的生命體：

- "在共享的資料連接埠上設定叢集間LIF"

- "在專用資料連接埠上設定叢集間的生命"
- "在自訂IPspaces中設定叢集間LIF"

步驟

使用ONTAP 「系統管理程式」或ONTAP 「系統資訊管理系統」CLI執行此工作。

系統管理員

1. 在本機叢集中、按一下 * 叢集 > 設定 * 。
2. 在 * 叢集間設定 * 區段中、按一下 * 新增網路介面 * 、然後輸入 IP 位址和子網路遮罩、以新增叢集間網路介面。

   在遠端叢集上重複此步驟。

3. 在遠端叢集中、按一下 * 叢集 > 設定 * 。
4. 按一下 ⋮ * 叢集對等點 * 區段、然後選取 * 產生通行密碼 * 。
5. 選取遠端 ONTAP 叢集版本。
6. 複製產生的複雜密碼。
7. 在本機叢集中的 * 叢集對等 * 下、按一下 ⋮ 並選取 * 對等叢集 * 。
8. 在 * 對等叢集 * 視窗中、貼上複雜密碼、然後按一下 * 起始叢集對等 * 。

CLI

1. 在目的地叢集上、建立與來源叢集的對等關係：

   ```
   cluster peer create -generate-passphrase -offer-expiration
   <MM/DD/YYYY HH:MM:SS|1...7days|1...168hours> -peer-addrs
   <peer_LIF_IPs> -initial-allowed-vserver-peers <svm_name|*> -ipspace
   <ipspace>
   ```

   如果您同時指定兩者 `-generate-passphrase` 和 `-peer-addrs`，僅在中指定其叢集間的生命體 `-peer-addrs` 可以使用產生的密碼。

   如果您不使用自訂 IPspace ，則可以忽略此 `-ipspace`選項。如"指令參考資料ONTAP"需詳細 `cluster peer create`資訊，請參閱。

   如果您在 ONTAP 9.6 或更新版本中建立對等關係、而不想加密跨叢集對等通訊、則必須使用 `-encryption-protocol-proposed none` 停用加密的選項。

   以下範例建立與未指定遠端叢集的叢集對等關係、並預先授權與 SVM 的對等關係 `vs1` 和 `vs2` 在本機叢集上：

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

下列範例會在叢集間LIF IP位址192.140.112.103和192.140.112.104與遠端叢集建立叢集對等關係、並預先授權與本機叢集上的任何SVM建立對等關係：

```
cluster02::> cluster peer create -generate-passphrase -peer-addrs
192.140.112.103,192.140.112.104 -offer-expiration 2days -initial
-allowed-vserver-peers *

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101,192.140.112.102
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

以下範例建立與未指定遠端叢集的叢集對等關係、並預先授權與 SVM 的對等關係`vs1` 和 `vs2` 在本機叢集上：

```
cluster02::> cluster peer create -generate-passphrase -offer
-expiration 2days -initial-allowed-vserver-peers vs1,vs2

                    Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
               Expiration Time: 6/7/2017 08:16:10 EST
  Initial Allowed Vserver Peers: vs1,vs2
            Intercluster LIF IP: 192.140.112.101
              Peer Cluster Name: Clus_7ShR (temporary generated)

Warning: make a note of the passphrase - it cannot be displayed
again.
```

2. 在來源叢集上、驗證來源叢集到目的地叢集的驗證：

```
cluster peer create -peer-addrs <peer_LIF_IPs> -ipspace <ipspace>
```

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

下列範例驗證本機叢集到叢集間LIF IP位址192.140.112.101和192.140.112.102的遠端叢集：

```
cluster01::> cluster peer create -peer-addrs
192.140.112.101,192.140.112.102

Notice: Use a generated passphrase or choose a passphrase of 8 or
more characters.
        To ensure the authenticity of the peering relationship, use
a phrase or sequence of characters that would be hard to guess.

Enter the passphrase:
Confirm the passphrase:

Clusters cluster02 and cluster01 are peered.
```

出現提示時、請輸入對等關係的通關密碼。

3. 確認已建立叢集對等關係：

```
cluster peer show -instance
```

```
cluster01::> cluster peer show -instance

                                Peer Cluster Name: cluster02
                    Remote Intercluster Addresses: 192.140.112.101,
192.140.112.102
                Availability of the Remote Cluster: Available
                               Remote Cluster Name: cluster2
                               Active IP Addresses: 192.140.112.101,
192.140.112.102
                             Cluster Serial Number: 1-80-123456
                    Address Family of Relationship: ipv4
                Authentication Status Administrative: no-authentication
                   Authentication Status Operational: absent
                                   Last Update Time: 02/05 21:05:41
                       IPspace for the Relationship: Default
```

4. 檢查對等關係中節點的連線能力和狀態：

```
cluster peer health show
```

```
cluster01::> cluster peer health show
Node       cluster-Name                Node-Name
             Ping-Status               RDB-Health Cluster-Health
Avail…
---------- --------------------------- ---------  ---------------
--------
cluster01-01
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
cluster01-02
           cluster02                   cluster02-01
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
                                       cluster02-02
             Data: interface_reachable
             ICMP: interface_reachable true       true
true
```

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作...	請參閱此內容...
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"Volume災難恢復準備總覽"

建立 **ONTAP** 叢集間 **SVM** 對等關係

您可以使用 `vserver peer create` 命令、在本機叢集和遠端叢集上的 SVM 之間建立對等關係。

開始之前

- 來源叢集和目的地叢集必須執行對等關係。

- 您必須擁有遠端叢集上SVM的「預先授權」對等關係。

  如需詳細資訊、請參閱 "建立叢集對等關係"。

關於這項工作

您可以透過在 `-initial-allowed-vserver`建立集群對等關係時的選項。如需更多資訊、請參閱 "建立叢集對等關係"。

步驟

1. 在資料保護目的地叢集上、顯示預先授權用於對等的SVM：

   `vserver peer permission show`

   ```
   cluster02::> vserver peer permission show
   Peer Cluster         Vserver               Applications
   -------------------  --------------------  --------------------
   cluster02            vs1,vs2               snapmirror
   ```

2. 在資料保護來源叢集上、建立與資料保護目的地叢集上預先授權SVM的對等關係：

   `vserver peer create -vserver local_SVM -peer-vserver remote_SVM`

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

   以下範例在本機 SVM 之間建立對等關係 `pvs1` 以及預先授權的遠端 SVM `vs1`：

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   ```

3. 驗證SVM對等關係：

   `vserver peer show`

   ```
   cluster01::> vserver peer show
               Peer        Peer                           Peering
   Remote
   Vserver     Vserver     State        Peer Cluster      Applications
   Vserver
   ----------- ----------- ------------ ----------------- --------------
   ---------
   pvs1        vs1         peered       cluster02         snapmirror
   vs1
   ```

新增 **ONTAP** 叢集間 **SVM** 對等關係

如果您在設定叢集對等關係之後建立SVM、則需要手動新增SVM的對等關係。您可以使用 `vserver peer create` 命令來建立 SVM 之間的對等關係。建立對等關係之後、即可執行 `vserver peer accept` 在遠端叢集上授權對等關係。

開始之前

來源叢集和目的地叢集必須執行對等關係。

關於這項工作

您可以在同一個叢集中的SVM之間建立對等關係、以進行本機資料備份。如"指令參考資料ONTAP"需詳細 `vserver peer create`資訊，請參閱。

系統管理員偶爾會使用 `vserver peer reject`命令來拒絕建議的 SVM 對等關係。如果 SVM 之間的關係處於 `rejected`狀態，您必須先刪除關係，才能建立新關係。如"指令參考資料ONTAP"需詳細 `vserver peer reject`資訊，請參閱。

步驟

1. 在資料保護來源叢集上、與資料保護目的地叢集上的SVM建立對等關係：

   `vserver peer create -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`* `-applications snapmirror|file-copy|lun-copy -peer-cluster` *`remote_cluster`*

   以下範例在本機 SVM 之間建立對等關係`pvs1` 以及遠端 SVM`vs1`

   ```
   cluster01::> vserver peer create -vserver pvs1 -peer-vserver vs1
   -applications snapmirror -peer-cluster cluster02
   ```

   如果本機和遠端SVM的名稱相同、您必須使用_local name_建立SVM對等關係：

   ```
   cluster01::> vserver peer create -vserver vs1 -peer-vserver
   vs1 -applications snapmirror -peer-cluster cluster01
   -local-name cluster1vs1LocallyUniqueName
   ```

2. 在資料保護來源叢集上、確認對等關係已啟動：

   `vserver peer show-all`

   如"指令參考資料ONTAP"需詳細 `vserver peer show-all`資訊，請參閱。

   以下範例顯示 SVM 之間的對等關係`pvs1` 和 SVM`vs1` 已初始化：

```
cluster01::> vserver peer show-all
            Peer        Peer                         Peering
Vserver     Vserver     State      Peer Cluster      Applications
--------    --------    ---------  -------------     ------------
pvs1        vs1         initiated   Cluster02          snapmirror
```

3. 在資料保護目的地叢集上、顯示擱置中的SVM對等關係：

   `vserver peer show`

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

   下列範例列出的擱置對等關係 `cluster02`：

```
cluster02::> vserver peer show

                    Peer                Peer
Vserver             Vserver             State
-----------         -----------         ------------
vs1                 pvs1                pending
```

4. 在資料保護目的地叢集上、授權擱置的對等關係：

   `vserver peer accept -vserver` *`local_SVM`* `-peer-vserver` *`remote_SVM`*

   如"指令參考資料ONTAP"需詳細 `vserver peer accept`資訊，請參閱。

   以下範例授權本機 SVM 之間的對等關係 `vs1` 以及遠端 SVM `pvs1`：

```
cluster02::> vserver peer accept -vserver vs1 -peer-vserver pvs1
```

5. 驗證SVM對等關係：

   `vserver peer show`

```
cluster01::> vserver peer show
            Peer        Peer                            Peering
Remote
Vserver     Vserver     State        Peer Cluster       Applications
Vserver
----------- ----------- ------------ ------------------ --------------
---------
pvs1        vs1         peered       cluster02          snapmirror
vs1
```

啟用對等關係上的 ONTAP 叢集對等加密

從ONTAP 推出支援支援功能的9.6開始、所有新建立的叢集對等關係、預設都會啟用叢集對等加密。叢集對等加密使用預先共用金鑰（PSK）和傳輸安全層（TLS）來保護跨叢集對等通訊。這會在連接叢集之間增加一層安全性。

關於這項工作

如果您要將對等叢集升級至ONTAP 支援的9.6或更新版本、而且對等關係是在ONTAP 更新版本的版本為32、9.5或更早版本時建立、則必須在升級後手動啟用叢集對等加密。對等關係中的兩個叢集都必須執行ONTAP 不支援的9.6或更新版本、才能啟用叢集對等加密。

步驟

1. 在目的地叢集上、啟用與來源叢集通訊的加密：

   ```
   cluster peer modify source_cluster -auth-status-admin use-authentication
   -encryption-protocol-proposed tls-psk
   ```

2. 出現提示時、請輸入通關密碼。
3. 在資料保護來源叢集上、啟用與資料保護目的地叢集通訊的加密：

   ```
   cluster peer modify data_protection_destination_cluster -auth-status-admin
   use-authentication -encryption-protocol-proposed tls-psk
   ```

4. 出現提示時、請輸入在目的地叢集上輸入的相同通關密碼。

如"指令參考資料ONTAP"需詳細 `cluster peer modify`資訊，請參閱。

移除對等關係中的 ONTAP 叢集對等加密

根據預設、ONTAP 叢集對等加密功能會在所有在支援支援支援支援的對等關係上啟用。如果您不想使用加密來進行跨叢集對等通訊、可以停用加密。

步驟

1. 在目的地叢集上、修改與來源叢集的通訊、以停止使用叢集對等加密：
   - 若要移除加密、但保留驗證、請輸入：

```
cluster peer modify <source_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

- 若要移除加密與驗證：
  i. 修改叢集對等原則以允許未驗證的存取：

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

  ii. 修改加密與驗證存取：

```
cluster peer modify <source_cluster> -auth-status no-
authentication
```

2. 出現提示時、請輸入複雜密碼。
3. 重新輸入密碼以確認密碼。
4. 在來源叢集上、停用與目的地叢集通訊的加密：
   - 若要移除加密、但保留驗證、請輸入：

```
cluster peer modify <destination_cluster> -auth-status-admin use-
authentication -encryption-protocol-proposed none
```

   - 若要移除加密與驗證：
     i. 修改叢集對等原則以允許未驗證的存取：

```
cluster peer policy modify -is-unauthenticated-access-permitted
true
```

     ii. 修改加密與驗證存取：

```
cluster peer modify <destination_cluster> -auth-status no-
authentication
```

5. 出現提示時、請輸入並重新輸入您在目的地叢集上使用的相同密碼。

管理本機快照

瞭解如何管理本機 **ONTAP** 快照

_snapshot 是磁碟區的唯讀時間點映像。映像會佔用最少的儲存空間，而且效能成本也可忽略不計，因為它只會記錄自上次快照以來檔案的變更。

您可以使用快照來還原磁碟區的全部內容，或是恢復個別檔案或 LUN 。快照會儲存在磁碟區的目錄中。`.snapshot`

在ONTAP 9.4 及更高版本中， FlexVol volume最多可包含 1023 個快照。在ONTAP 9.3 及更早版本中，一個磁碟區最多可包含 255 個快照。

> 從 ONTAP 9.8 開始， FlexGroup 磁碟區可以包含 1023 個快照。如需更多資訊、請參閱 "使用快照保護 FlexGroup 磁碟區"。

了解**ONTAP**長期保留快照

策略類型為「vault」或「mirror-vault」的SnapMirror關係允許直接在SnapMirror關係的輔助磁碟區上建立快照。這些快照將作為備份保留在目標位置。這些快照通常是為了長期保留而創建的，稱為長期保留快照。

您可以透過在SnapMirror策略規則中指定快照建立計劃、快照名稱前綴、 SnapMirror標籤和保留計數來建立長期保留快照。無論來源上的保留規則為何，此快照都會保留在SnapMirror目標磁碟區上。

長期保留快照僅適用於FlexVol SnapMirror設定。您無法為FlexGroup SnapMirror設定建立長期保留快照。

在SnapMirror級聯關係中，只能在級聯的最後一個磁碟區上建立長期保留快照。

相關資訊

- "了解級聯部署的工作原理"
- "定義 ONTAP SnapMirror 排程以在目的地上建立本機複本"

設定自訂快照原則

瞭解如何設定自訂 **ONTAP** 快照原則

snapshot 原則 _ 定義系統建立快照的方式。原則會指定何時建立快照，要保留多少份複本，以及如何命名這些快照。例如，系統可能每天在上午 *12* ： *10* 建立一個快照，保留兩個最新的複本，並將複本命名為「 *daily._timestamp.* 」 。

磁碟區的預設原則會根據下列排程自動建立快照，並刪除最舊的快照，以便為較新的複本提供空間：

- 每小時最多六個快照、每小時五分鐘拍攝一次。
- 每週一至週六、午夜後 10 分鐘、最多可拍攝兩個每日快照。
- 每個星期日午夜後 15 分鐘、最多拍攝兩個每週快照。

除非您在建立磁碟區時指定快照原則，否則該磁碟區會繼承與其內含儲存虛擬機器（ SVM ）相關聯的快照原則。

何時設定自訂 **ONTAP** 快照原則

如果預設的快照原則不適用於磁碟區，您可以設定自訂原則來修改快照的頻率，保留和名稱。排程主要取決於作用中檔案系統的變更速度。

您可能每小時都備份大量使用的檔案系統、例如資料庫、而每天備份一次極少使用的檔案。即使是資料庫、您也通常每天執行一或兩次完整備份、同時每小時備份交易記錄。

其他因素包括檔案對貴組織的重要性、服務層級協議（SLA）、恢復點目標（RPO）、以及恢復時間目標（RTO）。一般而言，您應該只保留必要數量的快照。

建立 **ONTAP** 快照工作排程

快照原則至少需要一個快照工作排程。您可以使用 System Manager 或 `job schedule cron create`命令來建立工作排程。如"指令參考資料ONTAP"需詳細 `job schedule cron create` 資訊，請參閱。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"建立快照作業計劃。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

根據預設， ONTAP 會在工作排程名稱中附加時間戳記，以形成快照名稱。

如果您同時指定日期和星期的值、則會將這些值視為獨立的值。例如、包含日期規格的 cron 排程 `Friday` 以及月份規格 `13` 每週五及每月第 13 天都會執行、不只是每週五的第 13 天。

範例 **30.** 步驟

系統管理員

1. 瀏覽至 * 保護 > 概述 * 並展開 * 本機原則設定 * 。
2. 在 * 排程 * 窗格中、按一下 → 。
3. 在 **Scheduls** 窗口中，單擊 + Add 。
4. 在 * 新增排程 * 視窗中、輸入排程名稱、然後選擇內容和排程類型。
5. 按一下「 * 儲存 * 」。

CLI

1. 建立工作排程：

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

從功能性的9.10.1開始ONTAP 、您可以在工作排程中加入Vserver：

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

以下範例建立名為的工作排程 `myweekly` 週六上午 3 ： 00 開始：

```
cluster1::> job schedule cron create -name myweekly -dayofweek
"Saturday" -hour 3 -minute 0
```

下列範例會建立名為的排程 `myweeklymulti` 指定多天、小時和分鐘：

```
job schedule cron create -name myweeklymulti -dayofweek
"Monday,Wednesday,Sunday" -hour 3,9,12 -minute 0,20,50
```

建立 **ONTAP** 快照原則

Snapshot 原則會指定何時建立快照，要保留多少份複本，以及如何命名這些快照。例如，系統可能每天在上午 12 ： 10 建立一個快照，保留兩個最新的複本，並將其命名為「 daily.*timestamp* 」。快照原則最多可包含五個工作排程。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"建立快照策略。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

根據預設， ONTAP 會在工作排程名稱中附加時間戳記，以形成快照名稱：

```
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

您可以視需要以首碼取代工作排程名稱。

。 `snapmirror-label` 選項適用於 SnapMirror 複寫。如需詳細資訊、請參閱 "定義原則規則"。

步驟

您可以使用系統管理員或 ONTAP CLI 建立快照原則。此程序僅會在本機叢集上建立快照原則。

系統管理員

1. 瀏覽至 * 保護 > 概述 * 並展開 * 本機原則設定 * 。
2. 在 * Snapshot Policis* 窗格中，單擊 → 。
3. 在 **Snapshot Policis** 選項卡中，單擊 + Add 。
4. 在 * 新增快照原則 * 視窗中，輸入原則名稱，然後選擇範圍。
5. 按一下 + Add 。
6. 若要選取排程、請按一下目前顯示的排程名稱、按一下 ⌄ 、然後選擇不同的排程。
7. 輸入要保留的最大快照數，並視需要輸入 SnapMirror 標籤和 SnapLock 保留期間。
8. 按一下「 * 儲存 * 」 。

CLI

1. 建立快照原則：

```
volume snapshot policy create -vserver <SVM> -policy <policy_name>
-enabled true|false -schedule1 <schedule1_name> -count1
<copies_to_retain> -prefix1 <snapshot_prefix> -snapmirror-label1
<snapshot_label> ... -schedule5 <schedule5_name> -count5
<copies_to_retain> -prefix5 <snapshot_prefix> -snapmirror-label5
<snapshot_label>
```

以下範例建立一個快照原則，其名稱 `snap_policy_daily`是根據排程執行 `daily`。策略最多有五個快照，每個快照都帶有名稱 `daily.timestamp`和 `SnapMirror 標籤 `daily`：

```
cluster1::> volume snapshot policy create -vserver vs0 -policy
snap_policy_daily -schedule1 daily -count1 5 -snapmirror-label1
daily
```

手動管理快照

手動建立和刪除快照

您可以在無法等待排程快照建立時手動建立快照，也可以在不再需要快照時刪除快照。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"建立按需快照。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

手動建立快照

您可以使用系統管理員或 ONTAP CLI 手動建立快照。

系統管理員

步驟

1. 導覽至*儲存>磁碟區*並選擇*快照*標籤。
2. 按一下 + Add 。
3. 在 *Add a snapshot * （添加快照 * ）窗口中，接受默認的快照名稱或根據需要進行編輯。
4. * 選用 * ：新增 SnapMirror 標籤。
5. 按一下「 * 新增 * 」。

CLI

1. 建立快照：

```
volume snapshot create -vserver <SVM> -volume <volume> -snapshot
<snapshot_name>
```

手動刪除快照

您可以使用系統管理員或 ONTAP CLI 手動刪除快照。

系統管理員

步驟

1. 瀏覽至 * 儲存 > Volumes （磁碟區） * 、然後選取 * Snapshot Copies （快照複本） * 標籤。
2. 找到要刪除的快照，單擊 ，然後選擇 * 刪除 * 。
3. 在 * 刪除 snapshot * 視窗中，選取 * 刪除 snapshot * 。
4. 按一下*刪除*。

CLI

1. 使用 `volume snapshot show`命令來驗證您要刪除的快照。

```
volume snapshot show -vserver <SVM> -volume <volume>
```

在此範例中，命令會顯示 SVM VS3 中 Volume vol3 上的快照。

```
cluster::> volume snapshot show -vserver vs3 -volume vol3

                                                  ---Blocks---
Vserver  Volume  Snapshot                  Size   Total% Used%
-------- ------- ------------------------ -----  ------ -----
vs3      vol3
                 snap1.2013-05-01_0015   100KB   0%    38%
                 snap1.2013-05-08_0015   76KB    0%    32%
                 snap2.2013-05-09_0010   76KB    0%    32%
                 snap2.2013-05-10_0010   76KB    0%    32%
                 snap3.2013-05-10_1005   72KB    0%    31%
                 snap3.2013-05-10_1105   72KB    0%    31%
                 snap3.2013-05-10_1205   72KB    0%    31%
                 snap3.2013-05-10_1305   72KB    0%    31%
                 snap3.2013-05-10_1405   72KB    0%    31%
                 snap3.2013-05-10_1505   72KB    0%    31%
10 entries were displayed.
```

2. 刪除快照：

如果您想要...	輸入此命令...
刪除單一快照	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name_`

如果您想要...	輸入此命令...
刪除多個快照	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot _snapshot_name1_[,_snapshot_name2_,...]`
刪除所有快照	`volume snapshot delete -vserver _svm_name_ -volume _vol_name_ -snapshot *`

刪除快照之前，請先計算可回收空間

從 ONTAP 9.10.1 開始，您可以使用系統管理員選取要刪除的快照，並在刪除這些快照之前計算可回收的空間。

步驟

1. 按一下「儲存設備>磁碟區」。
2. 選取您要從中刪除快照的磁碟區。
3. 點選“快照”。
4. 選取一或多個快照。
5. 按一下*「計算可回收空間」*。

管理快照保留

瞭解如何管理 **ONTAP** 快照保留區

_snapshot reserve 會預留一定百分比的磁碟空間供快照使用，預設為 5% 。由於快照在快照保留空間用盡時會佔用作用中檔案系統的空間，因此您可能需要視需要增加快照保留空間。或者，您也可以在保留空間已滿時自動刪除快照。

何時增加快照保留

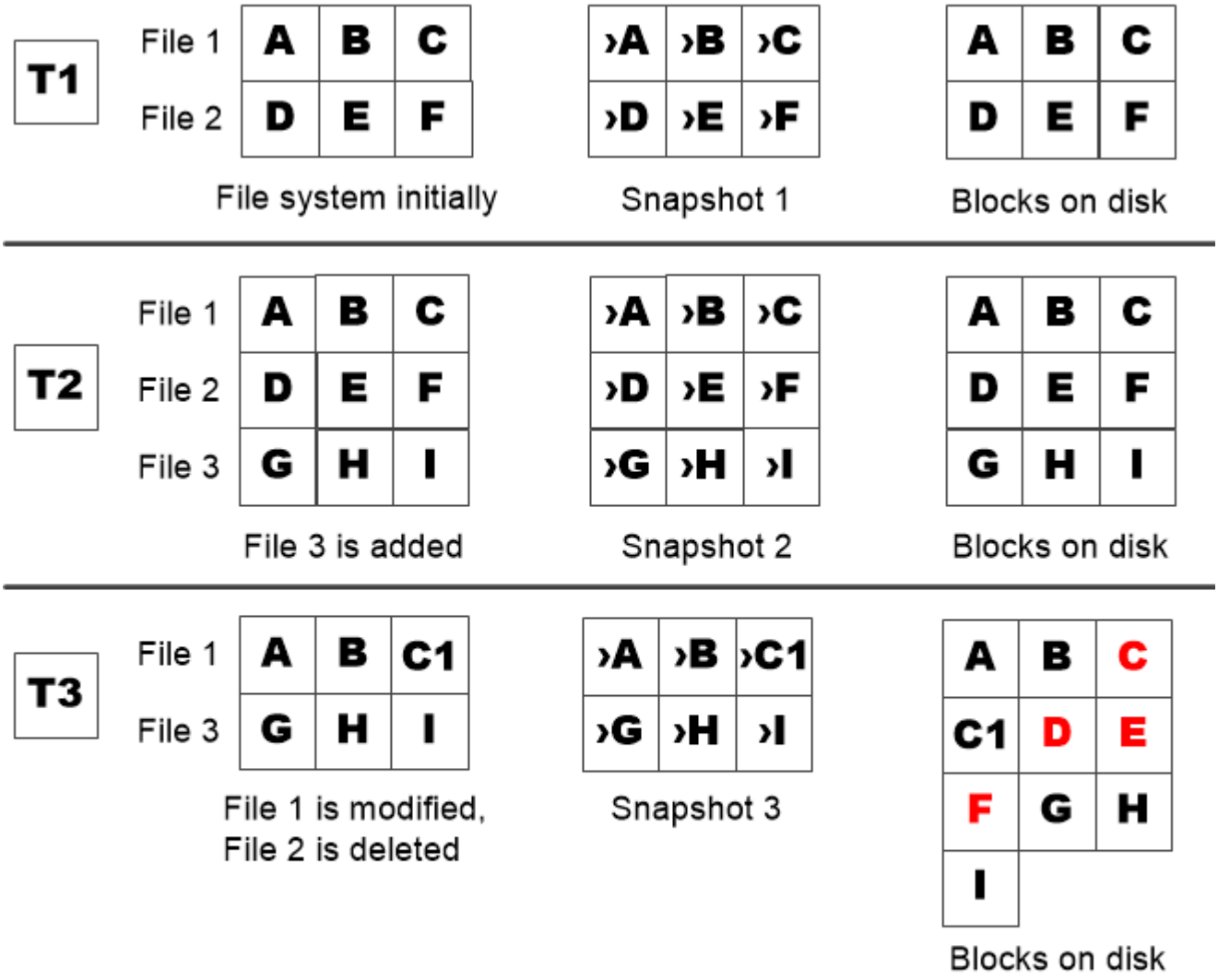
在決定是否增加快照保留時，請務必記住，快照記錄只會在上次快照建立後變更檔案。只有在修改或刪除作用中檔案系統中的區塊時、才會佔用磁碟空間。

這表示檔案系統的變更率是決定快照所用磁碟空間量的關鍵因素。無論您建立多少個快照，如果使用中的檔案系統尚未變更，快照都不會佔用磁碟空間。

例如，包含資料庫交易記錄的 FlexVol volume 可能會有高達 20% 的快照保留空間，以因應其較高的變更率。您不僅想要建立更多快照來擷取更頻繁的資料庫更新，還想要擁有更大的快照保留空間來處理快照所佔用的額外磁

碟空間。

快照包含指向區塊的指標，而非區塊的複本。您可以將指標視為區塊上的「宣告」：ONTAP 「保留」區塊，直到刪除快照為止。



A Snapshot copy consumes disk space only when blocks in the active file system are modified or deleted.

刪除受保護檔案的方式、會導致檔案空間比預期要小

即使刪除使用該區塊的檔案，快照仍會指向某個區塊。這說明了為什麼用盡快照保留空間可能會導致相反的直覺結果，導致刪除整個檔案系統所產生的可用空間比檔案系統佔用的空間更少。

請考慮下列範例。刪除任何檔案之前、 `df` 命令輸出如下所示：

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 3000000 0       100%
/vol/vol0/.snapshot 1000000 500000  500000   50%
```

刪除整個檔案系統並建立磁碟區快照之後，命令會 `df`產生下列輸出：

```
Filesystem           kbytes  used    avail  capacity
/vol/vol0/           3000000 2500000 500000   83%
/vol/vol0/.snapshot 1000000 3500000 0       350%
```

如輸出所示，除了刪除前使用的 0.5 GB 之外，目前快照也會使用先前使用中檔案系統所使用的全部 3 GB 。

由於快照所使用的磁碟空間現在已超過快照保留空間，因此 2.5 GB 的「空間」會溢入保留給作用中檔案的空間，因此您有 0.5 GB 的可用空間可容納您合理預期需要 3 GB 的檔案。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

監控 ONTAP 快照磁碟使用量

您可以使用命令來監控快照磁碟使用量 `df`。此命令會顯示作用中檔案系統和快照保留區中的可用空間量。

步驟

1. 顯示快照磁碟使用量： `df`

   以下範例顯示快照磁碟使用量：

   ```
   cluster1::> df
   Filesystem           kbytes  used    avail  capacity
   /vol/vol0/           3000000 3000000 0        100%
   /vol/vol0/.snapshot 1000000 500000  500000    50%
   ```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

檢查磁碟區上可用的 ONTAP 快照保留區

您可能想要使用命令的參數 `volume show`來檢查磁碟區上有多少可用的快照保留空間 `snapshot-reserve-available`。如"指令參考資料ONTAP"需詳細 `volume show`資訊，請參閱。

步驟

1. 檢查磁碟區上可用的快照保留區：

   ```
   vol show -vserver SVM -volume volume -fields snapshot-reserve-available
   ```

   以下範例顯示可用的快照保留 `vol1`：

```
cluster1::> vol show -vserver vs0 -volume vol1 -fields snapshot-reserve-
available

vserver volume snapshot-reserve-available
------- ------ --------------------------
vs0     vol1   4.84GB
```

修改 ONTAP 快照保留

您可能想要設定較大的快照保留空間，以防止快照使用保留給作用中檔案系統的空間。當您不再需要足夠的快照空間時，可以減少快照保留。

步驟

1. 修改快照保留：

   `volume modify -vserver` *SVM* `-volume` *volume* `-percent-snapshot-space` *snap_reserve*

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

   以下範例將快照保留設定為 `vol1` 10% ：

   ```
   cluster1::> volume modify -vserver vs0 -volume vol1 -percent-snapshot
   -space 10
   ```

自動刪除 ONTAP 快照

您可以使用 `volume snapshot autodelete modify`命令，在超過 Snapshot 保留時觸發自動刪除快照。依預設，最舊的快照會先刪除。如"指令參考資料ONTAP"需詳細 `volume snapshot autodelete modify`資訊，請參閱。

關於這項工作

當沒有要刪除的快照時， LUN 和檔案複本會被刪除。

步驟

1. 自動刪除快照：

   `volume snapshot autodelete modify -vserver` *SVM* `-volume` *volume* `-enabled true|false -trigger volume|snap_reserve`

   下列範例會在快照保留空間用盡時自動刪除快照 `vol1`：

   ```
   cluster1::> volume snapshot autodelete modify -vserver vs0 -volume vol1
   -enabled true -trigger snap_reserve
   ```

從快照還原檔案

從 **NFS** 或 **SMB** 用戶端上的 **ONTAP** 快照還原檔案

NFS 或 SMB 用戶端上的使用者可以直接從快照還原檔案，而無需儲存系統管理員介入。

檔案系統中的每個目錄都包含一個子目錄，命名為 NFS 和 SMB 使用者可存取的子目錄 `.snapshot`。`.snapshot`子目錄包含與磁碟區快照對應的子目錄：

```
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
```

每個子目錄都包含快照所參照的檔案。如果使用者不小心刪除或覆寫檔案，他們可以將檔案從 Snapshot 子目錄複製到讀寫目錄，將檔案還原到父讀寫目錄：

```
$ ls my.txt
ls: my.txt: No such file or directory
$ ls .snapshot
daily.2017-05-14_0013/              hourly.2017-05-15_1106/
daily.2017-05-15_0012/              hourly.2017-05-15_1206/
hourly.2017-05-15_1006/             hourly.2017-05-15_1306/
$ ls .snapshot/hourly.2017-05-15_1306/my.txt
my.txt
$ cp .snapshot/hourly.2017-05-15_1306/my.txt .
$ ls my.txt
my.txt
```

啟用和停用 **NFS** 和 **SMB** 用戶端存取 **ONTAP** 快照目錄

您可以使用命令的 ONTAP CLI 選項來 `volume modify`啟用和停用快照目錄的存取 `-snapdir-access`，從 ONTAP 9.10.1 開始，您可以使用系統管理員來啟用或停用用戶端系統來存取磁碟區上的快照目錄。啟用存取可讓用戶端看到快照目錄，並允許 Windows 用戶端將磁碟機對應至快照目錄，以檢視及存取其內容。然後 NFS 和 SMB 用戶端可以從快照還原檔案或 LUN 。

您可以編輯磁碟區設定或編輯磁碟區的共用設定，來啟用或停用對磁碟區快照目錄的存取。

透過編輯磁碟區來啟用或停用用戶端對快照目錄的存取

步驟

您可以使用 ONTAP 系統管理員或 ONTAP CLI 來啟用和停用用戶端快照目錄存取。根據預設，用戶端可存取磁碟區上的 Snapshot 目錄。

系統管理員

1. 按一下「儲存設備>磁碟區」。
2. 選取包含您要顯示或隱藏之快照目錄的磁碟區。
3. 按一下 ⋮ 並選取 * 編輯 * 。
4. 在*快照（本機）設定*部分中，選擇或取消選擇*向客戶端顯示快照目錄*。
5. 按一下「 * 儲存 * 」。

CLI

1. 檢查快照目錄存取狀態：

   ```
   volume show -vserver <SVM_name> -volume <vol_name> -fields snapdir-
   access
   ```

   範例：

   ```
   clus1::> volume show -vserver vs0 -volume vol1 -fields snapdir-
   access
   vserver volume snapdir-access
   ------- ------ --------------
   vs0     vol1   false
   ```

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

2. 啟用或停用快照目錄存取：

   ```
   volume modify -vserver <SVM_name> -volume <vol_name> -snapdir-access
   <true|false>
   ```

   以下範例可在 vol1 上啟用快照目錄存取：

   ```
   clus1::> volume modify -vserver vs0 -volume vol1 -snapdir-access
   true
   Volume modify successful on volume vol1 of Vserver vs0.
   ```

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

透過編輯共用來啟用或停用用戶端對快照目錄的存取

根據預設，用戶端可存取磁碟區上的 Snapshot 目錄。

步驟

1. 按一下「儲存設備>共享區」。
2. 選取包含您要顯示或隱藏之快照目錄的磁碟區。
3. 按一下 ⋮ 並選取 * 編輯 * 。
4. 在 * 共用內容 * 區段中，選取或取消選取 * 允許用戶端存取快照目錄 * 。
5. 按一下「 * 儲存 * 」。

從 **ONTAP** 快照還原單一檔案

您可以使用 `volume snapshot restore-file`命令從快照還原單一檔案或 LUN 。如果您不想取代現有檔案、可以將檔案還原至父讀寫磁碟區中的其他位置。

關於這項工作

如果您要還原現有 LUN ，則會以快照形式建立並備份 LUN 複本。在還原作業期間、您可以從 LUN 讀取及寫入 LUN 。

預設會還原具有串流的檔案。

步驟

1. 列出磁碟區中的快照：

   ```
   volume snapshot show -vserver SVM -volume volume
   ```

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

   以下範例顯示中的快照 `vol1`：

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                  State    Size  Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
                  daily.2013-01-25_0010   valid   92KB      0%    0%
                  hourly.2013-01-25_0105  valid   228KB     0%    0%
                  hourly.2013-01-25_0205  valid   236KB     0%    0%
                  hourly.2013-01-25_0305  valid   244KB     0%    0%
                  hourly.2013-01-25_0405  valid   244KB     0%    0%
                  hourly.2013-01-25_0505  valid   244KB     0%    0%

   7 entries were displayed.
   ```

2. 從快照還原檔案：

   ```
   volume snapshot restore-file -vserver SVM -volume volume -snapshot snapshot
   -path file_path -restore-path destination_path
   ```

如"指令參考資料ONTAP"需詳細 `volume snapshot restore-file`資訊，請參閱。

以下範例還原檔案 `myfile.txt`：

```
cluster1::> volume snapshot restore-file -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010 -path /myfile.txt
```

從 **ONTAP** 快照還原部分檔案

您可以使用 `volume snapshot partial-restore-file`命令將資料範圍從快照還原至 LUN 或 NFS 或 SMB 容器檔案，前提是您知道資料的起始位元組偏移和位元組數。您可以使用此命令來還原主機上的其中一個資料庫、該資料庫會將多個資料庫儲存在同一個LUN中。

從 ONTAP 9.12.1 開始，使用的磁碟區可SnapMirror 主動同步進行部分還原。

步驟

1. 列出磁碟區中的快照：

   `volume snapshot show -vserver` *`SVM`* `-volume` *`volume`*

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

   以下範例顯示中的快照 `vol1`：

   ```
   clus1::> volume snapshot show -vserver vs1 -volume vol1

   Vserver Volume Snapshot                  State    Size  Total% Used%
   ------- ------ ---------- ----------- ------   -----  ------ -----
   vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
                  daily.2013-01-25_0010   valid   92KB      0%    0%
                  hourly.2013-01-25_0105  valid   228KB     0%    0%
                  hourly.2013-01-25_0205  valid   236KB     0%    0%
                  hourly.2013-01-25_0305  valid   244KB     0%    0%
                  hourly.2013-01-25_0405  valid   244KB     0%    0%
                  hourly.2013-01-25_0505  valid   244KB     0%    0%

   7 entries were displayed.
   ```

2. 從快照還原部分檔案：

   `volume snapshot partial-restore-file -vserver` *`SVM`* `-volume` *`volume`* `-snapshot` *`snapshot`* `-path` *`file_path`* `-start-byte` *`starting_byte`* `-byte-count` *`byte_count`*

   起始位元組偏移和位元組數必須是4、096的倍數。

   下列範例還原檔案的前 4,096 位元組 `myfile.txt`：

```
cluster1::> volume snapshot partial-restore-file -vserver vs0 -volume
vol1 -snapshot daily.2013-01-25_0010 -path /myfile.txt -start-byte 0
-byte-count 4096
```

從 **ONTAP** 快照還原磁碟區的內容

您可以從快照還原，將磁碟區恢復到較早的時間點。您可以使用 System Manager 或 `volume snapshot restore`命令，從快照還原磁碟區的內容。如"指令參考資料ONTAP"需詳細 `volume snapshot restore`資訊，請參閱。

關於這項工作

如果磁碟區具有 SnapMirror 關係，請在從快照還原後立即手動複寫磁碟區的所有鏡射複本。否則可能導致無法使用的鏡像複本、必須刪除並重新建立。

步驟

您可以使用系統管理員或 ONTAP CLI ，從較早的快照還原。

系統管理員

1. 按一下「儲存設備」、然後選取一個磁碟區。
2. 在 * Snapshot Copies * （快照複本 * ）下，按一下 ⋮ 您要還原的快照旁的，然後選取 * Restore * （還原 * ）。

CLI

1. 列出磁碟區中的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

以下範例顯示中的快照 `vol1`：

```
clus1::> volume snapshot show -vserver vs1 -volume vol1

Vserver Volume Snapshot                  State    Size  Total% Used%
------- ------ ---------- ----------- ------   -----  ------ -----
vs1     vol1   hourly.2013-01-25_0005  valid   224KB     0%    0%
               daily.2013-01-25_0010   valid   92KB      0%    0%
               hourly.2013-01-25_0105  valid   228KB     0%    0%
               hourly.2013-01-25_0205  valid   236KB     0%    0%
               hourly.2013-01-25_0305  valid   244KB     0%    0%
               hourly.2013-01-25_0405  valid   244KB     0%    0%
               hourly.2013-01-25_0505  valid   244KB     0%    0%

7 entries were displayed.
```

2. 從快照還原磁碟區的內容：

```
volume snapshot restore -vserver <SVM> -volume <volume> -snapshot
<snapshot>
```

下列範例還原的內容 `vol1`：

```
cluster1::> volume snapshot restore -vserver vs0 -volume vol1
-snapshot daily.2013-01-25_0010
```

SnapMirror Volume複寫

瞭解 SnapMirror Volume 複寫

瞭解 ONTAP SnapMirror 非同步災難恢復

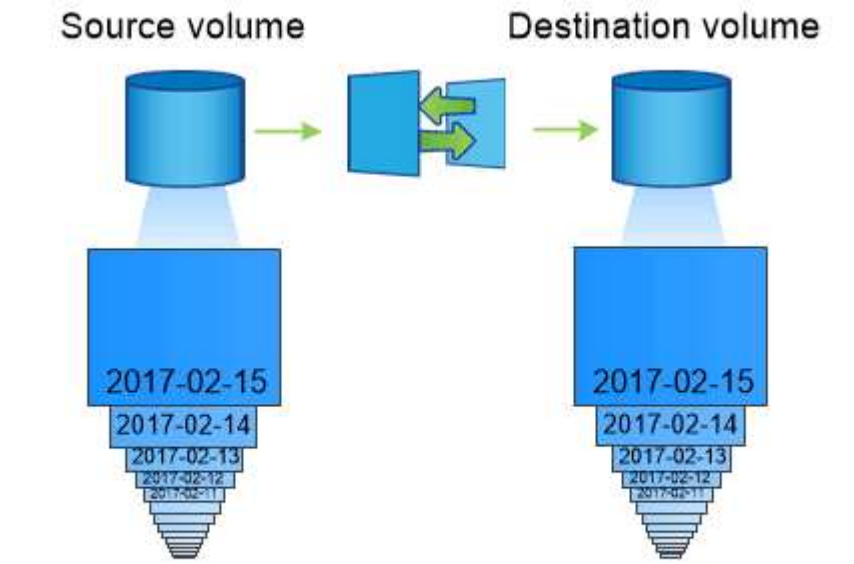
_SnapMirror是災難恢復技術、專為從一線儲存設備容錯移轉到位於地理位置遠端站台的二線儲存設備而設計。顧名思義、SnapMirror會在二線儲存設備中建立工作資料的複本（或鏡射）、以便在主站台發生災難時、繼續提供資料。

如果主要站台仍可用於提供資料、您只需將任何需要的資料傳回該站台、而不需要從鏡像為用戶端提供服務。如同容錯移轉使用案例所暗示、次要系統上的控制器應與主要系統上的控制器相當或幾乎等同、以有效率地從鏡射儲存設備提供資料。

資料保護關係

資料會在磁碟區層級鏡射。主要儲存設備中的來源磁碟區與次要儲存設備中的目的地磁碟區之間的關係稱為 _ 資料保護關係。 _ 磁碟區所在的叢集和從磁碟區提供資料"已有速度"的 SVM 必須是。對等關係可讓叢集和 SVM 安全地交換資料。

下圖說明 SnapMirror 資料保護關係：



A SnapMirror data protection relationship typically mirrors the Snapshot copies available on the source volume.

資料保護關係的範圍

您可以直接在磁碟區之間或在擁有磁碟區的SVM之間建立資料保護關係。在_SVM資料保護關係中、系統會複寫SVM組態的全部或部分內容、從NFS匯出、SMB共用到RBAC、以及SVM所擁有的磁碟區資料。

您也可以將 SnapMirror 用於特殊的資料保護應用程式：

- SVM根磁碟區的_負載共用mirror _複本可確保在節點中斷或容錯移轉時、資料仍可存取。
- 「_SURFVolumes SnapLock 」之間的資料保護關係可讓您將WORM檔案複寫到二線儲存設備。

  "利用SnapLock NetApp技術歸檔及法規遵循"

- 從 ONTAP 9 · 13.1 開始，您可以使用 SnapMirror 異步來保護一致性群組。從 ONTAP 9.14.1 開始，您可以使用 SnapMirror 非同步功能，使用一致性群組關係，將 Volume 精細的快照複寫到目的地叢集。如需更多資訊、請參閱 設定 SnapMirror 非同步保護。

SnapMirror資料保護關係如何初始化

第一次叫用SnapMirror時、它會執行從來源磁碟區到目的地磁碟區的_基準傳輸_。關聯的_SnapMirror原則_定義了基準的內容和任何更新。

預設 SnapMirror 原則下的基礎傳輸 `MirrorAllSnapshots` 涉及下列步驟：

- 製作來源 Volume 的快照。
- 將快照及其參照的所有資料區塊傳輸至目的地 Volume 。
- 將來源磁碟區上的剩餘快照傳輸到目的地磁碟區，以便在「 'active' 」鏡像毀損時使用。

SnapMirror資料保護關係如何更新

更新是非同步的、會依照您設定的排程進行。保留會鏡射來源上的快照原則。

在原則下的每個更新中， SnapMirror 都 `MirrorAllSnapshots`會建立來源磁碟區的快照，並傳輸自上次更新後所建立的快照和任何快照。在原則命令的 `MirrorAllSnapshots`下列輸出中， `snapmirror policy show`請注意下列事項：

- `Create Snapshot`為「 'true' 」，表示 `MirrorAllSnapshots`在 SnapMirror 更新關係時建立快照。
- `MirrorAllSnapshots`具有規則「 `shm_Created 」和「 `all_source_snapshots 」，表示 SnapMirror 更新關係時，會同時傳輸 SnapMirror 建立的快照和自上次更新後建立的任何快照。

```
cluster_dst::> snapmirror policy show -policy MirrorAllSnapshots -instance

                     Vserver: vs0
      SnapMirror Policy Name: MirrorAllSnapshots
      SnapMirror Policy Type: async-mirror
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: SnapMirror asynchronous policy for mirroring
all snapshots
                              and the latest active file system.
       Total Number of Rules: 2
                  Total Keep: 2
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              all_source_snapshots    1  false       0 -
-
```

MirrorLatest原則

預先設定的 `MirrorLatest`**原則運作方式與完全相同** `MirrorAllSnapshots`，只有在初始化和更新時才會傳輸由 SnapMirror 建立的快照。

```
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
```

相關資訊

- "SnapMirror 策略顯示"

瞭解 **ONTAP SnapMirror** 同步災難恢復

從 ONTAP 9 5 開始、 SnapMirror 同步（ SM-S ）技術在所有至少有 16 GB 記憶體的

FAS 和 AFF 平台、以及所有 ONTAP Select 平台上均受到支援。SnapMirror 同步技術是一項每個節點的授權功能、可在 Volume 層級提供同步資料複寫。

這項功能可滿足金融、醫療及其他管制產業的法規及國家要求、在需要零資料遺失的情況下進行同步複寫。

允許 **SnapMirror** 同步作業

每個 HA 配對的 SnapMirror 同步複寫作業數上限取決於控制器機型。

下表列出每個 HA 配對所允許的 SnapMirror 同步作業數、視平台類型和 ONTAP 版本而定。

平台	ONTAP 9.14.1 至ONTAP 9.11.1	零點9.10.1 ONTAP	部分9.9.1 ONTAP	發行版本早於2009年9月9日ONTAP
AFF	400	200	160	80
ASA	400	200	160	80
FAS	80	80	80	40.
ONTAP Select	40.	40.	40.	20.

支援的功能

下表說明 SnapMirror 同步支援的功能、以及提供支援的 ONTAP 版本。

功能	第一版支援	其他資訊
SnapMirror 同步關係主要磁碟區上的防毒軟體	ONTAP 9.6	
應用程式建立的快照複寫	更新ONTAP	如果快照在拍攝時帶有適當的標籤 `snapshot create`操作，使用 CLI 或ONTAP API， SnapMirror在靜止應用程式後同步複製快照（包括使用者建立的快照或使用外部腳本建立的快照）。使用快照策略建立的計劃快照不會被複製。有關複製應用程式創建的快照的更多信息，請參閱"NetApp知識庫：如何使用SnapMirror同步複製應用程式建立的快照"。
複製自動刪除	ONTAP 9.6	
SnapMirror 同步來源和目的地支援 FabricPool 集合體的分層原則為「無」、「快照」或「自動」。	版本9.5 ONTAP	無法將目的地Volume的FabricPool 目的地集合體設為All Tiering原則。
FC	版本9.5 ONTAP	所有延遲不超過 10 毫秒的網路
FC-NVMe	更新ONTAP	
檔案複製	更新ONTAP	
SnapMirror 同步關係主要 Volume 上的 FPolicy	ONTAP 9.6	

SnapMirror 同步關係的主要 Volume 上的硬配額和軟配額	ONTAP 9.6	配額規則不會複寫到目的地、因此配額資料庫不會複寫到目的地。
叢集內同步關係	ONTAP 9.14.1.	當來源和目的地磁碟區放置在不同的 HA 配對上時、就會提供高可用度。如果整個叢集當機、則只有在叢集恢復之前、才能存取磁碟區。叢集內 SnapMirror 同步關係將有助於達到同步每個 HA 配對的關係的整體限制。
iSCSI	版本9.5 ONTAP	
LUN複製與NVMe命名空間複製	更新ONTAP	
以應用程式建立的快照作為後盾的 LUN 複本	更新ONTAP	
混合式傳輸協定存取（ NFS v3 和 SMB ）	ONTAP 9.6	
NDMP / NDMP 還原	ONTAP 9.13.1.12.9.11.9.11.	來源叢集和目的地叢集都必須執行 ONTAP 9.13.1 或更新版本、才能搭配 SnapMirror 同步使用 NDMP 。如需詳細資訊、請參閱 使用 NDMP 複本傳輸資料。
僅限在 AFF / ASA 平台上執行不中斷的 SnapMirror 同步作業（ n ）。	ONTAP 9.12.1	支援不中斷營運、可讓您在不排程停機時間的情況下執行許多常見的維護工作。支援的作業包括接管與恢復、以及在兩個叢集之間保留一個節點的磁碟區移動。
NFS v4.2	零點9.10.1 ONTAP	
NFS v4.0	ONTAP 9.6	
NFS v4.1	ONTAP 9.6	
NVMe / TCP	9.10.1	
移除高中繼資料作業頻率限制	ONTAP 9.6	
使用TLS 1.2加密技術、確保傳輸中的敏感資料安全無虞	ONTAP 9.6	
單一檔案與部分檔案還原	ONTAP 9.13.1.12.9.11.9.11.	
SMB 2.0 或更新版本	ONTAP 9.6	
SnapMirror 同步鏡射鏡射串聯	ONTAP 9.6	來自 SnapMirror 同步關係目的地 Volume 的關係必須是 SnapMirror 非同步關係。
SVM 災難恢復	ONTAP 9.6	* SnapMirror 同步來源也可以是 SVM 災難恢復來源、例如、將 SnapMirror 同步化為單一連線的開機組態、以及將 SVM 災難恢復視為另一方的開機組態。* SnapMirror 同步來源不能是 SVM 災難恢復目的地、因為 SnapMirror 同步不支援串聯資料保護來源。您必須先釋放同步關係、才能在目的地叢集中執行 SVM 災難恢復反轉重新同步。* SnapMirror 同步目的地不能是 SVM 災難恢復來源、因為 SVM 災難恢復不支援 DP 磁碟區的複寫。同步來源的反轉重新同步會導致 SVM 災難恢復、但目的地叢集中的 DP Volume 除外。

磁帶型還原至來源磁碟區	ONTAP 9.13.1.12.9.11.9.11.	
NAS的來源與目的地磁碟區之間的時間戳記同位元	ONTAP 9.6	如果您已從ONTAP 還原9.5升級ONTAP 為還原9.6、則時間戳記只會複寫到來源Volume中的任何新檔案和修改的檔案。來源Volume中現有檔案的時間戳記不會同步。

不支援的功能

SnapMirror 同步關係不支援下列功能：

- 自主勒索軟體保護
- 一致性群組
- DP_最佳化（DPO）系統
- 資料量FlexGroup
- 資料量FlexCache
- 全域節流
- 在扇出組態中、只有一個關係可以是 SnapMirror 同步關係；來源磁碟區的所有其他關係都必須是 SnapMirror 非同步關係。
- LUN 搬移
- 內部組態MetroCluster
- 混合式SAN與NVMe存取
  LUN和NVMe命名空間不支援在同一個磁碟區或SVM上。
- SnapCenter
- 資料量SnapLock
- 防竄改快照
- 在目的地磁碟區上使用dump和SMtape進行磁帶備份或還原
- 來源磁碟區的處理量層（QoS下限）
- Volume SnapRestore
- VVOL

操作模式

SnapMirror 同步會根據所使用的 SnapMirror 原則類型、提供兩種作業模式：

- *同步模式*在同步模式下、應用程式I/O作業會平行傳送至主要和次要儲存系統。如果由於任何原因而未完成對二線儲存設備的寫入、則允許應用程式繼續寫入一線儲存設備。當錯誤狀況得到修正時、 SnapMirror 同步技術會自動與次要儲存設備重新同步、並以同步模式從主要儲存設備恢復複寫至次要儲存設備。在同步模式中、RPO=0和RTO非常低、直到發生二線複寫故障、導致RPO和RTO無法確定、但等於修復導致二線複寫失敗並完成重新同步的問題所需時間。
- *StrictSync 模式 * SnapMirror 同步可以選擇在 StrictSync 模式下運行。如果由於任何原因未完成對二線儲存設備的寫入、應用程式I/O就會失敗、因此可確保一線與二線儲存設備完全相同。只有在 SnapMirror 關係恢

復為 `InSync`狀態後、主應用程式的 I/O 才會恢復。如果主儲存設備故障、則可在容錯移轉後、在二線儲存設備上恢復應用程式I/O、而不會遺失資料。在StrictSync模式中、RPO永遠為零、RTO極低。

關係狀態

SnapMirror 同步關係的狀態在 `InSync`正常操作期間始終處於狀態。如果 SnapMirror 傳輸因任何原因而失敗、則目的地不會與來源同步、 `OutofSync`因此可以進入狀態。

對於 SnapMirror 同步關係，系統會 `InSync` `OutofSync`以固定的時間間隔自動檢查關係狀態或）。如果關係狀態為 `OutofSync`、 ONTAP 會自動觸發自動重新同步程序、將關係恢復至 `InSync`狀態。只有在傳輸因任何作業（例如來源或目的地的非計畫性儲存容錯移轉或網路中斷）而失敗時、才會觸發自動重新同步。使用者啟動的作業 `snapmirror quiesce`、例如和、 `snapmirror break`不會觸發自動重新同步。

如果 `OutofSync`在 StrictSync 模式中 SnapMirror 同步關係的關係狀態變成、則會停止對主要 Volume 的所有 I/O 作業。 `OutofSync`同步模式中的 SnapMirror 同步關係狀態不會中斷主要磁碟區的主要和 I/O 作業、

相關資訊

- "NetApp 技術報告 4733 ： SnapMirror 同步組態與最佳實務做法"
- "SnapMirror中斷"
- "SnapMirror靜止"

預設 **ONTAP** 資料保護原則

ONTAP 包含數個預設的保護原則、可用於資料保護關係。您使用的原則取決於保護關係類型。

如果預設原則不符合您的資料保護關係需求，您可以"建立自訂原則"。

預設保護原則和說明清單

以下說明預設保護原則及其相關的原則類型。

名稱	說明	原則類型
非同步	統一化的 SnapMirror 非同步和資料保險箱原則、可鏡射最新的作用中檔案系統、以及每日和每週快照、每小時傳輸排程。	非同步
AutomatedFailov	SnapMirror 同步原則、提供零 RTO 保證、讓用戶端 I/O 不會因複寫失敗而中斷。	同步
AutomatedFailOverDuplex	SnapMirror 同步原則、提供零 RTO 保證和雙向同步複寫。	同步
CloudBackupDefault	具有每日規則的資料保險箱原則。	非同步
持續	S3 貯體鏡射原則。	持續
DailyBackup	具有每日規則和每日傳輸排程的資料保險箱原則。	非同步
DPDefault	用於鏡射所有快照和最新作用中檔案系統的 SnapMirror 非同步原則。	非同步
MirrorAllSnapshots	用於鏡射所有快照和最新作用中檔案系統的 SnapMirror 非同步原則。	非同步

名稱	說明	原則類型
MirrorAllSnapshotsDiscardNetwork	用於鏡射所有快照和最新作用中檔案系統的 SnapMirror 非同步原則（不包括網路組態）。	非同步
MirrorAndVault	統一化的 SnapMirror 非同步和資料保險箱原則、用於鏡射最新的作用中檔案系統、以及每日和每週快照。	非同步
MirrorAndVaultDiscardNetwork	統一化的 SnapMirror 非同步和資料保險箱原則、用於鏡射最新的作用中檔案系統、以及不含網路組態的每日和每週快照。	非同步
MirrorLatest	用於鏡射最新作用中檔案系統的 SnapMirror 非同步原則。	非同步
SnapCenterSync	使用應用程式建立的 Snapshot 組態、 SnapMirror 同步 for SnapCenter 的原則。	同步
StrictSync	SnapMirror 同步原則：用戶端存取會在複寫失敗時中斷。	同步
同步	SnapMirror 同步原則、不會在複寫失敗時中斷用戶端存取。	同步
Unified7年	統一化 SnapMirror 原則、保留 7 年。	非同步
XDPDefault	包含每日和每週規則的資料保險箱原則。	非同步

瞭解 **ONTAP StrictSync** 和同步原則支援的工作負載

StrictSync與Sync原則支援所有使用FC、iSCSI和FC-NVMe傳輸協定的LUN型應用程式、以及適用於資料庫、VMware、配額、SMB等企業應用程式的NFSv3與NFSv3傳輸協定。從 ONTAP 9 6 開始、 SnapMirror 同步可用於電子設計自動化（ EDA ）、主目錄和軟體建置工作負載等企業檔案服務。

在《S49.5同步政策》中ONTAP 、您需要考量幾個重要方面、同時選擇NFSv3或NFSv3工作負載。工作負載的資料讀取或寫入作業量並非考量因素、因為同步原則可處理高讀取或寫入IO工作負載。在Sets9.5中ONTAP 、檔案建立、目錄建立、檔案權限變更或目錄權限變更過多的工作負載可能不適用（這些工作負載稱為高中繼資料工作負載）。高中繼資料工作負載的典型範例是DevOps工作負載、您可以在其中建立多個測試檔案、執行自動化、以及刪除檔案。另一個範例是在編譯期間產生多個暫存檔的平行建置工作負載。高速寫入中繼資料活動的影響在於、這可能會導致鏡像之間的同步暫時中斷、進而中斷用戶端的讀取和寫入IOS。

從 ONTAP 9 6 開始、這些限制就會移除、 SnapMirror 同步可用於包含多使用者環境的企業檔案服務工作負載、例如主目錄和軟體建置工作負載。

相關資訊

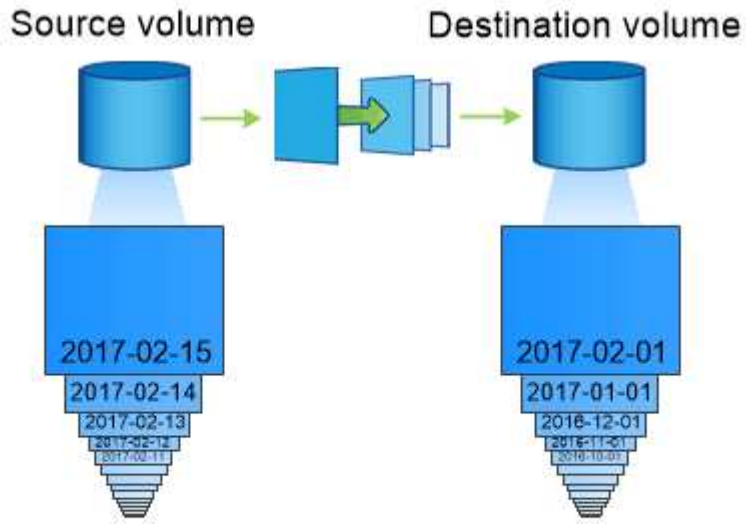
"SnapMirror 同步組態與最佳實務做法"

瞭解使用 **ONTAP SnapMirror** 技術的資料保險箱歸檔

SnapMirror保存原則取代SnapVault 了支援支援SnapMirror 9.3及更新版本的功能。ONTAP您可以使用 SnapMirror 資料保險箱原則進行磁碟對磁碟快照複寫，以符合標準及其他治理相關目的。與 SnapMirror 關係不同的是，目的地通常只包含來源 Volume 中目前的快照，資料保險箱目的地通常會保留在較長時間內建立的時間點快照。

例如，您可能想要在 20 年內保留每月資料快照，以符合貴企業的政府會計法規。由於不需要從保存庫儲存設備提供資料、因此您可以在目的地系統上使用速度較慢、成本較低的磁碟。

下圖說明SnapMirror Vault資料保護關係。



A SnapVault data protection relationship typically retains point-in-time Snapshot copies created over a longer period than the Snapshot copies on the source volume.

如何初始化保存資料保護關係

關係的SnapMirror原則定義了基礎的內容和任何更新。

預設資料保險箱原則下的基準傳輸 `XDPDefault`會建立來源磁碟區的快照，然後將該複本及其參照的資料區塊傳輸至目的地磁碟區。與 SnapMirror 關係不同的是，資料保險箱備份不會在基準線中包含較舊的快照。

如何更新保存資料保護關係

更新是非同步的、會依照您設定的排程進行。您在關係原則中定義的規則，可識別哪些新快照要包含在更新中，以及保留多少份複本。原則中定義的標籤（例如「每月」）必須符合來源上快照原則中定義的一或多個標籤。否則、複寫會失敗。

在原則下的每個更新中， SnapMirror 都 `XDPDefault`會傳輸自上次更新後所建立的快照，前提是這些快照的標籤必須符合原則規則中定義的標籤。在原則命令的 `XDPDefault`下列輸出中， `snapmirror policy show`請注意下列事項：

- `Create Snapshot`為 "`FALSE" ，表示 `XDPDefault` SnapMirror 更新關係時不會建立快照。
- `XDPDefault`有「 daily 」和「 'faily' 」規則，表示 SnapMirror 更新關係時，會傳輸來源上所有標籤相符的快照。

```
cluster_dst::> snapmirror policy show -policy XDPDefault -instance

                       Vserver: vs0
      SnapMirror Policy Name: XDPDefault
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Default policy for XDP relationships with
daily and weekly
                              rules.
       Total Number of Rules: 2
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep   Preserve Warn
Schedule Prefix
                              ----------------     ----   -------- ----
-------- ------
                              daily                   7   false       0 -
-
                              weekly                 52   false       0 -
-
```

相關資訊

- "SnapMirror 策略顯示"

瞭解 **ONTAP SnapMirror** 統一化複寫

SnapMirror _統一化複寫_可讓您在同一個目的地磁碟區上設定災難恢復與歸檔。當統一化複寫適當時、它可協助您減少所需的二線儲存設備數量、限制基礎傳輸數量、以及減少網路流量。

如何初始化統一化資料保護關係

與SnapMirror一樣、統一化資料保護會在您第一次叫用時執行基準傳輸。關係的SnapMirror原則定義了基礎的內容和任何更新。

根據預設統一資料保護原則進行的基準傳輸 `MirrorAndVault`會建立來源磁碟區的快照，然後將該複本及其參照的資料區塊傳輸至目的地磁碟區。與資料保險箱歸檔一樣，統一化資料保護也不包括基礎中較舊的快照。

如何更新統一化資料保護關係

在原則下的每個更新中， SnapMirror 都 `MirrorAndVault`會建立來源磁碟區的快照，並傳輸自上次更新後所建立

的快照和任何快照，前提是它們的標籤必須符合快照原則規則中定義的標籤。在原則命令的 `MirrorAndVault` 下列輸出中， `snapmirror policy show`請注意下列事項：

- `Create Snapshot`為「 'true' 」，表示 `MirrorAndVault`在 SnapMirror 更新關係時建立快照。
- `MirrorAndVault`有「 sim_Created 」，「 daily 」和「 'faily' 等規則，表示 SnapMirror 更新關係時，會同時傳輸 SnapMirror 建立的快照和來源上具有相符標籤的快照。

```
cluster_dst::> snapmirror policy show -policy MirrorAndVault -instance

                    Vserver: vs0
      SnapMirror Policy Name: MirrorAndVault
      SnapMirror Policy Type: mirror-vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
            Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: true
                     Comment: A unified SnapMirror synchronous and
SnapVault policy for
                              mirroring the latest file system and daily
and weekly snapshots.
       Total Number of Rules: 3
                  Total Keep: 59
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              sm_created              1  false       0 -
-
                              daily                   7  false       0 -
-
                              weekly                 52  false       0 -
-
```

Unified7年政策

預先設定的 `Unified7year`原則運作方式與完全相同， `MirrorAndVault`只是第四條規則會每月傳輸快照並保留 7 年。

```
                          Rules: SnapMirror Label     Keep   Preserve Warn
Schedule Prefix
                                 ----------------     ----   -------- ----
-------- ------
                                 sm_created              1   false       0 -
-
                                 daily                   7   false       0 -
-
                                 weekly                 52   false       0 -
-
                                 monthly                84   false       0 -
-
```

避免可能的資料毀損

統一複寫會將基準傳輸的內容限制在初始化時由 SnapMirror 建立的快照上。在每次更新時， SnapMirror 會建立來源的另一個快照，並傳輸該快照和任何標籤符合快照原則規則中定義的標籤的新快照。

您可以在目的地上建立最後傳輸的快照複本，以防止更新的快照毀損。無論來源上的保留規則為何，此「本機複本」都會保留，因此即使來源上不再提供 SnapMirror 原本傳輸的快照，也可以在目的地上取得該快照的複本。

何時使用統一化資料複寫

您需要權衡維護完整鏡像的優點、以及統一化複寫在減少二線儲存設備數量、限制基礎傳輸數量及減少網路流量方面所提供的優勢。

決定統一化複寫是否適當的關鍵因素、在於作用中檔案系統的變更率。舉例來說，傳統鏡像可能更適合儲存資料庫交易記錄每小時快照的磁碟區。

相關資訊

- "SnapMirror 策略顯示"

當 **ONTAP** 資料保護目的地磁碟區自動成長時

在資料保護鏡射傳輸期間、如果來源磁碟區已經成長、目的地磁碟區的大小會自動增加、前提是包含該磁碟區的集合體中有可用空間。

無論目的地上的任何自動成長設定為何、都會發生此行為。您無法限制磁碟區的成長、也無法防止ONTAP 不穩定地成長。

根據預設、資料保護磁碟區會設為 `grow_shrink` AutoSize 模式、可讓磁碟區根據已用空間量來增加或縮小。資料保護磁碟區的最大自動調整大小等於FlexVol 最大的尺寸、而且取決於平台。例如：

- FAS8200 、預設 DP Volume max-autossize = 100TB

如需詳細資訊、請參閱 "NetApp Hardware Universe"。

您可以使用_fan-Out_部署、將資料保護延伸到多個次要系統。您可以使用_Cascade部署、將資料保護延伸至第三系統。

扇出和串聯部署都支援 SnapMirror DR 、 SnapVault 或統一複寫的任何組合。從 ONTAP 9 5 開始、 SnapMirror 同步關係可支援使用一或多個 SnapMirror 非同步關係的扇出部署。在扇出組態中、只有一個關係可以是 SnapMirror 同步關係、來源磁碟區的所有其他關係都必須是 SnapMirror 非同步關係。SnapMirror 同步關係也支援串聯部署（從 ONTAP 9 開始）；不過、 SnapMirror 同步關係的目的地 Volume 的關係必須是 SnapMirror 非同步關係。SnapMirror 主動同步（從 ONTAP 9.13.1 開始支援）也支援開機組態。

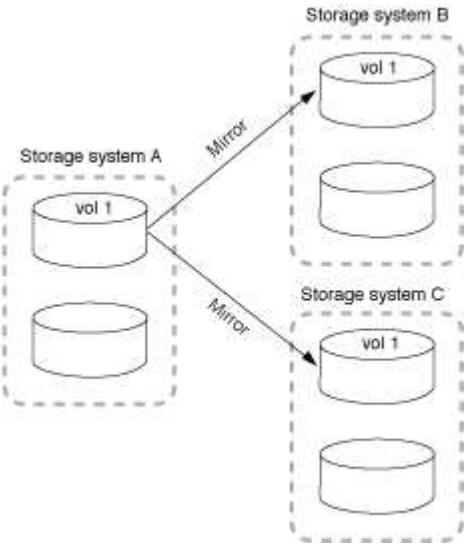
您可以使用_fan-In部署、在多個主要系統和單一次要系統之間建立資料保護關係。每個關係都必須在次要系統上使用不同的磁碟區。

您應該知道、屬於扇出或串聯組態一部分的磁碟區可能需要較長的時間重新同步。看到 SnapMirror 關係報告並不罕見長時間內的「準備」狀態。

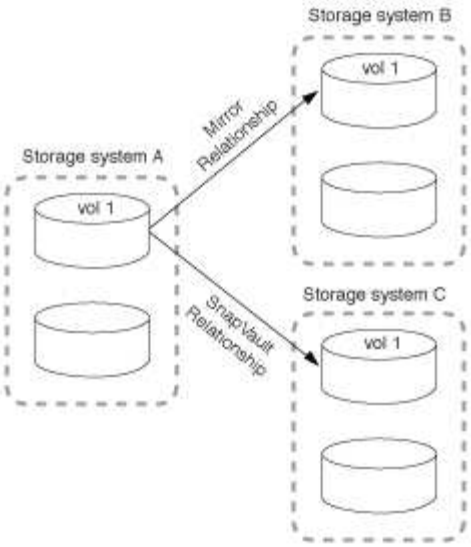
連出部署的運作方式

SnapMirror支援_multier-mirror和_mirror保存庫_的連出部署。

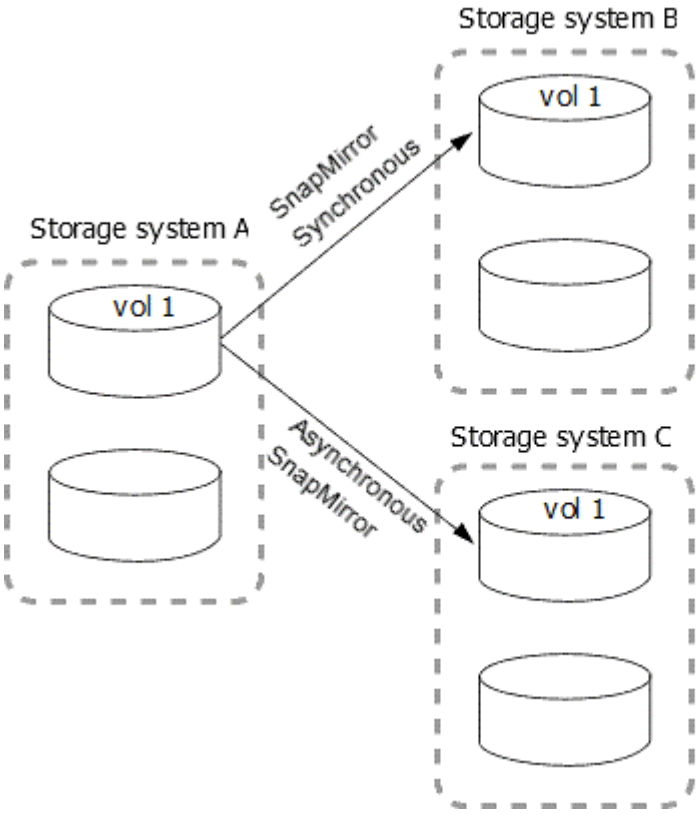
多重鏡射扇出部署是由與多個次要Volume具有鏡射關係的來源Volume所組成。



鏡射保存庫的扇出部署是由來源磁碟區所組成、該磁碟區與次要磁碟區具有鏡射關係、SnapVault 且與不同次要Volume之間存在不相關性。



從 ONTAP 9 開始、您可以使用 SnapMirror 同步關係進行開機部署；不過、在開機組態中、只有一個關係可以是 SnapMirror 同步關係、來源 Volume 的所有其他關係都必須是 SnapMirror 非同步關係。



串聯部署的運作方式

SnapMirror支援_鏡射鏡射_、鏡射-保存庫、_資料保存鏡射_和_資料保險箱-保存庫_串聯部署。

鏡射鏡射鏡射串聯部署包含一系列關係、其中來源磁碟區會鏡射至次要磁碟區、而次要磁碟區則會鏡射至第三個磁碟區。如果次要Volume無法使用、您可以在不執行新的基礎傳輸的情況下、同步主要和第三個Volume之間的關係。

在級聯磁碟區的關係中， ONTAP 9 的所有版本僅支援在級聯的最終SnapMirror目標磁碟區上保留長期快照。在級聯備份的任何中間磁碟區上啟用長期保留快照會導致備份和快照遺失。如果您使用了不支援的配置，即在級聯

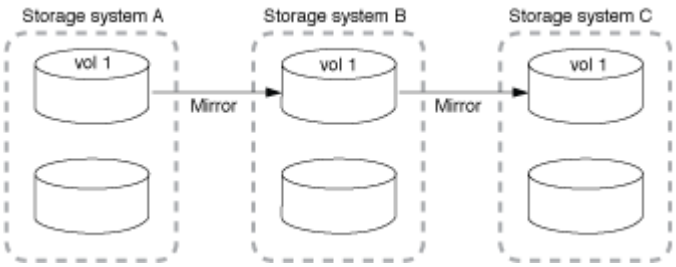
的任何中間磁碟區上啟用了長期保留快照，請聯絡技術支援並參考以下資訊： "NetApp知識庫：不支援級聯啟用長期保留 (LTR) 快照的捲" 尋求幫助。

以下ONTAP版本不允許您在級聯中的任何磁碟區上啟用長期保留快照，但最終的SnapMirror目標磁碟區除外。

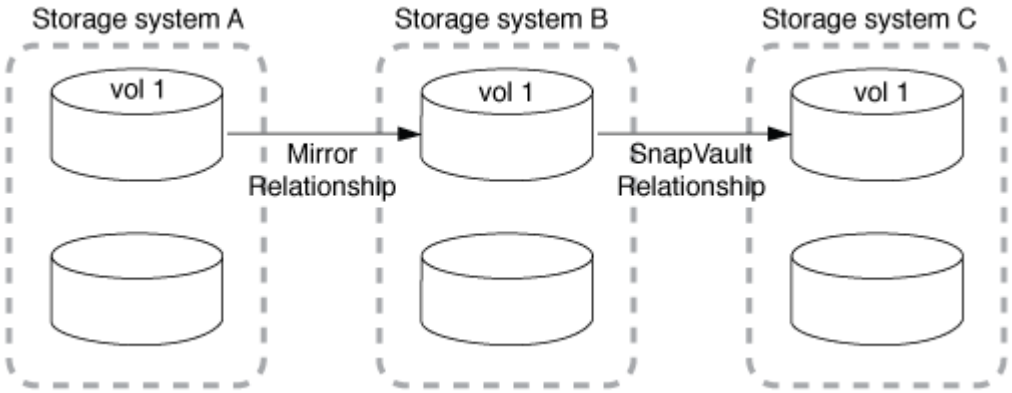
- 9.15.1 及更高版本
- 9.14.1P2 和 P4 至 P14
- 9.13.1P9至P17
- 9.12.1 P12 至 P19
- 9.11.1P15至P20
- 9.10.1P18至P20
- 9.9.1P20

詳細了解"長期保留快照"。

從 ONTAP 9 6 開始、鏡射鏡射串聯部署支援 SnapMirror 同步關係。只有主要和次要磁碟區可以處於 SnapMirror 同步關係中。二線磁碟區與三線磁碟區之間的關係必須是非同步的。



鏡射儲存庫串聯部署包含一系列關係、其中來源磁碟區會鏡射至次要磁碟區、而次要磁碟區則會保存至第三個磁碟區。



也支援 Vault-鏡像和 Vault-Vault 級聯部署：

- 資料保存鏡射串聯部署包含一系列關係、其中來源磁碟區會以資料儲存至次要磁碟區、而次要磁碟區則會鏡射至第三個磁碟區。
- 保險庫-保險庫級聯部署由一系列關係組成，其中源卷被保險庫到輔助卷，而輔助卷被保險庫到第三卷。

相關資訊

- 使用 SnapMirror 主動式同步、在扇出組態中恢復保護

瞭解 **ONTAP SnapMirror** 授權

從功能介紹9.3開始ONTAP 、授權已簡化、可在ONTAP 各個執行個體之間進行複寫。在版本支援的部分、SnapMirror授權可同時支援資料保存和鏡射關係。ONTAP您可以使用 SnapMirror 授權來支援備份和災難恢復使用案例的 ONTAP 複寫。

在 ONTAP 9.3 版本之前，需要另一個 SnapVault 授權來設定 ONTAP 執行個體之間的 *Vault* 關係，其中 DP 執行個體可以保留更多快照以支援保留時間較長的備份使用案例，而且需要 SnapMirror 授權來設定 ONTAP 執行個體之間的 _mirror _ 關係，每個 ONTAP 執行個體都會保留相同數量的快照（即 _mirror _ 映像），以支援叢集容錯移轉。SnapMirror 和 SnapVault 授權繼續用於 ONTAP 8.x 和 9.x 版本、並受到支援。

雖然 SnapVault 授權持續運作且同時支援 ONTAP 8.x 與 9.x 版本、 SnapMirror 授權可用於取代 SnapVault 授權、並可用於鏡射與資料保險箱組態。

對於非同步複寫、ONTAP 從ONTAP 使用支援功能的支援功能支援功能的支援功能、一開始使用單一統一化複寫引擎來設定延伸資料保護模式（XDP）原則、其中SnapMirror授權可設定為鏡射原則、資料保存原則或鏡射保存原則。來源叢集和目的地叢集都需要SnapMirror授權。如果已安裝SnapMirror授權、則不需要使用此功能。SnapVaultSnapMirror 非同步永久授權包含在安裝在新 AFF 和 FAS 系統上的 ONTAP One 軟體套件中。

資料保護組態限制是由多項因素決定、包括ONTAP 您的版次、硬體平台和安裝的授權。如需詳細資訊、請參閱 "Hardware Universe"。

SnapMirror 同步授權

從 ONTAP 9 開始、支援 SnapMirror 同步關係。您需要下列授權才能建立 SnapMirror 同步關係：

- 來源叢集和目的地叢集都需要 SnapMirror 同步授權。

  SnapMirror 同步授權是的一部分"ONTAP 單一授權套件"。

  如果您的系統是在 2019 年 6 月之前隨 Premium 或 Flash 產品組合一起購買、您可以從 NetApp 支援網站下載 NetApp 主金鑰、以取得所需的 SnapMirror 同步授權： "主要授權金鑰"。

- 來源叢集和目的地叢集都需要SnapMirror授權。

SnapMirror 雲端授權

從 ONTAP 9.8 開始， SnapMirror 雲端授權可將快照從 ONTAP 執行個體非同步複寫至物件儲存端點。複寫目標可以使用內部部署物件存放區、S3和S3相容的公有雲物件儲存服務來設定。SnapMirror 雲端關係可從 ONTAP 系統支援至預先合格的物件儲存目標。

SnapMirror 雲端不提供獨立式授權。每ONTAP 個叢集只需要一份授權。除了 SnapMirror 雲端授權之外、也需要 SnapMirror 非同步授權。

您需要下列授權才能建立 SnapMirror 雲端關係：

- SnapMirror 授權和 SnapMirror 雲端授權、可直接複寫至物件儲存區端點。
- 設定多原則複寫工作流程（例如、磁碟對磁碟對雲端）時、所有 ONTAP 執行個體都需要 SnapMirror 授權、而只有直接複寫到物件儲存端點的來源叢集才需要 SnapMirror 雲端授權。

從 ONTAP 9.9.1 開始"使用 System Manager 進行 SnapMirror 雲端複寫"，您可以。

授權的 SnapMirror 雲端協力廠商應用程式清單已發佈在 NetApp 網站上。

資料保護最佳化授權

資料保護最佳化（ DPO ）授權不再銷售、而且目前平台不支援 DPO ；不過、如果您在支援的平台上安裝 DPO 授權、 NetApp 會持續提供支援、直到該平台的可用性結束為止。

ONTAP One 授權套件不隨附 DPO 、如果系統上安裝了 DPO 授權、您就無法升級至 ONTAP One 授權套件。

如需支援平台的相關資訊、請參閱 "Hardware Universe"。

ONTAP DPO 系統功能增強

從ONTAP 使用支援的支援功能支援的不FlexVol 支援功能9.6開始、安裝DP_Optimized（DPO）授權後、支援的不支援功能數量將會增加。從 ONTAP 9.4 開始，具有 DPO 授權的系統支援 SnapMirror 備份，跨磁碟區背景重複資料刪除，使用快照區塊做為捐助者，以及壓縮。

從功能支援的支援範圍ONTAP 僅為2、FlexVol 500 FlexVol 個支援的二線或資料保護系統上的最大支援數量已增加、可讓您在容錯移轉模式下、將每個節點的支援數量擴充至2、500個、或最多5、000個。FlexVol 磁碟區的增加是透過啟用"DP_Optimized （ DPO ） 授權"的。"SnapMirror授權"來源節點和目的地節點上仍需要。

從版本號9.4開始ONTAP 、DPO系統有下列功能增強功能：

- SnapMirror備份：在DPO系統中、複寫流量的優先順序與用戶端工作負載的優先順序相同。

  SnapMirror備份在DPO系統上預設為停用。

- Volume背景重複資料刪除技術和跨Volume背景重複資料刪除技術：在DPO系統中啟用Volume背景重複資料刪除技術和跨Volume背景重複資料刪除技術。

  您可以執行 `storage aggregate efficiency cross-volume-dedupe start -aggregate` *`aggregate_name`* `-scan-old-data true` 刪除現有資料的命令。最佳實務做法是在非尖峰時間執行命令、以降低對效能的影響。

  如"指令參考資料ONTAP"需詳細 `storage aggregate efficiency cross-volume-dedupe start`資訊，請參閱。

- 使用快照區塊做為捐助者，可增加節省成本：使用中檔案系統無法使用但夾在快照中的資料區塊，會作為磁碟區重複資料刪除的捐助者。

  新資料可以與快照中的資料進行重複資料刪除，也能有效共用快照區塊。增加的捐贈空間可節省更多成本，尤其是當磁碟區有大量快照時。

- 壓縮：預設會在DPO磁碟區上啟用資料壓縮功能。

瞭解 **ONTAP SnapMirror** 命令中的路徑名稱模式比對

您可以在中使用模式比對來指定來源和目的地路徑 `snapmirror` 命令。

`snapmirror` 命令會使用下列格式的完整路徑名稱： `vserver:volume` 。您可以透過不輸入SVM名稱來縮寫路徑名稱。如果您這麼做、就會出現 `snapmirror` 命令會假設使用者的本機 SVM 內容。

假設 SVM 稱為「 'vserver1' 」、而 Volume 稱為「 'vol1' 」、則完整路徑名稱為 `vserver1:vol1`。

您可以在路徑中使用星號（*）做為萬用字元、以選取符合條件的完整路徑名稱。下表提供使用萬用字元選取一系列磁碟區的範例。

*	符合所有路徑。
vs*	將所有 SVM 和 Volume 與以開頭的 SVM 名稱配對 vs。
:*src	將所有 SVM 與包含的磁碟區名稱配對 src 文字。
:vol	將所有 SVM 與以開頭的磁碟區名稱配對 vol。

```
vs1::> snapmirror show -destination-path *:*dest*

Progress
Source              Destination  Mirror        Relationship  Total
Last
Path          Type  Path         State         Status        Progress
Healthy Updated
------------ ---- ------------ ------------- -------------- ----------
------- --------
vs1:sm_src2
              DP   vs2:sm_dest1
                                 Snapmirrored  Idle           -
true    -
```

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

瞭解 ONTAP SnapMirror 關係作業的延伸查詢

您可以使用_extended Queris_同時在許多SnapMirror關係上執行SnapMirror作業。例如、您可能有多個未初始化的SnapMirror關係、您想要使用一個命令進行初始化。

關於這項工作

您可以將延伸查詢套用至下列SnapMirror作業：

- 正在初始化未初始化的關係

- 恢復靜止的關係
- 重新同步中斷的關係
- 正在更新閒置關係
- 中止關係資料傳輸

步驟

1. 在許多關係上執行SnapMirror作業：

   snapmirror command {-state state } *

   下列命令可初始化中的 SnapMirror 關係 `Uninitialized` 州：

   ```
   vs1::> snapmirror initialize {-state Uninitialized} *
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

SnapMirror ONTAP 關係的相容版本

在建立 SnapMirror 資料保護關係之前、來源和目的地磁碟區必須執行相容的 ONTAP 版本。在升級 ONTAP 之前、您應確認目前的 ONTAP 版本與目標 ONTAP 版本相容、以因應 SnapMirror 關係。

統一化複寫關係

對於類型為「'XDP'」的SnapMirror關係、使用內部部署或Cloud Volumes ONTAP 更新版本：

從0版開始ONTAP ：

- ONTAP 9.x.0 版本為純雲端版本、支援 Cloud Volumes ONTAP 系統。發行版本之後的星號（*）表示為純雲端版本。

  ONTAP 9.16.0 是僅限雲端部署規則的例外，因為它提供了以下支援："ASA r2 系統" 。發布版本後的加號（+）表示該版本同時支援ASA r2 和雲端。 ASA r2 系統僅支援與其他ASA r2 系統SnapMirror關係。

- ONTAP 9.x 版本為一般版本、可同時支援內部部署和 Cloud Volumes ONTAP 系統。

  如果"進階容量平衡"在執行 ONTAP 9.16.1 或更新版本的叢集中的磁碟區上啟用，則不支援 SnapMirror 傳輸至執行 ONTAP 9.16.1 之前版本 ONTAP 的叢集。

  互通性是雙向的。

- ONTAP 9.4 及更高版本的互通性*

版本…ONTAP	與這些先前ONTAP 版本的功能互通…																					
	9.18.1	9.17.1	9.16.1.	9.16.0+	9.15.1..	9.15.0*	9.14.1.	9.14.0%*	9.13.1.12.9.12.9.	9.13.0*	9.12.1	9.12.0*	9.11.1.	9.11.0*	9.10.1	9.10.5*	9.9.1	9.9.3.0*	9.8	9.7%	9.6%	9.5.
9.18.1	是	是	是	是	是	否	是	否	是	是	否	否	否	否	否	否	否	否	否	否	否	否
9.17.1	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否	否	否	否	否	否	否
9.16.1.	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否	否	否	否	否
9.16.0+	是	是	是	是	是	否	是	否	是	否	是	否	是	否	是	否	否	否	否	否	否	否
9.15.1..	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否	否
9.15.0*	否	是	是	否	是	是	是	否	是	否	是	否	是	否	是	否	是	否	否	否	否	否
9.14.1.	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否	否
9.14.0%*	否	是	是	否	是	否	是	是	是	否	是	否	是	否	是	否	是	否	否	否	否	否
9.13.1.12.9.12.9.	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否	否
9.13.0*	否	是	是	否	是	否	是	否	是	是	是	否	是	否	是	否	是	否	是	否	否	否
9.12.1	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否	否

9.12.0*	否	否	是	否	是	否	是	否	是	否	是	是	是	否	是	否	是	否	是	是	否	否
9.11.1.	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	否
9.11.0*	否	否	否	否	是	否	是	否	是	否	是	否	是	是	是	否	是	否	是	是	是	否
9.10.1	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.10.5*	否	否	否	否	是	否	是	否	是	否	是	否	是	否	是	是	是	否	是	是	是	是
9.9.1	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.9.3.0*	否	否	否	否	否	否	是	否	是	否	是	否	是	否	是	否	是	是	是	是	是	是
9.8	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是	是	是
9.7%	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是	是	是
9.6%	否	否	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是	是	是
9.5.	否	否	否	否	否	否	否	否	否	否	否	否	否	否	是	是	是	是	是	是	是	是

SnapMirror 同步關係

ONTAP 雲端執行個體不支援 SnapMirror 同步。

版本…ONTAP	與這些先前ONTAP 版本的功能互通…													
	9.18.1	9.17.1	9.16.1.	9.15.1..	9.14.1.	9.13.1.12.9.12.9.	9.12.1	9.11.1.	9.10.1	9.9.1	9.8	9.7%	9.6%	9.5.
9.18.1	是	是	是	是	是	是	是	否	否	否	否	否	否	否
9.17.1	是	是	是	是	是	是	是	否	否	否	否	否	否	否
9.16.1.	是	是	是	是	是	是	是	是	否	否	否	否	否	否
9.15.1..	是	是	是	是	是	是	是	是	是	否	否	否	否	否

9.14.1.	是	是	是	是	是	是	是	是	是	是	是	否	否	否
9.13.1.12.9.12.9.	是	是	是	是	是	是	是	是	是	是	是	是	否	否
9.12.1	是	是	是	是	是	是	是	是	是	是	是	是	否	否
9.11.1.	否	否	是	是	是	是	是	是	是	是	否	否	否	否
9.10.1	否	否	否	是	是	是	是	是	是	是	是	否	否	否
9.9.1	否	否	否	否	是	是	是	是	是	是	是	是	否	否
9.8	否	否	否	否	是	是	是	否	是	是	是	是	是	否
9.7%	否	否	否	否	否	是	是	否	否	是	是	是	是	是
9.6%	否	否	否	否	否	否	否	否	否	否	是	是	是	是
9.5.	否	否	否	否	否	否	否	否	否	否	否	是	是	是

SnapMirror SVM 災難恢復關係

- 此矩陣適用於從ONTAP 9.10.1 開始的 SVM 資料移動遷移功能。
- 您可以使用 SVM DR 來遷移不符合指定限制的 SVM。 "SVM遷移（SVM資料遷移）"。
- 在這兩種情況下，來源叢集和目標叢集之間最多可以有 2 個主要的*較新的* ONTAP版本，但要求目標版本必須與來源ONTAP版本相同或更新。

對於 **SVM** 災難恢復資料和 **SVM** 保護：

SVM 災難恢復僅支援在執行相同版本 ONTAP 的叢集之間進行。* SVM 複寫不支援版本獨立性 * 。

對於 **SVM** 移轉的 **SVM** 災難恢復：

- 從來源上的舊版 ONTAP 到目的地上的相同或更新版本 ONTAP 、都支援單一方向的複寫。
- 目標叢集上的 ONTAP 版本必須不超過兩個更新的主要內部部署版本，或兩個更新的主要雲端版本（從 ONTAP 9.0.0 開始），如下表所示。
  - 長期資料保護使用案例不支援複寫。

發行版本之後的星號（*）表示為純雲端版本。

若要判斷支援、請在左表欄中找到來源版本、然後在頂端列中找到目的地版本（適用於相似版本的 DR/Migration 、適用於較新版本的 Migration ）。

如果您使用的是ONTAP 9.10.1 或更高版本，則可以使用 "SVM資料移動性" 使用特性而不是 SVM DR 將 SVM 從一個叢集遷移到另一個叢集。

來源	目的地

	9.5.	9.6%	9.7%	9.8	9.9.3.0*	9.9.1	9.10.5*	9.10.1	9.11.0*	9.11.1.	9.12.0*	9.12.1	9.13.0*	9.13.1.12.9.12.9.	9.14.0%*	9.14.1.	9.15.0*	9.15.1..	9.16.0	9.16.1.	9.17.1	9.18.1
9.5.	災難恢復/移轉	移轉	移轉																			
9.6%		災難恢復/移轉	移轉	移轉																		
9.7%			災難恢復/移轉	移轉	移轉																	
9.8				災難恢復/移轉	移轉	移轉		移轉														
9.9.3.0*					災難恢復/移轉	移轉	移轉	移轉	移轉	移轉												
9.9.1						災難恢復/移轉	移轉	移轉	移轉	移轉												
9.10.5*							災難恢復/移轉	移轉	移轉	移轉	移轉	移轉										

9.10.1								災難恢復/移轉	移轉	移轉	移轉	移轉								
9.11.0*									災難恢復/移轉	移轉	移轉	移轉	移轉	移轉						
9.11.1.										災難恢復/移轉	移轉	移轉	移轉	移轉						
9.12.0*											災難恢復/移轉	移轉	移轉	移轉	移轉	移轉				
9.12.1												災難恢復/移轉	移轉	移轉	移轉	移轉				
9.13.0*													災難恢復/移轉	移轉	移轉	移轉	移轉	移轉		
9.13.1.12.9.12.9.														災難恢復/移轉	移轉	移轉	移轉	移轉		
9.14.0%*															災難恢復/移轉	移轉	移轉	移轉	移轉	移轉

9.14.1.																災難恢復/移轉	移轉	移轉	移轉		
9.15.0*																	災難恢復/移轉	移轉	移轉	移轉	
9.15.1..																		災難恢復/移轉	移轉	移轉	
9.16.0																			災難恢復/移轉	移轉	移轉	移轉
9.16.1.																				災難恢復/移轉	移轉	移轉
9.17.1																					災難恢復/移轉	移轉
9.18.1																						災難恢復/移轉

SnapMirror 災難恢復關係

對於類型為「DP」和原則類型「as同步 鏡射」的SnapMirror關係：

DP型鏡像無法從ONTAP 版本資訊的版本資訊中進行初始化、ONTAP 且在版本資訊的版本資訊中完全不支援。如需詳細資訊、請參閱 "取代資料保護SnapMirror關係"。

在下表中、左欄顯示ONTAP 來源Volume上的版本資訊、而上方列則顯示ONTAP 您在目的地Volume上可以使用的版本資訊。

來源	目的地								
	9.11.1.	9.10.1	9.9.1	9.8	9.7%	9.6%	9.5.	9.4.	9.3.
9.11.1.	是的	否	否	否	否	否	否	否	否
9.10.1	是的	是的	否	否	否	否	否	否	否
9.9.1	是的	是的	是的	否	否	否	否	否	否
9.8	否	是的	是的	是的	否	否	否	否	否
9.7%	否	否	是的	是的	是的	否	否	否	否
9.6%	否	否	否	是的	是的	是的	否	否	否
9.5.	否	否	否	否	是的	是的	是的	否	否
9.4.	否	否	否	否	否	是的	是的	是的	否
9.3.	否	否	否	否	否	否	是的	是的	是的

互通性並非雙向的。

瞭解 **ONTAP SnapMirror** 限制

在建立資料保護關係之前、您應該先瞭解SnapMirror的基本限制。

- 目的地Volume只能有一個來源Volume。

  來源Volume可以有多個目的地Volume。目的地Volume可以是任何類型SnapMirror複寫關係的來源Volume。

- 視陣列機型而定、您最多可以從單一來源磁碟區中排出八或十六個目的地磁碟區。請參閱 "Hardware Universe" 以瞭解特定組態的詳細資料。
- 您無法將檔案還原至SnapMirror DR關係的目的地。
- 來源SnapVault 或目的地的資料不可以是32位元。
- 來源磁碟區SnapVault 不應是FlexClone磁碟區。

  這種關係可以運作、但FlexClone Volume所提供的效率將無法保留。

設定 SnapMirror Volume 複寫

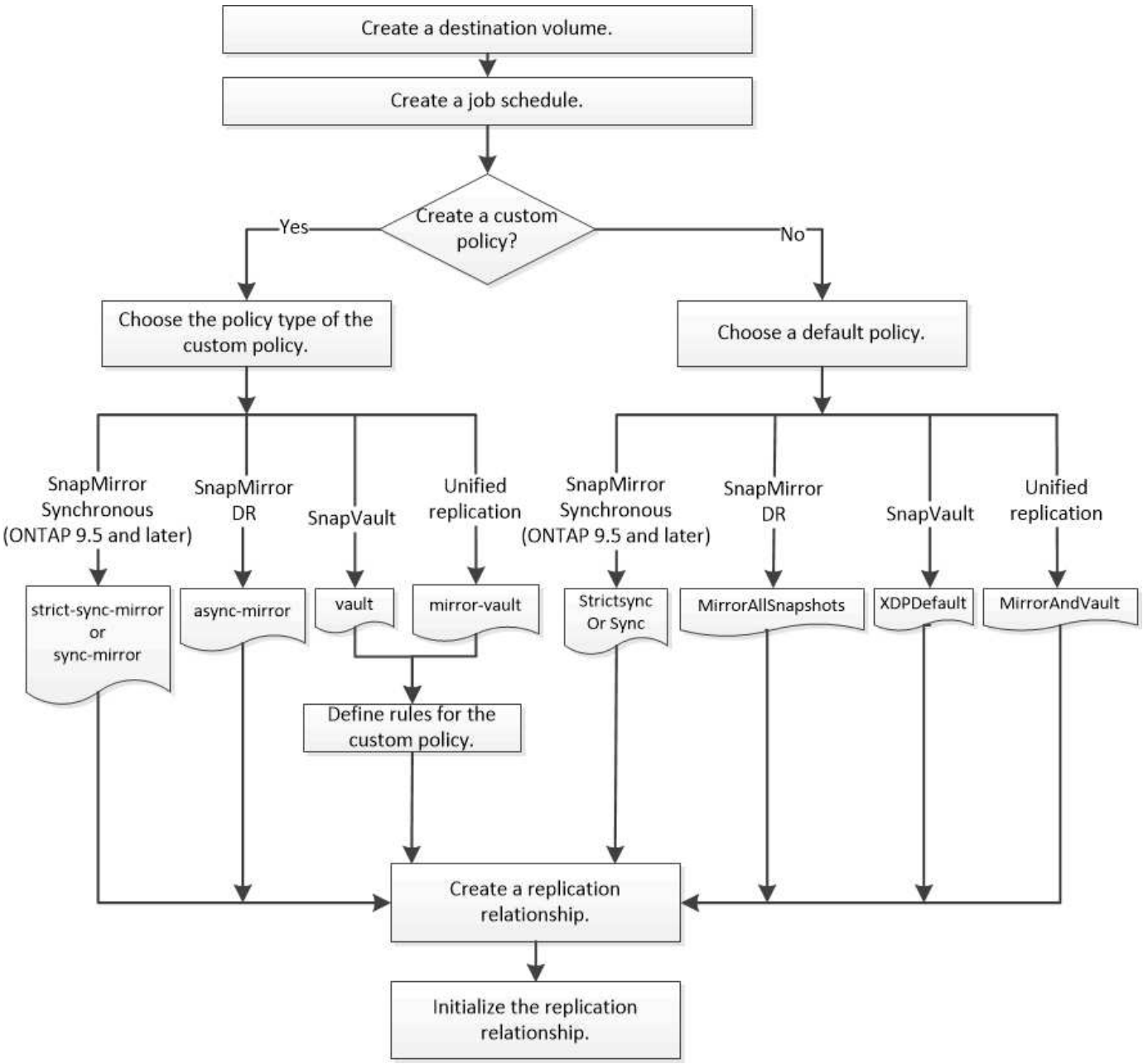
ONTAP SnapMirror 複寫工作流程

SnapMirror提供三種資料保護關係：SnapMirror DR、歸檔（先前稱為SnapVault 「支援」）和統一化複寫。您可以遵循相同的基本工作流程來設定每種類型的關係。

從 ONTAP 9.9.1 的一般可用度開始、 "SnapMirror 主動同步" 提供零恢復時間目標（零 RTO ）或透明應用程式容錯移轉（ TAF ）、可在 SAN 環境中自動容錯移轉業務關鍵應用程式。

對於每種類型的SnapMirror資料保護關係、工作流程都相同：建立目的地Volume、建立工作排程、指定原則、建立及初始化關係。

從功能介紹9.3開始ONTAP 、您可以使用 `snapmirror protect` 命令可在單一步驟中設定資料保護關係。即使您使用 `snapmirror protect`、您必須瞭解工作流程中的每個步驟。



相關資訊

- "SnapMirror保護"

在一個步驟中設定 **ONTAP SnapMirror** 複寫關係

從ONTAP 9.3 開始，您可以使用 `snapmirror protect`命令透過一個步驟配置資料保護關

係。您指定要複製的磁碟區清單、目標叢集上的 SVM、作業計劃和SnapMirror策略。`snapmirror protect`完成剩下的工作。

開始之前

- 來源與目的地叢集和SVM必須進行對等關係。

  "叢集與SVM對等關係"

- 目的地Volume上的語言必須與來源Volume上的語言相同。

關於這項工作

。 `snapmirror protect` 命令會選擇與指定 SVM 相關聯的集合體。如果SVM沒有相關聯的Aggregate、則會從叢集中的所有Aggregate中進行選擇。集合體的選擇取決於可用空間量和集合體上的磁碟區數量。

。 `snapmirror protect` 然後命令會執行下列步驟：

- 為要複寫之磁碟區清單中的每個磁碟區建立具有適當類型和保留空間量的目的地磁碟區。
- 設定適合您所指定原則的複寫關係。
- 初始化關係。

目的地 Volume 的名稱為格式 *source_volume_name_dst*。如果與現有名稱發生衝突、命令會在磁碟區名稱加上一個數字。您可以在命令選項中指定字首和/或字尾。後置字元會取代系統提供的 `dst` 後置字元。

在ONTAP 9.4 及更高版本中，目標磁碟區最多可包含 1019 個快照。在ONTAP 9.3 及更早版本中，目標磁碟區最多可包含 251 個快照。

初始化可能會很耗時。 `snapmirror protect` 不需要等到初始化完成後再完成工作。因此、您應該使用 `snapmirror show` 命令、而非 `job show` 判斷初始化何時完成的命令。

從 ONTAP 9 5 開始、可以使用 `snapmirror protect`命令建立 SnapMirror 同步關係。

詳細了解 `snapmirror protect`在"指令參考資料ONTAP" 。

步驟

1. 只需一個步驟即可建立及初始化複寫關係：

   執行此命令之前、您必須以必要的值取代尖括號中的變數。

   ```
   snapmirror protect -path-list <SVM:volume> -destination-vserver
   <destination_SVM> -policy <policy> -schedule <schedule> -auto-initialize
   <true|false> -destination-volume-prefix <prefix> -destination-volume
   -suffix <suffix>
   ```

   您必須從目的地SVM或目的地叢集執行此命令。。 `-auto-initialize` 選項預設為「 'true' 」。

   以下範例使用預設值建立及初始化 SnapMirror DR 關係 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAllSnapshots -schedule
replication_daily
```

您可以視需要使用自訂原則。如需詳細資訊、請參閱 "建立自訂複寫原則"。

下列範例使用預設值建立及初始化 SnapVault 關係 `XDPDefault` 原則：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy XDPDefault -schedule
replication_daily
```

下列範例使用預設值建立及初始化統一化複寫關係 `MirrorAndVault` 原則：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_backup -policy MirrorAndVault
```

以下範例使用預設 `Sync`原則建立及初始化 SnapMirror 同步關係：

```
cluster_dst::> snapmirror protect -path-list svm1:volA, svm1:volB
-destination-vserver svm_sync -policy Sync
```

對於 SnapVault 和統一化複寫原則，您可能會發現定義排程來建立目的地上最後傳輸的快照複本很有用。如需更多資訊、請參閱 "定義在目的地上建立本機複本的排程"。

完成後

使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

相關資訊

- "工作展示"

一次設定一個複寫關係步驟

建立 **ONTAP SnapMirror** 目的地 **Volume**

您可以在目的地上使用 `volume create`命令來建立目的地 Volume 。目的地Volume的大小應與來源Volume相同或更大。如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。

步驟

1. 建立目的地Volume：

   `volume create -vserver SVM -volume volume -aggregate aggregate -type DP -size size`

   以下範例建立一個名為的 2-GB 目的地磁碟區 `volA_dst`：

   ```
   cluster_dst::> volume create -vserver SVM_backup -volume volA_dst
   -aggregate node01_aggr -type DP -size 2GB
   ```

建立 **ONTAP SnapMirror** 複寫工作排程

工作排程會決定SnapMirror何時自動更新排程指派的資料保護關係。您可以使用 System Manager 或 `job schedule cron create`命令來建立複寫工作排程。如"指令參考資料ONTAP"需詳細 `job schedule cron create`資訊，請參閱。

關於這項工作

您可以在建立資料保護關係時指派工作排程。如果您未指派工作排程、則必須手動更新關係。

步驟

您可以使用系統管理員或 ONTAP CLI 建立複寫工作排程。

系統管理員

1. 瀏覽至 * 保護 > 概述 * 、然後展開 * 本機原則設定 * 。
2. 在 * 排程 * 窗格中、按一下 →。
3. 在 **Scheduls** 窗口中，單擊 + Add 。
4. 在 * 新增排程 * 視窗中、輸入排程名稱、然後選擇內容和排程類型。
5. 按一下「 * 儲存 * 」。

CLI

1. 建立工作排程：

```
job schedule cron create -name <job_name> -month <month> -dayofweek
<day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
```

適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

從功能性的9.10.1開始ONTAP 、您可以在工作排程中加入Vserver：

```
job schedule cron create -name <job_name> -vserver <Vserver_name>
-month <month> -dayofweek <day_of_week> -day <day_of_month> -hour
<hour> -minute <minute>
```

ⓘ Volume SnapMirror 關係中 FlexVol Volume 的最低支援排程（ RPO ）為 5 分鐘。Volume SnapMirror 關係中 FlexGroup Volume 的最低支援排程（ RPO ）為 30 分鐘。

以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

自訂 **SnapMirror** 複寫原則

建立自訂 **ONTAP SnapMirror** 複寫原則

如果關聯的預設原則不適用、您可以建立自訂複寫原則。例如，您可能想要壓縮網路傳輸中的資料，或是修改 SnapMirror 嘗試傳輸快照的次數。

您可以在建立複寫關聯時使用預設或自訂原則。對於自訂歸檔（前身為 SnapVault ）或統一化複寫原則，您必須定義一或多個 _rules ，以決定在初始化和更新期間傳輸哪些快照。您可能也想要定義在目的地上建立本機快照的排程。

複寫原則的_policy類型_決定其支援的關係類型。下表顯示可用的原則類型。

原則類型	關係類型
非同步鏡射	SnapMirror災難恢復
保存庫	SnapVault
鏡射保存庫	統一化複寫
嚴格同步鏡射	StrictSync 模式中的 SnapMirror 同步（從 ONTAP 9 開始支援）
同步鏡射	同步模式中的 SnapMirror 同步（從 ONTAP 9 開始支援）。 5

建立自訂複寫原則時、最好先建立預設原則之後的原則模型。

步驟

您可以使用系統管理員或 ONTAP CLI 建立自訂資料保護原則。從 ONTAP 9.11.1 開始、您可以使用系統管理員來建立自訂鏡射和資料保險箱原則、以及顯示和選取舊版原則。此功能也可在ONTAP 《》ONTAP 的更新版修補程式《》中找到。

在來源與目的地叢集上建立自訂保護原則。

系統管理員

1. 按一下「保護>總覽>本機原則設定」。
2. 在 * 保護原則 * 下、按一下 →。
3. 在 * 保護原則 * 窗格中，按一下 + Add 。
4. 輸入新原則名稱、然後選取原則範圍。
5. 選擇原則類型。若要新增僅儲存庫或純鏡射原則、請選擇*非同步*、然後按一下*使用舊版原則類型*。
6. 填寫必填欄位。
7. 按一下「 * 儲存 * 」。
8. 在另一個叢集上重複這些步驟。

CLI

1. 建立自訂複寫原則：

```
snapmirror policy create -vserver <SVM> -policy _policy_ -type
<async-mirror|vault|mirror-vault|strict-sync-mirror|sync-mirror>
-comment <comment> -tries <transfer_tries> -transfer-priority
<low|normal> -is-network-compression-enabled <true|false>
```

從 ONTAP 9.5 開始，您可以使用參數來指定建立 SnapMirror 同步關係通用快照排程的排程 `-common-snapshot-schedule`。根據預設， SnapMirror 同步關係的一般快照排程為一小時。您可以為 SnapMirror 同步關係的快照排程指定 30 分鐘到 2 小時的值。

以下範例為SnapMirror DR建立自訂複寫原則、以啟用資料傳輸的網路壓縮：

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
DR_compressed -type async-mirror -comment "DR with network
compression enabled" -is-network-compression-enabled true
```

下列範例建立SnapVault 一套適用於整個流程的自訂複寫原則：

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_snapvault -type vault
```

下列範例建立統一化複寫的自訂複寫原則：

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_unified -type mirror-vault
```

下列範例會在 StrictSync 模式中建立 SnapMirror 同步關係的自訂複寫原則：

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
my_strictsync -type strict-sync-mirror -common-snapshot-schedule
my_sync_schedule
```

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

完成後

對於「資料保險箱」和「鏡射資料保險箱」原則類型，您必須定義規則，以決定在初始化和更新期間傳輸哪些快照。

使用 `snapmirror policy show`命令驗證SnapMirror策略是否已建立。

詳細了解 `snapmirror policy show`在"指令參考資料ONTAP" 。

定義 **ONTAP SnapMirror** 原則的規則

對於具有或 `mirror-vault`原則類型的自訂原則 `vault`，您必須定義至少一個規則，以決定在初始化和更新期間傳輸哪些快照。您也可以使用或 `mirror-vault`原則類型來定義預設原則的規則 `vault`。

關於這項工作

每個具有或 `mirror-vault`原則類型的原則都 `vault`必須有一個規則，指定要複寫哪些快照。例如，規則 `bi-monthly`表示只應複寫指派 `SnapMirror` 標籤的快照 `bi-monthly`。您可以在來源上設定快照原則時指定 SnapMirror 標籤。

每種原則類型都與一或多個系統定義的規則相關聯。當您指定原則類型時、這些規則會自動指派給該原則。下表顯示系統定義的規則。

系統定義的規則	用於原則類型	結果
SM_已 建立	非同步鏡射、鏡射-保存庫、同步、StrictSync	由 SnapMirror 建立的快照會在初始化與更新時傳輸。
all_source_snapshots	非同步鏡射	來源上的新快照會在初始化和更新時傳輸。
每日	保存庫、鏡射保存庫	在初始化和更新時，會傳輸來源上具有 SnapMirror 標籤的新快照 `daily`。
每週	保存庫、鏡射保存庫	在初始化和更新時，會傳輸來源上具有 SnapMirror 標籤的新快照 `weekly`。

每月	鏡射保存庫	在初始化和更新時，會傳輸來源上具有 SnapMirror 標籤的新快照 `monthly`。
應用程式一致	同步、StrictSync	來源上有 SnapMirror 標籤的快照 `app_consistent`會同步複寫到目的地。從 ONTAP 9.7 開始支援。

除了「as同步 鏡射」原則類型之外、您可以視需要為預設或自訂原則指定其他規則。例如：

- 對於預設 `MirrorAndVault`原則，您可以建立一個規則，稱為 `bi-monthly`將來源上的快照與 SnapMirror 標籤配對 `bi-monthly`。
- 對於原則類型的自訂原則 `mirror-vault`，您可以建立一個規則，稱為 `bi-weekly`將來源上的快照與 SnapMirror 標籤配對 `bi-weekly`。

步驟

1. 定義原則規則：

   `snapmirror policy add-rule -vserver` *SVM* `-policy` *policy_for_rule* `-snapmirror -label` *snapmirror-label* `-keep` *retention_count*

   以下範例新增了帶有 SnapMirror 標籤的規則 `bi-monthly` 至預設值 `MirrorAndVault` 原則：

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label bi-monthly -keep 6
   ```

   以下範例新增了帶有 SnapMirror 標籤的規則 `bi-weekly` 自訂 `my_snapvault` 原則：

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_snapvault -snapmirror-label bi-weekly -keep 26
   ```

   以下範例新增了帶有 SnapMirror 標籤的規則 `app_consistent` 自訂 `Sync` 原則：

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy Sync
   -snapmirror-label app_consistent -keep 1
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror policy add-rule`資訊，請參閱。

   接著您可以從符合此 SnapMirror 標籤的來源叢集複寫快照：

   ```
   cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot
   snapshot1 -snapmirror-label app_consistent
   ```

定義 ONTAP SnapMirror 排程以在目的地上建立本機複本

對於 SnapVault 和統一複寫關係，您可以在目的地上建立上次傳輸快照的複本，以防止更新快照毀損。無論來源上的保留規則為何，此「本機複本」都會保留，因此即使來源上不再提供 SnapMirror 原本傳輸的快照，目的地上也會提供該快照的複本。

關於這項工作

您可以在 `-schedule`選項 `snapmirror policy add-rule`命令。

步驟

1. 定義在目的地上建立本機複本的排程：

   ```
   snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror
   -label snapmirror-label -schedule schedule
   ```

   如需如何建立工作排程的範例，請參閱"建立複寫工作排程"。

   下列範例將建立本機複本的排程新增至預設值 `MirrorAndVault` 原則：

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   MirrorAndVault -snapmirror-label my_monthly -schedule my_monthly
   ```

   下列範例新增了建立自訂本機複本的排程 `my_unified` 原則：

   ```
   cluster_dst::> snapmirror policy add-rule -vserver svm1 -policy
   my_unified -snapmirror-label my_monthly -schedule my_monthly
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror policy add-rule`資訊，請參閱。

建立 ONTAP SnapMirror 複寫關係

主要儲存設備中的來源磁碟區與次要儲存設備中的目的地磁碟區之間的關係稱為 _ 資料保護關係。 _ 您可以使用 `snapmirror create`命令來建立 SnapMirror DR ， SnapVault 或統一化複寫資料保護關係。

> ⓘ 此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"建立複製關係。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

從ONTAP 功能完善的9.11.1開始、您可以使用System Manager來選取預先建立和自訂的鏡像和資料保存原則、顯示和選取舊有原則、以及在保護磁碟區和儲存VM時、覆寫保護原則中定義的傳輸排程。此功能也可在ONTAP 《》ONTAP 的更新版修補程式《》中找到。

如果您使用ONTAP 的是更新ONTAP 版本的更新版本的更新版本的更新版本的更新版本、且您使用System Manager設定SnapMirror、則如果ONTAP 您打算升級至版本的更新版本的更新版本、則應使用更新版本的更新版本的更新版本。9.9.1P13或更新版本的ONTAP 更新版本以及更新版本的更新版本的更新版本ONTAP ONTAP 。

開始之前

- 來源與目的地叢集和SVM必須進行對等關係。

  "叢集與SVM對等關係"

- 目的地Volume上的語言必須與來源Volume上的語言相同。

關於這項工作

直到使用SnapMirror 9.3之前ONTAP 、在DP模式中叫用SnapMirror、而在XDP模式中叫用SnapMirror、使用不同的複寫引擎、並採用不同的版本相依方法：

- 在DP模式中叫用的SnapMirror使用_版本相依_複寫引擎、ONTAP 而在其中、必須在主要和次要儲存設備上使用相同的版本：

```
cluster_dst::>  snapmirror create -type DP -source-path ... -destination
-path ...
```

- 在XDP模式中叫用的SnapMirror使用_版本彈性_複寫引擎、可在ONTAP 一線和二線儲存設備上支援不同的版本：

```
cluster_dst::>  snapmirror create -type XDP -source-path ...
-destination-path ...
```

隨著效能提升、版本靈活的SnapMirror的顯著效益、超過了以版本相依模式取得的複寫處理量的小優勢。因此、從ONTAP 功能更新9.3開始、XDP模式已成為新的預設值、而在命令列或新的或現有指令碼中、DP模式的任何調用、都會自動轉換為XDP模式。

現有的關係不受影響。如果某個關係已經是DP類型、則會繼續是DP類型。下表顯示您可以預期的行為。

如果您指定...	類型為...	預設原則（如果您未指定原則）是...
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
什麼都沒有	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	XDPDefault（SnapVault 晚餐）

另請參閱下列程序中的範例。

轉換的唯一例外情況如下：

- SVM資料保護關係仍預設為DP模式。

  明確指定 XDP 以取得預設的 XDP 模式 `MirrorAllSnapshots` 原則。

- 負載共用資料保護關係仍預設為DP模式。
- 將資料保護關係預設為DP模式。SnapLock
- 如果您設定下列全叢集選項、DP的明確調用仍會繼續預設為DP模式：

  ```
  options replication.create_data_protection_rels.enable on
  ```

  如果您未明確叫用DP、則會忽略此選項。

從 ONTAP 9.14.1 開始 `-backoff-level` 、選項會新增至 `snapmirror create`、和命令、 `snapmirror modify` `snapmirror restore` 讓您可以指定每個關係的回溯層級。只有 FlexVol SnapMirror 關係才支援此選項。選用命令會指定因用戶端作業而導致的 SnapMirror 備份層級。退貨值可以是高、中或無。預設值為高。

從 ONTAP 9 開始、支援 SnapMirror 同步關係。

在ONTAP 9.4 及更高版本中，目標磁碟區最多可包含 1019 個快照。在ONTAP 9.3 及更早版本中，目標磁碟區最多可包含 251 個快照。

步驟

您可以使用系統管理員或 ONTAP CLI 來建立複寫關係。

系統管理員

1. 選取要保護的磁碟區或LUN：按一下「儲存設備>磁碟區」或「儲存設備> LUN」、然後按一下所需的磁碟區或LUN名稱。
2. 單擊。 Protect
3. 選取目的地叢集和儲存VM。
4. 預設會選取非同步原則。若要選取同步原則、請按一下*更多選項*。
5. 按一下*保護*。
6. 按一下所選磁碟區或LUN的* SnapMirror（本機或遠端）*索引標籤、確認保護設定正確。

CLI

1. 從目的地叢集建立複寫關係：

   執行此命令之前、您必須以必要的值取代尖括號中的變數。

   ```
   snapmirror create -source-path <SVM:volume> -destination-path
   <SVM:volume> -type <DP|XDP> -schedule <schedule> -policy <policy>
   ```

   此 `schedule`參數不適用於建立 SnapMirror 同步關係。

   以下範例使用預設值建立 SnapMirror DR 關係 `MirrorLatest` 原則：

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorLatest
   ```

   下列範例使用預設值建立 SnapVault 關係 `XDPDefault` 原則：

   ```
   cluster_dst::> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   XDPDefault
   ```

   下列範例使用預設值建立統一化的複寫關係 `MirrorAndVault` 原則：

   ```
   cluster_dst:> snapmirror create -source-path svm1:volA -destination
   -path svm_backup:volA_dst -type XDP -schedule my_daily -policy
   MirrorAndVault
   ```

   下列範例使用自訂建立統一複寫關係 `my_unified` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily -policy
my_unified
```

下列範例使用預設 `Sync`原則建立 SnapMirror 同步關係：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy Sync
```

下列範例使用預設 `StrictSync`原則建立 SnapMirror 同步關係：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy StrictSync
```

以下範例建立SnapMirror DR關係。在 DP 類型自動轉換為 XDP 且未指定原則的情況下、原則預設為 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type DP -schedule my_daily
```

以下範例建立SnapMirror DR關係。如果未指定任何類型或原則、則原則預設為 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -schedule my_daily
```

以下範例建立SnapMirror DR關係。未指定原則時、原則預設為 `XDPDefault` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -schedule my_daily
```

以下示例使用預定義的策略創建 SnapMirror 同步關係 `SnapCenterSync`：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst -type XDP -policy SnapCenterSync
```

預先定義的原則 `SnapCenterSync`**類型為** `Sync`。此原則會複寫以「 app_sisticent 」建立的任何快照 `snapmirror-label`。

完成後

使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

相關資訊

- "建立並刪除 SnapMirror 容錯移轉測試磁碟區"。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作...	請參閱此內容...
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"Volume備份：SnapVault 使用功能概述"

相關資訊

- "SnapMirror建立"

初始化 **ONTAP SnapMirror** 複寫關係

對於所有關係類型，初始化會執行 *baseline transfer* ：它會建立來源 Volume 的快照，然後將該複本及其參照的所有資料區塊傳輸至目的地 Volume 。否則、傳輸內容取決於原則。

開始之前

來源與目的地叢集和SVM必須進行對等關係。

"叢集與SVM對等關係"

關於這項工作

初始化可能會很耗時。您可能想要在非尖峰時間執行基準傳輸。

從 ONTAP 9 開始、支援 SnapMirror 同步關係。

您應該知道，如果檔案系統因任何原因重新啟動，例如節點重新啟動、接管/恢復或崩潰，則初始化將不會自動恢復，必須手動重新啟動。

步驟

1. 初始化複寫關係：

```
snapmirror initialize -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

您必須從目的地SVM或目的地叢集執行此命令。

以下範例初始化來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup` ：

```
cluster_dst::> snapmirror initialize -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

確保 **ONTAP** 鏡射資料保險箱部署中有通用的快照

您可以使用 `snapmirror snapshot-owner create`命令用於在鏡像-保險庫部署中的輔助伺服器上保留標籤的快照。這樣做可以確保存在用於更新保險庫關係的通用快照。

關於這項工作

如果您使用鏡射資料保險箱的扇出或串聯部署組合，請記住，如果來源和目的地磁碟區上不存在一般快照，更新將會失敗。

這絕不是鏡射資料保險箱扇出或串聯部署中的鏡射關係問題，因為 SnapMirror 在執行更新之前，一律會先建立來源磁碟區的快照。

不過，這可能是資料保險箱關係的問題，因為 SnapMirror 在更新資料保險箱關係時，不會建立來源 Volume 的快照。您需要使用 `snapmirror snapshot-owner create`來確保在資料保險箱關係的來源和目的地上至少有一個通用快照。"深入瞭解資料保護扇出部署和串聯部署"。

步驟

1. 在來源磁碟區上，將擁有者指派給您要保留的標記快照：

   ```
   snapmirror snapshot-owner create -vserver <SVM> -volume <volume> -snapshot
   <snapshot> -owner <owner>
   ```

   以下範例指派 `ApplicationA`為快照的擁有者 `snap1`：

   ```
   clust1::> snapmirror snapshot-owner create -vserver vs1 -volume vol1
   -snapshot snap1 -owner ApplicationA
   ```

   詳細了解 `snapmirror snapshot-owner create`在"指令參考資料ONTAP" 。

2. 如所述、更新鏡射關係 "手動更新複寫關係"。

   或者、您也可以等待鏡射關係的排程更新。

3. 將標示好的快照傳輸至資料保險箱目的地：

   ```
   snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
   snapshot
   ```

   以下範例傳輸 **`snap1`**快照

```
clust1::> snapmirror update -vserver vs1 -volume vol1
-source-snapshot snap1
```

當資料保險箱關係更新時，會保留標示的快照。

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

4. 在來源磁碟區上，將擁有者從標有的快照中移除：

   `snapmirror snapshot-owner delete -vserver` *SVM* `-volume` *volume* `-snapshot` *snapshot* `-owner` *owner*

   下列範例會移除 `ApplicationA`為快照擁有者 `snap1`：

```
clust1::> snapmirror snapshot-owner delete -vserver vs1 -volume vol1
-snapshot snap1 -owner ApplicationA
```

   如"指令參考資料ONTAP"需詳細 `snapmirror snapshot-owner delete`資訊，請參閱。

範例：設定 **ONTAP SnapMirror** 資料保險箱 **-** 資料保險箱串聯

範例將具體說明如何一次設定一個步驟的複寫關係。您可以使用範例中設定的資料保險箱串聯部署來保留超過 251 個標示為的快照 `my-weekly`。

開始之前

來源與目的地叢集和SVM必須進行對等關係。

關於這項工作

範例假設如下：

- 您已在來源叢集上使用 SnapMirror 標籤， `my-weekly`和 `my-monthly`設定快照 `my-daily`。
- 您已設定在第二和第三目的地叢集上命名的目的地磁碟區 `volA`。
- 您已設定在第二和第三目的地叢集上命名的複寫工作排程 `my_snapvault`。

範例顯示如何根據兩個自訂原則建立複寫關係：

- 此 `snapvault_secondary`原則會在次要目的地叢集上保留 7 個每日， 52 個每週和 180 個每月快照。
- 會 `snapvault_tertiary policy`在第三個目的地叢集上保留 250 個每週快照。

步驟

1. 在次要目的地叢集上，建立 `snapvault_secondary`原則：

```
cluster_secondary::> snapmirror policy create -policy snapvault_secondary
-type vault -comment "Policy on secondary for vault to vault cascade" -vserver
svm_secondary
```

2. 在次要目的地叢集上，定義 `my-daily`原則的規則：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-daily -keep 7 -vserver svm_secondary
```

3. 在次要目的地叢集上，定義 `my-weekly`原則的規則：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-weekly -keep 52 -vserver svm_secondary
```

4. 在次要目的地叢集上，定義 `my-monthly`原則的規則：

```
cluster_secondary::> snapmirror policy add-rule -policy snapvault_secondary
-snapmirror-label my-monthly -keep 180 -vserver svm_secondary
```

5. 在次要目的地叢集上、驗證原則：

```
cluster_secondary::> snapmirror policy show snapvault_secondary -instance
```

```
                    Vserver: svm_secondary
      SnapMirror Policy Name: snapvault_secondary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on secondary for vault to vault
cascade
       Total Number of Rules: 3
                  Total Keep: 239
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-daily                7  false       0 -
-
                              my-weekly              52  false       0 -
-
                              my-monthly            180  false       0 -
-
```

6. 在次要目的地叢集上、建立與來源叢集的關係：

```
cluster_secondary::> snapmirror create -source-path svm_primary:volA
-destination-path svm_secondary:volA -type XDP -schedule my_snapvault -policy
```

```
snapvault_secondary
```

7. 在次要目的地叢集上、初始化與來源叢集的關係：

```
cluster_secondary::> snapmirror initialize -source-path svm_primary:volA
-destination-path svm_secondary:volA
```

8. 在第三個目的地叢集上，建立 `snapvault_tertiary`原則：

```
cluster_tertiary::> snapmirror policy create -policy snapvault_tertiary -type
vault -comment "Policy on tertiary for vault to vault cascade" -vserver
svm_tertiary
```

9. 在第三個目的地叢集上，定義 `my-weekly`原則的規則：

```
cluster_tertiary::> snapmirror policy add-rule -policy snapvault_tertiary
-snapmirror-label my-weekly -keep 250 -vserver svm_tertiary
```

10. 在第三目的地叢集上、確認原則：

```
cluster_tertiary::> snapmirror policy show snapvault_tertiary -instance
```

```
                    Vserver: svm_tertiary
      SnapMirror Policy Name: snapvault_tertiary
      SnapMirror Policy Type: vault
                Policy Owner: cluster-admin
                 Tries Limit: 8
           Transfer Priority: normal
   Ignore accesstime Enabled: false
     Transfer Restartability: always
 Network Compression Enabled: false
             Create Snapshot: false
                     Comment: Policy on tertiary for vault to vault
cascade
       Total Number of Rules: 1
                  Total Keep: 250
                       Rules: SnapMirror Label     Keep  Preserve Warn
Schedule Prefix
                              ----------------     ----  -------- ----
-------- ------
                              my-weekly             250  false       0 -
-
```

11. 在第三個目的地叢集上、建立與第二個叢集的關係：

```
cluster_tertiary::> snapmirror create -source-path svm_secondary:volA
-destination-path svm_tertiary:volA -type XDP -schedule my_snapvault -policy
snapvault_tertiary
```

12. 在第三個目的地叢集上、初始化與第二個叢集的關係：

```
cluster_tertiary::> snapmirror initialize -source-path svm_secondary:volA
-destination-path svm_tertiary:volA
```

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略新增規則"
- "SnapMirror 策略創建"
- "SnapMirror 策略顯示"

管理SnapMirror Volume複寫

將現有的 ONTAP SnapMirror DP 類型關係轉換為 XDP

如果您要升級ONTAP 至更新版本的版本、則必須先將DP類型的關係轉換成XDP、然後再升級。不支援DP類型的關係。ONTAP您可以輕鬆地將現有的DP類型關係轉換成XDP、以善用靈活版本的SnapMirror。

在升級ONTAP 至版本更新至版本更新ONTAP 之前、您必須先將現有的DP類型關係轉換成XDP、才能升級至版本更新。

關於這項工作

- SnapMirror不會自動將現有的DP類型關係轉換為XDP。若要轉換關係、您必須中斷並刪除現有的關係、建立新的XDP關係、然後重新同步關係。
- 規劃轉換時、您應該注意、XDP SnapMirror關係的背景準備和資料倉儲階段可能需要很長時間。SnapMirror關係報告長時間處於「準備」狀態、並不罕見。

> 將SnapMirror關係類型從DP轉換為XDP之後、與空間相關的設定（例如自動調整大小和空間保證）將不再複寫到目的地。

步驟

1. 從目的地叢集、確定SnapMirror關係為DP類型、鏡射狀態為Snapmirror、關係狀態為閒置、關係健全：

```
snapmirror show -destination-path <SVM:volume>
```

下列範例顯示的輸出 `snapmirror show` 命令：

```
cluster_dst::>snapmirror show -destination-path svm_backup:volA_dst

Source Path: svm1:volA
Destination Path: svm_backup:volA_dst
Relationship Type: DP
SnapMirror Schedule: -
Tries Limit: -
Throttle (KB/sec): unlimited
Mirror State: Snapmirrored
Relationship Status: Idle
Transfer Snapshot: -
Snapshot Progress: -
Total Progress: -
Snapshot Checkpoint: -
Newest Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Newest Snapshot Timestamp: 06/27 10:00:55
Exported Snapshot: snapmirror.10af643c-32d1-11e3-954b-
123478563412_2147484682.2014-06-27_100026
Exported Snapshot Timestamp: 06/27 10:00:55
Healthy: true
```

您可能會發現保留命令輸出複本有助於 `snapmirror show`追蹤現有的關聯性設定。如"指令參考資料ONTAP"需詳細 `snapmirror show`資訊，請參閱。

2. 從來源和目的地磁碟區，確保兩個磁碟區都有通用的快照：

```
volume snapshot show -vserver <SVM> -volume <volume>
```

下列範例顯示 `volume snapshot show` 來源和目的地磁碟區的輸出：

```
cluster_src:> volume snapshot show -vserver vsm1 -volume volA
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm1 volA
weekly.2014-06-09_0736 valid 76KB 0% 28%
weekly.2014-06-16_1305 valid 80KB 0% 29%
daily.2014-06-26_0842 valid 76KB 0% 28%
hourly.2014-06-26_1205 valid 72KB 0% 27%
hourly.2014-06-26_1305 valid 72KB 0% 27%
hourly.2014-06-26_1405 valid 76KB 0% 28%
hourly.2014-06-26_1505 valid 72KB 0% 27%
hourly.2014-06-26_1605 valid 72KB 0% 27%
daily.2014-06-27_0921 valid 60KB 0% 24%
hourly.2014-06-27_0921 valid 76KB 0% 28%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
valid 44KB 0% 19%
11 entries were displayed.


cluster_dest:> volume snapshot show -vserver svm_backup -volume volA_dst
---Blocks---
Vserver Volume Snapshot State Size Total% Used%
-------- ------- ------------------------------ -------- --------
------ -----
svm_backup volA_dst
weekly.2014-06-09_0736 valid 76KB 0% 30%
weekly.2014-06-16_1305 valid 80KB 0% 31%
daily.2014-06-26_0842 valid 76KB 0% 30%
hourly.2014-06-26_1205 valid 72KB 0% 29%
hourly.2014-06-26_1305 valid 72KB 0% 29%
hourly.2014-06-26_1405 valid 76KB 0% 30%
hourly.2014-06-26_1505 valid 72KB 0% 29%
hourly.2014-06-26_1605 valid 72KB 0% 29%
daily.2014-06-27_0921 valid 60KB 0% 25%
hourly.2014-06-27_0921 valid 76KB 0% 30%
snapmirror.10af643c-32d1-11e3-954b-123478563412_2147484682.2014-06-
27_100026
```

3. 若要確保在轉換期間不會執行排程的更新、請停止現有的DP類型關係：

```
snapmirror quiesce -source-path <SVM:volume> -destination-path
<SVM:volume>
```

您必須從目的地SVM或目的地叢集執行此命令。

以下範例會暫停來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

4. 打破現有的DP類型關係：

```
snapmirror break -destination-path <SVM:volume>
```

您必須從目的地SVM或目的地叢集執行此命令。

以下範例打破來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror break -destination-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

5. 如果在目的地磁碟區上啟用自動刪除快照功能，請停用它：

```
volume snapshot autodelete modify -vserver _SVM_ -volume _volume_
-enabled false
```

以下範例停用目的地磁碟區上的快照自動刪除 `volA_dst`：

```
cluster_dst::> volume snapshot autodelete modify -vserver svm_backup
-volume volA_dst -enabled false
```

6. 刪除現有的DP類型關係：

```
snapmirror delete -destination-path <SVM:volume>
```

如"指令參考資料ONTAP"需詳細 `snapmirror-delete`資訊，請參閱。

您必須從目的地SVM或目的地叢集執行此命令。

以下範例刪除來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror delete -destination-path svm_backup:volA_dst
```

7. 在來源上釋放原始伺服器 SVM 災難恢復關係：

```
snapmirror release -destination-path <SVM:volume> -relationship-info
-only true
```

以下範例發佈 SVM 災難恢復關係：

```
cluster_src::> snapmirror release -destination-path svm_backup:volA_dst
-relationship-info-only true
```

如"指令參考資料ONTAP"需詳細 `snapmirror release`資訊，請參閱。

8. 您可以使用從保留的輸出 `snapmirror show` 建立新 XDP 類型關係的命令：

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume>  -type XDP -schedule <schedule> -policy <policy>
```

新關係必須使用相同的來源和目的地Volume。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

您必須從目的地SVM或目的地叢集執行此命令。

以下範例在來源磁碟區之間建立 SnapMirror 災難恢復關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup` 使用預設值 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror create -source-path svm1:volA -destination
-path svm_backup:volA_dst
-type XDP -schedule my_daily -policy MirrorAllSnapshots
```

9. 重新同步來源與目的地磁碟區：

```
snapmirror resync -source-path <SVM:volume> -destination-path
<SVM:volume>
```

為了縮短重新同步時間，您可以使用 `-quick-resync`選項，但您應該意識到儲存效率節省可能會遺失。

> 您必須從目的地SVM或目的地叢集執行此命令。雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

以下範例重新同步來源 Volume 之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

詳細了解 `snapmirror resync`在"指令參考資料ONTAP" 。

10. 如果您停用自動刪除快照功能，請重新啟用：

```
volume snapshot autodelete modify -vserver <SVM> -volume <volume>
-enabled true
```

完成後

1. 使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

2. 一旦 SnapMirror XDP 目的地磁碟區開始依照 SnapMirror 原則定義更新快照，請使用來源叢集的命令輸出 `snapmirror list-destinations`來顯示新的 SnapMirror XDP 關係。

DP 型關係的其他資訊

從 ONTAP 9.3 開始， XDP 模式是預設模式，在命令列或新的或現有指令碼中， DP 模式的任何調用都會自動轉換為 XDP 模式。

現有的關係不受影響。如果某個關係已經是DP類型、則會繼續是DP類型。從 ONTAP 9.5 開始，如果未指定資料保護模式或將 XDP 模式指定為關係類型，則 MirrorAndVault 是預設原則。下表顯示預期行為。

如果您指定…	類型為…	預設原則（如果您未指定原則）是…
DP	XDP	MirrorAllSnapshots（SnapMirror DR）
什麼都沒有	XDP	MirrorAndVault（統一化複寫）
XDP	XDP	MirrorAndVault（統一化複寫）

如表所示，在不同情況下指派給 XDP 的預設原則，可確保轉換維持與先前類型的功能等效。當然、您可以視需要使用不同的原則、包括統一化複寫的原則：

如果您指定…	政策是…	結果是…
DP	MirrorAllSnapshots	SnapMirror災難恢復
XDPDefault	SnapVault	MirrorAndVault
統一化複寫	XDP	MirrorAllSnapshots
SnapMirror災難恢復	XDPDefault	SnapVault

轉換的唯一例外情況如下：

- SVM資料保護關係在ONTAP 更新版本的更新版本中、仍預設為DP模式。

  從ONTAP SVM 9.4開始、SVM資料保護關係預設為XDP模式。

- 根Volume負載共享資料保護關係仍預設為DP模式。
- 在更新版本的版本中、資料保護關係仍預設為DP模式。SnapLock ONTAP

  從ONTAP S廳9.5開始、SnapLock 資料保護關係預設為XDP模式。

- 如果您設定下列全叢集選項、DP的明確調用仍會繼續預設為DP模式：

  ```
  options replication.create_data_protection_rels.enable on
  ```

  如果您未明確叫用DP、則會忽略此選項。

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

轉換 **ONTAP SnapMirror** 關聯的類型

從 ONTAP 9 開始、支援 SnapMirror 同步。您可以將 SnapMirror 非同步關係轉換為 SnapMirror 同步關係、反之亦然、而無需執行基準傳輸。

關於這項工作

您無法透過變更 SnapMirror 原則，將 SnapMirror 非同步關係轉換為 SnapMirror 同步關係，反之亦然。

步驟

- * 將 SnapMirror 非同步關係轉換為 SnapMirror 同步關係 *

a. 從目的地叢集刪除 SnapMirror 非同步關係：

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

b. 在來源叢集中，釋放 SnapMirror 關係而不刪除一般快照：

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM>:<destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

c. 從目的地叢集建立 SnapMirror 同步關係：

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM>:<destination_volume> -policy sync-mirror
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

d. 重新同步 SnapMirror 同步關係：

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

- * 將 SnapMirror 同步關係轉換為 SnapMirror 非同步關係 *

a. 從目的地叢集、請將現有的 SnapMirror 同步關係：

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

b. 從目的地叢集刪除 SnapMirror 非同步關係：

```
snapmirror delete -destination-path <SVM:volume>
```

```
cluster2::>snapmirror delete -destination-path vs1_dr:vol1
```

c. 在來源叢集中，釋放 SnapMirror 關係而不刪除一般快照：

```
snapmirror release -relationship-info-only true -destination-path
<destination_SVM:destination_volume>
```

```
cluster1::>snapmirror release -relationship-info-only true
-destination-path vs1_dr:vol1
```

d. 從目的地叢集建立 SnapMirror 非同步關係：

```
snapmirror create -source-path src_SVM:src_volume -destination-path
<destination_SVM:destination_volume> -policy MirrorAllSnapshots
```

```
cluster2::>snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy sync
```

e. 重新同步 SnapMirror 同步關係：

```
snapmirror resync -destination-path <destination_SVM:destination_volume>
```

```
cluster2::>snapmirror resync -destination-path vs1_dr:vol1
```

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

轉換 **ONTAP SnapMirror** 同步關係的模式

從 ONTAP 9 開始、支援 SnapMirror 同步關係。您可以將 SnapMirror 同步關係的模式從 StrictSync 轉換為 Sync 、反之亦然。

關於這項工作

您無法修改 SnapMirror 同步關係的原則來轉換其模式。

步驟

1. 從目的地叢集、請將現有的 SnapMirror 同步關係：

```
snapmirror quiesce -destination-path <destination_SVM>:<destination_volume>
```

```
cluster2::> snapmirror quiesce -destination-path vs1_dr:vol1
```

2. 從目的地叢集刪除現有的 SnapMirror 同步關係：

   `snapmirror delete -destination-path <destination_SVM>:<destination_volume>`

```
cluster2::> snapmirror delete -destination-path vs1_dr:vol1
```

3. 在來源叢集中，釋放 SnapMirror 關係而不刪除一般快照：

   `snapmirror release -relationship-info-only true -destination-path <destination_SVM>:<destination_volume>`

```
cluster1::> snapmirror release -relationship-info-only true -destination
-path vs1_dr:vol1
```

4. 從目的地叢集、透過指定要轉換 SnapMirror 同步關係的模式來建立 SnapMirror 同步關係：

   `snapmirror create -source-path vs1:vol1 -destination-path <destination_SVM>:<destination_volume> -policy Sync|StrictSync`

```
cluster2::> snapmirror create -source-path vs1:vol1 -destination-path
vs1_dr:vol1 -policy Sync
```

5. 從目的地叢集重新同步SnapMirror關係：

   `snapmirror resync -destination-path <destination_SVM>:<destination_volume>`

```
cluster2::> snapmirror resync -destination-path vs1_dr:vol1
```

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

建立並刪除 **ONTAP SnapMirror** 容錯移轉測試磁碟區

從 ONTAP 9.14.1 開始、您可以使用系統管理員建立磁碟區複本、在不中斷主動式

SnapMirror 關係的情況下測試 SnapMirror 容錯移轉和災難恢復。完成測試後、您可以清除相關資料並刪除測試 Volume 。

建立 **SnapMirror** 容錯移轉測試 **Volume**

關於這項工作

- 您可以在同步和 SnapMirror 非同步關係上執行容錯移轉測試。
- 建立磁碟區複本以執行災難恢復測試。
- 複製磁碟區會建立在與 SnapMirror 目的地相同的儲存 VM 上。
- 您可以使用 FlexVol 和 FlexGroup SnapMirror 關係。
- 如果所選關係已存在測試複本、則無法為該關係建立另一個複本。
- 不支援 SnapLock 資料保險箱關係。

開始之前

- 您必須是叢集管理員。
- SnapMirror 授權必須安裝在來源叢集和目的地叢集上。

步驟

1. 在目的地叢集上、選取 * 保護 > 關係 * 。
2. 選取 ⋮ 關係來源旁邊的、然後選擇 * 測試容錯移轉 * 。
3. 在 * 測試容錯移轉 * 視窗中、選取 * 測試容錯移轉 * 。
4. 選取 * 儲存 > Volumes （磁碟區） * 、然後確認已列出測試容錯移轉磁碟區。
5. 選擇 * 儲存 > 共用 * 。
6. 選取 + Add 並選擇 * 共用 * 。
7. 在 * 新增共用 * 視窗的 * 共用名稱 * 欄位中、輸入共用的名稱。
8. 在 * 資料夾 * 欄位中、選取 * 瀏覽 * 、選取測試複製磁碟區、然後選取 * 儲存 * 。
9. 在 * 新增共用 * 視窗的底部、選擇 * 儲存 * 。
10. 在 * 儲存 > 共用 * 窗格中，找到您建立的共用，然後選取 ⌄ 以檢視共用資訊。
11. 在 **SMB/CIFS Access** 下，複製或記下共用的存取路徑，例如 `\\123.456.7.890\failover_test`。
12. 使用 SMB 存取路徑在用戶端上開啟共用區，並確認測試磁碟區具有讀寫功能。

清理容錯移轉資料並刪除測試磁碟區

完成容錯移轉測試之後、您可以清除與測試 Volume 相關的所有資料、然後將其刪除。

步驟

1. 在目的地叢集上、選取 * 保護 > 關係 * 。
2. 選取 ⋮ 關係來源旁邊的、然後選擇 * 清除測試容錯移轉 * 。
3. 在 * 清除測試容錯移轉 * 視窗中、選取 * 清除 * 。
4. 選取 * 儲存 > 磁碟區 * 、並確認測試磁碟區已刪除。

從**SnapMirror DR**目的地**Volume**提供資料

使 **ONTAP SnapMirror** 目的地 **Volume** 可寫入

您必須先將目的地Volume設定為可寫入、才能將資料從磁碟區提供給用戶端。若要在來源無法使用時從鏡射目的地提供資料、請停止排程傳輸至目的地、然後中斷SnapMirror關係、使目的地可寫入。

關於這項工作

您必須從目的地SVM或目的地叢集執行此工作。

步驟

您可以使用系統管理員或 ONTAP CLI 、將目的地磁碟區設為可寫入。

系統管理員

1. 選取保護關係：按一下 * 保護 > 關係 * 、然後按一下所需的磁碟區名稱。
2. 單擊。 ⋮
3. 停止排程的傳輸：按一下*暫停*。
4. 使目的地可寫入：按一下*中斷*。
5. 移至主*關係*頁面、確認關係狀態顯示為「中斷」。

後續步驟

將目的地 Volume 設為可寫入後、您需要 "反向重新同步複寫關係" 執行此操作。

當停用的來源磁碟區再次可用時、您應該再次反轉重新同步關係、將目前資料複製到原始來源磁碟區。

CLI

1. 停止排程的目的地傳輸：

   ```
   snapmirror quiesce -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   下列範例會停止來源磁碟區之間的排程傳輸 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

   ```
   cluster_dst::> snapmirror quiesce -source-path svm1:volA
   -destination-path svm_backup:volA_dst
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

2. 停止持續傳輸至目的地：

   ```
   snapmirror abort -source-path <SVM:volume|cluster://SVM/volume>
   -destination-path <SVM:volume|cluster://SVM/volume>
   ```

   ⓘ SnapMirror 同步關係不需要此步驟（從 ONTAP 9 開始支援）。

   下列範例會停止來源磁碟區之間的持續傳輸 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

   ```
   cluster_dst::> snapmirror abort -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror abort`資訊，請參閱。

3. 打破SnapMirror DR關係：

```
snapmirror break -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume>
```

以下範例打破來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror break -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

後續步驟

將目的地 Volume 設為可寫入後、您需要 "重新同步複寫關係" 執行此操作。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作...	請參閱此內容...
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"Volume災難恢復總覽"

設定 **ONTAP SnapMirror** 目的地 **Volume** 以進行資料存取

將目的地Volume設為可寫入後、您必須設定該磁碟區以進行資料存取。NAS用戶端、NVMe子系統和SAN主機可從目的地Volume存取資料、直到重新啟動來源Volume為止。

NAS環境：

1. 將NAS磁碟區掛載至命名空間、其路徑與來源SVM中的來源磁碟區掛載路徑相同。
2. 將適當的ACL套用到目的地磁碟區的SMB共用區。
3. 將NFS匯出原則指派給目的地Volume。
4. 將配額規則套用至目的地Volume。
5. 將用戶端重新導向至目的地Volume。
6. 在用戶端上重新掛載 NFS 和 SMB 共用。

SAN 環境：

1. 將磁碟區中的LUN對應至適當的啟動器群組。
2. 對於iSCSI、請從SAN主機啟動器建立iSCSI工作階段至SAN LIF。
3. 在SAN用戶端上、執行儲存設備重新掃描、以偵測連接的LUN。

如需NVMe環境的相關資訊、請參閱 "SAN管理"。

重新啟動原始 **ONTAP SnapMirror** 來源磁碟區

當您不再需要從目的地提供資料時、可以重新建立來源與目的地磁碟區之間的原始資料保護關係。

關於這項工作

- 以下程序假設原始來源Volume中的基準線完整無缺。如果基準不完整、您必須先建立並初始化您要從中處理資料的磁碟區與原始來源磁碟區之間的關係、然後再執行程序。
- XDP SnapMirror關係的背景準備和資料倉儲階段可能需要很長時間。SnapMirror關係報告長時間處於「準備」狀態、並不罕見。

步驟

1. 反轉原始資料保護關係：

   `snapmirror resync -source-path SVM:volume -destination-path SVM:volume`

   如"指令參考資料ONTAP"需詳細 `snapmirror resync`資訊，請參閱。

   > 您必須從原始來源SVM或原始來源叢集執行此命令。雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。如果來源和目的地上不存在一般快照，則命令會失敗。用於 `snapmirror initialize` 重新初始化關係。如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

   以下範例反轉原始來源 Volume 之間的關係、 `volA` 開啟 `svm1`以及您要提供資料的磁碟區、 `volA_dst` 開啟 `svm_backup`：

   ```
   cluster_src::> snapmirror resync -source-path svm_backup:volA_dst
   -destination-path svm1:volA
   ```

2. 當您準備重新建立對原始來源的資料存取時、請停止對原始目的地Volume的存取。其中一種方法是停止原始目的地SVM：

   `vserver stop -vserver SVM`

   > 您必須從原始目的地SVM或原始目的地叢集執行此命令。此命令會停止使用者對整個原始目的地SVM的存取。您可能想要使用其他方法停止存取原始目的地Volume。

   下列範例會停止原始目的地SVM：

   ```
   cluster_dst::> vserver stop svm_backup
   ```

   如"指令參考資料ONTAP"需詳細 `vserver stop`資訊，請參閱。

3. 更新反轉的關係：

`snapmirror update -source-path SVM:volume -destination-path SVM:volume`

您必須從原始來源SVM或原始來源叢集執行此命令。

以下範例更新了您要從中提供資料的磁碟區之間的關係、 `volA_dst` 開啟 `svm_backup`和原始來源`Volume`、 `volA` 開啟 `svm1`：

```
cluster_src::> snapmirror update -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

4. 從原始來源SVM或原始來源叢集、停止針對反向關係進行排程傳輸：

`snapmirror quiesce -source-path SVM:volume -destination-path SVM:volume`

您必須從原始來源SVM或原始來源叢集執行此命令。

下列範例會停止在原始目的地Volume之間的排程傳輸、 `volA_dst` 開啟 `svm_backup`和原始來源`Volume`、 `volA` 開啟 `svm1`：

```
cluster_src::> snapmirror quiesce -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

5. 當完成最後的更新、且關係指出關係狀態為「靜止」時、請從原始來源SVM或原始來源叢集執行下列命令、以中斷反向關係：

`snapmirror break -source-path SVM:volume -destination-path SVM:volume`

您必須從原始來源SVM或來源叢集執行此命令。

下列範例打破了原始目的地Volume之間的關係、 `volA_dst` 開啟 `svm_backup`和原始來源`Volume`、 `volA` 開啟 `svm1`：

```
cluster_scr::> snapmirror break -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

6. 從原始來源SVM或原始來源叢集刪除反向的資料保護關係：

`snapmirror delete -source-path SVM:volume -destination-path SVM:volume`

您必須從原始來源SVM或原始來源叢集執行此命令。

以下範例刪除原始來源磁碟區之間的反向關係、 `volA` 開啟 `svm1`以及您要提供資料的磁碟區、 `volA_dst` 開啟 `svm_backup`：

```
cluster_src::> snapmirror delete -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

如"指令參考資料ONTAP"需詳細 `snapmirror delete`資訊，請參閱。

7. 從原始目的地SVM或原始目的地叢集釋放反向關係。

`snapmirror release -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

您必須從原始目的地SVM或原始目的地叢集執行此命令。

下列範例會在原始目的地Volume之間釋出相反的關係、 `volA_dst` 開啟 `svm_backup`和原始來源 `Volume`、 `volA` 開啟 `svm1`：

```
cluster_dst::> snapmirror release -source-path svm_backup:volA_dst
-destination-path svm1:volA
```

如"指令參考資料ONTAP"需詳細 `snapmirror release`資訊，請參閱。

8. 從原始目的地重新建立原始資料保護關係：

`snapmirror resync -source-path` *`SVM:volume`* `-destination-path` *`SVM:volume`*

以下範例重新建立原始來源磁碟區之間的關係、 `volA` 開啟 `svm1`和原始目的地 `Volume` 、 `volA_dst` 開啟 `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror resync`資訊，請參閱。

9. 如有需要、請啟動原始目的地SVM：

`vserver start -vserver` *`SVM`*

下列範例會啟動原始目的地SVM：

```
cluster_dst::> vserver start svm_backup
```

如"指令參考資料ONTAP"需詳細 `vserver start`資訊，請參閱。

完成後

使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

從**SnapMirror**目的地**Volume**還原檔案

從 **ONTAP SnapMirror** 目的地還原檔案， **LUN** 或 **NVMe** 命名空間

您可以從快照還原單一檔案， LUN ，一組檔案或 LUN ，或從 SnapMirror 目的地磁碟區還原 NVMe 命名空間。從 ONTAP 9 7 開始、您也可以從 SnapMirror 同步目的地還原 NVMe 命名空間。您可以將檔案還原至原始來源磁碟區或不同的磁碟區。

開始之前

若要從 SnapMirror 同步目的地還原檔案或 LUN （從 ONTAP 9 開始支援）、您必須先刪除並釋放關係。

關於這項工作

您要還原檔案或LUN（目的地Volume）的磁碟區必須是讀寫磁碟區：

- 如果來源和目的地磁碟區有通用快照， SnapMirror 會執行 _ 遞增還原 _ （這通常是還原至原始來源磁碟區的情況）。
- 否則， SnapMirror 會執行 _baseline 還原，其中指定的快照及其參照的所有資料區塊都會傳輸到目的地 Volume 。

步驟

1. 列出目的地 Volume 中的快照：

   ```
   volume snapshot show -vserver <SVM> -volume volume
   ```

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

   以下範例顯示目的地上的快照 `vserverB:secondary1`：

```
cluster_dst::> volume snapshot show -vserver vserverB -volume secondary1

Vserver     Volume      Snapshot                State    Size  Total%
Used%
-------     ------      ---------- ----------- ------   -----  ------
-----
vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
0%
                        daily.2013-01-25_0010   valid   92KB      0%
0%
                        hourly.2013-01-25_0105  valid   228KB     0%
0%
                        hourly.2013-01-25_0205  valid   236KB     0%
0%
                        hourly.2013-01-25_0305  valid   244KB     0%
0%
                        hourly.2013-01-25_0405  valid   244KB     0%
0%
                        hourly.2013-01-25_0505  valid   244KB     0%
0%

7 entries were displayed.
```

2. 從 SnapMirror 目的地磁碟區的快照中還原單一檔案或 LUN ，或是一組檔案或 LUN ：

```
snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, … -source-snapshot
snapshot -file-list <source_file_path,@destination_file_path>
```

您必須從目的地SVM或目的地叢集執行此命令。

以下命令將文件和 `file2`原始目標卷中的快照 `daily.2013-01-25_0010`恢復 `file1`到原始 `secondary1`源卷活動文件系統中的同一位置 `primary1`：

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list /dir1/file1,/dir2/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

以下命令將文件和 `file2`原始目標卷中的快照 `daily.2013-01-25_0010`恢復 `file1`到原始 `secondary1`源卷活動文件系統中的不同位置 `primary1`。

目的地檔案路徑以@符號開頭、接著是原始來源Volume根目錄下的檔案路徑。在此範例中、 `file1` 還原至

/dir1/file1.new 檔案 2 會還原至 /dir2.new/file2 開啟 primary1：

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,@/dir2.new/file2

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

以下命令可將檔案和 file3`原始目的地 Volume 中的 `secondary1`快照 `daily.2013-01-25_0010`還原 `file1`到原始來源 Volume 作用中檔案系統中的不同位置，並從 `snap1`還原 `file2`到作用中檔案系統中的相同 `primary1`位置 `primary1。

在此範例中、檔案 file1 還原至 /dir1/file1.new 和 file3 還原至 /dir3.new/file3：

```
cluster_dst::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010 -file-list
/dir/file1,@/dir1/file1.new,/dir2/file2,/dir3/file3,@/dir3.new/file3

[Job 3479] Job is queued: snapmirror restore for the relationship with
destination vserverA:primary1
```

相關資訊

- "SnapMirror還原"

從 **ONTAP SnapMirror** 目的地還原磁碟區內容

您可以從 SnapMirror 目的地磁碟區的快照還原整個磁碟區的內容。您可以將磁碟區的內容還原至原始來源磁碟區或其他磁碟區。

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"恢復資料。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

還原作業的目的地Volume必須是下列其中一項：

- 讀寫磁碟區（在這種情況下， SnapMirror 會執行 _ 遞增還原 _ ，前提是來源磁碟區和目的地磁碟區具有通用快照（通常是還原至原始來源磁碟區的情況）。

  如果沒有通用快照，則命令會失敗。您無法將磁碟區的內容還原至空白的讀寫磁碟區。

- 空白的資料保護磁碟區，在這種情況下， SnapMirror 會執行 _ 基準還原 _ ，其中指定的快照及其參照的所有資料區塊都會傳輸到來源磁碟區。

還原磁碟區的內容是一項顛覆性的作業。當SnapVault 還原作業執行時、SMB流量不得在還原主磁碟區上執行。

如果還原作業的目的地Volume已啟用壓縮功能、且來源Volume未啟用壓縮功能、請停用目的地Volume上的壓縮功能。還原作業完成後、您需要重新啟用壓縮。

在執行還原之前、會停用為目的地Volume定義的任何配額規則。您可以使用 `volume quota modify` 還原作業完成後重新啟動配額規則的命令。

當磁碟區中的資料遺失或毀損時，您可以從較早的快照還原資料。

此程序會以舊版快照版本的資料取代來源磁碟區上的目前資料。您應該在目的地叢集上執行此工作。

步驟

您可以使用系統管理員或 ONTAP CLI 還原磁碟區的內容。

系統管理員

1. 按一下「保護>關係」、然後按一下來源Volume名稱。
2. 按一下 ⋮ 、然後選取 * 還原 * 。
3. 在*來源*下、預設會選取來源Volume。如果您要選擇來源以外的磁碟區、請按一下*其他Volume *。
4. 在 * 目的地 * 下，選擇您要還原的快照。
5. 如果來源與目的地位於不同的叢集上、請在遠端叢集上按一下*保護>關係*、以監控還原進度。

CLI

1. 列出目的地 Volume 中的快照：

   ```
   volume snapshot show -vserver <SVM> -volume <volume>
   ```

   以下範例顯示目的地上的快照 `vserverB:secondary1`：

   ```
   cluster_dst::> volume snapshot show -vserver vserverB -volume
   secondary1

   Vserver     Volume      Snapshot                State    Size
   Total% Used%
   -------     ------      ---------- ----------- ------   -----
   ------ -----
   vserverB    secondary1  hourly.2013-01-25_0005  valid   224KB     0%
   0%
                           daily.2013-01-25_0010   valid   92KB      0%
   0%
                           hourly.2013-01-25_0105  valid   228KB     0%
   0%
                           hourly.2013-01-25_0205  valid   236KB     0%
   0%
                           hourly.2013-01-25_0305  valid   244KB     0%
   0%
                           hourly.2013-01-25_0405  valid   244KB     0%
   0%
                           hourly.2013-01-25_0505  valid   244KB     0%
   0%

   7 entries were displayed.
   ```

2. 從 SnapMirror 目的地磁碟區的快照還原磁碟區的內容：

   ```
   snapmirror restore -source-path <SVM:volume>|<cluster://SVM/volume>
   -destination-path <SVM:volume>|<cluster://SVM/volume> -source-snapshot
   ```

<snapshot>

您必須從原始來源SVM或原始來源叢集執行此命令。

以下命令可從原始目的地 Volume 中的快照 `daily.2013-01-25_0010`還原原始來源 `Volume `secondary1`的內容 `primary1`：

```
cluster_src::> snapmirror restore -source-path vserverB:secondary1
-destination-path vserverA:primary1 -source-snapshot daily.2013-01-
25_0010

Warning: All data newer than snapshot daily.2013-01-25_0010 on
volume vserverA:primary1 will be deleted.

Do you want to continue? {y|n}: y

[Job 34] Job is queued: snapmirror restore from source
vserverB:secondary1 for the snapshot daily.2013-01-25_0010.
```

3. 重新掛載還原的磁碟區、然後重新啟動所有使用該磁碟區的應用程式。

其他方法可在**ONTAP** 不一樣的情況下執行

若要執行這些工作...	請參閱此內容...
System Manager Classic（ONTAP 適用於更新版本的更新版本）	"使用SnapVault 功能概述進行Volume還原"

相關資訊

- "SnapMirror還原"
- "Volume Snapshot顯示"

手動更新 **ONTAP SnapMirror** 複寫關係

如果來源磁碟區已移動、更新失敗、您可能需要手動更新複寫關係。

關於這項工作

SnapMirror會中止從移動的來源Volume進行的任何傳輸、直到您手動更新複寫關係為止。

從 ONTAP 9 開始、支援 SnapMirror 同步關係。雖然來源與目的地磁碟區在這些關係中始終保持同步、但從次要叢集取得的檢視只會以每小時為單位與主要磁碟區進行同步。如果您想要檢視目的地的時間點資料、您應該執行 `snapmirror update`命令來執行手動更新。

步驟

1. 手動更新複寫關係：

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, …
-destination-path <SVM:volume>|<cluster://SVM/volume>, …
```

您必須從目的地SVM或目的地叢集執行此命令。如果來源和目的地上不存在一般快照，則命令會失敗。用於 `snapmirror initialize` 重新初始化關係。如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

以下範例更新來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

```
cluster_src::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

重新同步 **ONTAP SnapMirror** 複寫關係

當目的地 Volume 可寫入之後，更新失敗之後，您需要重新同步複寫關係，因為來源和目的地磁碟區上不存在一般快照，或者您想要變更關係的複寫原則。

從功能介紹9.8開始ONTAP 、您可以使用System Manager執行反向重新同步作業、刪除現有的保護關係、並反轉來源與目的地磁碟區的功能。然後、您可以在修復或更換來源時、使用目的地磁碟區來提供資料、更新來源、並重新建立系統的原始組態。

System Manager 不支援反向重新同步處理至無法處理的關係。您可以使用 ONTAP CLI 執行具有無法消除的重新同步作業。

關於這項工作

- 雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。
- 屬於扇出或串聯組態一部分的磁碟區可能需要較長的時間才能重新同步。SnapMirror關係報告長時間處於「準備」狀態、並不罕見。
- 從ONTAP 9.13.1 開始， ONTAP預設嘗試使用快速重新同步來減少重新同步時間。若要預設啟用快速重新同步功能，必須滿足以下條件：
  - FlexVol卷上沒有克隆卷
  - 使用 MirrorAllSnapshots 策略時

使用 `-quick-resync` 由於傳輸資料區塊的儲存效率降低，重新同步目標磁碟區可能會佔用額外的空間。這部分額外的空間消耗會在重新同步目標上透過線上或複製後儲存效率應用來回收。

這 `-quick-resync` 參數為可選參數。您可以使用以下方法啟用或停用快速重新同步： `-quick -resync true|false` 參數 `snapmirror resync` 命令。

有關更多信息 `-quick-resync`參見 "指令參考資料ONTAP"。

步驟

您可以使用系統管理員或 ONTAP CLI 來執行此工作。如果您使用 ONTAP CLI 、無論您是將目的地磁碟區設為可寫入、或是正在更新複寫關係、程序都一樣。

System Manager 回復重新同步

"中斷關係"將目的地設為可寫入後、請反向重新同步關係：

1. 在目的地叢集上、按一下*保護>關係*。
2. 將游標移至您要反轉的中斷關係上、按一下 ⋮、然後選取 * 反轉重新同步 * 。
3. 在 * 反向重新同步關係 * 視窗中、按一下 * 反向重新同步 * 。
4. 在*關係*下、檢視*傳輸狀態*的關係、以監控反轉重新同步進度。

後續步驟

當原始來源再次可用時、您可以中斷反轉的關係、並執行另一個反向重新同步作業、以重新建立原始關係。反向重新同步程序會將任何變更從提供資料的站台複製到原始來源、並使原始來源重新讀取。

System Manager 重新同步

1. 按一下 * 保護 > 關係 * 。
2. 將游標移至您要重新同步的關係上方、然後按一下 ⋮ 、再選取 * 中斷 * 。
3. 當關係狀態顯示「中斷」時、按一下、 ⋮ 然後選取 * 重新同步 * 。
4. 在*關係*下、檢查關係狀態以監控重新同步進度。重新同步完成時、狀態會變更為「鏡射」。

CLI

1. 重新同步來源與目的地磁碟區：

```
snapmirror resync -source-path <SVM:volume|cluster://SVM/volume>
-destination-path <SVM:volume|cluster://SVM/volume> -type DP|XDP
-policy <policy>
```

ⓘ 您必須從目的地SVM或目的地叢集執行此命令。

以下範例重新同步上的來源磁碟區與上的目的地磁碟區之間的關係 `volA svm1 volA_dst svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror resync`資訊，請參閱。

相關資訊

- "重新同步 ONTAP SnapMirror 目的地 SVM 上的資料"

刪除 ONTAP SnapMirror Volume 複寫關係

您可以使用 `snapmirror delete`和 `snapmirror release`命令來刪除磁碟區複寫關係。然後您可以手動刪除不需要的目的地Volume。

關於這項工作

此命令會 `snapmirror release`從來源中刪除任何 SnapMirror 建立的快照。您可以使用 `-relationship-info-only`選項來保留快照。

步驟

1. 靜止複寫關係：

   ```
   snapmirror quiesce -destination-path <SVM:volume>|<cluster://SVM/volume>
   ```

   ```
   cluster_dst::> snapmirror quiesce -destination-path svm_backup:volA_dst
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

2. （選用）如果您需要將目的地磁碟區設為讀寫磁碟區、請中斷複寫關係。如果您打算刪除目的地Volume、或是不需要讀取/寫入磁碟區、可以跳過此步驟：

   ```
   snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   ```
   cluster_dst::> snapmirror break -source-path svm1:volA -destination-path
   svm_backup:volA_dst
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

3. 刪除複寫關係：

   ```
   snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>, …
   -destination-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

   ⓘ 您必須從目的地叢集或目的地SVM執行此命令。

   以下範例刪除來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`：

   ```
   cluster_dst::> snapmirror delete -source-path svm1:volA -destination
   -path svm_backup:volA_dst
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror delete`資訊，請參閱。

4. 來自來源SVM的版本複寫關係資訊：

   ```
   snapmirror release -source-path <SVM:volume>|<cluster://SVM/volume>, …
   ```

`-destination-path <SVM:volume>|<cluster://SVM/volume>, …`

您必須從來源叢集或來源SVM執行此命令。

下列範例會從來源 SVM 發佈指定複寫關係的資訊 `svm1`：

```
cluster_src::> snapmirror release -source-path svm1:volA -destination
-path svm_backup:volA_dst
```

如"指令參考資料ONTAP"需詳細 `snapmirror release`資訊，請參閱。

管理 **ONTAP SnapMirror** 磁碟區的儲存效率

SnapMirror 可保留來源和目的地磁碟區的儲存效率、除非目的地磁碟區上已啟用後處理資料壓縮。在這種情況下、目的地磁碟區上的所有儲存效率都會遺失。若要修正此問題、您必須停用目的地磁碟區的後處理壓縮、手動更新關係、並重新啟用儲存效率。

關於這項工作

您可以使用 `volume efficiency show`命令來判斷是否在磁碟區上啟用效率。如"指令參考資料ONTAP"需詳細 `volume efficiency show`資訊，請參閱。

您可以查看SnapMirror稽核記錄並找出傳輸說明、藉此檢查SnapMirror是否維持儲存效率。如果顯示傳輸說明 `transfer_desc=Logical Transfer with Storage Efficiency`， SnapMirror 將保持存儲效率。如果顯示傳輸說明 `transfer_desc=Logical Transfer`， SnapMirror 不會維持儲存效率。例如：

```
Fri May 22 02:13:02 CDT 2020 ScheduledUpdate[May 22 02:12:00]:cc0fbc29-
b665-11e5-a626-00a09860c273 Operation-Uuid=39fbcf48-550a-4282-a906-
df35632c73a1 Group=none Operation-Cookie=0 action=End source=<sourcepath>
destination=<destpath> status=Success bytes_transferred=117080571
network_compression_ratio=1.0:1 transfer_desc=Logical Transfer - Optimized
Directory Mode
```

開始之前

- 來源與目的地叢集和SVM必須進行對等關係。

  "叢集與SVM對等關係"

- 您必須停用目的地磁碟區上的後處理壓縮。
- 使用儲存設備進行邏輯傳輸：從 ONTAP 9.3 開始、不再需要手動更新即可重新啟用儲存效率。如果SnapMirror偵測到後處理壓縮已停用、則會在下次排程更新時自動重新啟用儲存效率。來源和目的地都必須執行ONTAP 不支援的9.3。
- 從功能性的9.3開始ONTAP 、AFF 在FAS 目的地Volume可寫入後、系統會以不同於功能性的方式管理儲存效率設定：
  - 使用以下方法將目標磁碟區設定為可寫入後 `snapmirror break`命令，卷上的快取策略將自動設定為

`auto (預設).

這種行為FlexVol 僅適用於不適用於FlexGroup 功能區、不適用於功能區。

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

- 重新同步時，快取策略會自動設定為 `none` ，並且無論您的原始設定如何，重複資料刪除和內聯壓縮都會自動停用。您必須視需要手動修改設定。

啟用儲存效率的手動更新可能相當耗時。您可能想要在非尖峰時間執行作業。

步驟

1. 更新複寫關係並重新啟用儲存效率：

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>, ...
-destination-path <SVM:volume>|<cluster://SVM/volume>, ... -enable
-storage-efficiency true
```

您必須從目的地SVM或目的地叢集執行此命令。如果來源和目的地上不存在一般快照，則命令會失敗。用於 `snapmirror initialize` 重新初始化關係。如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

以下範例更新來源磁碟區之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA_dst` 開啟 `svm_backup`並重新提高儲存效率：

```
cluster_dst::> snapmirror update -source-path svm1:volA -destination
-path svm_backup:volA_dst -enable-storage-efficiency true
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

使用 **ONTAP SnapMirror** 全域節流

全域網路節流功能適用於SnapVault 每節點層級的所有SnapMirror和SnapMirror傳輸。

關於這項工作

SnapMirror全域節流可限制傳入和/或傳出SnapMirror和SnapVault SnapMirror傳輸所使用的頻寬。此限制會在叢集中的所有節點上強制整個叢集。

例如、如果傳出節流設定為100 Mbps、叢集中的每個節點都會將傳出頻寬設為100 Mbps。如果停用全域節流、則會在所有節點上停用此功能。

雖然資料傳輸率通常以每秒位元數（bps）表示、但節流值必須以每秒千位元組（KB）為單位輸入。

在 ONTAP 9.9.1 及更早版本中，油門對傳輸或負載分配鏡射傳輸沒有影響 `volume move`。從 ONTAP 9.10.0 開始，您可以指定一個選項來節流 Volume Move 作業。如需詳細資訊、請參閱 "如何在 ONTAP 9.10 及更新版本中調節音量移動"。

全域節流可搭配SnapMirror和SnapVault SnapMirror傳輸的個別關係節流功能。在每個關係傳輸的總頻寬超過全域節流的值之前、會強制執行每個關係節流、之後會強制執行全域節流。節流值 `0` 表示全域節流已停用。

SnapMirror 全域節流對 SnapMirror 同步關係在同步時沒有影響。不過、當 SnapMirror 同步關係執行非同步傳輸階段（例如初始化作業或非同步事件之後）時、這些限制會影響它們。因此、不建議使用 SnapMirror 同步關係來啟用全域節流。

步驟

1. 啟用全域節流：

   ```
   options -option-name replication.throttle.enable on|off
   ```

   以下範例說明如何啟用 SnapMirror 全域節流功能 `cluster_dst`：

   ```
   cluster_dst::> options -option-name replication.throttle.enable on
   ```

2. 指定目的地叢集上傳入傳輸所使用的最大總頻寬：

   ```
   options -option-name replication.throttle.incoming.max_kbs <KBps>
   ```

   建議的最小節流頻寬為每秒 4 KB （ KBps ），最大值為每秒 2 TB （ Tbps ）。此選項的預設值為 `unlimited`，表示使用的總頻寬不受限制。

   以下範例說明如何將傳入傳輸所使用的最大總頻寬設定為每秒 100 MB （ Mbps ）：

   ```
   cluster_dst::> options -option-name
   replication.throttle.incoming.max_kbs 12500
   ```

   每秒 100 MB （ Mbps ） = 每秒 12500 KB （ KBps ）

3. 指定來源叢集上傳出傳輸所使用的最大總頻寬：

   ```
   options -option-name replication.throttle.outgoing.max_kbs <KBps>
   ```

   建議的最小節流頻寬為4 KB、最大值為2 Tbps。此選項的預設值為 `unlimited`，表示使用的總頻寬不受限制。參數值以千位元組 / 秒 （ KBps ）為單位。

   下列範例說明如何將傳出傳輸所使用的最大總頻寬設定為100 Mbps：

   ```
   cluster_src::> options -option-name
   replication.throttle.outgoing.max_kbs 12500
   ```

管理SnapMirror SVM複寫

瞭解 ONTAP SnapMirror SVM 複寫

您可以使用SnapMirror在SVM之間建立資料保護關係。在此類型的資料保護關係中、系統會複寫SVM組態的全部或部分內容、從NFS匯出、SMB共用到RBAC、以及SVM擁有的磁碟區中的資料。

支援的關係類型

只能複寫資料服務SVM。支援下列資料保護關係類型：

- SnapMirror DR_ ，其中目的地通常只包含目前在來源上的快照。

  從ONTAP 功能更新至功能更新至功能更新、當您使用鏡射儲存庫原則時、此行為將有所變更。從 ONTAP 9.9.1 開始，您可以在來源和目的地上建立不同的快照原則，而目的地上的快照不會被來源上的快照覆寫：

  - 在正常的排程作業、更新和重新同步期間、不會從來源覆寫到目的地
  - 在中斷作業期間不會刪除這些項目。
  - 它們不會在反轉重新同步作業期間刪除。
    當您使用 ONTAP 9.9.1 及更新版本來使用 mirror 保存原則來設定 SVM 災難關係時、原則的行為如下：
  - 來源的使用者定義快照原則不會複製到目的地。
  - 系統定義的快照原則不會複製到目的地。
  - 不會將 Volume 與使用者和系統定義的快照原則關聯，複製到目的地。+ SVM：
- *SnapMirror* 統一複製，其中目標配置為 DR 和長期保留。

如需 SnapMirror 統一複寫的詳細資訊、請參閱 "SnapMirror統一化複寫基礎"。

複寫原則的_policy類型_決定其支援的關係類型。下表顯示可用的原則類型。

原則類型	關係類型
非同步鏡射	SnapMirror災難恢復
鏡射保存庫	統一化複寫

XDP取代**DP**做**ONTAP** 為**SVM**複寫的預設值、如《**SVM 9.4**的預設值

從ONTAP SVM 9.4開始、SVM資料保護關係預設為XDP模式。SVM資料保護關係在ONTAP 更新版本的更新版本中、仍預設為DP模式。

現有關係不受 XDP 預設值影響。如果某個關係已經是DP類型、則會繼續是DP類型。下表顯示您可以預期的行為。

如果您指定…	類型為…	預設原則（如果您未指定原則）是…

DP	XDP	MirrorAllSnapshots（SnapMirror DR）
什麼都沒有	XDP	MirrorAllSnapshots（SnapMirror DR）
XDP	XDP	MirrorAndVault（統一複寫）

您可以在這裡找到有關將 DP 關係轉換為 XDP 關係的資訊，以及其他詳細資料："將現有的 ONTAP DP 類型關係轉換為 XDP"。

SVM複寫不支援版本獨立性。在 SVM 災難恢復組態中、目的地 SVM 必須位於執行與來源 SVM 叢集相同 ONTAP 版本的叢集上、才能支援容錯移轉和容錯回復作業。

"SnapMirror ONTAP 關係的相容版本"

如何複寫**SVM**組態

SVM複寫關係的內容取決於下列欄位的互動：

- 。 `-identity-preserve true` 的選項 `snapmirror create` 命令會複寫整個 SVM 組態。

  。 `-identity-preserve false` 選項僅複寫 SVM 的磁碟區和驗證與授權組態、以及中列出的通訊協定和名稱服務設定 "在 SVM 災難恢復關係中複寫的組態"。

- 。 `-discard-configs network` 的選項 `snapmirror policy create` 命令會從 SVM 複寫中排除生命與相關網路設定、以供來源和目的地 SVM 位於不同子網路的情況使用。
- 。 `-vserver-dr-protection unprotected` 的選項 `volume modify` 命令會將指定的 Volume 排除在 SVM 複寫之外。

否則、SVM複寫幾乎與Volume複寫相同。您幾乎可以使用與用於磁碟區複寫相同的SVM複寫工作流程。

支援詳細資料

下表顯示SnapMirror SVM複寫的支援詳細資料。

資源或功能	支援詳細資料
部署類型	• 單一來源至單一目的地 • 從ONTAP 功能檔9.4開始、您只能將風扇輸出至兩個目的地。 根據預設、每個來源SVM只允許一個身分識別保留真正的關係。

關係類型	• SnapMirror 災難恢復 • SnapMirror統一複製
複寫範圍	僅限叢集間。您無法在同一個叢集中複寫SVM。
自主勒索軟體保護	• 從 ONTAP 9.12.1 開始支援。如需更多資訊、請參閱 "自主勒索軟體保護"。
一致性群組非同步支援	從 ONTAP 9.14.1 開始、當一致性群組存在時、最多可支援 32 個 SVM 災難恢復關係。請參閱 "保護一致性群組" 和 "一致性群組限制" 以取得更多資訊。
FabricPool	從 ONTAP 9.6 開始， FabricPool 支援 SnapMirror SVM 複寫。在 SVM DR 關係中，來源和目的地磁碟區不需要使用 FabricPool 集合體，但它們必須使用相同的分層原則。 從 ONTAP 9.12.1 開始， FabricPool 和 FlexGroup 磁碟區可支援 SnapMirror SVM 複寫，並搭配使用。在 9.12.1 之前，這些功能中的任何兩項都能一起運作，但並非全部三項都能一起運作。

MetroCluster	從 ONTAP 9.11.1 開始、 MetroCluster 組態中 SVM 災難恢復關係的兩端都可以做為額外 SVM 災難恢復組態的來源。 從ONTAP 支援使用支援SnapMirror 9.5開始、MetroCluster SnapMirror SVM複寫功能可在各種組態上執行。 • 在早於 ONTAP 9.10.X 的版本中、 MetroCluster 組態不能是 SVM 災難恢復關係的目的地。 • 在 ONTAP 9.10.1 及更新版本中、 MetroCluster 組態可以是 SVM 災難恢復關係的目的地、僅供移轉之用、而且必須符合中所述的所有必要要求 "TR-4966 ：將 SVM 移轉至 MetroCluster 解決方案"。 • 只有MetroCluster 在整個SVM組態中有作用中的SVM、才能成為SVM災難恢復關係的來源。 來源可以是切換前的同步來源SVM、或是切換後的同步目的地SVM。 • 當某個支援區組態處於穩定狀態時、由於該磁碟區不在線上、所以無法將該支援區同步目的地SVM作為SVM災難恢復關係的來源。MetroCluster MetroCluster • 當同步來源 SVM 是 SVM 災難恢復關係的來源時、來源 SVM 災難恢復關係資訊會複寫到 MetroCluster 合作夥伴。 • 在切換和切換程序期間、複寫至 SVM 災難恢復目的地可能會失敗。 不過、切換或切換程序完成後、下一個 SVM 災難恢復排程更新將會成功。
一致性群組	從 ONTAP 9.14.1 開始支援。如需詳細資訊、請參閱保護一致性群組。
SS3 ONTAP	SVM 災難恢復不支援。
SnapMirror同步	SVM 災難恢復不支援。
版本獨立	不支援。

Volume加密	• 來源上的加密磁碟區會在目的地上加密。 • 必須在目的地上設定內建金鑰管理程式或KMIP伺服器。 • 目的地會產生新的加密金鑰。 • 如果目的地不包含支援Volume .Encryption的節點、則複寫會成功、但目的地磁碟區不會加密。

在 **SVM** 災難恢復關係中複寫的組態

下表顯示的互動 `snapmirror create -identity-preserve` 選項和 `snapmirror policy create -discard-configs network` 選項：

組態已複寫		**-identity-preserve true**		**-identity-preserve false**
		* 政策不含 `-discard -configs network` 設定 *	* 政策與 `-discard -configs network` 設定 *	
網路	NAS生命里	是的	否	否
LIF Kerberos組態	是的	否	否	SAN LIF
否	否	否	防火牆原則	是的
是的	否	服務原則	是的	是的
否	路由	是的	否	否
廣播網域	否	否	否	子網路
否	否	否	IPSpace	否
否	否	中小企業	SMB 伺服器	是的
是的	否	本機群組和本機使用者	是的	是的
是的	權限	是的	是的	是的
陰影複製	是的	是的	是的	BranchCache
是的	是的	是的	伺服器選項	是的

是的	是的	伺服器安全性	是的	是的
否	主目錄、共享	是的	是的	是的
symlink	是的	是的	是的	Fpolicy原則、FSecurity原則及FSecurity NTFS
是的	是的	是的	名稱對應與群組對應	是的
是的	是的	稽核資訊	是的	是的
是的	NFS	匯出原則	是的	是的
否	匯出原則規則	是的	是的	否
NFS 伺服器	是的	是的	否	RBAC
安全性憑證	是的	是的	否	登入使用者、公開金鑰、角色和角色組態
是的	是的	是的	SSL	是的
是的	否	名稱服務	DNS和DNS主機	是的
是的	否	UNIX使用者與UNIX群組	是的	是的
是的	Kerberos領域和Kerberos金鑰區塊	是的	是的	否
LDAP與LDAP用戶端	是的	是的	否	網路群組
是的	是的	否	NIS	是的
是的	否	網路與網路存取	是的	是的
否	Volume	物件	是的	是的
是的	快照和快照原則	是的	是的	是的
自動刪除原則	否	否	否	效率原則

是的	是的	是的	配額原則和配額原則規則	是的
是的	是的	恢復佇列	是的	是的
是的	根Volume	命名空間	是的	是的
是的	使用者資料	否	否	否
qtree	否	否	否	配額
否	否	否	檔案層級QoS	否
否	否	屬性：根磁碟區的狀態、空間保證、大小、自動調整大小及檔案總數	否	否
否	儲存QoS	QoS原則群組	是的	是的
是的	光纖通道（FC）	否	否	否
iSCSI	否	否	否	LUN
物件	是的	是的	是的	igroup
否	否	否	連接埠集	否
否	否	序號	否	否
否	SNMP	v3使用者	是的	是的

SVM 災難恢復儲存限制

下表顯示每個儲存物件所支援的磁碟區和 SVM 災難恢復關係的建議上限。您應該注意、限制通常取決於平台。請參閱 "Hardware Universe" 以瞭解特定組態的限制。

儲存物件	限制
SVM	300個彈性磁碟區
HA配對	1、000個彈性磁碟區
叢集	128 SVM 災難關係

相關資訊

- "SnapMirror建立"
- "SnapMirror 策略創建"

複寫SVM組態

ONTAP SnapMirror SVM 複寫工作流程

SnapMirror SVM複寫涉及建立目的地SVM、建立複寫工作排程、以及建立和初始化SnapMirror關係。

您應該判斷哪一個複寫工作流程最符合您的需求：

- "複寫整個SVM組態"
- "從SVM複寫中排除LIF及相關的網路設定"
- "從 SVM 組態中排除網路、名稱服務及其他設定"

在 ONTAP SnapMirror 目的地 SVM 上放置 Volume 的條件

將磁碟區從來源SVM複寫到目的地SVM時、請務必瞭解選取Aggregate的條件。

根據下列條件選取Aggregate：

- 磁碟區一律放在非根Aggregate上。
- 非根Aggregate是根據可用的可用空間和已裝載於Aggregate上的磁碟區數量來選取。

  具有更多可用空間和較少磁碟區的集合體會被優先分配。選取具有最高優先順序的Aggregate。

- 來源磁碟區FabricPool 位於目的地FabricPool 的Sichaggregate上、具有相同的分層原則。
- 如果來源SVM上的磁碟區位於Flash Pool Aggregate上、則該磁碟區會放置在目的地SVM上的Flash Pool Aggregate上、如果有此類Aggregate存在且有足夠的可用空間。
- 如果是 `-space-guarantee` 複寫的磁碟區選項設為 `volume`，只有可用空間大於 Volume 大小的集合體才會被視為。
- 根據來源Volume大小、在複寫期間、目的地SVM上的Volume大小會自動增加。

  如果您要預先保留目的地SVM的大小、則必須調整磁碟區大小。磁碟區大小不會根據來源SVM在目的地SVM上自動縮小。

如果您想要將磁碟區從一個集合體移到另一個集合體、可以使用 `volume move` 目的地 SVM 上的命令。

複寫整個 ONTAP SVM 組態

您可以建立 SVM 災難恢復（ SVM DR ）關係、將一個 SVM 組態複寫到另一個。在主要站台發生災難時、您可以快速啟動目的地 SVM 。

開始之前

來源與目的地叢集和SVM必須進行對等關係。
如需詳細資訊、請參閱 "建立叢集對等關係" 和 "建立SVM叢集間對等關係"。

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

關於這項工作

此工作流程假設您已使用預設原則或自訂複寫原則。

從 ONTAP 9.9.1 開始，當您使用鏡射資料保險箱原則時，可以在來源和目的地 SVM 上建立不同的快照原則，而目的地上的快照不會被來源上的快照覆寫。如需更多資訊、請參閱 "瞭解SnapMirror SVM複寫"。

請從目的地完成此程序。如果您需要建立新的保護原則、例如、當來源儲存 VM 已設定 SMB 時、您應該建立原則並使用 * Identity Preserve * 選項。如需詳細資訊、請參閱 "建立自訂資料保護原則"。

步驟

您可以從系統管理員或 ONTAP CLI 執行此工作。

系統管理員

1. 在目的地叢集上、按一下*保護>關係*。
2. 在 * 關係 * 下、按一下 * 保護 * 、然後選擇 * 儲存 VM （ DR ） * 。
3. 選取保護原則。如果您已建立自訂保護原則、請選取該原則、然後選擇您要複寫的來源叢集和儲存VM。您也可以輸入新的儲存VM名稱來建立新的目的地儲存VM。
4. 如有需要、請變更目的地設定以覆寫身分保留、並納入或排除網路介面和傳輸協定。
5. 按一下「 * 儲存 * 」。

CLI

1. 建立目的地SVM：

   ```
   vserver create -vserver <SVM_name> -subtype dp-destination
   ```

   SVM名稱在來源叢集和目的地叢集之間必須是唯一的。

   下列範例建立名為的目的地 SVM `svm_backup`：

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-
   destination
   ```

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

2. 從目的地叢集、使用建立 SVM 對等關係 `vserver peer create` 命令。

   如需詳細資訊、請參閱 "建立SVM叢集間對等關係"。

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

3. 建立複寫工作排程：

   ```
   job schedule cron create -name <job_name> -month <month> -dayofweek
   <day_of_week> -day <day_of_month> -hour <hour> -minute <minute>
   ```

   適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

   > SVM SnapMirror 關係中 FlexVol Volume 的最低支援排程（ RPO ）為 15 分鐘。SVM SnapMirror 關係中 FlexGroup Volume 的最低支援排程（ RPO ）為 30 分鐘。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

```
cluster_dst::> job schedule cron create -name my_weekly -dayofweek
saturday -hour 3 -minute 0
```

如"指令參考資料ONTAP"需詳細 `job schedule cron create`資訊，請參閱。

4. 從目的地SVM或目的地叢集建立複寫關係：

```
snapmirror create -source-path <SVM_name>: -destination-path
<SVM_name>: -type <DP|XDP> -schedule <schedule> -policy <policy>
-identity-preserve true
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：

以下範例使用預設值建立 SnapMirror DR 關係 `MirrorAllSnapshots` 原則：

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy
MirrorAllSnapshots -identity-preserve true
```

下列範例使用預設值建立統一化的複寫關係 `MirrorAndVault` 原則：

```
cluster_dst:> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy MirrorAndVault
-identity-preserve true
```

假設您已建立具有原則類型的自訂原則 `async-mirror`下例建立 SnapMirror DR 關係：

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_mirrored
-identity-preserve true
```

假設您已建立具有原則類型的自訂原則 `mirror-vault`下例建立統一的複寫關係：

```
cluster_dst::> snapmirror create -source-path svm1: -destination
-path svm_backup: -type XDP -schedule my_daily -policy my_unified
-identity-preserve true
```

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

5. 停止目的地SVM：

```
vserver stop -vserver <SVM_name>
```

下列範例會停止名為 SVM_backup 的目的地 SVM ：

```
cluster_dst::> vserver stop -vserver svm_backup
```

如"指令參考資料ONTAP"需詳細 `vserver stop`資訊，請參閱。

6. 從目的地SVM或目的地叢集、初始化SVM複寫關係：

```
snapmirror initialize -source-path <SVM_name>: -destination-path
<SVM_name>:
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination -path` 選項：

以下範例初始化來源 SVM 之間的關係、 `svm1`以及目的地 `SVM` 、 `svm_backup`：

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

從 **ONTAP SnapMirror SVM** 複寫中排除生命與相關網路設定

如果來源和目的地 SVM 位於不同的子網路、您可以使用 `-discard-configs network` 的選項 `snapmirror policy create` 從 SVM 複寫中排除生命與相關網路設定的命令。

開始之前

來源與目的地叢集和SVM必須進行對等關係。

如需詳細資訊、請參閱 "建立叢集對等關係" 和 "建立SVM叢集間對等關係"。

關於這項工作

。 `-identity-preserve` 的選項 `snapmirror create` 命令必須設為 `true` 當您建立 SVM 複寫關係時。

步驟

1. 建立目的地SVM：

```
vserver create -vserver SVM -subtype dp-destination
```

SVM名稱在來源叢集和目的地叢集之間必須是唯一的。

下列範例建立名為的目的地 SVM `svm_backup`：

```
cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
```

2. 從目的地叢集、使用建立 SVM 對等關係 `vserver peer create` 命令。

   如需詳細資訊、請參閱 "建立SVM叢集間對等關係"。

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

3. 建立工作排程：

   ```
   job schedule cron create -name job_name -month month -dayofweek day_of_week
   -day day_of_month -hour hour -minute minute
   ```

   適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

   > SVM SnapMirror 關係中 FlexVol Volume 的最低支援排程（ RPO ）為 15 分鐘。SVM SnapMirror 關係中 FlexGroup Volume 的最低支援排程（ RPO ）為 30 分鐘。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. 建立自訂複寫原則：

   ```
   snapmirror policy create -vserver SVM -policy policy -type async-
   mirror|vault|mirror-vault -comment comment -tries transfer_tries -transfer
   -priority low|normal -is-network-compression-enabled true|false -discard
   -configs network
   ```

   以下範例為SnapMirror DR建立自訂複寫原則、排除LIF：

   ```
   cluster_dst::> snapmirror policy create -vserver svm1 -policy
   DR_exclude_LIFs -type async-mirror -discard-configs network
   ```

   下列範例會建立自訂的複寫原則、以利統一化複寫、不含lifs：

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy
unified_exclude_LIFs -type mirror-vault -discard-configs network
```

考慮在來源叢集上建立相同的自訂 SnapMirror 原則、以供未來容錯移轉和容錯回復案例使用。

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

5. 從目的地SVM或目的地叢集、執行下列命令以建立複寫關係：

```
snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP
-schedule schedule -policy policy -identity-preserve true|false -discard
-configs true|false
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱下列範例。

以下範例建立SnapMirror DR關係、排除LIF：

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy DR_exclude_LIFs
-identity-preserve true
```

以下範例建立SnapMirror統一化複寫關係、排除lifs：

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_weekly -policy unified_exclude_LIFs
-identity-preserve true -discard-configs true
```

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

6. 停止目的地SVM：

```
vserver stop
```

SVM name

下列範例會停止名為 SVM_backup 的目的地 SVM ：

```
cluster_dst::> vserver stop -vserver svm_backup
```

7. 從目的地SVM或目的地叢集初始化複寫關係：

```
snapmirror initialize -source-path SVM: -destination-path SVM:
```

以下範例初始化來源之間的關係、 `svm1` 以及目的地、 `svm_backup`：

```
cluster_dst::> snapmirror initialize -source-path svm1: -destination
-path svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

完成後

您必須在目的地SVM上設定網路和傳輸協定、以便在發生災難時存取資料。

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略創建"

使用 **ONTAP** 從 **SVM** 複寫中排除網路，名稱服務及其他設定

您可能想要從 SVM 複寫關係中排除網路，名稱服務和其他設定，以避免與目的地 SVM 發生衝突或組態差異。

您可以使用 `-identity-preserve false` 的選項 `snapmirror create` 僅複寫 SVM 的磁碟區和安全組態的命令。部分傳輸協定和名稱服務設定也會保留下來。

關於這項工作

如需保留的傳輸協定和名稱服務設定清單、請參閱 "在SVM DR關係中複寫的組態"。

開始之前

來源與目的地叢集和SVM必須進行對等關係。

如需詳細資訊、請參閱 "建立叢集對等關係" 和 "建立SVM叢集間對等關係"。

步驟

1. 建立目的地SVM：

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

   SVM名稱在來源叢集和目的地叢集之間必須是唯一的。

   下列範例建立名為的目的地 SVM `svm_backup`：

   ```
   cluster_dst:> vserver create -vserver svm_backup -subtype dp-destination
   ```

2. 從目的地叢集、使用建立 SVM 對等關係 `vserver peer create` 命令。

   如需詳細資訊、請參閱 "建立SVM叢集間對等關係"。

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

3. 建立複寫工作排程：

   `job schedule cron create -name job_name -month month -dayofweek day_of_week -day day_of_month -hour hour -minute minute`

   適用於 `-month`、 `-dayofweek`和 `-hour`，您可以指定 `all` 可分別在每月、每週的某一天和每小時運行作業。

   > SVM SnapMirror 關係中 FlexVol Volume 的最低支援排程（ RPO ）為 15 分鐘。SVM SnapMirror 關係中 FlexGroup Volume 的最低支援排程（ RPO ）為 30 分鐘。

   以下範例建立名為的工作排程 `my_weekly` 週六上午 3 ： 00 開始：

   ```
   cluster_dst::> job schedule cron create -name my_weekly -dayofweek
   "Saturday" -hour 3 -minute 0
   ```

4. 建立不含網路、名稱服務及其他組態設定的複寫關係：

   `snapmirror create -source-path SVM: -destination-path SVM: -type DP|XDP -schedule schedule -policy policy -identity-preserve false`

   > 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱下列範例。 您必須從目的地SVM或目的地叢集執行此命令。

   以下範例使用預設值建立 SnapMirror DR 關係 `MirrorAllSnapshots` 原則。此關係不包括網路、名稱服務及其他組態設定、不包括SVM複寫：

   ```
   cluster_dst::> snapmirror create -source-path svm1: -destination-path
   svm_backup: -type XDP -schedule my_daily -policy MirrorAllSnapshots
   -identity-preserve false
   ```

   下列範例使用預設值建立統一化的複寫關係 `MirrorAndVault` 原則。此關係不包括網路、名稱服務及其他組態設定：

   ```
   cluster_dst:> snapmirror create svm1: -destination-path svm_backup:
   -type XDP -schedule my_daily -policy MirrorAndVault -identity-preserve
   false
   ```

   假設您已建立具有原則類型的自訂原則 `async-mirror`下例建立 SnapMirror DR 關係。此關係不包括網路、名稱服務及其他組態設定、不包括SVM複寫：

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_mirrored -identity
-preserve false
```

假設您已建立具有原則類型的自訂原則 `mirror-vault`下例建立統一的複寫關係。此關係不包括網路、名稱服務及其他組態設定、不包括SVM複寫：

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup: -type XDP -schedule my_daily -policy my_unified -identity
-preserve false
```

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

5. 停止目的地SVM：

   `vserver stop`

   `SVM name`

   下列範例會停止名為DV1的目的地SVM：

   ```
   destination_cluster::> vserver stop -vserver dvs1
   ```

6. 如果您使用SMB、也必須設定SMB伺服器。

   請參閱 "僅限SMB：建立SMB伺服器"。

7. 從目的地SVM或目的地叢集、初始化SVM複寫關係：

   `snapmirror initialize -source-path` *`SVM_name`*`: -destination-path` *`SVM_name`*`:`

   如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

完成後

您必須在目的地SVM上設定網路和傳輸協定、以便在發生災難時存取資料。

指定用於 **ONTAP SnapMirror SVM DR** 關係的本機層

建立災難恢復 SVM 之後，您可以使用 `aggr-list`選項搭配 `vserver modify`命令來限制用來裝載 SVM DR 目的地 Volume 的本機層。

步驟

1. 建立目的地SVM：

   `vserver create -vserver` *`SVM`* `-subtype dp-destination`

2. 修改災難恢復 SVM 的 Aggr-list 以限制用於託管災難恢復 SVM 卷的本地層：

```
cluster_dest::> vserver modify -vserver SVM -aggr-list <comma-separated-list>
```

在 DR 關係中為 ONTAP SnapMirror 目的地 SVM 建立 SMB 伺服器

如果來源 SVM 具有 SMB 組態，而且您選擇設定 `identity-preserve`為 `false`，則必須為目的地 SVM 建立 SMB 伺服器。某些 SMB 組態需要 SMB 伺服器，例如 SnapMirror 關係初始化期間的共用區。

步驟

1. 使用命令啟動目的地 SVM `vserver start` 。

```
destination_cluster::> vserver start -vserver dvs1
[Job 30] Job succeeded: DONE
```

如"指令參考資料ONTAP"需詳細 `vserver start`資訊，請參閱。

2. 確認目的地 SVM 位於中 `running` 狀態和子類型為 `dp-destination` 使用 `vserver show` 命令。

```
destination_cluster::> vserver show
                                    Admin      Operational Root
Vserver  Type    Subtype            State      State       Volume
Aggregate
-------- ------- ----------       ---------- ----------- ----------
----------
dvs1     data    dp-destination    running    running       -         -
```

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

3. 使用建立 LIF `network interface create` 命令。

```
destination_cluster::>network interface create -vserver dvs1 -lif NAS1
-role data -data-protocol cifs -home-node destination_cluster-01 -home
-port a0a-101  -address 192.0.2.128 -netmask 255.255.255.128
```

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

4. 使用建立航線 `network route create` 命令。

```
destination_cluster::>network route create -vserver dvs1 -destination
0.0.0.0/0
-gateway 192.0.2.1
```

"網路管理"

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

5. 使用設定 DNS `vserver services dns create` 命令。

```
destination_cluster::>vserver services dns create -domains
mydomain.example.com -vserver
dvs1 -name-servers 192.0.2.128 -state enabled
```

如"指令參考資料ONTAP"需詳細 `vserver services dns create`資訊，請參閱。

6. 使用新增慣用的網域控制站 `vserver cifs domain preferred-dc add` 命令。

```
destination_cluster::>vserver cifs domain preferred-dc add -vserver dvs1
-preferred-dc
192.0.2.128 -domain mydomain.example.com
```

如"指令參考資料ONTAP"需詳細 `vserver cifs domain preferred-dc add`資訊，請參閱。

7. 使用建立 SMB 伺服器 `vserver cifs create` 命令。

```
destination_cluster::>vserver cifs create -vserver dvs1 -domain
mydomain.example.com
-cifs-server CIFS1
```

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

8. 使用停止目的地 SVM `vserver stop` 命令。

```
destination_cluster::> vserver stop -vserver dvs1
[Job 46] Job succeeded: DONE
```

如"指令參考資料ONTAP"需詳細 `vserver stop`資訊，請參閱。

從 **ONTAP SnapMirror SVM DR** 關係中排除磁碟區

根據預設、會複寫來源SVM的所有RW資料磁碟區。如果您不想保護來源 SVM 上的所有磁

碟區、可以使用 `-vserver-dr-protection unprotected` 的選項 `volume modify` 從 SVM 複寫中排除磁碟區的命令。

步驟

1. 從SVM複寫中排除磁碟區：

   `volume modify -vserver *SVM* -volume *volume* -vserver-dr-protection unprotected`

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

   以下範例排除磁碟區 `volA_src` 從 SVM 複寫：

   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection unprotected
   ```

   如果您稍後想要在原本排除的SVM複寫中加入一個Volume、請執行下列命令：

   `volume modify -vserver *SVM* -volume *volume* -vserver-dr-protection protected`

   以下範例包括 Volume `volA_src` 在 SVM 複寫中：

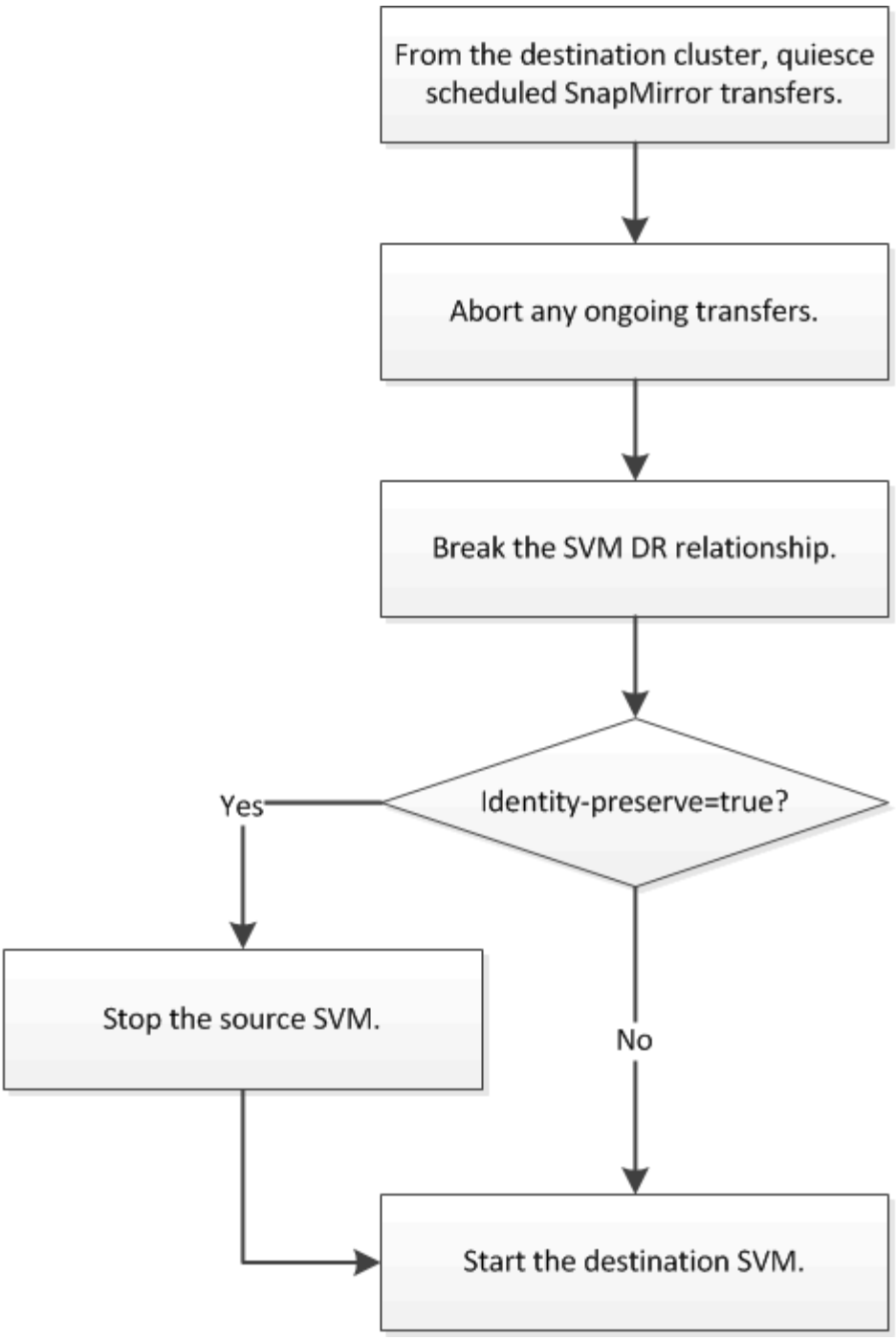
   ```
   cluster_src::> volume modify -vserver SVM1 -volume volA_src -vserver-dr
   -protection protected
   ```

2. 如所述建立及初始化SVM複寫關係 "複寫整個SVM組態"。

從 **SnapMirror SVM DR** 目的地提供資料

ONTAP SnapMirror SVM 災難恢復工作流程

若要從災難中恢復並從目的地SVM提供資料、您必須啟動目的地SVM。啟動目的地SVM包括停止排程的SnapMirror傳輸、中止進行中的SnapMirror傳輸、打破複寫關係、停止來源SVM、以及啟動目的地SVM。



將 **ONTAP SnapMirror SVM** 目的地 **Volume** 設定為可寫入

您必須先將SVM目的地磁碟區設為可寫入、才能將資料提供給用戶端。

此程序與磁碟區複寫程序大致相同、但有一項例外。如果您在建立 SVM 複寫關係時設定 `-identity -preserve true` 、則必須先停止來源 SVM 、然後再啟動目的地 SVM 。

關於這項工作

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

在災難恢復案例中、您無法從來源SVM執行SnapMirror更新至災難恢復目的地SVM、因為您的來源SVM及其資料將無法存取、而且自上次重新同步後的更新可能損毀或毀損。

從功能介紹9.8開始ONTAP 、您可以在災難發生後、使用System Manager啟動目的地儲存VM。啟動目的地儲存VM會使SVM目的地磁碟區可寫入、並可讓您將資料提供給用戶端。

步驟

您可以從系統管理員或 ONTAP CLI 執行此工作。

系統管理員

1. 如果可以存取來源叢集、請確認SVM已停止：瀏覽至* Storage > Storage VMS*、然後查看SVM的* State *欄。
2. 如果來源 SVM 狀態為「執行中」、請停止：選取 ⋮ 並選擇 * 停止 * 。
3. 在目的地叢集上、找到所需的保護關係：瀏覽至*保護>關係*。
4. 將游標移至所需的來源儲存 VM 名稱上、按一下 ⋮、然後選擇 * 啟動目的地儲存 VM* 。
5. 在 * 啟動目的地儲存 VM* 視窗中、選取 * 啟動目的地儲存 VM 並中斷關係 * 。
6. 按一下「啟動」。

CLI

1. 從目標 SVM 或目標集群，使 SVM 處於靜默狀態以停止到目標的計劃傳輸：

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會停止來源 SVM 之間的排程傳輸 `svm1` 以及目的地 SVM `svm_backup`：

```
cluster_dst::> snapmirror quiesce -source-path svm1: -destination
-path svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

2. 從目的地SVM或目的地叢集停止持續傳輸至目的地：

```
snapmirror abort -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會停止來源 SVM 之間的持續傳輸 `svm1` 以及目的地 SVM `svm_backup`：

```
cluster_dst::> snapmirror abort -source-path svm1: -destination-path
svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror abort`資訊，請參閱。

3. 從目的地SVM或目的地叢集、中斷複寫關係：

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例打破來源 SVM 之間的關係 `svm1` 以及目的地 SVM `svm_backup`：

```
cluster_dst::> snapmirror break -source-path svm1: -destination-path
svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

4. 如果您已設定 `-identity-preserve true` 建立 SVM 複寫關係時、請停止來源 SVM ：

```
vserver stop -vserver <SVM>
```

下列範例會停止來源 SVM `svm1`：

```
cluster_src::> vserver stop svm1
```

5. 啟動目的地SVM：

```
vserver start -vserver <SVM>
```

下列範例會啟動目的地 SVM `svm_backup`：

```
cluster_dst::> vserver start svm_backup
```

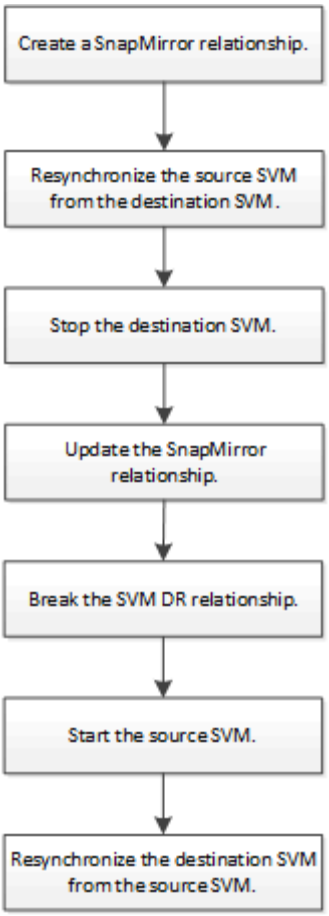
完成後

如所述、設定SVM目的地磁碟區以進行資料存取 "設定目的地Volume以進行資料存取"。

重新啟動 SnapMirror 來源 SVM

ONTAP SnapMirror 來源 SVM 重新啟用工作流程

如果來源SVM發生災難後仍存在、您可以重新啟動它、並重新建立SVM災難恢復關係來保護它。



重新啟動原始 **ONTAP SnapMirror** 來源 **SVM**

當您不再需要從目的地提供資料時、可以重新建立來源SVM與目的地SVM之間的原始資料保護關係。此程序與磁碟區複寫程序大致相同、但有一項例外。在重新啟動來源SVM之前、您必須先停止目的地SVM。

開始之前

- 如果您在處理資料時增加了目的地Volume的大小、則在重新啟動來源Volume之前、您應該手動增加原始來源Volume的最大自動大小、以確保其能夠充分擴充。

"當目的地Volume自動成長時"

叢集管理員應在重新啟動原始來源 SVM 之前暫停客戶端的寫入操作，以避免資料遺失。

關於這項工作

從 ONTAP 9 。 11.1 開始、您可以 `-quick-resync true` `snapmirror resync`在執行 SVM DR 關係的反向重新同步時、使用命令的 CLI 選項、縮短災難恢復排練期間的重新同步時間。快速重新同步可繞過資料倉儲的重建與還原作業、縮短返回正式作業所需的時間。如"指令參考資料ONTAP"需詳細 `snapmirror resync`資訊，請參閱。

快速重新同步並不會保留目的地磁碟區的儲存效率。啟用快速重新同步可能會增加目的地磁碟區所使用的磁碟區空間。

此程序假設原始來源Volume中的基準線不變。如果基準不完整、您必須先建立並初始化您要從中處理資料的磁

碟區與原始來源磁碟區之間的關係、然後再執行程序。

從ONTAP 9.8 開始，您可以使用系統管理員在災難發生後重新啟動來源儲存 VM。

步驟

您可以使用系統管理員或ONTAP CLI 執行此任務。

系統管理器**ONTAP 9.17.1** 及更高版本

1. 在目標叢集上，選擇所需的保護關係：按一下「保護」>「複製」。
2. 將滑鼠懸停在來源名稱上，然後按一下 ⋮ 然後點選“反向同步”。
3. 在 * 反向重新同步關係 * 視窗中、按一下 * 反向重新同步 * 。

   此關係從 複製 表中消失，現在由原始來源叢集管理。

4. 在原始來源叢集上，按一下“保護”>“複製”，然後檢查狀態是否顯示“已鏡像”，以驗證反向重新同步是否完成。
5. 在原始目標叢集上，導覽至*叢集 > 儲存虛擬機器*。
6. 找到儲存虛擬機，將遊標懸停在儲存虛擬機名稱上，然後按一下 ⋮ 然後點擊“停止”。
7. 在「停止儲存虛擬機器」視窗中，按一下「停止」。
8. 在來源叢集上，導覽至“保護”>“複製”，找到要重新啟動的儲存虛擬機，將遊標懸停在儲存虛擬機名稱上，然後按一下 ⋮ 然後按一下「啟動目標儲存 VM」。
9. 在“啟動目標儲存 VM”視窗中，選擇“啟動目標儲存 VM 並斷開連接”，然後按一下“啟動”。
10. 返回「複製」頁面後，再次將遊標懸停在儲存虛擬機器名稱上，然後按一下 ⋮ 然後點選“反向同步”。

系統管理器**ONTAP 9.16.1** 及更早版本

1. 在目標叢集上，選擇所需的保護關係：按一下「保護」>「關係」。
2. 將滑鼠懸停在來源名稱上，然後按一下 ⋮ 然後點選“反向同步”。
3. 在 * 反向重新同步關係 * 視窗中、按一下 * 反向重新同步 * 。

   由於該關係現在由原始來源叢集管理，因此該關係從 關係 表中消失。

4. 在原始來源叢集上，按一下“保護 > 關係”，然後檢查狀態是否顯示為“已鏡像”，以驗證反向重新同步是否完成。
5. 在原始目標叢集上，導覽至「儲存 > 儲存虛擬機器」。
6. 找到儲存虛擬機，將遊標懸停在儲存虛擬機名稱上，然後按一下 ⋮ 然後點擊“停止”。
7. 在「停止儲存虛擬機器」視窗中，按一下「停止」。
8. 在來源叢集上，找到儲存虛擬機器（現在是反向關係中的來源 SVM），將遊標停留在 SVM 名稱上，然後按一下 ⋮ 然後按一下「啟動目標儲存 VM」。
9. 在“啟動目標儲存 VM”視窗中，選擇“啟動目標儲存 VM 並斷開連接”，然後按一下“啟動”。
10. 返回「關係」頁面後，再次將遊標懸停在儲存虛擬機器名稱上，然後按一下 ⋮ 然後點選“反向同步”。

CLI

1. 從原始來源SVM或原始來源叢集、使用與原始SVM DR關係相同的組態、原則及身分保留設定、建立反向SVM DR關係：

```
snapmirror create -source-path <SVM>: -destination-path <SVM>:
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例在您用來提供資料的 SVM 之間建立關係、 `svm_backup`和原始來源 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror create -source-path svm_backup:
-destination-path svm1:
```

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

2. 從原始來源SVM或原始來源叢集、執行下列命令以反轉資料保護關係：

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

如果來源和目的地上不存在一般快照，則命令會失敗。用於 `snapmirror initialize`重新初始化關係。

以下範例反轉原始來源 SVM 之間的關係、 `svm1`以及您要從中提供資料的 `SVM` 、 `svm_backup`：

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1:
```

使用-quick重新同步選項的範例：

```
cluster_src::> snapmirror resync -source-path svm_backup:
-destination-path svm1: -quick-resync true
```

3. 當您準備重新建立對原始來源SVM的資料存取時、請停止原始目的地SVM、以中斷目前連線至原始目的地SVM的所有用戶端。

```
vserver stop -vserver <SVM>
```

下列範例會停止目前正在處理資料的原始目的地SVM：

```
cluster_dst::> vserver stop svm_backup
```

4. 使用驗證原始目的地 SVM 是否處於停止狀態 `vserver show` 命令。

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default    stopped    stopped     rv
aggr1
```

5. 從原始來源SVM或原始來源叢集、執行下列命令以執行反向關係的最終更新、將所有變更從原始目的地SVM傳輸至原始來源SVM：

```
snapmirror update -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例更新了您用來提供資料的原始目的地 SVM 之間的關係,`svm_backup`和原始來源 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror update -source-path svm_backup:
-destination-path svm1:
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

6. 從原始來源SVM或原始來源叢集、執行下列命令停止針對反向關係所排程的傳輸：

```
snapmirror quiesce -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會停止您要從哪個 SVM 傳送資料、 `svm_backup`和原始 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror quiesce -source-path svm_backup:
-destination-path svm1:
```

7. 當完成最後的更新、且關係指出關係狀態為「靜止」時、請從原始來源SVM或原始來源叢集執行下列命令、以中斷反向關係：

```
snapmirror break -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例打破了您用來提供資料的原始目的地 SVM 之間的關係、 `svm_backup`和原始來源 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror break -source-path svm_backup:
-destination-path svm1:
```

如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

8. 如果原始來源SVM先前已停止、請從原始來源叢集啟動原始來源SVM：

```
vserver start -vserver <SVM>
```

下列範例會啟動原始來源SVM：

```
cluster_src::> vserver start svm1
```

9. 從原始目的地SVM或原始目的地叢集重新建立原始資料保護關係：

```
snapmirror resync -source-path <SVM>: -destination-path <SVM>:
```

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例重新建立原始來源 SVM 之間的關係、 `svm1`和原始目的地 `SVM` 、 `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1: -destination
-path svm_backup:
```

10. 從原始來源SVM或原始來源叢集、執行下列命令以刪除反轉的資料保護關係：

```
snapmirror delete -source-path <SVM>: -destination-path <SVM>:
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例刪除原始目的地 SVM 之間的反向關係、 `svm_backup`和原始來源 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror delete -source-path svm_backup:
-destination-path svm1:
```

11. 從原始目的地SVM或原始目的地叢集、釋出反轉的資料保護關係：

```
snapmirror release -source-path <SVM>: -destination-path <SVM>:
```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會釋出原始目的地 SVM 、 SVM_backup 與原始來源 SVM 之間的反向關係、 `svm1`

```
cluster_dst::> snapmirror release -source-path svm_backup:
-destination-path svm1:
```

下一步

- 使用 `snapmirror show` 用於驗證 SnapMirror 關係是否已建立的命令。

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

- 從客戶端還原對原始來源 SVM 的寫入操作。

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror初始化"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

重新啟動 **FlexGroup Volume** 的原始 **ONTAP SnapMirror** 來源 **SVM**

當您不再需要從目的地提供資料時、可以重新建立來源SVM與目的地SVM之間的原始資料保護關係。若要在使用FlexGroup 完SVM時重新啟動原始來源SVM、您需要執行一些其他步驟、包括刪除原始SVM DR關係、並在反轉關係之前釋出原始關係。您也需要釋出反轉

的關係、並在停止排程傳輸之前重新建立原始關係。

步驟

1. 從原始目的地SVM或原始目的地叢集刪除原始SVM DR關係：

   ```
   snapmirror delete -source-path SVM: -destination-path SVM:
   ```

   > 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例刪除原始來源 SVM 、 svm1 和原始目的地 SVM 之間的原始關係、 `svm_backup`：

   ```
   cluster_dst::> snapmirror delete -source-path svm1: -destination-path
   svm_backup:
   ```

2. 從原始來源 SVM 或原始來源叢集，釋放原始關係，同時保持快照不變：

   ```
   snapmirror release -source-path SVM: -destination-path SVM: -relationship-info
   -only true
   ```

   > 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例發佈原始來源 SVM 、 svm1 和原始目的地 SVM 之間的原始關係、 `svm_backup`。

   ```
   cluster_src::> snapmirror release -source-path svm1: -destination-path
   svm_backup: -relationship-info-only true
   ```

3. 從原始來源SVM或原始來源叢集、使用與原始SVM DR關係相同的組態、原則及身分保留設定、建立反向SVM DR關係：

   ```
   snapmirror create -source-path SVM: -destination-path SVM:
   ```

   > 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例在您用來提供資料的 SVM 之間建立關係、 `svm_backup`和原始來源 `SVM 、 `svm1`：

   ```
   cluster_src::> snapmirror create -source-path svm_backup: -destination
   -path svm1:
   ```

4. 從原始來源SVM或原始來源叢集、執行下列命令以反轉資料保護關係：

   ```
   snapmirror resync -source-path SVM: -destination-path SVM:
   ```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

如果來源和目的地上不存在一般快照，則命令會失敗。用於 `snapmirror initialize`重新初始化關係。

以下範例反轉原始來源 SVM 之間的關係、 `svm1`以及您要從中提供資料的 `SVM` 、 `svm_backup`：

```
cluster_src::> snapmirror resync -source-path svm_backup: -destination
-path svm1:
```

5. 當您準備重新建立對原始來源SVM的資料存取時、請停止原始目的地SVM、以中斷目前連線至原始目的地SVM的所有用戶端。

   `vserver stop -vserver` *SVM*

   下列範例會停止目前正在處理資料的原始目的地SVM：

```
cluster_dst::> vserver stop svm_backup
```

6. 使用驗證原始目的地 SVM 是否處於停止狀態 `vserver show` 命令。

```
cluster_dst::> vserver show
                                 Admin      Operational Root
Vserver        Type    Subtype   State      State       Volume
Aggregate
--------       ------- ---------- ---------- ----------- ----------
----------
svm_backup     data    default   stopped    stopped     rv
aggr1
```

7. 從原始來源SVM或原始來源叢集、執行下列命令以執行反向關係的最終更新、將所有變更從原始目的地SVM傳輸至原始來源SVM：

   `snapmirror update -source-path` *SVM*`:` `-destination-path` *SVM*`:`

   您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例更新了您用來提供資料的原始目的地 SVM 之間的關係,`svm_backup`和原始來源 `SVM` 、 `svm1`：

```
cluster_src::> snapmirror update -source-path svm_backup: -destination
-path svm1:
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

8. 從原始來源SVM或原始來源叢集、執行下列命令停止針對反向關係所排程的傳輸：

   `snapmirror quiesce -source-path` *SVM*`: -destination-path` *SVM*`:`

   您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   下列範例會停止您要從哪個 SVM 傳送資料、 `svm_backup`和原始 `SVM` 、 `svm1`：

   ```
   cluster_src::> snapmirror quiesce -source-path svm_backup: -destination
   -path svm1:
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror quiesce`資訊，請參閱。

9. 當完成最後的更新、且關係指出關係狀態為「靜止」時、請從原始來源SVM或原始來源叢集執行下列命令、以中斷反向關係：

   `snapmirror break -source-path` *SVM*`: -destination-path` *SVM*`:`

   您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例打破了您用來提供資料的原始目的地 SVM 之間的關係、 `svm_backup`和原始來源 `SVM` 、 `svm1`：

   ```
   cluster_src::> snapmirror break -source-path svm_backup: -destination
   -path svm1:
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

10. 如果原始來源SVM先前已停止、請從原始來源叢集啟動原始來源SVM：

    `vserver start -vserver` *SVM*

    下列範例會啟動原始來源SVM：

    ```
    cluster_src::> vserver start svm1
    ```

11. 從原始來源SVM或原始來源叢集刪除反轉的SVM DR關係：

`snapmirror delete -source-path SVM: -destination-path SVM:`

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例刪除原始目的地 SVM 、 SVM_backup 與原始來源 SVM 之間的反向關係、 `svm1`：

```
cluster_src::> snapmirror delete -source-path svm_backup: -destination
-path svm1:
```

12. 從原始目的地 SVM 或原始目的地叢集，釋放相反的關係，同時保持快照不變：

`snapmirror release -source-path SVM: -destination-path SVM: -relationship-info -only true`

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會釋出原始目的地SVM、SVM_Backup與原始來源SVM、svm1之間的反向關係：

```
cluster_dst::> snapmirror release -source-path svm_backup: -destination
-path svm1: -relationship-info-only true
```

13. 從原始目的地SVM或原始目的地叢集、重新建立原始關係。使用與原始SVM DR關係相同的組態、原則和身分保留設定：

`snapmirror create -source-path SVM: -destination-path SVM:`

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例在原始來源 SVM 之間建立關係、 `svm1`和原始目的地 `SVM 、 `svm_backup`：

```
cluster_dst::> snapmirror create -source-path svm1: -destination-path
svm_backup:
```

14. 從原始目的地SVM或原始目的地叢集重新建立原始資料保護關係：

`snapmirror resync -source-path SVM: -destination-path SVM:`

> 您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例重新建立原始來源 SVM 之間的關係、 `svm1`和原始目的地 `SVM 、 `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror初始化"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"

重新同步 **ONTAP SnapMirror** 目的地 **SVM** 上的資料

執行災難恢復演習時、可選擇跳過完整的資料倉儲重建、讓您更快恢復正式作業。ONTAP

從功能介紹9.8開始ONTAP 、您可以使用System Manager、在保護關係中斷的情況下、重新同步來源儲存VM與目的地儲存VM的資料與組態詳細資料、並重新建立關係。

您只能從原始關係的目的地執行重新同步作業。重新同步會刪除目的地儲存VM中比來源儲存VM中資料新的任何資料。

步驟

您可以使用系統管理員或 ONTAP CLI 來執行此工作。

系統管理員

1. 從目的地選取所需的保護關係：按一下 * 保護 > 關係 * 。
2. （可選）選擇*執行快速重新同步*、以在災難恢復演練期間跳過完整的資料倉儲重建。
3. 按一下 ⋮ 並按一下 * 重新同步 * 。
4. 在*關係*下、檢視*傳輸狀態*以監控關係的重新同步進度。

CLI

1. 從目的地叢集重新同步關係：

```
snapmirror resync -source-path <svm>: -destination-path <svm>:
-quick-resync true|false
```

相關資訊

- "SnapMirror 重新同步"

將 ONTAP SnapMirror Volume DR 關係轉換為 SVM DR 關係

您可以將磁碟區之間的複寫關係、轉換成擁有磁碟區的儲存虛擬機器（SVM）之間的複寫關係、前提是來源（根磁碟區除外）上的每個磁碟區都要複寫、 而且來源（包括根磁碟區）上的每個磁碟區都與目的地上的磁碟區名稱相同。

關於這項工作

如有必要，請在 SnapMirror 關係閒置時使用 `volume rename`命令重新命名目的地 Volume 。如"指令參考資料ONTAP"需詳細 `volume rename`資訊，請參閱。

步驟

1. 從目的地SVM或目的地叢集執行下列命令、重新同步來源與目的地磁碟區：

   ```
   snapmirror resync -source-path <SVM:volume> -destination-path <SVM:volume>
   -type DP|XDP -policy <policy>
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror resync`資訊，請參閱。

   ⓘ 雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

   以下範例重新同步來源 Volume 之間的關係 `volA` 開啟 `svm1` 以及目的地Volume `volA` 開啟 `svm_backup`：

   ```
   cluster_dst::> snapmirror resync -source-path svm1:volA -destination
   -path svm_backup:volA
   ```

2. 如所述、在來源和目的地SVM之間建立SVM複寫關係 "複寫SVM組態"。

   您必須使用 `-identity-preserve true` 的選項 `snapmirror create` 建立複寫關係時的命令。

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

3. 停止目的地SVM：

   ```
   vserver stop -vserver SVM
   ```

   如"指令參考資料ONTAP"需詳細 `vserver stop`資訊，請參閱。

   下列範例會停止目的地 SVM `svm_backup`：

   ```
   cluster_dst::> vserver stop svm_backup
   ```

4. 從目的地SVM或目的地叢集執行下列命令、重新同步來源和目的地SVM：

   ```
   snapmirror resync -source-path <SVM>: -destination-path <SVM>: -type DP|XDP
   -policy <policy>
   ```

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

雖然重新同步不需要基準傳輸、但這可能很耗時。您可能想要在非尖峰時間執行重新同步。

以下範例重新同步來源 SVM 之間的關係 `svm1` 以及目的地 SVM `svm_backup`：

```
cluster_dst::> snapmirror resync -source-path svm1: -destination-path
svm_backup:
```

相關資訊

- "SnapMirror建立"
- "SnapMirror 重新同步"

刪除 ONTAP SnapMirror SVM 複寫關係

您可以使用 `snapmirror delete`和 `snapmirror release`命令來刪除 SVM 複寫關係。然後您可以手動刪除不需要的目的地Volume。如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

關於這項工作

此命令會 `snapmirror release`從來源中刪除任何 SnapMirror 建立的快照。您可以使用 `-relationship-info-only`選項來保留快照。

步驟

1. 從目的地SVM或目的地叢集執行下列命令、以中斷複寫關係：

   `snapmirror break -source-path SVM: -destination-path SVM:`

   您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

   以下範例打破來源 SVM 之間的關係 `svm1` 以及目的地 SVM `svm_backup`：

   ```
   cluster_dst::> snapmirror break -source-path svm1: -destination-path
   svm_backup:
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror break`資訊，請參閱。

2. 從目的地SVM或目的地叢集執行下列命令、以刪除複寫關係：

   `snapmirror delete -source-path SVM: -destination-path SVM:`

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

以下範例刪除來源 SVM 之間的關係 `svm1` 以及目的地 SVM `svm_backup`：

```
cluster_dst::> snapmirror delete -source-path svm1: -destination-path
svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror delete`資訊，請參閱。

3. 從來源叢集或來源SVM執行下列命令、以從來源SVM釋出複寫關係資訊：

`snapmirror release -source-path` *SVM*`: -destination-path` *SVM*`:`

您必須在中的 SVM 名稱後面輸入一個冒號（：） `-source-path` 和 `-destination-path` 選項：請參閱以下範例。

下列範例會從來源 SVM 發佈指定複寫關係的資訊 `svm1`：

```
cluster_src::> snapmirror release -source-path svm1: -destination-path
svm_backup:
```

如"指令參考資料ONTAP"需詳細 `snapmirror release`資訊，請參閱。

管理SnapMirror根Volume複寫

瞭解 ONTAP SnapMirror 根磁碟區複寫

NAS環境中的每個SVM都有獨特的命名空間。SVM根磁碟區（包含作業系統和相關資訊）是命名空間階層的起點。為了確保在節點中斷或容錯移轉的情況下、用戶端仍可存取資料、您應該建立SVM根磁碟區的負載共用鏡射複本。

SVM根磁碟區的負載共用鏡像主要用途不再是用於負載共用、而是用於災難恢復。

- 如果根磁碟區暫時無法使用、負載共用鏡像會自動提供root Volume資料的唯讀存取權。
- 如果根磁碟區永久無法使用、您可以升級其中一個負載共用磁碟區、以提供對根磁碟區資料的寫入存取權。

建立並初始化 ONTAP 負載共用鏡射關係

您應該為叢集中提供 NAS 資料的每個 SVM 根磁碟區建立一個負載共用映像 (LSM)。對於包含兩個或更多 HA 對的集群，您應該考慮使用 SVM 根卷的負載共享鏡像，以確保在 HA 對的兩個節點都發生故障時，客戶端仍然可以存取命名空間。負載共享鏡像不適用於包含單一 HA 對的叢集。

開始之前

從ONTAP 9.16.1 開始，當您建立負載共享鏡像關係時，目標 SVM 無法啟用儲存限制。

關於這項工作

如果您在同一個節點上建立LSM、但該節點無法使用、則會發生單一故障點、而且您沒有第二個複本、無法確保用戶端仍可存取資料。但是、當您在含有根磁碟區的節點以外的節點上建立LSM、或是在不同的HA配對上建立LSM時、資料仍可在中斷時存取。

例如、在四節點叢集中、三個節點上有根磁碟區：

- 對於HA 1節點1上的根磁碟區、請在HA 2節點1或HA 2節點2上建立LSM。
- 對於HA 1節點2上的根磁碟區、請在HA 2節點1或HA 2節點2上建立LSM。
- 對於HA 2節點1上的根磁碟區、請在HA 1節點1或HA 1節點2上建立LSM。

步驟

1. 建立LSM的目的地Volume：

```
volume create -vserver <SVM> -volume <volume> -aggregate <aggregate>
-type DP -size <size>
```

目的地Volume的大小應與根Volume相同或更大。

最佳做法是使用後綴（例如）來命名根卷和目標卷 `_root` 和 `_m1`。

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

以下範例為根磁碟區建立負載共用鏡射磁碟區 `svm1_root` 在中 `cluster_src`：

```
cluster_src:> volume create -vserver svm1 -volume svm1_m1 -aggregate
aggr_1 -size 1gb -state online -type DP
```

2. "建立複製工作排程"。
3. 在SVM根磁碟區與LSM目的地磁碟區之間建立負載共用鏡射關係：

```
snapmirror create -source-path <SVM:volume> -destination-path
<SVM:volume> -type LS -schedule <schedule>
```

以下範例在根磁碟區之間建立負載共用鏡像關係 `svm1_root` 以及負載共用鏡射磁碟區 `svm1_m1`：

```
cluster_src::> snapmirror create -source-path svm1:svm1_root
-destination-path svm1:svm1_m1 -type LS -schedule hourly
```

負載共用鏡像的類型屬性會從變更 `DP` 至 `LS`。

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

4. 初始化負載共用鏡像：

```
snapmirror initialize-ls-set -source-path <SVM:volume>
```

以下範例初始化根磁碟區的負載共用鏡像 `svm1_root`：

```
cluster_src::> snapmirror initialize-ls-set -source-path svm1:svm1_root
```

如"指令參考資料ONTAP"需詳細 `snapmirror initialize`資訊，請參閱。

更新 ONTAP 負載共用鏡射關係

SVM 根磁碟區的負載共用鏡像（ LSM ）關係會在 SVM 中的磁碟區掛載或卸載之後，以及包含該選項的作業 `junction-path`期間，自動更新 SVM 根磁碟區的負載共用鏡像（ LSM ）關係 `volume create`。如果您想要在下次排程更新之前更新LSM關係、可以手動更新該關係。

在下列情況下、負載共用鏡射關係會自動更新：

- 現在是進行排程更新的時候了
- 在SVM根磁碟區的磁碟區上執行掛載或卸載作業
- 一個 `volume create`發出的命令包括 `junction-path`選項

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

步驟

1. 手動更新負載共用鏡射關係：

執行此命令之前、您必須以必要的值取代尖括號中的變數。

```
snapmirror update-ls-set -source-path <SVM:volume>
```

以下範例更新根磁碟區的負載共用鏡射關係 `svm1_root`：

```
cluster_src::> snapmirror update-ls-set -source-path svm1:svm1_root
```

如"指令參考資料ONTAP"需詳細 `snapmirror update`資訊，請參閱。

升級 ONTAP 負載共用鏡像

如果根磁碟區永久無法使用、您可以升級負載共用鏡像（LSM）磁碟區、以提供對根磁碟區資料的寫入存取權。

開始之前

您必須使用進階權限層級命令來執行此工作。

步驟

1. 變更為進階權限層級：

```
set -privilege advanced
```

2. 升級LSM Volume：

   執行此命令之前、您必須以必要的值取代尖括號中的變數。

```
snapmirror promote -destination-path <SVM:volume>
```

   以下範例將會提升 Volume `svm1_m2` 作為新的 SVM 根 Volume ：

```
cluster_src::*> snapmirror promote -destination-path svm1:svm1_m2

Warning: Promote will delete the offline read-write volume
         cluster_src://svm1/svm1_root and replace it with
         cluster_src://svm1/svm1_m2. Because the volume is offline,
         it is not possible to determine whether this promote will
         affect other relationships associated with this source.
Do you want to continue? {y|n}: y
```

   輸入 `y`。利用此功能、LSM磁碟區可成為讀寫磁碟區、並可在存取時刪除原始根磁碟區。ONTAP

   如果最近未進行更新、則升級的根Volume可能沒有原始根磁碟區中的所有資料。

   如"指令參考資料ONTAP"需詳細 `snapmirror promote`資訊，請參閱。

3. 返回管理權限層級：

```
set -privilege admin
```

4. 依照您用於根磁碟區的命名慣例、重新命名所升級的磁碟區：

   執行此命令之前、您必須以必要的值取代尖括號中的變數。

```
volume rename -vserver <SVM> -volume <volume> -newname <new_name>
```

以下範例將重新命名升級的 Volume `svm1_m2` 名稱 `svm1_root`：

```
cluster_src::> volume rename -vserver svm11 -volume svm1_m2 -newname
svm1_root
```

5. 如中步驟 3 至步驟 4 所述、保護重新命名的根 Volume "建立及初始化負載共用鏡射關係"。

備份到雲端

安裝 ONTAP SnapMirror 雲端授權

SnapMirror 雲端關係可以使用預先合格的協力廠商備份應用程式來協調。從 ONTAP 9 9.1 開始、您也可以使用系統管理員來協調 SnapMirror 雲端複寫。使用系統管理員協調內部部署 ONTAP 與物件儲存備份時、需要 SnapMirror 和 SnapMirror 雲端容量授權。您也需要申請並安裝 SnapMirror 雲端 API 授權。

關於這項工作

SnapMirror 雲端和 SnapMirror S3 授權是叢集授權、而非節點授權、因此未隨附 ONTAP One 授權套件。這些授權包含在個別的 ONTAP One 相容性套件中。如果您想要啟用 SnapMirror 雲端、您需要申請此套件。

此外、將 SnapMirror 雲端備份協調至物件儲存設備的系統管理員需要 SnapMirror 雲端 API 金鑰。此 API 授權為單一執行個體叢集範圍的授權、表示不需要在叢集中的每個節點上安裝。

步驟

您需要申請並下載 ONTAP One 相容性套件和 SnapMirror 雲端 API 授權、然後使用系統管理員進行安裝。

1. 找出並記錄您要授權的叢集的叢集 UUID 。

   當您提交要求為叢集訂購 ONTAP One 相容性套件時、必須提供叢集 UUID 。

2. 請聯絡您的 NetApp 銷售團隊、並索取 ONTAP One 相容性套件。
3. 請依照 NetApp 支援網站上提供的指示、申請 SnapMirror 雲端 API 授權。

   "申請 SnapMirror 雲端 API 授權金鑰"

4. 當您收到並下載授權檔案後、請使用系統管理員將 ONTAP 雲端相容性 NLF 和 SnapMirror 雲端 API NLF 上傳至叢集：
   a. 按一下*叢集>設定*。
   b. 在 * 設定 * 視窗中、按一下 * 授權 * 。
   c. 在 **Licenses** 窗口中，單擊 + Add 。
   d. 在「新增授權」對話方塊中、按一下「瀏覽」以選取您下載的NLF、然後按一下「新增」將檔案上傳至叢集。

相關資訊

"使用SnapMirror將資料備份到雲端"

"NetApp軟體授權搜尋"

使用 **ONTAP SnapMirror** 將資料備份到雲端

從功能升級到功能升級到ONTAP 功能升級到功能升級、您可以使用System Manager將資料備份到雲端、並將資料從雲端儲存設備還原到不同的磁碟區。您可以使用StorageGRID Suse或ONTAP SS3做為雲端物件儲存區。

從 ONTAP 9.18.1 開始：

- SnapMirror cloud 支援在 MetroCluster 組態上的 FlexGroup 磁碟區進行備份與還原作業，並使用現有的 "REST API ONTAP"。此功能可讓您在切換與切回後，針對由合作夥伴站點維護的 MetroCluster 組態上的 FlexGroup 磁碟區建立 SnapMirror cloud 關係。

從 ONTAP 9.16.1 開始：

- SnapMirror 雲端備份支援扇出關係。這表示可以在兩個不同的物件存放區上同時建立 SnapMirror 備份。有了 ONTAP 9.16.1 ， SnapMirror 雲端可支援兩種扇出關係。扇出可以是兩個物件儲存區，也可以是兩個不同物件儲存區中的一或兩個貯體。建立兩個以上的扇出關係的嘗試將會失敗。
- SnapMirror 雲端支援使用現有的更有效率的同步處理程序來備份移轉至雲端"REST API ONTAP"的磁碟區。此功能可支援從雲端中移轉的磁碟區到相同目的地物件儲存區端點的 SnapMirror 雲端備份，而無需執行重新基準作業。支援 FlexVol 和 FlexGroup 磁碟區。

在使用 SnapMirror 雲端功能之前、您應該先向 NetApp 支援網站申請 SnapMirror 雲端 API 授權金鑰："申請 SnapMirror 雲端 API 授權金鑰"。依照指示、您應該簡單說明您的商機、並透過傳送電子郵件至提供的電子郵件地址來申請API金鑰。您應該會在24小時內收到電子郵件回應、並提供如何取得API金鑰的進一步指示。

新增雲端物件存放區

在您設定 SnapMirror 雲端備份之前、您需要新增 StorageGRID 或 ONTAP S3 雲端物件存放區。

步驟

1. 按一下「保護>總覽>雲端物件存放區」。
2. 按一下 + Add 。

使用預設原則進行備份

您可以使用預設的雲端保護原則 DailyBackup 、為現有的磁碟區快速設定 SnapMirror 雲端備份。

步驟

1. 按一下「保護>總覽」、然後選取「將磁碟區備份到雲端」。
2. 如果這是您第一次備份至雲端、請在授權欄位中輸入您的 SnapMirror 雲端 API 授權金鑰、如圖所示。
3. 按一下*驗證並繼續*。
4. 選取來源Volume。

5. 選取雲端物件存放區。
6. 按一下「 * 儲存 * 」。

建立自訂的雲端備份原則

如果您不想將預設的 DailyBackup 雲端原則用於 SnapMirror 雲端備份、您可以建立自己的原則。

步驟

1. 按一下「保護>總覽>本機原則設定」、然後選取「保護原則」。
2. 按一下「新增」、然後輸入新的原則詳細資料。
3. 在*原則類型*區段中、選取*備份至雲端*、表示您正在建立雲端原則。
4. 按一下「 * 儲存 * 」。

從「*** Volumes** 」（*磁碟區）頁面建立備份

當您想要一次為多個磁碟區選取及建立雲端備份，或是想要使用自訂保護原則時，可以使用 System Manager * Volumes * 頁面。

步驟

1. 按一下「儲存設備>磁碟區」。
2. 選取您要備份到雲端的磁碟區、然後按一下* Protect *。
3. 在* Protect Volume*視窗中、按一下*更多選項*。
4. 選取原則。

   您可以選取預設原則DailyBackup或您建立的自訂雲端原則。

5. 選取雲端物件存放區。
6. 按一下「 * 儲存 * 」。

從雲端還原

您可以使用System Manager將備份的資料從雲端儲存設備還原至來源叢集上的不同磁碟區。

> 如果您使用的是 ONTAP 9.16.1 或更新版本，而您正在執行 SnapMirror 雲端單一檔案還原至 FlexGroup 磁碟區，則只能將檔案還原至 FlexGroup 磁碟區中的新目錄，而且必須在目的地 FlexGroup 磁碟區上將精細資料設為 `advanced`。如需設定選項的詳細資訊 `-granular-data advanced`，請參閱"重新分配檔案資料以平衡 ONTAP FlexGroup 磁碟區"。

步驟

1. 從 SnapMirror 對雲端關係的來源叢集、按一下 * 儲存 > Volumes （磁碟區） * 。
2. 選取您要還原的磁碟區。
3. 選取*備份至雲端*索引標籤。
4. 按一下 ⋮ 您要還原的來源磁碟區旁的以顯示功能表、然後選取 * 還原 * 。
5. 在「來源」下、選取儲存VM、然後輸入要還原資料的磁碟區名稱。

6. 在 * 目的地 * 下，選取您要還原的快照。
7. 按一下「 * 儲存 * 」。

刪除 **SnapMirror** 雲端關係

您可以使用System Manager刪除雲端關係。

步驟

1. 按一下「儲存設備>磁碟區」、然後選取您要刪除的磁碟區。
2. 按一下 ⋮ 來源磁碟區旁的、然後選取 * 刪除 * 。
3. 如果您要刪除雲端物件存放區端點、請選取*刪除雲端物件存放區端點（選用）*。
4. 按一下*刪除*。

移除雲端物件存放區

如果雲端物件存放區不是雲端備份關係的一部分、您可以使用System Manager來移除它。當雲端物件存放區是雲端備份關係的一部分時、就無法刪除。

步驟

1. 按一下「保護>總覽>雲端物件存放區」。
2. 選取您要刪除的物件存放區、按一下 ⋮ 並選取 * 刪除 * 。

使用**NetApp**備份和恢復備份數據

從ONTAP 9.9.1 開始，您可以使用 System Manager 透過NetApp備份和還原服務備份雲端中的資料。

備份和復原支援FlexVol讀寫磁碟區和資料保護 (DP) 磁碟區。從ONTAP 9.12.1 開始，備份和復原支援FlexGroup捲和SnapLock磁碟區。

詳細了解"NetApp備份與復原" 。

開始之前

您應該執行以下步驟在NetApp控制台中建立帳戶。對於服務帳戶，您需要建立「帳戶管理員」角色。 （其他服務帳戶角色沒有從系統管理員建立連線所需的權限。）

1. "在NetApp控制台中建立帳戶" 。
2. "在NetApp控制台中建立控制台代理"與以下雲端提供者之一合作：
   - Microsoft Azure
   - Amazon Web Services（AWS）
   - Google Cloud Platform（GCP）
   - StorageGRID （ ONTAP 9.10.1 ）

從ONTAP 9.10.1 開始，您可以選擇StorageGRID作為雲端備份供應商，但前提是NetApp Console 部署在本機。控制台代理必須安裝在本機，並可透過NetApp控制台軟體即服務 (SaaS) 應用程式使用。

3. "在NetApp控制台中訂閱NetApp備份與復原"（需要適當的許可證）。
4. "使用NetApp控制台產生存取金鑰和金鑰"。

使用**NetApp**控制台註冊集群

您可以使用控制台或系統管理員向NetApp控制台註冊叢集。

步驟

1. 在System Manager中、前往* Protection Overview *。
2. 在 * NetApp Backup and Recovery* 下，提供以下詳細資訊：
   - 用戶端ID
   - 用戶端秘密金鑰
3. 選擇*註冊並繼續*。

啟用**NetApp**備份與復原

在叢集註冊到NetApp控制台後，您需要啟用NetApp備份和還原並啟動第一次備份到雲端。

步驟

1. 在系統管理器中，選擇 * 保護 > 概述 * ，然後滾動至 Cloud Backup Service 部分。
2. 輸入* Client ID*和* Client Secret *。

   從 ONTAP 9.10.1 開始，您可以選擇 * 深入瞭解使用雲端的成本 * ，瞭解使用雲端的成本。

3. 選取 * 連線並啟用 Cloud Backup Service * 。
4. 在「啟用NetApp備份和復原」頁面上，根據您選擇的提供者提供以下詳細資訊。

對於這家雲端供應商…	輸入下列資料…
Azure	• Azure訂閱ID • 區域 • 資源群組名稱（現有或新）
AWS	• AWS帳戶ID • 存取金鑰 • 秘密金鑰 • 區域

Google Cloud Project（GCP）	• Google Cloud專案名稱 • Google Cloud Access金鑰 • Google Cloud秘密金鑰 • 區域
StorageGRID （ONTAP 9.10.1 及更高版本，僅適用於NetApp控制台的本機部署）	• 伺服器 • SG 存取金鑰 • SG秘密金鑰

5. 選擇*保護原則*：
   - 現有原則：選擇現有原則。
   - 新政策：指定名稱並設定傳輸排程。

     從ONTAP 功能支援的版本起、您可以指定是否要使用Azure或AWS進行歸檔。

     如果您使用Azure或AWS為磁碟區啟用歸檔、則無法停用歸檔。

     如果您啟用Azure或AWS的歸檔、請指定下列項目：

     - 磁碟區歸檔的天數。
     - 要保留在歸檔中的備份數。指定「 0 」（零）以歸檔至最新備份。
     - 對於AWS、請選取歸檔儲存類別。
6. 選取您要備份的磁碟區。
7. 選擇*保存*。

編輯用於**NetApp**備份和復原的保護策略

您可以變更NetApp Backup and Recovery 使用的保護策略。

步驟

1. 在系統管理器中，選擇 * 保護 > 概述 * ，然後滾動至 Cloud Backup Service 部分。
2. 選擇 ，然後選擇 * 編輯 * 。
3. 選擇*保護原則*：
   - 現有原則：選擇現有原則。
   - 新政策：指定名稱並設定傳輸排程。

     從ONTAP 功能支援的版本起、您可以指定是否要使用Azure或AWS進行歸檔。

     如果您使用Azure或AWS為磁碟區啟用歸檔、則無法停用歸檔。

如果您啟用Azure或AWS的歸檔、請指定下列項目：

- 磁碟區歸檔的天數。
- 要保留在歸檔中的備份數。指定「 0 」（零）以歸檔至最新備份。
- 對於AWS、請選取歸檔儲存類別。

4. 選擇*保存*。

保護雲端上的新磁碟區或**LUN**

當您建立新的Volume或LUN時、可以建立SnapMirror保護關係、以便備份至磁碟區或LUN的雲端。

開始之前

- 您應該擁有SnapMirror授權。
- 應設定叢集間的LIF。
- 應設定NTP。
- 叢集必須執行 ONTAP 9.9.1 或更新版本。

關於這項工作

下列叢集組態無法保護雲端上的新磁碟區或LUN：

- 叢集不能位於MetroCluster 一個不符合需求的環境中。
- 不支援SVM-DR。
- 無法使用NetApp Backup and Recovery 備份FlexGroup磁碟區。

步驟

1. 配置磁碟區或LUN時、請在System Manager的* Protection（保護）頁面上、選取標有 Enable SnapMirror（本機或遠端）*的核取方塊。
2. 選擇備份和復原策略類型。
3. 如果未啟用備份和恢復，請選擇*使用NetApp備份和還原啟用備份*。

保護雲端上現有的磁碟區或**LUN**

您可以為現有的磁碟區和LUN建立SnapMirror保護關係。

步驟

1. 選取現有的磁碟區或 LUN ，然後選取 * 保護 * 。
2. 在「保護卷」頁面上，指定「使用NetApp備份和復原進行備份」作為保護策略。
3. 選取 * 保護 * 。
4. 在* Protection（保護）頁面上、選取標有 Enable SnapMirror（本機或遠端）*的核取方塊。
5. 選擇*連線並啟用NetApp備份與復原*。

從備份檔案還原資料

只有在使用NetApp控制台時，您才可以執行備份管理作業，例如還原資料、更新關係和刪除關係。請參閱"從備份檔案還原資料"了解更多。

利用SnapLock NetApp技術歸檔及法規遵循

了解ONTAP SnapLock

對於使用WORM儲存設備、以未經修改的形式保留檔案以供法規遵循和治理之用的組織而言、VMware是高效能的法規遵循解決方案。SnapLock

SnapLock 有助於防止資料遭到刪除、變更或重新命名、以符合 SEC 17a-4(f) 、 HIPAA 、 FINRA 、 CFTC 和 GDPR 等法規。利用此功能、您可以建立特殊用途的磁碟區、以便在指定保留期間或無限期儲存檔案、並將檔案提交至不可刪除、不可寫入的狀態SnapLock 。支援使用CIFS和NFS等標準開放式檔案傳輸協定、在檔案層級執行此保留作業SnapLock 。支援的開放式SnapLock 檔案傳輸協定為NFS（版本2、3和4）和CIFS（SMB 1.0、2.0和3.0）。

使用 SnapLock ，您可以將檔案和快照提交至 WORM 儲存設備，並設定受 WORM 保護資料的保留期間。SnapLock WORM 儲存設備使用 NetApp 快照技術，並可運用 SnapMirror 複寫和 SnapVault 備份作為基礎技術，為資料提供備份還原保護。深入瞭解 WORM 儲存設備"符合WORM儲存設備、使用NetApp SnapLock 技術- TR-4526"：。

您可以使用應用程式、透過NFS或CIFS將檔案提交至WORM、或使用SnapLock 「更新」功能、自動將檔案提交至WORM。您可以使用_WORM可應用檔案_來保留遞增寫入的資料、例如記錄資訊。如需詳細資訊、請參閱"使用Volume附加模式建立WORM可應用檔案"。

支援資料保護方法、可滿足大部分的法規遵循需求：SnapLock

- 您可以在次要儲存設備上使用 SnapLock for SnapVault 來保護 WORM 快照。請參閱。 "將快照提交至WORM"
- 您可以使用SnapMirror將WORM檔案複寫到另一個地理位置、以便進行災難恢復。請參閱 "鏡射WORM檔案"。

SnapLock是ONTAP的一項基於許可證的功能。一個許可證即可讓您在嚴格的合規模式下使用SnapLock ，以滿足 SEC 規則 17a-4(f) 等外部要求，以及在較為寬鬆的企業模式下使用 SnapLock，以滿足內部強制規定的數位資產保護要求。SnapLock許可證是以下部分的一部分： "ONTAP One" 軟體套件。

支援所有的支援功能、包括所有的不全系統和不全系統ONTAP Select FAS AFF SnapLock 。不只是軟體解決方案、而是整合式硬體與軟體解決方案SnapLock 。這項區分對於嚴格的 WORM 法規（例如 SEC 17a-4(f) ）而言非常重要、因為它需要整合式的硬體與軟體解決方案。如需詳細資訊、請 "SEC 提供給代理商與經銷商有關使用電子儲存媒體的指引"參閱。

您可以使用**SnapLock** 什麼功能

設定SnapLock 完整套功能後、您可以完成下列工作：

- "將檔案提交至WORM"
- "將快照提交至 WORM 以進行次儲存"
- "鏡射WORM檔案以進行災難恢復"

- "在訴訟期間使用「合法持有」來保留WORM檔案"
- "使用權限刪除功能刪除WORM檔案"
- "設定檔案保留期間"
- "移動SnapLock 一個流通量的資料"
- "鎖定快照以防止勒索軟體攻擊"
- "檢閱 SnapLock 搭配稽核記錄的使用情形"
- "使用SnapLock 功能完善的API"

符合法規及企業模式**SnapLock**

不一致性與企業模式的差異主要在於每種模式保護WORM檔案的層級：SnapLock

供應模式SnapLock	保護層級	保留期間刪除WORM檔案
法規遵循模式	在磁碟層級	無法刪除
企業模式	在檔案層級	合規管理員可以使用經過審核的「特權刪除」程式進行刪除

保留期間結束後、您必須負責刪除不再需要的任何檔案。一旦檔案已提交至WORM（無論是在「法規遵循」或「企業」模式下）、即使保留期間已過期、也無法加以修改。

您無法在保留期間內或之後移動WORM檔案。您可以複製WORM檔案、但複本不會保留WORM特性。

下表顯示SnapLock 「不符合需求」和「企業」模式所支援的功能差異：

能力	符合法規SnapLock	企業版SnapLock
使用特殊權限刪除來啟用及刪除檔案	否	是的
重新初始化磁碟	否	是的
在SnapLock 保留期間銷毀整合資料和磁碟區	否	是、SnapLock 除了不包括不含資訊的稽核記錄磁碟區
重新命名Aggregate或Volume	否	是的
使用非NetApp磁碟	否	否
使用此功能進行稽核記錄SnapLock	是的	是的、從ONTAP SES9.5開始

支援且不支援**SnapLock** 的功能

下表顯示SnapLock 支援的功能、包括「不符合需求」模式SnapLock 、「不符合需求」模式或「不符合需求」

模式、或兩者：

功能	支援SnapLock 不受支援的功能	支援SnapLock 支援不受支援的企業
一致性群組	否	否
加密磁碟區	是的，詳細了解加密與SnapLock 功能 。	是的，詳細了解加密與SnapLock 功能 。
FabricPools on SnapLock	否	是的、從ONTAP 功能性的問題9.8開始。深入瞭解 不只是在企業級集合體上SnapLock FabricPool。
Flash Pool Aggregate	是的。	是的。
FlexClone	您可以複製SnapLock 不全的資料、但無法複製SnapLock 到一個實體磁碟區上的檔案。	您可以複製SnapLock 不全的資料、但無法複製SnapLock 到一個實體磁碟區上的檔案。
資料量FlexGroup	是的、從ONTAP 功能性的問題9.11.1開始。深入瞭解 [flexgroup]。	是的、從ONTAP 功能性的問題9.11.1開始。深入瞭解 [flexgroup]。
LUN	不可以深入瞭解 LUN 支援 使用 SnapLock 。	不可以深入瞭解 LUN 支援 使用 SnapLock 。
內部組態MetroCluster	是的、從ONTAP 0到3開始。深入瞭解 支援 MetroCluster。	是的、從ONTAP 0到3開始。深入瞭解 支援 MetroCluster。
多重管理驗證（ MAV ）	是、從 ONTAP 9.13.1 開始。深入瞭解 MAV 支援。	是、從 ONTAP 9.13.1 開始。深入瞭解 MAV 支援。
SAN	否	否
單一檔案SnapRestore 的功能	否	是的
SnapMirror 主動同步	否	否
SnapRestore	否	是的
SM磁帶	否	否
SnapMirror同步	否	否
SSD	是的。	是的。

儲存效率功能	是的、從ONTAP 0到9：9.1開始。 深入瞭解 儲存效率支援。	是的、從ONTAP 0到9：9.1開始。 深入瞭解 儲存效率支援。

不只是在企業級集合體上**SnapLock FabricPool**

FabricPools支援SnapLock 以ONTAP 概念9.8開頭的支援於支援的功能不全企業集合體。不過、您的客戶團隊需要開啟產品差異要求、記錄您瞭解FabricPool 到、由於SnapLock 雲端管理員可以刪除這些資料、因此不再以不受保護的方式、將階層至公有雲或私有雲的資料分層。

任何資料若以公有雲或私有雲為基礎、都不再受到支援、因為資料可由雲端管理員刪除SnapLock FabricPool 。

資料量**FlexGroup**

支援以支援從停止9.11.1開始的不支援的功能、但不支援下列功能ONTAP FlexGroup SnapLock ：

- 合法持有
- 以事件為基礎的保留
- 支援的支援從功能9.12.1開始SnapLock SnapVault ONTAP

您也應該瞭解下列行為：

- 一個現象區的Volume法規遵循時鐘（VCC）FlexGroup 由根部的VCC決定。所有非根成員的VCC都會與根VCC密切同步。
- 僅能在整個的整個過程中設定組態屬性。SnapLock FlexGroup個別成員不能具有不同的組態內容、例如預設保留時間和自動提交期間。

LUN 支援

只有在將非 SnapLock 磁碟區上建立的快照傳輸至 SnapLock 磁碟區以作為 SnapLock 資料保險箱關係一部分的情況下， SnapLock 磁碟區才支援 LUN 。讀取 / 寫入 SnapLock 磁碟區不支援 LUN 。不過，包含 LUN 的 SnapMirror 來源磁碟區和目的地磁碟區都支援防竄改快照。

支援 **MetroCluster**

支援的支援功能因不相同的情況而異、不只是「符合需求」模式和「支援不符合需求」模式SnapLock SnapLock MetroCluster SnapLock 。

符合法規**SnapLock**

- 從ONTAP 功能更新至功能更新至功能更新至功能更新至功能更新SnapLock 至功能MetroCluster 更新。
- 從ONTAP 支援《支援SnapLock 不符合要求》的功能、開始時、鏡射集合體支援《支援不符合要求》、但前提是集合體只能用於裝載SnapLock 不符合要求的稽核記錄磁碟區。
- SVM特有SnapLock 的功能區組態可透過MetroCluster 以下功能複製到主要和次要站台：

企業版**SnapLock**

- 支援SnapLock Enterprise聚合。

- 從ONTAP 支援使用支援功能支援使用SnapLock 權限刪除功能的支援功能、以支援使用支援功能的支援功能。
- SVM特有SnapLock 的支援功能、可透過MetroCluster 使用支援功能複製到這兩個站台。

零售組態與法規遵循時鐘**MetroCluster**

下列組態使用兩種法規遵循時鐘機制：Volume Compliance Clock(VCC)和System Compliance Clock, SCC)。MetroClusterVCC和SCC適用於所有SnapLock 的各種版本。當您在節點上建立新磁碟區時、其VCC會以該節點上SCC的目前值初始化。建立磁碟區之後、就會一律使用VCC追蹤磁碟區和檔案保留時間。

當磁碟區複寫到另一個站台時、其VCC也會複寫。當發生磁碟區切換時、例如從站台A切換至站台B、VCC會在站台B上繼續更新、而站台A上的SCC會在站台A離線時停止。

當站台A重新上線且執行磁碟區切換時、站台A SCC時鐘會重新啟動、而Volume的VCC則會繼續更新。由於VCC會持續更新、無論切換和切換作業為何、檔案保留時間不取決於SCC時鐘、也不會延展。

多重管理驗證（ **MAV** ）支援

從 ONTAP 9.13.1 開始、叢集管理員可以在叢集上明確啟用多重管理驗證、以在執行某些 SnapLock 作業之前要求仲裁核准。啟用 MAV 時、 SnapLock Volume 內容（例如預設保留時間、最短保留時間、最長保留時間、磁碟區附加模式、自動認可期間和特權刪除）將需要仲裁核准。深入瞭解 "MAV"。

儲存效率

從功能支援的支援範圍ONTAP 從支援支援儲存SnapLock 效率的9.9到9.9.1、例如資料壓縮、跨Volume重複資料刪除、SnapLock 以及針對功能區和集合體的調適性壓縮。如需儲存效率的詳細資訊、請參閱 "ONTAP 儲存效率總覽"。

加密

支援以軟體和硬體為基礎的加密技術、可確保儲存媒體在重新調整用途、退回、放錯地方或遭竊時、無法讀取閒置的資料。ONTAP

*免責聲明：*如果驗證金鑰遺失、或驗證嘗試失敗次數超過指定限制、導致磁碟機永久鎖定、NetApp無法保證自我加密磁碟機或磁碟區上的SnapLock保護WORM檔案將可擷取。您有責任確保驗證失敗。

SnapLock聚合支援加密磁碟區。

7-Mode轉換

您可以使用7-Mode Transition Tool的Copy Based Transition（CBT）功能、將SnapLock 靜止磁碟區從7-Mode移轉至ONTAP VMware。目的地Volume、Compliance或Enterprise的指令檔模式必須符合來源Volume的指令碼模式。SnapLock SnapLock您無法使用無複製轉換（CFT）來移轉SnapLock 版本。

設定**SnapLock** 功能

了解如何設定**ONTAP SnapLock**

在使用 SnapLock 之前、您需要完成各種工作來設定 SnapLock "安裝 SnapLock 授權""法規遵循時鐘"、例如為每個主控 SnapLock Volume 的集合節點、初始化、為執行 ONTAP 9 10.1 之前版本的 ONTAP 叢集建立 SnapLock Aggregate "建立並掛載 SnapLock Volume"

等。

初始化**ONTAP**合規性時鐘

SnapLock 使用 *Volume Compliance Clock* 來防止竄改、以免改變 WORM 檔案的保留期。您必須先在裝載 SnapLock Aggregate 的每個節點上初始化 _ 系統整合時鐘 _ 。

從 ONTAP 9.14.1 開始，您可以在沒有 SnapLock 磁碟區或沒有啟用快照鎖定的磁碟區時，初始化或重新初始化系統相容時鐘。重新初始化的功能可讓系統管理員在系統初始化可能不正確的情況下重設系統相容性時鐘、或是修正系統上的時鐘漂移。在 ONTAP 9.13.1 版及更早版本中、一旦您初始化節點上的規範時鐘、就無法重新初始化它。

開始之前

若要重新初始化法規遵循時鐘：

- 叢集中的所有節點都必須處於健全狀態。
- 所有磁碟區都必須處於線上狀態。
- 恢復佇列中沒有任何磁碟區。
- 無法存在 SnapLock 磁碟區。
- 沒有啟用快照鎖定的磁碟區。

初始化法規遵循時鐘的一般需求：

- 您必須是叢集管理員才能執行此工作。
- "SnapLock 授權必須安裝在節點上"。

關於這項工作

系統相容時鐘的時間由 *Volume Compliance Clock* 繼承、後者控制磁碟區上 WORM 檔案的保留時間。當您建立新的 SnapLock Volume 時、 Volume Compliance 時鐘會自動初始化。

> 系統相容時鐘的初始設定是以目前的硬體系統時鐘為基礎。因此、在每個節點上初始化系統相容性時鐘之前、您應該先確認系統時間和時區是否正確。在節點上初始化系統相容性時鐘之後、當啟用鎖定的 SnapLock 磁碟區或磁碟區存在時、就無法重新初始化它。

步驟

您可以使用 ONTAP CLI 初始化法規遵循時鐘、或從 ONTAP 9.12.1 開始、使用系統管理員來初始化法規遵循時鐘。

系統管理員

1. 瀏覽至*叢集>總覽*。
2. 在「節點」區段中、按一下「初始化**SnapLock** 功能不一致時鐘」。
3. 要顯示 **Compliance Clock** 列並驗證是否已初始化 Compliance Clock, 請在 **Cluster > Overview >** 節點 * 部分中單擊 ***Show/Hide** 並選擇 SnapLock Compliance Clock* 。

CLI

1. 初始化系統相容時鐘：

   `snaplock compliance-clock initialize -node` *`node_name`*

   下列命令會初始化系統的 Compliance Clock On `node1`：

   ```
   cluster1::> snaplock compliance-clock initialize -node node1
   ```

   如"指令參考資料ONTAP"需詳細 `snaplock compliance-clock initialize`資訊，請參閱。

2. 出現提示時、請確認系統時鐘正確、且您想要初始化 Compliance Clock:

   ```
   Warning: You are about to initialize the secure ComplianceClock of
   the node "node1" to the current value of the node's system clock.
   This procedure can be performed only once on a given node, so you
   should ensure that the system time is set correctly before
   proceeding.

   The current node's system clock is: Mon Apr 25 06:04:10 GMT 2016

   Do you want to continue? (y|n): y
   ```

3. 針對裝載SnapLock 一個Eregate的每個節點、重複此程序。

啟用 **NTP** 組態系統的法規遵循時鐘重新同步

設定 NTP 伺服器後，您可以啟用SnapLock Compliance時脈同步功能。

開始之前

- 此功能僅適用於進階權限層級。
- 您必須是叢集管理員才能執行此工作。
- "SnapLock 授權必須安裝在節點上"。
- 此功能僅適用於Cloud Volumes ONTAP Sf/、ONTAP Select Sf/及VSim平台。

關於這項工作

當 SnapLock 安全時鐘精靈偵測到超出臨界值的偏移時、 ONTAP 會使用系統時間來重設系統和 Volume Compliance 時鐘。24小時的時間會設為偏移臨界值。這表示系統相容時鐘只有在偏差超過一天的情況下、才會與系統時鐘同步。

SnapLock 安全時鐘精靈會偵測到偏差、並將法規遵循時鐘變更為系統時間。任何試圖修改系統時間以強制 Compliance 時鐘與系統時間同步的嘗試都會失敗、因為 Compliance 時鐘只有在系統時間與 NTP 時間同步時、才會與系統時間同步。

步驟

1. 配置 NTP 伺服器時啟用SnapLock Compliance時脈同步功能：

   `snaplock compliance-clock ntp`

   以下命令啟用系統合規時鐘同步功能：

   ```
   cluster1::*> snaplock compliance-clock ntp modify -is-sync-enabled true
   ```

   如"指令參考資料ONTAP"需詳細 `snaplock compliance-clock ntp modify`資訊，請參閱。

2. 出現提示時、請確認已設定的NTP伺服器是受信任的、而且通訊通道是安全的、以啟用此功能：
3. 檢查功能是否已啟用：

   `snaplock compliance-clock ntp show`

   以下指令檢查系統合規時鐘同步功能是否啟用：

   ```
   cluster1::*> snaplock compliance-clock ntp show

   Enable clock sync to NTP system time: true
   ```

   如"指令參考資料ONTAP"需詳細 `snaplock compliance-clock ntp show`資訊，請參閱。

建立**ONTAP SnapLock**聚合

您使用的是 Volume `-snaplock-type` 指定法規遵循或企業 SnapLock Volume 類型的選項。對於ONTAP 版本早於版本的版本、您必須建立獨立SnapLock 的集合體。從ONTAP 版本S59.10.1開始、SnapLock 相同的集合體上可以存在不含SnapLock的不含SnapLock磁碟區；因此SnapLock 、如果您使用ONTAP 的是版本S59.10.1、則不再需要建立個別的不含SnapLock的集合體。

開始之前

- 您必須是叢集管理員才能執行此工作。
- "必須安裝授權"節點上的 SnapLock 。本授權包含在"ONTAP One"中。
- "節點上的規範時鐘必須初始化"。
- 如果您已將磁碟分割為「root」、「data1」和「dat2」、則必須確保備援磁碟可用。

升級考量

升級ONTAP 至版本的過程中、現有SnapLock 的不含SnapLock和不含SnapLock的支援集合體會升級、以支援SnapLock 同時存在的不含支援功能的功能、但現有SnapLock 的不含更新功能的不含更新功能。例如、資料壓縮、跨磁碟區重複資料刪除、以及跨磁碟區背景重複資料刪除等欄位都維持不變。在現有Aggregate上建立的新SnapLock 增功能區、預設值與非SnapLock Volume相同、新磁碟區和Aggregate的預設值則取決於平台。

還原考量

如果您需要還原ONTAP 至版本低於9.10.1的版本、則必須將所有SnapLock 的「還原法規遵循」、SnapLock 「還原企業」和SnapLock 「還原功能」移至自己SnapLock 的「還原集合體」。

關於這項工作

- 您無法使用SyncMirror 「指令集」選項來建立「法規遵循」集合體。
- 只有當使用Aggregate來裝載資訊稽核記錄磁碟區時、您MetroCluster 才能在整個資訊區組態中建立鏡射的法規遵循集合體SnapLock 。

> 在不鏡射和無鏡射的Aggregate上、支援使用支援功能的支援。MetroCluster SnapLock僅在無鏡射的集合體上支援「符合性」SnapLock 。

步驟

1. 建立SnapLock 一個不只一個的集合體：

```
storage aggregate create -aggregate <aggregate_name> -node <node_name>
-diskcount <number_of_disks> -snaplock-type <compliance|enterprise>
```

下列命令會建立 SnapLock `Compliance` Aggregate 命名 `aggr1` 開啟三個磁碟 `node1`：

```
cluster1::> storage aggregate create -aggregate aggr1 -node node1
-diskcount 3 -snaplock-type compliance
```

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

創建並掛載**ONTAP SnapLock**卷

您必須為要提交至 WORM 狀態的檔案或快照建立 SnapLock Volume 。從ONTAP 功能升級到功能升級到功能升級、您所建立的任何磁碟區、無論集合體類型為何、預設都會建立為非SnapLock Volume。您必須使用此 `-snaplock-type`選項，將 `Compliance` 或 `Enterprise` 指定為 `SnapLock` 類型，以明確建立 `SnapLock Volume` 。默認情況下， `SnapLock` 類型設置爲 `non-snaplock`。

開始之前

- 此資訊必須在線上。SnapLock
- 您應該"確認已安裝 SnapLock 授權"。如果節點上未安裝 SnapLock 授權、則必須安裝"安裝"該授權。本授權隨附於"ONTAP One"。在 ONTAP One 之前、 SnapLock 授權已包含在安全性與法規遵循套件中。安全性

與法規遵循套件已不再提供、但仍有效。雖然目前並不需要"升級至 ONTAP One"、但現有客戶仍可選擇。

- "節點上的規範時鐘必須初始化"。

關於這項工作

只要SnapLock 具備適當的功能、您就能隨時銷毀或重新命名Enterprise Volume。在保留期間結束之前、您無法銷毀Compliance Volume。您永遠無法重新命名Compliance Volume。

您可以複製SnapLock 不全的資料、但無法複製SnapLock 到一個實體磁碟區上的檔案。實體複本磁碟區SnapLock 將與父磁碟區相同的實體類型。

> SnapLock 磁碟區不支援 LUN 。只有在將非 SnapLock 磁碟區上建立的快照傳輸至 SnapLock 磁碟區以作為 SnapLock 資料保險箱關係一部分的情況下， SnapLock 磁碟區才支援 LUN 。讀取 / 寫入 SnapLock 磁碟區不支援 LUN 。不過，包含 LUN 的 SnapMirror 來源磁碟區和目的地磁碟區都支援防竄改快照。

使用ONTAP 「系統管理程式」或ONTAP 「系統資訊管理系統」CLI執行此工作。

系統管理員

從《支持》9.12.1開始ONTAP 、您可以使用System Manager來建立SnapLock 一份《支持》。

步驟

1. 瀏覽至*儲存設備>磁碟區*、然後按一下*新增*。
2. 在* Add Volume（添加Volume）窗口中，單擊 More Options（更多選項）。
3. 輸入新的Volume資訊、包括Volume的名稱和大小。
4. 選取*啟用SnapLock Sing*、然後選擇SnapLock 「支援」或「企業」等「支援」類型。
5. 在「自動提交檔案」區段中、選取「修改」、然後輸入檔案在自動提交之前應保持不變的時間量。最小值為5分鐘、最大值為10年。
6. 在「資料保留」區段中、選取最短和最長保留期間。
7. 選取預設保留期間。
8. 按一下「 * 儲存 * 」。
9. 在「* Volumes 」（*磁碟區）頁面中選取新的磁碟區、以驗證SnapLock 各項功能設定。

CLI

1. 建立SnapLock 一個流通量：

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise>
```

如"指令參考資料ONTAP"需詳細 `volume create`資訊，請參閱。以下選項不適用於 `SnapLock Volume ： `-nvfail，-atime-update，-is-autobalance-eligible，-space-mgmt -try-first`和 `vmalign。

下列命令會建立 SnapLock `Compliance` Volume 命名 `vol1` 開啟 `aggr1` 開啟 `vs1`：

```
cluster1::> volume create -vserver vs1 -volume vol1 -aggregate aggr1
-snaplock-type compliance
```

掛載SnapLock 一個流通量

您可以在SnapLock SVM命名空間的交會路徑上掛載一個支援NAS用戶端存取的功能。

開始之前

此版本必須在線上。SnapLock

關於這項工作

- 您只能在SnapLock SVM的根目錄下掛載一個SfNetApp Volume。
- 您無法在SnapLock 一個穩定磁碟區下掛載一般磁碟區。

步驟

1. 掛載SnapLock 一個流通量：

   `volume mount -vserver *SVM_name* -volume *volume_name* -junction-path *path*`

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

   下列命令會掛載名為的 SnapLock Volume `vol1` 至交會路徑 `/sales` 在中 `vs1` 命名空間：

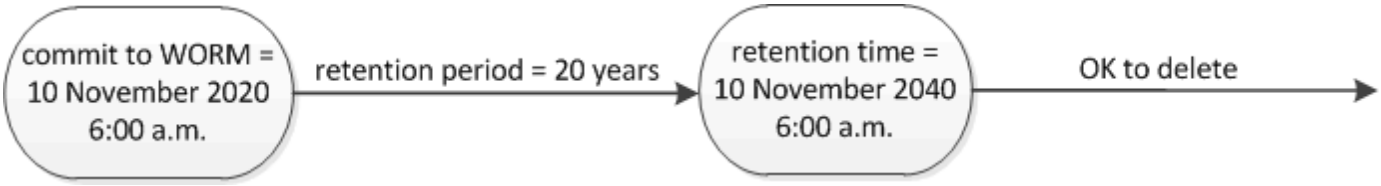
   ```
   cluster1::> volume mount -vserver vs1 -volume vol1 -junction-path /sales
   ```

設定**ONTAP SnapLock**保留時間

您可以明確設定檔案的保留時間、也可以使用磁碟區的預設保留期間來導出保留時間。除非您明確設定保留時間、SnapLock 否則使用預設保留期間來計算保留時間。您也可以在事件發生後設定檔案保留。

關於保留期間與保留時間

WORM檔案的_ret課程 期間_指定了將檔案提交至WORM狀態之後、必須保留的時間長度。WORM檔案的_保留時間_是指不再需要保留檔案的時間。以2020年11月10日上午6：00提交至WORM狀態的檔案保留期間為20年、保留時間為2040年11月10日上午6：00



從《支援資料》9.10.1開始ONTAP 、您可以設定保留時間至10月26日、3058日、保留期限最長可達100年。當您延長保留日期時、舊版原則會自動轉換。在《支援更新版本》中、除非您將預設保留期間設為無限、否則支援的保留時間上限為2071年1月19日（GMT）。ONTAP

重要的複寫考量

使用2071年1月19日（GMT）之後的保留日期、與SnapLock 某個來源磁碟區建立SnapMirror關係時、目的地叢集必須執行ONTAP 版本號為「更新版本」、否則SnapMirror傳輸將會失敗。

重要的還原考量

當有任何文件的保留期晚於「2071 年 1 月 19 日上午 8:44:07」時， ONTAP會阻止您將叢集從ONTAP 9.10.1還原到早期ONTAP版本。

瞭解保留期間

「不符合法規遵循」或「企業」Volume有四個保留期間：SnapLock

- 最短保留期 (`min`）、預設值為 0
- 最長保留期間 (`max`）、預設為 30 年
- 預設保留期間、預設值等於 `min` 適用於從 ONTAP 9.10.1 開始的法規遵循模式和企業模式。在版本早於《支

援》的版本中、預設保留期間取決於模式：ONTAP ONTAP

- 對於規範模式、預設值為等於 `max`。
- 對於 Enterprise 模式、預設值等於 `min`。

- 未指定的保留期間。

> 在ONTAP 9.10.1 之前的版本中，如果您在將合規模式文件提交到 WORM 狀態之前沒有明確設定保留時間，並且沒有修改預設值，則該文件將保留 30 年。此更改_無法_撤銷。同樣，在ONTAP 9.10.1 及更高版本中，如果您在將企業模式文件提交到 WORM 狀態之前沒有明確設定保留時間，並且沒有修改預設值，則該文件將保留 0 年，或者實際上根本不會保留。

從 ONTAP 9.8 開始、您可以將磁碟區中檔案的保留期間設定為 `unspecified`，以便在您設定絕對保留時間之前保留檔案。只要新的絕對保留時間晚於您先前設定的絕對時間、您就可以將檔案的絕對保留時間設定為未指定保留時間、並將其設回絕對保留時間。

從ONTAP 零件版本9.12.1開始、保留期間設為的WORM檔案 `unspecified` 保證保留期間設定SnapLock為針對該現象進行設定的最短保留期間。當您從變更檔案保留期間時 `unspecified` 若要達到絕對保留時間、指定的新保留時間必須大於檔案上已設定的最短保留時間。

設定預設保留期間

您可以使用 `volume snaplock modify` 用於設定 SnapLock 磁碟區上檔案的預設保留期間的命令。

開始之前

此版本必須在線上。SnapLock

關於這項工作

下表顯示預設保留期間選項的可能值：

> 預設保留期間必須大於或等於（>=）最短保留期間、且小於或等於（<=）最長保留期間。

價值	單位	附註
0 - 65535	秒	
0 - 24	時數	
0 - 365	天	
0 - 12	數月	
0 - 100	年	從ONTAP 功能升級到功能升級到功能升級。對於早期ONTAP 版本的版本、此值為0 - 70。
最大	-	使用最長保留期間。

價值	單位	附註
最小	-	使用最短保留期間。
無限	-	永遠保留檔案。
未指定	-	保留檔案、直到設定絕對保留期間為止。

最大和最小保留期間的值和範圍是相同的、但除外 `max` 和 `min`，不適用。如需此工作的詳細資訊、請參閱 "設定保留時間總覽"。

您可以使用 `volume snaplock show`命令來檢視磁碟區的保留期間設定。如"指令參考資料ONTAP"需詳細 `volume snaplock show`資訊，請參閱。

將檔案提交至WORM狀態之後、您可以延長但不能縮短保留期間。

步驟

1. 設定SnapLock 適用於現象區上檔案的預設保留期間：

   `volume snaplock modify -vserver` *`SVM_name`* `-volume` *`volume_name`* `-default -retention-period` *`default_retention_period`* `-minimum-retention-period` *`min_retention_period`* `-maximum-retention-period` *`max_retention_period`*

   如"指令參考資料ONTAP"需詳細 `volume snaplock modify`資訊，請參閱。

   下列範例假設先前尚未修改最小和最大保留期間。

   下列命令會將規範或企業Volume的預設保留期間設為20天：

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period 20days
   ```

   下列命令會將Compliance Volume的預設保留期間設為70年：

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -maximum
   -retention-period 70years
   ```

   下列命令會將Enterprise Volume的預設保留期間設為10年：

   ```
   cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
   -retention-period max -maximum-retention-period 10years
   ```

   下列命令會將Enterprise Volume的預設保留期間設為10天：

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -minimum
-retention-period 10days
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period min
```

下列命令會將Compliance Volume的預設保留期間設為無限：

```
cluster1::> volume snaplock modify -vserver vs1 -volume vol1 -default
-retention-period infinite -maximum-retention-period infinite
```

明確設定檔案的保留時間

您可以修改檔案的上次存取時間、明確設定檔案的保留時間。您可以透過NFS或CIFS使用任何適當的命令或程式來修改上次存取時間。

關於這項工作

將檔案提交至WORM之後、您可以延長但不能縮短保留時間。保留時間會儲存在中 `atime` 檔案欄位。

> 您無法將檔案的保留時間明確設定為 `infinite`。只有在使用預設保留期間來計算保留時間時、才能使用該值。

步驟

1. 使用適當的命令或程式來修改您要設定其保留時間的檔案上次存取時間。

   在UNIX Shell中、使用下列命令將保留時間設定為2020年11月21日上午6：00在名為的檔案上 `document.txt`：

   ```
   touch -a -t 202011210600 document.txt
   ```

   > 您可以使用任何適當的命令或程式來修改Windows中的上次存取時間。

設定事件發生後的檔案保留期間

從ONTAP 使用支援功能《支援功能》的《支援功能SnapLock 》（ETR__）開始、您可以定義事件發生後、檔案保留的時間長度。

開始之前

- 您必須SnapLock 是管理員才能執行此工作。

  "建立SnapLock 一個管理員帳戶"

- 您必須登入安全連線（SSH、主控台或ZAPI）。

關於這項工作

事件保留原則_定義事件發生後的檔案保留期間。原則可套用至單一檔案或目錄中的所有檔案。

- 如果檔案不是WORM檔案、則會在原則中定義的保留期間內、將其提交至WORM狀態。
- 如果檔案是WORM檔案或WORM可應用檔案、其保留期間將會延長至原則中定義的保留期間。

您可以使用法規遵循模式或企業模式磁碟區。

EBR原則無法套用至合法持有的檔案。

如需進階使用"符合法規的WORM儲存設備、採用NetApp SnapLock 技術"、請參閱。

使用**EBR**延長現有**WORM**檔案的保留期間
當您想要延長現有WORM檔案的保留期間時、EBR非常方便。例如、貴公司的政策可能是在員工變更扣繳選項後、保留未修改的員工W-4記錄三年。另一項公司政策可能要求在員工離職後保留W-4記錄五年。 在此情況下、您可以建立保留五年的EBR原則。員工終止聘僱（「事件」）後、您會將EBR原則套用至員工的W-4記錄、延長其保留期間。這通常比手動延長保留期間更容易、尤其是涉及大量檔案時。

步驟

1. 建立EBR原則：

   `snaplock event-retention policy create -vserver` *`SVM_name`* `-name` *`policy_name`* `-retention-period` *`retention_period`*

   下列命令會建立 EBR 原則 `employee_exit` 開啟 `vs1` 保留期為十年：

   ```
   cluster1::>snaplock event-retention policy create -vserver vs1 -name
   employee_exit -retention-period 10years
   ```

2. 套用EBR原則：

   `snaplock event-retention apply -vserver` *`SVM_name`* `-name` *`policy_name`* `-volume` *`volume_name`* `-path` *`path_name`*

   下列命令會套用 EBR 原則 `employee_exit` 開啟 `vs1` 目錄中的所有檔案 `d1`：

   ```
   cluster1::>snaplock event-retention apply -vserver vs1 -name
   employee_exit -volume vol1 -path /d1
   ```

相關資訊

- "建立事件保留原則SnapLock"
- "適用事件保留SnapLock"

建立受ONTAP SnapLock保護的稽核日誌

如果您使用的是 ONTAP 9.9.1 或更早版本、則必須先建立 SnapLock Aggregate 、然後建立受 SnapLock 保護的稽核記錄、才能執行特殊權限刪除或 SnapLock Volume 搬移。稽核日誌會記錄SnapLock 建立和刪除不支援的管理員帳戶、修改記錄磁碟區、是否啟用特殊權限刪除、特殊權限刪除作業、SnapLock 以及執行不需執行任何資料的Volume搬移作業。

從 ONTAP 9.10.1 開始、您不再建立 SnapLock Aggregate 。您必須"明確建立 SnapLock Volume"將 Compliance 或 Enterprise 指定為 SnapLock 類型、以使用 SnapLock 類型選項。

開始之前

如果您使用的是 ONTAP 9.9.1 或更早版本、則必須是叢集管理員才能建立 SnapLock Aggregate 。

關於這項工作

在記錄檔保留期間結束之前、您無法刪除稽核記錄。即使保留期間已過、您也無法修改稽核記錄。這適用於SnapLock 「不符合需求」和「企業」模式。

> ⓘ 在更新版本的版本中、您無法使用無法稽核記錄的「功能不全企業版」磁碟區。ONTAP SnapLock您必須使用SnapLock 「不符合需求」量。在更新版本的版本中、您可以使用「更新版本」或「更新版本」來記錄稽核記錄。ONTAP SnapLock SnapLock在所有情況下、稽核記錄磁碟區都必須掛載在連接路徑上 `/snaplock_audit_log`。沒有其他磁碟區可以使用此交會路徑。

您可以在中找到 SnapLock 稽核記錄 `/snaplock_log` 位於稽核記錄磁碟區根目錄下的目錄、位於名為的子目錄中 `privdel_log` （特權刪除作業）和 `system_log` （其他一切）。稽核記錄檔名稱包含第一次記錄作業的時間戳記、可讓您在執行作業的大約時間內輕鬆搜尋記錄。

- 您可以使用 `snaplock log file show` 命令以檢視稽核記錄磁碟區上的記錄檔。
- 您可以使用 `snaplock log file archive` 命令將目前的記錄檔歸檔並建立新的記錄檔、這在您需要將稽核記錄檔資訊記錄在個別檔案中時非常有用。

深入瞭解 `snaplock log file show`及 `snaplock log file archive` "指令參考資料ONTAP"。

> ⓘ 資料保護磁碟區無法用作SnapLock 不完善的稽核記錄磁碟區。

步驟

1. 建立SnapLock 一個不只一個的集合體。

   建立SnapLock 一個不只一個的集合體

2. 在您要設定稽核記錄的SVM上、建立SnapLock 一個SVM Volume。

   建立SnapLock 一個流通量

3. 設定SVM進行稽核記錄：

   ```
   snaplock log create -vserver SVM_name -volume snaplock_volume_name -max-log
   -size size -retention-period default_retention_period
   ```

稽核記錄檔的最短預設保留期間為六個月。如果受影響檔案的保留期間比稽核記錄的保留期間長、則記錄的保留期間會繼承檔案的保留期間。因此、如果使用特殊權限刪除刪除的檔案保留期間為10個月、而稽核記錄的保留期間為8個月、則記錄的保留期間將延長至10個月。如需保留時間與預設保留期間的詳細資訊，請參閱"設定保留時間"。

下列命令可進行設定 `SVM1` 用於使用 SnapLock Volume 進行稽核記錄 `logVol`。稽核日誌的最大大小為20 GB、保留8個月。

```
SVM1::> snaplock log create -vserver SVM1 -volume logVol -max-log-size
20GB -retention-period 8months
```

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

4. 在您設定用於稽核記錄的 SVM 上、將 SnapLock 磁碟區掛載到連接路徑 `/snaplock_audit_log`。

   掛載SnapLock 一個流通量

驗證ONTAP SnapLock設置

您可以使用 `volume file fingerprint start` 和 `volume file fingerprint dump` 用於檢視檔案與磁碟區的重要資訊的命令、包括檔案類型（一般、 WORM 或 WORM 可擴充）、磁碟區到期日等。

步驟

1. 產生檔案指紋：

   ```
   volume file fingerprint start -vserver <SVM_name> -file <file_path>
   ```

   ```
   svm1::> volume file fingerprint start -vserver svm1 -file
   /vol/sle/vol/f1
   File fingerprint operation is queued. Run "volume file fingerprint show
   -session-id 16842791" to view the fingerprint session status.
   ```

   此命令會產生一個工作階段 ID 、您可以將其用作輸入 `volume file fingerprint dump` 命令。

   您可以使用 `volume file fingerprint show` 使用工作階段 ID 來監控指紋操作的進度的命令。在嘗試顯示指紋之前、請先確認作業已完成。

2. 顯示檔案的指紋：

   ```
   volume file fingerprint dump -session-id <session_ID>
   ```

   ```
   svm1::> volume file fingerprint dump -session-id 33619976
           Vserver:svm1
           Session-ID:33619976
   ```

```
        Volume:slc_vol
        Path:/vol/slc_vol/f1
        Data
Fingerprint:MOFJVevxNSJm3C/4Bn5oEEYH51CrudOzZYK4r5Cfy1g=Metadata

Fingerprint:8iMjqJXiNcqgXT5XuRhLiEwIrJEihDmwS0hrexnjgmc=Fingerprint
Algorithm:SHA256
        Fingerprint Scope:data-and-metadata
        Fingerprint Start Time:1460612586
        Formatted Fingerprint Start Time:Thu Apr 14 05:43:06 GMT 2016
        Fingerprint Version:3
        **SnapLock License:available**
        Vserver UUID:acf7ae64-00d6-11e6-a027-0050569c55ae
        Volume MSID:2152884007
        Volume DSID:1028
        Hostname:my_host
        Filer ID:5f18eda2-00b0-11e6-914e-6fb45e537b8d
        Volume Containing Aggregate:slc_aggr1
        Aggregate ID:c84634aa-c757-4b98-8f07-eefe32565f67
        **SnapLock System ComplianceClock:1460610635
        Formatted SnapLock System ComplianceClock:Thu Apr 14 05:10:35
GMT 2016
        Volume SnapLock Type:compliance
        Volume ComplianceClock:1460610635
        Formatted Volume ComplianceClock:Thu Apr 14 05:10:35 GMT 2016
        Volume Expiry Date:1465880998**
         Is Volume Expiry Date Wraparound:false
        Formatted Volume Expiry Date:Tue Jun 14 05:09:58 GMT 2016
        Filesystem ID:1028
        File ID:96
        File Type:worm
        File Size:1048576
        Creation Time:1460612515
        Formatted Creation Time:Thu Apr 14 05:41:55 GMT 2016
        Modification Time:1460612515
        Formatted Modification Time:Thu Apr 14 05:41:55 GMT 2016
        Changed Time:1460610598
        Is Changed Time Wraparound:false
        Formatted Changed Time:Thu Apr 14 05:09:58 GMT 2016
        Retention Time:1465880998
        Is Retention Time Wraparound:false
        Formatted Retention Time:Tue Jun 14 05:09:58 GMT 2016
        Access Time:-
        Formatted Access Time:-
        Owner ID:0
        Group ID:0
```

```
        Owner SID:-
        Fingerprint End Time:1460612586
        Formatted Fingerprint End Time:Thu Apr 14 05:43:06 GMT 2016
```

管理WORM檔案

使用ONTAP SnapLock管理 WORM 文件

您可以使用下列方式管理WORM檔案：

- "將檔案提交至WORM"
- "在資料保險箱目的地上將快照提交至 WORM"
- "鏡射WORM檔案以進行災難恢復"
- "訴訟期間保留WORM檔案"
- "刪除WORM檔案"

使用ONTAP SnapLock將文件提交至 WORM

您可以手動或自動提交檔案至WORM（一次寫入、多次讀取）。您也可以建立WORM可應用檔案。

手動將檔案提交至WORM

您可以將檔案變成唯讀、以手動方式將檔案提交至WORM。您可以透過NFS或CIFS使用任何適當的命令或程式、將檔案的讀寫屬性變更為唯讀。如果您想要確保應用程式已完成寫入檔案的作業、使檔案不會提前提交、或是因為大量磁碟區而導致自動提交掃描程式發生擴充問題、則可以選擇手動提交檔案。

開始之前

- 您想要提交的檔案必須位於SnapLock 一個流通不全的流通不全的流通不全。
- 檔案必須可寫入。

關於這項工作

Volume 體能時鐘時間會寫入 `ctime` 執行命令或程式時的檔案欄位。「完成時鐘時間」可決定何時達到檔案的保留時間。

步驟

1. 使用適當的命令或程式、將檔案的讀寫屬性變更為唯讀。

   在 UNIX Shell 中、請使用下列命令建立名為的檔案 `document.txt` 唯讀：

   ```
   chmod -w document.txt
   ```

   在 Windows Shell 中、使用下列命令建立名為的檔案 `document.txt` 唯讀：

```
attrib +r document.txt
```

自動將檔案提交至**WORM**

利用此功能、您可以自動將檔案提交至WORM。SnapLock如果檔案在自動認可期間沒有變更、則自動認可功能會將檔案提交至 SnapLock 磁碟區的 WORM 狀態
持續時間。自動提交功能預設為停用。

開始之前

- 您想要自動提交的檔案必須位於SnapLock 一個流通於一個不流通的資料冊上。
- 此版本必須在線上。SnapLock
- 此數據區必須是讀寫磁碟區。SnapLock

「自動提交」功能會掃描磁碟區中的所有檔案、並在符合自動提交需求時提交檔案。SnapLock檔案準備好自動提交、到SnapLock 實際由該程式執行自動提交之間可能有一段時間間隔。不過、只要檔案系統符合自動提交的資格、仍可保護檔案免遭修改和刪除。

關於這項工作

_autodit句點_指定檔案在自動提交之前必須保持不變的時間量。在自動提交期間結束之前變更檔案、會重新啟動檔案的自動提交期間。

下表顯示自動提交期間的可能值：

價值	單位	附註
無	-	預設值。
5 - 4256000	分鐘	-
1 - 87600	時數	-
1 - 3650	天	-
1 - 120	數月	-
1 - 10	年	-

最小值為5分鐘、最大值為10年。

步驟

1. 將SidVolume上的所有檔案自動複製到SnapLock WORM：

```
volume snaplock modify -vserver SVM_name -volume volume_name -autocommit
-period autocommit_period
```

如"指令參考資料ONTAP"需詳細 `volume snaplock modify`資訊，請參閱。

下列命令會自動認可磁碟區上的檔案 `vol1` SVM VS1 的檔案只要維持不變 5 小時：

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -autocommit
-period 5hours
```

建立**WORM**可應用檔案

WORM可應用檔案會保留以遞增方式寫入的資料、例如記錄項目。您可以使用任何適當的命令或程式來建立WORM可應用檔案、或是使用SnapLock 「以次磁碟區附加模式_」功能來建立WORM可應用檔案。

使用命令或程式建立**WORM**可應用檔案

您可以透過NFS或CIFS使用任何適當的命令或程式來建立WORM應用檔案。WORM可應用檔案會保留以遞增方式寫入的資料、例如記錄項目。資料會以256 KB區塊附加至檔案。寫入每個區塊時、先前的區塊會受到WORM保護。在保留期間結束之前、您無法刪除檔案。

開始之前

WORM可應用檔案必須位在SnapLock 一個流通不全的磁碟區上。

關於這項工作

資料不需要依序寫入作用中的256 KB區塊。當資料寫入檔案的位元組n x 256kb+1時、先前的256 KB區段會受到WORM保護。

任何超出目前使用中 256 KB 區塊的無序寫入、都會導致作用中的 256 KB 區塊重設為最新偏移、並導致寫入較舊偏移的作業失敗、並出現「唯讀檔案系統（ ROFS ）」錯誤。寫入偏移量視用戶端應用程式而定。不符合 WORM 附加檔案寫入文意的用戶端可能會導致寫入內容的不正確終止。因此、建議您確保用戶端遵循無序寫入的偏移限制、或是以同步模式掛載檔案系統以確保同步寫入。

步驟

1. 使用適當的命令或程式、以所需的保留時間建立零長度檔案。

   在UNIX Shell中、使用下列命令將保留時間設定為2020年11月21日上午6：00在名為的零長度檔案上 `document.txt`：

   ```
   touch -a -t 202011210600 document.txt
   ```

2. 使用適當的命令或程式、將檔案的讀寫屬性變更為唯讀。

   在 UNIX Shell 中、請使用下列命令建立名為的檔案 `document.txt` 唯讀：

   ```
   chmod 444 document.txt
   ```

3. 使用適當的命令或程式、將檔案的讀寫屬性變更回可寫入。

此步驟不視為法規遵循風險、因為檔案中沒有資料。

在 UNIX Shell 中、請使用下列命令建立名為的檔案 `document.txt` 可寫入：

```
chmod 777 document.txt
```

4. 使用適當的命令或程式開始將資料寫入檔案。

   在 UNIX Shell 中、使用下列命令將資料寫入 `document.txt`：

   ```
   echo test data >> document.txt
   ```

   當您不再需要將資料附加至檔案時、請將檔案權限改回唯讀。

使用**Volume**附加模式建立**WORM**可應用檔案

從ONTAP 功能介紹的功能中、您可以使用SnapLock 「不只是功能、也就是功能」（VAM）來建立WORM可應用檔案、這是預設的功能。WORM可應用檔案會保留以遞增方式寫入的資料、例如記錄項目。資料會以256 KB區塊附加至檔案。寫入每個區塊時、先前的區塊會受到WORM保護。在保留期間結束之前、您無法刪除檔案。

開始之前

- WORM可應用檔案必須位在SnapLock 一個流通不全的磁碟區上。
- SnapLock 磁碟區必須卸載，且快照和使用者建立的檔案必須是空的。

關於這項工作

資料不需要依序寫入作用中的256 KB區塊。當資料寫入檔案的位元組n x 256kb+1時、先前的256 KB區段會受到WORM保護。

如果您為磁碟區指定自動提交期間、則不會修改超過自動提交期間的WORM可應用檔案將會提交至WORM。

VAM不支援SnapLock 在不支援的稽核記錄磁碟區上。

步驟

1. 啟用 VAM ：

   `volume snaplock modify -vserver *SVM_name* -volume *volume_name* -is-volume-append -mode-enabled true|false`

   如"指令參考資料ONTAP"需詳細 `volume snaplock modify`資訊，請參閱。

   下列命令可在磁碟區上啟用 VAM `vol1` SVM`vs1`：

```
cluster1::>volume snaplock modify -vserver vs1 -volume vol1 -is-volume
-append-mode-enabled true
```

2. 使用適當的命令或程式來建立具有寫入權限的檔案。

   檔案預設為可應用WORM。

將快照提交到**ONTAP**保管庫目標上的 **WORM**

您可以在次要儲存設備上使用 SnapLock for SnapVault 來保護 WORM 快照。您可以在資料保險箱目的地上執行所有的基本 SnapLock 工作。目的地磁碟區會自動以唯讀方式掛載，因此不需要明確將快照提交至 WORM 。

開始之前

- 如果您要使用系統管理員來設定關係、來源叢集和目的地叢集都必須執行 ONTAP 9.15.1 或更新版本。
- 在目的地叢集上：
  - "安裝SnapLock 不必要的授權"。
  - "初始化法規遵循時鐘"。
  - 如果您將 CLI 與早於 9.10.1 的 ONTAP 版本搭配使用、 "建立 SnapLock Aggregate"。
- 保護原則的類型必須為「保存庫」。
- 來源與目的地集合體必須為64位元。
- 來源Volume不能SnapLock 是一個不全的Volume。
- 如果您使用的是 ONTAP CLI 、則必須在中建立來源和目的地磁碟區 "已對等的叢集" 和 "SVM"。

關於這項工作

來源磁碟區可以使用NetApp或非NetApp儲存。

您無法重新命名承諾為 WORM 狀態的快照。

您可以複製SnapLock 不全的資料、但無法複製SnapLock 到一個實體磁碟區上的檔案。

SnapLock 磁碟區不支援 LUN 。只有在將非 SnapLock 磁碟區上建立的快照傳輸至 SnapLock 磁碟區以作為 SnapLock 資料保險箱關係一部分的情況下， SnapLock 磁碟區才支援 LUN 。讀取 / 寫入 SnapLock 磁碟區不支援 LUN 。但是， SnapMirror 來源磁碟區和包含 LUN 的目的地磁碟區都支援防竄改快照。

從ONTAP 版本S59.10.1開始、SnapLock 相同的集合體上可以存在不含SnapLock的不含SnapLock磁碟區；因此SnapLock 、如果您使用ONTAP 的是版本S59.10.1、則不再需要建立個別的不含SnapLock的集合體。您可以使用 Volume '-SnapLock 類型 ' 選項來指定 Compliance 或 Enterprise SnapLock Volume 類型。在不早於版本的發行版中、從Aggregate繼承了「不更新版本」、「不更新版本」或「企業版本」ONTAP ONTAP SnapLock 。不支援具有版本彈性的目的地Volume。目的地Volume的語言設定必須符合來源Volume的語言設定。

做為保存目的地的流通量會指派預設保留期間給它。SnapLock此期間的值一開始設定SnapLock 為0年以上、而SnapLock 「不符合需求」量則設定為30年以上。每個 NetApp 快照都會一開始使用此預設保留期間來提交。

如有需要、可延長保留期間。如需更多資訊、請參閱 "設定保留時間總覽"。

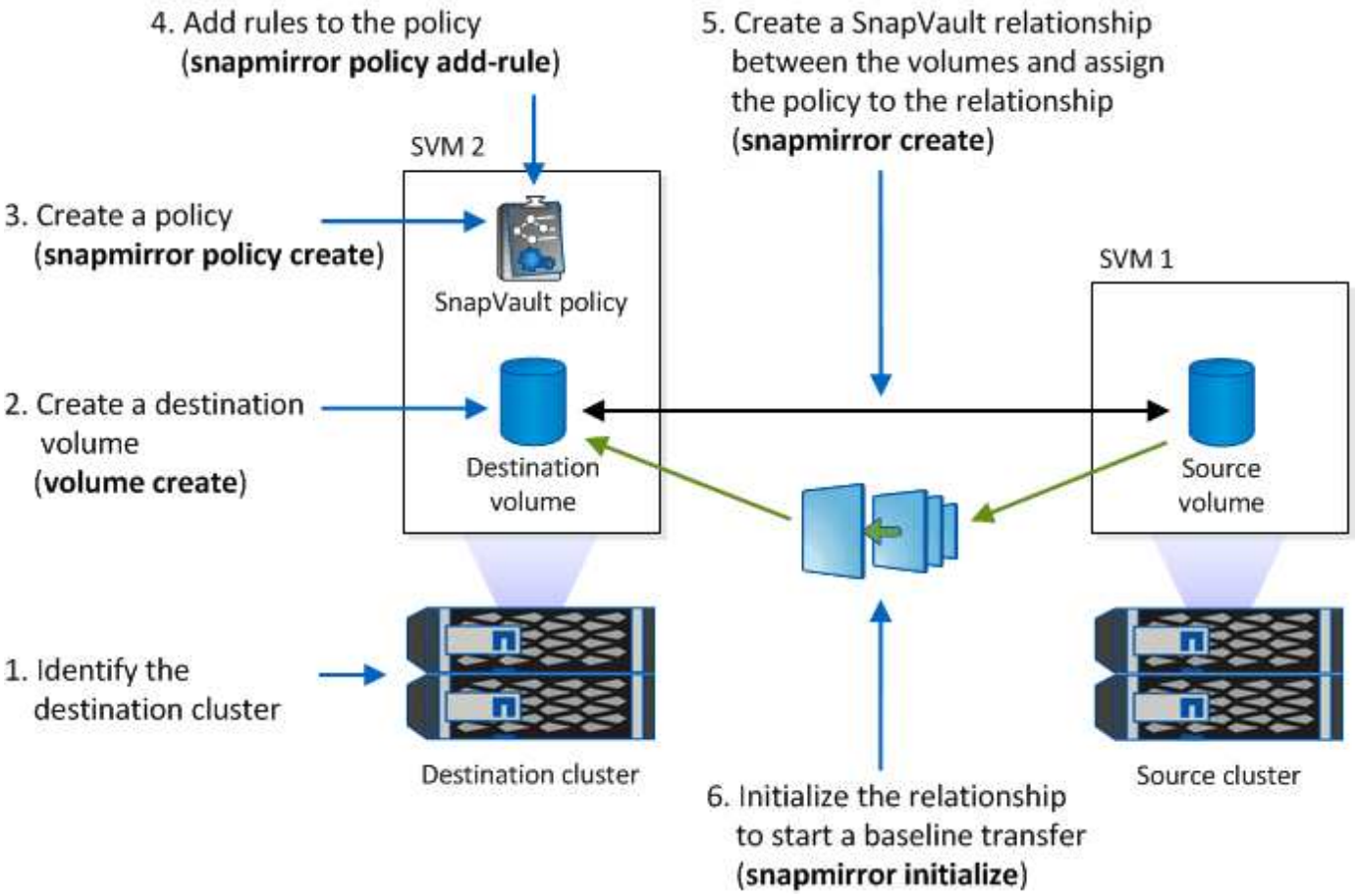
從 ONTAP 9.14.1 開始，您可以在 SnapMirror 關係的 SnapMirror 原則中指定特定 SnapMirror 標籤的保留期間，以便在規則中指定的保留期間內，保留從來源到目的地磁碟區的複寫快照。如果未指定保留期間、則會使用目的地 Volume 的預設保留期間。

從 ONTAP 9.13.1 開始，您可以建立 FlexClone ，並在執行磁碟區複製建立作業時，將選項設為 `non-snaplock`，並將快照指定為「父快照」，以即時還原 SnapLock 資料保險箱關係目的地 SnapLock 磁碟區上的鎖定 `snaplock-type`快照。深入瞭解 "使用 SnapLock 類型建立 FlexClone Volume"。

對於部分組態、您應該注意下列事項：MetroCluster

- 您只能在SnapVault 同步來源的SVM之間建立「不支援」關係、而不能在同步來源SVM和同步目的地SVM之間建立「不支援」關係。
- 您可以從SnapVault 同步來源SVM上的磁碟區、建立從資料服務SVM到資料服務SVM的不一樣關係。
- 您可以從SnapVault 資料服務SVM上的磁碟區、建立一個從同步來源SVM上DP磁碟區的不同步關係。

下圖顯示初始化 SnapLock 資料保險箱關係的程序：



步驟

您可以使用 ONTAP CLI 建立 SnapLock 資料保險箱關係、或從 ONTAP 9.15.1 開始、使用系統管理員建立 SnapLock 資料保險箱關係。

系統管理員

1. 如果磁碟區尚未存在，請在來源叢集上瀏覽至 * 儲存 > Volumes （磁碟區） * ，然後選取 * 新增 * 。
2. 在 * 新增 Volume * 視窗中、選擇 * 更多選項 * 。
3. 輸入磁碟區名稱、大小、匯出原則和共用名稱。
4. 儲存您的變更。
5. 在目的地叢集上，瀏覽至 * 保護 > 關係 * 。
6. 在 * 來源 * 欄上方，選取 * 保護 * ，然後從功能表中選擇 * 磁碟區 * 。
7. 在 * 保護 Volumes （卷） * 窗口中，選擇 * Vault* 作爲保護策略。
8. 在 * 來源 * 區段中，選取您要保護的叢集，儲存 VM 和 Volume 。
9. 在 * 目的地 * 區段的 * 組態詳細資料 * 下，選取 * 鎖定目的地快照 * ，然後選擇 * SnapLock for SnapVault * 作為鎖定方法。如果所選原則類型不是類型，未安裝 SnapLock 授權，或未初始化規範時鐘，則不會顯示鎖定方法 * `vault` 。
10. 如果尚未啟用、請選取 * 初始化 SnapLock 法規遵循時鐘 * 。
11. 儲存您的變更。

CLI

1. 在目的地叢集上、建立類型為的 SnapLock 目的地 Volume `DP` 大小與來源 Volume 相同或更大：

```
volume create -vserver <SVM_name> -volume <volume_name> -aggregate
<aggregate_name> -snaplock-type <compliance|enterprise> -type DP
-size <size>
```

下列命令會建立一個名為的 2GB SnapLock Compliance Volume `dstvolB` 在中 `SVM2` 在 Aggregate 上 `node01_aggr`：

```
cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
node01_aggr -snaplock-type compliance -type DP -size 2GB
```

2. 在目的地叢集上、 "設定預設保留期間"。
3. "建立新的複寫關係" 在非 SnapLock 來源和您建立的新 SnapLock 目的地之間。

此範例使用一項原則來建立與目的地 SnapLock Volume 的新 SnapMirror 關係 `dstvolB`，該原則 `XDPDefault`會在每小時排程中標示為每天和每週的快照資料保險箱：

```
cluster2::> snapmirror create -source-path SVM1:srcvolA -destination
-path SVM2:dstvolB -vserver SVM2 -policy XDPDefault -schedule hourly
```

"建立自訂複寫原則" 或是 "自訂排程" 如果可用的預設值不適用。

4. 在目的地 SVM 上、初始化建立的 SnapVault 關係：

```
snapmirror initialize -destination-path <destination_path>
```

下列命令可初始化來源磁碟區之間的關係 `srcvolA` 開啟 `SVM1` 以及目的地Volume `dstvolB` 開啟 `SVM2`：

```
cluster2::> snapmirror initialize -destination-path SVM2:dstvolB
```

5. 在關係初始化及閒置後，使用 `snapshot show`目的地上的命令來驗證套用至複寫快照的 SnapLock 到期時間。

本範例列出磁碟區上具有 SnapMirror 標籤和 SnapLock 到期日的快照 `dstvolB`：

```
cluster2::> snapshot show -vserver SVM2 -volume dstvolB -fields
snapmirror-label, snaplock-expiry-time
```

相關資訊

- "叢集與SVM對等關係"
- "使用SnapVault 功能進行Volume備份"
- "SnapMirror初始化"

使用**ONTAP SnapMirror**鏡像 **WORM** 檔案以實現災難復原

您可以使用SnapMirror將WORM檔案複寫到其他地理位置、以進行災難恢復及其他用途。來源Volume和目的地Volume都必須設定SnapLock 為供使用、而且這兩個Volume必須具有相同SnapLock 的功能、即相同的功能、法規遵循或企業。複寫磁碟區和檔案的SnapLock 所有關鍵功能。

先決條件

來源與目的地磁碟區必須在具有連接程序的SVM的連接叢集中建立。如需更多資訊、請參閱 "叢集與SVM對等關係"。

關於這項工作

- 從ONTAP 功能完善的9.5開始、您可以使用XDP（延伸資料保護）類型的SnapMirror關係來複寫WORM檔案、而非DP（資料保護）類型關係。XDP模式ONTAP 與版本無關、能夠區分儲存在同一個區塊中的檔案、讓重新同步複寫的法規遵循模式磁碟區變得更加容易。如需如何將現有DP類型關係轉換成XDP類型關係的相關資訊、請參閱 "資料保護"。
- 若由SnapMirror判斷會SnapLock 導致資料遺失、則針對法規遵循模式磁碟區、對DP類型SnapMirror關係進行重新同步作業將會失敗。如果重新同步作業失敗、您可以使用 `volume clone create` 建立目的地Volume 複本的命令。然後、您可以重新同步來源磁碟區與實體複本。
- SnapLock卷的SnapMirror關係僅支持 `MirrorAllSnapshots`非同步鏡像類型策略。 SnapLock磁碟區的保留

期由其所保存的所有 WORM 檔案的最大保留期決定。由於目標是來源的 DR 副本，因此目標SnapLock磁碟區的保留期將與來源相同。

- 支援不同步磁碟區之間XDP類型的SnapMirror關係SnapLock 、即使目的地上的資料與中斷後的來源資料有所不同、也能在中斷後支援重新同步。

  在重新同步時、如果偵測到來源與目的地之間的資料差異、而非一般快照、則會在目的地上剪下新的快照、以擷取此差異。新的快照和通用快照都會以下列保留時間鎖定：

  - 目的地的Volume過期時間
  - 如果磁碟區過期時間過去或尚未設定、則快照會鎖定30天
  - 如果目的地具有合法保留、實際的 Volume 過期期間會被遮罩、並顯示為「無限期」；但是、快照會在實際的 Volume 過期期間內鎖定。

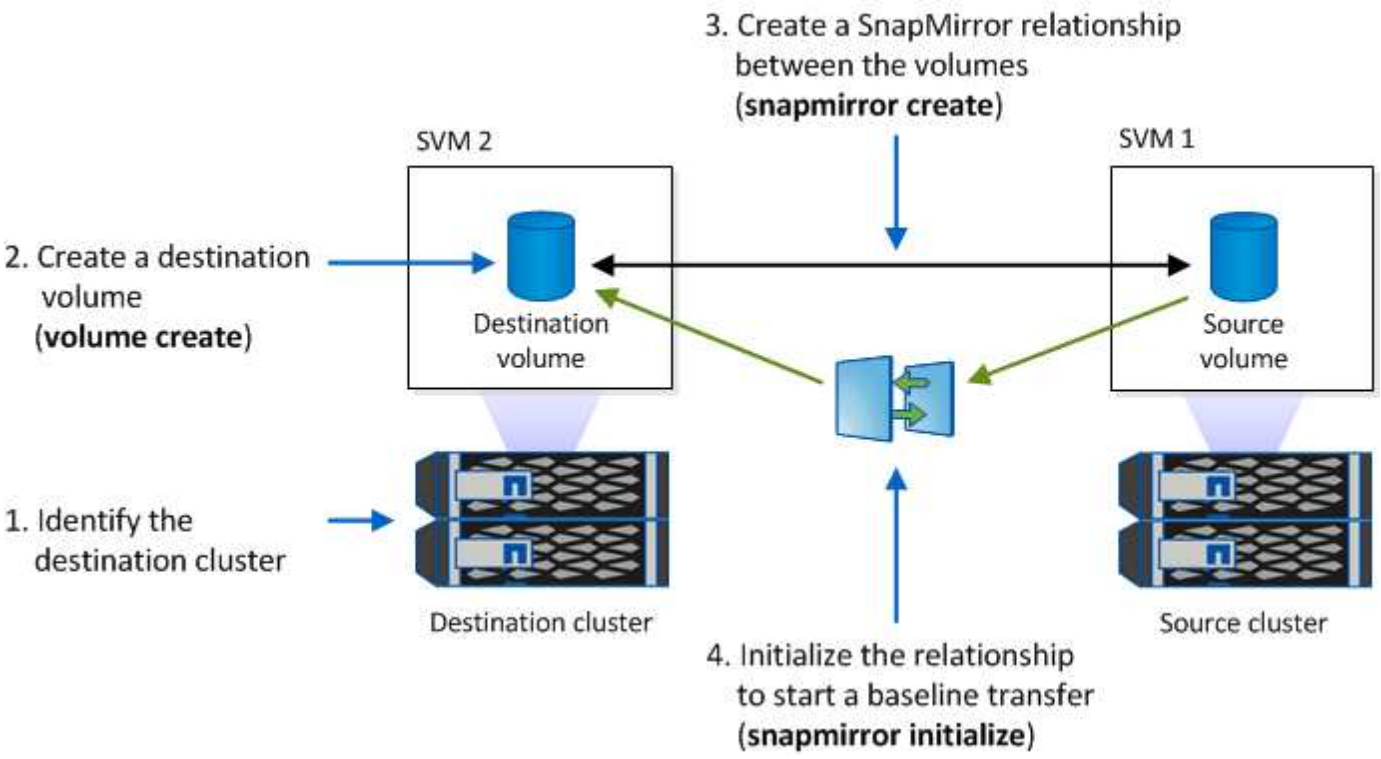
如果目的地Volume的到期期間晚於來源、則目的地到期期間會保留、且不會在來源Volume重新同步後的到期期間覆寫。

如果目的地擁有與來源不同的合法保留、則不允許重新同步。來源與目的地必須具有相同的合法持有、或在嘗試重新同步之前、必須釋出目的地上的所有合法持有。

在目的地磁碟區上建立鎖定的快照，以擷取分散的資料，可透過執行命令的 CLI 將其複製到來源 `snapmirror update -s snapshot`。複製一次的快照也會繼續鎖定來源。

- 不支援SVM資料保護關係。
- 不支援負載共用資料保護關係。

下圖顯示初始化SnapMirror關係的程序：



系統管理員

從ONTAP 功能完善的9.12.1開始、您可以使用System Manager來設定WORM檔案的SnapMirror複寫。

步驟

1. 瀏覽至*儲存>磁碟區*。
2. 按一下*顯示/隱藏*、然後選取* SnapLock 「功能類型」、以在「功能區」視窗中顯示該欄。
3. 找SnapLock 到一個流通量。
4. 按一下 ⋮ 並選取 * 保護 * 。
5. 選擇目的地叢集和目的地儲存VM。
6. 按一下*「更多選項」*。
7. 選擇*顯示舊政策*、然後選取* DPDefault（舊版）*。
8. 在「目的地組態詳細資料」區段中、選取*置換傳輸排程*、然後選取*每小時*。
9. 按一下「 * 儲存 * 」 。
10. 在來源磁碟區名稱左側、按一下箭頭以展開磁碟區詳細資料、然後在頁面右側檢閱遠端SnapMirror保護詳細資料。
11. 在遠端叢集上、瀏覽至*保護關係*。
12. 找出關係、然後按一下目的地Volume名稱、即可檢視關係詳細資料。
13. 確認目的地Volume SnapLock 的類型與SnapLock 其他資訊不全。

CLI

1. 識別目的地叢集。
2. 在目標叢集"安裝 SnapLock 授權"、、"初始化法規遵循時鐘"和上、如果您使用早於 9.10.1 的 ONTAP 版本、"建立 SnapLock Aggregate"。
3. 在目的地叢集上、建立類型為的 SnapLock 目的地 Volume `DP` 大小與來源 Volume 相同或大於：

   ```
   volume create -vserver SVM_name -volume volume_name -aggregate
   aggregate_name -snaplock-type compliance|enterprise -type DP -size size
   ```

   > 從ONTAP 9.10.1 開始， SnapLock和非SnapLock磁碟區可以存在於同一個聚合上；因此，如果您使用ONTAP 9.10.1，則不再需要建立單獨的SnapLock聚合。您可以使用volume -snaplock-type選項指定Compliance或Enterprise SnapLock磁碟區類型。在ONTAP 9.10.1 之前的ONTAP版本中， SnapLock模式（Compliance 或 Enterprise）是從聚合繼承的。目標磁碟區的語言設定必須與來源磁碟區的語言設定相符。

   下列命令會建立 2 GB SnapLock `Compliance` Volume 命名 `dstvolB` 在中 `SVM2` 在 Aggregate 上 `node01_aggr`：

   ```
   cluster2::> volume create -vserver SVM2 -volume dstvolB -aggregate
   node01_aggr -snaplock-type compliance -type DP -size 2GB
   ```

4. 在目的地SVM上、建立SnapMirror原則：

`snapmirror policy create -vserver SVM_name -policy policy_name`

下列命令會建立 SVM 範圍的原則 `SVM1-mirror`：

```
SVM2::> snapmirror policy create -vserver SVM2 -policy SVM1-mirror
```

5. 在目的地SVM上、建立SnapMirror排程：

   `job schedule cron create -name schedule_name -dayofweek day_of_week -hour hour -minute minute`

   下列命令會建立一個名為的 SnapMirror 排程 `weekendcron`：

   ```
   SVM2::> job schedule cron create -name weekendcron -dayofweek
   "Saturday, Sunday" -hour 3 -minute 0
   ```

6. 在目的地SVM上、建立SnapMirror關係：

   `snapmirror create -source-path source_path -destination-path destination_path -type XDP|DP -policy policy_name -schedule schedule_name`

   以下命令可在來源磁碟區之間建立 SnapMirror 關係 `srcvolA` 開啟 `SVM1` 以及目的地Volume `dstvolB` 開啟 `SVM2`，然後指派原則 `SVM1-mirror` 和排程 `weekendcron`：

   ```
   SVM2::> snapmirror create -source-path SVM1:srcvolA -destination
   -path SVM2:dstvolB -type XDP -policy SVM1-mirror -schedule
   weekendcron
   ```

   XDP類型ONTAP 可在SHD9.5或更新版本中找到。您必須使用ONTAP 更新版本的DP類型。

7. 在目的地SVM上、初始化SnapMirror關係：

   `snapmirror initialize -destination-path destination_path`

   初始化程序會將_基準線傳輸_傳送到目的地Volume。SnapMirror 會建立來源磁碟區的快照，然後將複本及其參照的所有資料區塊傳輸至目的地磁碟區。它也會將來源磁碟區上的任何其他快照傳輸至目的地磁碟區。

   下列命令可初始化來源磁碟區之間的關係 `srcvolA` 開啟 `SVM1` 以及目的地Volume `dstvolB` 開啟 `SVM2`：

   ```
   SVM2::> snapmirror initialize -destination-path SVM2:dstvolB
   ```

相關資訊

- "叢集與SVM對等關係"
- "Volume災難恢復準備"
- "資料保護"
- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 策略創建"

使用**ONTAP SnapLock**合法保留功能在訴訟期間保留 **WORM** 文件

從使用支援功能《支援功能》的《支援功能》（Flash）開始ONTAP 、您可以在訴訟期間保留法規遵循模式的WORM檔案。

開始之前

- 您必須SnapLock 是管理員才能執行此工作。

  "建立SnapLock 一個管理員帳戶"

- 您必須登入安全連線（SSH、主控台或ZAPI）。

關於這項工作

「合法持有」下的檔案、其行為類似WORM檔案、保留期不固定。您有責任指定法律保留期間何時結束。

您可以置於「合法保留」下的檔案數量、取決於磁碟區上可用的空間。

步驟

1. 開始合法持有：

   ```
   snaplock legal-hold begin -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   下列命令會針對中的所有檔案啟動合法保留 `vol1`：

   ```
   cluster1::>snaplock legal-hold begin -litigation-name litigation1
   -volume vol1 -path /
   ```

2. 結束合法持有：

   ```
   snaplock legal-hold end -litigation-name <litigation_name> -volume
   <volume_name> -path <path_name>
   ```

   下列命令會結束中所有檔案的合法保留 `vol1`：

```
cluster1::>snaplock legal-hold end -litigation-name litigation1 -volume
vol1 -path /
```

相關資訊

- "不合法的保留開始SnapLock"
- "終止合法持有SnapLock"

使用**ONTAP SnapLock**刪除 **WORM** 文件

您可以使用權限刪除功能、在保留期間刪除企業模式WORM檔案。使用此功能之前、您必須先建立SnapLock 一個支援系統管理員帳戶、然後再使用帳戶啟用此功能。

建立**SnapLock** 一個管理員帳戶

您必須擁有SnapLock 管理員權限才能執行特殊權限刪除。這些權限是在vsadmin-SnapLock角色中定義。如果您尚未被指派該角色、您可以要求叢集管理員建立一個SVM系統管理員帳戶SnapLock 、以執行此功能的管理員角色。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須登入安全連線（SSH、主控台或ZAPI）。

步驟

1. 建立SnapLock 具備管理員角色的SVM系統管理員帳戶：

   security login create -vserver SVM_name -user-or-group-name user_or_group_name -application application -authmethod authentication_method -role role -comment comment

   下列命令可啟用 SVM 管理員帳戶 `SnapLockAdmin` 使用預先定義的 `vsadmin-snaplock` 存取角色 `SVM1` 使用密碼：

   ```
   cluster1::> security login create -vserver SVM1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role vsadmin-
   snaplock
   ```

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

啟用特殊權限刪除功能

您必須在含有您要刪除的WORM檔案的Enterprise Volume上明確啟用特殊權限刪除功能。

關於這項工作

的值 `-privileged-delete` 選項可決定是否啟用特權刪除。可能的值包括 `enabled`、 `disabled`和

`permanently-disabled。

> `permanently-disabled`
> 為終端機狀態。將狀態設為之後、您無法在磁碟區上啟用特殊權限刪除
> `permanently-disabled`。

步驟

1. 啟用SnapLock 適用於某個《不支援的企業級」Volume的特殊權限刪除功能：

   volume snaplock modify -vserver *SVM_name* -volume *volume_name* -privileged -delete disabled|enabled|permanently-disabled

   下列命令可啟用 Enterprise Volume 的特殊權限刪除功能 `dataVol` 開啟 `SVM1`：

   ```
   SVM1::> volume snaplock modify -vserver SVM1 -volume dataVol -privileged
   -delete enabled
   ```

刪除企業模式**WORM**檔案

您可以使用權限刪除功能、在保留期間刪除企業模式WORM檔案。

開始之前

- 您必須SnapLock 是管理員才能執行此工作。
- 您必須已建立SnapLock 一套不必要的稽核記錄、並在Enterprise Volume上啟用特殊權限刪除功能。

關於這項工作

您無法使用權限刪除作業來刪除過期的WORM檔案。您可以使用 `volume file retention show`命令來檢視要刪除的 WORM 檔案保留時間。如"指令參考資料ONTAP"需詳細 `volume file retention show`資訊，請參閱。

步驟

1. 刪除企業Volume上的WORM檔案：

   volume file privileged-delete -vserver *SVM_name* -file *file_path*

   下列命令會刪除檔案 `/vol/dataVol/f1` 在SVM上`SVM1`：

   ```
   SVM1::> volume file privileged-delete -file /vol/dataVol/f1
   ```

行動**ONTAP SnapLock**卷

從ONTAP 功能不全的9.8開始、您可以將SnapLock 一個功能不全的磁碟區移到同一類型的目的地集合體、無論是企業或法規遵循。您必須被指派SnapLock 「不穩定」安全角色、才能移動SnapLock 一個「不穩定」的Volume。

建立SnapLock 一個不穩定的系統管理員帳戶

您必須擁有SnapLock 執行SnapLock 「不穩定」Volume搬移的「不安全」管理員權限。這項權限是以「*SURE* SnapLock 」角色授予您、此角色於ONTAP 《SURE9.8（介紹於本文件）」中介紹。如果您尚未被指派該角色、您可以要求叢集管理員建立SnapLock 一個具備SnapLock 此功能的可靠安全使用者。

開始之前

- 您必須是叢集管理員才能執行此工作。
- 您必須登入安全連線（SSH、主控台或ZAPI）。

關於這項工作

與與管理SVM相關的vsadmin-SnapLock角色不同、這個角色與資料SVM相關聯。SnapLock

步驟

1. 建立SnapLock 具備管理員角色的SVM系統管理員帳戶：

   `security login create -vserver` *`SVM_name`* `-user-or-group-name` *`user_or_group_name`* `-application` *`application`* `-authmethod` *`authentication_method`* `-role` *`role`* `-comment` *`comment`*

   下列命令可啟用 SVM 管理員帳戶 `SnapLockAdmin` 使用預先定義的 `snaplock` 存取管理 SVM 的角色 `cluster1` 使用密碼：

   ```
   cluster1::> security login create -vserver cluster1 -user-or-group-name
   SnapLockAdmin -application ssh -authmethod password -role snaplock
   ```

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

移動SnapLock 一個流通量的資料

您可以使用 `volume move` 將 SnapLock Volume 移至目的地 Aggregate 的命令。

開始之前

- 您必須先建立受SnapLock保護的稽核記錄、才能執行SnapLock 循環Volume移動。

  "建立稽核記錄"。

- 如果您使用ONTAP 的是版本早於ONTAP 《不符合指令》9.10.1的版本、則目的地Aggregate必須與SnapLock 您想要移動的《不符合法規》或《企業對企業》的《不符合指令》（Compliance to Compliance）相同的《不SnapLock 符合指令》（Enterprise to Enterprise）。從ONTAP 功能更新至功能更新至功能更新至功能更新至功能更新至功能更新至功能更新SnapLock 的版本。從功能更新至功能更新至功能更新至功能更新至功能更新至功能更新的版本。
- 您必須是SnapLock 具備「非安全性」角色的使用者。

步驟

1. 使用安全連線、登入ONTAP 到「叢集管理LIF」：

   `ssh snaplock_user@cluster_mgmt_ip`

2. 移動SnapLock 一個流通量：

   volume move start -vserver *SVM_name* -volume *SnapLock_volume_name* -destination -aggregate *destination_aggregate_name*

3. 檢查Volume Move作業的狀態：

   volume move show -volume *SnapLock_volume_name* -vserver *SVM_name* -fields volume,phase,vserver

鎖定**ONTAP**快照以防止勒索軟體攻擊

從 ONTAP 9.12.1 開始，您可以鎖定非 SnapLock 磁碟區上的快照，以防止勒索軟體攻擊。鎖定快照可確保快照不會意外或惡意刪除。

您可以使用 SnapLock Compliance 時鐘功能將快照鎖定一段指定的時間，以便在快照達到到期時間之前無法刪除快照。鎖定快照可防止竄改，防止勒索軟體威脅。如果磁碟區遭到勒索軟體攻擊，您可以使用鎖定的快照來恢復資料。

從 ONTAP 9.14.1 開始，快照鎖定功能可支援 SnapLock 資料保險箱目的地和非 SnapLock SnapMirror 目的地磁碟區上的長期保留快照。使用與相關的 SnapMirror 原則規則來設定保留期間現有原則標籤，即可啟用快照鎖定。此規則會覆寫在磁碟區上設定的預設保留期間。如果 SnapMirror 標籤沒有相關的保留期間、則會使用磁碟區的預設保留期間。

防竄改的快照需求與考量

- 如果您使用的是 ONTAP CLI 、叢集中的所有節點都必須執行 ONTAP 9.12.1 或更新版本。如果您使用的是 System Manager 、則所有節點都必須執行 ONTAP 9.13.1 或更新版本。
- "SnapLock 授權必須安裝在叢集上"。本授權包含在"ONTAP One"中。
- "叢集上的規範時鐘必須初始化"。
- 在磁碟區上啟用快照鎖定功能時，您可以將叢集升級至 ONTAP 9.12.1 之後的 ONTAP 版本；不過，除非所有鎖定的快照都已達到到期日，並已刪除，且快照鎖定功能已停用，否則您無法還原至舊版的 ONTAP 。
- 快照鎖定時，磁碟區過期時間會設為快照的到期時間。如果鎖定多個快照，則磁碟區過期時間會反映所有快照中最長的過期時間。
- 鎖定快照的保留期間優先於快照保留計數，這表示如果鎖定快照的快照保留期間尚未過期，則保留數量限制將不會生效。
- 在 SnapMirror 關係中，您可以在鏡射資料保險箱原則規則上設定保留期間，如果目的地磁碟區已啟用快照鎖定功能，則會將保留期間套用至複寫至目的地的快照。保留期間優先於保留計數；例如，即使超過保留計數，仍會保留未超過過期的快照。
- 您可以重新命名非 SnapLock 磁碟區上的快照。僅當原則為MirrorAllSnapshots時、SnapMirror關係的主要磁碟區上的Snapshot重新命名作業才會反映在次要磁碟區上。對於其他原則類型，重新命名的快照不會在更新期間傳播。
- 如果您使用的是 ONTAP CLI ，只有在鎖定的快照是最新的時，才能使用命令來還原鎖定的快 `volume snapshot restore`照。如果在還原快照之後仍有任何未過期的快照，則快照還原作業將會失敗。

防竄改快照支援的功能

- "Cloud Volumes ONTAP"

- 資料量FlexGroup

  FlexGroup 磁碟區支援快照鎖定。快照鎖定只會發生在根組成快照上。只有在根組成的到期時間已過時、才FlexGroup 允許刪除此功能。

- 從系統轉換為FlexVol FlexGroup

  您可以將具有鎖定快照的 FlexVol volume 轉換為 FlexGroup Volume 。轉換後，快照仍會保持鎖定狀態。

- SnapMirror 非同步

  規範時鐘必須同時在來源和目的地上初始化。

- SVM 資料移動性（用於將 SVM 從來源叢集移轉或重新定位至目的地叢集）

  從 ONTAP 9.14.1 開始支援。

- SnapMirror 原則規則使用 `-schedule` 參數
- SVM DR

  規範時鐘必須同時在來源和目的地上初始化。

- Volume複製與檔案複製

  您可以從鎖定的快照建立磁碟區複本和檔案複本。

- 資料量FlexCache

  從ONTAP 9.16.1 開始受支援。

不支援的功能

防竄改快照目前不支援下列功能：

- 一致性群組
- "FabricPool"

  防竄改的快照可提供不可刪除的保護。由於 FabricPool 需要刪除資料的能力，因此無法在同一個磁碟區上啟用 FabricPool 和快照鎖定。

- SMtape
- SnapMirror 主動同步
- SnapMirror 同步

建立磁碟區時啟用快照鎖定

從 ONTAP 9.12.1 開始，您可以在建立新磁碟區時，或在 CLI 中使用和 `volume modify`**命令選項** `volume create`**修改現有磁碟區時，啟用快照鎖定** `-snapshot-locking-enabled`。從 ONTAP 9.13.1 開始，您可以使用系統管理員來啟用快照鎖定。

系統管理員

1. 瀏覽至 * 儲存 > 磁碟區 * 、然後選取 * 新增 * 。
2. 在 * 新增 Volume * 視窗中、選擇 * 更多選項 * 。
3. 輸入磁碟區名稱、大小、匯出原則和共用名稱。
4. 選取 * 啟用 Snapshot 鎖定 * 。如果未安裝 SnapLock 授權、則不會顯示此選項。
5. 如果尚未啟用、請選取 * 初始化 SnapLock 法規遵循時鐘 * 。
6. 儲存您的變更。
7. 在 *Volumes （卷） * 窗口中，選擇您更新的卷，然後選擇 *Overview （總覽） * 。
8. 驗證 * SnapLock 快照鎖定 * 是否顯示爲 * 已啓用 * 。

CLI

1. 若要建立新的磁碟區並啟用快照鎖定，請輸入下列命令：

   ```
   volume create -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

   下列命令可在名為 vol1 的新磁碟區上啟用快照鎖定：

   ```
   > volume create -volume vol1 -aggregate aggr1 -size 100m -snapshot
   -locking-enabled true
   Warning: snapshot locking is being enabled on volume "vol1" in
   Vserver "vs1". It cannot be disabled until all locked snapshots are
   past their expiry time. A volume with unexpired locked snapshots
   cannot be deleted.
   Do you want to continue: {yes|no}: y
   [Job 32] Job succeeded: Successful
   ```

在現有磁碟區上啟用快照鎖定

從 ONTAP 9.12.1 開始，您可以使用 ONTAP CLI 在現有磁碟區上啟用快照鎖定。從 ONTAP 9.13.1 開始，您可以使用系統管理員在現有的磁碟區上啟用快照鎖定。

系統管理員

1. 瀏覽至*儲存>磁碟區*。
2. 選擇 ⋮ 並選擇 * 編輯 > Volume * 。
3. 在 * 編輯 Volume * 視窗中，找到 Snapshot （本機）設定區段，然後選取 * 啟用快照鎖定 * 。

   如果未安裝 SnapLock 授權、則不會顯示此選項。

4. 如果尚未啟用、請選取 * 初始化 SnapLock 法規遵循時鐘 * 。
5. 儲存您的變更。
6. 在 *Volumes （卷） * 窗口中，選擇您更新的卷，然後選擇 *Overview （總覽） * 。
7. 驗證* SnapLock快照鎖定*是否顯示為*已啟用*。

CLI

1. 若要修改現有的磁碟區以啟用快照鎖定，請輸入下列命令：

   ```
   volume modify -vserver <vserver_name> -volume <volume_name> -snapshot
   -locking-enabled true
   ```

建立鎖定的快照原則並套用保留

從 ONTAP 9.12.1 開始，您可以建立快照原則來套用快照保留期間，並將原則套用至磁碟區，以鎖定指定期間的快照。您也可以手動設定保留期間來鎖定快照。從 ONTAP 9.13.1 開始，您可以使用系統管理員建立快照鎖定原則，並將其套用至磁碟區。

建立快照鎖定原則

系統管理員

1. 瀏覽至 * 儲存 > 儲存 VM* 、然後選取儲存 VM 。
2. 選取 * 設定 * 。
3. 找到 *Snapshot policies * 並選擇 →。
4. 在 * 新增 Snapshot Policy* 視窗中、輸入原則名稱。
5. 選取 + Add 。
6. 提供快照排程詳細資料，包括排程名稱，要保留的最大快照數，以及 SnapLock 保留期間。
7. 在 * SnapLock 保留期間 * 欄中，輸入保留快照的小時數，天數，月數或年數。例如，保留期為 5 天的快照原則，會從建立快照之日起將快照鎖定 5 天，而且在該期間無法刪除快照。支援下列保留期間範圍：
   - 年數： 0 - 100
   - 月數： 0 - 1200
   - 天數： 0 - 36500
   - 營業時間： 0 - 24
8. 儲存您的變更。

CLI

1. 若要建立快照原則，請輸入下列命令：

   ```
   volume snapshot policy create -policy <policy_name> -enabled true
   -schedule1 <schedule1_name> -count1 <maximum snapshots> -retention-period1
   <retention_period>
   ```

   下列命令會建立快照鎖定原則：

   ```
   cluster1> volume snapshot policy create -policy lock_policy -enabled
   true -schedule1 hourly -count1 24 -retention-period1 "1 days"
   ```

   如果快照處於作用中保留狀態，則不會取代該快照；也就是說，如果有鎖定的快照尚未過期，則保留計數將不會生效。

將鎖定原則套用至磁碟區

系統管理員

1. 瀏覽至*儲存>磁碟區*。
2. 選擇 ⋮ 並選擇 * 編輯 > Volume * 。
3. 在 * 編輯 Volume * 視窗中，選取 * 排程快照 * 。
4. 從清單中選取鎖定快照原則。
5. 如果尚未啟用快照鎖定，請選取 * 啟用快照鎖定 * 。
6. 儲存您的變更。

CLI

1. 若要將快照鎖定原則套用至現有的磁碟區，請輸入下列命令：

   ```
   volume modify -volume <volume_name> -vserver <vserver_name> -snapshot
   -policy <policy_name>
   ```

在手動建立快照期間套用保留期間

您可以在手動建立快照時套用快照保留期間。必須在磁碟區上啟用 Snapshot 鎖定，否則會忽略保留期間設定。

系統管理員

1. 瀏覽至 * 儲存 > 磁碟區 * 、然後選取磁碟區。
2. 在 Volume 詳細資料頁面中，選取 * Snapshots* 標籤。
3. 選取 + Add 。
4. 輸入快照名稱和 SnapLock 到期時間。您可以選取行事曆來選擇保留到期日和時間。
5. 儲存您的變更。
6. 在「 * 磁碟區 > 快照 * 」頁面中，選取 * 顯示 / 隱藏 * ，然後選擇 * SnapLock 過期時間 * 以顯示 * SnapLock 過期時間 * 欄，並確認已設定保留時間。

CLI

1. 若要手動建立快照並套用鎖定保留期間，請輸入下列命令：

   ```
   volume snapshot create -volume <volume_name> -snapshot <snapshot name>
   -snaplock-expiry-time <expiration_date_time>
   ```

   下列命令會建立新的快照，並設定保留期間：

   ```
   cluster1> volume snapshot create -vserver vs1 -volume vol1 -snapshot
   snap1 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

將保留期間套用至現有的快照

系統管理員

1. 瀏覽至 * 儲存 > 磁碟區 * 、然後選取磁碟區。
2. 在 Volume 詳細資料頁面中，選取 * Snapshots* 標籤。
3. 選取快照，選取⋮，然後選擇 * 修改 SnapLock 過期時間 * 。您可以選取行事曆來選擇保留到期日和時間。
4. 儲存您的變更。
5. 在「 * 磁碟區 > 快照 * 」頁面中，選取 * 顯示 / 隱藏 * ，然後選擇 * SnapLock 過期時間 * 以顯示 * SnapLock 過期時間 * 欄，並確認已設定保留時間。

CLI

1. 若要手動將保留期間套用至現有的快照，請輸入下列命令：

   ```
   volume snapshot modify-snaplock-expiry-time -volume <volume_name> -snapshot
   <snapshot name> -snaplock-expiry-time <expiration_date_time>
   ```

   以下範例將保留期間套用至現有的快照：

   ```
   cluster1> volume snapshot modify-snaplock-expiry-time -volume vol1
   -snapshot snap2 -snaplock-expiry-time "11/10/2022 09:00:00"
   ```

修改現有原則以套用長期保留

在 SnapMirror 關係中，您可以在鏡射資料保險箱原則規則上設定保留期間，如果目的地磁碟區已啟用快照鎖定功能，則會將保留期間套用至複寫至目的地的快照。保留期間優先於保留計數；例如，即使超過保留計數，仍會保留未超過過期的快照。

從 ONTAP 9.14.1 開始，您可以新增規則來設定快照的長期保留，以修改現有的 SnapMirror 原則。此規則用於覆寫 SnapLock 資料保險箱目的地和非 SnapLock SnapMirror 目的地磁碟區上的預設磁碟區保留期間。

1. 將規則新增至現有的 SnapMirror 原則：

   ```
   snapmirror policy add-rule -vserver <SVM name> -policy <policy name>
   -snapmirror-label <label name> -keep <number of snapshots> -retention-period
   [<integer> days|months|years]
   ```

   下列範例建立規則、將 6 個月的保留期間套用至現有的「 LockVault 」原則：

   ```
   snapmirror policy add-rule -vserver vs1 -policy lockvault -snapmirror
   -label test1 -keep 10 -retention-period "6 months"
   ```

   如"指令參考資料ONTAP"需詳細 `snapmirror policy add-rule`資訊，請參閱。

一致性群組

了解ONTAP一致性組

一致性群組是以單一單元管理的磁碟區集合。在 ONTAP 中、一致性群組可為跨越多個磁碟區的應用程式工作負載提供簡易的管理和保護保證。

您可以使用一致性群組來簡化儲存管理。想像您擁有一個橫跨20個LUN的重要資料庫。您可以個別管理 LUN 、或將 LUN 視為單獨的資料集、將其組織成單一一致性群組。

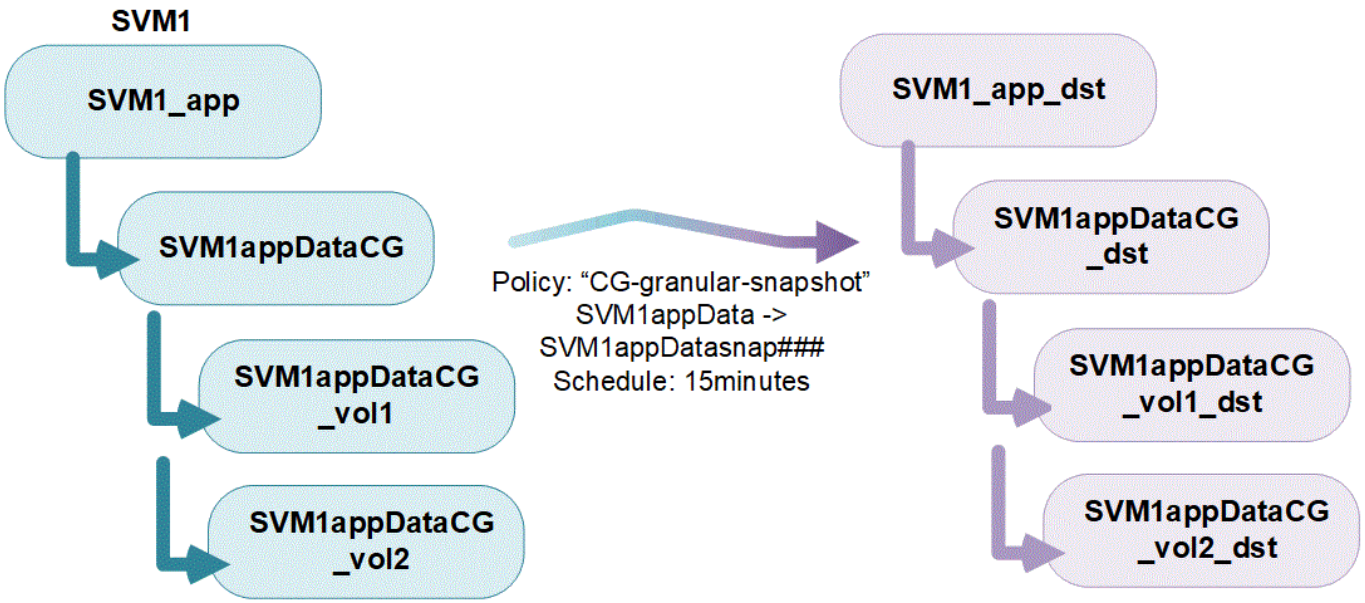
一致性群組可簡化應用程式工作負載管理，提供易於設定的本機和遠端保護原則，並可在某個時間點同時為一組磁碟區提供一致的當機或應用程式一致的快照。一致性群組的快照可還原整個應用程式工作負載。

瞭解一致性群組

一致性群組可支援FlexVol 任何不受傳輸協定（NAS、SAN或NVMe）限制的SESSESE Volume、並可透過ONTAP 「RESSREST API」或「System Manager」（系統管理程式）的「* Storage（儲存設備）> Consistency Groups（一致性群組）*」功能表項目從 ONTAP 9.14.1 開始、一致性群組可透過 ONTAP CLI 進行管理。

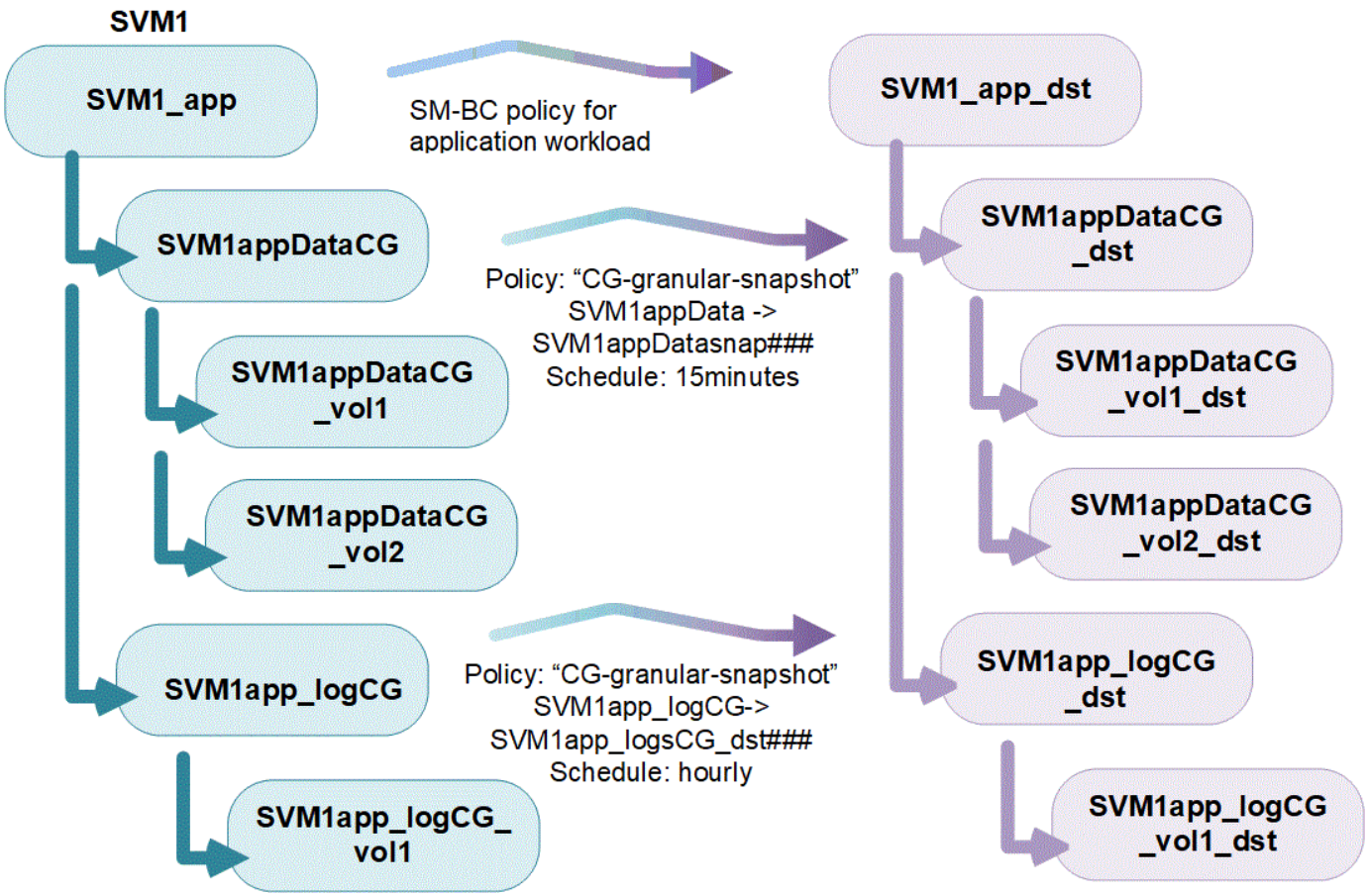
一致性群組可以是個別實體（即磁碟區集合）、也可以是由其他一致性群組所組成的階層式關係。個別磁碟區可以擁有自己的 Volume 精細快照原則。此外、整個群組的快照原則也可能一致。一致性群組只能有一個 SnapMirror 作用中同步關係和共用 SnapMirror 原則、可用於恢復整個一致性群組。

下圖說明如何使用個別一致性群組。託管在上的應用程式資料 `SVM1`**橫跨兩個磁碟區：** `vol1`**和** `vol2`。一致性群組的快照原則每 15 分鐘擷取一次資料快照。



較大的應用程式工作負載可能需要多個一致性群組。在這些情況下，您可以建立階層式一致性群組，其中單一一致性群組會成為父一致性群組的子元件。父一致性群組最多可包含五個子一致性群組。如同個別一致性群組、遠端 SnapMirror 主動式同步保護原則可套用至一致性群組（父群組和子群組）的整個組態、以恢復應用程式工作負載。

在下列範例中，應用程式是裝載於 `SVM1`。系統管理員已建立父一致性群組， `SVM1_app`其中包括兩個子一致性群組： `SVM1appDataCG`資料和 `SVM1app_logCG`記錄。每個子一致性群組都有自己的快照原則。中的磁碟區快照 `SVM1appDataCG`每 15 分鐘拍攝一次。的快照 `SVM1app_logCG`是每小時拍攝一次。父一致性群組 `SVM1_app`具有 SnapMirror 作用中同步原則，可複寫資料，確保在發生災難時仍能繼續提供服務。



從功能支援的版本起、一致性群組即為支援ONTAP 複製 並修改一致性的成員 新增或移除磁碟區 在System Manager和ONTAP the靜止API中。從 ONTAP 9.12.1 開始、 ONTAP REST API 也支援：

- 使用新的NFS或SMB磁碟區或NVMe命名空間來建立一致性群組。
- 將新的或現有的NFS或SMB磁碟區或NVMe命名空間新增至現有的一致性群組。

如需ONTAP 更多有關靜態API的資訊、請參閱 "REST API參考文件ONTAP"。

監控一致性群組

從 ONTAP 9.13.1 開始、一致性群組提供即時和歷史容量與效能監控、提供應用程式效能與個別一致性群組的深入見解。

監控資料會每五分鐘重新整理一次、最多可維護一年。您可以追蹤下列項目的計量：

- 效能： IOPS 、延遲和處理量
- 容量：大小、使用邏輯、可用

您可以在 System Manager 中一致性群組功能表的「 **Overview** （概要）」 標籤中檢視監控資料、或是在 REST API 中要求資料。從 ONTAP 9.14.1 開始，您可以使用命令 CLI 來檢視一致性群組度量 `consistency-`

`group metrics show`。如"指令參考資料ONTAP"需詳細 `consistency-group metrics show`資訊，請參閱。

> 在 ONTAP 9.13.1 中、您只能使用 REST API 擷取歷史指標。從 ONTAP 9.14.1 開始，系統管理員也提供歷史指標。

保護一致性群組

一致性群組提供應用程式一致的保護、確保資料在多個磁碟區或生命體之間的一致性。建立一致性群組的快照時，一致性群組上會建立「 Fence 」。Fence 會啟動 I/O 佇列，直到快照作業完成為止，確保資料在一致性群組中所有實體之間的時間點一致性。Fence 可能會在快照建立作業期間造成短暫延遲，例如排程快照原則或使用 System Manager 建立快照。在和中深入瞭解 REST API 和 CLI "指令參考資料ONTAP"的內容"ONTAP REST API 文件"。

一致性群組透過以下方式提供保護：

- Snapshot原則
- SnapMirror 主動同步
- [mcc] （從ONTAP 版本號《2019年9月11日》開始）
- SnapMirror 非同步 （從 ONTAP 9.13.1 開始）
- "SVM 災難恢復" （從 ONTAP 9.14.1 開始）

建立一致性群組不會自動啟用保護。建立一致性群組時或建立一致性群組之後、都可以設定本機和遠端保護原則。

若要在一致性群組上設定保護、請參閱 "保護一致性群組"。

若要使用遠端保護，您必須符合的要求SnapMirror 主動同步。

> SnapMirror 主動同步關係無法在掛載用於 NAS 存取的磁碟區上建立。

一致性群組的多重管理驗證支援

從 ONTAP 9 。 16.1 開始，您可以使用含一致性群組的多重管理驗證（ MAV ），確保某些作業（例如建立，修改或刪除一致性群組）只能在指定管理員核准之後執行。如此可防止遭入侵，惡意或缺乏經驗的系統管理員對現有組態進行不必要的變更。

"深入瞭解"

一致性群組的**MetroCluster** 不一致性

從ONTAP 功能更新9.11.1開始、您可以在MetroCluster 叢集上以全新的Volume配置一致性群組、並以功能更新的方式進行配置。這些磁碟區會配置在鏡射的集合體上。

配置好磁碟區之後、您可以在鏡射與無鏡射的集合體之間移動與一致性群組相關的磁碟區。因此、與一致性群組相關聯的磁碟區可位於鏡射Aggregate、無鏡射Aggregate或兩者上。您可以修改包含與一致性群組相關聯之磁碟區的鏡射Aggregate、使其變成無鏡射。同樣地、您也可以修改包含與一致性群組相關之磁碟區的無鏡射Aggregate、以啟用鏡射功能。

與放置在鏡射集合體上的一致性群組相關聯的磁碟區和快照會複寫到遠端站台（站台 B ）。站台 B 上的磁碟區內容為一致性群組提供寫入順序保證、可讓您在發生災難時從站台 B 恢復。您可以在執行 ONTAP 9.11.1 或更

新版本的叢集上，使用一致性群組與 REST API 和系統管理員來存取一致性群組快照。從 ONTAP 9.14.1 開始，您也可以使用 ONTAP CLI 存取快照。

如果與一致性群組相關聯的部分或所有磁碟區位於目前無法存取的無鏡射集合體上、則一致性群組上的Get或Delete作業會如同本機磁碟區或託管集合體離線一樣運作。

複寫的一致性群組組態

如果站台B執行ONTAP 的是版本號為NetApp 9.10.1或更新版本、則只有與鏡射集合體上的一致性群組相關聯的磁碟區會複寫到站台B如果兩個站台都執行ONTAP 的是版本號為「更新版本」、則一致性群組組態只會複寫到站台B。將站台B升級ONTAP 至支援版9.11.1之後、站台A上的一致性群組資料若將其所有相關的磁碟區放在鏡射集合體上、則會複寫至站台B

> 為了獲得最佳儲存效能和可用性，建議您為鏡像聚合保留至少 20% 的可用空間。雖然建議非鏡像聚合使用 10% 的空間，但額外的 10% 空間可供檔案系統吸收增量變更。由於 ONTAP 的基於寫入時重定向快照的架構，增量變更提高了鏡像聚合的空間利用率。未能遵守這些最佳實踐可能會對績效產生負面影響。

升級考量

當升級至 ONTAP 9 。 10.1 或更新版本時，使用 ONTAP 9 第 8 和 9.9.1 節中的 SnapMirror 主動式同步建立的一致性群組（先前稱為 SnapMirror 業務連續性）會自動升級，並可在系統管理員的 * 儲存 > 一致性群組 * 或 ONTAP REST API 中進行管理"SnapMirror 主動式同步升級與還原考量"，以取得有關從 ONTAP 9 第 8 或 9.9.1 節升級的詳細資訊，請參閱。

在 REST API 中建立的一致性群組快照可透過 System Manager 的一致性群組介面、以及一致性群組 REST API 端點來管理。從 ONTAP 9.14.1 開始，一致性群組快照也可透過 ONTAP CLI 進行管理。

> 使用 ONTAPI 命令建立的快 `cg-start` `cg-commit`照無法辨識為一致性群組快照，因此無法透過系統管理員的一致性群組介面或 ONTAP REST API 中的一致性群組端點進行管理。從 ONTAP 9.14.1 開始，如果您使用 SnapMirror 非同步原則，這些快照可以鏡射到目的地 Volume 。如需更多資訊、請參閱 設定 SnapMirror 非同步。

各版本支援的功能

	ONTAP 9.16.1.	**ONTAP 9.15.1.1**	**ONTAP 9.14.1.**	**ONTAP 9.13.1.12 .9.11.9.1 1.**	**ONTAP 9.12.1**	**零點9.11. 1. ONTAP**	**零點9.10. 1 ONTAP**
階層式一致性群組	✓	✓	✓	✓	✓	✓	✓
利用快照提供本機保護	✓	✓	✓	✓	✓	✓	✓
SnapMirror 主動同步	✓	✓	✓	✓	✓	✓	✓
支援 MetroCluster	✓	✓	✓	✓	✓	✓	
兩階段認可（僅限 REST API ）	✓	✓	✓	✓	✓	✓	
應用程式與元件標籤	✓	✓	✓	✓	✓		
複製一致性群組	✓	✓	✓	✓	✓		
新增和移除磁碟區	✓	✓	✓	✓	✓		

	ONTAP 9.16.1.	ONTAP 9.15.1.1	ONTAP 9.14.1.	ONTAP 9.13.1.12 .9.11.9.1 1.	ONTAP 9.12.1	零點9.11. 1. ONTAP	零點9.10. 1 ONTAP
使用新的 NAS 磁碟區建立 CGS	✓	✓	✓	✓	僅REST API		
使用新的 NVMe 命名空間建立 CGS	✓	✓	✓	✓	僅REST API		
在子一致性群組之間移動磁碟區	✓	✓	✓	✓			
修改一致性群組幾何	✓	✓	✓	✓			
監控	✓	✓	✓	✓			
多管理員驗證	✓						
SnapMirror 非同步（僅限單一一致性群組）	✓	✓	✓	✓			
SVM 災難恢復（僅限單一一致性群組）	✓	✓	✓				
CLI 支援	✓	✓	✓				

深入瞭解一致性群組

相關資訊

- "ONTAP 自動化文件"
- SnapMirror 主動同步

- SnapMirror 非同步災難恢復基礎知識
- "本文檔MetroCluster"
- "多管理員驗證"
- "指令參考資料ONTAP"

了解ONTAP一致性組限制

規劃及管理一致性群組時、請同時考量叢集與父或子一致性群組範圍內的物件限制。

強制限制

下表擷取一致性群組的限制。使用 SnapMirror 主動式同步、將一致性群組套用到個別的限制。如需詳細資訊、請參閱 "SnapMirror 主動同步限制"。

限制	範圍	最低	最大值
一致性群組數	叢集	0%	與叢集 * 中的最大磁碟區數相同
父一致性群組數	叢集	0%	與叢集中的最大Volume數相同
個別與父一致性群組的數量	叢集	0%	與叢集中的最大Volume數相同
一致性群組中的磁碟區數量	單一一致性群組	1 個 Volume	80 個磁碟區
SnapMirror 非同步一致性群組中的磁碟區數量	單一一致性群組	1 個 Volume	• 在 ONTAP 9.15.1 及更新版本中： 80 個 Volume • 在 ONTAP 9.13.1 和 9.14.1 中： 16 個 Volume
父一致性群組子系中的磁碟區數目	父一致性群組	1 個 Volume	80 個磁碟區
子一致性群組中的磁碟區數目	子一致性群組	1 個 Volume	80 個磁碟區
父一致性群組中的子一致性群組數	父一致性群組	1 個一致性群組	5 個一致性群組
存在一致性群組的 SVM 災難恢復關係數（從 ONTAP 9.14.1 開始提供）	叢集	0%	32.

｛Asterisk｝ 使用 SnapMirror 非同步功能、最多可託管 50 個一致性群組。

未強制執行的限制

一致性群組支援的最少快照排程為 30 分鐘。這是基於"測試 FlexGroup Volume"，它與一致性組共享相同的

Snapshot 基礎架構。

配置單一ONTAP一致性組

可以使用現有的磁碟區或新的 LUN 或磁碟區來建立一致性群組（視 ONTAP 版本而定）。磁碟區或 LUN 一次只能與一個一致性群組建立關聯。

關於這項工作

- 在 ONTAP 9.10.1 至 9.11.1 中、不支援在建立一致性群組之後修改其成員磁碟區。

  從 ONTAP 9.12.1 開始、您可以修改一致性群組的成員磁碟區。如需此程序的詳細資訊、請參閱 修改一致性群組。

- 從ONTAP 9.17.1 開始，您可以選擇 NVMe 協定將主機對應到SnapMirror主動同步設定中 VMware 工作負載的 NVMe 子系統。

使用新的 **LUN** 或磁碟區建立一致性群組

在 ONTAP 9.10.1 至 9.12.1 中、您可以使用新的 LUN 建立一致性群組。從 ONTAP 9.13.1 開始、 System Manager 也支援使用新的 NVMe 命名空間或新的 NAS 磁碟區來建立一致性群組。（從 ONTAP 9.12.1 開始、ONTAP REST API 也支援此功能。）

系統管理員（**ONTAP 9.16.1** 及更早版本）

步驟

1. 選擇*儲存>一致性群組*。
2. 選取 **+Add** 、然後選取儲存物件的傳輸協定。

   在 ONTAP 9.10.1 至 9.12.1 中、新儲存物件的唯一選項是 使用新的 **LUN** 。從 ONTAP 9.13.1 開始、System Manager 支援使用新的 NVMe 命名空間和新的 NAS 磁碟區來建立一致性群組。

3. 命名一致性群組。指定磁碟區或 LUN 的數量、以及每個磁碟區或 LUN 的容量。
   a. 應用程式類型*：如果您使用**ONTAP** 的是更新版本的版本、請選取應用程式類型。如果未選取任何值、系統將預設指派類型為「其他*」。深入瞭解中的標記一致性 應用程式與元件標籤。如果您打算使用遠端保護原則建立一致性群組、則必須使用 * 其他 * 。
   b. 對於 新 **LUN** ：選擇主機作業系統和 LUN 格式。輸入主機啟動器資訊。
   c. 對於 新 **NAS Volume** ：根據 SVM 的 NAS 組態、選擇適當的匯出選項（ NFS 或 SMB/CIFS ）。
   d. 對於 新的 **NVMe** 命名空間 ：選取主機作業系統和 NVMe 子系統。
4. 若要設定保護原則、新增子一致性群組或存取權限、請選取 * 更多選項 * 。
5. 選擇*保存*。
6. 請返回工作完成後顯示的主要一致性群組功能表、確認您的一致性群組已建立。如果您設定了保護原則、當您在適當的原則（遠端或本機）下看到綠色保護罩時、就會知道它已套用。

系統管理員（**ONTAP 9.17.1** 及更高版本）

步驟

1. 選擇*保護>一致性群組*。
2. 選取 **+Add** 、然後選取儲存物件的傳輸協定。
3. 為一致性組命名。指定磁碟區或 LUN 的數量以及每個磁碟區或 LUN 的容量。應用程式類型：選擇應用程式類型。如果未選擇任何值，則一致性組將預設指派其他類型。了解更多關於標記一致性的信息，請參閱應用程式與元件標籤 。如果您打算建立具有遠端保護策略的一致性群組，則必須使用*其他*。
   a. 對於 新 **LUN** ：選擇主機作業系統和 LUN 格式。輸入主機啟動器資訊。
   b. 對於 新 **NAS Volume** ：根據 SVM 的 NAS 組態、選擇適當的匯出選項（ NFS 或 SMB/CIFS ）。
   c. 對於 新的 **NVMe** 命名空間 ：選取主機作業系統和 NVMe 子系統。
4. 若要設定保護原則、新增子一致性群組或存取權限、請選取 * 更多選項 * 。
5. 選擇*保存*。
6. 請返回工作完成後顯示的主要一致性群組功能表、確認您的一致性群組已建立。如果您設定了保護原則、當您在適當的原則（遠端或本機）下看到綠色保護罩時、就會知道它已套用。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 建立新的一致性群組與新的磁碟區。具體參數取決於磁碟區是 SAN 、 NVMe 或 NFS 。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

使用 **NFS** 磁碟區建立一致性群組

1. 建立一致性群組：

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -volume-prefix <prefix_for_new_volume_names>
-volume-count <number> -size <size> -export-policy <policy_name>
```

使用 **SAN** 磁碟區建立一致性群組

1. 建立一致性群組：

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency-group-name> -lun <lun_name> -size <size> -lun-count <number>
-lun-os-type <LUN_operating_system_format> -igroup <igroup_name>
```

使用 **NVMe** 命名空間建立一致性群組

1. 建立一致性群組：

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -namespace <namespace_name> -volume-count <number>
-namespace-count <number> -size <size> -subsystem <subsystem_name>
```

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

完成後

1. 確認您的一致性群組已使用建立 `consistency-group show` 命令。

如"指令參考資料ONTAP"需詳細 `consistency-group show`資訊，請參閱。

使用現有磁碟區建立一致性群組

您可以使用現有的磁碟區來建立一致性群組。

系統管理員（**ONTAP 9.16.1** 及更早版本）

步驟

1. 選擇*儲存>一致性群組*。
2. 選擇「**+**新增」、然後選擇「使用現有磁碟區」。
3. 命名一致性群組、然後選取儲存VM。
   a. 應用程式類型*：如果您使用**ONTAP** 的是更新版本的版本、請選取應用程式類型。如果未選取任何值、系統將預設指派類型為「其他*」。深入瞭解中的標記一致性 應用程式與元件標籤。如果一致性組具有 SnapMirror 活動同步關係，則必須使用 * 其他 * 。

      在 ONTAP 9.15.1 之前的 ONTAP 版本中， SnapMirror 活動同步稱爲 SnapMirror 業務連續性。

4. 選取要納入的現有磁碟區。只有尚未納入一致性群組的磁碟區可供選擇。

   如果使用現有磁碟區建立一致性群組、一致性群組就會支援FlexVol 使用各種功能。可以將具有或 SnapMirror 同步或 SnapMirror 非同步關係的磁碟區新增至一致性群組、但這些磁碟區並不具備一致性群組感知功能。一致性群組不支援與 SVMDR 關係的 S3 儲存區或儲存 VM 。

5. 選擇*保存*。
6. 確認已建立一致性群組、方法是回到 ONTAP 工作完成後出現的主要一致性群組功能表。如果您已選擇保護原則、請從功能表中選取您的一致性群組、以確認該原則已正確設定。如果您設定了保護原則、當您在適當的原則（遠端或本機）下方看到綠色盾牌時、就會知道它已套用。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 建立與現有磁碟區一致的群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 發行 `consistency-group create` 命令。。 `-volumes` 參數接受以逗號分隔的磁碟區名稱清單。

   ```
   consistency-group create -vserver <SVM_name> -consistency-group
   <consistency-group-name> -volume <volumes>
   ```

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

2. 使用檢視一致性群組 `consistency-group show` 命令。

   如"指令參考資料ONTAP"需詳細 `consistency-group show`資訊，請參閱。

後續步驟

- 保護一致性群組
- 修改一致性群組
- 複製一致性群組

配置分層ONTAP一致性組

階層式一致性群組可讓您管理跨越多個磁碟區的大型工作負載、建立父一致性群組、作為子一致性群組的保護傘。

階層式一致性群組具有父群組、最多可包含五個個別的一致性群組。階層式一致性群組可支援跨一致性群組或個別磁碟區的不同本機快照原則。如果您使用遠端保護原則、則會套用至整個階層式一致性群組（父和子）。

從 ONTAP 9.13.1 開始、您就可以 修改一致性群組的幾何 和 在子一致性群組之間移動磁碟區。

如需一致性群組的物件限制、請參閱 一致性群組的物件限制。

使用新的 **LUN** 或磁碟區建立階層式一致性群組

建立階層式一致性群組時、您可以使用新的LUN來填入群組。從 ONTAP 9.13.1 開始、您也可以使用新的 NVMe 命名空間和 NAS 磁碟區。

系統管理員

步驟

1. 選擇*儲存>一致性群組*。
2. 選取 **+Add** 、然後選取儲存物件的傳輸協定。

   在 ONTAP 9.10.1 至 9.12.1 中、新儲存物件的唯一選項是 使用新的 **LUN** 。從 ONTAP 9.13.1 開始、System Manager 支援使用新的 NVMe 命名空間和新的 NAS 磁碟區來建立一致性群組。

3. 命名一致性群組。指定磁碟區或 LUN 的數量、以及每個磁碟區或 LUN 的容量。
   a. 應用程式類型*：如果您使用**ONTAP** 的是更新版本的版本、請選取應用程式類型。如果未選取任何值、系統將預設指派類型為「其他*」。深入瞭解中的標記一致性 應用程式與元件標籤。如果您打算使用遠端保護原則、則必須選擇 * 其他 * 。
4. 選取主機作業系統和LUN格式。輸入主機啟動器資訊。
   a. 對於 新 **LUN** ：選擇主機作業系統和 LUN 格式。輸入主機啟動器資訊。
   b. 對於 新 **NAS Volume** ：根據 SVM 的 NAS 組態、選擇適當的匯出選項（ NFS 或 SMB/CIFS ）。
   c. 對於 新的 **NVMe** 命名空間 ：選取主機作業系統和 NVMe 子系統。
5. 若要新增子一致性群組、請選取 * 更多選項 * 、然後選取 *+ 新增子一致性群組 * 。
6. 選取效能層級、 LUN 或磁碟區數量、以及每個 LUN 或磁碟區的容量。根據您使用的傳輸協定、指定適當的匯出組態或作業系統資訊。
7. 您也可以選擇本機快照原則、並設定存取權限。
8. 重複最多五個子一致性群組。
9. 選擇*保存*。
10. 請返回主一致性群組功能表、確認您的一致性群組已建立、ONTAP 一旦完成此工作、就會顯示在該功能表中。如果您設定保護原則、請查看適當的原則（遠端或本機）、此原則應會顯示綠色的遮罩、並勾選其中的核取符號。

CLI

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

在 CLI 中建立具有新磁碟區的階層式一致性群組時、您必須個別建立每個子一致性群組。

步驟

1. 使用建立新的一致性群組 `consistency-group create` 命令。

```
consistency-group create -vserver <SVM_name> -consistency-group
<consistency_group_name> -parent-consistency-group
<parent_consistency_group_name> -volume-prefix <volume_prefix> -volume
-count <number_of_volumes> -size <size>
```

2. 當 CLI 提示時、請確認您要建立新的父一致性群組。輸入。 `y`
3. 或者、重複步驟 1 以建立更多子一致性群組。

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

使用現有的磁碟區建立階層式一致性群組

您可以將現有的磁碟區組織成階層式一致性群組。

系統管理員

步驟

1. 選擇*儲存>一致性群組*。
2. 選擇「+新增」、然後選擇「使用現有磁碟區」。
3. 選取儲存VM。
4. 選取要納入的現有磁碟區。只有尚未納入一致性群組的磁碟區可供選擇。
5. 若要新增子一致性群組、請選取*+新增子一致性群組*。建立必要的一致性群組、並自動命名。
   a. 元件類型*：如果您使用**ONTAP** 的是更新版本的版本、請選取「資料」、「記錄」或「其他」等元件類型。如果未選取任何值、系統將預設指派類型為「其他*」。深入瞭解中的標記一致性 應用程式與元件標籤。如果您打算使用遠端保護原則、則必須使用 * 其他 * 。
6. 將現有磁碟區指派給每個一致性群組。
7. 您也可以選擇本機快照原則。
8. 重複最多五個子一致性群組。
9. 選擇*保存*。
10. 請返回主一致性群組功能表、確認您的一致性群組已建立、ONTAP 一旦完成此工作、就會顯示在該功能表中。如果您已選擇保護原則、請從功能表中選取一致性群組、以確認其設定正確；在適當的原則類型下、您會看到一個綠色的遮罩、其中會有核取符號。

CLI

從 ONTAP 9.14.1 開始、您可以使用 CLI 建立階層式一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 配置新的父一致性群組、並將磁碟區指派給新的子一致性群組：

   ```
   consistency-group create -vserver <svm_name> -consistency-group
   <child_consistency_group_name> -parent-consistency-group
   <parent_consistency_group_name> -volumes <volume_names>
   ```

2. 輸入 `y` 確認您要建立新的父和子一致性群組。

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

後續步驟

- 修改一致性群組的幾何
- 修改一致性群組
- 保護一致性群組

保護ONTAP一致性組

一致性群組可輕鬆管理跨多個磁碟區的SAN、NAS和NVMe應用程式的本機和遠端保護。

建立一致性群組不會自動啟用保護。保護原則可以在建立時或建立一致性群組之後設定。您可以使用下列方法來保護一致性群組：

- 本機快照
- SnapMirror 主動同步（在 9.15.1 之前的 ONTAP 版本中稱爲 SnapMirror 業務連續性）
- MetroCluster （自 9.11.1 起）
- SnapMirror 非同步（從 9.13.1 開始）
- 非同步 SVM 災難恢復（從 9.14.1 開始）

如果您使用巢狀一致性群組、可以為父和子一致性群組設定不同的保護原則。

從 ONTAP 9.11.1 開始建立雙階段一致性群組快照，一致性群組提供。兩階段快照作業會執行預先檢查，確保成功擷取快照。

可以針對整個一致性群組、階層式組態中的單一一致性群組、或是一致性群組中的個別磁碟區進行還原。您可以選取要從中恢復的一致性群組，選取快照類型，然後識別要作為還原基礎的快照，以達成恢復。如需此程序的詳細資訊，請參閱"從較早的快照還原磁碟區"。

設定本機快照原則

設定本機快照保護原則可讓您建立橫跨一致性群組中所有磁碟區的原則。

關於這項工作

一致性群組支援的最少快照排程為 30 分鐘。這是基於"測試 FlexGroup Volume"，它與一致性組共享相同的 Snapshot 基礎架構。

系統管理員

步驟

1. 選擇*儲存>一致性群組*。
2. 從一致性群組功能表中選取您所建立的一致性群組。
3. 在一致性群組的總覽頁面右上角、選取*編輯*。
4. 選取*計劃快照（本地）*旁邊的複選框。
5. 選取快照原則。若要設定新的自訂原則，請參閱"建立自訂資料保護原則"。
6. 選擇*保存*。
7. 返回一致性群組總覽功能表。在 * 快照（本機） * 下的左欄中，狀態會顯示為 「 protected 」（已保護）。

CLI

從 ONTAP 9.14.1 開始、您可以使用 CLI 修改一致性群組的保護原則。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 發出下列命令來設定或修改保護原則：

   如果您要修改子系一致性的保護原則、則必須使用來識別父一致性群組 `-parent-consistency-group` *`parent_consistency_group_name`* 參數。

   ```
   consistency-group modify -vserver svm_name -consistency-group
   consistency_group_name -snapshot-policy policy_name
   ```

建立隨需快照

如果您需要在正常排程原則之外建立一致性群組的快照，可以根據需要建立一個快照。

系統管理員

步驟

1. 瀏覽至 * 儲存 * > * 一致性群組 * 。
2. 選取您要為其建立隨選快照的一致性群組。
3. 切換至 * Snapshot Copies （快照複本） * 標籤、然後選取 **+Add** （ **+Add** ）。
4. 提供 * 名稱 * 和 * SnapMirror 標籤 * 。在 * 一致性 * 的下拉式功能表中、選取 * 應用程式一致 * 或 * 損毀一致 * 。
5. 選擇*保存*。

CLI

從 ONTAP 9.14.1 開始，您可以使用 CLI 建立一致性群組的隨選快照。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 建立快照：

   根據預設，快照類型會當機一致。您可以使用選用參數修改快照類型 `-type`。

   ```
   consistency-group snapshot create -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

建立雙階段一致性群組快照

從 ONTAP 9.11.1 開始，一致性群組支援建立一致性群組（ CG ）快照的兩階段承諾，在提交快照之前執行預先檢查。此功能只能搭配ONTAP 使用靜態API。

建立兩階段 CG 快照僅適用於建立快照，不提供一致性群組或還原一致性群組。

兩階段 CG 快照可將快照建立程序分為兩個階段：

1. 在第一階段， API 會執行預先檢查並觸發建立快照。第一階段包括逾時參數，指定快照成功提交的時間量。
2. 如果第一階段中的要求成功完成，您可以從第一階段開始，在指定的時間間隔內叫用第二階段，並將快照提交至適當的端點。

開始之前

- 若要使用兩階段 CG 快照建立，叢集中的所有節點都必須執行 ONTAP 9.11.1 或更新版本。
- 一致性群組執行個體一次只支援一個作用中的一致性群組快照作業呼叫，無論是一階段或兩階段。嘗試在另一個正在執行的快照作業時叫用快照作業，會導致失敗。
- 當您叫用快照建立時，您可以設定 5 到 120 秒之間的選擇性逾時值。如果未提供逾時值、則作業會在預設的 7 秒時逾時。在 API 中，使用參數設定逾時值 `action_timeout`。在 CLI 中，使用 `-timeout`旗標。

步驟

您可以使用 REST API 或從 ONTAP 9.14.1 開始，使用 ONTAP CLI 完成兩階段快照。System Manager 不支援此作業。

如果您使用 API 來叫用快照建立，則必須使用 API 來提交快照。如果使用 CLI 調用快照創建，則必須使用 CLI 提交快照。不支援混合方法。

CLI

從 ONTAP 9.14.1 開始，您可以使用 CLI 建立兩階段快照。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 啟動快照：

   ```
   consistency-group snapshot start -vserver svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name [-timeout time_in_seconds
   -write-fence {true|false}]
   ```

2. 驗證是否已拍攝快照：

   ```
   consistency-group snapshot show
   ```

3. 提交快照：

   ```
   consistency-group snapshot commit svm_name -consistency-group
   consistency_group_name -snapshot snapshot_name
   ```

API

1. 叫用快照建立。使用參數將 POST 要求傳送至一致性群組端點 `action=start`。

   ```
   curl -k -X POST 'https://<IP_address>/application/consistency-
   groups/<cg-uuid>/snapshots?action=start&action_timeout=7' -H
   "accept: application/hal+json" -H "content-type: application/json"
   -d '
   {
     "name": "<snapshot_name>",
     "consistency_type": "crash",
     "comment": "<comment>",
     "snapmirror_label": "<SnapMirror_label>"
   }'
   ```

2. 如果 POST 要求成功，則輸出會包含快照 UUID 。使用該 uuid 提交修補程式要求以提交快照。

```
curl -k -X PATCH 'https://<IP_address>/application/consistency-
groups/<cg_uuid>/snapshots/<snapshot_id>?action=commit' -H "accept:
application/hal+json" -H "content-type: application/json"

For more information about the ONTAP REST API, see
link:https://docs.netapp.com/us-en/ontap-
automation/reference/api_reference.html[API reference^] or the
link:https://devnet.netapp.com/restapi.php[ONTAP REST API page^] at
the NetApp Developer Network for a complete list of API endpoints.
```

設定一致性群組的遠端保護

一致性群組可透過 SnapMirror 主動式同步提供遠端保護、從 ONTAP 9 。 13.1 開始即為 SnapMirror 非同步。

使用 **SnapMirror** 主動同步設定保護

您可以使用 SnapMirror 主動式同步，確保將在一致性群組上建立的一致性群組快照複製到目的地。若要深入瞭解 SnapMirror 作用中同步或如何使用 CLI 設定 SnapMirror 作用中同步處理，請參閱設定保護以確保營運不中斷。

開始之前

- SnapMirror 主動同步關係無法在掛載用於 NAS 存取的磁碟區上建立。
- 來源叢集和目的地叢集中的原則標籤必須相符。
- SnapMirror 主動式同步功能預設不會複寫快照，除非已將具有 SnapMirror 標籤的規則新增至預先定義的 `AutomatedFailOver`原則，且快照是以該標籤建立的。

  若要深入瞭解此程序、請參閱 "使用 SnapMirror 主動同步進行保護"。

- 串聯部署 SnapMirror 主動同步不支援。
- 從 ONTAP 9.13.1 開始、您可以不中斷營運 將磁碟區新增至一致性群組 使用主動 SnapMirror 主動同步關係。對一致性群組所做的任何其他變更、都需要您中斷 SnapMirror 作用中同步關係、修改一致性群組、然後重新建立並重新同步關係。

若要使用 CLI 設定 SnapMirror 主動式同步、請參閱 使用 SnapMirror 主動同步進行保護。

System Manager 的步驟

1. 確保您已符合 "使用 SnapMirror 主動同步的先決條件"。
2. 選擇*儲存>一致性群組*。
3. 從一致性群組功能表中選取您所建立的一致性群組。
4. 在總覽頁面右上角、選取*更多*、然後選取*保護*。
5. System Manager 會自動填入來源端資訊。為目的地選取適當的叢集和儲存VM。選取保護原則。確保選中*初始化關係*。
6. 選擇*保存*。

7. 一致性群組需要初始化及同步處理。返回 **consistency group** 功能表、確認同步已成功完成。旁邊會顯示 *SnapMirror （遠端） * 狀態 `Protected` 。

設定 **SnapMirror** 非同步

從 ONTAP 9.13.1 開始、您可以為單一一致性群組設定 SnapMirror 非同步保護。從 ONTAP 9.14.1 開始，您可以使用 SnapMirror 非同步功能，使用一致性群組關係，將 Volume 精細的快照複寫到目的地叢集。

關於這項工作

若要複寫 Volume 精細的快照，您必須執行 ONTAP 9.14.1 或更新版本。對於 MirrorAndVault 和 Vault 原則，Volume 精細快照原則的 SnapMirror 標籤必須符合一致性群組的 SnapMirror 原則規則。Volume 精細快照符合一致性群組 SnapMirror 原則的保留值，該原則是在一致性群組快照之外的情況下進行計算。例如，如果您有原則在目的地上保留兩個快照，則可以有兩個 Volume 精細快照和兩個一致性群組快照。

當重新同步 SnapMirror 與 Volume 精細快照的關係時，您可以使用旗標保留 Volume 精細的快照 `-preserve`。保留比一致性群組快照更新的 Volume 精細快照。如果沒有一致性群組快照，則無法在重新同步作業中傳輸 Volume 精細的快照。

開始之前

- SnapMirror 非同步保護僅適用於單一一致性群組。階層式一致性群組不支援此功能。若要將階層式一致性群組轉換成單一一致性群組、請參閱 修改一致性群組架構。
- 來源叢集和目的地叢集中的原則標籤必須相符。
- 您可以不中斷營運 將磁碟區新增至一致性群組 使用主動 SnapMirror 非同步關係。對一致性群組所做的任何其他變更、都需要您中斷 SnapMirror 關係、修改一致性群組、然後重新建立並重新同步關係。
- 啟用 SnapMirror 非同步保護的一致性群組有不同的限制。如需詳細資訊、請參閱 一致性群組限制。
- 如果您已為多個個別磁碟區設定 SnapMirror 非同步保護關係，則可以將這些磁碟區轉換成一致性群組，同時保留現有的快照。若要成功轉換磁碟區：
  - 磁碟區必須有通用的快照。
  - 您必須打破現有的 SnapMirror 關係、 將磁碟區新增至單一一致性群組，然後使用以下工作流程重新同步關係。

步驟

1. 從目的地叢集選取 * 儲存 > 一致性群組 * 。
2. 從一致性群組功能表中選取您所建立的一致性群組。
3. 在總覽頁面右上角、選取*更多*、然後選取*保護*。
4. System Manager 會自動填入來源端資訊。為目的地選取適當的叢集和儲存VM。選取保護原則。確保選中*初始化關係*。

   選取非同步原則時、您可以選擇「 置換傳輸排程 」。

   SnapMirror 非同步的一致性群組支援的最低排程（恢復點目標、或 RPO ）為 30 分鐘。

5. 選擇*保存*。
6. 一致性群組需要初始化及同步處理。返回 **consistency group** 功能表、確認同步已成功完成。旁邊會顯示 *SnapMirror （遠端） * 狀態 `Protected` 。

設定 **SVM** 災難恢復

從 ONTAP 9.14.1 開始，SVM 災難恢復支援一致性群組，可讓您將一致性群組資訊從來源叢集鏡射到目的地叢集。

如果您要在已包含一致性群組的 SVM 上啟用 SVM 災難恢復、請遵循的 SVM 組態工作流程 系統管理員 或 CLI ONTAP。

如果您要將一致性群組新增至 SVM 、而 SVM 是處於作用中且健全的 SVM 災難恢復關係中、則必須從目的地叢集更新 SVM 災難恢復關係。如需詳細資訊、請參閱 手動更新複寫關係。您必須在擴充一致性群組時隨時更新關係。

限制

- SVM 災難恢復不支援階層式一致性群組。
- SVM 災難恢復不支援使用 SnapMirror 非同步保護的一致性群組。您必須先中斷 SnapMirror 關係、才能設定 SVM 災難恢復。
- 兩個叢集都必須執行 ONTAP 9.14.1 或更新版本。
- 包含一致性群組的 SVM 災難恢復組態不支援開機關係。
- 如需其他限制、請參閱 一致性群組限制。

視覺化關係

System Manager 會在 * 保護 > 資料庫關聯圖 * 功能表下、視覺化 LUN 對應。當您選取來源關係時、System Manager會顯示來源關係的視覺化。選取磁碟區之後、您可以深入瞭解這些關係、以查看包含的LUN清單和啟動器群組關係。此資訊可從個別的 Volume 檢視下載為 Excel 活頁簿、下載作業會在背景執行。

相關資訊

- "複製一致性群組"
- "設定快照"
- "建立自訂資料保護原則"
- "從快照中恢復"
- "從較早的快照還原磁碟區"
- "SnapMirror 主動式同步總覽"
- "ONTAP 自動化文件"
- SnapMirror 非同步災難恢復基礎知識

修改**ONTAP**一致性群組中的成員卷

從 ONTAP 9.12.1 開始、您可以移除磁碟區或新增磁碟區（擴充一致性群組）來修改一致性群組。從 ONTAP 9.13.1 開始、如果子一致性群組共用同一個父磁碟區、您就可以在它們之間移動磁碟區。

將磁碟區新增至一致性群組

從 ONTAP 9.12.1 開始、您可以不中斷地將磁碟區新增至一致性群組。

關於這項工作

- 您無法新增與其他一致性群組相關聯的磁碟區。
- 一致性群組支援NAS、SAN和NVMe傳輸協定。
- 如果調整在整體範圍內、您可以一次最多新增 16 個磁碟區至一致性群組 一致性群組限制。
- 從 ONTAP 9 。 13.1 開始、您可以使用主動式 SnapMirror 主動式同步或 SnapMirror 非同步保護原則、以不中斷營運的方式將磁碟區新增至一致性群組。
- 當您將磁碟區新增至受 SnapMirror 主動式同步保護的一致性群組時、 SnapMirror 主動式同步關係狀態會變更為「展開」、直到為新磁碟區設定鏡像和保護為止。如果在完成此程序之前發生主叢集上的災難、一致性群組會在容錯移轉作業中還原為其原始組成。
- 在 ONTAP 9.12.1 及更早版本中、您無法在 SnapMirror 主動式同步關係中將磁碟區新增至一致性群組。您必須先刪除 SnapMirror 主動同步關係、修改一致性群組、然後使用 SnapMirror 主動同步還原保護。
- 從 ONTAP 9.12.1 開始、 ONTAP REST API 支援新增 *new* 或現有磁碟區至一致性群組。如需ONTAP 更多有關靜態API的資訊、請參閱 "REST API參考文件ONTAP"。

  從 ONTAP 9.13.1 開始、系統管理員就支援此功能。
- 展開一致性群組時，在修改之前擷取的一致性群組快照將視為部分快照。任何以該快照為基礎的還原作業，都會在快照的時間點反映一致性群組。
- 如果您使用ONTAP 的是從版本9.10.1到9.11.1、則無法修改一致性群組。若要變更ONTAP 《支援一致性》（NetApp）9.10.1或9.11.1中的一致性群組組態、您必須刪除一致性群組、然後建立新的一致性群組來加入您要的磁碟區。
- 從 ONTAP 9.14.1 開始，您可以在使用 SnapMirror 非同步時，將 Volume 精細的快照複寫到目的地叢集。使用 SnapMirror 非同步擴充一致性群組時，只有在 SnapMirror 原則為 MirrorAll 或 MirrorAndVault 時，才會在擴充一致性群組之後複寫 Volume 精細的快照。只會複寫比基準一致性群組快照更新的 Volume 精細快照。
- 如果您將磁碟區新增至 SVM 災難復原關係（從ONTAP 9.14.1 開始支援）中的一致性群組，則必須在擴充一致性群組後從目標叢集更新 SVM 災難復原關係。有關更多信息，請參閱手動更新複寫關係 。
- 如果您將 NVMe 與ONTAP 9.17.1 一起使用，則無法修改一致性群組。

範例 **31.** 步驟

系統管理員

從 ONTAP 9.12.1 開始、您可以使用系統管理員來執行此作業。

1. 選擇*儲存>一致性群組*。
2. 選取您要修改的一致性群組。
3. 如果要修改單一一致性群組、請在* Volumes（磁碟區）功能表頂端、選取 More（更多）、然後選取 expand（*擴充）*以新增磁碟區。

   如果您要修改子一致性群組、請識別您要修改的父一致性群組。選取 **>** 按鈕以檢視子一致性群組、然後選取 ⋮ 您要修改的子一致性群組名稱旁的。從該功能表中選取*展開*。

4. 選取最多16個磁碟區以新增至一致性群組。
5. 選擇*保存*。當作業完成時、請在一致性群組的 * Volumes * （磁碟區）功能表中檢視新增的磁碟區。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 將磁碟區新增至一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

新增現有磁碟區

1. 發出下列命令。。 `-volumes` 參數接受以逗號分隔的磁碟區清單。

   僅包含 `-parent-consistency-group` 如果一致性群組處於階層關係中、則為參數。

   ```
   consistency-group volume add -vserver svm_name -consistency-group
   consistency_group_name -parent-consistency-group parent_consistency_group
   -volume volumes
   ```

新增磁碟區

新增磁碟區的程序取決於您使用的傳輸協定。

僅包括 `-parent-consistency-group`如果一致性組具有層次關係，則為參數。

- 若要新增新的 Volume 而不匯出：

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  child_consistency_group -parent-consistency-group existingParentCg -volume
  volume_name -size size
  ```

- 若要新增 NFS 磁碟區：

  ```
  consistency-group volume create -vserver SVM_name -consistency-group
  ```

```
consistency-group-name -volume volume-prefix -volume-count number -size
size -export-policy policy_name
```

- 若要新增 SAN 磁碟區：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency-group-name -lun lun_name -size size -lun-count number -igroup
igroup_name
```

- 若要新增 NVMe 命名空間：

```
consistency-group volume create -vserver SVM_name -consistency-group
consistency_group_name -namespace namespace_name -volume-count number
-namespace-count number -size size -subsystem subsystem_name
```

從一致性群組移除磁碟區

不會刪除從一致性群組移除的磁碟區。它們在叢集中仍處於作用中狀態。

關於這項工作

- 您無法從 SnapMirror 主動同步或 SVM 災難恢復關係中的一致性群組移除 Volume 。您必須先刪除 SnapMirror 作用中同步關係、才能修改一致性群組、然後重新建立關係。
- 如果一致性群組在移除作業之後沒有磁碟區、則會刪除一致性群組。
- 從一致性群組移除磁碟區時，一致性群組的現有快照仍會保留，但視為無效。現有的快照無法用來還原一致性群組的內容。Volume 精細快照仍有效。
- 如果您從叢集刪除磁碟區、它會自動從一致性群組中移除。
- 若要變更ONTAP 《支援一致性》（NetApp）9.10.1或9.11.1中一致性群組的組態、您必須先刪除一致性群組、然後再建立新的一致性群組與所需的成員磁碟區。
- 從叢集中刪除磁碟區將自動將其從一致性群組中刪除。

系統管理員

從 ONTAP 9.12.1 開始、您可以使用系統管理員來執行此作業。

步驟

1. 選擇*儲存>一致性群組*。
2. 選取您要修改的單一或子一致性群組。
3. 在* Volumes（磁碟區）*功能表中、選取您要從一致性群組中移除的個別磁碟區旁的核取方塊。
4. 選取*從一致性群組中移除磁碟區*。
5. 確認您瞭解移除磁碟區將導致一致性群組的所有快照失效，並選取 * 移除 * 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 CLI 從一致性群組中移除磁碟區。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

步驟

1. 移除磁碟區。。 `-volumes` 參數接受以逗號分隔的磁碟區清單。

   僅包含 `-parent-consistency-group` 如果一致性群組處於階層關係中、則為參數。

   ```
   consistency-group volume remove -vserver SVM_name -consistency-group
   consistency_group_name -parent-consistency-group
   parent_consistency_group_name -volume volumes
   ```

在一致性群組之間移動磁碟區

從 ONTAP 9.13.1 開始、您可以在共用父實體的子一致性群組之間移動磁碟區。

關於這項工作

- 您只能在同一個父一致性群組之下巢狀的一致性群組之間移動磁碟區。
- 現有的一致性群組快照無效，無法再作為一致性群組快照存取。個別 Volume 快照仍有效。
- 父一致性群組的快照仍然有效。
- 如果將所有磁碟區移出子一致性群組、則該一致性群組將會刪除。
- 一致性群組的修改必須遵守 一致性群組限制。

系統管理員

從 ONTAP 9.12.1 開始、您可以使用系統管理員來執行此作業。

步驟

1. 選擇*儲存>一致性群組*。
2. 選取包含您要移動之磁碟區的父一致性群組。找到子一致性群組、然後展開「**Volumes**」（磁碟區）功能表。選取您要移動的磁碟區。
3. 選擇 移動 。
4. 選擇是要將磁碟區移至新的一致性群組、還是要移至現有群組。
   a. 若要移至現有的一致性群組、請選取 現有子一致性群組 、然後從下拉式功能表中選擇一致性群組的名稱。
   b. 若要移至新的一致性群組、請選取 新的子一致性群組 。輸入新子一致性群組的名稱、然後選取元件類型。
5. 選擇 移動 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 在一致性群組之間移動磁碟區。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

將磁碟區移至新的子一致性群組

1. 下列命令會建立新的子一致性群組、其中包含指定的磁碟區。

   建立新的一致性群組時，您可以指定新的快照， QoS 和分層原則。

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -new-consistency-group
   consistency_group_name [-snapshot-policy policy -qos-policy policy -tiering
   -policy policy]
   ```

將磁碟區移至現有的子一致性群組

1. 重新指派磁碟區。。 `-volumes` 參數接受以逗號分隔的磁碟區名稱清單。

   ```
   consistency-group volume reassign -vserver SVM_name -consistency-group
   source_child_consistency_group -parent-consistency-group
   parent_consistency_group -volume volumes -to-consistency-group
   target_consistency_group
   ```

相關資訊

- 一致性群組限制

- 複製一致性群組

修改ONTAP一致性組幾何結構

從 ONTAP 9.13.1 開始、您可以修改一致性群組的幾何。修改一致性群組的幾何可讓您變更子或父一致性群組的組態、而不會中斷進行中的 IO 作業。

修改一致性群組幾何資料會影響一致性群組的現有快照。如需詳細資訊、請參閱您要執行的幾何特定修改。

> 您無法修改以遠端保護原則設定的一致性群組幾何。您必須先中斷保護關係、修改幾何、然後還原遠端保護。

新增子一致性群組

從 ONTAP 9.13.1 開始、您可以將新的子一致性群組新增至現有的父一致性群組。

關於這項工作

- 父一致性群組最多可包含五個子一致性群組。請參閱 一致性群組限制 其他限制。
- 您無法將子一致性群組新增至單一一致性群組。您必須優先 [促銷] 接著您可以新增子一致性群組。
- 在展開作業之前擷取的一致性群組現有快照將視為部分快照。任何以該快照為基礎的還原作業，都會在快照的時間點反映一致性群組。

範例 **32.** 步驟

系統管理員

從 ONTAP 9.13.1 開始、您可以使用系統管理員執行此作業。

新增子一致性群組

1. 選擇*儲存>一致性群組*。
2. 選取您要新增子一致性群組的父一致性群組。
3. 在父一致性群組名稱旁、選取「 更多 」、然後選擇「新增子一致性群組」。
4. 輸入一致性群組的名稱。
5. 選擇您要新增或現有的磁碟區。
   a. 如果您要新增現有的磁碟區、請選取 現有的磁碟區 、然後從下拉式功能表中選擇磁碟區。
   b. 如果您要新增新的磁碟區、請選取 新的磁碟區 、然後指定磁碟區數量及其大小。
6. 選取 新增 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 新增子一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

新增具有新磁碟區的子一致性群組

1. 建立新的一致性群組。提供一致性群組名稱、磁碟區首碼、磁碟區數量、磁碟區大小、儲存服務、 和匯出原則名稱：

   ```
   consistency-group create -vserver SVM_name -consistency-group
   consistency_group -parent-consistency-group parent_consistency_group
   -volume-prefix prefix -volume-count number -size size -storage-service
   service -export-policy policy_name
   ```

新增具有現有磁碟區的子一致性群組

1. 建立新的一致性群組。。 `volumes` 參數接受以逗號分隔的磁碟區名稱清單。

   ```
   consistency-group create -vserver SVM_name -consistency-group
   new_consistency_group -parent-consistency-group parent_consistency_group
   -volumes volume
   ```

分離子一致性群組

從 ONTAP 9.13.1 開始、您可以將子一致性群組從其父群組中移除、將其轉換為個別一致性群組。

關於這項工作

- 分離子一致性群組會導致父一致性群組的快照無效且無法存取。Volume 精細快照仍有效。
- 個別一致性群組的現有快照仍然有效。
- 如果現有的單一一致性群組名稱與您要分離的子一致性群組名稱相同、則此作業將會失敗。如果您遇到此案例、則在中斷連線時必須重新命名一致性群組。

範例 **33.** 步驟

系統管理員

從 ONTAP 9.13.1 開始、您可以使用系統管理員執行此作業。

分離子一致性群組

1. 選擇*儲存>一致性群組*。
2. 選取包含要分離之子系的父一致性群組。
3. 在要分離的子一致性組旁邊，選擇 更多 ，然後選擇 分離父級 。
4. 您也可以重新命名一致性群組、然後選取應用程式類型。
5. 選擇 分離 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 分離子一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

分離子一致性群組

1. 分離一致性群組。您也可以使用重新命名分離的一致性群組 `-new-name` 參數。

```
consistency-group detach -vserver SVM_name -consistency-group
child_consistency_group -parent-consistency-group parent_consistency_group
[-new-name new_name]
```

將現有的單一一致性群組移至父一致性群組下

從 ONTAP 9.13.1 開始、您可以將現有的單一一致性群組轉換成子一致性群組。您可以將一致性群組移至現有父一致性群組之下、或在移動作業期間建立新的父一致性群組。

關於這項工作

- 父一致性群組必須有四個或更少的子項目。父一致性群組最多可包含五個子一致性群組。請參閱 一致性群組限制 其他限制。
- 在此作業之前擷取的 _父 / 母一致性群組現有快照視為部分快照。任何以其中一個快照為基礎的還原作業，都會反映快照時間點的一致性群組。
- 單一一致性群組的現有一致性群組快照仍然有效。

範例 **34.** 步驟

系統管理員

從 ONTAP 9.13.1 開始、您可以使用系統管理員執行此作業。

將現有的單一一致性群組移至父一致性群組下

1. 選擇*儲存>一致性群組*。
2. 選取您要轉換的一致性群組。
3. 選擇「 更多 」、然後選擇「在不同一致性群組下移動」 ** 。
4. 您也可以輸入一致性群組的新名稱、然後選取元件類型。根據預設、元件類型為其他。
5. 選擇是否要移轉至現有的父一致性群組、或建立新的父一致性群組：
   a. 若要移轉至現有的父一致性群組、請選取 現有一致性群組 、然後從下拉式功能表中選擇一致性群組。
   b. 若要建立新的父一致性群組、請選取 新一致性群組 、然後提供新一致性群組的名稱。
6. 選擇 移動 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 將單一一致性群組移至父一致性群組下。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

將一致性群組移至新的父一致性群組下

1. 建立新的父一致性群組。。 `-consistency-groups` 參數會將任何現有的一致性群組移轉至新父群組。

```
consistency-group attach -vserver svm_name -consistency-group
parent_consistency_group -consistency-groups child_consistency_group
```

將一致性群組移至現有一致性群組下

1. 移動一致性群組：

```
consistency-group add -vserver SVM_name -consistency-group
consistency_group -parent-consistency-group parent_consistency_group
```

推廣子項一致性群組

從 ONTAP 9.13.1 開始、您可以將單一一致性群組升級為父一致性群組。當您將單一一致性群組提升為父群組時、也會建立新的子一致性群組、繼承原始單一一致性群組中的所有磁碟區。

關於這項工作

- 如果您想要將子一致性群組轉換成父一致性群組、則必須先將其轉換成父一致性群組 [detach] 然後，子一致

性群組會遵循此程序。

- 在您提升一致性群組之後，一致性群組的現有快照仍有效。

系統管理員

從 ONTAP 9.13.1 開始、您可以使用系統管理員執行此作業。

推廣子項一致性群組

1. 選擇*儲存>一致性群組*。
2. 選取您要升級的一致性群組。
3. 選擇「 更多 」、然後選擇「升級至父一致性群組」。
4. 輸入一個 名稱 ，然後爲子一致性組選擇一個 組件類型 。
5. 選擇 升級 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 將單一一致性群組移至父一致性群組下。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

推廣子項一致性群組

1. 推廣一致性群組。此命令會建立一個父一致性群組和一個子一致性群組。

```
consistency-group promote -vserver SVM_name -consistency-group
existing_consistency_group -new-name new_child_consistency_group
```

將父實體降級為單一一致性群組

從 ONTAP 9.13.1 開始、您可以將父一致性群組降級為單一一致性群組。降級父級會展平一致性群組的階層、移除所有相關的子一致性群組。一致性群組中的所有磁碟區將保留在新的單一一致性群組之下。

關於這項工作

- 將 父子 一致性群組的現有快照降級為單一一致性後，這些快照仍然有效。該父實體的任何相關 _*Chive* 一致性群組的現有快照，在降級時即失效。子一致性群組中的個別磁碟區快照仍可作為磁碟區精細快照存取。

範例 **35.** 步驟

系統管理員

從 ONTAP 9.13.1 開始、您可以使用系統管理員執行此作業。

降級一致性群組

1. 選擇*儲存>一致性群組*。
2. 選取您要降級的父一致性群組。
3. 選擇「 更多 」、然後選擇「降級為單一一致性群組」 ** 。
4. 系統將會發出警告訊息、告知您所有相關的子一致性群組都將被刪除、而其磁碟區將移至新的單一一致性群組之下。選擇 降級 以確認您瞭解其影響。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 降級一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

降級一致性群組

1. 降級一致性群組。使用選用功能 `-new-name` 重新命名一致性群組的參數。

   ```
   consistency-group demote -vserver SVM_name -consistency-group
   parent_consistency_group [-new-name new_consistency_group_name]
   ```

修改**ONTAP**一致性群組應用程式和元件標籤

從 ONTAP 9.12.1 開始、一致性群組支援元件和應用程式標記。應用程式與元件標籤是一種管理工具、可讓您篩選及識別一致性群組中的不同工作負載。

關於這項工作

一致性群組提供兩種類型的標籤：

- *應用程式標籤：這些標籤適用於個別與父一致性群組。應用程式標籤提供工作負載標記、例如MongoDB、Oracle或SQL Server。一致性群組的預設應用程式標記為「其他」。
- *元件標籤：階層式一致性群組中的子項目具有元件標籤、而非應用程式標籤。元件標籤的選項包括「data」（資料）、「logs」（記錄）或「other」（其他）。預設值為「其他」。

您可以在建立一致性群組或建立一致性群組之後套用標記。

如果一致性組具有 SnapMirror 活動同步關係，則必須使用 * 其他 * 作爲應用程序或組件標記。

步驟

從 ONTAP 9.12.1 開始、您可以使用系統管理員修改應用程式和元件標籤。從 ONTAP 9.14.1 開始、您可以使用

ONTAP CLI 修改應用程式和元件標籤。

系統管理員

1. 選擇*儲存>一致性群組*。
2. 選取您要修改其標記的一致性群組。選擇 ⋮ 一致性群組名稱旁邊的 * 編輯 * 。
3. 在下拉式功能表中、選擇適當的應用程式或元件標籤。
4. 選擇*保存*。

CLI

從 ONTAP 9.14.1 開始、您可以使用 ONTAP CLI 修改現有一致性群組的應用程式或元件標籤。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

修改應用程式標籤

1. 應用程式標籤接受數量有限的預設字串。若要查看已接受的字串清單、請執行下列命令：
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type ?`
2. 從輸出中選擇適當的字串、然後修改一致性群組：
   `consistency-group modify -vserver` *`svm_name`* `-consistency-group` *`consistency_group`* `-application-type application_type`

修改元件標籤

1. 修改元件類型。元件類型可以是資料、記錄或其他。如果您使用的是 SnapMirror 主動式同步、則必須是「其他」。
   `consistency-group modify -vserver` *`svm`* `-consistency-group` *`child_consistency_group`* `-parent-consistency-group` *`parent_consistency_group`* `-application-component-type [data|logs|other]`

克隆**ONTAP**一致性組

從 ONTAP 9.12.1 開始、您可以複製一致性群組、以建立一致性群組及其內容的複本。複製一致性群組會建立一致性群組組態的複本、其中繼資料（例如應用程式類型）、以及所有磁碟區及其內容（例如檔案、目錄、LUN或NVMe命名空間）。

關於這項工作

複製一致性群組時，您可以使用其目前組態來複製，但可以使用現有的一致性群組快照來複製磁碟區內容。

只有整個一致性群組才支援複製一致性群組。您無法在階層關係中複製個別子一致性群組：只能複製完整的一致性群組組態。

當您複製一致性群組時、不會複製下列元件：

- igroup
- LUN對應
- NVMe子系統
- NVMe命名空間子系統對應

開始之前

- 當您複製一致性群組時、ONTAP 如果未指定共用名稱、則不會為複製的磁碟區建立SMB共用區。* 如果未指定連接路徑、則不會掛載複製的一致性群組。
- 如果您嘗試根據不反映一致性群組目前組成磁碟區的快照來複製一致性群組，作業將會失敗。
- 複製一致性群組之後、您需要執行適當的對應作業。

  請參閱 將igroup對應至多個LUN 或 將NVMe命名空間對應至子系統 以取得更多資訊。

- SnapMirror 主動式同步關係中的一致性群組或任何相關的 DP 磁碟區不支援複製一致性群組。

系統管理員

步驟

1. 選擇*儲存>一致性群組*。
2. 從「一致性群組」功能表中選取您要複製的一致性群組。
3. 在一致性群組的總覽頁面右上角、選取* Clone（複製）*。
4. 輸入新的複製一致性群組名稱、或接受預設名稱。
   a. 如果您要啟用、請選擇 "精簡配置"。
   b. 如果您要將一致性群組與其來源分離、並為複製的一致性群組分配額外的磁碟空間、請選擇*分割Clone（分割複製）*。
5. 若要複製目前狀態下的一致性群組，請選擇「新增快照」。

   若要根據快照複製一致性群組，請選擇 * 使用現有的 SnapShot * 。選取此選項將會開啟新的子功能表。選擇您要作為複製作業基礎的快照。

6. 選擇* Clone（克隆）*。
7. 返回「一致性群組」功能表、確認您的一致性群組已複製完成。

CLI

從 ONTAP 9.14.1 開始、您可以使用具有叢集管理認證的 CLI 來複製一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

複製一致性群組

1. 命令會 `consistency-group clone create`以目前的時間點狀態複製一致性群組。若要以快照作為複製作業的基礎，請加入 `-source-snapshot`參數。

   ```
   consistency-group clone create -vserver svm_name -consistency-group
   clone_name -source-consistency-group consistency_group_name [-source-
   snapshot snapshot_name]
   ```

   如"指令參考資料ONTAP"需詳細 `consistency-group clone create`資訊，請參閱。

後續步驟

- 將igroup對應至多個LUN
- 將NVMe命名空間對應至子系統

刪除**ONTAP**一致性組

如果您決定不再需要一致性群組、可以將其刪除。

關於這項工作

- 刪除一致性群組會刪除一致性群組的執行個體、而且不會影響組成的磁碟區或 LUN 。刪除一致性群組並不會導致刪除每個磁碟區上的快照，但這些快照將無法作為一致性群組快照來存取。不過，快照仍可作為一般的 Volume 精細快照來管理。
- 如果刪除一致性群組中的所有磁碟區、 ONTAP 會自動刪除一致性群組。
- 刪除父一致性群組會刪除所有相關的子一致性群組。
- 如果您使用ONTAP 的版本介於9.10.1至9.12.0之間、則只有在刪除磁碟區本身時、才能從一致性群組中移除磁碟區、在此情況下、磁碟區會自動從一致性群組中移除。從 ONTAP 9.12.1 開始、您可以從一致性群組中移除磁碟區、而無需刪除一致性群組。如需此程序的詳細資訊、請參閱 修改一致性群組。

範例 **36.** 步驟

系統管理員

1. 選擇*儲存>一致性群組*。
2. 選取您要刪除的一致性群組。
3. 在一致性群組名稱旁、選取 ⋮ * 刪除 * 。

CLI

從 ONTAP 9.14.1 開始、您可以使用 CLI 刪除一致性群組。

開始之前

- 您必須處於管理權限層級、才能執行此工作。
- 從ONTAP 9.15.1 開始，任何具有管理員權限等級的使用者都可以執行此任務。在ONTAP 9.14.1 中，您必須是叢集或 SVM 管理員才能執行此任務。

刪除一致性群組

1. 刪除一致性群組：

```
consistency-group delete -vserver svm_name -consistency-group
consistency_group_name
```

SnapMirror 主動同步

簡介

了解**ONTAP SnapMirror**主動同步

SnapMirror主動同步，也稱為SnapMirror業務連續性 (SM-BC)，可讓業務服務在整個網站發生故障時繼續運作。該技術使應用程式能夠無縫地故障轉移到輔助副本，而無需人工幹預或自訂腳本。

NetApp SnapMirror主動同步 (SM-as) 旨在提供更細微、更低成本、更易於使用的應用程式層級保護，並具有自動故障轉移功能。 SnapMirror主動同步使關鍵任務業務服務即使在整個站點發生故障時也能繼續運作。借助SnapMirror主動同步，您現在可以在不同地理位置的網站之間同步複製應用程式的多個磁碟區（透過將它們新增至一致性群組）。當主副本發生中斷時，您可以自動故障轉移到輔助副本，從而實現第一層應用程式的業務連

續性。

一些國家針對金融機構的規定要求企業定期從其二級資料中心提供服務。 SnapMirror主動同步及其高可用性叢集可實現這些資料中心切換，從而實現業務連續性。

從ONTAP 9.9.1 開始， SnapMirror主動同步在AFF和全快閃 SAN 陣列 (ASA) 叢集上支援。主群集和輔助群集必須是同一種類型： ASA、 ASA r2 或AFF。 SnapMirror主動同步使用 iSCSI 或 FCP LUN 或 NVMe 命名空間保護應用程式。

SnapMirror主動同步支援對稱和非對稱配置。 ONTAP 9.15.1 中引入了對對稱主動/主動的支援。對稱主動/主動配置允許受保護 LUN 的兩個副本透過雙向同步複製執行讀寫 I/O 操作，從而使每個 LUN 副本能夠滿足本地 I/O 請求。

自 2024 年 7 月起、先前以 PDF 格式發佈的技術報告內容已與 ONTAP 產品文件整合。ONTAP SnapMirror 主動式同步文件現在包含來自 _TR-4878 的內容： SnapMirror 主動式同步。

效益

SnapMirror 主動式同步提供下列優點：

- 業務關鍵應用程式的持續可用度。
- 能夠從主要和次要站台交替主控關鍵應用程式。
- 使用一致性群組來簡化應用程式管理、以確保依寫入順序的一致性。
- 測試每個應用程式的容錯移轉功能。
- 即時建立鏡射複本、不會影響應用程式可用度。
- 能夠在同一個 ONTAP 叢集中部署受保護和不受保護的工作負載。
- LUN、NVMe 命名空間、NVMe 子系統或儲存單元身分保持不變，因此應用程式將它們視為共用虛擬裝置。
- 能夠靈活地重複使用次叢集、為開發測試、 UAT 或報告用途建立即時複本、而不影響應用程式效能或可用度。

SnapMirror主動同步功能可保護您的資料 LUN 或 NVMe 命名空間，使應用程式能夠透明地進行故障轉移，從而在災難發生時保持業務連續性。有關更多信息，請參閱"使用案例" 。

主要概念

SnapMirror主動同步使用一致性群組來確保您的資料被複製。 SnapMirror主動同步使用ONTAP Mediator，或從ONTAP 9.17.1 開始使用 Cloud Mediator 進行自動故障轉移，確保在災難發生時能夠提供資料。在規劃SnapMirror主動同步部署時，請務必了解SnapMirror主動同步及其架構中的基本概念。

不對稱性和對稱性

在對稱主動/主動配置中，兩個站點均可存取本地儲存以進行主動 I/O。對稱主動/主動配置針對叢集應用程式進行了最佳化，包括 VMware vMSC、Windows 故障轉移叢集（含 SQL）以及 Oracle RAC。

在非對稱主動/主動配置中，輔助站點上的資料被代理到 LUN、命名空間或儲存單元。

如需詳細資訊、請參閱 SnapMirror 主動同步架構。

一致性群組

對於AFF和ASA系統"一致性群組"是FlexVol磁碟區的集合，為必須保護以確保業務連續性的應用程式工作負載提供一致性保證。在ASA r2 系統中，一致性群組是儲存單元的集合。

一致性組的目的是同時對磁碟區或儲存單元集合進行快照，從而確保在某個時間點集合的崩潰一致性副本。一致性組確保資料集的所有磁碟區都處於靜止狀態，然後在同一時間點進行快照。這為支援資料集的磁碟區或儲存單元提供了資料一致的還原點。因此，一致性組可以維護相關的寫入順序一致性。如果您決定保護應用程式以實現業務連續性，則必須將與此應用程式對應的磁碟區或儲存單元群組新增至一致性群組中，以便在來源一致性群組和目標一致性群組之間建立資料保護關係。來源一致性群組和目標一致性群組必須包含相同數量和類型的磁碟區。

組成

單一磁碟區、LUN 或 NVMe 命名空間（從ONTAP 9.17.1 開始），是SnapMirror活動同步關係中受保護的一致性群組的一部分。

資訊媒體**ONTAP**

這"資訊媒體ONTAP"接收有關對等ONTAP叢集和節點的運行狀況信息，在兩者之間進行協調，並確定每個節點/叢集是否運行正常且正在運行。 ONTAP調解ONTAP提供以下方面的運作狀況資訊：

- 對等 ONTAP 叢集
- 對等 ONTAP 叢集節點
- 一致性群組（定義 SnapMirror 主動式同步關係中的容錯移轉單元）；針對每個一致性群組、會提供下列資訊：
  - 複寫狀態：未初始化、同步或不同步
  - 主複本所在的叢集
  - 作業內容（用於規劃的容錯移轉）

透過此 ONTAP Mediator 健全狀況資訊、叢集可以區分不同類型的故障、並判斷是否要執行自動容錯移轉。ONTAP 調解器是 SnapMirror 主動同步仲裁中的三方之一，同時具有兩個 ONTAP 叢集（主要和次要）。要達成共識、法定人數中至少有兩方必須同意某項作業。

> 從 ONTAP 9.15.1 開始，系統管理員會顯示任一叢集的 SnapMirror 作用中同步關係狀態。您也可以從系統管理員的任一叢集監控 ONTAP Mediator 的狀態。在早期版本的 ONTAP 中、系統管理員會顯示來源叢集的 SnapMirror 主動式同步關係狀態。

ONTAP雲端調解器

ONTAP Cloud Mediator 從ONTAP 9.17.1 開始可用。 ONTAPONTAP Cloud Mediator 提供與ONTAP Mediator 相同的服務，但它使用NetApp控制台託管在雲端。

規劃的容錯移轉

一種手動操作、可變更 SnapMirror 主動式同步關係中的複本角色。主要站台會變成次要站台、次要站台則成為主要站台。

自動非計畫性容錯移轉（**AUFO**）

一種自動操作、可執行容錯移轉至鏡射複本。此作業需要 ONTAP Mediator 協助、以偵測主要複本是否無法使用。

一級和一級偏差

SnapMirror 主動式同步採用一項主要原則、優先選用主要複本、以便在網路分割區中提供 I/O 服務。

primer-bias 是一種特殊的仲裁實作、可改善 SnapMirror 主動式同步保護資料集的可用度。如果主複本可用、當 ONTAP Mediator 無法從兩個叢集連線時、主偏置即會生效。

從 ONTAP 9.15.1 開始、 SnapMirror 主動同步支援主要優先與主要偏置。主要複本會在 System Manager 中指定、並以 REST API 和 CLI 輸出。

不同步（**OOS**）

當應用程式 I/O 未複寫到次要儲存系統時、會報告為 不同步 。不同步狀態表示次要磁碟區不會與主要（來源）同步、也不會發生 SnapMirror 複寫。

如果鏡像狀態是 `Snapmirrored`，這表明SnapMirror關係已建立且資料傳輸已完成，這意味著目標磁碟區與來源磁碟區保持同步。

SnapMirror 主動式同步支援自動重新同步、讓複本恢復至不同步狀態。

從 ONTAP 9.15.1 開始、 SnapMirror 主動式同步支援 "自動重新設定排風扇組態"。

統一且不一致的組態

- 統一主機存取 表示兩個站台的主機都會連線到兩個站台上儲存叢集的所有路徑。跨站台路徑會跨越距離延伸。
- 非統一主機存取 表示每個站台中的主機僅連線至同一個站台中的叢集。不連接跨站台路徑和延伸路徑。

任何 SnapMirror 主動式同步部署都支援統一的主機存取；非統一的主機存取僅支援對稱式主動 / 主動式部署。

零RPO

RPO 是指恢復點目標、這是指在指定期間內可接受的資料遺失量。零 RPO 表示無法接受資料遺失。

零RTO

RTO 是指恢復時間目標、這是應用程式在中斷、故障或其他資料遺失事件後、在不中斷營運的情況下、恢復正常作業所能接受的時間量。零 RTO 表示無法接受停機時間量。

ONTAP版本支援的SnapMirror主動同步配置

對SnapMirror主動同步的支援因ONTAP版本的不同而有所差異：

版本ONTAP	支援的集群	支援的傳輸協定	支援的組態

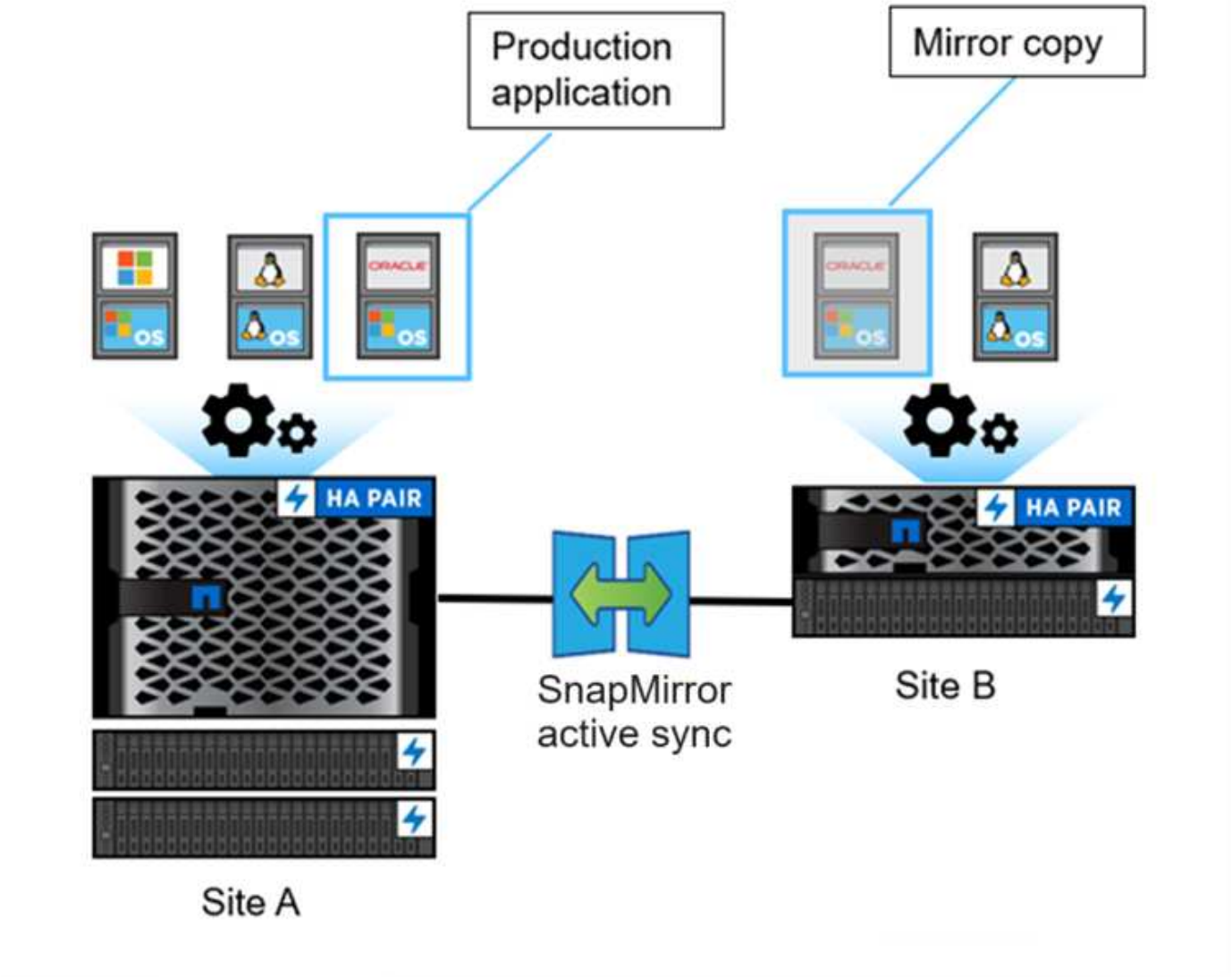
9.17.1 及更高版本	• AFF • ASA • C 系列 • ASA r2	• iSCSI • FC • 適用於 VMware 工作負載的 NVMe	• 非對稱主動/主動 非對稱主動/主動不支援ASA r2和 NVMe。有關 NVMe 支援的更多信息，請參閱"NVMe 組態、支援和限制" 。 • 對稱式主動 / 主動式
9.16.1 及更新版本	• AFF • ASA • C 系列 • ASA r2	• iSCSI • FC	• 非對稱主動/主動 • 對稱主動/主動 對稱主動/主動配置支援ONTAP 9.16.1 及更高版本中的 4 節點叢集。對於ASA r2，僅支援 2 節點叢集。
9.15.1 及更高版本	• AFF • ASA • C 系列	• iSCSI • FC	• 非對稱主動/主動 • 對稱主動/主動 對稱主動/主動配置支援ONTAP 9.15.1 中的 2 節點叢集。ONTAPONTAP及更高版本支援 4 節點叢集。
9.9.1及更新版本	• AFF • ASA • C 系列	• iSCSI • FC	非對稱主動/主動

主集群和輔助集群必須是同一種類型： "ASA" ， "ASA r2"或AFF。

ONTAP SnapMirror主動同步架構

SnapMirror主動同步架構支援兩個叢集上的主動工作負載，其中主要工作負載可同時由兩個叢集提供服務。一些國家針對金融機構的規定要求企業也定期從其二級資料中心提供服務，這被稱為「Tick-Tock」部署，而SnapMirror主動同步功能可以實現這一目標。

透過將儲存虛擬機器 (SVM) 中不同磁碟區的特定於應用程式的 LUN 或 NVMe 命名空間新增至一致性群組，在來源儲存系統和目標儲存系統之間建立用於保障業務連續性的資料保護關係。在正常運作情況下，企業應用程式會寫入主一致性群組，主一致性群組會將此 I/O 同步複製到鏡像一致性群組。



即使資料保護關係中存在兩個獨立的資料副本，由於SnapMirror主動同步維護相同的 LUN 或 NVMe 命名空間標識，應用程式主機會將其視為具有多條路徑的共用虛擬設備，同時一次僅寫入一個 LUN 或 NVMe 命名空間副本。當故障導致主儲存系統離線時， ONTAP會偵測到此故障並使用調解器進行重新確認；如果ONTAP和調解器都無法 ping 通主站點，ONTAP將執行自動故障轉移操作。此過程導致僅對特定應用程式進行故障轉移，而無需先前為實現故障轉移所需的手動幹預或腳本。

其他要考量的重點：

- 支援不受保護的無鏡射磁碟區、以確保業務持續運作。
- 對於受保護的磁碟區來說、僅支援其他一種 SnapMirror 非同步關係、以確保營運不中斷。
- 串聯拓撲不支援保護業務持續運作。

調解員的作用

SnapMirror主動同步使用調解器作為SnapMirror主動同步副本的被動見證。如果發生網路分區或某個副本不可用， SnapMirror主動同步將使用調解器來確定哪個副本繼續提供 I/O 服務，同時停止另一個副本上的 I/O。除了本機ONTAP調解器之外，從ONTAP 9.17.1 開始，您還可以安裝ONTAP Cloud Mediator 以在雲端部署中提供相同的功能。您可以使用ONTAP調解器或ONTAP Cloud Mediator，但不能同時使用兩者。

調解器在SnapMirror主動同步配置中扮演著至關重要的角色，它充當被動仲裁見證，確保仲裁的維護，並在故障期間方便資料存取。它充當控制器的 ping 代理，以確定對等控制器的活躍性。雖然調解器不會主動觸發切換操作，但它提供了一項至關重要的功能，允許倖存節點在網路通訊出現問題時檢查其配對節點的狀態。作為仲裁見證， ONTAP調解器提供了一條通往對等叢集的備用路徑（實際上充當了代理）。

此外，它允許集群在仲裁過程中獲取此資訊。它使用節點管理 LIF 和叢集管理 LIF 進行通訊。它透過多條路徑建立冗餘連接，以區分站台故障和交換機間連結 (ISL) 故障。當叢集因事件而與調解器軟體及其所有節點失去連線時，將被視為不可存取。這將觸發警報並啟用自動故障轉移到輔助站點中的鏡像一致性群組，確保客戶端的 I/O 不間斷。複製資料路徑依賴偵測訊號機制，如果網路故障或事件持續超過一定時間，可能導致偵測訊號故障，從而導致關係不同步。但是，冗餘路徑（例如 LIF 故障轉移到另一個連接埠）可以維持偵測訊號並防止此類中斷。

資訊媒體**ONTAP**

ONTAP調解器安裝在第三個故障域中，與它監控的兩個ONTAP叢集不同。此設定包含三個關鍵組件：

- 主 ONTAP 叢集裝載 SnapMirror 主動式同步主要一致性群組
- 主控鏡射一致性群組的次要 ONTAP 叢集
- 資訊媒體ONTAP

ONTAP調解器用於以下目的：

- 建立仲裁
- 透過自動容錯移轉（ AUFO ）提供持續可用度
- 計畫性容錯移轉（ PFO ）

ONTAP Mediator 1.7 可以管理十對集群，以實現業務連續性。

當ONTAP調解器不可用時，您無法執行計劃或自動故障轉移。應用程式資料繼續同步複製，不會中斷，實現零資料遺失。

ONTAP雲端調解器

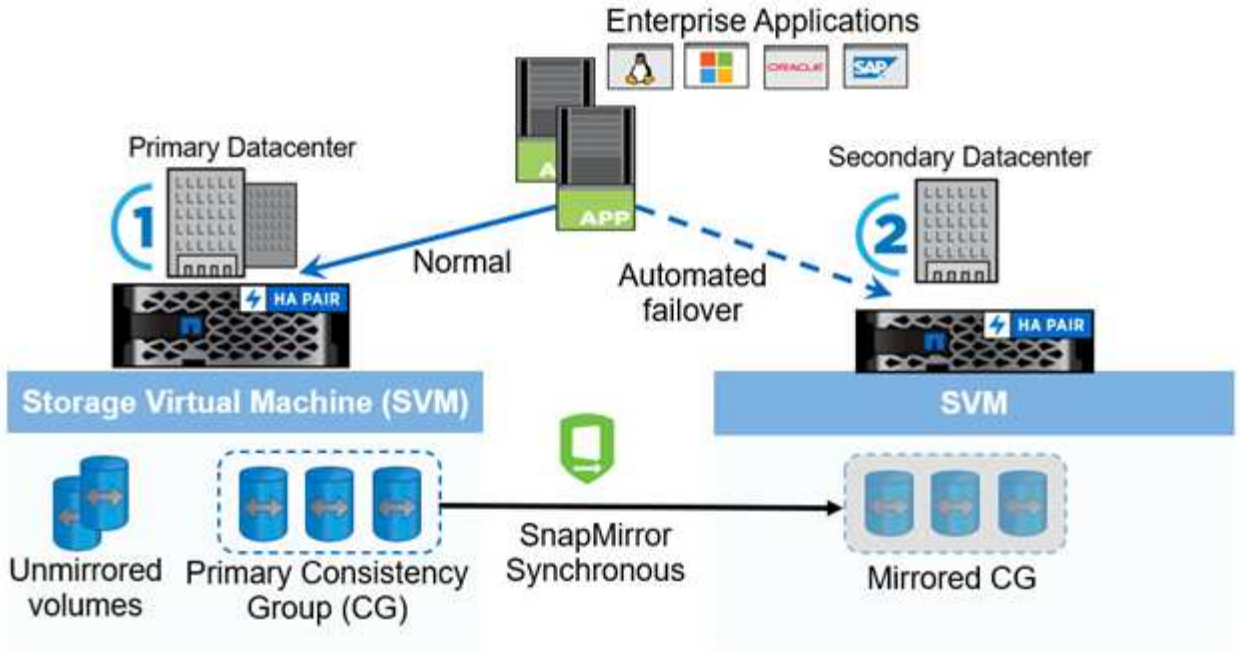
從ONTAP 9.17.1 開始， ONTAP Cloud Mediator 可作為NetApp控制台中的基於雲端的服務使用，以與SnapMirror主動同步一起使用。與ONTAP Mediator 類似， ONTAP Cloud Mediator 在SnapMirror主動同步關係中提供以下功能：

- 為 HA 或SnapMirror活動同步元資料提供持久且受保護的儲存。
- 做為 ping Proxy 、以實現控制器的活力。
- 提供同步節點健全狀況查詢功能、以協助仲裁判斷。

ONTAP Cloud Mediator 透過使用NetApp Console 雲端服務作為您無需管理的第三個站點，協助簡化SnapMirror主動同步部署。Cloud Mediator 服務提供與本地ONTAP Mediator 相同的功能；然而， ONTAP Cloud Mediator 降低了維護第三個站點的操作複雜性。相較之下， ONTAP Mediator 以軟體包形式提供，必須安裝在第三個站點運行的 Linux 主機上，該主機具有獨立的電源和網路基礎架構才能運作。

SnapMirror主動同步操作工作流程

下圖說明了 SnapMirror 主動同步的高層設計。



此圖顯示主資料中心儲存 VM （ SVM ）上裝載的企業應用程式。SVM 包含五個磁碟區、其中三個是一致性群組的一部分。一致性群組中的三個磁碟區會鏡射到次要資料中心。在一般情況下、所有寫入作業都會執行至主要資料中心；實際上、此資料中心是 I/O 作業的來源、而次要資料中心則是目的地。

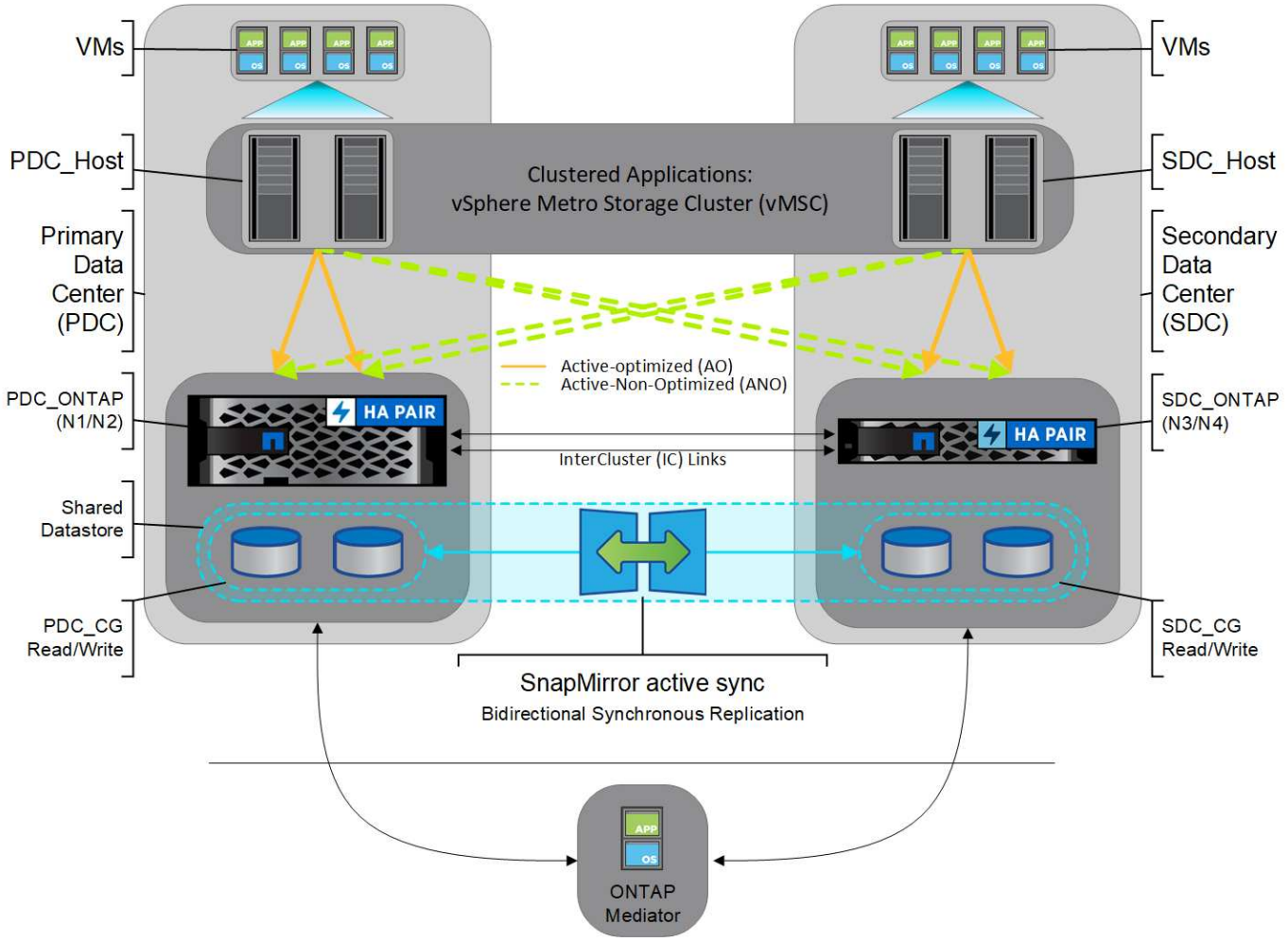
如果主資料中心發生災難， ONTAP會指示輔助資料中心充當主資料中心，為所有 I/O 作業提供服務。僅對一致性群組中鏡像的磁碟區提供服務。與 SVM 上其他兩個磁碟區相關的任何操作都會受到災難事件的影響。

對稱式主動 / 主動式

SnapMirror 主動式同步提供非對稱式解決方案。

在非對稱配置中，主儲存副本公開主動最佳化路徑並主動為客戶端 I/O 提供服務。輔助站點使用遠端路徑進行 I/O。輔助站點的儲存路徑被視為主動非最佳化路徑。寫入 LUN 的存取由輔助站台代理。非對稱配置不支援 NVMe 協定。

在「對稱主動/主動」配置中，主動最佳化路徑在兩個站點上均公開，特定於主機且可配置，這意味著任一側的主機都可以存取本地儲存進行主動 I/O。從ONTAP 9.16.1 開始，最多四個節點的叢集支援對稱主動/主動配置。從ONTAP 9.17.1 開始，對稱主動/主動配置在雙節點叢集上支援 NVMe 協定。



對稱式主動 / 主動式是專為叢集式應用程式所設計、包括 VMware Metro Storage Cluster 、 Oracle RAC 、以及 Windows Failover Clustering with SQL 。

ONTAP SnapMirror主動同步的用例

全球互聯的商業環境要求在發生網路攻擊、停電或自然災害等中斷時，快速恢復關鍵業務應用程式數據，並且不丟失任何數據。在金融領域以及遵守《一般資料保護規範》（GDPR）等監管要求的領域，這些要求更加突出。

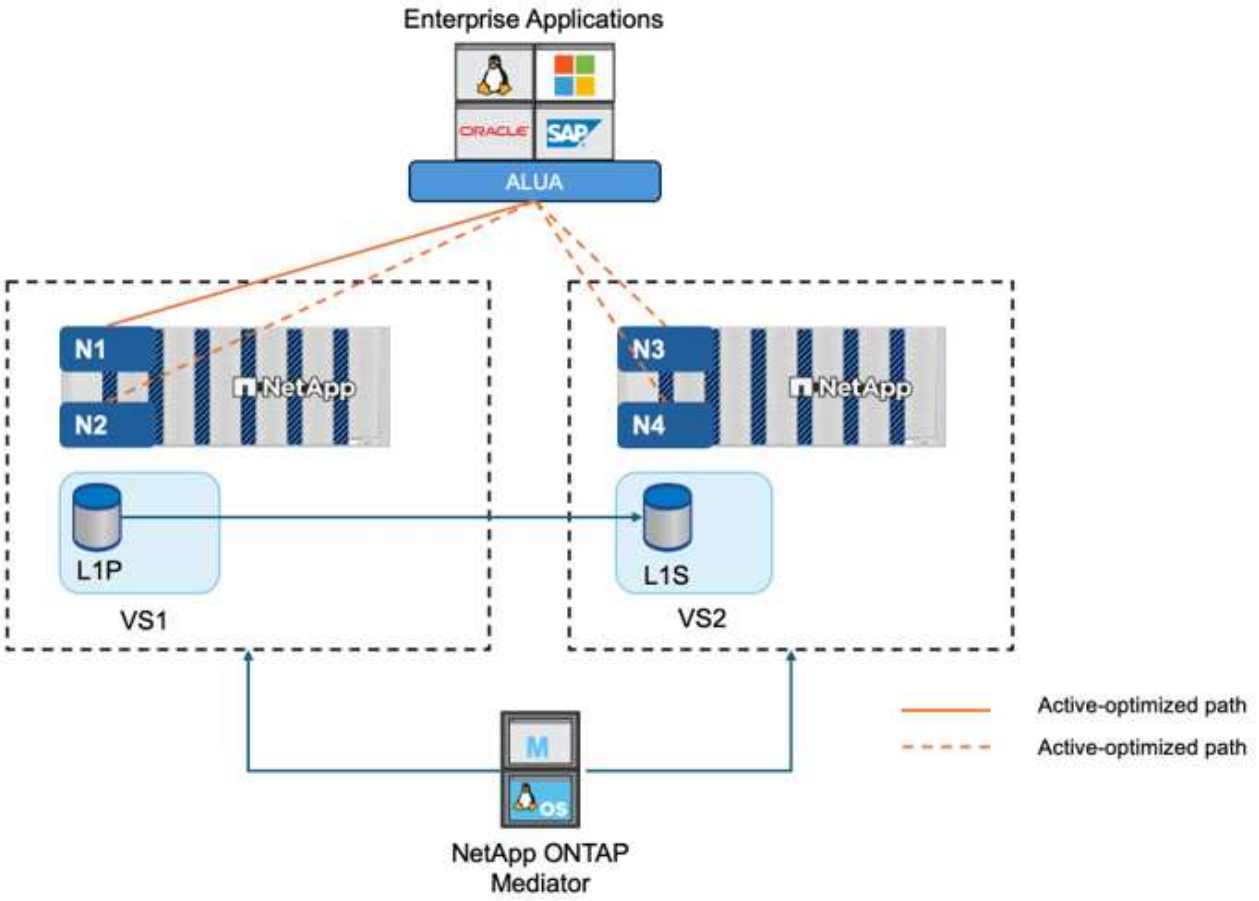
SnapMirror 主動同步提供下列使用案例：

零恢復時間目標（ **RTO** ）的應用程式部署

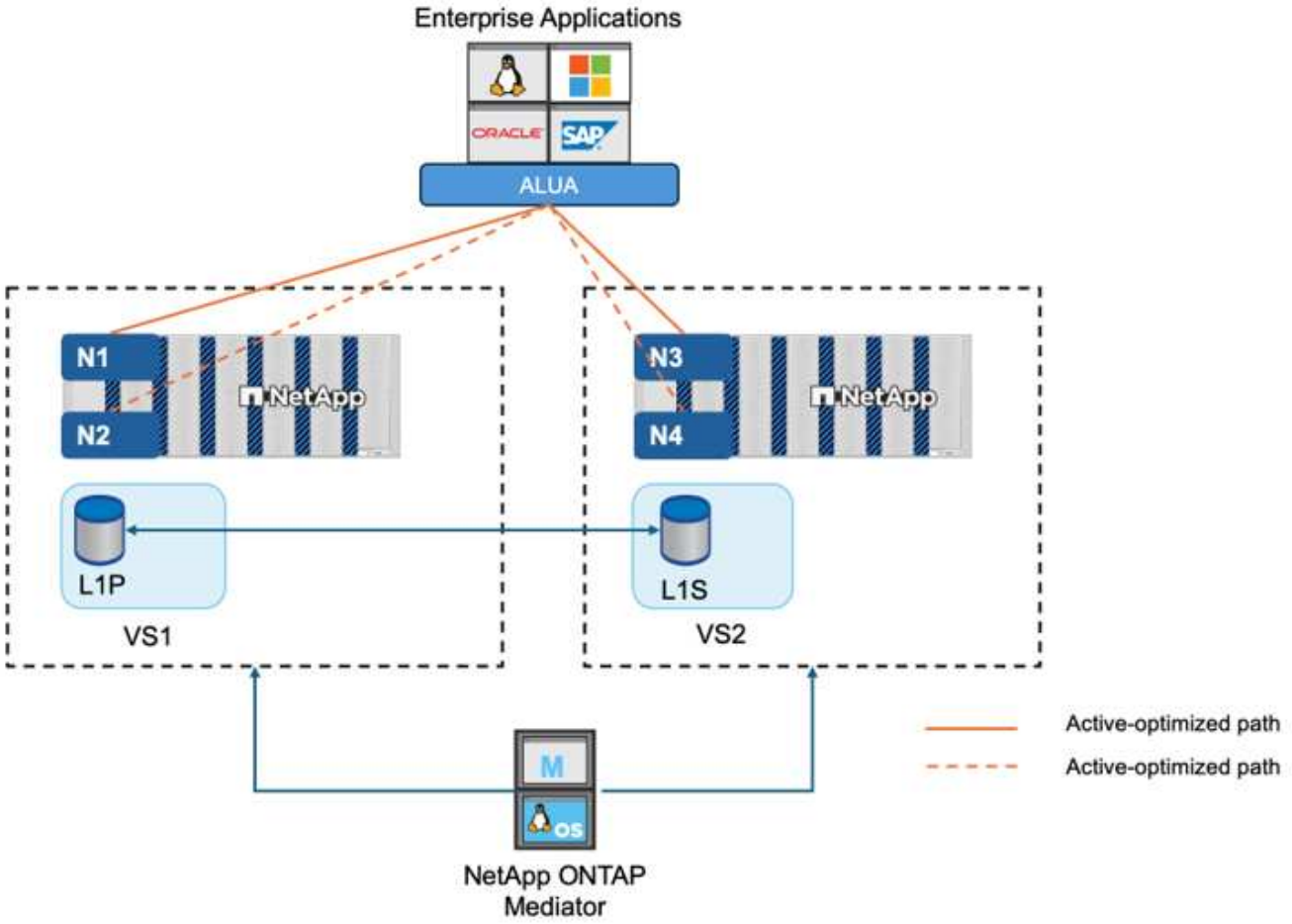
在SnapMirror主動同步部署中，您有一個主叢集和一個輔助叢集。主集群中的 LUN `L1P`) 有一面鏡子 `L1S`)；兩個 LUN 共享相同的序號，並向主機報告為讀寫 LUN。然而，在非對稱配置中，讀寫操作僅對主 LUN 進行。`L1P` .任何寫入鏡像 `L1S`由代理商提供服務。

應用程式部署，實現零 **RTO** 或透明應用程式容錯移轉（ **TAF** ）

TAF 基於主機 MPIO 軟體的路徑故障轉移，以實現對儲存的無中斷存取。兩個 LUN 副本（例如，主磁碟區 (L1P) 和鏡像副本 (L1S)）具有相同的標識（序號），並向主機報告為可讀寫。然而，在非對稱配置中，讀寫操作僅由主磁碟區提供。傳送到鏡像副本的 I/O 會被代理到主副本。根據非對稱邏輯單元存取 (ALUA) 的存取狀態「主動最佳化」(A/O)，主機到 L1 的首選路徑是 VS1:N1。 ONTAPONTAP是部署的一部分，主要用於在主磁碟區發生儲存中斷時執行故障轉移（計劃內或計劃外）。



TAF 有兩種運作模式：自動故障轉移和自動故障轉移雙工。在自動故障轉移模式下，讀寫作業僅由主磁碟區處理，因此傳送至鏡像副本（鏡像副本無法自行處理寫入作業）的 IO 會被代理到主副本。在自動故障轉移雙工模式下，主副本和輔助副本均可處理 IO，因此無需代理。



如果您使用 NVMe 透過ONTAP 9.17.1 進行主機訪問，則僅支援 AutomatedFailoverDuplex 策略。

SnapMirror Active Sync 使用 ALUA 、這種機制可讓應用程式主機多重路徑軟體、其路徑會通告優先順序、並可讓應用程式主機與儲存陣列進行通訊。ALUA 會將擁有 LUN 的控制器和其他控制器的作用中最佳化路徑標記為非最佳化路徑、只有在主要路徑故障時才會使用。

SnapMirror主動同步與 NVMe 協定使用非對稱命名空間存取 (ANA)，這使得應用程式主機能夠發現受保護的 NVMe 命名空間的最佳化路徑和非最佳化路徑。ONTAP目標會發佈對應的路徑狀態，以使應用程式主機能夠使用受保護 NVMe 命名空間的最佳路徑。

叢集式應用程式

叢集應用程式（包括 VMware Metro Storage Cluster、Oracle RAC 和帶有 SQL 的 Windows 故障轉移叢集）需要同時訪問，以便虛擬機器可以故障轉移到其他網站而不會產生任何效能開銷。SnapMirror主動同步對稱主動/主動透過雙向複製在本地提供 IO 服務，以滿足叢集應用程式的要求。從ONTAP 9.16.1 開始，四節點叢集配置支援對稱主動/主動，擴展了ONTAP 9.15.1 中的雙節點叢集限制。

災難案例

在地理位置分散的站台之間、同步複寫多個磁碟區以供應用程式使用。當主應用程式中斷時、您可以自動容錯移轉至次複本、從而為第一層應用程式提供營運持續性。當主叢集所在的站台發生災難時、主機多重路徑軟體會將叢集的所有路徑標記為關閉、並使用來自次叢集的路徑。結果是 ONTAP Mediator 啟用的無中斷容錯移轉功能、可移轉至鏡像複本。

擴展應用程式支援

SnapMirror主動同步透過易於使用的應用程式級粒度和自動故障轉移提供了靈活性。 SnapMirror主動同步使用

經過驗證的 IP 網路SnapMirror同步複製，透過 LAN 或 WAN 高速複製數據，從而在虛擬和實體環境中為業務關鍵型應用程式（如 Oracle、Microsoft SQL Server 等）實現高數據可用性和快速資料複製。

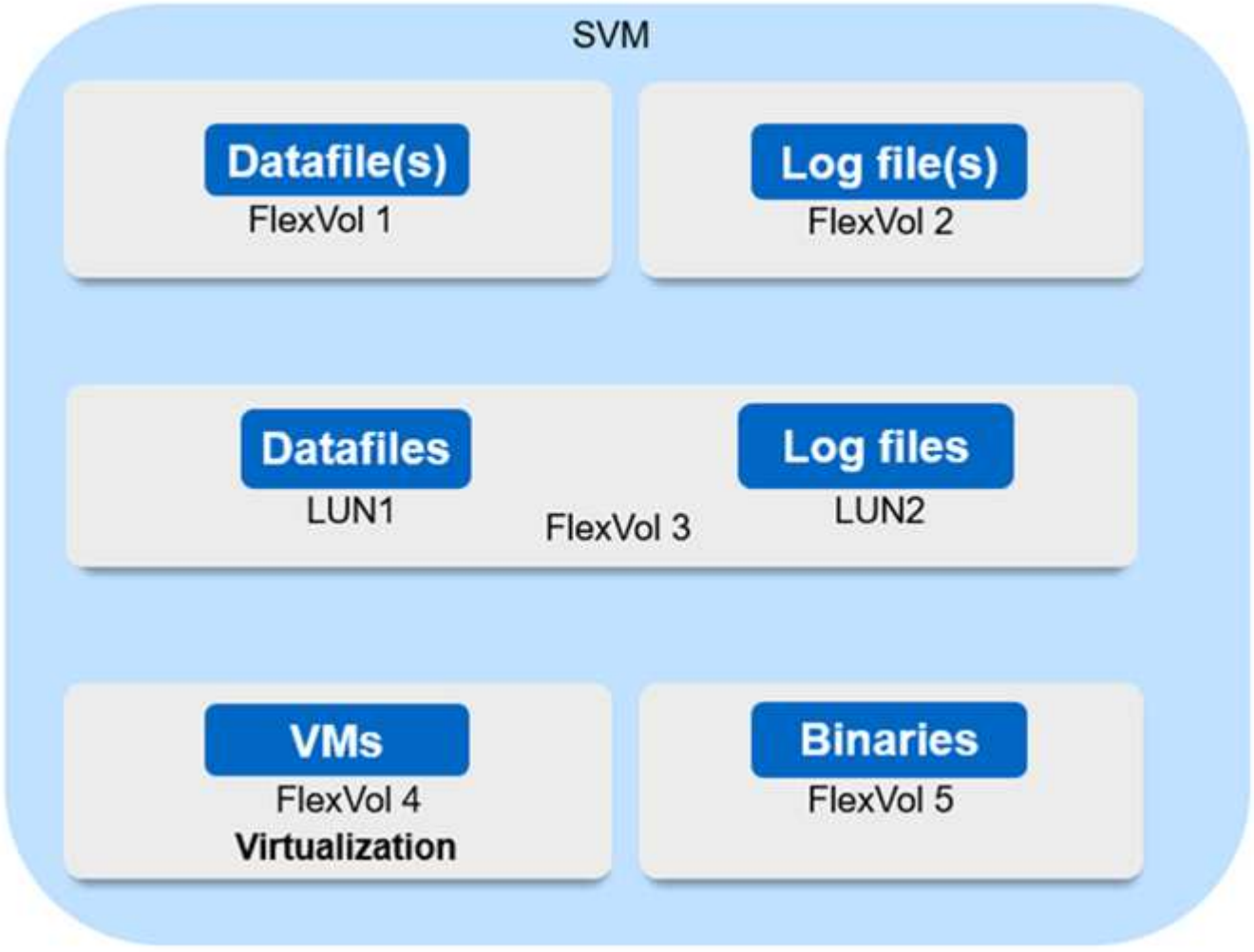
SnapMirror主動同步功能使關鍵任務業務服務即使在整個站點發生故障的情況下也能繼續運行，並將 TAF 保存到輔助副本。無需手動幹預或額外的腳本即可觸發此故障轉移。

ONTAP SnapMirror主動同步的部署策略和最佳實踐

重要的是，您的資料保護策略要明確識別需要保護以確保業務連續性的工作負載。資料保護策略中最關鍵的一步是明確企業應用程式資料佈局，以便您可以決定如何分配資料量並保護業務連續性。由於故障轉移發生在每個應用程式的一致性群組級別，因此請確保將必要的資料磁碟區新增至一致性群組。

SVM 組態

此圖擷取 SnapMirror 主動同步的建議儲存 VM （ SVM ）組態。



- 對於資料磁碟區：
  - 隨機讀取工作負載與循序寫入隔離、因此根據資料庫大小、資料和記錄檔通常會放置在不同的磁碟區上。
    - 對於大型關鍵資料庫、單一資料檔案位於 FlexVol 1 上、其對應的記錄檔位於 FlexVol 2 上。

- 為了獲得更好的整合效果、會將中小型非關鍵資料庫分組、讓所有資料檔案都位於 FlexVol 1 上、而其對應的記錄檔則位於 FlexVol 2 上。不過、您將會因為這項分組而喪失應用程式層級的精細度。

  - 另一個變體是將所有檔案放在同一個 FlexVol 3 中、 LUN 1 中有資料檔案、 LUN 2 中有其記錄檔。

- 如果您的環境已虛擬化、您將會在資料存放區中共享各種企業應用程式的所有 VM 。一般而言、 VM 和應用程式二進位檔會使用 SnapMirror 以非同步方式複寫。

規劃

ONTAP SnapMirror主動同步的先決條件

規劃 SnapMirror 主動式同步部署時、請確保您符合各種硬體、軟體和系統組態需求。

硬體

下表概述支援的 NetApp 叢集組態。

叢集類型	支援的機型	支援的功能	支援的最大叢集節點數
AFF	A 系列， C 系列	自動容錯移轉雙工（對稱式主動 / 主動式），自動容錯移轉（非對稱式主動 / 主動式）	• 2（ONTAP 9.9.1 或更高版本） • 4（採用對稱主動/主動配置的ONTAP 9.16.1 ）
ASA	A 系列， C 系列	自動容錯移轉雙工（對稱式主動 / 主動式），自動容錯移轉（非對稱式主動 / 主動式）	• 2（ONTAP 9.9.1 或更高版本 • 4（採用對稱主動/主動配置的ONTAP 9.16.1 ）
ASA r2	全部	自動故障轉移雙工（對稱主動/主動）	• 2（ONTAP 9.17.1 或更早版本） • 4（ONTAP 9.18.1 或更高版本）

下表概述叢集類型之間的複寫功能。

叢集類型 1	叢集類型 2.	是否支援複寫？
AFF A 系列	AFF C 系列	是的
ASA r2 A系列	ASA R2 C系列	是的
AFF	ASA	否
ASA	ASA r2	否

ASA r2	ASA r2	是的

軟體

- ONTAP 9.9.1 或更新版本
- 不適用1.2版或更新版本的資訊ONTAP
- 執行下列程式之一的 ONTAP Mediator 的 Linux 伺服器或虛擬機器：

ONTAP Mediator 版本	支援的Linux版本
1.11	• Red Hat Enterprise Linux ◦ 相容：9.5 [1] ◦ 推薦：10.1、10.0、9.7、9.6、9.4 和 8.10 • Rocky Linux 10.1、9.7 和 8.10 • Oracle Linux 10.0 和 9.6
1.10	• Red Hat Enterprise Linux ◦ 相容：9.5 [1] ◦ 建議：10.0、9.6、9.4 和 8.10 • Rocky Linux 10.0、9.6 和 8.10
1.9.1	• Red Hat Enterprise Linux ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.5、9.4、9.2、9.0、8.10 和 8.8 • Rocky Linux 9.5 和 8.10
1.9	• Red Hat Enterprise Linux ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.5、9.4、9.2、9.0、8.10 和 8.8 • Rocky Linux 9.5 和 8.10
1.8	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.4、9.3、9.2、9.1、9.0、8.10、8.9 和 8.8 • Rocky Linux 9.4 和 8.10

1.1.7	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.3、9.2、9.1、9.0、8.9 和 8.8 • Rocky Linux 9.3 和 8.9
1.6.	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 建議：9.2、9.1、9.0 和 8.8 • Rocky Linux 9.2 和 8.8
1.5.	• Red Hat Enterprise Linux：8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.4.	• Red Hat Enterprise Linux：8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.3.	• Red Hat Enterprise Linux：8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.2.	• Red Hat Enterprise Linux：8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6

1. 相容意味著 Red Hat 不再支援這些 RHEL 版本，但仍可在這些版本上安裝ONTAP Mediator。

授權

以下SnapMirror許可證是作為ONTAP One 許可證套件的一部分提供，並且必須在兩個叢集上應用：

- SnapMirror 同步
- SnapMirror

> 如果您的ONTAP儲存系統是在 2019 年 6 月之前購買的，請參閱 "ONTAP主許可證密鑰" 取得所需的SnapMirror同步許可證。

- 對於 vSphere Metro Storage Cluster (vMSC)，需要 VMware vSphere 授權。

網路環境

- 叢集間延遲往返時間（ RTT ）必須少於 10 毫秒。
- 從 ONTAP 9.14.1 開始、 "SCSI-3 持續保留" 支援 SnapMirror 主動式同步。

支援的傳輸協定

SnapMirror主動同步支援 SAN 協定。

- 從ONTAP 9.9.1 開始支援 FC 和 iSCSI 協定。
- 從ONTAP 9.17.1 開始，VMware 工作負載支援 NVMe 協定。

  SnapMirror主動同步不支援以下 NVMe 協定：

  - 4 節點對稱主動/主動配置
  - 非對稱主動/主動配置
  - 一致性組大小的變化

    使用 NVMe 傳輸協定搭配 SnapMirror 主動式同步時、您無法以不中斷營運的方式擴充或縮減一致性群組。使用 NVMe 傳輸協定搭配 SnapMirror 主動式同步時、一致性群組擴充和縮減作業會造成中斷。

  - 同一一致性組中的 LUN 和命名空間共存。

IPSpace

SnapMirror主動同步需要使用預設 IP 空間來建立叢集對等關係。不支援自訂 IP 空間。

NTFS安全型態

SnapMirror 主動式同步磁碟區 * 不 * 支援 NTFS 安全樣式。

資訊媒體**ONTAP**

- ONTAP Mediator 必須在外部進行設定並連接到 ONTAP 以實現透明的應用程式故障轉移。
- 為了充分發揮功能並啟用自動計劃外故障轉移，外部 ONTAP 調解器應與 ONTAP 叢集一起設定。
- ONTAP 調解器必須安裝在第三個故障域中，與兩個 ONTAP 叢集分開。
- 安裝 ONTAP Mediator 時，您應該將自簽名憑證替換為由主流可靠 CA 簽署的有效憑證。
- 有關 ONTAP 調解器的更多信息，請參閱"準備安裝 ONTAP 調解器" 。

其他先決條件

- 在ONTAP 9.15.1 之前的版本中，讀寫目標磁碟區（在非對稱主動-主動模式下從 DP 轉換為讀寫的磁碟區）不支援SnapMirror主動同步關係。在使用讀寫磁碟區之前，您必須先建立磁碟區級SnapMirror關係式（非同步或同步），然後刪除該關係，將其轉換為 DP 磁碟區。有關詳細信息，請參閱"將現有的 SnapMirror 關係轉換成 SnapMirror 主動同步" 。
- 使用SnapMirror主動同步的儲存虛擬機器無法以客戶端電腦加入 Active Directory。

更多資訊

- "Hardware Universe"
- "ONTAP Mediator 概述"

ONTAP SnapMirror主動同步互通性

SnapMirror 主動式同步可與 ONTAP 中的許多作業系統、應用程式主機及其他功能相容。

如需此處未涵蓋的特定支援能力和互通性詳細資料、請參閱互通性對照表工具（ Interoperability Matrix Tool ("IMT"）。

應用程式主機

SnapMirror主動同步支援虛擬機器管理程序，包括 Hyper-V、ESXi、Red Hat Enterprise Linux (RHEL)、Windows Server 等作業系統以及 vSphere Metro Storage Cluster (vMSC) 等叢集解決方案，以及從ONTAP 9.14.1 開始的 Windows Server 故障轉移叢集。

作業系統

SnapMirror 主動同步可支援多種作業系統、包括：

- AIX via PVR （從 ONTAP 9.11.1 開始）
- HP-UX （從 ONTAP 9.10.1 開始）
- Solaris 11.4 （從 ONTAP 9.10.1 開始）

AIX

從ONTAP 9.11.1 開始，AIX 透過標準工程功能策略差異請求 (FPVR) 支援SnapMirror主動同步，但需遵守以下規定：

- SnapMirror 主動式同步可提供零 RPO 資料保護、但 AIX 的容錯移轉程序需要額外的步驟才能識別路徑變更。非根 Volume 群組一部分的 LUN 將會暫停 I/O 、直到出現 `cfgmgr` 命令已執行。這可以自動化、而且大多數應用程式都能在不中斷營運的情況下恢復作業。
- 屬於根 Volume 群組的 LUN 通常不應受到 SnapMirror 主動式同步的保護。無法執行 `cfgmgr` 容錯移轉後的命令、表示需要重新開機才能識別 SAN 路徑中的變更。您仍然可以對根磁碟區群組實現零 RPO 資料保護、但容錯移轉將會中斷運作。

請洽詢您的 NetApp 客戶團隊、以取得有關 SnapMirror 與 AIX 進行主動同步的更多資訊。

HP-UX

從 ONTAP 9.10.1 開始，支援適用於 HP-UX 的 SnapMirror Active Sync 。

使用 **HP-UX** 自動進行非計畫性容錯移轉

當主集群和輔助集群之間的連接遺失，且主集群和中介集群之間的連接也丟失時，雙事件故障可能會導致隔離主集群上發生自動計劃外故障轉移 (AUFO) 事件。與其他 AUFO 事件不同，這被認為是一種罕見事件。

- 在這種情況下、在 HP-UX 主機上恢復 I/O 可能需要 120 秒以上的時間。視執行的應用程式而定、這可能不會導致任何I/O中斷或錯誤訊息。
- 若要進行修正、您必須重新啟動 HP-UX 主機上的應用程式、使中斷容錯度低於 120 秒。

Solaris

從 ONTAP 9.10.1 開始、 SnapMirror 主動式同步支援 Solaris 11.4 。

為確保在SnapMirror主動同步環境中發生計劃外站點故障轉移切換時 Solaris 用戶端應用程式不會中斷，請修改預設 Solaris 作業系統設定。若要使用建議的設定配置 Solaris，請參閱"NetApp知識庫：Solaris 主機支援SnapMirror主動同步中的建議設置"。

ONTAP 互通性

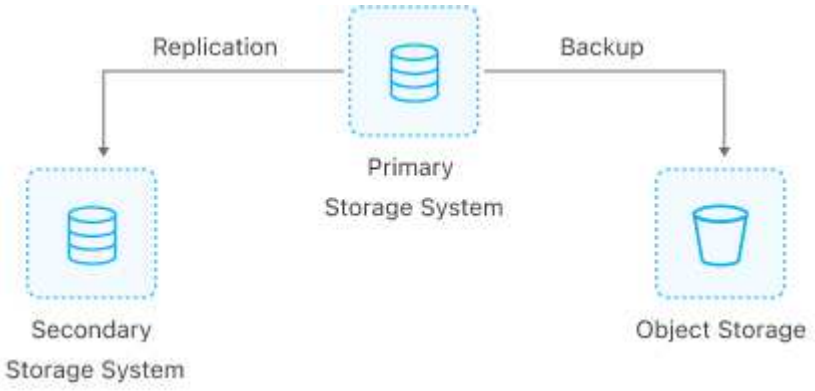
SnapMirror 主動式同步功能與 ONTAP 元件整合、可擴充其資料保護功能。

FabricPool

SnapMirror 主動式同步支援 FabricPool 上的來源和目的地磁碟區、其分層原則為「無」、「快照」或「自動」。SnapMirror 主動同步不支援使用「全部」分層原則的 FabricPool 集合體。

連出組態

在連出組態，您的來源磁碟區可以鏡像到SnapMirror活動同步目標端點和一個SnapMirror非同步關係。



SnapMirror 主動式同步可支援 `MirrorAllSnapshots`原則，並從 `ONTAP 9.11.1` 開始 `MirrorAndVault`支援連出組態原則。`SnapMirror` 作用中同步處理原則不支援開機組態 `XDPDefault`。

從 ONTAP 9.15.1 開始、 SnapMirror 主動式同步可在容錯移轉事件之後、自動在扇出式階段重新設定。如果從主要站台到次要站台的容錯移轉成功、則會自動重新設定第三站台、將次要站台視為來源站台。非同步扇出腿可以是一致性群組關係，也可以是一種無關的磁碟區關係。重新設定將適用於上述任一種情況。重新設定是由計畫性或非計畫性的容錯移轉所觸發。在容錯回復至主要站台時、也會進行重新設定。

如需在舊版 ONTAP 中管理您的扇出組態的相關資訊、請參閱 在連出組態中恢復保護。

NDMP 還原

從 ONTAP 9.13.1 開始，您可以使用 NDMP 來複製及還原資料SnapMirror 主動式同步。使用 NDMP 可讓您將資料移至 SnapMirror 主動式同步來源、以完成還原而不需暫停保護。這在扇出組態中特別有用。

SnapCenter

SnapCenter 支援 SnapMirror 主動式同步"SnapCenter 5.0"，從開始。SnapCenter 可建立快照，用於保護及恢復應用程式和虛擬機器，以應用程式層級的精細度提供永遠可用的儲存解決方案。

SnapRestore

SnapMirror 主動式同步支援部分和單一檔案 SnapRestore 。

單一檔案 SnapRestore

從 ONTAP 9.11.1 開始， 單一檔案SnapRestore 的功能SnapMirror 作用中同步磁碟區支援。您可以從從 SnapMirror 作用中同步來源複寫到目的地的快照，還原單一檔案。由於磁碟區可以包含一或多個 LUN 、因此此功能可協助您實作不中斷營運的還原作業、以精細的方式還原單一 LUN 、而不會中斷其他 LUN 。單一檔案 SnapRestore 有兩個選項：就地和異地。

部分檔案 SnapRestore

從 ONTAP 9.12.1 開始， "部分 LUN 還原"SnapMirror 作用中同步磁碟區支援。您可以從應用程式建立的快照還原資料，這些快照已在 SnapMirror 作用中同步來源（ Volume ）和目的地（ Snapshot ）磁碟區之間複寫。如果您需要還原在同一個 LUN 上儲存多個資料庫的主機上的資料庫、則可能需要部分 LUN 或檔案還原。使用此功能時、您必須知道資料和位元組數的起始位元組偏移。

大型LUN和大型磁碟區

大型 LUN 和大型磁碟區（大於 100 TB ）的支援取決於您所使用的 ONTAP 版本和平台。

ONTAP 9.12.1P2 及更新版本

- 對於 ONTAP 9 。 12.1 P2 及更新版本、 SnapMirror 主動式同步支援大型 LUN 、以及 ASA 和 AFF （ A 系列和 C 系列）上大於 100 TB 的大型磁碟區。主叢集和次叢集的類型必須相同： ASA 或 AFF 。支援從 AFF A 系列複寫至 AFF C 系列、反之亦然。

> ⓘ 對於 ONTAP 9.12.1P2 版及更新版本、您必須確保主要和次要叢集都是 All Flash SAN Array （ ASA ）或 All Flash Array （ AFF ）、而且兩者都已安裝 ONTAP 9.12.1 P2 或更新版本。如果次要叢集執行的版本早於 ONTAP 9.12.1P2 、或陣列類型與主要叢集不同、則當主要磁碟區的容量大於 100 TB 時、同步關係可能會不同步。

ONTAP 9.9.1 - 9.12.1P1

- 對於 ONTAP 9.9.1 和 9.12.1 P1 （含）之間的 ONTAP 版本、大型 LUN 和大於 100TB 的大型磁碟區僅在 All Flash SAN 陣列上受支援。支援從 AFF A 系列複寫至 AFF C 系列、反之亦然。

> ⓘ 對於 ONTAP 9.9.1 和 9.12.1 P2 之間的 ONTAP 版本、您必須確保主叢集和次叢集都是 All Flash SAN 陣列、而且兩者都已安裝 ONTAP 9.9.1 或更新版本。如果次要叢集執行的版本早於 ONTAP 9.9.1 、或不是 All Flash SAN 陣列、則當主要磁碟區成長超過 100 TB 時、同步關係可能會不同步。

更多資訊

- "如何設定用於 SnapMirror 主動同步的 AIX 主機"

ONTAP SnapMirror主動同步的物件限制

準備使用 SnapMirror 主動式同步時、請注意下列物件限制。

叢集中的一致性群組

使用 SnapMirror 主動同步的叢集一致性群組限制是根據關係計算、並取決於所使用的 ONTAP 版本。限制與平台無關。

版本**ONTAP**	最大關係數
更新版本ONTAP	50*
零點9.10.1 ONTAP	20.
部分9.9.1 ONTAP	5.

｛Asterisk｝ 從 ONTAP 9.16.1 開始， SnapMirror 主動式同步支援對稱式雙主動 / 主動式組態中的四節點叢集。在四節點叢集中，支援 100 個一致性群組。

每個一致性群組的磁碟區

每個一致性群組與 SnapMirror 主動式同步的最大磁碟區數量不受平台限制。

版本**ONTAP**	一致性群組關係中支援的磁碟區數量上限
ONTAP 9.15.1 及更新版本	80
ONTAP 9.10.1-9.14.1	16.
部分9.9.1 ONTAP	12.

磁碟區

SnapMirror 主動同步中的 Volume 限制是根據端點數量而非關係數量來計算。具有 12 個磁碟區的一致性群組、可在主叢集和次叢集上提供 12 個端點。SnapMirror 主動式同步和 SnapMirror 同步關係都有助於達到端點總數。

這些限制適用於FAS、 AFF和ASA系統。如果您擁有ASA r2 系統（ASA A1K、 ASA A90、 ASA A70、 ASA A50、 ASA A30 或ASA A20），請參閱"ASA R2 說明文件" 。

下表列出每個平台的最大端點數。

平台	每個 **HA** 的端點用於 **SnapMirror** 主動同步			每個 **HA** 的整體同步和 **SnapMirror** 主動同步端點		
	更新版本ONTAP	零點9.10.1 ONTAP	部分9.9.1 ONTAP	更新版本ONTAP	零點9.10.1 ONTAP	部分9.9.1 ONTAP
AFF	400*	200	60	400	200	80
ASA	400*	200	60	400	200	80

｛Asterisk｝ 從 ONTAP 9.16.1 開始， SnapMirror 主動式同步支援對稱式雙主動 / 主動式組態中的四節點叢集。四節點叢集的總上限為 800 個端點。

SAN物件限制

下表包含 SAN 物件限制。無論平台為何、限制都適用。

SnapMirror主動同步關係中的對象	數
每個磁碟區的LUN數量	• 256 （ ONTAP 9.9.1 - ONTAP 9.15.0 ） • 512 （ ONTAP 9.15.1 及更新版本）
每個 2 x 2 SnapMirror主動同步解決方案的唯一 LUN、命名空間或儲存單元的數量	4 、 096
每個 4 x 4 SnapMirror主動同步解決方案的唯一 LUN、命名空間或儲存單元的數量（從ONTAP 9.16.1 開始提供）	6 、 144
每個 SVM 的 LIF（至少有一個磁碟區處於SnapMirror主動同步關係中）	256
每個節點的叢集間生命量	4.
每個叢集的叢集間生命量	8.

NVMe 物件限制

從ONTAP 9.17.1 開始， SnapMirror主動同步支援 NVMe 協定。下表列出了 NVMe 物件的限制。

SnapMirror主動同步關係中的最大物件數	數
每個節點的命名空間映射數量	4K
簇大小	2個節點
每個 HA 對的一致性組數量	50
單一 NVMe SnapMirror活動同步一致性群組中的磁碟區數	80
HA 對中的捲數	400
每個一致性組的 NVMe 子系統	16.
每個一致性組的命名空間映射	256

相關資訊

- "Hardware Universe"
- "一致性群組限制"

設定

為**SnapMirror**主動同步配置**ONTAP**集群

SnapMirror主動同步使用對等叢集在發生故障轉移時保護您的資料。在為SnapMirror主動同步設定ONTAP Mediator 或ONTAP Cloud Mediator 之前，必須先確保叢集已正確設定。

開始之前

在設定ONTAP Mediator 或ONTAP Cloud Mediator 之前，您應該確認以下內容：

1. 集群之間存在集群對等關係。

   SnapMirror 主動同步對於叢集對等關係而言、需要預設的 IPspace 。不支援自訂 IPspace 。

   "建立叢集對等關係"

2. 在每個叢集上建立 SVM。

   "建立SVM"

3. 每個叢集上的 SVM 之間存在對等關係。

   "建立SVM對等關係"

4. 您的 LUN 中存在磁碟區。

   "建立Volume"

5. 在兩個叢集中的每個節點上至少建立一個 SAN LIF（FC 或 iSCSI，視情況而定）。

   "叢集SAN環境中的LIF考量"

   "建立LIF"

6. 建立必要的 LUN 並將其對應到 igroup，用於將 LUN 對應到應用程式主機上的啟動器。

   "建立LUN並對應igroup"

7. 重新掃描應用程式主機以發現任何新的 LUN。

為**SnapMirror**主動同步配置**ONTAP**調解器

SnapMirror 主動式同步使用對等叢集，在發生容錯移轉情況時保護您的資料。ONTAP 調解器是一項關鍵資源，它透過監控每個叢集的運作狀況來確保業務連續性。若要設定 SnapMirror 主動同步，您必須先安裝 ONTAP 調解器，並驗證主叢集和輔助叢集是否已正確設定。

安裝 ONTAP Mediator 並配置叢集後， 使用自簽名憑證初始化 ONTAP 調解器以進行 SnapMirror 主動同步 。您必須如此建立、初始化及對應 SnapMirror 主動式同步的一致性群組。

資訊媒體**ONTAP**

ONTAP 調解器為 SnapMirror 主動同步關係中的 ONTAP 叢集所使用的高可用性 (HA) 元資料提供持久且受保護的儲存。此外， ONTAP Mediator 還提供同步節點健全狀況查詢功能，以協助仲裁判斷，並做為偵測控制器活躍度的 Ping Proxy 。

每個叢集對等關係只能與單一 ONTAP Mediator 執行個體關聯。HA Mediator 執行個體不受支援。當叢集與其他叢集處於多個對等關係中時，可使用下列 ONTAP Mediator 選項：

- 如果在每個關係上設定 SnapMirror 主動式同步，則每個叢集對等關係都可以擁有自己唯一的 ONTAP Mediator 執行個體。

- 叢集可以對所有對等關係使用相同的 ONTAP Mediator 執行個體。

例如，如果叢集 B 與叢集 A ，叢集 C 和叢集 D 之間有對等關係，則在每個關係上設定 SnapMirror 作用中同步時，所有三個叢集對等關係都可以擁有唯一的關聯 ONTAP Mediator 執行個體。或者，叢集 B 也可以對所有三個對等關係使用相同的 ONTAP Mediator 執行個體。在此案例中，叢集會列出三次相同的 ONTAP Mediator 執行個體。

從ONTAP 9.17.1 開始，您可以設定"ONTAP雲端調解器"但是，要在SnapMirror主動同步配置中監控叢集的運作狀況，您不能同時使用這兩個中介器。

如果您將SnapMirror主動同步和ONTAP Mediator 或ONTAP Cloud Mediator 與ONTAP 9.17.1 一起使用，則應查看"發行說明 ONTAP"有關這些配置的重要資訊。

ONTAP 調解器的先決條件

- ONTAP Mediator 本身包含一組先決條件。您必須先滿足這些先決條件，然後才能安裝 ONTAP Mediator。

  有關詳細信息，請參閱"準備安裝ONTAP調解器服務" 。

- 預設情況下， ONTAP調解器透過 TCP 連接埠 31784 提供服務。您應確保連接埠 31784 在ONTAP叢集和ONTAP調解器之間處於開啟狀態且可用。

安裝 **ONTAP** 調解器並確認叢集配置

執行下列每個步驟來安裝 ONTAP 調解器並驗證叢集配置。對於每個步驟、您都應該確認已執行特定組態。每個步驟都包含您需要遵循的特定程序連結。

步驟

1. 在驗證來源叢集和目標叢集是否配置正確之前，請安裝 ONTAP 調解器。

   準備安裝或升級 ONTAP 調解器

2. 確認叢集之間存在叢集對等關係。

   SnapMirror 主動同步對於叢集對等關係而言、需要預設的 IPspace 。不支援自訂 IPspace 。

   "為SnapMirror主動同步配置ONTAP集群"

使用自簽名憑證初始化 **ONTAP** 調解器以進行 **SnapMirror** 主動同步

安裝 ONTAP 調解器並確認叢集配置後，必須初始化 ONTAP 調解器以進行叢集監控。您可以使用 System Manager 或 ONTAP CLI 初始化 ONTAP 調解器。

系統管理員

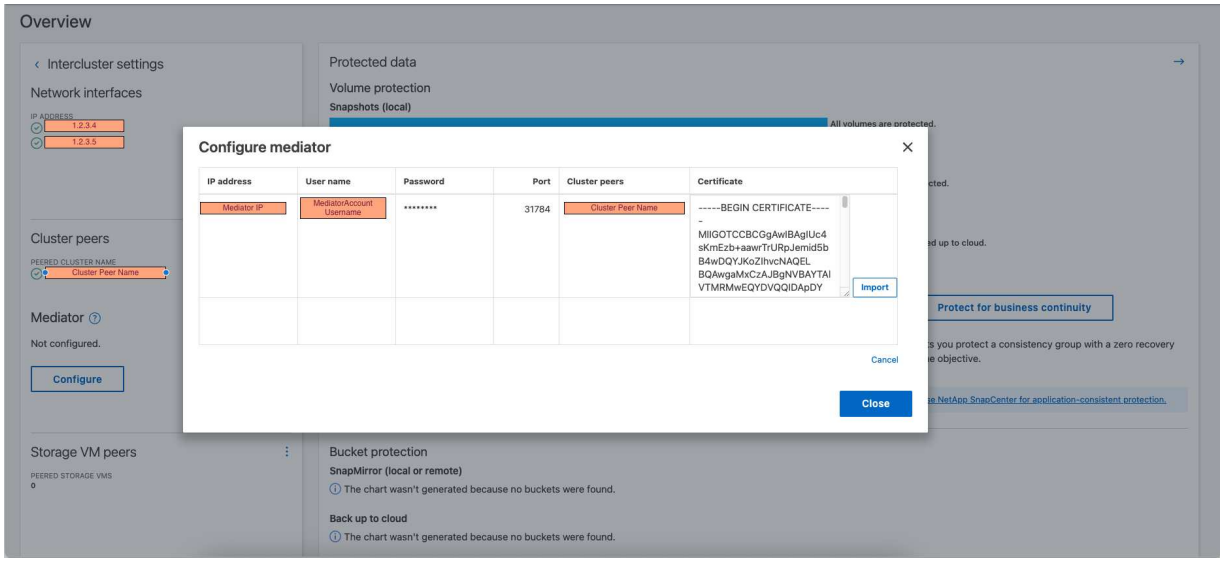
使用系統管理器，您可以設定 ONTAP 調解器以實現自動故障轉移。如果您尚未使用第三方驗證的SSL憑證和CA、也可以將自行簽署的SSL和CA更換為第三方驗證的SSL憑證和CA。

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

ONTAP Mediator 1.9 及更新版本

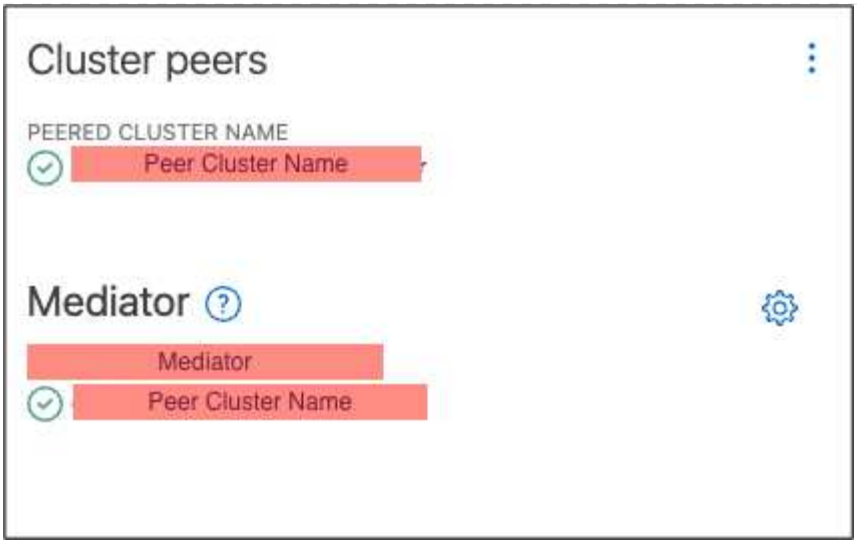
1. 瀏覽至* Protection > Overview > Mediator > Configure *。
2. 選擇“新增”，然後輸入下列 ONTAP 調解器資訊：
   - IPV4位址
   - 使用者名稱
   - 密碼
   - 憑證
3. 您可以使用兩種方式提供「憑證」輸入：
   - * 選項（ a ） * ：選取 * Import （匯入） * 以瀏覽至 `intermediate.crt`檔案並將其匯入。
   - * 選項（ b ） * ：複製檔案內容 `intermediate.crt`，並將其貼到 * 憑證 * 欄位。

   正確輸入所有詳細資料後、所提供的憑證會安裝在所有對等叢集上。



證書新增完成後，ONTAP 調解器將會新增至 ONTAP 叢集。

下列影像示範 ONTAP Mediator 組態成功：

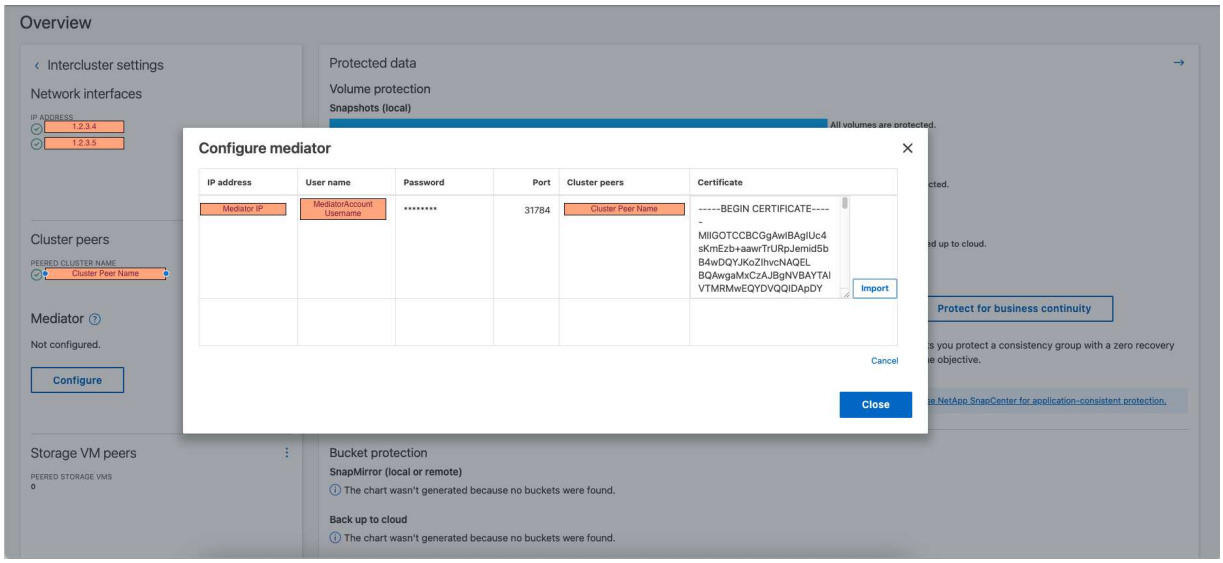


。

ONTAP Mediator 1.8 及更早版本

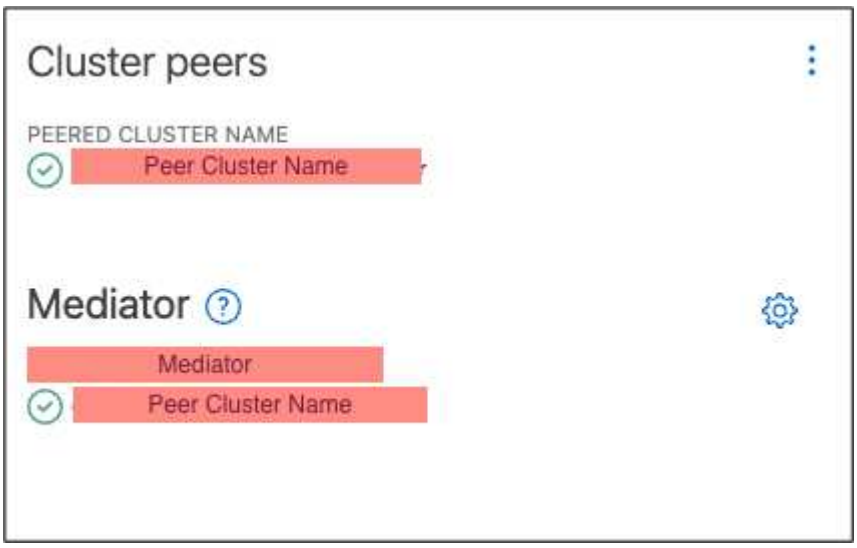
1. 瀏覽至* Protection > Overview > Mediator > Configure *。
2. 選擇"新增"，然後輸入下列 ONTAP 調解器資訊：
   - IPV4位址
   - 使用者名稱
   - 密碼
   - 憑證
3. 您可以使用兩種方式提供「憑證」輸入：
   - * 選項（ a ） * ：選取 * Import （匯入） * 以瀏覽至 `ca.crt`檔案並將其匯入。
   - * 選項（ b ） * ：複製檔案內容 `ca.crt`，並將其貼到 * 憑證 * 欄位。

   正確輸入所有詳細資料後、所提供的憑證會安裝在所有對等叢集上。



證書新增完成後，ONTAP 調解器將會新增至 ONTAP 叢集。

下列影像示範 ONTAP Mediator 組態成功：



。

CLI

您可以使用 ONTAP CLI 從主叢集或輔助叢集初始化 ONTAP 調解器。當您發出 `mediator add`指令時，ONTAP Mediator 會自動新增到另一個叢集。

使用 ONTAP 調解器監控 SnapMirror 主動同步關係時，如果沒有有效的自簽名憑證或憑證授權單位 (CA) 證書，則無法在 ONTAP 中初始化 ONTAP 調解器。您可以將有效的憑證新增至對等叢集的憑證存放區。使用 ONTAP 調解器監控 MetroCluster IP 系統時，初始設定後不會使用 HTTPS；因此，不需要憑證。

ONTAP Mediator 1.9 及更新版本

1. 從 ONTAP Mediator Linux VM/ 主機軟體安裝位置尋找 ONTAP Mediator CA 憑證 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`。
2. 將有效的憑證授權單位新增至對等叢集上的憑證存放區。

   範例：

   ```
   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

3. 將 ONTAP Mediator CA 憑證新增至 ONTAP 叢集。出現提示時，插入從 ONTAP Mediator 取得的 CA 憑證。在所有對等叢集上重複這些步驟：

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   範例：

   ```
   [root@ontap-mediator ~]# cd
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

   [root@ontap-mediator_config]# cat intermediate.crt
   -----BEGIN CERTIFICATE-----
   <certificate_value>
   -----END CERTIFICATE-----
   ```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 檢視使用產生的憑證名稱所安裝的自我簽署 CA 憑證：

   `security certificate show -common-name <common_name>`

   範例：

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- -------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                          ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 在其中一個叢集上初始化 ONTAP 調解器。ONTAP 調解器將自動新增至另一個叢集：

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   範例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 您也可以選擇檢查工作 ID 狀態 `job show -id`，以確認 SnapMirror Mediator ADD 命令是否成功。

   範例：

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- -------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. 檢查 ONTAP Mediator 組態的狀態：

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status`指示 SnapMirror 一致性群組關係是否與 ONTAP 調解器同步；狀態為 `true`表示同步成功。

ONTAP Mediator 1.8 及更早版本

1. 從 ONTAP Mediator Linux VM/ 主機軟體安裝位置尋找 ONTAP Mediator CA 憑證 `cd /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`。
2. 將有效的憑證授權單位新增至對等叢集上的憑證存放區。

   範例：

```
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

3. 將 ONTAP Mediator CA 憑證新增至 ONTAP 叢集。出現提示時、請插入從 ONTAP Mediator 取得的 CA 憑證。在所有對等叢集上重複這些步驟：

   ```
   security certificate install -type server-ca -vserver <vserver_name>
   ```

   範例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

4. 檢視使用產生的憑證名稱所安裝的自我簽署 CA 憑證：

   `security certificate show -common-name <common_name>`

   範例：

```
C1_test_cluster::*> security certificate show -common-name
ONTAPMediatorCA
Vserver    Serial Number   Certificate Name
Type
---------- --------------- ------------------------------------
------------
C1_test_cluster
           6BFD17DXXXXX7A71BB1F44D0326D2DEEXXXXX
                           ONTAPMediatorCA
server-ca
    Certificate Authority: ONTAP Mediator CA
          Expiration Date: Thu Feb 15 14:35:25 2029
```

5. 在其中一個叢集上初始化 ONTAP 調解器。ONTAP 調解器將自動新增至另一個叢集：

   `snapmirror mediator add -mediator-address <ip_address> -peer-cluster <peer_cluster_name> -username user_name`

   範例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin
Notice: Enter the mediator password.

Enter the password: ******
Enter the password again: ******
```

6. 您也可以選擇檢查工作 ID 狀態 `job show -id`，以確認 SnapMirror Mediator ADD 命令是否成功。

   範例：

```
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.


C1_test_cluster::*> snapmirror mediator add -peer-cluster
C2_test_cluster -type on-prem -mediator-address 1.2.3.4 -username
mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Running

Description: Creating a mediator entry

C1_test_cluster::*> job show -id 87
                            Owning
Job ID Name                 Vserver           Node           State
------ -------------------- ----------------- --------------
----------
87     mediator add         C1_test_cluster   C2_test        Success

Description: Creating a mediator entry

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
Type
---------------- ---------------- ----------------- -------------
-------
1.2.3.4          C2_test_cluster  connected         true
on-prem

C1_test_cluster::*>
```

7. 檢查 ONTAP Mediator 組態的狀態：

```
snapmirror mediator show
```

```
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected        true
```

`Quorum Status`指示 SnapMirror 一致性群組關係是否與 ONTAP 調解器同步；狀態為 `true`表示同步成功。

使用協力廠商憑證重新初始化 **ONTAP Mediator**

您可能需要重新初始化 ONTAP 調解器。在某些情況下，例如 ONTAP 調解器 IP 位址變更、憑證過期等，可能需要重新初始化 ONTAP 調解器。

下列程序說明當自我簽署的憑證需要由協力廠商憑證取代時，針對特定案例重新初始化 ONTAP Mediator 。

關於這項工作

您需要將 SnapMirror 主動同步叢集的自簽名證書替換為第三方證書，從 ONTAP 中刪除 ONTAP 調解器配置，然後新增 ONTAP 調解器。

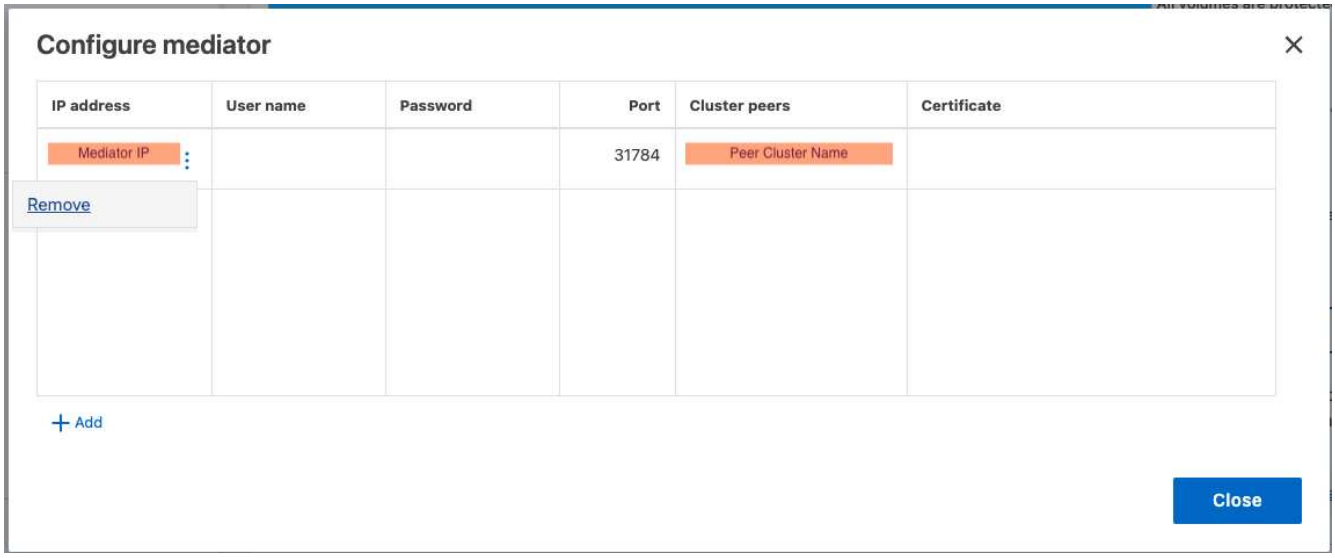
系統管理員

使用系統管理器，您需要從 ONTAP 叢集中刪除使用舊的自簽名憑證設定的 ONTAP 調解器版本，然後使用新的第三方憑證重新設定 ONTAP 叢集。

步驟

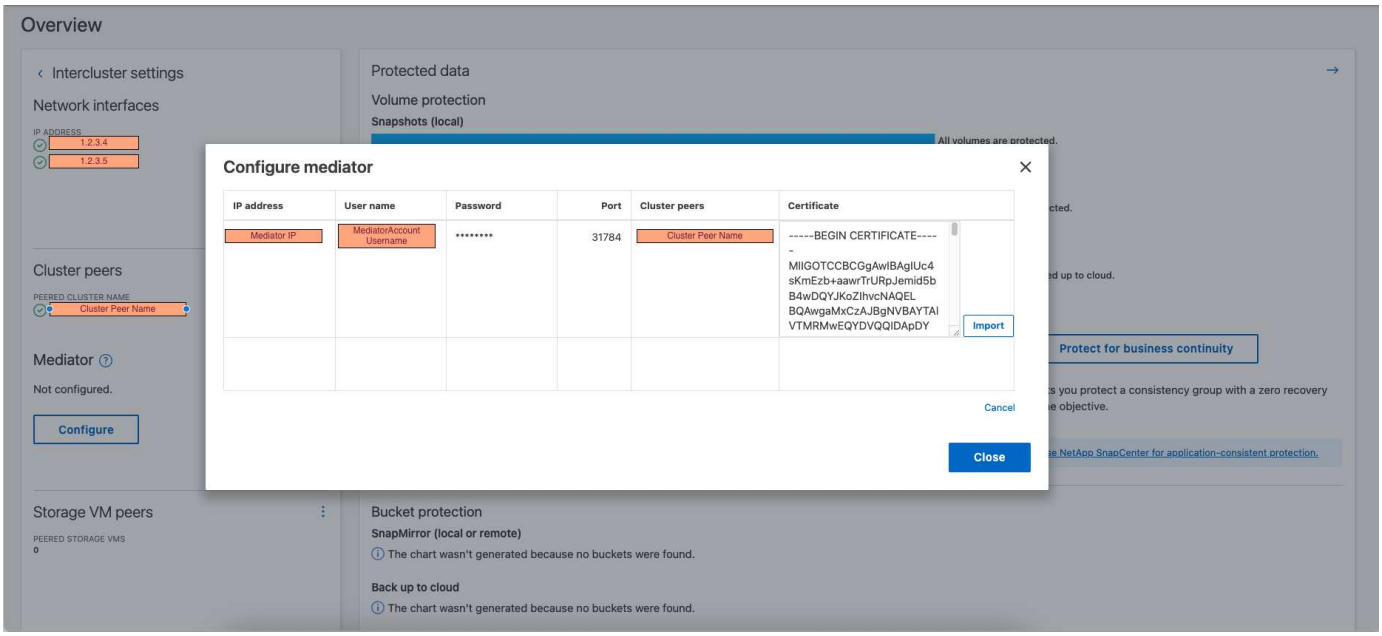
1. 選擇選單選項圖示並選擇*刪除*以刪除 ONTAP Mediator。

此步驟不會從 ONTAP 叢集移除自我簽署的 server-ca 。NetApp 建議您先瀏覽 * 憑證 * 索引標籤、然後手動移除、再執行下列步驟以新增協力廠商憑證：



2. 使用正確的憑證再次新增 ONTAP 調解器。

ONTAP 調解器現已設定新的第三方自簽章憑證。



CLI

您可以使用 ONTAP CLI 將自簽名憑證取代為第三方證書，從而從主叢集或輔助叢集重新初始化 ONTAP 調解器。

ONTAP Mediator 1.9 及更新版本

1. 當您為所有叢集使用自我簽署憑證時，請移除先前安裝的自我 `intermediate.crt`簽署憑證。在以下範例中、有兩個叢集：

   範例：

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 使用從 SnapMirror 主動式同步叢集移除先前設定的 ONTAP Mediator `-force true` ：

   範例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 請參閱中所述的步驟"以信任的協力廠商憑證取代自我簽署的憑證"，以取得如何從次級 CA 取得憑證的指示，稱為 `intermediate.crt`。以信任的協力廠商憑證取代自我簽署的憑證

具有某些屬性，這些屬性是從需要傳送至檔案中定義的 PKI 授權單位的要求所 `intermediate.crt`衍生而來 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. 從 ONTAP Mediator Linux VM/ 主機軟體安裝位置新增第三方 ONTAP Mediator CA 憑證 `intermediate.crt`：

   範例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat intermediate.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. 將檔案新增 `intermediate.crt`至對等叢集。對所有對等叢集重複此步驟：

   範例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 從 SnapMirror 主動同步叢集移除先前設定的 ONTAP Mediator ：

   範例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. 再次新增 ONTAP 調解器：

   範例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` 指出 SnapMirror 一致性群組關係是否與中介者同步；狀態為 `true` 表示同步成功。

ONTAP Mediator 1.8 及更早版本

1. 當您為所有叢集使用自我簽署憑證時，請移除先前安裝的自我 `ca.crt`簽署憑證。在以下範例中、有兩個叢集：

   範例：

```
 C1_test_cluster::*> security certificate delete -vserver
C1_test_cluster -common-name ONTAPMediatorCA
 2 entries were deleted.

 C2_test_cluster::*> security certificate delete -vserver
C2_test_cluster -common-name ONTAPMediatorCA *
 2 entries were deleted.
```

2. 使用從 SnapMirror 主動式同步叢集移除先前設定的 ONTAP Mediator `-force true` ：

   範例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster   connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -force true

Warning: You are trying to remove the ONTAP Mediator configuration
with force. If this configuration exists on the peer cluster, it
could lead to failure of a SnapMirror failover operation. Check if
this configuration
         exists on the peer cluster C2_test_cluster and remove it as
well.
Do you want to continue? {y|n}: y

Info: [Job 136] 'mediator remove' job queued

C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

3. 請參閱中所述的步驟"以信任的協力廠商憑證取代自我簽署的憑證"，以取得如何從次級 CA 取得憑證的指示，稱為 `ca.crt`。以信任的協力廠商憑證取代自我簽署的憑證

   > 具有某些屬性，這些屬性是從需要傳送至檔案中定義的 PKI 授權單位的要求所 `ca.crt`衍生而來 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`

4. 從 ONTAP Mediator Linux VM/ 主機軟體安裝位置新增第三方 ONTAP Mediator CA 憑證 `ca.crt`：

   範例：

```
[root@ontap-mediator ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@ontap-mediator_config]# cat ca.crt
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

5. 將檔案新增 `intermediate.crt`至對等叢集。對所有對等叢集重複此步驟：

   範例：

```
C1_test_cluster::*> security certificate install -type server-ca
-vserver C1_test_cluster

Please enter Certificate: Press when done
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

You should keep a copy of the CA-signed digital certificate for
future reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: D86D8E4E87142XXX

The certificate's generated name for reference: ONTAPMediatorCA

C1_test_cluster::*>
```

6. 從 SnapMirror 主動同步叢集移除先前設定的 ONTAP Mediator ：

   範例：

```
C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true

C1_test_cluster::*> snapmirror mediator remove -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster

Info: [Job 86] 'mediator remove' job queued
C1_test_cluster::*> snapmirror mediator show
This table is currently empty.
```

7. 再次新增 ONTAP 調解器：

   範例：

```
C1_test_cluster::*> snapmirror mediator add -mediator-address
1.2.3.4 -peer-cluster C2_test_cluster -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 87] 'mediator add' job queued

C1_test_cluster::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
1.2.3.4          C2_test_cluster  connected         true
```

   `Quorum Status` 指出 SnapMirror 一致性群組關係是否與中介者同步；狀態為 `true` 表示同步成功。

相關資訊

- "工作展示"
- "刪除安全性憑證"
- "安全性憑證安裝"
- "安全證書展示"
- "SnapMirror 中介添加"
- "SnapMirror 中介器刪除"
- "SnapMirror 中介顯示"

準備配置ONTAP Cloud Mediator

在你之前"配置ONTAP Cloud Mediator" ，您必須確保滿足先決條件。

防火牆需求

網域控制器上的防火牆設定必須允許 HTTPS 流量 `api.bluexp.netapp.com`來自兩個集群。

代理伺服器要求

如果您使用代理伺服器進行SnapMirror主動同步，請確保已建立代理伺服器並且您具有以下代理伺服器資訊：

- HTTPS代理IP
- 連接埠
- 使用者名稱
- 密碼

延遲

NetApp控制台雲端伺服器和SnapMirror主動同步叢集對等點之間的建議 ping 延遲小於 200 毫秒。

根 **CA** 憑證

檢查集群的證書

ONTAP預先安裝了知名的根 CA 證書，因此在大多數情況下，您不需要安裝NetApp控制台伺服器的根 CA 憑證。在開始ONTAP Cloud Mediator 設定之前，您可以檢查叢集以驗證憑證是否存在：

範例：

```
C1_cluster% openssl s_client -showcerts -connect
api.bluexp.netapp.com:443|egrep "s:|i:"
depth=2 C = US, O = DigiCert Inc, OU = www.digicert.com, CN = DigiCert
Global Root G2
verify return:1
depth=1 C = US, O = Microsoft Corporation, CN = Microsoft Azure RSA TLS
Issuing CA 04
verify return:1
depth=0 C = US, ST = WA, L = Redmond, O = Microsoft Corporation, CN =
*.azureedge.net
verify return:1
 0 s:/C=US/ST=WA/L=Redmond/O=Microsoft Corporation/CN=*.azureedge.net
   i:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
 1 s:/C=US/O=Microsoft Corporation/CN=Microsoft Azure RSA TLS Issuing CA
04
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
 2 s:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
```

```
   i:/C=US/O=DigiCert Inc/OU=www.digicert.com/CN=DigiCert Global Root G2
<====

C1_cluster::> security certificate show -common-name DigiCert*
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
C1_cluster 0CE7E0EXXXXX46FE8FE560FC1BFXXXXX DigiCertAssuredIDRootCA
server-ca
    Certificate Authority: DigiCert Assured ID Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 0B931C3XXXXX67EA6723BFC3AF9XXXXX DigiCertAssuredIDRootG2
server-ca
    Certificate Authority: DigiCert Assured ID Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 0BA15AFXXXXXA0B54944AFCD24AXXXXX DigiCertAssuredIDRootG3
server-ca
    Certificate Authority: DigiCert Assured ID Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 083BE05XXXXX46B1A1756AC9599XXXXX DigiCertGlobalRootCA server-ca
    Certificate Authority: DigiCert Global Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 033AF1EXXXXXA9A0BB2864B11D0XXXXX DigiCertGlobalRootG2 server-ca
    Certificate Authority: DigiCert Global Root G2
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 055556BXXXXXA43535C3A40FD5AXXXXX DigiCertGlobalRootG3 server-ca
    Certificate Authority: DigiCert Global Root G3
          Expiration Date: Fri Jan 15 17:30:00 2038

C1_cluster 02AC5C2XXXXX409B8F0B79F2AE4XXXXX DigiCertHighAssuranceEVRootCA
server-ca
    Certificate Authority: DigiCert High Assurance EV Root CA
          Expiration Date: Mon Nov 10 05:30:00 2031

C1_cluster 059B1B5XXXXX2132E23907BDA77XXXXX DigiCertTrustedRootG4 server-
ca
    Certificate Authority: DigiCert Trusted Root G4
          Expiration Date: Fri Jan 15 17:30:00 2038
```

檢查代理伺服器是否安裝了證書

如果您使用代理程式連接到NetApp控制台中的ONTAP Cloud Mediator 服務，請確保代理伺服器的根 CA 憑證已

安裝在ONTAP中：

範例：

```
C1_cluster% openssl s_client -showcerts -proxy <ip:port> -connect
api.bluexp.netapp.com:443 |egrep "s:|i:"
```

下載**CA**憑證：

如果需要，您可以從憑證授權單位的網站下載根 CA 憑證並將其安裝在叢集上。

範例：

```
C1_cluster::> security certificate install -type server-ca -vserver
C1_cluster

C2_cluster::> security certificate install -type server-ca -vserver
C2_cluster
```

為**SnapMirror**主動同步設定**ONTAP Cloud Mediator**

從ONTAP 9.17.1 開始，您可以使用ONTAP Cloud Mediator 監控每個叢集的運作狀況，從而實現業務連續性。 ONTAPCloud Mediator 是一項基於雲端的服務。將ONTAP Cloud Mediator當您將ONTAP Cloud Mediator 與SnapMirror主動同步結合使用時，必須先確認已配置NetApp控制台服務和客戶端訊息，並確保叢集對等連線正確。

與ONTAP Mediator 一樣， ONTAP Cloud Mediator 為SnapMirror主動同步關係中的ONTAP叢集所使用的高可用性 (HA) 元資料提供持久且受保護的儲存。 ONTAPONTAP Mediator 提供同步節點運作狀況查詢功能，以協助確定仲裁數量，並可用作控制器活躍度偵測的 ping 代理程式。

> 如果您將SnapMirror主動同步和ONTAP Mediator 或ONTAP Cloud Mediator 與ONTAP 9.17.1 一起使用，則應查看"發行說明 ONTAP"有關這些配置的重要資訊。

開始之前

在設定ONTAP Cloud Mediator 之前，您應該確認以下資訊：

- 叢集已配置。

  "為SnapMirror主動同步配置ONTAP集群"

- 您已從NetApp控制台複製了您的NetApp控制台組織 ID，並建立了一個控制台成員服務帳戶，以便在配置ONTAP Cloud Mediator 時使用。建立服務帳戶時，必須將組織設定為您設定ONTAP Cloud Mediator 的訂閱。類別必須設定為“應用程式”，角色類型必須設定為“ONTAP Mediator 設定角色”。建立角色時，必須儲存客戶端 ID 和客戶端金鑰。

  "新增NetApp控制台成員和服務帳戶"

步驟

您可以使用系統管理員或ONTAP CLI 新增ONTAP Cloud Mediator。

系統管理員

1. 導航至*保護>概述>中介*並選擇*新增*。
2. 在「新增中介器」視窗中，選擇「雲端」作為中介器類型並輸入以下資訊：
   - NetApp控制台組織 ID
   - NetApp控制台用戶端 ID
   - NetApp控制台用戶端金鑰
3. 選擇集群對等方。
4. 如果您正在使用 HTTP 代理且尚未配置，請輸入本機和遠端主機的 HTTP 代理資訊。

   建議您為每個叢集對等體使用不同的代理伺服器。
5. 可選：如果需要在ONTAP中安裝根 CA 證書，尤其是在使用代理伺服器時，請將證書貼到提供的文字方塊中。
6. 選取*「Add*」。
7. 導覽至 保護>概覽 並檢查SnapMirror活動同步叢集和ONTAP Cloud Mediator 之間的關係狀態。

CLI

1. 配置ONTAP Cloud Mediator：
   ```
   snapmirror mediator add -peer-cluster <peerClusterName> -type cloud -bluexp
   -org-id <NetApp Console Organization ID> -service-account-client-id
   <Service Account Client ID> -use-http-proxy-local <true|false> -use-http
   -proxy-remote <true|false>
   ```
2. 檢查ONTAP Cloud Mediator 狀態：
   ```
   snapmirror mediator show
   ```

   範例：

   ```
   C1_cluster::> snapmirror mediator show
   Mediator Address Peer Cluster     Connection Status Quorum Status
   Type
   ---------------- ---------------- ----------------- -------------
   -------
   0.0.0.0          C2_cluster       connected         true
   cloud
   ```

使用**ONTAP SnapMirror**主動同步進行保護

SnapMirror 主動式同步提供非對稱式保護、從 ONTAP 9.15.1 開始提供對稱式主動 / 主動式保護。

使用 SnapMirror 主動同步設定非對稱式保護包括在 ONTAP 來源叢集上選取 LUN 、並將其新增至一致性群組。

開始之前

- 您必須擁有 SnapMirror 同步授權。
- 您必須是叢集或儲存VM管理員。
- 一致性群組中的所有組成磁碟區都必須位於單一儲存 VM （ SVM ）中。
  - LUN可位於不同的磁碟區。
- 來源與目的地叢集不能相同。
- 您無法在 ASA 叢集和非 ASA 叢集之間建立 SnapMirror 主動式同步一致性群組關係。
- SnapMirror 主動同步對於叢集對等關係而言、需要預設的 IPspace 。不支援自訂IPspace。
- 一致性群組的名稱必須是唯一的。
- 次要（目的地）叢集上的磁碟區必須是 DP 類型。
- 主要和次要 SVM 必須處於對等關係中。

步驟

您可以使用 ONTAP CLI 或系統管理員來設定一致性群組。

從ONTAP 9.10.1 開始， ONTAP在 System Manager 中提供了一致性群組端點和選單，從而提供了額外的管理公用程式。如果您使用的是ONTAP 9.10.1 或更高版本，請參閱"設定一致性群組"然後"設定保護"建立SnapMirror主動同步關係。

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

系統管理員

1. 在主叢集上、瀏覽至 * 保護 > 總覽 > 保護業務持續運作 > 保護 LUN* 。
2. 選取您要保護的 LUN 、並將其新增至保護群組。
3. 選取目的地叢集和SVM。
4. 依預設會選取「初始化關係」。按一下「儲存」開始保護。
5. 請前往*儀表板>效能*以驗證LUN的IOPS活動。
6. 在目的地叢集上、使用System Manager驗證是否已同步保護營運不中斷關係：保護>關係。

CLI

1. 從目的地叢集建立一致性群組關係。
   `destination::> snapmirror create -source-path` *`source-path`* `-destination-path` *`destination-path`* `-cg-item-mappings` *`volume-paths`* `-policy` *`policy-name`*

   您可以使用對應最多 12 個組成 Volume `cg-item-mappings` 上的參數 `snapmirror create` 命令。

   以下範例建立兩個一致性群組： `cg_src_ on the source with `vol1` 和 `vol2` 以及鏡射目的地一致性群組、 `cg_dst`。

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy AutomatedFailOverDuplex
   ```

2. 從目的地叢集初始化一致性群組。

   `destination::>snapmirror initialize -destination-path` *`destination-consistency-group`*

3. 確認初始化作業已成功完成。狀態應為 `InSync`。

   ```
   snapmirror show
   ```

4. 在每個叢集上建立一個 igroup 、以便將 LUN 對應至應用程式主機上的啟動器。
   `lun igroup create -igroup` *`name`* `-protocol` *`fcp|iscsi`* `-ostype` *`os`* `-initiator` *`initiator_name`*

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

5. 在每個叢集上、將 LUN 對應至 igroup ：

   `lun map -path` *`path_name`* `-igroup` *`igroup_name`*

6. 使用驗證 LUN 對應是否成功完成 `lun map` 命令。然後、您可以在應用程式主機上探索新的 LUN 。

設定對稱式主動 / 主動式保護

您可以使用系統管理員或 ONTAP CLI 建立對稱保護。在這兩個介面中、都有不同的步驟 統一且不一致的組態。

開始之前

- 兩個叢集都必須執行 ONTAP 9.15.1 或更新版本。
- 對稱的主動 / 主動式組態需要 `AutomatedFailoverDuplex` 保護原則。或者、您也可以 建立自訂 SnapMirror 原則 已提供 `-type` 是 `automated-failover-duplex`。
- 在 ONTAP 9.15.1 中，只有雙節點叢集才支援對稱式主動 / 主動式。
- 從 ONTAP 9.16.1 GA 開始， SnapMirror 主動式同步可支援四節點叢集上的對稱式主動 / 主動式組態。
  - 若要在四節點叢集上使用 SnapMirror 主動式同步，您必須執行 ONTAP 9.16.1 GA 或更新版本。
  - 在部署四節點組態之前建立叢集對等關係，您必須先執行。
  - 檢閱限制是否有四節點叢集。
  - 如果您還原至雙節點叢集，則必須先從叢集移除 SnapMirror 作用中同步關係，然後才能還原。
  - 您可以使用四節點組態來升級儲存設備和控制器。此程序不中斷運作，可在將磁碟區移入新節點的同時擴充叢集。如需更多資訊、請參閱 "重新整理叢集"。
- 從ONTAP 9.17.1 開始，只有當兩個叢集都執行ONTAP 9.17.1 或更高版本時，您才能在 NVMe 命名空間上配置對稱主動/主動保護。

使用 **SCSI SnapMirror**主動同步配置來設定對稱主動/主動保護

步驟

您可以使用 System Manager 或ONTAP CLI 透過 SCSI 協定主機對映配置對稱主動/主動保護。

系統管理員

統一組態的步驟

1. 在主要站台上、 "使用新的 LUN 建立一致性群組。"
   a. 建立一致性群組時、請指定主機啟動器以建立 igroup 。
   b. 選中核取方塊以 啟用 **SnapMirror** 、然後選擇 `AutomatedFailoverDuplex` 原則。
   c. 在出現的對話方塊中，選取「 複寫啟動器群組 」核取方塊來複寫 igroup 。在 編輯鄰近設定 中，為主機設定近端 SVM 。
   d. 選擇 儲存 。

非統一組態的步驟

1. 在主要站台上、 "使用新的 LUN 建立一致性群組。"
   a. 建立一致性群組時、請指定主機啟動器以建立 igroup 。
   b. 選中核取方塊以 啟用 **SnapMirror** 、然後選擇 `AutomatedFailoverDuplex` 原則。
   c. 選取「 儲存 」以建立 LUN 、一致性群組、 igroup 、 SnapMirror 關係及 igroup 對應。
2. 在次要站台上、建立一個 igroup 並對應 LUN 。
   a. 瀏覽至 主機 > **SAN** 啟動器群組 。
   b. 選取「 **+Add** 」以建立新的群組群組。
   c. 提供一個 名稱 ，選擇 主機作業系統 ，然後選擇 啟動器群組成員 。
   d. 選擇 保存 以初始化關係。
3. 將新的 igroup 對應到目的地 LUN 。
   a. 瀏覽至 儲存空間 > **LUN** 。
   b. 選取要對應到 igroup 的所有 LUN 。
   c. 選擇「 更多 」、然後選擇「對應至啟動器群組」 ** 。

CLI

統一組態的步驟

1. 建立新的 SnapMirror 關係、將應用程式中的所有磁碟區分組。請務必指定 `AutomatedFailOverDuplex` 建立雙向同步複寫的原則。

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   範例：以下範例建立兩個一致性群組：來源上的 cg_src（具有 vol1 和 vol2）以及目標上的鏡像一致性群組 cg_dst。

```
destination::> snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
AutomatedFailOverDuplex
```

2. 初始化 SnapMirror 關係：
`snapmirror initialize -destination-path <destination-consistency-group>`
3. 請等待、確認作業已成功完成 `Mirrored State` 以顯示為 `SnapMirrored` 和 `Relationship Status` 做為 `Insync`。

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. 在主機上、根據您的需求、設定主機連線能力、並存取每個叢集。
5. 建立 igroup 組態。設定本機叢集上啟動器的慣用路徑。指定選項，可將組態複寫到對等叢集，以實現反關聯。

   ```
   SiteA::> igroup create -vserver <svm_name> -ostype <os_type> -igroup
   <igroup_name> -replication-peer <peer_svm_name> -initiator <host>
   ```

   從 ONTAP 9.16.1 開始，請使用 `-proximal-vserver local`此命令中的參數。

   ```
   SiteA::> igroup add -vserver <svm_name> -igroup <igroup_name> -ostype
   <os_type> -initiator <host>
   ```

   從 ONTAP 9.16.1 開始，請使用 `-proximal-vserver peer`此命令中的參數。

6. 在主機上探索路徑、並驗證主機是否有主動 / 最佳化路徑、可從偏好的叢集前往儲存 LUN 。
7. 部署應用程式並在叢集之間分散 VM 工作負載、以達到所需的負載平衡。

非統一組態的步驟

1. 建立新的 SnapMirror 關係、將應用程式中的所有磁碟區分組。請務必指定 `AutomatedFailOverDuplex` 建立雙向同步複寫的原則。

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   範例：以下範例建立兩個一致性群組：來源上的 cg_src（具有 vol1 和 vol2）以及目標上的鏡像一致性群組 cg_dst。

   ```
   destination::> snapmirror create -source-path vs1_src:/cg/cg_src
   -destination-path vs1_dst:/cg/cg_dst -cg-item-mappings
   vol_src1:@vol_dst1,vol_src2:@vol_dst2 -policy
   AutomatedFailOverDuplex
   ```

2. 初始化 SnapMirror 關係：
   `snapmirror initialize -destination-path <destination-consistency-group>`
3. 請等待、確認作業已成功完成 `Mirrored State` 以顯示為 `SnapMirrored` 和 `Relationship Status` 做為 `Insync`。

   ```
   snapmirror show -destination-path <destination_path>
   ```

4. 在主機上、根據您的需求、設定主機連線能力、並存取每個叢集。
5. 在來源叢集和目的地叢集上建立 igroup 組態。

   ```
   # primary site
   SiteA::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_1_name_>

   # secondary site
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup_name> -initiator
   <host_2_name>
   ```

6. 在主機上探索路徑、並驗證主機是否有主動 / 最佳化路徑、可從偏好的叢集前往儲存 LUN 。
7. 部署應用程式並在叢集之間分散 VM 工作負載、以達到所需的負載平衡。

使用 **NVMe SnapMirror**主動同步配置來設定對稱主動/主動保護

開始之前

除了配置對稱主動/主動保護的要求之外，您還應該注意使用 NVMe 協定時支援和不支援的配置。

- 一致性組可以有一個或多個子系統。
- 一致性群組內的磁碟區可以具有來自多個子系統的命名空間對應。
- 子系統不能有屬於多個一致性群組的命名空間映射。
- 子系統不能具有一些屬於一致性群組的命名空間映射和一些不屬於一致性群組的命名空間映射。
- 子系統必須具有屬於相同一致性群組的命名空間映射。

步驟

從ONTAP 9.17.1 開始，您可以使用 System Manager 或ONTAP CLI 建立一致性群組並使用 NVMe 協定主機對應配置對稱主動/主動保護。

系統管理員

1. 在主站點上， "使用新磁碟區或 NVMe 命名空間建立一致性群組。"
2. 選擇 **+**新增 並選擇 使用新的 **NVMe** 命名空間。
3. 輸入一致性組名稱。
4. 選擇*更多*。
5. 在“保護”部分中，選擇“啟用SnapMirror”，然後選擇 `AutomatedFailoverDuplex`政策。
6. 在 主機映射 部分中，選擇 現有 **NVMe** 子系統 或 新 **NVMe** 子系統。
7. 選擇“鄰近”可更改近端 SVM。預設選擇來源 SVM。
8. 如果需要，請添加另一個 NVMe 子系統。

CLI

1. 建立新的SnapMirror關係，將所有包含應用程式使用的所有 NVMe 命名空間的磁碟區分組。確保指定 `AutomatedFailOverDuplex`建立雙向同步複製的策略。

   ```
   snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source_volume:@destination_volume>
   -policy AutomatedFailOverDuplex
   ```

   範例：

   ```
   DST::> snapmirror create -source-path vs_src:/cg/cg_src_1
   -destination-path vs_dst:/cg/cg_dst_1 -cg-item-mappings
   vs_src_vol1:@vs_dst_vol1,vs_src_vol2:@vs_dst_vol2 -policy
   AutomatedFailOverDuplex
   ```

2. 初始化 SnapMirror 關係：
   `snapmirror initialize -destination-path <destination-consistency-group>`

   範例：

   ```
   DST::> snapmirror initialize -destination-path vs1:/cg/cg_dst_1
   ```

3. 請等待、確認作業已成功完成 `Mirrored State` 以顯示為 `SnapMirrored` 和 `Relationship Status` 做為 `Insync`。

   ```
   snapmirror show -destination-path <destination_path>
   ```

   與主磁碟區中的 NVMe 命名空間關聯的 NVMe 子系統會自動複製到輔助叢集。

4. 在主機上、根據您的需求、設定主機連線能力、並存取每個叢集。
5. 指定與每個主機最接近的 SVM。這樣，主機就可以使用首選叢集中的路徑存取 NVMe 命名空間。這可能是主叢集中的 SVM，也可能是 DR 叢集中的 SVM。

以下指令表示SVM VS_A距離主機H1較近，並將VS_A設定為近端SVM：

```
SiteA::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H1_NQN>
-proximal-vservers <VS_A>
```

以下命令表示 SVM VS_B 距離主機 H2 較近，並將 VS_B 設定為近端 SVM：

```
SiteB::> vserver nvme subsystem host add -subsystem ss1 -host-nqn <H2_NQN>
-proximal-vservers <VS_B>
```

6. 從主機發現路徑並驗證主機是否具有從首選叢集到儲存的活動/最佳化路徑。
7. 部署應用程式並在叢集之間分散 VM 工作負載、以達到所需的負載平衡。

相關資訊

- "SnapMirror建立"
- "SnapMirror初始化"
- "SnapMirror 顯示"

將現有的**ONTAP SnapMirror**關係轉換為**SnapMirror**主動同步關係

如果您已設定 SnapMirror 保護、則可將關係轉換為 SnapMirror 主動同步。從 ONTAP 9.15.1 開始、您可以將關係轉換為使用對稱式主動 / 主動式保護。

將現有的 **iSCSI** 或 **FC SnapMirror**關係轉換為不對稱**SnapMirror**主動同步關係

如果來源叢集和目標叢集之間已存在 iSCSI 或 FC SnapMirror同步關係，您可以將其轉換為非對稱SnapMirror主動同步關係。這樣，您就可以將鏡像磁碟區與一致性群組關聯，從而確保多磁碟區工作負載的 RPO 為零。此外，如果您需要還原到建立SnapMirror主動同步關係之前的時間點，您可以保留現有的SnapMirror快照。

關於這項工作

- 您必須是主叢集和次叢集上的叢集和 SVM 管理員。
- 您無法變更SnapMirror原則、將零RPO轉換為零RTO同步。
- 在發行之前、您必須確定 LUN 已取消對應 `snapmirror create` 命令。

  如果次要磁碟區上的現有 LUN 已對應、則會對應 `AutomatedFailover` 原則已設定為 `snapmirror create` 命令會觸發錯誤。

開始之前

- 主集群和輔助集群之間必須存在零 RPO SnapMirror同步關係。
- 必須先取消對應目的地磁碟區上的所有 LUN 、才能建立零 RTO SnapMirror 關係。
- SnapMirror 主動同步僅支援 SAN 傳輸協定（非 NFS/CIFS ）。確保沒有為NAS存取安裝一致性群組的任何成員。
- "資訊媒體ONTAP" 必須為SnapMirror主動同步進行設定。

步驟

1. 從次叢集、對現有關係執行 SnapMirror 更新：

   ```
   SiteB::>snapmirror update -destination-path vs1_dst:vol1
   ```

2. 驗證SnapMirror更新是否成功完成：

   ```
   SiteB::>snapmirror show
   ```

3. 暫停每個零 RPO 同步關係：

   ```
   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

   SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
   ```

4. 刪除零RPO同步關係：

   ```
   SiteB::>snapmirror delete -destination-path vs1_dst:vol1

   SiteB::>snapmirror delete -destination-path vs1_dst:vol2
   ```

5. 釋放來源 SnapMirror 關係，但保留一般快照：

   ```
   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol1

   SiteA::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol2
   ```

6. 建立零 RTO SnapMirror 同步關係：

   ```
   SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
   vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
   AutomatedFailover
   ```

7. 重新同步一致性群組：

   ```
   SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
   ```

8. 重新掃描主機LUN I/O路徑、以還原LUN的所有路徑。

將現有的 **iSCSI** 或 **FC SnapMirror**關係轉換為對稱主動/主動

從ONTAP 9.15.1 開始，您可以將現有的 iSCSI 或 FC SnapMirror關係轉換為SnapMirror主動同步對稱主動/主動關係。

開始之前

- 您必須執行 ONTAP 9.15.1 或更新版本。
- 主叢集與次叢集之間必須存在零 RPO SnapMirror 同步關係。
- 必須先取消對應目的地磁碟區上的所有 LUN 、才能建立零 RTO SnapMirror 關係。
- SnapMirror 主動同步僅支援 SAN 傳輸協定（非 NFS/CIFS ）。確保沒有為NAS存取安裝一致性群組的任何成員。

- "資訊媒體ONTAP" 必須為SnapMirror主動同步進行設定。

步驟

1. 從次叢集、對現有關係執行 SnapMirror 更新：

```
SiteB::>snapmirror update -destination-path vs1_dst:vol1
```

2. 驗證SnapMirror更新是否成功完成：

```
SiteB::>snapmirror show
```

3. 暫停每個零 RPO 同步關係：

```
SiteB::>snapmirror quiesce -destination-path vs1_dst:vol1

SiteB::>snapmirror quiesce -destination-path vs1_dst:vol2
```

4. 刪除零RPO同步關係：

```
SiteB::>snapmirror delete -destination-path vs1_dst:vol1

SiteB::>snapmirror delete -destination-path vs1_dst:vol2
```

5. 釋放來源 SnapMirror 關係，但保留一般快照：

```
SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol1

SiteA::>snapmirror release -relationship-info-only true -destination-path
vs1_dst:vol2
```

6. 使用 AutomatedFailoverDuplex 原則建立零 RTO SnapMirror 同步關係：

```
SiteB::> snapmirror create -source-path vs1_src:/cg/cg_src -destination-path
vs1_dst:/cg/cg_dst -cg-item-mappings vol1:@vol1,vol2:@vol2 -policy
AutomatedFailoverDuplex
```

7. 如果現有主機是本機的主要叢集、請將主機新增至次要叢集、並建立連線、以各自存取每個叢集。
8. 在次要站台上、刪除與遠端主機相關聯的 igroup 上的 LUN 對應。

   確保 igroup 不包含非複寫 LUN 的對應。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

9. 在主要站台上、修改現有主機的啟動器組態、以設定本機叢集上啟動器的近端路徑。

```
SiteA::> igroup initiator add-proximal-vserver -vserver <svm_name> -initiator
<host> -proximal-vserver <server>
```

10. 為新主機新增一個新的 igroup 和啟動器、並設定主機與本機站台的相似性。Ennable igroup 複寫可複寫組態、並反轉遠端叢集上的主機位置。

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator host2
-proximal-vserver vsB
```

11. 探索主機上的路徑、並驗證主機是否有主動 / 最佳化路徑、可從偏好的叢集前往儲存 LUN
12. 部署應用程式、並將 VM 工作負載分散至叢集。
13. 重新同步一致性群組：

```
SiteB::> snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

14. 重新掃描主機LUN I/O路徑、以還原LUN的所有路徑。

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror靜止"
- "SnapMirror版本"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

轉換**ONTAP SnapMirror**主動同步關係類型

從 ONTAP 9.15.1 開始、您可以在不同類型的 SnapMirror 主動同步保護之間進行轉換：從非對稱到對稱主動 / 主動、反之亦然。

轉換成對稱的主動 / 主動關係

您可以將具有非對稱保護的 iSCSI 或 FC SnapMirror主動同步關係轉換為使用對稱主動/主動。

開始之前

- 兩個叢集都必須執行 ONTAP 9.15.1 或更新版本。
- 對稱的主動 / 主動式組態需要 `AutomatedFailoverDuplex` 保護原則。或者、您也可以 建立自訂 SnapMirror 原則 已提供 `-type` 是 `automated-failover-duplex`。

系統管理員

統一組態的步驟

1. 移除目的地 igroup ：
   a. 在目的地叢集上、瀏覽至 主機 > **SAN** 啟動器群組 。
   b. 選擇帶有 SnapMirror 關係的 igroup ，然後選擇 刪除 。
   c. 在對話方塊中、選擇「 取消對應相關的 **LUN** 」方塊、然後選擇「 ** 刪除」。
2. 編輯 SnapMirror 主動同步關係。
   a. 瀏覽至 保護 > 關係 。
   b. 選擇要修改的關係旁邊的 kabob 菜單，然後選擇 編輯 。
   c. 將 保護原則 修改為 AutomatedFailoverDuplex 。
   d. 選擇 `AutoMatedFailoverDuplex` 提示對話方塊以修改主機鄰近設定。對於啓動器，請選擇適當的選項 啓動器近端 ，然後選擇 保存 。
   e. 選擇 儲存 。
3. 在 保護 功能表中、確認關係顯示為時作業成功 `InSync`。

非統一組態的步驟

1. 移除目的地 igroup ：
   a. 在次要站台上、瀏覽至 主機 > **SAN** 啟動器群組 。
   b. 選擇帶有 SnapMirror 關係的 igroup ，然後選擇 刪除 。
   c. 在對話方塊中、選擇「 取消對應相關的 **LUN** 」方塊、然後選擇「 ** 刪除」。
2. 建立新的 igroup ：
   a. 在目的地站台上的 **SAN** 啟動器群組 功能表中、選取 新增 。
   b. 提供一個 名稱 ，選擇 主機作業系統 ，然後選擇 啟動器群組成員 。
   c. 選擇 儲存 。
3. 將新的 igroup 對應到目的地 LUN 。
   a. 瀏覽至 儲存空間 > **LUN** 。
   b. 選取要對應到 igroup 的所有 LUN 。
   c. 選擇「 更多 」、然後選擇「對應至啟動器群組」 ** 。
4. 編輯 SnapMirror 主動同步關係。
   a. 瀏覽至 保護 > 關係 。
   b. 選擇要修改的關係旁邊的 kabob 菜單，然後選擇 編輯 。
   c. 將 保護原則 修改為 AutomatedFailoverDuplex 。
   d. 選取 AutoMatedFailoverDuplex 會起始修改主機鄰近設定的選項。對於啓動器，請選擇適當的選項 啓動器近端 ，然後選擇 保存 。
   e. 選擇 儲存 。

5. 在 保護 功能表中、確認關係顯示為時作業成功 `InSync`。

CLI

統一組態的步驟

1. 從修改 SnapMirror 原則 `AutomatedFailover` 至 `AutomatedFailoverDuplex`：

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. 修改原則會觸發重新同步。等待重新同步完成、並確認關係是否屬實 `Insync`：

```
snapmirror show -destination-path <destination_path>
```

3. 如果現有主機是本機的主要叢集、請將主機新增至第二個叢集、並建立連線、以各自存取每個叢集。
4. 在次要站台上、刪除與遠端主機相關聯的 igroup 上的 LUN 對應。

> 確保 igroup 不包含非複寫 LUN 的對應。

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
```

5. 在主站台上，將權限等級設為 `advanced`：

```
SiteA::> set -privilege advanced
```

6. 修改現有主機的啟動器組態，以設定本機叢集上啟動器的近端路徑。

```
SiteA::*> igroup initiator add-proximal-vserver -vserver <svm_name>
-initiator <host> -proximal-vserver <server>
```

> 完成此步驟後，您可以將權限等級設回 admin 。

7. 為新主機新增一個新的 igroup 和啟動器、並設定主機與本機站台的相似性。Ennable igroup 複寫可複寫組態、並反轉遠端叢集上的主機位置。

```
SiteA::> igroup modify -vserver vsA -igroup ig1 -replication-peer vsB
SiteA::> igroup initiator add-proximal-vserver -vserver vsA -initiator
host2 -proximal-vserver vsB
```

8. 探索主機上的路徑、並驗證主機是否有主動 / 最佳化路徑、可從偏好的叢集前往儲存 LUN
9. 部署應用程式、並將 VM 工作負載分散至叢集。

非統一組態的步驟

1. 從修改 SnapMirror 原則 `AutomatedFailover` 至 `AutomatedFailoverDuplex`：

```
snapmirror modify -destination-path <destination_path> -policy
AutomatedFailoverDuplex
```

2. 修改原則會觸發重新同步。等待重新同步完成、並確認關係是否屬實 `Insync`：

   ```
   snapmirror show -destination-path <destination_path>
   ```

3. 如果現有主機是主叢集的本機主機、請將該主機新增至第二個叢集、並建立連線能力、以各自存取每個叢集。
4. 在次要站台上、為新主機新增一個新的 igroup 和 initiator 、並設定主機與本機站台的相似性。將 LUN 對應至 igroup 。

   ```
   SiteB::> igroup create -vserver <svm_name> -igroup <igroup>
   SiteB::> igroup add -vserver <svm_name> -igroup <igroup> -initiator
   <host_name>
   SiteB::> lun mapping create -igroup <igroup> -path <path_name>
   ```

5. 探索主機上的路徑、並驗證主機是否有主動 / 最佳化路徑、可從偏好的叢集前往儲存 LUN
6. 部署應用程式、並將 VM 工作負載分散至叢集。

從對稱主動/主動關係轉換為非對稱 **iSCSI** 或 **FC** 關係

如果您已使用 iSCSI 或 FC 配置了對稱主動/主動保護，則可以使用ONTAP CLI 將關係轉換為非對稱保護。

步驟

1. 將所有 VM 工作負載移至來源叢集的本機主機。
2. 移除未管理 VM 執行個體的主機的 igroup 組態，然後修改 igroup 組態以終止 igroup 複寫。

   ```
   igroup modify -vserver <svm_name> -igroup <igroup> -replication-peer -
   ```

3. 在次要站台上、取消對應 LUN 。

   ```
   SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup> -path <>
   ```

4. 在次要站台上、刪除對稱的主動 / 主動關係。

   ```
   SiteB::> snapmirror delete -destination-path <destination_path>
   ```

5. 在主要站台上，釋放對稱的主動 / 主動關係。
   ```
   SiteA::> snapmirror release -destination-path <destination_path> -relationship
   -info-only true
   ```
6. 從次要站台，使用原則建立與同一組磁碟區的關係 `AutomatedFailover`，以重新同步關係。

   ```
   SiteB::> snapmirror create -source-path <source_path> -destination-path
   <destination_path> -cg-item-mappings <source:@destination> -policy
   AutomatedFailover
   SiteB::> snapmirror resync -destination-path vs1:/cg/cg1_dst -policy
   <policy_type>
   ```

重新建立關聯之前，次要站台上的一致性群組需要"待刪除"使用。目的地 Volume "必須轉換為 DP 類型"。若要將磁碟區轉換為 DP ，請使用非原則執行 `snapmirror resync`命令 -`AutomatedFailover： MirrorAndVault， MirrorAllSnapshots`或 `Sync。

7. 確認關係鏡射狀態為 `Snapmirrored` 關係狀態為 `Insync`。

   ```
   snapmirror show -destination-path destination_path
   ```

8. 重新探索主機的路徑。

相關資訊

- "SnapMirror刪除"
- "SnapMirror修改"
- "SnapMirror版本"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

管理 SnapMirror 主動同步並保護資料

在ONTAP一致性組之間建立通用快照

除了定期排程的快照作業之外，您也可以手動在主要 SnapMirror 一致性群組中的磁碟區和次要 SnapMirror 一致性群組中的磁碟區之間建立通用的"Snapshot"資料。

關於這項工作

排程的快照建立時間間隔為 12 小時。

開始之前

- SnapMirror群組關係必須同步。

步驟

1. 建立一般快照：

   ```
   destination::>snapmirror update -destination-path vs1_dst:/cg/cg_dst
   ```

2. 監控更新進度：

   ```
   destination::>snapmirror show -fields newest-snapshot
   ```

相關資訊

- "SnapMirror 顯示"

在SnapMirror主動同步關係中執行ONTAP叢集的計畫故障轉移

在 SnapMirror 主動式同步關係中的 ONTAP 叢集計畫性容錯移轉中、您可以切換主要和次要叢集的角色、讓次要叢集從主要叢集接管。在容錯移轉期間、次要叢集通常會在不中斷

用戶端作業的情況下、於本機處理輸入和輸出要求。

您可能想要執行規劃的容錯移轉、以測試災難恢復組態的健全狀況、或是在主叢集上執行維護。

關於這項工作

計畫性的容錯移轉是由次要叢集的系統管理員啟動。此作業需要切換主要和次要角色、以便次要叢集從主要叢集接管。然後、新的主叢集便可開始在本機處理輸入和輸出要求、而不會中斷用戶端作業。

開始之前

- SnapMirror 主動同步關係必須同步。
- 當不中斷營運進行中時、您無法啟動計畫性的容錯移轉。不中斷營運包括 Volume 搬移、集合重新定位和儲存容錯移轉。
- ONTAP Mediator 必須設定、連線、並且達到仲裁。

步驟

您可以使用 ONTAP CLI 或系統管理員來執行規劃的容錯移轉。

系統管理員

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

1. 在 System Manager 中、選取「 保護」 > 「總覽」 > 「關係」 。
2. 識別您要容錯移轉的 SnapMirror 作用中同步關係。在其名稱旁邊、選取 … 在關係名稱旁、選取「 容錯移轉 」。
3. 若要監控容錯移轉的狀態、請使用 `snapmirror failover show` 在 ONTAP CLI 中。

CLI

1. 從目的地叢集啟動容錯移轉作業：

   ```
   destination::>snapmirror failover start -destination-path
   vs1_dst:/cg/cg_dst
   ```

2. 監控容錯移轉的進度：

   ```
   destination::>snapmirror failover show
   ```

3. 當容錯移轉作業完成時、您可以從目的地監控 SnapMirror 同步保護關係狀態：

   ```
   destination::>snapmirror show
   ```

相關資訊

- "SnapMirror 故障轉移顯示"
- "SnapMirror 故障轉移啟動"
- "SnapMirror 顯示"

當主集群宕機或隔離時，會觸發自動非計劃故障轉移 (AUFO) 操作。ONTAP Mediator 偵測故障轉移發生時，並執行自動非計劃故障轉移到輔助叢集。 此操作只能在ONTAP中介器的協助下執行。輔助集群將轉換為主集群並開始為客戶端提供服務。此作業僅能在 ONTAP Mediator 的協助下執行。

在自動非計畫性容錯移轉之後、重新掃描主機LUN I/O路徑是非常重要的、如此一來、I/O路徑就不會遺失。

在非計畫性容錯移轉之後重新建立保護關係

您可以使用系統管理員或 ONTAP CLI 重新建立保護關係。

系統管理員

步驟

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

1. 導航至*保護>關係*並等待關係狀態顯示“InSync”。
2. 若要恢復原始來源叢集的作業、請按一下 ⋮ 並選取 * 容錯移轉 * 。

CLI

您可以使用監控自動非計畫性容錯移轉的狀態 `snapmirror failover show` 命令。

例如：

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

請參閱 "EMS 參考" 以瞭解事件訊息及修正行動。

在容錯移轉後、恢復風扇輸出組態的保護

從 ONTAP 9.15.1 開始、 SnapMirror 主動式同步可在容錯移轉事件之後、自動在扇出式階段重新設定。非同步扇出腿可以是一致性群組關係，也可以是一種無關的磁碟區關係。如需更多資訊、請參閱 "連出組態"。

如果您使用的是 ONTAP 9.14.1 或更早版本、而且在 SnapMirror 主動同步關係中的次要叢集上發生容錯移轉、SnapMirror 非同步目的地就會變得不正常。您必須刪除和重新建立與 SnapMirror 非同步端點的關係、以手動還原保護。

步驟

1. 確認容錯移轉已成功完成：
   `snapmirror failover show`
2. 在 SnapMirror 非同步端點上、刪除扇出端點：
   `snapmirror delete -destination-path` *`destination_path`*
3. 在第三個站台上、在新的 SnapMirror 主動式同步主磁碟區和非同步扇出目的地磁碟區之間建立 SnapMirror 非同步關係：
   `snapmirror create -source-path` *`source_path`* `-destination-path` *`destination_path`* `-policy MirrorAllSnapshots -schedule` *`schedule`*
4. 重新同步關係：
   `snapmirror resync -destination-path` *`destination_path`*
5. 確認關係狀態和健全狀況：
   `snapmirror show`

相關資訊

- "SnapMirror建立"
- "SnapMirror刪除"
- "SnapMirror 故障轉移顯示"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

監控**ONTAP SnapMirror**主動同步操作

您可以監控下列 SnapMirror 主動式同步作業、以確保 SnapMirror 主動式同步組態的健全狀況：

- 資訊媒體ONTAP
- 計畫性容錯移轉作業
- 自動非計畫性容錯移轉作業
- SnapMirror 主動同步可用度

> 從 ONTAP 9.15.1 開始，系統管理員會顯示任一叢集的 SnapMirror 作用中同步關係狀態。您也可以從系統管理員的任一叢集監控 ONTAP Mediator 的狀態。

資訊媒體**ONTAP**

在正常作業期間、應連接 ONTAP Mediator 狀態。如果它處於任何其他狀態、這可能表示發生錯誤。您可以檢閱 "事件管理系統（EMS）訊息" 以判斷錯誤及適當的修正行動。

計畫性容錯移轉作業

您可以使用監控規劃的容錯移轉作業狀態和進度 `snapmirror failover show` 命令。例如：

```
ClusterB::> snapmirror failover start -destination-path vs1:/cg/dcg1
```

容錯移轉作業完成後、您可以監控來自新目的地叢集的 SnapMirror 保護狀態。例如：

```
ClusterA::> snapmirror show
```

請參閱 "EMS 參考" 以瞭解事件訊息和修正行動。

自動非計畫性容錯移轉作業

在非計畫性自動容錯移轉期間、您可以使用監控作業狀態 `snapmirror failover show` 命令。

```
ClusterB::> snapmirror failover show -instance
Start Time: 9/23/2020 22:03:29
         Source Path: vs1:/cg/scg3
    Destination Path: vs3:/cg/dcg3
     Failover Status: completed
        Error Reason:
            End Time: 9/23/2020 22:03:30
Primary Data Cluster: cluster-2
Last Progress Update: -
       Failover Type: unplanned
  Error Reason codes: -
```

請參閱 "EMS 參考" 以瞭解事件訊息及修正行動。

SnapMirror 主動同步可用度

您可以使用主叢集、次叢集或兩者的一系列命令、檢查 SnapMirror 主動式同步關係的可用性。

您使用的命令包括 `snapmirror mediator show` 用於檢查連線和仲裁狀態的主要和次要叢集命令 `snapmirror show` 命令、和 `volume show` 命令。例如：

```
SMBC_A::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_B           connected         true

SMBC_B::*> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.236.172.86    SMBC_A           connected         true

SMBC_B::*> snapmirror show -expand

Progress
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/cg1 XDP  vs1:/cg/cg1_dp Snapmirrored Insync -         true    -
vs0:vol1    XDP  vs1:vol1_dp  Snapmirrored Insync   -         true    -
2 entries were displayed.

SMBC_A::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1
vserver volume is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------ -------------- ------------------------ --------------
vs0     vol1   true           false                    Consensus

SMBC_B::*> volume show -fields is-smbc-master,smbc-consensus,is-smbc-
failover-capable -volume vol1_dp
vserver volume  is-smbc-master is-smbc-failover-capable smbc-consensus
------- ------- -------------- ------------------------ --------------
vs1     vol1_dp false          true                     No-consensus
```

相關資訊

- "SnapMirror 故障轉移顯示"
- "SnapMirror 故障轉移啟動"
- "SnapMirror 中介顯示"

新增或刪除**ONTAP**一致性群組或刪除卷

隨著應用程式工作負載需求的變更、您可能需要從一致性群組新增或移除磁碟區、以確保營運不中斷。在主動 SnapMirror 主動同步關係中新增和移除磁碟區的程序、取決於您使用

的 ONTAP 版本。

在大多數情況下、這是一項破壞性程序、需要您刪除 SnapMirror 關係、修改一致性群組、然後恢復保護。從 ONTAP 9.13.1 開始、將磁碟區新增至具有主動 SnapMirror 關係的一致性群組、是一項不中斷營運的作業。

關於這項工作

- 在 ONTAP 9.9.1 中、您可以使用 ONTAP CLI 將磁碟區新增或移除至一致性群組。
- 從功能性的9.10.1開始ONTAP 、建議您自行管理 "一致性群組" 透過System Manager或ONTAP 透過靜止API。

  如果您想要新增或移除磁碟區來變更一致性群組的組成、則必須先刪除原始關聯、然後以新的組成方式再次建立一致性群組。

- 從ONTAP 9.13.1 開始，您可以無中斷地從來源或目標新增磁碟區至具有活動SnapMirror關係的一致性群組。 NVMe協定不支援此操作。

  移除磁碟區是一項破壞性作業。在移除磁碟區之前、您必須先刪除 SnapMirror 關係。

ONTAP 9.9.1-9.13.0

開始之前

- 您無法在中開始修改一致性群組 `InSync` 州/省。
- 目的地Volume應為DP類型。
- 您新增以擴充一致性群組的新磁碟區，必須在來源磁碟區和目的地磁碟區之間有一對通用快照。

步驟

兩個磁碟區對應中顯示的範例： `vol_src1 ←→ vol_dst1` 和 `vol_src2 ←→ vol_dst2`、端點之間的一致性群組關係 `vs1_src:/cg/cg_src` 和 `vs1_dst:/cg/cg_dst`。

1. 在來源叢集和目的地叢集上，使用命令驗證來源叢集和目的地叢集之間是否有通用的快照 `snapshot show -vserver *svm_name* -volume *volume_name* -snapshot *snapmirror*`

   ```
   source::>snapshot show -vserver vs1_src -volume vol_src3 -snapshot
   snapmirror*

   destination::>snapshot show -vserver vs1_dst -volume vol_dst3 -snapshot
   snapmirror*
   ```

2. 如果不存在通用快照，請建立並初始化 FlexVol SnapMirror 關係：

   ```
   destination::>snapmirror initialize -source-path vs1_src:vol_src3
   -destination-path vs1_dst:vol_dst3
   ```

3. 刪除一致性群組關係：

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

4. 釋放來源 SnapMirror 關係並保留一般快照：

   ```
   source::>snapmirror release -relationship-info-only true -destination-path
   vs1_dst:vol_dst3
   ```

5. 取消對應LUN並刪除現有的一致性群組關係：

   ```
   destination::>lun mapping delete -vserver vs1_dst -path <lun_path> -igroup
   <igroup_name>
   ```

   ⓘ 目的地LUN會取消對應、而主要複本上的LUN則會繼續為主機I/O提供服務

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst

   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   -relationship-info-only true
   ```

6. 如果您使用的是**ONTAP 9.10.1** 至 **9.13.0**，請刪除來源上的一致性群組，然後重新建立該一致性群組，並使其組成正確。遵循 "刪除一致性群組" 中的步驟，然後按"設定單一一致性群組"。ONTAP必須在系統管理員中或使用ONTAP REST API 執行刪除和建立操作；沒有 CLI 程序。

。如果您使用的是 ONTAP 9.9.1 、請跳至下一個步驟。 **

7. 使用新的組成方式在目的地上建立新的一致性群組：

```
destination::>snapmirror create -source-path vs1_src:/cg/cg_src
-destination-path vs1_dst:/cg/cg_dst -cg-item-mappings vol_src1:@vol_dst1,
vol_src2:@vol_dst2, vol_src3:@vol_dst3
```

8. 重新同步零RTO一致性群組關係、以確保其同步：

```
destination::>snapmirror resync -destination-path vs1_dst:/cg/cg_dst
```

9. 重新對應您在步驟5中未對應的LUN：

```
destination::> lun map -vserver vs1_dst -path lun_path -igroup igroup_name
```

10. 重新掃描主機LUN I/O路徑、以還原LUN的所有路徑。

ONTAP 9.13.1 及更新版本

從 ONTAP 9.13.1 開始，您可以不中斷地將磁碟區新增至具有作用中 SnapMirror 主動式同步關係的一致性群組。SnapMirror 主動同步支援從來源或目的地新增磁碟區。

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

如需從來源一致性群組新增磁碟區的詳細資訊、請參閱 修改一致性群組。

從目的地叢集新增磁碟區

1. 在目標叢集上、選取「 保護 」 > 「 ** 關係」 。
2. 找到您要新增磁碟區的 SnapMirror 組態。選擇然後選擇 展開 。
3. 選取要將其磁碟區新增至一致性群組的磁碟區關係
4. 選擇 展開 。

相關資訊

- "SnapMirror刪除"
- "SnapMirror初始化"
- "SnapMirror版本"
- "SnapMirror 重新同步"

使用**ONTAP SnapMirror**主動同步進行升級與恢復

從 ONTAP 9.9.1 開始支援 SnapMirror 主動同步。根據您要升級或還原的 ONTAP 版本，升級和還原 ONTAP 叢集或控制器會對 SnapMirror 作用中同步關係產生影響。

重新整理叢集

從 ONTAP 9.16.1 開始， SnapMirror 主動式同步支援對稱式雙主動 / 主動式組態中的四節點叢集。您可以使用四節點叢集來升級控制器和儲存設備。

開始之前

- 查看 "四節點叢集的需求"。
- 您可以在技術更新程序期間建立非對稱組態，但在完成重新整理後，您應該回到對稱組態。
- 這些指示適用於現有的四節點組態，其中包含 50 個或更少的一致性群組和 400 個或更少的磁碟區端點。

步驟

1. "將所有 SnapMirror 作用中同步磁碟區移至 _ 單一 _ 高可用度（ HA ）配對"。
2. "從叢集中移除未使用的節點"。
3. "將新節點新增至叢集"。
4. "移動所有磁碟區"進入新節點。
5. "從叢集中移除未使用的節點"然後將它們替換"使用新節點"。

使用 **SnapMirror** 主動同步升級 **ONTAP**

若要使用 SnapMirror 主動式同步、來源叢集和目的地叢集上的所有節點都必須執行 ONTAP 9.9.1 或更新版本。

使用主動式 SnapMirror 主動式同步關係升級 ONTAP 時、您應該使用 自動不中斷升級（ andu ）。使用 andu 可確保 SnapMirror 主動同步關係在升級過程中保持同步且正常。

沒有設定步驟可準備 SnapMirror 主動同步部署以進行 ONTAP 升級。不過、建議您在升級之前和之後、檢查：

- SnapMirror 主動同步關係是同步的。
- 事件日誌中沒有與 SnapMirror 相關的錯誤。
- 這兩個叢集的 Mediator 都在線上且運作正常。
- 所有主機都能正確看到所有路徑以保護 LUN 。

> 當您將叢集從 ONTAP 9.9.1 或 9.9.1 升級至 ONTAP 9.10.1 及更新版本時、 ONTAP 會建立新的叢集 一致性群組 在來源叢集和目的地叢集上、都能使用 System Manager 來設定 SnapMirror 主動式同步關係。

> 。 `snapmirror quiesce` 和 `snampirror resume` SnapMirror 主動同步不支援命令。

從 **ONTAP 9.10.1** 還原至 **ONTAP 9.9.1**

若要將關係從 9.10.1 還原至 9.9.1 、必須刪除 SnapMirror 主動式同步關係、然後刪除 9.10.1 一致性群組執行個體。無法刪除具有作用中 SnapMirror 作用中同步關係的一致性群組。任何先前在9.9.1或更早版本中與另一個Smart Container或Enterprise App相關聯的更新至9.10.1的版次、將不再與還原相關聯。FlexVol刪除一致性群組不會刪除組成磁碟區或磁碟區精細快照。請參閱 "刪除一致性群組" 如需 ONTAP 9.10.1 及更新版本中此工作的詳細資訊、請參閱。

從 **ONTAP 9.9.1** 還原

> 相較於 ONTAP 9.9.1 之前的版本、混合式 ONTAP 叢集不支援 SnapMirror 主動式同步。

當您從 ONTAP 9.9.1 還原至較早版本的 ONTAP 時、您必須注意下列事項：

- 如果叢集主控 SnapMirror 作用中同步目的地、則除非關係中斷並刪除、否則不允許還原至 ONTAP 9.8 或更早版本。
- 如果叢集主控 SnapMirror 作用中同步來源、則在關係解除之前、不允許還原至 ONTAP 9.8 或更早版本。
- 還原至 ONTAP 9.8 或更早版本之前、必須刪除所有使用者建立的自訂 SnapMirror 主動同步原則。

若要符合這些要求、請參閱 "移除 SnapMirror 主動式同步組態"。

步驟

1. 確認您是否準備好還原、從 SnapMirror 主動同步關係中的其中一個叢集輸入下列命令：

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   ```

   下列輸出範例顯示叢集尚未準備好回復、並提供清理指示。

   ```
   cluster::> system node revert-to -version 9.7 -check-only
   Error: command failed: The revert check phase failed. The following
   issues must be resolved before revert can be completed. Bring the data
   LIFs down on running vservers. Command to list the running vservers:
   vserver show -admin-state running Command to list the data LIFs that are
   up: network interface show -role data -status-admin up Command to bring
   all data LIFs down: network interface modify {-role data} -status-admin
   down
   Disable snapshot policies.
       Command to list snapshot policies: "snapshot policy show".
       Command to disable snapshot policies: "snapshot policy modify
   -vserver
      * -enabled false"

      Break off the initialized online data-protection (DP) volumes and
   delete
      Uninitialized online data-protection (DP) volumes present on the
   local
      node.
       Command to list all online data-protection volumes on the local
   node:
      volume show -type DP -state online -node <local-node-name>
       Before breaking off the initialized online data-protection volumes,
      quiesce and abort transfers on associated SnapMirror relationships
   and
      wait for the Relationship Status to be Quiesced.
       Command to quiesce a SnapMirror relationship: snapmirror quiesce
       Command to abort transfers on a SnapMirror relationship: snapmirror
      abort
       Command to see if the Relationship Status of a SnapMirror
   relationship
      is Quiesced: snapmirror show
   ```

```
    Command to break off a data-protection volume: snapmirror break
    Command to break off a data-protection volume which is the
destination
   of a SnapMirror relationship with a policy of type "vault":
snapmirror
   break -delete-snapshots
    Uninitialized data-protection volumes are reported by the
"snapmirror
   break" command when applied on a DP volume.
    Command to delete volume: volume delete

   Delete current version snapshots in advanced privilege level.
    Command to list snapshots: "snapshot show -fs-version 9.9.1"
    Command to delete snapshots: "snapshot prepare-for-revert -node
   <nodename>"

   Delete all user-created policies of the type active-strict-sync-
mirror
   and active-sync-mirror.
   The command to see all active-strict-sync-mirror and active-sync-
mirror
   type policies is:
    snapmirror policy show -type
   active-strict-sync-mirror,active-sync-mirror
   The command to delete a policy is :
    snapmirror policy delete -vserver <SVM-name> -policy <policy-name>
```

2. 一旦您符合還原檢查的要求、請參閱 "還原ONTAP"。

相關資訊

- "網路介面"
- "SnapMirror中斷"
- "SnapMirror 策略刪除"
- "SnapMirror 策略顯示"
- "SnapMirror靜止"
- "SnapMirror 顯示"

刪除**ONTAP SnapMirror**活動同步配置

如果不再需要零 RTO SnapMirror 同步保護、您可以刪除 SnapMirror 主動同步關係。

移除非對稱組態

- 刪除 SnapMirror 主動同步關係之前、必須先取消對應目的地叢集中的所有 LUN 。

- 在LUN未對應且重新掃描主機之後、SCSI目標會通知主機LUN資源清冊已變更。零RTO次要磁碟區上的現有LUN會在零RTO關係刪除後變更、以反映新的身分識別。主機會將次要Volume LUN視為與來源Volume LUN無關的新LUN。
- 在刪除關聯之後、次要磁碟區仍會保留DP磁碟區。您可以核發 `snapmirror break` 將它們轉換為讀取 / 寫入的命令。
- 當關係未反轉時、在容錯移轉狀態中不允許刪除關係。

步驟

1. 從次要叢集移除來源端點與目的地端點之間的 SnapMirror 作用中同步一致性群組關係：

   ```
   destination::>snapmirror delete -destination-path vs1_dst:/cg/cg_dst
   ```

2. 從主叢集中，釋出一致性群組關係，以及為關係建立的快照：

   ```
   source::>snapmirror release -destination-path vs1_dst:/cg/cg_dst
   ```

3. 執行主機重新掃描以更新LUN庫存。
4. 從ONTAP 功能性的9.10.1開始、刪除SnapMirror關係並不會刪除一致性群組。如果您要刪除一致性群組、則必須使用System Manager或ONTAP REST API。請參閱 刪除一致性群組 以取得更多資訊。

刪除 **iSCSI** 或 **FC** 對稱主動/主動配置

您可以使用系統管理員或 ONTAP CLI 移除對稱組態。在這兩個介面中、都有不同的步驟 統一且不一致的組態。

系統管理員

統一組態的步驟

1. 在主要站台上、從 igroup 移除遠端主機並終止複寫。
   a. 瀏覽至 主機 > * SAN 啟動器群組 * 。
   b. 選擇要修改的 igroup ，然後選擇 編輯 。
   c. 移除遠端啟動器並終止 igroup 複寫。選擇 儲存 。
2. 在次要站台上、取消對應 LUN 以刪除複寫的關係。
   a. 瀏覽至 主機 > **SAN** 啟動器群組 。
   b. 選擇帶有 SnapMirror 關係的 igroup ，然後選擇 刪除 。
   c. 在對話方塊中、選擇「 取消對應相關的 **LUN** 」方塊、然後選擇「 ** 刪除」 。
   d. 瀏覽至 保護 > 關係 。
   e. 選擇 SnapMirror 主動同步關係，然後選擇 版本 以刪除關係。

非統一組態的步驟

1. 在主要站台上、從 igroup 移除遠端主機並終止複寫。
   a. 瀏覽至 主機 > * SAN 啟動器群組 * 。
   b. 選擇要修改的 igroup ，然後選擇 編輯 。
   c. 移除遠端啟動器並終止 igroup 複寫。選擇 儲存 。
2. 在次要站台上、移除 SnapMirror 主動同步關係。
   a. 瀏覽至 保護 > 關係 。
   b. 選擇 SnapMirror 主動同步關係，然後選擇 版本 以刪除關係。

CLI

統一組態的步驟

1. 將所有 VM 工作負載移至 SnapMirror 主動式同步的本地主機到來源叢集。
2. 在來源叢集上、從 igroup 移除啟動器、並修改 igroup 組態以終止 igroup 複寫。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -initiator <host2>
SiteA::> igroup modify -vserver <svm_name> -igroup <igroup_name> -os-type
<os_type> -replication-peer "-"
```

3. 在次要站台上、刪除 LUN 對應並移除 igroup 組態：

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 在次要站台上、刪除 SnapMirror 主動同步關係。

```
SiteB::> snapmirror delete -destination-path destination_path
```

5. 在主站點上，從主站點釋放 SnapMirror 主動同步關係。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 重新探索路徑、確認主機只能使用本機路徑。

非統一組態的步驟

1. 將所有 VM 工作負載移至 SnapMirror 主動式同步的本地主機到來源叢集。
2. 在來源叢集上、從 igroup 移除啟動器。

```
SiteA::> igroup remove -vserver <svm_name> -igroup <igroup_name> -initiator
<host2>
```

3. 在次要站台上、刪除 LUN 對應並移除 igroup 組態：

```
SiteB::> lun mapping delete -vserver <svm_name> -igroup <igroup_name> -path
<>
SiteB::> igroup delete -vserver <svm_name> -igroup <igroup_name>
```

4. 在次要站台上、刪除 SnapMirror 主動同步關係。

```
SiteB::> snapmirror delete -destination-path <destination_path>
```

5. 在主站點上，從主站點釋放 SnapMirror 主動同步關係。

```
SiteA::> snapmirror release -destination-path <destination_path>
```

6. 重新探索路徑、確認主機只能使用本機路徑。

刪除 **NVMe** 對稱主動/主動配置

系統管理員

步驟

1. 在來源叢集上，導覽至*保護>複製*。
2. 找到要刪除的關係，選擇⋮並選擇*刪除*。

CLI

1. 從目標叢集中刪除SnapMirror活動同步關係。

   ```
   snapmirror delete -destination-path <destination_path> -unmap-namespace
   true
   ```

   範例：

   ```
   DST::> snapmirror delete -destination-path vs1:/cg/cg_dst_1 -force
   true
   ```

   子系統及其命名空間已從輔助叢集中刪除。

2. 從來源叢集中，從主站點釋放SnapMirror主動同步關係。

   ```
   snapmirror release -destination-path <destination_path>
   ```

   範例：

   ```
   SRC::> snapmirror release -destination-path vs1:/cg/cg_dst_1
   ```

3. 重新探索路徑、確認主機只能使用本機路徑。

相關資訊

- "SnapMirror中斷"
- "SnapMirror刪除"
- "SnapMirror版本"

刪除**ONTAP**調解器或**ONTAP Cloud** 調解器

如果要從ONTAP叢集中刪除現有的ONTAP Mediator 或ONTAP Cloud Mediator 配置，可以使用 `snapmirror mediator remove`命令。例如，您一次只能使用一種類型的 Mediator，因此必須先移除一個實例，然後才能安裝另一個實例。

步驟

您可以透過完成以下步驟之一來刪除ONTAP Mediator 或ONTAP Cloud Mediator。

資訊媒體**ONTAP**

1. 移除ONTAP 此資訊器：

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   範例：

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP雲端調解器

1. 刪除ONTAP Cloud Mediator：

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   範例：

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

相關資訊

- "SnapMirror 中介器刪除"

疑難排解

ONTAP SnapMirror刪除作業在接管狀態下失敗

如果 `snapmirror delete`當SnapMirror活動同步一致性組關係處於接管狀態時，指令失敗。

問題：

在叢集上安裝 ONTAP 9.9.1 時，執行 `snapmirror delete`當 SnapMirror 活動同步一致性群組關係處於接管狀態時，指令失敗。

```
C2_cluster::> snapmirror delete  vs1:/cg/dd

Error: command failed: RPC: Couldn't make connection
```

解決方案

當 SnapMirror 主動同步關係中的節點處於接管狀態時，將「-force」選項設為 true 執行 SnapMirror 刪除和釋放操作。

```
C2_cluster::> snapmirror delete  vs1:/cg/dd -force true

Warning: The relationship between source "vs0:/cg/ss" and destination
         "vs1:/cg/dd" will be deleted, however the items of the
destination
         Consistency Group might not be made writable, deletable, or
modifiable
         after the operation. Manual recovery might be required.
Do you want to continue? {y|n}: y
Operation succeeded: snapmirror delete for the relationship with
destination "vs1:/cg/dd".
```

相關資訊

- "SnapMirror刪除"

建立ONTAP SnapMirror關係和初始化一致性組失敗

如果建立SnapMirror關係和一致性群組初始化失敗，請使用以下資訊。

問題：

建立SnapMirror關係和一致性群組初始化失敗。

解決方案：

確保您未超過每個叢集的一致性群組限制。SnapMirror 主動式同步中的一致性群組限制與平台不相關、且會因 ONTAP 版本而異。請參閱 "物件限制" 以取得 ONTAP 版本的特定指引。

錯誤：

如果一致性群組卡在初始化中、請使用 ONTAP REST API 、系統管理員或命令來檢查一致性群組初始化的狀態 `sn show -expand`。

從ONTAP 9.14.1 到 9.8， SnapMirror主動同步被稱為SnapMirror業務連續性 (SM-BC)。

解決方案：

如果一致性群組無法初始化、請移除 SnapMirror 作用中同步關係、刪除一致性群組、然後重新建立關係並將其初始化。此工作流程視ONTAP 您使用的版本而有所不同。

如果您使用的是 ONTAP 9.9.1	如果您使用ONTAP 的是版本不含更新版本的版本
1. "移除 SnapMirror 主動式同步組態" 2. "建立一致性群組關係、然後初始化一致性群組關係"	1. 在 * 保護 > 關係 * 下、找到一致性群組上的 SnapMirror 作用中同步關係。選擇，然後選擇 * 刪除 * 以刪除 SnapMirror 活動同步關係。 2. "刪除一致性群組" 3. "設定一致性群組"

計劃的**ONTAP**集群故障轉移失敗

如果計劃的故障轉移操作不成功，請使用下列資訊。

問題：

執行之後 `snapmirror failover start` 命令、的輸出 `snapmirror failover show` 命令會顯示一則訊息、表示正在進行不中斷營運。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs1:/cg/cg vs0:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
Failover cannot start because a volume move is running. Retry the command
once volume move has finished.
                                                                  08:35:04
08:35:04
```

原因：

在進行不中斷營運（包括磁碟區移動、集合體重新定位和儲存容錯移轉）時、無法開始計畫性的容錯移轉。

解決方案：

等待不中斷營運完成、然後再次嘗試容錯移轉作業。

相關資訊

- "SnapMirror 故障轉移顯示"
- "SnapMirror 故障轉移啟動"

ONTAP調解器或**ONTAP Cloud** 調解器無法存取或調解器仲裁狀態為 **false**

如果ONTAP調解器或ONTAP Cloud 調解器無法訪問，或調解器仲裁狀態為假，請使用下列資訊。

問題：

執行 `snapmirror failover start`命令，輸出為 `snapmirror failover show`指令會顯示一則訊息，表示ONTAP Mediator 或ONTAP Cloud Mediator 未配置。

看"設定 ONTAP Mediator 和叢集以進行 SnapMirror 主動式同步"或者"為SnapMirror主動同步設定ONTAP Cloud Mediator" 。

```
Cluster1::> snapmirror failover show
Source Destination Error
Path Path Type Status start-time end-time Reason
-------- ----------- -------- --------- ---------- ---------- ----------
vs0:/cg/cg vs1:/cg/cg planned failed 10/1/2020 10/1/2020 SnapMirror
failover cannot start because the source-side precheck failed. reason:
Mediator not configured.
05:50:42 05:50:43
```

原因：

中介器尚未設定、或網路連線問題。

解決方案：

如果未配置 ONTAP 調解器，則必須先配置 ONTAP 調解器，然後才能建立 SnapMirror 活動同步關係。修正任何網路連線問題。使用SnapMirror中介程序show命令、確認來源站台和目的地站台上的協調器已連線且仲裁狀態為true。如需詳細資訊、請參閱 "設定 ONTAP Mediator"。

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.234.10.143    cluster2         connected         true
```

相關資訊

- "SnapMirror 故障轉移顯示"
- "SnapMirror 故障轉移啟動"
- "SnapMirror 中介顯示"

ONTAP Cloud Mediator 可存取但回應緩慢

如果ONTAP Cloud Meditor 發生故障並發生錯誤，提示 ping 延遲高於建議延遲，請使用以下資訊。

問題：

系統管理員：Cloud Mediator 服務可以訪問，但響應緩慢。

CLI：`mediator add`命令失敗並出現錯誤：
`Error: command failed: The ping latency of the BlueXP cloud server is <x> ms which is higher than twice the recommended latency of 200 ms.`

原因：

叢集可能不在NetApp控制台雲端附近，或是存在網路路徑瓶頸。

解決方案：

- 檢查地理位置和與NetApp控制台雲（美國東部）的接近度。

- 優化網路路徑或解決瓶頸。
- 使用網路工具測量往返時間 (RTT)，並將延遲減少到建議的範圍內。
- 使用 HTTP 代理來提高效能。

看"為SnapMirror主動同步配置ONTAP Cloud Mediator 和集群" 。

站台**B**未觸發自動非計畫性容錯移轉

如果站點 A 上的故障不會觸發站點 B 上的非計劃性故障轉移，請使用下列資訊。

問題：

站台A故障不會觸發站台B上的非計畫性容錯移轉

可能原因**#1**：

ONTAP調解器或ONTAP Cloud 調解器未配置。要確定這是否是原因，請發出 `snapmirror mediator show`在網站 B 叢集上執行命令。

```
Cluster2::> snapmirror mediator show
This table is currently empty.
```

此範例表示網站 B 上未配置調解器。

解決方案：

確保兩個叢集上都配置了 Mediator，狀態為已連接，並且仲裁設定為 True。

可能原因 **#2** ：

SnapMirror一致性群組不同步。若要判斷原因是否為此、請檢視事件記錄、以檢視一致性群組在站台發生故障期間是否同步。

```
cluster::> event log show -event *out.of.sync*

Time                Node             Severity      Event
------------------- ---------------- -------------
---------------------------
10/1/2020 23:26:12  sti42-vsim-ucs511w ERROR       sms.status.out.of.sync:
Source volume "vs0:zrto_cg_556844_511u_RW1" and destination volume
"vs1:zrto_cg_556881_511w_DP1" with relationship UUID "55ab7942-03e5-11eb-
ba5a-005056a7dc14" is in "out-of-sync" status due to the following reason:
"Transfer failed."
```

解決方案：

請完成下列步驟、在站台B上執行強制容錯移轉

1. 從站台B取消對應屬於一致性群組的所有LUN

2. 使用刪除 SnapMirror 一致性群組關係 `force` 選項。
3. 輸入 `snapmirror break` 針對一致性群組組成磁碟區執行命令、將磁碟區從 DP 轉換為 R/W 、以啟用站台 B 的 I/O
4. 啟動站台A節點、以建立從站台B到站台A的零RTO關係
5. 使用站台 A 釋放一致性群組 `relationship-info-only`，以保留通用快照，並取消對應屬於一致性群組的 LUN 。
6. 使用同步原則或非同步原則設定磁碟區層級關係、將站台A上的磁碟區從右/右轉換為DP。
7. 發行 `snapmirror resync` 以同步處理關聯。
8. 刪除與站台A上同步原則的SnapMirror關係
9. 使用同步原則來釋放 SnapMirror 關係 `relationship-info-only true` 現場 B...
10. 建立站台B與站台A之間的一致性群組關係
11. 從站台A重新同步一致性群組、然後驗證一致性群組是否同步。
12. 重新掃描主機LUN I/O路徑、以還原LUN的所有路徑。

相關資訊

- "SnapMirror中斷"
- "SnapMirror 中介顯示"
- "SnapMirror 重新同步"

站點 **B** 與**ONTAP**調解器之間的連結以及站點 **A** 之間的連結均發生故障

若要檢查ONTAP調解器或ONTAP Cloud 調解器的連接，請使用 `snapmirror mediator show`命令。如果連線狀態為“不可達”，且網站 B 無法存取網站 A，您將看到類似以下的輸出。請依照解決方案中的步驟恢復連接

範例：

使用ONTAP Cloud Mediator 輸出“snapmirror mediator show”指令：

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster    Connection Status Quorum Status Type
---------------- ---------------- ----------------- ------------- -------
0.0.0.0          C1_cluster       unreachable       true          cloud
```

使用ONTAP Mediator 輸出“snapmirror mediator show”指令：

```
cluster::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
10.237.86.17     C1_cluster       unreachable       true
SnapMirror consistency group relationship status is out of sync.

C2_cluster::> snapmirror show -expand
Source            Destination Mirror  Relationship   Total
Last
Path        Type  Path        State   Status         Progress  Healthy
Updated
----------- ---- ------------ ------- -------------- --------- -------
--------
vs0:/cg/src_cg_1 XDP vs1:/cg/dst_cg_1 Snapmirrored OutOfSync - false   -
vs0:zrto_cg_655724_188a_RW1 XDP vs1:zrto_cg_655755_188c_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655733_188a_RW2 XDP vs1:zrto_cg_655762_188c_DP2 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655739_188b_RW1 XDP vs1:zrto_cg_655768_188d_DP1 Snapmirrored
OutOfSync - false -
vs0:zrto_cg_655748_188b_RW2 XDP vs1:zrto_cg_655776_188d_DP2 Snapmirrored
OutOfSync - false -
5 entries were displayed.

Site B cluster is unable to reach Site A.
C2_cluster::> cluster peer show
Peer Cluster Name         Cluster Serial Number Availability
Authentication
------------------------- --------------------- --------------
--------------
C1_cluster            1-80-000011           Unavailable    ok
```

解決方案

強制容錯移轉以啟用站台B的I/O、然後建立從站台B到站台A的零RTO關係請完成下列步驟、在站台B上執行強制容錯移轉

1. 從網站 B 取消對應屬於一致性群組的所有 LUN。這將會失敗，因此您必須先修改 igroup 以刪除複製對等 SVM，然後再刪除 LUN 對應。

範例：

```
C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_1                        igroup1       0
mixed
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
2 entries were displayed.

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_5 -igroup igroup1
Error: command failed: The peer cluster is unreachable and a SnapMirror
       Mediator is not configured. The configuration is locked for
replicated
       objects in this Vserver peer relationship on both clusters. The
only
       supported configuration change is to manually disable replication
on
       both sides of the relationship, after which configuration changes
are
       supported.
C1_cluster::> igroup modify -igroup igroup1 -replication-peer -

C1_cluster::> lun mapping delete -path /vol/cg1_lun/lun_1 -igroup igroup1

C1_cluster::> lun mapping show
Vserver    Path                                      Igroup   LUN ID
Protocol
---------- ----------------------------------------  -------  ------
--------
vs0        /vol/cg1_lun/lun_2                        igroup1       1
mixed
1 entries were displayed.
```

1. 使用force選項刪除SnapMirror一致性群組關係。
2. 輸入 SnapMirror Break 命令 (`snapmirror break -destination_path` *svm*`:_volume_`）在一致性群組組成的磁碟區上、將磁碟區從 DP 轉換為 RW 、以從站台 B 啟用 I/O

   您必須針對一致性群組中的每個關係發出 SnapMirror 中斷命令。例如、如果一致性群組中有三個磁碟區、您就會針對每個磁碟區發出命令。

3. 啟動站台A節點、以建立從站台B到站台A的零RTO關係
4. 在站台 A 上以僅限關係資訊來釋放一致性群組，以保留通用快照，並取消對應屬於一致性群組的 LUN 。
5. 使用同步原則或非同步原則設定磁碟區層級關係、將站台A上的磁碟區從RW轉換為DP。

6. 發行 `snapmirror resync` 同步關係的命令。
7. 刪除站台A上的SnapMirror與同步原則的關係
8. 在站台B上使用僅限關係資訊的true、以Sync原則釋放SnapMirror關係
9. 在站台 B 與站台 A 之間建立一致性群組關係
10. 從來源叢集重新同步一致性群組。驗證一致性群組狀態是否同步。
11. 重新掃描主機 LUN I/O 路徑、以還原 LUN 的所有路徑。

相關資訊

- "SnapMirror中斷"
- "SnapMirror 中介顯示"
- "SnapMirror 重新同步"
- "SnapMirror 顯示"

站點 **A** 與**ONTAP**調解器之間的連結以及站點 **B** 之間的連結均發生故障

使用 SnapMirror 主動式同步時、您可能會失去 ONTAP Mediator 或對等叢集之間的連線能力。您可以檢查 SnapMirror 主動同步關係不同部分的連線、可用度和共識狀態、然後強制恢復連線、藉此診斷問題。

要檢查的項目	**CLI** 命令	指標
站台A的中介者	`snapmirror mediator show`	連線狀態會顯示為 `unreachable`
站台B連線能力	`cluster peer show`	可用度顯示為 `unavailable`
SnapMirror 主動式同步 Volume 的一致狀態	`volume show` *`volume_name`* `-fields smbc-consensus`	。`sm-bc consensus` 欄位隨即顯示 `Awaiting-consensus`

有關診斷和解決此問題的更多信息，請參閱"NetApp知識庫：使用SnapMirror主動同步時，網站 A 與調解器之間的連結以及網站 B 之間的連結發生故障"。

相關資訊

- "集群對等顯示"
- "SnapMirror 中介顯示"

在目標磁碟區上設定隔離時， **ONTAP SnapMirror**刪除操作失敗

如果任何目標磁碟區設定了重定向防護，而SnapMirror刪除操作失敗，請使用下列資訊。

問題：

當任何目的地磁碟區設定了重新導向Fence時、SnapMirror刪除作業都會失敗。

解決方案

執行下列作業以重試重新導向、並從目的地磁碟區移除Fence。

- SnapMirror重新同步

- SnapMirror更新

當**ONTAP**主伺服器關閉時，磁碟區移動操作會卡住

如果當主站點在SnapMirror主動同步關係中關閉時，磁碟區移動操作會無限期地停留在切換延遲狀態，請使用下列資訊。

問題：

當主站點處於 SnapMirror 活動同步關係中時，卷移動操作將無限期地停留在轉換延遲狀態。
當主要站台當機時、次要站台會執行自動非計畫性容錯移轉（AUFO）。當磁碟區移動作業正在進行時、當AUFO觸發時、磁碟區移動就會卡住。

解決方案：

中止卡住的Volume Move執行個體、然後重新啟動Volume Move作業。

無法刪除快照時， **ONTAP SnapMirror**版本失敗

如果無法刪除快照時SnapMirror發布操作失敗，請使用下列資訊。

問題：

無法刪除快照時， SnapMirror 版本作業會失敗。

解決方案：

快照包含暫態標記。使用 `snapshot delete`帶選項的命令 `-ignore-owners`來移除暫態快照。
`snapshot delete -volume <volume_name> -snapshot <snapshot_name> -ignore-owners true -force true`

重試 `snapmirror release` 命令。

相關資訊

- "SnapMirror版本"

磁碟區移動參考快照顯示為**ONTAP SnapMirror**關係的最新快照

如果磁碟區移動參考快照在磁碟區移動操作後顯示為SnapMirror關係的最新快照，請使用下列資訊。

問題：

在一致性群組磁碟區上執行磁碟區移動作業之後，磁碟區移動參考快照可能會錯誤地顯示為 SnapMirror 關係的最新資料。

您可以使用下列命令來檢視最新的快照：

```
snapmirror show -fields newest-snapshot status -expand
```

解決方案：

手動執行 `snapmirror resync` 或是在磁碟區移動作業完成後、等待下一次自動重新同步作業。

相關資訊

- "SnapMirror 重新同步"
- "SnapMirror 顯示"

適用於 MetroCluster 和 SnapMirror 主動同步的 ONTAP 調解器

瞭解 ONTAP Mediator

本文檔指的是ONTAP Mediator 的本機版本。有關ONTAP Cloud Mediator（從ONTAP 9.17.1 開始提供）的信息，請參閱"SnapMirror主動同步文檔" 。

ONTAP 調解器為 ONTAP 功能提供了多種功能：

- 為 HA 中繼資料提供持續且有圍籬的儲存區。
- 做為 ping Proxy 、以實現控制器的活力。
- 提供同步節點健全狀況查詢功能、以協助仲裁判斷。

ONTAP 調解器提供兩項額外的 systemctl 服務：

- **`ontap_mediator.service`**

  維護用於管理 ONTAP 關係的 REST API 伺服器。

- **`mediator-scst.service`**

  控制 iSCSI 模組（ SCST ）的啟動和關閉。

提供給系統管理員的工具

提供給系統管理員的工具：

- **`/usr/local/bin/mediator_change_password`**

  提供目前 API 使用者名稱和密碼時、請設定新的 API 密碼。

- **`/usr/local/bin/mediator_change_user`**

  提供目前 API 使用者名稱和密碼時、請設定新的 API 使用者名稱。

- **`/usr/local/bin/mediator_generate_support_bundle`**

  產生本機的 tmz 檔案、其中包含與 NetApp 客戶支援部門通訊所需的所有實用支援資訊。 這包括應用程式組態、記錄和一些系統資訊。 套件會在本機磁碟上產生、並可視需要手動傳輸。 儲存位置：/opt/NetApp/data/support_bundles/

- **`/usr/local/bin/uninstall_ontap_mediator`**

  移除 ONTAP Mediator 套件和 SCST 核心模組。這包括所有組態、記錄和信箱資料。

- **`/usr/local/bin/mediator_unlock_user`**

如果達到驗證重試限制、就會釋放 API 使用者帳戶的鎖定。此功能用於防止暴力密碼推導。它會提示使用者輸入正確的使用者名稱和密碼。

- **`/usr/local/bin/mediator_add_user`**

  （僅支援）用於在安裝時新增 API 使用者。

特別注意事項

ONTAP Mediator 仰賴 SCST 來提供 iSCSI （請參閱 http://scst.sourceforge.net/index.html）。此套件是專為核心而在安裝期間編譯的核心模組。任何核心更新都可能需要重新安裝 SCST 。或者，解除安裝然後重新安裝 ONTAP Mediator，然後重新配置 ONTAP 關係。

伺服器作業系統核心的任何更新都應與 ONTAP 中的維護時段協調。

ONTAP Mediator 的新功能

每個版本都提供了 ONTAP Mediator 的新增強功能。最新功能。

增強功能

如需 SCST 版本資訊，請參閱SCST 支援對照表。

ONTAP Mediator 版本	增強功能
1.11	• 支援 RHEL ： ◦ 相容：9.5。 ◦ 推薦：10.1、10.0、9.7、9.6、9.4 和 8.10。 • 支援 Rocky Linux 10.1、9.7 和 8.10。 • 支援 Oracle Linux 10.0 和 9.6。 • 為MetroCluster IP 配置新增對 IPv6 的支援。 • 新增了對 fapolicyd 的支援。
1.10	• 支援 RHEL ： ◦ 相容：9.5。 ◦ 建議：10.0、9.6、9.4 和 8.10。 • 支援 Rocky Linux 10.0、9.6 和 8.10。 • 將 Python 基礎版本從 Python 3.9 升級到 Python 3.12。

1.9.1	• 支援 RHEL ： ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4。 ◦ 建議：9.5、9.4、9.2、9.0、8.10 和 8.8。 • 支援 Rocky Linux 9.5 和 8.10。 • 新增用於程式碼簽署驗證的憑證。 • 增加了使用以下方式跳過程式碼簽署檢查的支持 `-skip-code-signature-check` 旗幟。 • 安裝程式在偵測到過期代碼簽署憑證時會顯示警告。
1.9	• 支援 RHEL ： ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4。 ◦ 建議：9.5、9.4、9.2、9.0、8.10 和 8.8。 • 支援 Rocky Linux 9.5 和 8.10。 • 支援 RHEL 和 Rocky Linux 的 FIPS 。 • 新增效能增強功能，可擴充性更高。 • 改善檔案名稱以簡化 PKI 簽署憑證的設定。
1.8	• 支援 RHEL ： ◦ 相容：8.7、8.6、8.5 和 8.4。 ◦ 建議：9.4、9.3、9.2、9.1、9.0、8.10、8.9 和 8.8。 • 支援 Rocky Linux 9.4 和 8.10。
1.1.7	• 支援 RHEL ： ◦ 相容：8.7、8.6、8.5 和 8.4。 ◦ 推薦：9.3、9.2、9.1、9.0、8.9 和 8.8。 • 支援 Rocky Linux 9.3 和 8.9。 • 支援自我簽署憑證和協力廠商簽署憑證中的 SAN （主體替代名稱）資料。
1.6.	• Python 3.9 更新。 • 支援 RHEL ： ◦ 相容：8.7、8.6、8.5 和 8.4。 ◦ 建議：9.2、9.1、9.0 和 8.8。 • 支援 Rocky Linux 9.2 和 8.8。 • 不再支援 RHEL 7.x / CentOS 所有版本。

1.5.	• 支援 RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 和 7.6。 • 支援 CentOS 7.9、7.8、7.7 和 7.6。 • 包括 RHEL 7.x / CentOS 7.x 的過時警告 • 優化大型 SnapMirror 主動同步系統的速度。 • 安裝程式中新增了加密代碼簽章。
1.4.	• 支援 RHEL 8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 和 7.6。 • 支援 CentOS 7.9、7.8、7.7 和 7.6。 • 新增對 UFEI 型韌體安全開機（ SB ）的支援。
1.3.	• 支援 RHEL 8.3、8.2、8.1、8.0、7.9、7.8、7.7 和 7.6。 • 支援 CentOS 7.9、7.8、7.7 和 7.6。
1.2.	• 支援 RHEL 8.1、8.0、7.9、7.8、7.7 和 7.6。 • 支援 CentOS 7.9、7.8、7.7 和 7.6。 • 支援 HTTPS 信箱。 • 適用於 ONTAP 9.8+ MCC-IP AUSO 和 SnapMirror 主動同步 ZRTO 。
1.1.	• 支援 RHEL 8.0 和 7.6。 • 支援 CentOS 7.6 。 • 消除 Perl 的相依性。
1.0	• 支援 iSCSI 信箱。 • 適用於 ONTAP 9.7+ MCC-IP AUSO 。 • 支援 RHEL/CentOS 7.6 。

作業系統支援對照表

適用於 ONTAP Mediator 的作業系統	1.11	1.10	1.9.1	1.9	1.8	1.1.7	1.6.	1.5.	1.4.	1.3.	1.2.	1.1.	1.0
RHEL 10.1	是的	否	否	否	否	否	否	否	否	否	否	否	否
RHEL 10.0	是的	是的	是的	否	否	否	否	否	否	否	否	否	否

RHEL 9.7	是的	否	否	否	否	否	否	否	否	否	否	否	否
RHEL 9.6	是的	是的	是的	否	否	否	否	否	否	否	否	否	否
RHEL 9.5	相容	相容	是的	是的	否	否	否	否	否	否	否	否	否
RHEL 9.4	是的	是的	是的	是的	是的	否	否	否	否	否	否	否	否
RHEL 9.3	否	否	相容	相容	是的	是的	否	否	否	否	否	否	否
RHEL 9.2	否	否	是的	是的	是的	是的	是的	否	否	否	否	否	否
RHEL 9.1	否	否	相容	相容	是的	是的	是的	否	否	否	否	否	否
RHEL 9.0	否	否	是的	是的	是的	是的	是的	否	否	否	否	否	否
RHEL 8.10.	是的	是的	是的	是的	是的	否	否	否	否	否	否	否	否
RHEL 8.9	否	否	相容	相容	是的	是的	否	否	否	否	否	否	否
RHEL 8.8	否	否	是的	是的	是的	是的	是的	否	否	否	否	否	否
RHEL 8.7	否	否	相容	相容	是的	是的	是的	否	否	否	否	否	否
RHEL 8.6	否	否	相容	相容	是的	是的	是的	否	否	否	否	否	否
RHEL 8.5	否	否	相容	相容	是的	是的	是的	是的	是的	否	否	否	否
RHEL 8.4	否	否	相容	相容	是的	是的	是的	是的	是的	否	否	否	否
RHEL 8.3	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	否	否	否

RHEL 8.2	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	否	否	否
RHEL 8.1	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	是的	否	否
RHEL 8.0	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	是的	是的	否
RHEL 和 CentOS 7.9	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	相容	否	否
RHEL 和 CentOS 7.8	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	是的	否	否
RHEL 和 CentOS 7.7	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	是的	否	否
RHEL 和 CentOS 7.6	過時	過時	過時	過時	過時	過時	過時	是的	是的	是的	是的	是的	有（僅限 RHEL）
CentOS 8 和串流	否	否	否	否	否	否	否	否	否	否	不適用	不適用	不適用
Rocky Linux 10.0	是的	是的	否	否	否	否	否	否	否	否	否	否	否
Rocky Linux 9	是的	是的	是的	是的	是的	是的	是的	不適用	不適用	不適用	不適用	不適用	不適用
Rocky Linux 8	是的	是的	是的	是的	是的	是的	是的	不適用	不適用	不適用	不適用	不適用	不適用

Oracle Linux 10.0	是的	否	否	否	否	否	否	否	否	否	否	否	否
Oracle Linux 9	是的	否	否	否	否	否	否	否	否	否	否	否	否

- 「是」表示建議將作業系統用於 ONTAP Mediator 安裝，而且完全相容且受支援。
- 「否」表示作業系統和 ONTAP Mediator 不相容。
- 「相容」意味著 Red Hat 不再支援這些 RHEL 版本，但仍可在這些版本上安裝ONTAP Mediator。
- ONTAP Mediator 1.6 增加了對 Rocky Linux 9 和 8 的支援。
- ONTAP Mediator 1.5 是 RHEL 7.x 分支作業系統最後支援的版本。
- 所有版本的 CentOS 8 都因為重新建立分支而移除。CentOS Stream 被視為不適合的正式作業目標作業系統。沒有計畫支援。

SCST 支援對照表

下表顯示每個 ONTAP Mediator 版本支援的 SCST 版本。

ONTAP Mediator 版本	支援 **SCST** 的支援版本
ONTAP調解器 1.11	scst-3.9.tar.gz
ONTAP調解器 1.10	scst-3.9.tar.gz
ONTAP調解器 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.2	scst-3.4.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

安裝或升級

ONTAP 調解器安裝工作流程摘要

安裝 ONTAP Mediator 包括安裝準備、提供儲存庫存取權限、下載安裝套件、驗證程式碼簽署、安裝 ONTAP Mediator 套件以及執行安裝後設定任務。

"準備安裝或升級 **ONTAP** 調解器"

若要安裝或升級 ONTAP Mediator，您必須確保滿足所有先決條件。

"升級主機作業系統和 **Mediator**"

如果您要升級現有版本的 ONTAP Mediator，則必須先解除安裝舊版本，然後再安裝新版本。如果您是首次安裝 ONTAP Mediator，則可以跳過此步驟。

"提供存儲庫訪問"

您應該啟用對儲存庫的訪問，以便 ONTAP Mediator 可以在安裝過程中存取所需的軟體包。

"下載 **ONTAP Mediator** 安裝套件"

從 ONTAP Mediator 下載頁面下載 ONTAP Mediator 安裝套件。

"驗證 **ONTAP** 調解器安裝套件的程式碼簽名"

NetApp 建議在安裝 ONTAP Mediator 安裝套件之前驗證 ONTAP Mediator 程式碼簽署。

"安裝 **ONTAP** 調解器"

若要安裝 ONTAP Mediator，您必須取得安裝套件並在主機上執行安裝程式。

"驗證 **ONTAP** 調解器安裝"

安裝 ONTAP Mediator 後，請驗證它是否成功運作。

"執行安裝後配置任務"

安裝並執行 ONTAP Mediator 後，必須執行其他設定任務才能使用 ONTAP Mediator 功能。

安裝或升級**ONTAP Mediator**

要安裝或升級ONTAP Mediator，您需要滿足所有先決條件，下載安裝包，並在主機上執行安裝程式。

- 從 ONTAP 9.8 開始、您可以使用任何版本的 ONTAP Mediator 來監控 SnapMirror 主動式同步關係。

- 您可以使用任何版本的ONTAP Mediator 來監控MetroCluster IP 設定。

安裝與升級考量

在升級或安裝ONTAP Mediator 之前，請先查看以下幾點。

> ONTAP Mediator 1.8 及更早版本與 Red Hat Enterprise Linux (RHEL) FIPS 模式不相容，導致無法成功安裝。您可以使用以下命令檢查是否啟用了 FIPS 模式： `fips-mode-setup --check`命令。您可以使用以下方法停用 FIPS 模式： `fips-modesetup --disable`命令。停用 FIPS 模式後重新啟動以成功安裝ONTAP Mediator 1.8 或更早版本。

- 您應該將ONTAP Mediator 升級到最新版本。舊版仍然可以與所有ONTAP版本相容，但新版本包含針對第三方元件的安全性修補程式。
- 當您升級至新的 ONTAP Mediator 版本時，除非有更高版本，否則安裝程式會自動升級至建議的 SCST 版本。如需手動安裝較高 SCST 版本的說明，請參閱"管理 ONTAP Mediator"。如需支援的版本，請參閱"SCST 支援對照表"。

> - 如果安裝失敗，您可能需要升級至更新版本的ONTAP Mediator。
> - 自 2025 年 6 月 15 日起，您無法安裝或升級ONTAP Mediator 1.9 和 1.8，因為它們的代碼簽署憑證已過期。如果安裝或升級失敗，請改用ONTAP Mediator 1.9.1 修補程式版本。

- 如果您安裝 `yum-utils` 套件中、您可以使用 `needs-restarting` 命令。
- 從ONTAP Mediator 1.11 開始， MetroCluster IP 設定支援 IPv6。

主機需求

安裝 RHEL 或 Rocky Linux 並配置相關儲存庫時，請遵循這些要求。

> 如果您修改安裝或組態程序，可能需要執行其他步驟。

Linux 發佈要求

- 按照紅帽最佳實務安裝 RHEL 或 Rocky Linux。由於 CentOS 8.x 已停止維護，因此不建議使用與 CentOS 8.x 相容的版本。
- 安裝 ONTAP Mediator 時，請確保系統可以存取所需的儲存庫，以便安裝程式可以擷取並安裝所有必要的軟體相依性。
- 若要讓 yum 安裝程式在 RHEL 儲存庫中尋找相關軟體，請在安裝期間或之後使用有效的 Red Hat 訂閱來登錄系統。

> 如需詳細資訊，請參閱 Red Hat Subscription Manager 文件。

網路需求

請確定下列連接埠可供 ONTAP Mediator 使用且未使用：

連接埠/服務	來源	方向	目的地	目的

22/TCP	管理主機	傳入	資訊媒體ONTAP	（選用） SSH / ONTAP Mediator 管理
31784/TCP	叢集管理生命	傳入	資訊媒體伺服器ONTAP	（必填） REST API （ HTTPS ）
3260/TCP [1]	節點資料生命或節點管理生命	雙向	支援iSCSI目標ONTAP	（ MetroCluster IP 設定必需）信箱的 iSCSI 資料連接

對於 SMBC 客戶， ONTAP 不需要啟用或連線連接埠 3260 。

- 如果使用第三方防火牆，請參閱"防火牆需求ONTAP"。
- 對於無法存取網際網路的 Linux 主機，請確定所需的套件可在本機儲存庫中使用。

  如果您在 Linux 環境中使用鏈路聚合控制協議（ LACP ），請配置內核並將設置 `sysctl net.ipv4.conf.all.arp_ignore`爲 `2。

作業系統需求

您的作業系統必須符合下列需求：

- 64位元實體安裝或虛擬機器
- 8 GB RAM
- 1 GB 磁碟空間（用於應用程式安裝、伺服器記錄檔和資料庫）
- 使用者：root存取權

下表顯示每個版本的 ONTAP Mediator 所支援的作業系統。

ONTAP Mediator 版本	支援的Linux版本
1.11	• Red Hat Enterprise Linux ◦ 相容：9.5 [1] ◦ 推薦：10.1、10.0、9.7、9.6、9.4 和 8.10 • Rocky Linux 10.1、9.7 和 8.10 • Oracle Linux 10.0 和 9.6
1.10	• Red Hat Enterprise Linux ◦ 相容：9.5 [1] ◦ 建議：10.0、9.6、9.4 和 8.10 • Rocky Linux 10.0、9.6 和 8.10

1.9.1	• Red Hat Enterprise Linux ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.5、9.4、9.2、9.0、8.10 和 8.8 • Rocky Linux 9.5 和 8.10
1.9	• Red Hat Enterprise Linux ◦ 相容：9.3、9.1、8.9、8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.5、9.4、9.2、9.0、8.10 和 8.8 • Rocky Linux 9.5 和 8.10
1.8	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.4、9.3、9.2、9.1、9.0、8.10、8.9 和 8.8 • Rocky Linux 9.4 和 8.10
1.1.7	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 推薦：9.3、9.2、9.1、9.0、8.9 和 8.8 • Rocky Linux 9.3 和 8.9
1.6.	• 紅帽企業 Linux： ◦ 相容：8.7、8.6、8.5 和 8.4 [1] ◦ 建議：9.2、9.1、9.0 和 8.8 • Rocky Linux 9.2 和 8.8
1.5.	• Red Hat Enterprise Linux：8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.4.	• Red Hat Enterprise Linux：8.5、8.4、8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.3.	• Red Hat Enterprise Linux：8.3、8.2、8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6
1.2.	• Red Hat Enterprise Linux：8.1、8.0、7.9、7.8、7.7 與 7.6 • CentOS：7.9、7.8、7.7 和 7.6

1. 相容意味著 Red Hat 不再支援這些 RHEL 版本，但仍可在這些版本上安裝ONTAP Mediator。

作業系統所需的套件

ONTAP 調解器需要以下軟體包：

這些套件是由 ONTAP Mediator 安裝程式預先安裝或自動安裝。

所有RHEL/CentOS版本	RHEL 10.x / Rocky Linux 10 的附加軟體包	RHEL 9.x / Rocky Linux 9 的其他套件	適用於 RHEL 8.x / Rocky Linux 8 的其他套件
• OpenSSL • OpenSSL • kernel-devel-$ （ uname -r ） • 海灣合作委員會 • 製造 • libselinux-utils • 修補程式 • bzip2. • Perl-Data-Dumper • Perl-ExtUtils-MakeMaker.. • efibootmgr • mokutil	• python3.12 • python3.12-devel	• elfutils-libelf-devel • policycoreutils-python 公用程式 • python3. • python3-devel	• elfutils-libelf-devel • policycoreutils-python 公用程式 • RedHat-lsb核心 • python39. • python39-devel

該媒體夾安裝套件是一個自我解壓縮的tar檔案、其中包括：

- 一種RPM檔案、內含無法從支援版本儲存庫取得的所有相依性。
- 安裝指令碼。

建議使用有效的SSL憑證。

作業系統升級考量與核心相容性

- 您可以更新除核心之外的所有函式庫軟體包，但您可能需要重新啟動才能使ONTAP Mediator 中的變更生效。如果需要重啟，請安排停機時間。
- 你應該保持作業系統核心處於最新狀態。將核心核心升級到清單中列出的支援版本。"ONTAP Mediator 版本對照表" 。您必須重新啟動系統，因此請為此停機維護安排一個時段。
  - 重啟前卸載 SCST 核心模組，重啟後再重新安裝。
  - 在開始核心作業系統升級之前，請準備好受支援的 SCST 版本進行重新安裝。

- 核心版本必須符合作業系統版本。
- 請勿將核心升級至ONTAP Mediator 版本支援的作業系統版本以上，因為測試過的 SCST 模組可能無法正常運作。

啟用 **UEFI** 安全開機時，請安裝 **ONTAP Mediator**

ONTAP Mediator 可以安裝在啟用或不啟用 UEFI 安全開機的系統上。

關於這項工作

如果不需要 UEFI 安全開機，或者您正在疑難排解 ONTAP Mediator 安裝問題，您可以選擇在安裝 ONTAP Mediator 之前先停用 UEFI 安全開機。從您的機器設定停用 UEFI 安全開機選項。

如需停用 UEFI 安全開機的詳細指示，請參閱主機作業系統的文件。

若要安裝啟用了 UEFI 安全啟動的 ONTAP Mediator，您必須先註冊安全金鑰，然後服務才能啟動。金鑰是在 SCST 安裝的編譯步驟期間產生，並儲存為您機器上的私密公開金鑰配對。使用 `mokutil`公用程式將公開金鑰新增為電腦擁有者金鑰（ Mok ）至 UEFI 韌體，讓系統信任並載入簽署的模組。請將複雜密碼儲存 `mokutil`在安全的位置，因為重新啟動系統以啟動莫克語時，需要這樣做。

步驟

1. [[step 1 _UEFI] 檢查系統上是否已啟用 UEFI 安全開機：

```
mokutil --sb-state
```

結果會指出此系統上是否已啟用 UEFI 安全開機。

如果…	前往…
已啟用 UEFI 安全開機	
停用 UEFI 安全開機	"升級主機作業系統，然後升級 ONTAP Mediator"

- 系統會提示您建立必須儲存在安全位置的複雜密碼。您需要使用此密碼來啟用 UEFI Boot Manager 中的金鑰。
- ONTAP Mediator 1.2.0 及更早版本不支援此模式。

2. 如果 `mokutil`未安裝公用程式，請執行下列命令：

```
yum install mokutil
```

升級主機作業系統和 **ONTAP Mediator**

若要將主機作業系統 for ONTAP Mediator 升級至更新版本、您必須先解除安裝 ONTAP Mediator 。

關於這項工作

使用 leapp-upgrade 工具升級ONTAP Mediator 的主機作業系統前，請先解除安裝ONTAP Mediator。此工具會

檢查已註冊倉庫中是否有新的 RPM 版本。

ONTAP Mediator 安裝程式會安裝一個 .rpm 文件，leapp-upgrade 工具會將其包含在搜尋範圍內。由於安裝程式會解壓縮文件而不是從註冊的儲存庫下載文件，因此該工具找不到升級程式。您必須使用 leapp-upgrade 工具卸載該軟體包。

步驟

1. 備份日誌檔：

```
[rootmediator-host ~]# tar -czf ontap_mediator_file_backup.tgz -C
/opt/netapp/lib/ontap_mediator ./log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]# tar -tf ontap_mediator_file_backup.tgz
./log/
./log/ontap_mediator.log
./log/scstadmin.log
./log/ontap_mediator_stdout.log
./log/ontap_mediator_requests.log
./log/install_20230419134611.log
./log/scst.log
./log/ontap_mediator_syslog.log
./ontap_mediator/server_config/ontap_mediator.user_config.yaml
[rootmediator-host ~]#
```

2. 使用 leapp-upgrade 工具執行升級：

```
[rootmediator-host ~]# leapp preupgrade --target 8.4
  ..<snip upgrade checks>..
  ..<fix issues found>..
[rootmediator-host ~]# leapp upgrade --target 8.4
  ..<snip upgrade>..
[rootmediator-host ~]# cat /etc/os-release | head -2
NAME="Red Hat Enterprise Linux"
VERSION="8.4 (Ootpa)"
[rootmediator-host ~]#
```

3. 重新安裝ONTAP Mediator：

> 重新安裝 ONTAP Mediator 之後、請立即執行其餘步驟、以避免記錄檔遺失。

```
[rootmediator-host ~]# ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

  ..<snip installation>..
[rootmediator-host ~]#
```

4. 停止 ontap_mediator：

```
[rootmediator-host ~]# systemctl stop ontap_mediator
[rootmediator-host ~]#
```

5. 替換日誌檔：

```
[rootmediator-host ~]# tar -xf ontap_mediator_log_backup.tgz -C
/opt/netapp/lib/ontap_mediator
[rootmediator-host ~]#
```

6. 啟動 ontap_mediator：

```
[rootmediator-host ~]# systemctl start ontap_mediator
[rootmediator-host ~]#
```

7. 將所有ONTAP叢集重新連接到升級後的ONTAP中介器：

基於 IP 的MetroCluster

```
siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          false
                        siteA-node1             true          false
                        siteB-node2             true          false
                        siteB-node2             true          false
siteA::> metrocluster configuration-settings mediator remove
Removing the mediator and disabling Automatic Unplanned Switchover. It
may take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Automatic Unplanned Switchover is disabled for all nodes...
Removing mediator mailboxes...
Successfully removed the mediator.

siteA::> metrocluster configuration-settings mediator add -mediator
-address 172.31.40.122
Adding the mediator and enabling Automatic Unplanned Switchover. It may
take a few minutes to complete.
Please enter the username for the mediator: mediatoradmin
Please enter the password for the mediator:
Confirm the mediator password:
Successfully added the mediator.

siteA::> metrocluster configuration-settings mediator show
Mediator IP     Port    Node                    Configuration
Connection
                                                Status        Status
--------------- ------- ---------------------- -------------
-----------
172.31.40.122
                31784   siteA-node2             true          true
                        siteA-node1             true          true
                        siteB-node2             true          true
                        siteB-node2             true          true
siteA::>
```

SnapMirror 主動同步

對於SnapMirror主動同步，您無需重新安裝儲存在 /opt/netapp 之外的 TLS 憑證。備份並還原儲存在 /opt/netapp 中的憑證。

```
peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            unreachable       true

peer1::> snapmirror mediator remove -mediator-address 172.31.49.237
-peer-cluster peer2

Info: [Job 39] 'mediator remove' job queued

peer1::> job show -id 39
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
39     mediator remove      peer1      peer1-node1    Success
     Description: Removing entry in mediator

peer1::> security certificate show -common-name ONTAPMediatorCA
Vserver    Serial Number   Certificate Name                       Type
---------- --------------- -------------------------------------
------------
peer1
        4A790360081F41145E14C5D7CE721DC6C210007F
                         ONTAPMediatorCA                        server-
ca
    Certificate Authority: ONTAP Mediator CA
        Expiration Date: Mon Apr 17 10:27:54 2073

peer1::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

 peer1::> security certificate install -type server-ca -vserver peer1

Please enter Certificate: Press <Enter> when done
  ..<snip ONTAP Mediator CA public key>..

You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254
```

```
The certificate's generated name for reference: ONTAPMediatorCA

peer2::> security certificate delete -common-name ONTAPMediatorCA *
1 entry was deleted.

peer2::> security certificate install -type server-ca -vserver peer2

 Please enter Certificate: Press <Enter> when done
..<snip ONTAP Mediator CA public key>..


You should keep a copy of the CA-signed digital certificate for future
reference.

The installed certificate's CA and serial number for reference:
CA: ONTAP Mediator CA
serial: 44786524464C5113D5EC966779D3002135EA4254

The certificate's generated name for reference: ONTAPMediatorCA

peer1::> snapmirror mediator add -mediator-address 172.31.49.237 -peer
-cluster peer2 -username mediatoradmin

Notice: Enter the mediator password.

Enter the password:
Enter the password again:

Info: [Job: 43] 'mediator add' job queued

peer1::> job show -id 43
                            Owning
Job ID Name                 Vserver    Node           State
------ -------------------- ---------- -------------- ----------
43     mediator add         peer1      peer1-node2    Success
    Description: Creating a mediator entry

peer1::> snapmirror mediator show
Mediator Address Peer Cluster     Connection Status Quorum Status
---------------- ---------------- ----------------- -------------
172.31.49.237    peer2            connected         true

peer1::>
```

相關資訊

- "刪除安全性憑證"
- "安全性憑證安裝"
- "安全證書展示"
- "SnapMirror 中介添加"
- "SnapMirror 中介器刪除"
- "儲存 iscsi 啟動器顯示"

提供 **ONTAP Mediator** 安裝的儲存庫存取

您應該啟用對儲存庫的訪問，以便 ONTAP Mediator 可以在安裝過程中存取所需的軟體包。

步驟

1. 確定必須存取的儲存庫、如下表所示：

如果您的作業系統是…	您必須提供這些儲存庫的存取權限…
RHEL 10.x	• rhel-10-for-x86_64-baseos-rpms • rhel-10-for-x86_64-appstream-rpms
RHEL 9.x	• rhel-9-for-x86_64 — basos-rpms • rhel-9-for-x86_64 - AppStream-rpms
RHEL 8.x	• RHEL-8-for-x86_64：basos-rpms • RHEL-8-for-x86_64：AppStream：rpms
RHEL 7.x	• RHEL-7-server選用-rpms
CentOS 7.x	• C7.6.1810 -基礎儲存庫
Rocky Linux 10	• AppStream • 基礎
Rocky Linux 9	• AppStream • 基礎
Rocky Linux 8	• AppStream • 基礎

2. 請使用下列其中一個程序來啟用對上述儲存庫的存取、以便 ONTAP Mediator 在安裝過程中存取所需的套件。

如果 ONTAP 調解器依賴「extras」和「optional」儲存庫中的 Python 模組，則可能需要存取 `rhel-X-for-x86_64-extras-rpms`和 `rhel-X-for-x86_64-optional-rpms`文件。

RHEL 10.x 作業系統的安裝步驟

如果您的作業系統是 **RHEL 10.x**，請使用此程序來啟用對儲存庫的存取：

步驟

1. 訂閱所需的儲存庫：

```
subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
```

下列範例顯示此命令的執行：

```
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-baseos-rpms
Repository 'rhel-10-for-x86_64-baseos-rpms' is enabled for this system.
[root@localhost ~]# subscription-manager repos --enable rhel-10-for-x86_64-appstream-rpms
Repository 'rhel-10-for-x86_64-appstream-rpms' is enabled for this system.
```

2. 執行 `yum repolist` 命令。

新訂閱的儲存庫應會出現在清單中。

RHEL 9.x 作業系統的程序

如果您的作業系統為 * RHEL 9.x * 、請使用此程序來存取儲存庫：

步驟

1. 訂閱所需的儲存庫：

```
subscription-manager repos --enable rhel-9-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-9-for-x86_64-appstream-rpms
```

下列範例顯示此命令的執行：

```
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-baseos-rpms
Repository 'rhel-9-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-9-for-
x86_64-appstream-rpms
Repository 'rhel-9-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. 執行 `yum repolist` 命令。

新訂閱的儲存庫應會出現在清單中。

RHEL 8.x 作業系統的程序

如果您的作業系統是 * RHEL 8.x 、請使用此程序來存取儲存庫：

步驟

1. 訂閱所需的儲存庫：

```
subscription-manager repos --enable rhel-8-for-x86_64-baseos-rpms
```

```
subscription-manager repos --enable rhel-8-for-x86_64-appstream-rpms
```

下列範例顯示此命令的執行：

```
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-baseos-rpms
Repository 'rhel-8-for-x86_64-baseos-rpms' is enabled for this
system.
[root@localhost ~]# subscription-manager repos --enable rhel-8-for-
x86_64-appstream-rpms
Repository 'rhel-8-for-x86_64-appstream-rpms' is enabled for this
system.
```

2. 執行 `yum repolist` 命令。

新訂閱的儲存庫應會出現在清單中。

RHEL 7.x作業系統的程序

如果您的作業系統是 * RHEL 7.x * 、請使用此程序來存取儲存庫：

步驟

1. 訂閱所需的儲存庫：

```
subscription-manager repos --enable rhel-7-server-optional-rpms
```

下列範例顯示此命令的執行：

```
[root@localhost ~]# subscription-manager repos --enable rhel-7-
server-optional-rpms
Repository 'rhel-7-server-optional-rpms' is enabled for this system.
```

2. 執行 `yum repolist` 命令。

下列範例顯示此命令的執行。清單中應會顯示「RHEL-7-server選擇性-rpms」儲存庫。

```
[root@localhost ~]# yum repolist
Loaded plugins: product-id, search-disabled-repos, subscription-
manager
rhel-7-server-optional-rpms | 3.2 kB  00:00:00
rhel-7-server-rpms | 3.5 kB  00:00:00
(1/3): rhel-7-server-optional-rpms/7Server/x86_64/group
|  26 kB  00:00:00
(2/3): rhel-7-server-optional-rpms/7Server/x86_64/updateinfo
| 2.5 MB  00:00:00
(3/3): rhel-7-server-optional-rpms/7Server/x86_64/primary_db
| 8.3 MB  00:00:01
repo id                                        repo name
status
rhel-7-server-optional-rpms/7Server/x86_64   Red Hat Enterprise
Linux 7 Server - Optional (RPMs)   19,447
rhel-7-server-rpms/7Server/x86_64            Red Hat Enterprise
Linux 7 Server (RPMs)              26,758
repolist: 46,205
[root@localhost ~]#
```

CentOS 7.x作業系統的程序

如果您的作業系統為 * CentOS 7.x * 、請使用此程序來啟用儲存庫的存取：

下列範例顯示 CentOS 7.6 的儲存庫、可能無法用於其他 CentOS 版本。將基礎儲存庫用於您的CentOS版本。

步驟

1. 新增C7.6.1810 -基礎儲存庫。C7.6.1810 - 基礎資料保險箱儲存庫包含 ONTAP Mediator 所需的「 kernel-devel 」套件。
2. 將下列行新增至/etc/yum、repos.d/CentOS、Vault.repo。

```
[C7.6.1810-base]
name=CentOS-7.6.1810 - Base
baseurl=http://vault.centos.org/7.6.1810/os/$basearch/
gpgcheck=1
gpgkey=file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
enabled=1
```

3. 執行 `yum repolist` 命令。

   下列範例顯示此命令的執行。Centos-7.6.1810 -基礎儲存庫應出現在清單中。

```
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: distro.ibiblio.org
 * extras: distro.ibiblio.org
 * updates: ewr.edge.kernel.org
C7.6.1810-base                                | 3.6 kB  00:00:00
(1/2): C7.6.1810-base/x86_64/group_gz         | 166 kB  00:00:00
(2/2): C7.6.1810-base/x86_64/primary_db       | 6.0 MB  00:00:04
repo id                      repo name                status
C7.6.1810-base/x86_64        CentOS-7.6.1810 - Base   10,019
base/7/x86_64                CentOS-7 - Base          10,097
extras/7/x86_64              CentOS-7 - Extras        307
updates/7/x86_64             CentOS-7 - Updates       1,010
repolist: 21,433
[root@localhost ~]#
```

Rocky Linux 10、9 或 8 作業系統的程序

如果您的作業系統是 **Rocky Linux 10**、**Rocky Linux 9** 或 **Rocky Linux 8**，請使用下列步驟來啟用對儲存庫的存取：

步驟

1. 訂閱所需的儲存庫：

```
dnf config-manager --set-enabled baseos
```

```
dnf config-manager --set-enabled appstream
```

2. 執行 `clean` 營運：

```
dnf clean all
```

3. 確認儲存庫清單：

```
dnf repolist
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 10 - AppStream
baseos                          Rocky Linux 10 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                         repo name
appstream                       Rocky Linux 9 - AppStream
baseos                          Rocky Linux 9 - BaseOS
[root@localhost ~]#
```

```
[root@localhost ~]# dnf config-manager --set-enabled baseos
[root@localhost ~]# dnf config-manager --set-enabled appstream
[root@localhost ~]# dnf clean all
[root@localhost ~]# dnf repolist
repo id                          repo name
appstream                        Rocky Linux 8 - AppStream
baseos                           Rocky Linux 8 - BaseOS
[root@localhost ~]#
```

下載 **ONTAP Mediator** 安裝套件

下載ONTAP Mediator 安裝套件並進行安裝。

步驟

1. 從 ONTAP Mediator 下載頁面下載 ONTAP Mediator 安裝套件。

   "《資訊媒體》下載頁面ONTAP"

2. 請確保已將 Mediator 安裝包放置在目前工作目錄中：

   ```
   [root@sdot-r730-0003a-d6 ~]# ls ontap-mediator-1.11.0.tgz
   ```

   ```
   ontap-mediator-1.11.0.tgz
   ```

   針對1.4版及更早版本的資訊、安裝程式會命名為「」ONTAP `ontap-mediator`。

   如果您的系統無法存取互聯網，請確保安裝程式可以存取所需的軟體包。

3. 如有需要，請將 Mediator 安裝套件移至安裝目錄。
4. 解壓縮安裝程式套件：

   ```
   tar xvfz ontap-mediator-1.11.0.tgz
   ```

```
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
```

驗證**ONTAP** 《不實程式碼簽章》

NetApp建議在安裝前驗證ONTAP Mediator 程式碼簽章。此步驟是可選的。

開始之前

在驗證ONTAP Mediator 程式碼簽署之前，請確保您的系統符合這些要求。

- 自 2025 年 6 月 15 日起，您無法安裝或升級至ONTAP Mediator 1.9 和 1.8，因為代碼簽署驗證憑證已過期。請安裝或升級至ONTAP Mediator 1.11 或 1.10。
- 如果系統不符合下列要求，則不需要驗證程序，您可以直接前往"安裝ONTAP 《不知道如何安裝》套件"。

- 適用於基本驗證的Openssl版本1.0.2至3.0
- 適用於時間戳記授權（TSA）作業的OpenSSL 1.1.0版或更新版本
- 用於OCSP驗證的公共網際網路存取

下載包包含以下文件：

檔案	說明
`ONTAP-Mediator-production.pub`	用於驗證簽名的公開金鑰
`csc-prod-chain-ONTAP-Mediator.pem`	公共認證 CA 信任鏈結
`csc-prod-ONTAP-Mediator.pem`	用於產生金鑰的憑證
`ontap-mediator-1.11.0`	版本 1.11 的產品安裝執行檔
`ontap-mediator-1.11.0.sig`	SHA-256 經過雜湊、然後使用 CSC-prod 金鑰簽署 RSA 、以供安裝程式使用
`ontap-mediator-1.11.0.sig.tsr`	OCSCP 用於安裝程式簽章的撤銷要求

ontap-mediator-1.11.0.tsr	時間戳記簽署要求檔案
tsa-prod-ONTAP-Mediator.pem	TSR 的公開憑證
tsa-prod-chain-ONTAP-Mediator.pem	TSR 的公用憑證 CA 鏈

步驟

1. 執行撤銷檢查 csc-prod-ONTAP-Mediator.pem 使用線上憑證狀態傳輸協定（OCSP）。
   a. 找到憑證的 OCSP URL。開發者證書可能不提供 URI：

   ```
   openssl x509 -noout -ocsp_uri -in csc-prod-chain-ONTAP-Mediator.pem
   ```

   b. 為憑證產生OCSP要求。

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem
   -reqout req.der
   ```

   c. 連線至OCSP管理程式以傳送OCSP要求：

   ```
   openssl ocsp -issuer csc-prod-chain-ONTAP-Mediator.pem -CAfile csc-
   prod-chain-ONTAP-Mediator.pem -cert csc-prod-ONTAP-Mediator.pem  -url
   ${ocsp_uri} -resp_text -respout resp.der -verify_other csc-prod-
   chain-ONTAP-Mediator.pem
   ```

2. 針對本機主機驗證其信任鏈結和到期日：

   `openssl verify`

   ◦ openssl 路徑的版本必須有效 cert.pem （非自行簽署）。

   ```
   openssl verify -untrusted csc-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} csc-prod-ONTAP-Mediator.pem  # Failure action: The Code-
   Signature-Check certificate has expired or is invalid. Download a newer
   version of the ONTAP Mediator.
   openssl verify -untrusted tsa-prod-chain-ONTAP-Mediator.pem -CApath
   ${OPENSSLDIR} tsa-prod-ONTAP-Mediator.pem  # Failure action: The Time-
   Stamp certificate has expired or is invalid. Download a newer version of
   the ONTAP Mediator.
   ```

3. 核實 `ontap-mediator-1.11.0.sig.tsr`和 `ontap-mediator-1.11.0.tsr`使用關聯證書的檔案：

OpenSSL 3.x

```
openssl ts -verify -data ontap-mediator-1.11.0.sig -in ontap-mediator-1.11.0.sig.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -untrusted tsa-prod-ONTAP-Mediator.pem
```

OpenSSL 1.x

```
openssl ts -verify -data ontap-mediator-1.11.0 -in ontap-mediator-1.11.0.tsr -CAfile tsa-prod-chain-ONTAP-Mediator.pem -partial_chain
```

`.tsr`檔案包含與安裝程式關聯的時間戳記回應和程式碼簽署。處理過程確認時間戳具有 TSA 的有效簽名，且您的輸入檔案未發生變更。您的機器會在本機執行驗證。您無需訪問TSA伺服器。

4. 根據金鑰驗證簽名：

```
openssl -dgst -verify
```

```
openssl dgst -sha256 -verify ONTAP-Mediator-production.pub -signature ontap-mediator-1.11.0.sig ontap-mediator-1.11.0
```

安裝**ONTAP** 《不知道如何安裝》套件

若要安裝 ONTAP Mediator，您必須取得安裝套件並在主機上執行安裝程式。

步驟

1. 執行安裝程式並視需要回應提示：

```
./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

```
[root@scs000099753 ~]# ./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y
```

若要跳過安裝過程中的簽章檢查，請使用下列命令： `./ontap-mediator-1.11.0/ontap-mediator-1.11.0 -y --skip-code-signature-check`

安裝程式會建立所需的帳戶並安裝所需的軟體包。如果 Mediator 已安裝，則會提示您進行升級。

安裝示例（主控台輸出）**ONTAP**

```
[root@mediator_host ~]# tar -zxvf ontap-mediator-1.11.0.tgz
ontap-mediator-1.11.0/
ontap-mediator-1.11.0/csc-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/csc-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-ONTAP-Mediator.pem
ontap-mediator-1.11.0/tsa-prod-chain-ONTAP-Mediator.pem
ontap-mediator-1.11.0/ONTAP-Mediator-production.pub
ontap-mediator-1.11.0/ontap-mediator-1.11.0
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.tsr
ontap-mediator-1.11.0/ontap-mediator-1.11.0.sig
[root@mediator_host ~]#./ontap-mediator-1.11.0/ontap-mediator-1.11.0

ONTAP Mediator: Self Extracting Installer

+ Extracting the ONTAP Mediator installation/upgrade archive
+ Performing the ONTAP Mediator run-time code signature check
   Using openssl from the path: /usr/bin/openssl configured for
CApath:/etc/pki/tls
Error querying OCSP responder
80BBA032607F0000:error:1E800080:HTTP
routines:OSSL_HTTP_REQ_CTX_nbio:failed reading
data:crypto/http/http_client.c:549:
80BBA032607F0000:error:1E800067:HTTP
routines:OSSL_HTTP_REQ_CTX_exchange:error
receiving:crypto/http/http_client.c:901:server=http://ocsp.entrust.net:
80
   WARNING: The OCSP check failed while attempting to test the Code-
Signature-Check certificate
   Continue without code signature checking (only recommended if
integrity has been established manually)? yes/no: yes
 SKIPPING: Code signature check, manual override due to lack of OCSP
response
+ Unpacking the ONTAP Mediator installer

ONTAP Mediator requires two user accounts. One for the service
(netapp), and one for use by ONTAP to the mediator API (mediatoradmin).
Would you like to use the default account names: netapp +
mediatoradmin? (Y(es)/n(o)): yes



Enter ONTAP Mediator user account (mediatoradmin) password:
```

```
Re-Enter ONTAP Mediator user account (mediatoradmin) password:

+ Checking if SELinux is in enforcing mode
The installer will change the SELinux context type of
/opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi from type 'lib_t' to
'bin_t'.


+ Checking for default Linux firewall


+ Installing required packages.


Updating Subscription Management repositories.
Unable to read consumer identity

This system is not registered with an entitlement server. You can use
"rhc" or "subscription-manager" to register.

Last metadata expiration check: 5 days, 14:34:13 ago on Thu 10 Jul 2025
01:28:32 AM EDT.
Package openssl-1:3.2.2-16.el10.x86_64 is already installed.
Package libselinux-utils-3.8-1.el10.x86_64 is already installed.
Package perl-Data-Dumper-2.189-512.el10.x86_64 is already installed.
Package bzip2-1.0.8-25.el10.x86_64 is already installed.
Package efibootmgr-18-8.el10.x86_64 is already installed.
Package mokutil-2:0.6.0-11.el10.x86_64 is already installed.
Package policycoreutils-python-utils-3.8-1.el10.noarch is already
installed.
Package python3-3.12.9-1.el10.x86_64 is already installed.
Dependencies resolved.
================================================================================
================================================================================
================================================================================
=========================
 Package
Architecture                                        Version
Repository                                              Size
================================================================================
================================================================================
================================================================================
=========================
Installing:
 elfutils-libelf-devel
x86_64                                              0.192-5.el10
```

```
AppStream                                              50 k
 gcc
x86_64                                          14.2.1-7.el10
AppStream                                              37 M
 kernel-devel
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                              22 M
 make
x86_64                                          1:4.4.1-9.el10
BaseOS                                                591 k
 openssl-devel
x86_64                                          1:3.2.2-16.el10
AppStream                                             3.9 M
 patch
x86_64                                          2.7.6-26.el10
AppStream                                             134 k
 perl-ExtUtils-MakeMaker
noarch                                          2:7.70-513.el10
AppStream                                              297 k
 python3-devel
x86_64                                          3.12.9-1.el10
AppStream
 334 k
 python3-pip
noarch                                          23.3.2-7.el10
AppStream                                             3.2 M
Installing dependencies:
 annobin-docs
noarch                                          12.92-1.el10
AppStream                                              94 k
 annobin-plugin-gcc
x86_64                                          12.92-1.el10
AppStream                                             985 k
 bison
x86_64                                          3.8.2-9.el10
AppStream                                             1.0 M
 cmake-filesystem
x86_64                                          3.30.5-2.el10
AppStream                                              29 k
 cpp
x86_64                                          14.2.1-7.el10
AppStream                                              12 M
 dwz
x86_64                                          0.15-7.el10
AppStream                                             139 k
 efi-srpm-macros
```

```
noarch                                          6-6.el10
AppStream                                          25 k
 flex
x86_64                                          2.6.4-19.el10
AppStream                                         303 k
 fonts-srpm-macros
noarch                                          1:2.0.5-18.el10
AppStream                                          29 k
 forge-srpm-macros
noarch                                          0.4.0-6.el10
AppStream                                          23 k
 gcc-plugin-annobin
x86_64                                          14.2.1-7.el10
AppStream                                          62 k
 glibc-devel
x86_64                                          2.39-37.el10
AppStream                                         641 k
 go-srpm-macros
noarch                                          3.6.0-4.el10
AppStream                                          29 k
 kernel-headers
x86_64                                          6.12.0-55.9.1.el10_0
AppStream                                         2.3 M
 kernel-srpm-macros
noarch                                          1.0-25.el10
AppStream                                          11 k
 libxcrypt-devel
x86_64                                          4.4.36-10.el10
AppStream                                          33 k
 libzstd-devel
x86_64                                          1.5.5-9.el10
AppStream
  53 k
 lua-srpm-macros
noarch                                          1-15.el10
AppStream                                          10 k
 m4
x86_64                                          1.4.19-11.el10
AppStream                                         309 k
 ocaml-srpm-macros
noarch                                          10-4.el10
AppStream                                          10 k
 openblas-srpm-macros
noarch                                          2-19.el10
AppStream                                         9.0 k
 package-notes-srpm-macros
```

```
noarch                                          0.5-13.el10
AppStream                                          11 k
 perl-AutoSplit
noarch                                          5.74-512.el10
AppStream                                          23 k
 perl-Benchmark
noarch                                          1.25-512.el10
AppStream                                          28 k
 perl-CPAN-Meta-Requirements
noarch                                          2.143-11.el10
AppStream                                          39 k
 perl-CPAN-Meta-YAML
noarch                                          0.018-512.el10
AppStream                                          29 k
 perl-Devel-PPPort
x86_64                                          3.72-512.el10
AppStream                                         223 k
 perl-ExtUtils-Command
noarch                                          2:7.70-513.el10
AppStream                                          16 k
 perl-ExtUtils-Constant
noarch                                          0.25-512.el10
AppStream                                          47 k
 perl-ExtUtils-Install
noarch                                          2.22-511.el10
AppStream                                          47 k
 perl-ExtUtils-Manifest
noarch                                          1:1.75-511.el10
AppStream                                          37 k
 perl-ExtUtils-ParseXS
noarch                                          1:3.51-512.el10
AppStream                                         190 k
 perl-File-Compare
noarch                                          1.100.800-512.el10
AppStream                                          15 k
 perl-File-Copy
noarch                                          2.41-512.el10
AppStream                                          22 k
 perl-I18N-Langinfo
x86_64                                          0.24-512.el10
AppStream                                          28 k
 perl-JSON-PP
noarch                                          1:4.16-512.el10
AppStream                                          69 k
 perl-Test-Harness
noarch                                          1:3.48-512.el10
```

```
AppStream                                          288 k
 perl-lib
x86_64                                          0.65-512.el10
AppStream                                           16 k
 perl-srpm-macros
noarch                                          1-57.el10
AppStream                                          9.7 k
 perl-version
x86_64                                          8:0.99.32-4.el10
AppStream                                           68 k
 pyproject-srpm-macros
noarch                                          1.16.2-1.el10
AppStream                                           16 k
 python-srpm-macros
noarch                                          3.12-9.1.el10
AppStream                                           26 k
 python3-pyparsing
noarch                                          3.1.1-7.el10
BaseOS                                             273 k
 qt6-srpm-macros
noarch                                          6.8.1-3.el10
AppStream
 11 k
 redhat-rpm-config
noarch                                          288-1.el10
AppStream                                           83 k
 rust-toolset-srpm-macros
noarch                                          1.84.1-1.el10
AppStream                                           13 k
 systemtap-sdt-devel
x86_64                                          5.2-2.el10
AppStream                                           78 k
 systemtap-sdt-dtrace
x86_64                                          5.2-2.el10
AppStream                                           72 k
 zlib-ng-compat-devel
x86_64                                          2.2.3-1.el10
AppStream                                           41 k
Installing weak dependencies:
 perl-CPAN-Meta
noarch                                          2.150010-511.el10
AppStream                                          202 k
 perl-Encode-Locale
noarch                                          1.05-31.el10
AppStream                                           21 k
 perl-Time-HiRes
```

```
x86_64                                                 4:1.9777-511.el10
AppStream                                                  62 k
 perl-devel
x86_64                                                 4:5.40.1-512.el10
AppStream                                                 772 k
 perl-doc
noarch                                                 5.40.1-512.el10
AppStream                                                 4.9 M

Transaction Summary
================================================================================
================================================================================
================================================================================
=========================
Install  63 Packages

Total size: 94 M
Installed size: 282 M
Downloading Packages:
BaseOS Packages Red Hat Enterprise Linux 10
439 kB/s | 3.7 kB     00:00
Importing GPG key 0xFD431D51:
 Userid     : "Red Hat, Inc. (release key 2) <security@redhat.com>"
 Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
 Userid     : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
  Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
 From       : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing        :
1/1
  Installing       : perl-version-8:0.99.32-4.el10.x86_64
1/63
  Installing       : perl-File-Copy-2.41-512.el10.noarch
2/63
  Installing       : perl-CPAN-Meta-Requirements-2.143-11.el10.noarch
3/63
  Installing       : perl-Time-HiRes-4:1.9777-511.el10.x86_64
4/63
```

```
  Installing       : perl-JSON-PP-1:4.16-512.el10.noarch
5/63
  Installing       : perl-File-Compare-1.100.800-512.el10.noarch
6/63
  Installing       : perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch
7/63
  Installing       : m4-1.4.19-11.el10.x86_64
8/63
  Installing       : make-1:4.4.1-9.el10.x86_64
9/63
  Installing       : bison-3.8.2-9.el10.x86_64
10/63
  Installing       : flex-2.6.4-19.el10.x86_64
11/63
  Installing       : perl-ExtUtils-Command-2:7.70-513.el10.noarch
12/63
  Installing       : perl-ExtUtils-Manifest-1:1.75-511.el10.noarch
13/63
  Installing       : systemtap-sdt-devel-5.2-2.el10.x86_64
14/63
  Installing       : rust-toolset-srpm-macros-1.84.1-1.el10.noarch
15/63
  Installing       : qt6-srpm-macros-6.8.1-3.el10.noarch
16/63
  Installing       : python3-pip-23.3.2-7.el10.noarch
17/63
  Installing       : pyproject-srpm-macros-1.16.2-1.el10.noarch
18/63
  Installing       : perl-srpm-macros-1-57.el10.noarch
19/63
  Installing       : perl-lib-0.65-512.el10.x86_64
20/63
  Installing       : perl-doc-5.40.1-512.el10.noarch
21/63
  Installing       : perl-I18N-Langinfo-0.24-512.el10.x86_64
22/63
  Installing       : perl-Encode-Locale-1.05-31.el10.noarch
23/63
  Installing       : perl-ExtUtils-Constant-0.25-512.el10.noarch
24/63
  Installing       : perl-Devel-PPPort-3.72-512.el10.x86_64
25/63
  Installing       : perl-CPAN-Meta-YAML-0.018-512.el10.noarch
26/63
  Installing       : perl-CPAN-Meta-2.150010-511.el10.noarch
27/63
```

```
  Installing       : perl-Benchmark-1.25-512.el10.noarch
28/63
  Installing       : perl-Test-Harness-1:3.48-512.el10.noarch
29/63
  Installing       : perl-AutoSplit-5.74-512.el10.noarch
30/63
  Installing       : package-notes-srpm-macros-0.5-13.el10.noarch
31/63
  Installing       : openssl-devel-1:3.2.2-16.el10.x86_64
32/63
  Installing       : openblas-srpm-macros-2-19.el10.noarch
33/63
  Installing       : ocaml-srpm-macros-10-4.el10.noarch
34/63
  Installing       : lua-srpm-macros-1-15.el10.noarch
35/63
  Installing       : libzstd-devel-1.5.5-9.el10.x86_64
36/63
  Installing       : kernel-srpm-macros-1.0-25.el10.noarch
37/63
  Installing       : kernel-headers-6.12.0-55.9.1.el10_0.x86_64
38/63
  Installing       : libxcrypt-devel-4.4.36-10.el10.x86_64
39/63
  Installing       : glibc-devel-2.39-37.el10.x86_64
40/63
  Installing       : efi-srpm-macros-6-6.el10.noarch
41/63
  Installing       : dwz-0.15-7.el10.x86_64
42/63
  Installing       : cpp-14.2.1-7.el10.x86_64
43/63
  Installing       : gcc-14.2.1-7.el10.x86_64
44/63
  Installing       : gcc-plugin-annobin-14.2.1-7.el10.x86_64
45/63
  Installing       : cmake-filesystem-3.30.5-2.el10.x86_64
46/63
  Installing       : zlib-ng-compat-devel-2.2.3-1.el10.x86_64
47/63
  Installing       : elfutils-libelf-devel-0.192-5.el10.x86_64
48/63
  Installing       : annobin-docs-12.92-1.el10.noarch
49/63
  Installing       : annobin-plugin-gcc-12.92-1.el10.x86_64
50/63
```

```
  Installing       : fonts-srpm-macros-1:2.0.5-18.el10.noarch
51/63
  Installing       : forge-srpm-macros-0.4.0-6.el10.noarch
52/63
  Installing       : go-srpm-macros-3.6.0-4.el10.noarch
53/63
  Installing       : python-srpm-macros-3.12-9.1.el10.noarch
54/63
  Installing       : redhat-rpm-config-288-1.el10.noarch
55/63
  Running scriptlet: redhat-rpm-config-288-1.el10.noarch
55/63
  Installing       : python3-pyparsing-3.1.1-7.el10.noarch
56/63
  Installing       : systemtap-sdt-dtrace-5.2-2.el10.x86_64
57/63
  Installing       : perl-devel-4:5.40.1-512.el10.x86_64
58/63
  Installing       : perl-ExtUtils-Install-2.22-511.el10.noarch
59/63
  Installing       : perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch
60/63
  Installing       : kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Running scriptlet: kernel-devel-6.12.0-55.9.1.el10_0.x86_64
61/63
  Installing       : python3-devel-3.12.9-1.el10.x86_64
62/63
  Installing       : patch-2.7.6-26.el10.x86_64
63/63
  Running scriptlet: patch-2.7.6-26.el10.x86_64
63/63
Installed products updated.

Installed:
  annobin-docs-12.92-1.el10.noarch              annobin-plugin-gcc-
12.92-1.el10.x86_64            bison-3.8.2-9.el10.x86_64
cmake-filesystem-3.30.5-2.el10.x86_64           cpp-14.2.1-
7.el10.x86_64
  dwz-0.15-7.el10.x86_64                        efi-srpm-macros-6-
6.el10.noarch                  elfutils-libelf-devel-0.192-
5.el10.x86_64   flex-2.6.4-19.el10.x86_64                       fonts-
srpm-macros-1:2.0.5-18.el10.noarch
  forge-srpm-macros-0.4.0-6.el10.noarch         gcc-14.2.1-
7.el10.x86_64                          gcc-plugin-annobin-14.2.1-
7.el10.x86_64     glibc-devel-2.39-37.el10.x86_64                go-
```

```
srpm-macros-3.6.0-4.el10.noarch
  kernel-devel-6.12.0-55.9.1.el10_0.x86_64      kernel-headers-6.12.0-
55.9.1.el10_0.x86_64        kernel-srpm-macros-1.0-25.el10.noarch
libxcrypt-devel-4.4.36-10.el10.x86_64           libzstd-devel-1.5.5-
9.el10.x86_64
  lua-srpm-macros-1-15.el10.noarch              m4-1.4.19-
11.el10.x86_64                          make-1:4.4.1-9.el10.x86_64
ocaml-srpm-macros-10-4.el10.noarch              openblas-srpm-macros-2-
19.el10.noarch
  openssl-devel-1:3.2.2-16.el10.x86_64          package-notes-srpm-
macros-0.5-13.el10.noarch      patch-2.7.6-26.el10.x86_64
perl-AutoSplit-5.74-512.el10.noarch             perl-Benchmark-1.25-
512.el10.noarch
  perl-CPAN-Meta-2.150010-511.el10.noarch       perl-CPAN-Meta-
Requirements-2.143-11.el10.noarch  perl-CPAN-Meta-YAML-0.018-
512.el10.noarch   perl-Devel-PPPort-3.72-512.el10.x86_64          perl-
Encode-Locale-1.05-31.el10.noarch
  perl-ExtUtils-Command-2:7.70-513.el10.noarch  perl-ExtUtils-Constant-
0.25-512.el10.noarch       perl-ExtUtils-Install-2.22-511.el10.noarch
perl-ExtUtils-MakeMaker-2:7.70-513.el10.noarch  perl-ExtUtils-Manifest-
1:1.75-511.el10.noarch
  perl-ExtUtils-ParseXS-1:3.51-512.el10.noarch  perl-File-Compare-
1.100.800-512.el10.noarch       perl-File-Copy-2.41-512.el10.noarch
perl-I18N-Langinfo-0.24-512.el10.x86_64         perl-JSON-PP-1:4.16-
512.el10.noarch
  perl-Test-Harness-1:3.48-512.el10.noarch      perl-Time-HiRes-
4:1.9777-511.el10.x86_64          perl-devel-4:5.40.1-512.el10.x86_64
perl-doc-5.40.1-512.el10.noarch                 perl-lib-0.65-
512.el10.x86_64
  perl-srpm-macros-1-57.el10.noarch             perl-version-8:0.99.32-
4.el10.x86_64              pyproject-srpm-macros-1.16.2-1.el10.noarch
python-srpm-macros-3.12-9.1.el10.noarch         python3-devel-3.12.9-
1.el10.x86_64
  python3-pip-23.3.2-7.el10.noarch              python3-pyparsing-
3.1.1-7.el10.noarch             qt6-srpm-macros-6.8.1-3.el10.noarch
redhat-rpm-config-288-1.el10.noarch             rust-toolset-srpm-
macros-1.84.1-1.el10.noarch
  systemtap-sdt-devel-5.2-2.el10.x86_64         systemtap-sdt-dtrace-
5.2-2.el10.x86_64            zlib-ng-compat-devel-2.2.3-1.el10.x86_64

Complete!
OS package installations finished
+ Installing ONTAP Mediator. (Log: /root/ontap_mediator.vdizgQ/ontap-
mediator-1.11.0/ontap-mediator-1.11.0/install_20250715160240.log)
    This step takes several minutes. View progress in the log file.
    Sudoer config verified
```

```
    ONTAP Mediator rsyslog and logging rotation enabled
+ Install successful. (Moving log to
/opt/netapp/lib/ontap_mediator/log/install_20250715160240.log)
+ WARNING: This system supports UEFI
           Secure Boot (SB) is currently disabled on this system.
           If SB is enabled in the future, SCST will not work unless
the following action is taken:
           Using the keys in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys follow
           instructions in
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.modu
le-signing
           to sign the SCST kernel module. Note that a reboot is
needed.
     SCST does not start automatically when Secure Boot is enabled and
not configured properly.

+ Note: ONTAP Mediator generated a self-signed server certificate for
temporary use on
    this host. If the DNS name or IP address for the host is changed,
the certificate
    will no longer be valid. The default certificates should be
replaced with secure
    trusted certificates signed by a known certificate authority prior
to use for production.
    For more information, see /opt/netapp/lib/ontap_mediator/README

+ Note: ONTAP Mediator uses a kernel module compiled specifically for
the current
        OS. Using 'yum update' to upgrade the kernel might cause
service interruption.
    For more information, see /opt/netapp/lib/ontap_mediator/README
root@mediator_host:~# systemctl status ontap_mediator
● ontap_mediator.service - ONTAP Mediator
     Loaded: loaded (/etc/systemd/system/ontap_mediator.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
9s ago
 Invocation: 395e9479487e4e308be2ae030c800c7f
    Process: 28745
ExecStartPre=/opt/netapp/lib/ontap_mediator/tools/otm_logs_fs.sh
(code=exited, status=0/SUCCESS)
   Main PID: 28759 (python)
      Tasks: 1 (limit: 22990)
     Memory: 66.8M (peak: 68.8M)
        CPU: 2.865s
```

```
     CGroup: /system.slice/ontap_mediator.service
             └─28759 /opt/netapp/lib/ontap_mediator/pyenv/bin/python
/opt/netapp/lib/ontap_mediator/ontap_mediator/server

Jul 15 16:07:29 mediator_host systemd[1]: Starting
ontap_mediator.service - ONTAP Mediator...
Jul 15 16:07:29 mediator_host systemd[1]: Started
ontap_mediator.service - ONTAP Mediator.
root@mediator_host:~# systemctl status mediator-scst
● mediator-scst.service
     Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; preset: disabled)
     Active: active (running) since Tue 2025-07-15 16:07:29 EDT; 4min
15s ago
 Invocation: f1d3be6ca1f9492b943e61872676f384
    Process: 28653 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
    Process: 28738 ExecStartPost=/usr/sbin/modprobe scst_vdisk
(code=exited, status=0/SUCCESS)
   Main PID: 28696 (iscsi-scstd)
      Tasks: 1 (limit: 22990)
     Memory: 5.2M (peak: 35.2M)
        CPU: 547ms
     CGroup: /system.slice/mediator-scst.service
             └─28696 /usr/local/sbin/iscsi-scstd

Jul 15 16:07:28 mediator_host systemd[1]: Starting mediator-
scst.service...
Jul 15 16:07:29 mediator_host iscsi-scstd[28694]: max_data_seg_len
1048576, max_queued_cmds 2048
Jul 15 16:07:29 mediator_host scst[28653]: Loading and configuring SCST
Jul 15 16:07:29 mediator_host systemd[1]: Started mediator-
scst.service.
root@mediator_host:~#
```

註冊 **UEFI** 安全啟動的安全金鑰

從ONTAP Mediator 1.4 開始，UEFI 系統上啟用了安全啟動機制。啟用安全啟動後，安裝完成後必須採取額外步驟來註冊安全金鑰。

步驟

1. 依照 README 檔案中的說明對 SCST 核心模組進行簽署：

   ```
   /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
   signing
   ```

2. 找到所需的金鑰：

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
```

安裝完成後，系統輸出會提供 README 檔案和金鑰位置。

3. 將公開金鑰新增至莫克清單：

```
mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

您可以將私鑰保留在預設位置，也可以將其移動到安全位置。您必須將公鑰保存在現有位置，以便啟動管理器可以使用它。更多資訊請參閱 README.module-signing 檔案：

```
[root@hostname ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
```

4. 重新啟動主機，並使用裝置的 UEFI 啟動管理員批准新的 MOK。您需要使用提供的密碼短語。 `mokutil`實用性"啟用 UEFI 安全開機時，請安裝 ONTAP Mediator"。

對 **SCST** 核心模組進行簽名

安裝ONTAP Mediator 後，如果 systemctl 狀態 `mediator-scst`顯示為失敗（非活動狀態），請依照下列步驟對 SCST 核心模組進行簽署。

步驟

1. 在建置過程中，會產生一對公鑰/私鑰。 `/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`使用以下命令進入目錄：

```
[root@mediator-host ~]# ls
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/
README.module-signing scst_module_key.der scst_module_key.priv
[root@mediator-host ~]#
```

2. 執行以下命令，開始將公鑰匯入UEFI金鑰庫的過程：

```
[root@mediator-host ~]# mokutil --import
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
input password:
input password again:

[root@mediator-host ~]#
```

3. mokutil 軟體在匯入過程中會要求為此金鑰設定一個臨時密碼。
4. 確認導入過程是否已開始 `mokutil --list-new`然後重啟系統。引導程式啟動 EFI MOK 管理器。
5. 使用螢幕上的選單開啟 SCST 核心模組金鑰。啟動後，運行 `systemctl status mediator-scst`。服務啟動後，SCST 核心模組將被簽署。

確認 **ONTAP Mediator** 安裝狀態

安裝 ONTAP Mediator 後，請驗證它是否成功運作。

步驟

1. 查看 ONTAP 調解器的狀態：

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. 確認 ONTAP 調解器所使用的連接埠：

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp    0    0 0.0.0.0:31784    0.0.0.0:*       LISTEN

         tcp    0    0 0.0.0.0:3260     0.0.0.0:*       LISTEN

         tcp6   0    0 :::3260          :::*            LISTEN
```

安裝後 **ONTAP Mediator** 組態

安裝並執行 ONTAP Mediator 後，必須在 ONTAP 儲存系統中執行其他設定任務才能使用 ONTAP Mediator 功能：

- 若要在 MetroCluster IP 設定中使用 ONTAP 調解器，請參閱"透過 MetroCluster IP 配置來設定 ONTAP 調解器" 。
- 若要使用 SnapMirror 作用中同步處理，請參閱"安裝 ONTAP 調解器並確認 ONTAP 叢集配置"。

設定 **ONTAP Mediator** 安全性原則

ONTAP 調解器支援多種可設定的安全性設定。所有設定的預設值都是以唯讀檔案提供 `low_space_threshold_mib: 10`：

`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml`

放置在中的所有值 `ontap_mediator.user_config.yaml` 會覆寫預設值、並在所有 ONTAP Mediator 升級

中維護。

修改後 `ontap_mediator.user_config.yaml` ，重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

修改 **ONTAP Mediator** 屬性

如有需要，可修改本節所述的 ONTAP Mediator 屬性。

> 不應變更中的其他預設值 `ontap_mediator.config.yaml`，因為在 ONTAP Mediator 升級期間不會維護修改的值。

您可以將必要的變數複製到檔案中以覆寫預設設定，藉此修改 ONTAP Mediator 屬性 `ontap_mediator.user_config.yaml`。

安裝協力廠商 **SSL** 憑證

如果您需要以協力廠商 SSL 憑證取代預設的自我簽署憑證，請修改下列檔案中的某些屬性：

- `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`
- `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`

這些檔案中的變數用於控制 ONTAP Mediator 使用的憑證檔案。

ONTAP Mediator 1.9 及更新版本

下表列出的預設變數會包含在檔案中 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`。

變動	路徑
`cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`
`ca_key_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key`
`ca_serial_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl`
`cert_valid_days`	`1095`
`x509_passin_pwd`	`pass:ontap`

- `cert_valid_days`用於設定用戶端憑證的到期日。最大值為三年（ 1095 天）。
- `x509_passin_pwd`是簽署用戶端憑證的密碼。

下表列出的預設變數會包含在檔案中 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini`。

變動	路徑
`mediator_cert`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt`
`mediator_key`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key`
`ca_cert_path`	`/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt`

ONTAP Mediator 1.8 及更早版本

下表列出的預設變數會包含在檔案中 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml`。

變動	路徑
cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt
ca_key_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key
ca_serial_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl
cert_valid_days	1095
x509_passin_pwd	pass:ontap

- `cert_valid_days`用於設定用戶端憑證的到期日。最大值為三年（ 1095 天）。
- `x509_passin_pwd`是簽署用戶端憑證的密碼。

下表列出的預設變數會包含在檔案中 /opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini。

變動	路徑
mediator_cert	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt
mediator_key	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key
ca_cert_path	/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt

如果修改這些屬性，請重新啟動 ONTAP 調解器以套用變更。如需如何以協力廠商憑證取代預設憑證的詳細指示，請參閱"以信任的第三方憑證取代自我簽署的憑證"。

密碼攻擊保護

下列設定可防止暴力式密碼猜測攻擊。

若要啟用此功能，請設定和的 retry_limit`值 `window_seconds。

範例：

- 提供 5 分鐘的猜測時間、然後將計數重設為零故障：

```
authentication_lock_window_seconds: 300
```

- 如果在時間範圍內發生五次故障、請鎖定帳戶：

```
authentication_retry_limit: 5
```

- 設定在拒絕每次嘗試之前發生的延遲、以降低暴力式密碼猜測攻擊的影響、進而減緩攻擊速度。

```
authentication_failure_delay_seconds: 5
```

```
authentication_failure_delay_seconds: 0   # seconds (float) to delay
failed auth attempts prior to response, 0 = no delay
authentication_lock_window_seconds: null  # seconds (int) since the
oldest failure before resetting the retry counter, null = no window
authentication_retry_limit: null          # number of retries to allow
before locking API access, null = unlimited
```

密碼複雜度規則

下列欄位可控制 ONTAP Mediator API 使用者帳戶的密碼複雜度規則。

```
password_min_length: 8

password_max_length: 64

password_uppercase_chars: 0    # min. uppercase characters

password_lowercase_chars: 1    # min. lowercase character

password_special_chars: 1      # min. non-letter, non-digit

password_nonletter_chars: 2    # min. non-letter characters (digits,
specials, anything)
```

控制可用空間

有一些設定可控制磁碟上所需的可用空間 `/opt/netapp/lib/ontap_mediator`。

如果空間低於設定的臨界值、服務將會發出警告事件。

```
low_space_threshold_mib: 10
```

控制保留記錄空間

reserve_log_space 是由特定設定所控制。預設情況下，ONTAP Mediator 安裝會為日誌建立單獨的磁碟空間。安裝程式會建立一個新的固定大小文件，其磁碟空間總計為 700MB，專門用於 ONTAP Mediator 日誌記錄。

若要停用此功能並使用預設磁碟空間、請執行下列步驟：

1. 將 reserve_log_space 的值從 1 變更為 0 ：

   ```
   /opt/netapp/lib/ontap_mediator/tools/mediator_env
   ```

2. 重新啟動 Mediator ：

   a. `cat /opt/netapp/lib/ontap_mediator/tools/mediator_env | grep "RESERVE_LOG_SPACE"`

      ```
      RESERVE_LOG_SPACE=0
      ```

   b. `systemctl restart ontap_mediator`

若要重新啟用此功能，請將值從 0 變更為 1 ，然後重新啟動 Mediator 。

> 在磁碟空間之間切換不會清除現有記錄。 切換並重新啟動 Mediator 之後、所有先前的記錄都會備份、然後移至目前的磁碟空間。

管理 **ONTAP Mediator**

管理 ONTAP Mediator，包括變更使用者憑證、停止和重新啟用服務、驗證其運作狀況以及安裝或解除安裝 SCST 以進行主機維護。您也可以管理憑證、例如重新產生自我簽署的憑證、以信任的協力廠商憑證取代它們、以及疑難排解憑證相關問題。

變更使用者名稱

您可以使用下列程序變更使用者名稱。

關於這項工作

在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。

如果無法連線至此命令、您可能需要使用完整路徑來執行命令、如下列範例所示：

```
/usr/local/bin/mediator_username
```

步驟

選擇下列其中一個選項來變更使用者名稱：

- * 選項（ a ） * ：執行命令 `mediator_change_user` 並回應下列範例所示的提示：

```
[root@mediator-host ~]# mediator_change_user
Modify the Mediator API username by entering the following values:
    Mediator API User Name: mediatoradmin
                  Password:
New Mediator API User Name: mediator
The account username has been modified successfully.
[root@mediator-host ~]#
```

- * 選項（ b ） * ：執行下列命令：

```
MEDIATOR_USERNAME=mediator MEDIATOR_PASSWORD=mediator2
MEDIATOR_NEW_USERNAME=mediatoradmin mediator_change_user
```

```
[root@mediator-host ~]# MEDIATOR_USERNAME=mediator
MEDIATOR_PASSWORD='mediator2' MEDIATOR_NEW_USERNAME=mediatoradmin
mediator_change_user
The account username has been modified successfully.
[root@mediator-host ~]#
```

變更密碼

您可以使用下列程序變更密碼。

關於這項工作

在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。

如果無法連線至此命令、您可能需要使用完整路徑來執行命令、如下列範例所示：

```
/usr/local/bin/mediator_change_password
```

步驟

選擇下列其中一個選項來變更密碼：

- * 選項（ a ） * ：執行 `mediator_change_password` 命令並回應提示、如下列範例所示：

```
[root@mediator-host ~]# mediator_change_password
Change the Mediator API password by entering the following values:
   Mediator API User Name: mediatoradmin
              Old Password:
              New Password:
         Confirm Password:
The password has been updated successfully.
[root@mediator-host ~]#
```

- * 選項（ b ） * ：執行下列命令：

```
MEDIATOR_USERNAME=mediatoradmin MEDIATOR_PASSWORD=mediator1
MEDIATOR_NEW_PASSWORD=mediator2 mediator_change_password
```

範例顯示密碼已從「 media1 」變更為「 media2 」。

```
 [root@mediator-host ~]# MEDIATOR_USERNAME=mediatoradmin
MEDIATOR_PASSWORD=mediator1 MEDIATOR_NEW_PASSWORD=mediator2
mediator_change_password
 The password has been updated successfully.
 [root@mediator-host ~]#
```

停止 **ONTAP** 調解器

若要停止 ONTAP 調解器，請執行下列步驟：

步驟

1. 停止 ONTAP 調解器：

```
systemctl stop ontap_mediator
```

2. 停止 SCST ：

```
systemctl stop mediator-scst
```

3. 停用 ONTAP 調解器和 SCST：

```
systemctl disable ontap_mediator mediator-scst
```

重新啟用 **ONTAP** 調解器

若要重新啟用 ONTAP 調解器，請執行下列步驟：

步驟

1. 啟用 ONTAP 調解器和 SCST：

```
systemctl enable ontap_mediator mediator-scst
```

2. 啟動 SCST ：

```
systemctl start mediator-scst
```

3. 啟動 ONTAP Mediator ：

```
systemctl start ontap_mediator
```

驗證 ONTAP 調解器是否正常運作

安裝 ONTAP Mediator 後，請驗證它是否成功運作。

步驟

1. 查看 ONTAP 調解器的狀態：

   a. `systemctl status ontap_mediator`

```
[root@scspr1915530002 ~]# systemctl status ontap_mediator

 ontap_mediator.service - ONTAP Mediator
Loaded: loaded (/etc/systemd/system/ontap_mediator.service; enabled;
vendor preset: disabled)
Active: active (running) since Mon 2022-04-18 10:41:49 EDT; 1 weeks 0
days ago
Process: 286710 ExecStop=/bin/kill -s INT $MAINPID (code=exited,
status=0/SUCCESS)
Main PID: 286712 (uwsgi)
Status: "uWSGI is ready"
Tasks: 3 (limit: 49473)
Memory: 139.2M
CGroup: /system.slice/ontap_mediator.service
      ├─286712 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      ├─286716 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini
      └─286717 /opt/netapp/lib/ontap_mediator/pyenv/bin/uwsgi --ini
/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini

[root@scspr1915530002 ~]#
```

   b. `systemctl status mediator-scst`

```
[root@scspr1915530002 ~]# systemctl status mediator-scst
   Loaded: loaded (/etc/systemd/system/mediator-scst.service;
enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-04-18 10:41:47 EDT; 1
weeks 0 days ago
  Process: 286595 ExecStart=/etc/init.d/scst start (code=exited,
status=0/SUCCESS)
 Main PID: 286662 (iscsi-scstd)
    Tasks: 1 (limit: 49473)
   Memory: 1.2M
   CGroup: /system.slice/mediator-scst.service
           └─286662 /usr/local/sbin/iscsi-scstd

[root@scspr1915530002 ~]#
```

2. 確認 ONTAP 調解器所使用的連接埠：

   `netstat`

```
[root@scspr1905507001 ~]# netstat -anlt | grep -E '3260|31784'

         tcp   0   0 0.0.0.0:31784   0.0.0.0:*      LISTEN

         tcp   0   0 0.0.0.0:3260    0.0.0.0:*      LISTEN

         tcp6  0   0 :::3260         :::*           LISTEN
```

卸載 **ONTAP** 調解器

如有必要，您可以刪除 ONTAP Mediator。

開始之前

您必須先斷開 ONTAP 調解器與 ONTAP 之間的連接，然後才能將其移除。

關於這項工作

在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。

如果無法連線至此命令、您可能需要使用完整路徑來執行命令、如下列範例所示：

`/usr/local/bin/uninstall_ontap_mediator`

步驟

1. 卸載 ONTAP 調解器：

   `uninstall_ontap_mediator`

```
 [root@mediator-host ~]# uninstall_ontap_mediator

 ONTAP Mediator: Self Extracting Uninstaller

 + Removing ONTAP Mediator. (Log:
/tmp/ontap_mediator.GmRGdA/uninstall_ontap_mediator/remove.log)
 + Remove successful.
 [root@mediator-host ~]#
```

重新產生暫時自我簽署的憑證

從 ONTAP Mediator 1.7 開始、您可以使用下列程序重新產生暫時自我簽署的憑證。

此程序僅支援執行 ONTAP Mediator 1.7 或更新版本的系統。

關於這項工作

- 在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。
- 只有安裝 ONTAP 調解器後，由於主機的主機名稱或 IP 位址發生變更而導致產生的自簽章憑證已過時時，您才可以執行此任務。
- 當暫時自我簽署的憑證已由信任的協力廠商憑證取代之後、您不會使用此工作來重新產生憑證。如果沒有自我簽署的憑證、將導致此程序失敗。

步驟

若要為目前主機重新產生新的暫時自我簽署憑證、請執行下列步驟：

1. 重新啟動 ONTAP 調解器：

   ```
   ./make_self_signed_certs.sh overwrite
   ```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key
```

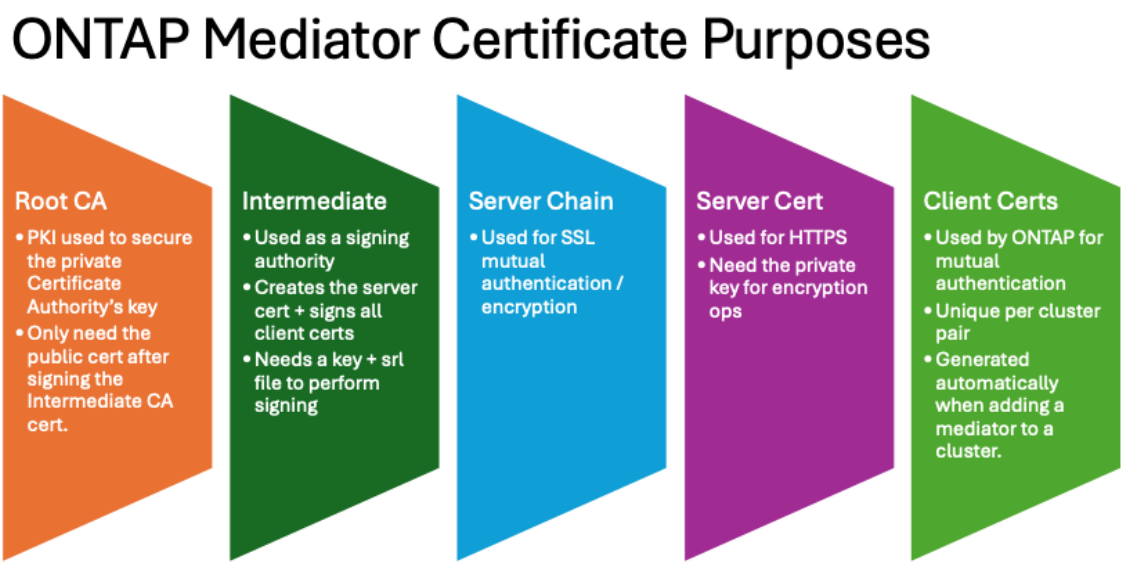
以信任的協力廠商憑證取代自我簽署的憑證

如果支援、您可以使用信任的第三方憑證來取代自我簽署的憑證。

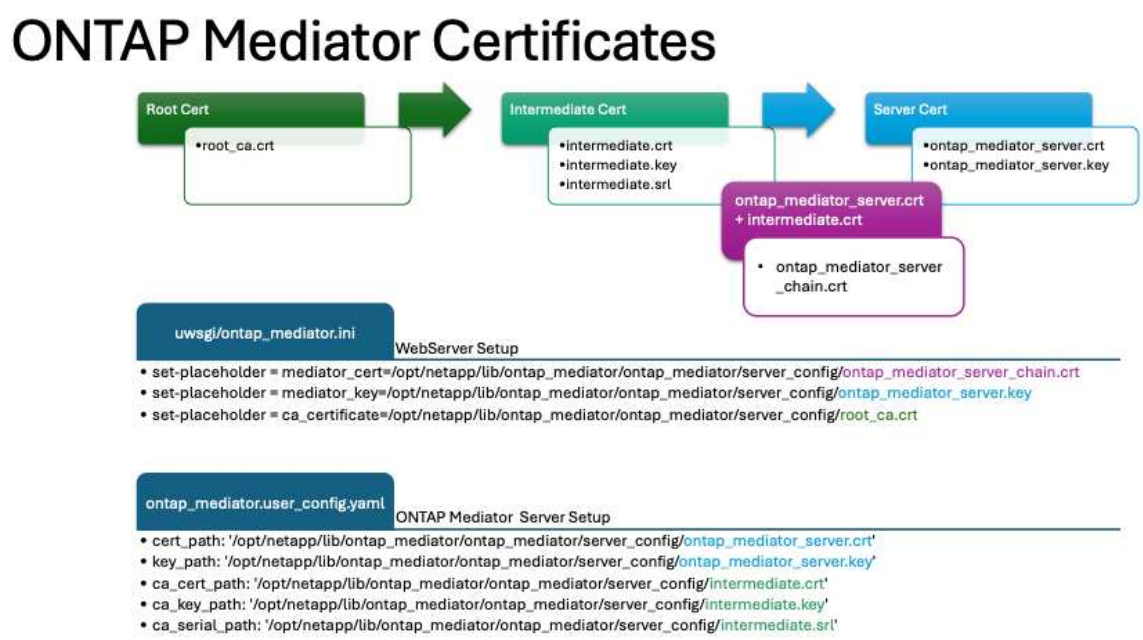
- 僅支援從 ONTAP 9 1.16.1 開始的協力廠商憑證，以及某些較早的 ONTAP 修補程式版本。請參閱。 "NetApp Bug Online Bug ID CONTAP-243278"
- 只有執行 ONTAP Mediator 1.7 或更新版本的系統才支援協力廠商憑證。

關於這項工作

- 在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。
- 如果產生的自我簽署憑證需要由從信任的次級憑證授權單位（ CA ）取得的憑證所取代、您可以執行此工作。若要達成此目標、您應該可以存取信任的公開金鑰基礎架構（ PKI ）授權。
- 下圖顯示每個 ONTAP Mediator 憑證的用途。



- 下圖顯示了 Web 伺服器設定和 ONTAP Mediator 設定的配置。



步驟 **1** ：從發行 **CA** 憑證的協力廠商取得憑證

您可以使用下列程序從 PKI 授權單位取得憑證。

以下範例示範如何以位於的協力廠商憑證參與者取代自我簽署的憑證參與者 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/`。

此範例說明了 ONTAP 調解器所需憑證的必要標準。您可以使用與此程序不同的方式、從 PKI 授權單位取得憑證。根據您的業務需求調整程序。

ONTAP Mediator 1.9 及更新版本

1. 建立私密金鑰 `intermediate.key`和組態檔 `openssl_ca.cnf`，供 PKI 授權單位用來產生憑證。

   a. 產生私密金鑰 `intermediate.key`：

      - 範例 *

```
openssl genrsa -aes256 -out intermediate.key 4096
```

   a. 組態檔案 `openssl_ca.cnf` （位於 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`）定義產生的憑證必須具有的內容。

2. 使用私密金鑰和組態檔案來建立憑證簽署要求 `intermediate.csr`：

   範例：

```
openssl req -key <private_key_name>.key -new -out
<certificate_csr_name>.csr -config <config_file_name>.cnf
```

```
[root@scs000216655 server_config]# openssl req -key intermediate.key
-new -config openssl_ca.cnf -out intermediate.csr
Enter pass phrase for intermediate.key:
[root@scs000216655 server_config]# cat intermediate.csr
-----BEGIN CERTIFICATE REQUEST-----
<certificate_value>
-----END CERTIFICATE REQUEST-----
```

3. 將憑證簽署要求傳送 `intermediate.csr`至 PKI 授權單位以供其簽署。

   PKI 機構驗證請求並簽署 `.csr`，生成證書 `intermediate.crt`。此外，您還需要獲得 `root_ca.crt`簽署的證書 `intermediate.crt`來自 PKI 機構的憑證。

> 對於SnapMirror業務連續性 (SM-BC) 集群，您必須新增 `intermediate.crt`和 `root_ca.crt`證書到ONTAP集群。看"為 SnapMirror 主動同步配置 ONTAP 調解器和集群"。

ONTAP Mediator 1.8 及更早版本

1. 建立私密金鑰 `ca.key`和組態檔 `openssl_ca.cnf`，供 PKI 授權單位用來產生憑證。

   a. 產生私密金鑰 `ca.key`：

      - 範例 *

```
openssl genrsa -aes256 -out ca.key 4096
```

   a. 組態檔案 `openssl_ca.cnf` （位於 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_ca.cnf`）定義產生的憑證必須具有的內容。

2. 使用私密金鑰和組態檔案來建立憑證簽署要求 `ca.csr`：

   範例：

   ```
   openssl req -key <private_key_name>.key -new -out
   <certificate_csr_name>.csr -config <config_file_name>.cnf
   ```

   ```
   [root@scs000216655 server_config]# openssl req -key ca.key -new
   -config openssl_ca.cnf -out ca.csr
   Enter pass phrase for ca.key:
   [root@scs000216655 server_config]# cat ca.csr
   -----BEGIN CERTIFICATE REQUEST-----
   <certificate_value>
   -----END CERTIFICATE REQUEST-----
   ```

3. 將憑證簽署要求傳送 `ca.csr`至 PKI 授權單位以供其簽署。

   PKI 授權單位會驗證要求並簽署 `.csr`、產生憑證 `ca.crt`。此外，您需要從 PKI 授權單位取得 `root_ca.crt that signed the `ca.crt`憑證。

   > 對於 SnapMirror Business Continuity （ SM-BC ）叢集、您必須將和憑證新增 `ca.crt` `root_ca.crt` 至 ONTAP 叢集。請參閱。 "為 SnapMirror 主動同步配置 ONTAP 調解器和集群"

步驟 **2** ：使用協力廠商 **CA** 認證簽署以產生伺服器憑證

ONTAP Mediator 1.9 及更新版本

伺服器憑證必須由私密金鑰和協力廠商憑證 `intermediate.crt`簽署 `intermediate.key`。此外，組態檔案還 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`包含特定屬性，可指定由 OpenSSL 發行的伺服器憑證所需的內容。

下列命令可產生伺服器憑證。

步驟

1. 若要產生伺服器憑證簽署要求（ CSR ）、請從資料夾執行下列命令 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`：

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. 要從 CSR 產生伺服器證書，請從 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`資料夾：

> 這些檔案是從 PKI 授權單位取得的。如果您使用的是不同的憑證名稱，請以相關的檔案名稱取代 `intermediate.crt`和 `intermediate.key`。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA
intermediate.crt -CAkey intermediate.key -CAcreateserial -sha512 -days 1095
-req -in ontap_mediator_server.csr -out ontap_mediator_server.crt
```

。此 `-CAcreateserial`選項用於產生 `intermediate.srl`檔案。

ONTAP Mediator 1.8 及更早版本

伺服器憑證必須由私密金鑰和協力廠商憑證 `ca.crt`簽署 `ca.key`。此外，組態檔案還 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/openssl_server.cnf`包含特定屬性，可指定由 OpenSSL 發行的伺服器憑證所需的內容。

下列命令可產生伺服器憑證。

步驟

1. 若要產生伺服器憑證簽署要求（ CSR ）、請從資料夾執行下列命令 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`：

```
openssl req -config openssl_server.cnf -extensions v3_req -nodes -newkey
rsa:4096 -sha512 -keyout ontap_mediator_server.key -out
ontap_mediator_server.csr
```

2. 要從 CSR 產生伺服器證書，請從 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config`資料夾：

> 這些檔案是從 PKI 授權單位取得的。如果您使用的是不同的憑證名稱，請以相關的檔案名稱取代 `ca.crt`和 `ca.key`。

```
openssl x509 -extfile openssl_server.cnf -extensions v3_req -CA ca.crt
```

```
-CAkey ca.key -CAcreateserial -sha512 -days 1095 -req -in
ontap_mediator_server.csr -out ontap_mediator_server.crt
```

- 此 `-CAcreateserial`選項用於產生 `ca.srl`檔案。

步驟 **3** ：在 **ONTAP Mediator** 組態中取代新的協力廠商 **CA** 憑證和伺服器憑證

ONTAP調解器 1.10 及更高版本

憑證設定透過位於下列位置的設定檔提供給 ONTAP 調解器 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 。檔案包含下列屬性：

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 和 `key_path` 為伺服器憑證變數。
- `ca_cert_path`、`ca_key_path`和 `ca_serial_path` 為 CA 憑證變數。

步驟

1. 以協力廠商憑證取代所有 `intermediate.*` 檔案。
2. 從和憑證建立憑證鏈結 `intermediate.crt` `ontap_mediator_server.crt` ：

   ```
   cat ontap_mediator_server.crt intermediate.crt >
   ontap_mediator_server_chain.crt
   ```

3. 更新 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`文件。

   更新 `ssl_keyfile`， `ssl_certfile` ，和 `ssl_ca_certs`：

   ```
   ssl_keyfile：
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key

   ssl_certfile：
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server_chain.crt

   ssl_ca_certs：
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

- 這 `ssl_keyfile`值是關鍵路徑 `ontap_mediator_server.crt`文件，即 `ontap_mediator_server.key`。
- 這 `ssl_certfile`值是 `ontap_mediator_server_chain.crt`文件。
- 這 `ssl_ca_certs`值是 `root_ca.crt`文件。

4. 確認新產生憑證的下列屬性已正確設定：
   - Linux 群組擁有者： `netapp:netapp`
   - Linux 權限： `600`
5. 重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

ONTAP調解器 1.9.1 和 1.9

憑證設定透過位於下列位置的設定檔提供給 ONTAP 調解器 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml` 。檔案包含下列屬性：

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/intermediate.srl'
```

- `cert_path` 和 `key_path` 為伺服器憑證變數。
- `ca_cert_path`、 `ca_key_path`和 `ca_serial_path` 為 CA 憑證變數。

步驟

1. 以協力廠商憑證取代所有 `intermediate.*` 檔案。
2. 從和憑證建立憑證鏈結 `intermediate.crt` `ontap_mediator_server.crt` ：

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

3. 更新 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 檔案。

更新、和的值 mediator_cert mediator_key ca_certificate：

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- mediator_cert`值是檔案的路徑 `ontap_mediator_server_chain.crt 。
- mediator_key value`是檔案中的金鑰路徑 `ontap_mediator_server.crt ，即 ontap_mediator_server.key。
- ca_certificate`值是檔案的路徑 `root_ca.crt 。

4. 確認新產生憑證的下列屬性已正確設定：
   - Linux 群組擁有者： netapp:netapp
   - Linux 權限： 600
5. 重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

憑證設定透過位於下列位置的設定檔提供給 ONTAP 調解器 /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.config.yaml 。檔案包含下列屬性：

```
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_medi
ator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

- cert_path 和 key_path 為伺服器憑證變數。
- ca_cert_path、 ca_key_path`和 `ca_serial_path 為 CA 憑證變數。

步驟

1. 以協力廠商憑證取代所有 `ca.*` 檔案。
2. 從和憑證建立憑證鏈結 `ca.crt` `ontap_mediator_server.crt` ：

   ```
   cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
   ```

3. 更新 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 檔案。

   更新、和的值 `mediator_cert` `mediator_key` `ca_certificate`：

   ```
   set-placeholder = mediator_cert =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server_chain.crt

   set-placeholder = mediator_key =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator_
   server.key

   set-placeholder = ca_certificate =
   /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
   ```

   - `mediator_cert`值是檔案的路徑 `ontap_mediator_server_chain.crt 。
   - `mediator_key value`是檔案中的金鑰路徑 `ontap_mediator_server.crt ，即 `ontap_mediator_server.key`。
   - `ca_certificate`值是檔案的路徑 `root_ca.crt 。
4. 確認新產生憑證的下列屬性已正確設定：
   - Linux 群組擁有者： `netapp:netapp`
   - Linux 權限： `600`
5. 重新啟動 ONTAP 調解器：

   ```
   systemctl restart ontap_mediator
   ```

步驟 **4** ：選擇性地為協力廠商憑證使用不同的路徑或名稱

ONTAP調解器 1.10 及更高版本

您可以使用名稱不同於其他名稱的協力廠商憑證 `intermediate.*`，或是將協力廠商憑證儲存在不同的位置。

步驟

1. 設定 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` 檔案以覆寫檔案中的預設變數值 `ontap_mediator.config.yaml` 。

   如果您是從 PKI 授權單位取得，並將其私密金鑰儲存在該位置，則 `intermediate.crt` `intermediate.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 檔案應如下例所示：

   > 如果您使用 `intermediate.crt` 來簽署 `ontap_mediator_server.crt` 憑證、`intermediate.srl` 則會產生檔案。如需詳細資訊、請參閱 步驟 2 ：使用協力廠商 CA 認證簽署以產生伺服器憑證 。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 如果您使用的憑證結構 `root_ca.crt`證書提供了 `intermediate.crt`簽署證書 `ontap_mediator_server.crt`證書，從建立證書鏈 `intermediate.crt`和 `ontap_mediator_server.crt`證書：

> 您應該已經從程序稍早的 PKI 授權單位取得 `intermediate.crt` 和 `ontap_mediator_server.crt` 憑證。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. 更新 `/opt/netapp/lib/ontap_mediator/uvicorn/config.json`文件。

更新 ssl_keyfile， ssl_certfile ，和 ssl_ca_certs：

```
ssl_keyfile：
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

ssl_certfile：
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

ssl_ca_certs：
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- 這 ssl_keyfile`值是關鍵路徑 `ontap_mediator_server.crt`文件，即 `ontap_mediator_server.key。
- 這 `ssl_certfile`值是 `ontap_mediator_server_chain.crt`文件。
- 這 `ssl_ca_certs`值是 `root_ca.crt`文件。

> 對於SnapMirror業務連續性 (SM-BC) 集群，您必須新增 `intermediate.crt`和 `root_ca.crt`證書到ONTAP集群。看"為 SnapMirror 主動同步配置 ONTAP 調解器和集群"。

c. 確認新產生憑證的下列屬性已正確設定：

- Linux 群組擁有者： netapp:netapp
- Linux 權限： 600

2. 當設定檔中的憑證更新後，重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

ONTAP調解器 1.9.1 和 1.9

您可以使用名稱不同於其他名稱的協力廠商憑證 intermediate.*，或是將協力廠商憑證儲存在不同的位置。

步驟

1. 設定 /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml 檔案以覆寫檔案中的預設變數值 ontap_mediator.config.yaml 。

   如果您是從 PKI 授權單位取得，並將其私密金鑰儲存在該位置，則 intermediate.crt intermediate.key /opt/netapp/lib/ontap_mediator/ontap_mediator/server_config ontap_mediator.user_config.yaml 檔案應如下例所示：

> 如果您使用 intermediate.crt 來簽署 ontap_mediator_server.crt 憑證、 intermediate.srl 則會產生檔案。如需詳細資訊、請參閱 步驟 2 ：使用協力廠商 CA 認證簽署以產生伺服器憑證 。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/interme
diate.srl'
```

a. 如果您使用的憑證結構 `root_ca.crt`證書提供了 `intermediate.crt`簽署證書 `ontap_mediator_server.crt`證書，從建立證書鏈 `intermediate.crt`和 `ontap_mediator_server.crt`證書：

> 您應該已經從程序稍早的 PKI 授權單位取得 `intermediate.crt` 和 `ontap_mediator_server.crt` 憑證。

```
cat ontap_mediator_server.crt intermediate.crt >
ontap_mediator_server_chain.crt
```

b. 更新 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 檔案。

更新、和的值 `mediator_cert` `mediator_key` `ca_certificate`：

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`值是檔案的路徑 `ontap_mediator_server_chain.crt`。
- 該 `mediator_key` 值是檔案中的金鑰路徑 `ontap_mediator_server.crt` ，即 `ontap_mediator_server.key`。
- `ca_certificate`值是檔案的路徑 `root_ca.crt`。

> 對於SnapMirror業務連續性 (SM-BC) 集群，您必須新增 `intermediate.crt`和 `root_ca.crt`證書到ONTAP集群。看"為 SnapMirror 主動同步配置 ONTAP 調解器和集群"。

c. 確認新產生憑證的下列屬性已正確設定：

- Linux 群組擁有者： `netapp:netapp`
- Linux 權限： `600`

2. 當設定檔中的憑證更新後，重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

ONTAP Mediator 1.8 及更早版本

您可以使用名稱不同於其他名稱的協力廠商憑證 `ca.*`，或是將協力廠商憑證儲存在不同的位置。

步驟

1. 設定 `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediator.user_config.yaml` 檔案以覆寫檔案中的預設變數值 `ontap_mediator.config.yaml`。

   如果您是從 PKI 授權單位取得，並將其私密金鑰儲存在該位置，則 `ca.crt` `ca.key` `/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config` `ontap_mediator.user_config.yaml` 檔案應如下例所示：

> 如果您使用 `ca.crt` 來簽署 `ontap_mediator_server.crt` 憑證、 `ca.srl` 則會產生檔案。如需詳細資訊、請參閱 步驟 2 ：使用協力廠商 CA 認證簽署以產生伺服器憑證。

```
[root@scs000216655 server_config]# cat
ontap_mediator.user_config.yaml

# This config file can be used to override the default settings in
ontap_mediator.config.yaml
# To override a setting, copy the property key from
ontap_mediator.config.yaml to this file and
# set the property to the desired value. e.g.,
#
# The default value for 'default_mailboxes_per_target' is 4 in
ontap_mediator.config.yaml
#
# To override this value with 6 mailboxes per target, add the
following key/value pair
# below this comment:
#
# 'default_mailboxes_per_target': 6
#
cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.crt'
key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_m
ediator_server.key'
ca_cert_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.crt'
ca_key_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.key'
ca_serial_path:
'/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ca.srl'
```

a. 如果您使用的是憑證結構、其中 `root_ca.crt` 的憑證提供 `ca.crt` 簽署憑證的憑證 `ontap_mediator_server.crt` 、請從和憑證建立憑證鏈結 `ca.crt` `ontap_mediator_server.crt` ：

> 您應該已經從程序稍早的 PKI 授權單位取得 `ca.crt` 和 `ontap_mediator_server.crt` 憑證。

```
cat ontap_mediator_server.crt ca.crt > ontap_mediator_server_chain.crt
```

b. 更新 `/opt/netapp/lib/ontap_mediator/uwsgi/ontap_mediator.ini` 檔案。

更新、和的值 `mediator_cert` `mediator_key` `ca_certificate` ：

```
set-placeholder = mediator_cert =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
```

```
or_server_chain.crt

set-placeholder = mediator_key =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/ontap_mediat
or_server.key

set-placeholder = ca_certificate =
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config/root_ca.crt
```

- `mediator_cert`值是檔案的路徑 `ontap_mediator_server_chain.crt`。
- 該 `mediator_key` 值是檔案中的金鑰路徑 `ontap_mediator_server.crt`，即 `ontap_mediator_server.key`。
- `ca_certificate`值是檔案的路徑 `root_ca.crt`。

> 對於 SnapMirror Business Continuity （ SM-BC ）叢集、您必須將和憑證新增 `ca.crt` `root_ca.crt` 至 ONTAP 叢集。請參閱。 "為 SnapMirror 主動同步配置 ONTAP 調解器和集群"

c. 確認新產生憑證的下列屬性已正確設定：

- Linux 群組擁有者： `netapp:netapp`
- Linux 權限： `600`

2. 當設定檔中的憑證更新後，重新啟動 ONTAP 調解器：

```
systemctl restart ontap_mediator
```

疑難排解憑證相關問題

您可以檢查憑證的某些內容。

驗證憑證過期

使用下列命令識別憑證有效範圍。

ONTAP Mediator 1.9 及更新版本

```
[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

ONTAP Mediator 1.8 及更早版本

```
[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        Validity
            Not Before: Feb 22 19:57:25 2024 GMT
            Not After : Feb 15 19:57:25 2029 GMT
```

驗證 CA 認證中的 X509v3 延伸

使用下列命令來驗證 CA 認證中的 X509v3 延伸。

ONTAP Mediator 1.9 及更新版本

中 `openssl_ca.cnf`定義的內容 `**v3_ca**`會顯示為 `X509v3 extensions intermediate.crt`。

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

ONTAP Mediator 1.8 及更早版本

中 `openssl_ca.cnf`定義的內容 `**v3_ca**`會顯示為 `X509v3 extensions ca.crt`。

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_ca.cnf
...
[ v3_ca ]
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, cRLSign, digitalSignature, keyCertSign

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...
        X509v3 extensions:
            X509v3 Subject Key Identifier:

9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27
            X509v3 Authority Key Identifier:

keyid:9F:06:FA:47:00:67:BA:B2:D4:82:70:38:B8:48:55:B5:24:DB:FC:27

            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Digital Signature, Certificate Sign, CRL Sign
```

驗證伺服器憑證和主體替代名稱中的 **X509v3** 副檔名

。 `v3_req` 中定義的內容 `openssl_server.cnf` 組態檔案會顯示為 `X509v3 extensions` 在憑證中。

在下面的例子中，你可以獲取 `alt_names`透過運行命令 `hostname -A`和 `hostname -I`在安裝了 ONTAP Mediator 的 Linux VM 上。

請洽詢您的網路管理員、以取得正確的變數值。

ONTAP Mediator 1.9 及更新版本

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in intermediate.crt
-text -noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

ONTAP Mediator 1.8 及更早版本

```
[root@mediator_host server_config]# pwd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config

[root@mediator_host server_config]# cat openssl_server.cnf
...
[ v3_req ]
basicConstraints       = CA:false
extendedKeyUsage       = serverAuth
keyUsage               = keyEncipherment, dataEncipherment
subjectAltName         = @alt_names

[ alt_names ]
DNS.1 = abc.company.com
DNS.2 = abc-v6.company.com
IP.1 = 1.2.3.4
IP.2 = abcd:abcd:abcd:abcd:abcd:abcd

[root@mediator_host server_config]# openssl x509 -in ca.crt -text
-noout
Certificate:
    Data:
...

        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            X509v3 Extended Key Usage:
                TLS Web Server Authentication
            X509v3 Key Usage:
                Key Encipherment, Data Encipherment
            X509v3 Subject Alternative Name:
                DNS:abc.company.com, DNS:abc-v6.company.com, IP
Address:1.2.3.4, IP Address:abcd:abcd:abcd:abcd:abcd:abcd
```

確認私密金鑰與憑證相符

您可以驗證特定私密金鑰是否與憑證相符。

請分別在金鑰和憑證上使用下列 OpenSSL 命令。

ONTAP Mediator 1.9 及更新版本

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
intermediate.key | openssl md5
Enter pass phrase for intermediate.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
intermediate.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

ONTAP Mediator 1.8 及更早版本

```
[root@mediator_host server_config]# openssl rsa -noout -modulus -in
ca.key | openssl md5
Enter pass phrase for ca.key:
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
[root@mediator_host server_config]# openssl x509 -noout -modulus -in
ca.crt | openssl md5
(stdin)= 14c6b98b0c7c59012b1de89eee4a9dbc
```

如果是 `-modulus` 這兩種配對的屬性都表示私密金鑰與憑證配對是相容的、可以彼此搭配使用。

確認伺服器憑證是從特定 CA 憑證建立

您可以使用下列命令來驗證伺服器憑證是從特定 CA 憑證建立的。

ONTAP Mediator 1.9 及更新版本

```
[root@mediator_host server_config]# openssl verify -CAfile root_ca.crt
--untrusted intermediate.crt ontap_mediator_server.crt
ontap_mediator_server.crt: OK
[root@mediator_host server_config]#
```

ONTAP Mediator 1.8 及更早版本

```
[root@mediator_host server_config]# openssl verify -CAfile ca.crt
ontap_mediator_server.crt
ontap_mediator_server.crt: OK
```

如果正在使用線上憑證狀態通訊協定 (OCSP) 驗證，請使用命令 "openssl 驗證"。

維護 **ONTAP Mediator** 的主機作業系統

確保定期維護ONTAP Mediator 的主機作業系統，以達到最佳效能。

重新啟動主機

僅當叢集健康時才重新啟動主機。當ONTAP調解器處於離線狀態時，叢集無法回應故障。重啟前請設定維護時間。

ONTAP調解器會在重新啟動期間自動恢復，並重新進入與ONTAP叢集先前配置的關係。

主機套件更新

更新核心以外的任何函式庫或 yum 套件。如果需要，請重新啟動主機以使變更生效。在重新啟動主機之前安排服務視窗。

如果您安裝 `yum-utils` 套件中、請使用 `needs-restarting` 偵測是否有任何套件變更需要重新開機的命令。

更新ONTAP調解器相依性後重新啟動，因為變更不會立即生效。

升級主機作業系統內核

SCST 必須針對您使用的核心進行編譯。若要更新作業系統，您需要安排時間進行維護。

步驟

請依照以下步驟升級主機作業系統核心。

> 升級核心之前，請檢查作業系統和ONTAP Mediator 版本是否相容。有關支援的版本，請參閱"作業系統支援對照表"。

1. 停止 ONTAP 調解器。
2. 卸載 SCST 包，請參閱[執行主機維護]。 （SCST 不提供升級機制。）
3. 升級作業系統、然後重新開機。
4. 重新安裝 SCST 套件。
5. 重新啟用 ONTAP 調解器。

執行主機維護

升級 VM 核心可能會導致與 SCST 模組的兼容性問題。手動卸載並重新安裝 SCST。

步驟 **1**：卸載 **SCST**

若要解除安裝 SCST，請使用適合您的ONTAP Mediator 版本的 tar 套件。

步驟

1. 下載適當的 SCST 套件（如下表所示）並解壓縮。

對於此版本 …	使用此 tar 套裝組合 …
ONTAP調解器 1.11	scst-3.9.tar.gz
ONTAP調解器 1.10	scst-3.9.tar.gz
ONTAP調解器 1.9.1	scst-3.8.0.tar.bz2
ONTAP Mediator 1.9	scst-3.8.0.tar.bz2
ONTAP Mediator 1.8	scst-3.8.0.tar.bz2
ONTAP Mediator 1.7	scst-3.7.0.tar.bz2
ONTAP Mediator 1.6	scst-3.7.0.tar.bz2
ONTAP Mediator 1.5	scst-3.6.0.tar.bz2
ONTAP Mediator 1.4	scst-3.6.0.tar.bz2
ONTAP Mediator 1.3	scst-3.5.0.tar.bz2
ONTAP Mediator 1.1	scst-3.4.0.tar.bz2
ONTAP Mediator 1.0	scst-3.3.0.tar.bz2

a. 從訪問開源包"SCST sourceforge 下載"。
b. 選擇*下載已發布版本*。
c. 將捆綁包提取到您的虛擬機器。

2. 在 `scst`目錄：
   a. `systemctl stop mediator-scst`
   b. `make scstadm_uninstall`
   c. `make iscsi_uninstall`
   d. `make usr_uninstall`
   e. `make scst_uninstall`
   f. `depmod`

步驟 2：安裝 SCST

若要手動安裝 SCST，您需要用於已安裝ONTAP Mediator 版本的 SCST tar 套件（請參閱SCST 表）。

在安裝ONTAP調解器之前執行此步驟。如果您使用的 SCST 版本比ONTAP Mediator 安裝程式捆綁的版本新，則安裝程式將跳過此步驟。

1. 在 `scst`目錄：
   a. `make 2release`
   b. `make scst_install`
   c. `make usr_install`
   d. `make iscsi_install`
   e. `make scstadm_install`
   f. `depmod`

      如果您是首次安裝並且想要預先安裝ONTAP Mediator，請在繼續下一步之前執行以下命令：

      ```
      mkdir -p
      /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys
      ```

   g. `cp scst/src/certs/scst_module_key.der /opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/`
   h. `patch /etc/init.d/scst < /opt/netapp/lib/ontap_mediator/systemd/scst.patch`

      如果您在首次安裝期間在ONTAP Mediator 之前預先安裝 SCST，請跳過此步驟。安裝程式應用相關的 SCST 修補程式。

2. 或者、如果已啟用安全開機、請在重新開機之前執行下列步驟：
   a. 確定每個檔名 `scst_vdisk`， `scst` ， 和 `iscsi_scst`模組：

      ```
      [root@localhost ~]# modinfo -n scst_vdisk
      [root@localhost ~]# modinfo -n scst
      [root@localhost ~]# modinfo -n iscsi_scst
      ```

   b. 決定核心版本：

      ```
      [root@localhost ~]# uname -r
      ```

   c. 使用核心對每個模組檔案進行簽名：

```
[root@localhost ~]# /usr/src/kernels/<KERNEL-RELEASE>/scripts/sign-
file \sha256 \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.priv \
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_modu
le_key.der \
_module-filename_
```

d. 使用韌體安裝 UEFI 金鑰。

有關安裝 UEFI 金鑰的說明、請參閱：

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/README.module-
signing
```

產生的 UEFI 金鑰位於：

```
/opt/netapp/lib/ontap_mediator/ontap_mediator/SCST_mod_keys/scst_module_key.de
r
```

3. 重新啟動系統：

```
reboot
```

主機變更為主機名稱或 IP

關於這項工作

- 在安裝了 ONTAP Mediator 的 Linux 主機上執行此任務。
- 只有當自簽章憑證因主機名稱或 IP 位址在安裝ONTAP Mediator 後發生變更而不再有效時，才應執行此操作。
- 臨時自簽名憑證被受信任的第三方憑證取代後，您就不再使用此任務來重新產生憑證。如果您沒有自簽名證書，則無法使用此程序。

步驟

為目前主機建立臨時自簽名憑證：

1. 重新啟動 ONTAP 調解器：

```
./make_self_signed_certs.sh overwrite
```

```
[root@xyz000123456 ~]# cd
/opt/netapp/lib/ontap_mediator/ontap_mediator/server_config
[root@xyz000123456 server_config]# ./make_self_signed_certs.sh overwrite

Adding Subject Alternative Names to the self-signed server certificate
#
# OpenSSL example configuration file.
Generating self-signed certificates
Generating RSA private key, 4096 bit long modulus (2 primes)
.....................................................................
.....................................................................
..................++++
.....................................................++++
e is 65537 (0x010001)
Generating a RSA private key
.................................................++++
.....................................................................
.....................................................................+++
+
writing new private key to 'ontap_mediator_server.key'
-----
Signature ok
subject=C = US, ST = California, L = San Jose, O = "NetApp, Inc.", OU =
ONTAP Core Software, CN = ONTAP Mediator, emailAddress =
support@netapp.com
Getting CA Private Key

[root@xyz000123456 server_config]# systemctl restart ontap_mediator
```

了解使用 ONTAP System Manager 進行 MetroCluster IP 網站管理

MetroCluster 組態會同步鏡射不同位置的兩個 ONTAP 叢集之間的資料和組態。從 ONTAP 9 開始、您可以使用系統管理員做為管理 MetroCluster IP 組態的簡化介面。

> 您只能在 MetroCluster IP 組態中使用系統管理員來執行 MetroCluster 作業。在 MetroCluster FC 組態中、您仍然可以使用系統管理員來管理 MetroCluster 組態中的每個節點、但無法執行任何 MetroCluster 專屬的作業。

一般而言、您可以在兩個不同的地理位置站台中、在 MetroCluster 組態中設定和設定叢集。接著您可以設定叢集之間的對等關係、以便它們同步及共用資料。對等網路中的兩個叢集提供雙向災難恢復（ DR ）、每個叢集都可以是另一個叢集的來源和備份。在八個節點或四個節點的 MetroCluster IP 組態中、每個站台都包含設定為一或兩個高可用度（ HA ）配對的儲存控制器。

您可以"安裝 ONTAP 調解器"在第三個位置監控節點及其 DR 合作夥伴的狀態。ONTAP Mediator 可以在災難發

生時實施調解器輔助計劃外切換 (MAUSO)。

您也可以執行交涉式的轉換、將其中一個叢集關閉以進行規劃的維護。合作夥伴叢集會處理兩個叢集的所有資料 I/O 作業、直到您啟動執行維護的叢集並執行切換作業為止。

您可以在中找到使用系統管理員設定及管理 MetroCluster IP 組態"本文檔MetroCluster"的程序。

使用磁帶備份來保護資料

了解**ONTAP FlexVol**卷的磁帶備份

支援透過網路資料管理傳輸協定（NDMP）進行磁帶備份與還原。ONTAPNDMP可讓您將儲存系統中的資料直接備份到磁帶、進而有效使用網路頻寬。支援傾印和SMTape引擎以進行磁帶備份。ONTAP

您可以使用NDMP相容的備份應用程式來執行傾印或SMTape備份或還原。僅支援NDMP版本4。

使用**dump**進行磁帶備份

dump 是一種快照型備份，可將檔案系統資料備份至磁帶。此資訊可將檔案、目錄及適用的存取控制清單（ACL）資訊備份到磁帶。ONTAP您可以備份整個Volume、整個qtree或子樹、而不是整個Volume或整個qtree。dump支援基礎、差異及遞增備份。

使用**SMTape**備份磁帶

SMTape 是 ONTAP 的快照型災難恢復解決方案，可將資料區塊備份到磁帶。您可以使用SMTaper對磁帶執行Volume備份。不過、您無法在qtree或子樹狀結構層級執行備份。SMTape支援基準備份、差異備份和遞增備份。

從 ONTAP 9.13.1 開始，使用 SMTape 的磁帶備份支援SnapMirror 主動同步。

ONTAP磁帶備份與復原工作流程

您可以使用支援NDMP的備份應用程式來執行磁帶備份與還原作業。

關於這項工作

磁帶備份與還原工作流程提供執行磁帶備份與還原作業所需的工作總覽。如需執行備份與還原作業的詳細資訊、請參閱備份應用程式文件。

步驟

1. 選擇支援NDMP的磁帶拓撲來設定磁帶庫組態。
2. 在儲存系統上啟用NDMP服務。

   您可以在節點層級或儲存虛擬機器（SVM）層級啟用NDMP服務。這取決於您選擇執行磁帶備份與還原作業的NDMP模式。

3. 使用NDMP選項來管理儲存系統上的NDMP。

   您可以在節點層級或SVM層級使用NDMP選項。這取決於您選擇執行磁帶備份與還原作業的NDMP模式。

您可以使用命令在節點層級修改 NDMP 選項，也可以在 SVM 層級使用 `vserver services ndmp modify`命令來修改 `NDMP 選項 `system services ndmp modify`。深入瞭解 `system services ndmp modify`及 `vserver services ndmp modify` "指令參考資料ONTAP"。

4. 使用支援NDMP的備份應用程式執行磁帶備份或還原作業。

   支援傾印和SMTape引擎以進行磁帶備份和還原。ONTAP

   如需使用備份應用程式（也稱為_Data Management Applications_或_DMAs_）執行備份或還原作業的詳細資訊、請參閱備份應用程式文件。

相關資訊

通用NDMP磁帶備份拓撲

瞭FlexVol 解適用於資料區的傾印引擎

ONTAP SMTape 和轉儲備份引擎的用例

支援兩個備份引擎：SMTape和dump。ONTAP您應該瞭解SM磁帶 和傾印備份引擎的使用案例、以協助您選擇備份引擎來執行磁帶備份和還原作業。

可在下列情況下使用傾印：

- 檔案與目錄的直接存取還原（DAR）
- 備份特定路徑中的子目錄或檔案子集
- 在備份期間排除特定檔案和目錄
- 保留備份的時間較長

SM磁帶 可用於下列情況：

- 災難恢復解決方案
- 在還原作業期間、保留備份資料上的重複資料刪除技術節約效益和重複資料刪除設定
- 大型磁碟區的備份

管理磁帶機

了解如何管理ONTAP磁帶驅動器

您可以在執行磁帶備份或還原作業之前、先驗證磁帶庫連線並檢視磁帶機資訊。您可以將非合格的磁帶機模擬到合格的磁帶機、以使用該磁帶機。除了檢視現有的別名之外、您也可以指派和移除磁帶別名。

當您將資料備份到磁帶時、資料會儲存在磁帶檔案中。檔案會標示磁帶檔案的分隔符號、而且檔案沒有名稱。您可以根據磁帶上的位置來指定磁帶檔案。您可以使用磁帶設備來寫入磁帶檔案。讀取磁帶檔案時、您必須指定與寫入磁帶檔案相同壓縮類型的裝置。

您可以使用命令來檢視叢集中磁帶機和媒體更換器的相關資訊、將磁帶機上線並離線、修改磁帶機匣位置、設定及清除磁帶機別名、以及重設磁帶機。您也可以檢視及重設磁帶機統計資料。

如果您想要...	使用此命令...
將磁帶機上線	`storage tape online`
清除磁帶機或媒體更換器的別名	`storage tape alias clear`
啟用或停用磁帶機的磁帶追蹤作業	`storage tape trace`
修改磁帶機匣的位置	`storage tape position`
重設磁帶機	`storage tape reset` 此命令僅適用於進階權限層級。
設定磁帶機或媒體更換器的別名	`storage tape alias set`
使磁帶機離線	`storage tape offline`
檢視所有磁帶機和媒體更換器的相關資訊	`storage tape show`
檢視連接至叢集的磁帶機相關資訊	• `storage tape show-tape-drive` • `system node hardware tape drive show`
檢視連接至叢集的媒體更換器相關資訊	`storage tape show-media-changer`
檢視有關連接至叢集之磁帶機的錯誤資訊	`storage tape show-errors`
查看ONTAP 連接至叢集中每個節點的所有支援且符合資格的磁帶機	`storage tape show-supported-status`
檢視連接至叢集中每個節點的所有磁帶機和媒體更換器別名	`storage tape alias show`
將磁帶機的統計資料讀取重設為零	`storage stats tape zero tape_name` 您必須在節點下使用此命令。

如果您想要...	使用此命令...
檢視ONTAP 支援的磁帶機	`storage show tape supported [-v]` 您必須在節點下使用此命令。您可以使用 `-v` 選項以檢視每個磁帶機的詳細資料。
檢視磁帶設備統計資料、瞭解磁帶效能並檢查使用模式	`storage stats tape tape_name` 您必須在節點下使用此命令。

相關資訊

- "儲存磁帶"
- "儲存磁帶秀"
- "儲存磁帶顯示支援狀態"
- "儲存磁帶顯示磁帶驅動器"
- "儲存磁帶別名清除"
- "儲存磁帶別名集"
- "儲存磁帶別名顯示"
- "儲存磁帶踪跡"

使用不合格的磁帶驅動器進行**ONTAP**磁帶備份

如果儲存系統可以模擬合格的磁帶機、您可以在該系統上使用非合格的磁帶機。然後、它會被視為合格的磁帶機。若要使用非合格的磁帶機、您必須先判斷它是否模擬任何合格的磁帶機。

關於這項工作

非合格的磁帶機是連接至儲存系統的磁帶機、ONTAP 但不受支援或不被支援。

步驟

1. 使用檢視連接至儲存系統的非合格磁帶機 `storage tape show-supported-status` 命令。

   以下命令顯示連接至儲存系統的磁帶機、以及每個磁帶機的支援與資格狀態。也會列出非合格的磁帶機。 `tape_drive_vendor_name` 是連接至儲存系統但不受 ONTAP 支援的非合格磁帶機。

```
cluster1::> storage tape show-supported-status -node Node1

          Node: Node1
                                     Is
          Tape Drive                 Supported  Support Status
          ---------------------      ---------  --------------
          "tape_drive_vendor_name"   false      Nonqualified tape drive
          Hewlett-Packard C1533A     true       Qualified
          Hewlett-Packard C1553A     true       Qualified
          Hewlett-Packard Ultrium 1  true       Qualified
          Sony SDX-300C              true       Qualified
          Sony SDX-500C              true       Qualified
          StorageTek T9840C          true       Dynamically Qualified
          StorageTek T9840D          true       Dynamically Qualified
          Tandberg LTO-2 HH          true       Dynamically Qualified
```

2. 模擬合格的磁帶機。

   "NetApp下載：磁帶設備組態檔案"

相關資訊

- 哪些是合格的磁帶機
- "儲存磁帶顯示支援狀態"

為ONTAP磁帶備份的磁帶磁碟機或媒體更換器指派磁帶別名

為了便於識別裝置、您可以將磁帶別名指派給磁帶機或媒體更換器。別名可在備份裝置的邏輯名稱與永久指派給磁帶機或媒體更換器的名稱之間提供對應關係。

步驟

1. 使用將別名指派給磁帶機或媒體交換器 `storage tape alias set` 命令。

   如"指令參考資料ONTAP"需詳細 `storage tape alias set`資訊，請參閱。

   您可以使用檢視磁帶機的序號（ SN ）資訊 `system node hardware tape drive show` 使用命令及磁帶庫的相關資訊 `system node hardware tape library show` 命令。

   下列命令會將別名設定為連接至節點cluster1-01的磁帶機、序號為SN[123456]L4：

   ```
   cluster-01::> storage tape alias set  -node cluster-01 -name st3
   -mapping SN[123456]L4
   ```

   下列命令會將別名設定為連接至節點cluster1-01的媒體更換器、序號為SN[65432]：

```
cluster-01::> storage tape alias set  -node cluster-01 -name mc1
-mapping SN[65432]
```

相關資訊

- 什麼是磁帶別名
- 移除磁帶別名
- "儲存磁帶別名集"

刪除磁帶磁碟機或媒體更換器的磁帶別名以進行**ONTAP**磁帶備份

您可以使用移除別名 `storage tape alias clear` 磁帶機或媒體更換器不再需要永久性別名時的命令。

步驟

1. 使用從磁帶機或媒體更換器中移除別名 `storage tape alias clear` 命令。

   如"指令參考資料ONTAP"需詳細 `storage tape alias clear`資訊，請參閱。

   下列命令會將別名清除作業的範圍指定至、以移除所有磁帶機的別名 `tape`：

   ```
   cluster-01::>storage tape alias clear -node cluster-01 -clear-scope tape
   ```

完成後

如果您使用NDMP執行磁帶備份或還原作業、則在從磁帶機或媒體更換器移除別名之後、您必須為磁帶機或媒體更換器指派新的別名、才能繼續存取磁帶設備。

相關資訊

- 什麼是磁帶別名
- 指派磁帶別名
- "儲存磁帶別名清除"

啟用或停用**ONTAP**磁帶預留

您可以使用控制 ONTAP 如何管理磁帶裝置保留 `tape.reservations` 選項。根據預設、磁帶保留已關閉。

關於這項工作

如果磁帶機、媒體更換器、橋接器或程式庫無法正常運作、啟用磁帶保留選項可能會造成問題。如果磁帶命令報告設備在沒有其他儲存系統使用設備時已保留、則應停用此選項。

步驟

1. 若要使用SCSI保留/釋放機制或SCSI持續保留sor來停用磁帶保留、請在叢集Shell輸入下列命令：

`options -option-name tape.reservations -option-value {scsi | persistent | off}`

`scsi` 選取 SCSI 保留 / 釋放機制。

`persistent` 選取 SCSI 持續保留。

`off` 停用磁帶保留。

相關資訊

磁帶保留內容

用於驗證磁帶庫連線的**ONTAP**指令

您可以檢視儲存系統與附加至儲存系統之磁帶庫組態之間的連線路徑相關資訊。您可以使用此資訊來驗證磁帶庫組態的連線路徑、或是疑難排解與連線路徑相關的問題。

您可以檢視下列磁帶庫詳細資料、以在新增或建立新的磁帶庫之後、或是在單一路徑或多重路徑存取磁帶庫中還原失敗路徑之後、驗證磁帶庫連線。您也可以在疑難排解路徑相關錯誤或存取磁帶庫失敗時使用此資訊。

- 磁帶庫附加的節點
- 裝置ID
- NDMP 路徑
- 磁帶庫名稱
- 目標連接埠和啟動器連接埠ID
- 單一路徑或多重路徑存取每個目標或FC啟動器連接埠的磁帶庫
- 路徑相關資料完整性詳細資料、例如「路徑錯誤」和「路徑限制」
- LUN群組和LUN數目

如果您想要...	使用此命令...
檢視叢集中磁帶庫的相關資訊	`system node hardware tape library show`
檢視磁帶庫的路徑資訊	`storage tape library path show`
檢視每個啟動器連接埠的磁帶庫路徑資訊	`storage tape library path show-by-initiator`
檢視儲存磁帶庫與叢集之間的連線資訊	`storage tape library config show`

相關資訊

- "儲存磁帶庫配置顯示"
- "系統節點硬體磁帶庫顯示"
- "儲存磁帶庫路徑顯示"

- "儲存磁帶庫路徑按啟動器顯示"

關於磁帶機

了解合格的ONTAP磁帶驅動器

您必須使用已通過測試且發現可在儲存系統上正常運作的合格磁帶機。您可以追蹤磁帶別名、也可以啟用磁帶保留功能、以確保在任何特定時間只有一個儲存系統存取磁帶機。

合格的磁帶機是已通過測試、可在儲存系統上正常運作的磁帶機。您ONTAP 可以使用磁帶組態檔案、將磁帶機限定為現有的版本。

ONTAP磁帶設定檔的格式

磁帶組態檔案格式包含廠商ID、產品ID及磁帶機壓縮類型詳細資料等欄位。此檔案也包含選用欄位、可用於啟用磁帶機的自動載入功能、以及變更磁帶機的命令逾時值。

下表顯示磁帶組態檔的格式：

項目	尺寸	說明
`vendor_id` （字串）	最多8個位元組	所報告的廠商 ID `SCSI Inquiry` 命令。
`product_id`（字串）	最多 16 個位元組	報告的產品 ID `SCSI Inquiry` 命令。
`id_match_size`（數量）		用於偵測要識別之磁帶機的產品ID位元組數、從查詢資料中產品ID的第一個字元開始算起。
`vendor_pretty` （字串）	最多 16 個位元組	如果此參數存在、則由命令顯示的字串指定、 `storage tape show -device-names`；否則，將顯示 INQ_VENDOL_ID 。
`product_pretty`（字串）	最多 16 個位元組	如果此參數存在、則由命令顯示的字串指定、 `storage tape show -device-names`；否則，將顯示 INQ_PRODUCT_ID 。

。 `vendor_pretty` 和 `product_pretty` 欄位為選用欄位、但如果其中一個欄位有值、則另一個欄位也必須有值。

下表說明各種壓縮類型（例如）的說明、密度代碼和壓縮演算法 `l`、 `m`、 `h`和 `a`：

項目	尺寸	說明
`{l	m	h
a}_description=(string)`	最多 24 個位元組	用於 nodesdesh 命令的列印字串、 `sysconfig -t` ，說明特定密度設定的特性。
`{l	m	h
a}_density=(hex codes)`		要在SCSI模式頁區塊描述元中設定的密度程式碼、對應於所需的l、m、h或a密度程式碼
`{l	m	h
a}_algorithm=(hex codes)`		要在SCSI壓縮模式頁面中設定的壓縮演算法、對應於密度代碼和所需的密度特性。

下表說明磁帶組態檔中可用的選用欄位：

欄位	說明
`autoload=(Boolean yes/no)`	此欄位設定為 `yes` 如果磁帶機具有自動載入功能、也就是插入磁帶匣之後、磁帶機就會準備就緒、無需執行 `SCSI load` （起動 / 停止裝置）命令。此欄位的預設值為 `no` 。
`cmd_timeout_0x`	個別逾時值。只有當您想要指定與磁帶驅動程式預設值不同的逾時值時、才必須使用此欄位。範例檔案會列出磁帶機使用的預設SCSI命令逾時值。逾時值可以以分鐘（m）、秒（s）或毫秒（ms）表示。 您不應變更此欄位。

您可以從 NetApp 支援網站下載及查看磁帶組態檔。

磁帶組態檔案格式範例

HP LTO5 Ultrium磁帶機的磁帶組態檔案格式如下：

```
vendor_id= 「 HP 」

product_id="Ultrium 5-SCSI"

id_match_size=9

vendor_pretty= 「 Hewlett-Packard 」
```

product_pretty="LTO-5"

l_description= 「LTO-3 （ro） /4 4/800GB 」

l_density= 0x00

l_algorithm= 0x00

m_description= 「LTO-3 （ro） /4 8/1600GB CMP 」

m_density= 0x00

m_algorithm= 0x01

h_description="LTO-5 1600GB"

h_density=0x58

h_algorithm= 0x00

a_description="LTO-5 3200GB CMP"

a_density=0x58

a_algorithm= 0x01

autoload= 是

相關資訊

- "NetApp工具：磁帶設備組態檔案"
- "儲存磁帶秀"

ONTAP儲存系統如何動態限定磁帶驅動器

儲存系統會將磁帶機的廠商ID和產品ID與磁帶資格表中所含的資訊配對、以動態方式驗證磁帶機的資格。

當您將磁帶機連接至儲存系統時、它會在磁帶探索期間所取得的資訊與內部磁帶鑑定表中的資訊之間尋找廠商ID和產品ID相符的項目。如果儲存系統發現相符項目、則會將磁帶機標示為合格、並可存取磁帶機。如果儲存系統找不到相符項目、磁帶機將維持不合格狀態、且無法存取。

磁帶設備總覽

了解**ONTAP**磁帶設備

磁帶設備是磁帶機的代表。這是磁帶機的特定回退類型與壓縮功能組合。

系統會針對每種回捲類型和壓縮功能組合、建立磁帶設備。因此、磁帶機或磁帶庫可以有多個與其相關聯的磁帶設備。您必須指定要移動、寫入或讀取磁帶的磁帶設備。

當您在儲存系統上安裝磁帶機或磁帶庫時ONTAP 、會建立與磁帶機或磁帶庫相關的磁帶設備。

支援的功能可偵測磁帶機和磁帶庫、並為其指派邏輯編號和磁帶設備。ONTAP將光纖通道、SAS及平行SCSI磁帶機與程式庫連接至介面連接埠時、即可偵測到它們。ONTAP支援介面時、可偵測這些磁碟機。ONTAP

ONTAP磁帶設備名稱的格式

每個磁帶設備都有一個以定義格式顯示的關聯名稱。此格式包含有關裝置類型、快退類型、別名和壓縮類型的資訊。

磁帶設備名稱的格式如下：

`rewind_type st alias_number compression_type`

`rewind_type` 為倒帶類型。

下列清單說明各種快退類型值：

- * r*

  在磁帶完成寫入磁帶檔案後、將其倒帶。ONTAP

- * nr*

  在磁帶完成寫入磁帶檔案後、不能將其倒帶。ONTAP當您想要在同一個磁帶上寫入多個磁帶檔案時、必須使用此快退類型。

- 您

  這是卸載/重新載入快退類型。使用此回捲類型時、磁帶庫會在磁帶到達磁帶檔案結尾時卸載磁帶、然後載入下一個磁帶（如果有）。

  您只能在下列情況下使用此快退類型：

  - 與此裝置相關聯的磁帶機位於磁帶庫中、或是處於磁帶庫模式的媒體交換器中。
  - 與此裝置相關的磁帶機連接至儲存系統。
  - 此磁帶機定義的磁帶庫磁帶順序中、有足夠的磁帶可供您執行作業。

ⓘ 如果您使用無快退裝置錄製磁帶、則必須在讀取之前將磁帶倒帶。

`st` 為磁帶機的標準指定。

`alias_number` 是 ONTAP 指派給磁帶機的別名。當檢測到新的磁帶機時、支援將別名指派給磁帶機。ONTAP ONTAP

`compression_type` 是磁帶上資料密度和壓縮類型的磁碟機專用程式碼。

下列清單說明的各種值 `compression_type`：

- * a *

最高壓縮率

- * h*

  高壓縮

- 米

  中度壓縮

- * l*

  低壓縮

範例

`nrst0a` 在磁帶機 0 上指定使用最高壓縮的無倒帶設備。

磁帶設備清單範例

以下範例顯示與HP Ultrium 2-SCSI相關的磁帶設備：

```
        Tape drive (fc202_6:2.126L1)  HP      Ultrium 2-SCSI
rst0l  -  rewind device,         format is: HP (200GB)
nrst0l -  no rewind device,      format is: HP (200GB)
urst0l -  unload/reload device, format is: HP (200GB)
rst0m  -  rewind device,         format is: HP (200GB)
nrst0m -  no rewind device,      format is: HP (200GB)
urst0m -  unload/reload device, format is: HP (200GB)
rst0h  -  rewind device,         format is: HP (200GB)
nrst0h -  no rewind device,      format is: HP (200GB)
urst0h -  unload/reload device, format is: HP (200GB)
rst0a  -  rewind device,         format is: HP (400GB w/comp)
nrst0a -  no rewind device,      format is: HP (400GB w/comp)
urst0a -  unload/reload device, format is: HP (400GB w/comp)
```

下列清單說明上述範例中的縮寫：

- GB - GB；這是磁帶的容量。
- 搭配壓縮功能；這會顯示壓縮後的磁帶容量。

支援同時運行的**ONTAP**磁帶設備數量

在光纖通道、SCSI或SAS附件的任何組合中、每個儲存系統（每個節點）最多可支援64個同步磁帶機連線、16個中型更換器、以及16個橋接器或路由器裝置。ONTAP

磁帶機或媒體交換器可以是實體或虛擬磁帶庫或獨立裝置中的裝置。

雖然儲存系統可以偵測到64個磁帶機連線、但同時執行的最大備份與還原工作階段數量取決於備份引擎的擴充性限制。

相關資訊

傾印備份與還原工作階段的擴充性限制

磁帶別名

磁帶別名總覽

混疊可簡化裝置識別程序。別名會將磁帶或媒體更換器的實體路徑名稱（PPN）或序號（SN）連結至持續但可修改的別名。

下表說明磁帶別名如何讓您確保磁帶機（或磁帶庫或媒體交換器）永遠與單一別名相關聯：

案例	重新指派別名
系統重新開機時	磁帶機會自動重新指派先前的別名。
當磁帶設備移至另一個連接埠時	別名可調整為指向新位址。
當多個系統使用特定的磁帶設備時	使用者可將所有系統的別名設定為相同。

當您從Data ONTAP f2 8.1.x升級Data ONTAP 至f2 8.2.x時、Data ONTAP 使用的磁帶別名功能會修改現有的磁帶別名。在這種情況下、您可能必須更新備份應用程式中的磁帶別名。

指派磁帶別名可在備份裝置（例如st0或mc1）的邏輯名稱與永久指派給連接埠、磁帶機或媒體更換器的名稱之間提供對應關係。

st0和st00是不同的邏輯名稱。

邏輯名稱和序號僅用於存取裝置。存取裝置之後、它會使用實體路徑名稱傳回所有錯誤訊息。

有兩種名稱可供別名使用：實體路徑名稱和序號。

了解物理路徑名

實體路徑名稱（PPN）是ONTAP 根據連接至儲存系統的SCSI-2/3介面卡或交換器（特定位置）、將資料指派給磁帶機和磁帶庫的數字位址順序。PPNS也稱為電子名稱。

直接附加裝置的 PPNS 使用下列格式： `host_adapter。 device_id_lun`

LUN 值只會顯示於 LUN 值不是零的磁帶與媒體交換器裝置、也就是 LUN 值為零的情況下 `lun` 不顯示 PPN 的一部分。

例如、PPN 8.6表示主機介面卡編號為8、裝置ID為6、邏輯單元編號（LUN）為0。

SAS磁帶設備也是直接附加的設備。例如、PPN 5c-4表示在儲存系統中、SAS HBA連接至插槽5、SAS磁帶連接至SAS HBA的連接埠C、且裝置ID為4。

連接光纖通道交換器的裝置 PPNS 使用下列格式： `switch:port_id。 device_id_lun`

例如、PPN my_switch:5.3L2表示連接至名為my_switch3之交換器連接埠5的磁帶機已設定裝置ID 3、且具有LUN 2。

LUN（邏輯單元編號）由磁碟機決定。Fibre Channel、SCSI磁帶機和程式庫、以及磁碟均具有PPN。

除非交換器名稱變更、磁帶機或磁帶庫移動、或磁帶機或磁帶庫重新設定、否則磁帶機和磁帶庫的PPNS不會變更。PPNS在重新開機後維持不變。例如、如果移除名為my_switch:5.3L2的磁帶機、並將具有相同裝置ID和LUN的新磁帶機連接至交換器my_switch5的連接埠、則可使用my_switch:5.3L2存取新的磁帶機。

了解序號

序號（SN）是磁帶機或媒體轉換器的唯一識別碼。根據SN（而非WWN）產生別名。ONTAP

由於SN是磁帶機或媒體更換器的唯一識別碼、因此無論磁帶機或媒體更換器的多個連線路徑為何、別名都會保持不變。這有助於儲存系統在磁帶庫組態中追蹤相同的磁帶機或媒體更換器。

即使您重新命名磁帶機或媒體轉換器所連接的Fibre Channel交換器、磁帶機或媒體轉換器的SN也不會變更。不過、如果您在磁帶庫中以新的磁帶機取代現有的磁帶機、ONTAP 則由於磁帶機的SN變更、所以會產生新的別名。此外、如果您將現有的磁帶機移至磁帶庫中的新插槽、或重新對應磁帶機的LUN、ONTAP 則會針對該磁帶機產生新的別名。

您必須使用新產生的別名來更新備份應用程式。

磁帶設備的 SN 使用下列格式： `SN[xxxxxxxxxx]L[X]`

`x` 為英數字元和 `Lx` 為磁帶裝置的 LUN 。如果 LUN 為 0 、則為 `Lx` 字串的一部分不會顯示。

每個SN最多包含32個字元；SN的格式不區分大小寫。

配置**ONTAP**多路徑磁帶存取時的注意事項

您可以從儲存系統設定兩條路徑、以存取磁帶庫中的磁帶機。如果其中一條路徑故障、儲存系統可以使用其他路徑存取磁帶機、而不需要立即修復故障路徑。這可確保磁帶作業可以重新啟動。

從儲存系統設定多重路徑磁帶存取時、您必須考量下列事項：

- 在支援LUN對應的磁帶庫中、若要以多重路徑存取LUN群組、LUN對應必須在每個路徑上對稱。

  磁帶機和媒體交換器會指派給磁帶庫中的LUN群組（一組共用相同啟動器路徑集的LUN）。LUN群組中的所有磁帶機都必須可供所有多個路徑上的備份與還原作業使用。

- 從儲存系統最多可設定兩個路徑、以存取磁帶庫中的磁帶機。
- 多重路徑磁帶存取支援負載平衡。預設會停用負載平衡。

在下列範例中、儲存系統會透過兩個啟動器路徑存取LUN群組0：0B和0d。在這兩個路徑中、LUN群組具有相同

的LUN編號、0和LUN數、5。儲存系統只能透過一個啟動器路徑3D存取LUN群組1。

```
STSW-3070-2_cluster::> storage tape library config show

Node                      LUN Group   LUN Count  Library Name  Library
Target Port  Initiator
------------------------ ----------- ---------- -------------
-------------------- -----
STSW-3070-2_cluster-01         0       5          IBM 3573-TL_1
510a09800000412d     0b

0d
                               1       2          IBM 3573-TL_2
50050763124b4d6f     3d

3 entries were displayed
```

相關資訊

- "儲存磁帶庫配置顯示"

了解如何為**ONTAP**儲存系統新增磁帶磁碟機和函式庫

您可以動態新增磁帶機和磁帶庫至儲存系統（無需讓儲存系統離線）。

當您新增新的媒體交換器時、儲存系統會偵測其存在、並將其新增至組態。如果別名資訊中已參照媒體變更器、則不會建立新的邏輯名稱。如果程式庫未被參照、儲存系統會為媒體更換器建立新的別名。

在磁帶庫組態中、您必須在目標連接埠的LUN 0上設定磁帶機或媒體交換器、ONTAP 以便在該目標連接埠上探索所有媒體交換器和磁帶機。

了解**ONTAP**磁帶預留

多個儲存系統可共用對磁帶機、媒體更換器、橋接器或磁帶庫的存取權。磁帶保留功能可針對所有磁帶機、媒體交換器、橋接器和磁帶庫、啟用SCSI保留/釋放機制或SCSI持續保留、確保在任何特定時間只有一個儲存系統存取裝置。

無論是否涉及交換器、共享程式庫中裝置的所有系統都必須使用相同的保留方法。

保留設備的SCSI保留/釋放機制在正常情況下運作良好。不過、在介面錯誤恢復程序期間、保留可能會遺失。如果發生這種情況、除了保留擁有者之外的啟動器也可以存取該裝置。

使用SCSI持續保留所做的保留不受錯誤恢復機制（例如迴圈重設或目標重設）的影響、但是並非所有的裝置都能正確實作SCSI持續保留。

在儲存系統之間傳輸資料

使用 **ndmpcopy** 傳輸**ONTAP**數據

。 ndmpcopy Nodesdesh 命令會在支援 NDMP v4 的儲存系統之間傳輸資料。您可以執行完整和遞增資料傳輸。您可以傳輸完整或部分磁碟區、qtree、目錄或個別檔案。

關於這項工作

使用發行版本的不限次數地進行遞增傳輸（一次完整備份、最多兩次遞增備份）ONTAP 。

從發行版的更新版本開始、遞增式傳輸最多只能有九個層級（一個完整備份、最多九個遞增備份）ONTAP 。

您可以執行 ndmpcopy 在來源與目的地儲存系統的 nodesdesh 命令列、或是既不是資料傳輸來源也不是目的地的儲存系統。您也可以執行 ndmpcopy 在單一儲存系統上、同時是資料傳輸的來源和目的地。

您可以使用中來源和目的地儲存系統的 IPv4 或 IPv6 位址 ndmpcopy 命令。路徑格式為 `/vserver_name/volume_name \[path\]`。

步驟

1. 在來源與目的地儲存系統上啟用NDMP服務：

如果您要在下列位置的來源或目的地執行資料傳輸：	使用下列命令...
SVM範圍的NDMP模式	`vserver services ndmp on` 對於管理 SVM 中的 NDMP 驗證、使用者帳戶是 admin 而且使用者角色是 admin 或 backup。在資料 SVM 中、使用者帳戶是 vsadmin 而且使用者角色是 vsadmin 或 vsadmin-backup 角色：
節點範圍的NDMP模式	`system services ndmp on`

2. 使用在儲存系統內或儲存系統之間傳輸資料 ndmpcopy Nodesdesh以下 的命令：

```
::> system node run -node <node_name> < ndmpcopy [options]
source_IP:source_path destination_IP:destination_path [-mcs {inet|inet6}] [-
mcd {inet|inet6}] [-md {inet|inet6}]
```

在ndmpcopy中不支援DNS名稱。您必須提供來源和目的地的IP位址。來源IP位址或目的地IP位址不支援回送位址（127.0.0.1）。

- 。 ndmpcopy 命令會決定控制連線的位址模式、如下所示：
  - 控制連線的位址模式會對應所提供的IP位址。
  - 您可以使用來覆寫這些規則 -mcs 和 -mcd 選項：
- 如果來源或目的地是ONTAP 指不支援的系統、則視NDMP模式（節點範圍或SVM範圍）而定、請使用允許存取目標Volume的IP位址。

- source_path 和 destination_path 是磁碟區、 qtree 、目錄或檔案精細層級之前的絕對路徑名稱。
- -mcs 指定與來源儲存系統的控制連線的慣用定址模式。

  inet 表示 IPv4 位址模式和 inet6 表示 IPv6 位址模式。
- -mcd 指定與目的地儲存系統的控制連線的慣用定址模式。

  inet 表示 IPv4 位址模式和 inet6 表示 IPv6 位址模式。
- -md 指定來源與目的地儲存系統之間資料傳輸的慣用定址模式。

  inet 表示 IPv4 位址模式和 inet6 表示 IPv6 位址模式。

  如果您不使用 -md 中的選項 ndmpcopy 命令時、資料連線的定址模式如下所示：

  - 如果為控制連線指定的任一位址是IPv6位址、則資料連線的位址模式為IPv6。
  - 如果控制連線指定的兩個位址都是 IPv4 位址、則為 ndmpcopy 命令會先嘗試資料連線的 IPv6 位址模式。

    如果失敗、命令會使用IPv4位址模式。

    如果指定IPv6位址、則必須以方括弧括住。

    此範例命令會從來源路徑移轉資料 (source_path）到目的地路徑 (destination_path）。

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password>
 -st md5 -dt md5 192.0.2.129:/<src_svm>/<src_vol>
192.0.2.131:/<dst_svm>/<dst_vol>
```

+
此命令範例明確設定控制連線和資料連線、以使用IPv6位址模式：

```
> ndmpcopy -sa admin:<ndmp_password> -da admin:<ndmp_password> -st md5
-dt md5 -mcs inet6 -mcd inet6 -md
 inet6 [2001:0db8:1:1:209:6bff:feae:6d67]:/<src_svm>/<src_vol>
[2001:0ec9:1:1:200:7cgg:gfdf:7e78]:/<dst_svm>/<dst_vol>
```

如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

ndmpcopy命令的選項

您應該瞭解 Nodesdesh 命令可用於成功的選項 `ndmpcopy`"傳輸資料"。

下表列出可用的選項。

選項	說明
-sa username：[password]	此選項可設定來源驗證使用者名稱和密碼、以連線至來源儲存系統。這是必填選項。 對於沒有管理權限的使用者、您必須指定使用者系統產生的NDMP專屬密碼。系統產生的密碼對管理員和非管理員使用者都是必填的。
-da username：[password]	此選項可設定用於連線至目的地儲存系統的目的地驗證使用者名稱和密碼。這是必填選項。
-st {md5	text}
此選項可設定連線至來源儲存系統時所使用的來源驗證類型。這是必要選項、因此使用者應提供 text 或 md5 選項。	-dt {md5
text}	此選項可設定連線至目的地儲存系統時要使用的目的地驗證類型。
-l	此選項會將用於傳輸的傾印層級設定為指定的層級值。有效值為 0、 1、至 9、其中 0 表示完整傳輸和 1 至 9 指定遞增傳輸。預設值為 0。
-d	此選項可產生ndmpcopy除錯記錄訊息。ndmpcopy 除錯記錄檔位於中 /mroot/etc/log 根 Volume 。ndmpcopy 除錯記錄檔名稱位於中 ndmpcopy.yyyymmdd 格式。
-f	此選項可啟用強制模式。此模式可在中覆寫系統檔案 /etc 位於 7-Mode 磁碟區根目錄的目錄。
-h	此選項會列印說明訊息。
-p	此選項會提示您輸入來源和目的地授權的密碼。此密碼會覆寫指定的密碼 -sa 和 -da 選項： 只有當命令在互動式主控台中執行時、才能使用此選項。
-exclude	此選項會將指定的檔案或目錄排除在資料傳輸所指定的路徑之外。該值可以是以逗號分隔的目錄或檔案名稱清單，例如 **.pst`**或 `.txt。支援的最大排除模式數為 32 ，支援的最大字元數為 255 。

NDMP for FlexVol 需求

了解ONTAP FlexVol卷的 NDMP

網路資料管理傳輸協定（NDMP）是一種標準化的傳輸協定、用於控制主要與次要儲存設備（例如儲存系統和磁帶庫）之間的備份、還原及其他類型的資料傳輸。

藉由在儲存系統上啟用NDMP支援、您可以讓該儲存系統與支援NDMP的網路附加備份應用程式（也稱為_Data Management Applications_或_DMAs_）、資料伺服器和參與備份或還原作業的磁帶伺服器進行通訊。所有網路通訊都是透過TCPIP或TCP/IP / IPv6網路進行。NDMP也提供對磁帶機和中型更換器的低階控制。

您可以在節點範圍NDMP模式或儲存虛擬機器（SVM）範圍NDMP模式下執行磁帶備份與還原作業。

使用NDMP時、您必須注意必須考量的事項、環境變數清單、以及支援的NDMP磁帶備份拓撲。您也可以啟用或停用增強的DAR功能。驗證ONTAP NDMP存取儲存系統時、支援的兩種驗證方法為：純文字和挑戰。

相關資訊

支援的環境變數ONTAP

關於NDMP操作模式

了解ONTAP NDMP 操作模式

您可以選擇在節點層級或儲存虛擬機器（ SVM ）層級執行磁帶備份與還原作業。若要在SVM層級成功執行這些作業、必須在SVM上啟用NDMP服務。

如果您從Data ONTAP NetApp 8.2升級Data ONTAP 至更新版本8.3、則在從8.2升級至8.3後、8.2中使用的NDMP操作模式將繼續保留。

如果您安裝的新叢集Data ONTAP 採用了SVM範圍的NDMP模式、則NDMP預設為SVM範圍的NDMP模式。若要在節點範圍的NDMP模式中執行磁帶備份與還原作業、您必須明確啟用節點範圍的NDMP模式。

了解節點範圍的ONTAP NDMP 模式

在節點範圍的NDMP模式中、您可以在節點層級執行磁帶備份與還原作業。從8.2升級到8.3後、將繼續保留在用作執行動作的NDMP模式。Data ONTAP

在節點範圍的NDMP模式中、您可以在擁有該磁碟區的節點上執行磁帶備份與還原作業。若要執行這些作業、您必須在擁有磁碟區或磁帶裝置的節點上、於裝載LIF上建立NDMP控制連線。

此模式已過時、將在未來的主要版本中移除。

了解 SVM 範圍的ONTAP NDMP 模式

如果在SVM上啟用NDMP服務、您可以在儲存虛擬機器（SVM）層級成功執行磁帶備份與還原作業。如果備份應用程式支援駕駛室內擴充、您可以備份及還原叢集SVM不同節點上託管的所有Volume。

您可以在不同的LIF類型上建立NDMP控制連線。在SVM範圍的NDMP模式中、這些LIF屬於資料SVM或管理SVM。只有在擁有此LIF的SVM上啟用NDMP服務時、才能在LIF上建立連線。

資料LIF屬於資料SVM、而叢集間LIF、節點管理LIF及叢集管理LIF則屬於管理SVM。

在SVM範圍的NDMP模式中、磁碟區和磁帶設備的備份與還原作業可用度取決於建立NDMP控制連線的LIF類型、以及電纜擴充的狀態。如果您的備份應用程式支援CAB擴充功能、而且磁碟區和磁帶設備共用相同的關聯性、則備份應用程式可以執行本機備份或還原作業、而非三向備份或還原作業。

相關資訊

管理節點範圍NDMP模式的命令

使用**ONTAP NDMP** 服務時的注意事項

在儲存系統上啟動NDMP服務時、您必須考量許多因素。

- 每個節點最多可支援16個並行備份、還原、或使用連接的磁帶機結合使用兩個節點。
- NDMP服務可應NDMP備份應用程式的要求、產生檔案歷程記錄資料。

  備份應用程式會使用檔案歷程記錄、以最佳化方式從備份映像還原所選的資料子集。對於儲存系統和備份應用程式而言、產生和處理檔案歷程記錄可能會耗費大量時間和CPU資源。

  SMTape不支援檔案歷程記錄。

  如果您的資料保護設定為災難恢復（即恢復整個備份映像）、您可以停用產生檔案歷史記錄、以縮短備份時間。請參閱備份應用程式文件、以判斷是否可以停用產生NDMP檔案歷程記錄。

- NDMP的防火牆原則預設會在所有LIF類型上啟用。
- 在節點範圍的NDMP模式中、若要備份FlexVol 某個支援區、您必須使用備份應用程式、在擁有該磁碟區的節點上啟動備份。

  不過、您無法備份節點根磁碟區。

- 您可以在防火牆原則允許的情況下、從任何LIF執行NDMP備份。

  如果您使用資料LIF、則必須選取未設定容錯移轉的LIF。如果資料LIF在NDMP作業期間容錯移轉、NDMP作業就會失敗、必須重新執行。

- 在節點範圍的NDMP模式和儲存虛擬機器（SVM）範圍NDMP模式中、NDMP資料連線使用與NDMP控制連線相同的LIF。
- 在LIF移轉期間、持續的備份與還原作業會中斷。

  在LIF移轉之後、您必須啟動備份與還原作業。

- NDMP 備份路徑的格式為 */vserver_name/volume_name/path_name*。

  `*path_name*`為選用，並指定目錄，檔案或快照的路徑。

- 使用傾印引擎將SnapMirror目的地備份至磁帶時、只會備份磁碟區中的資料。

  不過、如果SnapMirror目的地是使用SMTape備份到磁帶、則中繼資料也會備份。SnapMirror關係及相關的中繼資料不會備份到磁帶。因此、在還原期間、只會還原該磁碟區上的資料、但不會還原相關的SnapMirror關係。

相關資訊

叢集感知備份擴充的功能

"系統管理"

環境變數

了解**ONTAP NDMP** 支援的環境變量

環境變數用於在啟用NDMP的備份應用程式與儲存系統之間、傳達備份或還原作業的相關資訊。

例如、如果使用者指定備份應用程式應備份 `/vserver1/vol1/dir1`**備份應用程式會將檔案系統環境變數設為** `/vserver1/vol1/dir1`。同樣地、如果使用者指定備份應為層級1備份、則備份應用程式會將層級環境變數設為1（一）。

環境變數的設定與檢查通常對備份管理員來說是透明的、也就是備份應用程式會自動設定。

備份管理員很少指定環境變數；不過、您可能想要變更備份應用程式所設定的環境變數值、以描述或解決功能性或效能問題。例如、系統管理員可能想要暫時停用檔案歷程記錄產生功能、以判斷備份應用程式處理檔案歷程記錄資訊是否造成效能問題或功能問題。

許多備份應用程式都能提供方法來覆寫或修改環境變數、或是指定其他環境變數。如需相關資訊、請參閱備份應用程式文件。

支援的環境變數**ONTAP**

ONTAP支援環境變量，這些變數具有相關的預設值。但是，您可以手動修改這些預設值。

如果您手動修改備份應用程式所設定的值、應用程式的行為可能無法預測。這是因為備份或還原作業可能無法執行備份應用程式所期望的作業。但在某些情況下、審慎的修改可能有助於找出或解決問題。

下表列出傾印和SMTape常見的環境變數、以及僅支援傾印和SMTape的變數。這些表格也說明ONTAP 如何使用支援的環境變數：

在大多數情況下、具有值的變數、 `Y` 也接受 `T` 和 `N` 也接受 `F`。

轉儲和**SMTape**支援的環境變數

環境變數	有效值	預設	說明
偵錯	`Y` 或 `N`	`N`	指定列印偵錯資訊。
檔案系統	`string`	`none`	指定要備份之資料的根目錄路徑名稱。

環境變數	有效值	預設	說明
NDMP版本	`return_only`	`none`	您不應該修改NDMP版本變數。透過備份作業建立的NDMP版本變數會傳回NDMP版本。 在備份期間、將NDMP版本變數設定為供內部使用、並將其傳遞至備份應用程式以供參考。ONTAPNDMP工作階段的NDMP版本並未使用此變數設定。
PathName_分隔 符號	`return_value`	`none`	指定路徑名稱分隔符號字元。 此字元取決於要備份的檔案系統。對於這個變數、會指派字元「'/'」ONTAP。NDMP伺服器會先設定此變數、再開始磁帶備份作業。
類型	`dump` 或 `smtape`	`dump`	指定執行磁帶備份與還原作業所支援的備份類型。
詳細資訊	`Y` 或 `N`	`N`	在執行磁帶備份或還原作業時增加記錄訊息。

支援傾印的環境變數

環境變數	有效值	預設	說明
ACL_start	`return_only`	`none`	由備份作業所建立的acl_start變數是直接存取還原或可重新啟動NDMP備份作業所使用的偏移值。 偏移值是傾印檔案中的位元組偏移值、ACL資料（傳遞V）會在備份結束時開始傳回。若要讓直接存取還原作業正確還原備份資料、則必須在開始還原作業時、將ACL_start值傳遞給還原作業。NDMP可重新啟動的備份作業會使用ACL_start值、與備份串流的非重新啟動部分開始的備份應用程式進行通訊。
基準日期	`0`、 `-1`或 `DUMP_DATE` 價值	`-1`	指定遞增備份的開始日期。 設定為時 `-1`， base_date 遞增說明符被禁用。設定為時 `0` 在 0 級備份中、會啟用遞增備份。在初始備份之後、先前遞增備份中的dump日期變數值會指派給base日期變數。 這些變數是層級/更新型遞增備份的替代方案。
直接	`Y` 或 `N`	`N`	指定還原應直接快轉至檔案資料所在磁帶上的位置、而非掃描整個磁帶。 為了讓直接存取恢復正常運作、備份應用程式必須提供定位資訊。如果此變數設為 `Y`，備份應用程式會指定檔案或目錄名稱及定位資訊。
DMP_NAME	`string`	`none`	指定多個子樹備份的名稱。 此變數是多個子樹狀結構備份的必要項目。

環境變數	有效值	預設	說明
dump日期	`return_value`	`none`	您不會直接變更此變數。如果 base_date 變數設為以外的值、則會由備份建立 `-1`。 dump日期變數的衍生方式是將32位元層級值預先置於傾印軟體所計算的32位元時間值。層級會從傳入base日期變數的最後一個層級值遞增。產生的值會做為後續遞增備份的base日期值。
已啟用增強型_DAR	`Y` 或 `N`	`N`	指定是否啟用增強的DAR功能。增強的DAR功能可支援目錄DAR和含有NT串流的檔案DAR。它可提升效能。 只有在符合下列條件時、才能在還原期間增強DAR： • 支援增強的DAR。ONTAP • 備份期間會啟用檔案歷程記錄（HIST=Y）。 • 。`ndmpd.offset_map.enable` 選項設定為 `on`。 • enabled_DAR 變數設為 `Y` 還原期間。

環境變數	有效值	預設	說明
排除	`pattern_string`	`none`	指定備份資料時排除的檔案或目錄。 排除清單是以逗號分隔的檔案或目錄名稱清單。如果檔案或目錄的名稱符合清單中的其中一個名稱、則會從備份中排除。 在排除清單中指定名稱時、適用下列規則： • 必須使用檔案或目錄的確切名稱。 • 通配符星號（*）必須是字串的第一個或最後一個字元。 每個字串最多可有兩個星號。 • 檔案或目錄名稱中的逗號必須以反斜槓開頭。 • 排除清單最多可包含32個名稱。 如果您將non-quota樹狀結構設為、則不會排除指定要排除備份的檔案或目錄 `Y` 同時。

環境變數	有效值	預設	說明
擷取	Y、 N`或 `E	N	指定要還原備份資料集的子樹狀結構。 備份應用程式會指定要擷取的子樹狀結構名稱。如果指定的檔案符合其內容已備份的目錄、則會以遞歸方式擷取該目錄。 若要在還原期間重新命名檔案、目錄或 qtree 而不使用 DAR 、您必須將 Extract 環境變數設為 E。
Extract（擷取ACL）	Y 或 N	Y	指定在還原作業中還原備份檔案的ACL。 預設值是在還原資料時還原ACL、但DARs（DIRECT = Y）除外。
力	Y 或 N	N	決定還原作業是否必須檢查目的地磁碟區上的磁碟區空間和inode可用度。 將此變數設為 Y 使還原作業略過檢查目的地路徑上的磁碟區空間和 inode 可用度。 如果目的地Volume上沒有足夠的磁碟區空間或inode可用、還原作業會恢復目的地Volume空間和inode可用度所允許的資料量。當磁碟區空間或inode無法使用時、還原作業會停止。

環境變數	有效值	預設	說明
Hist	`Y` 或 `N`	`N`	指定將檔案歷程記錄資訊傳送至備份應用程式。 大多數商業備份應用程式都會將 HIST 變數設為 `Y`。如果您想要提高備份作業的速度、或是想要疑難排解檔案歷程記錄集合的問題、您可以將此變數設為 `N`。 您不應將 HIST 變數設為 `Y` 如果備份應用程式不支援檔案歷程記錄。

環境變數	有效值	預設	說明
Ignore（忽略）_CTIME	`Y` 或 `N`	`N`	指定檔案在上次遞增備份之後、只有其ctime值變更時、才會遞增備份。 有些應用程式（例如掃毒軟體）會變更inode內檔案的ctime值、即使檔案或其屬性尚未變更。因此、遞增備份可能會備份尚未變更的檔案。。 `IGNORE_CTIME` 只有在增量備份因 ctime 值被修改而佔用不可接受的時間或空間時、才應指定變數。

環境變數	有效值	預設	說明
ignore qtree	`Y` 或 `N`	`N`	指定還原作業不會從備份的qtree還原qtree資訊。
層級	`0-31`	`0`	指定備份層級。 層級0會複製整個資料集。遞增備份層級（以0以上的值指定）、複製自上次遞增備份以來的所有檔案（新增或修改的）。例如、層級1會自層級0備份後備份新的或修改過的檔案、層級2會備份自層級1備份以來的新檔案或修改過的檔案、依此類推。
清單	`Y` 或 `N`	`N`	列出備份的檔案名稱和inode編號、而不實際還原資料。
list_qtree	`Y` 或 `N`	`N`	列出備份的qtree、但不實際還原資料。
多重樹狀結構名稱	`string`	`none`	指定備份是多個子樹狀結構備份。 字串中會指定多個子樹狀結構、此字串是以新行分隔、以null終止的子樹狀結構名稱清單。子樹是以與其一般根目錄相關的路徑名稱來指定、必須將其指定為清單的最後一個元素。 如果您使用此變數、也必須使用DMP_name變數。
NDMP、UNICODE、全高	`Y` 或 `N`	`N`	指定除了檔案歷程記錄資訊中檔案的NFS名稱之外、還要包含一個統一碼名稱。 大多數備份應用程式不會使用此選項、除非備份應用程式是設計來接收這些額外的檔案名稱、否則不應設定此選項。也必須設定HIST變數。
			問題、`IGNORE_CTIME` 在

環境變數	有效值	預設	說明
否_ACLS	Y 或 N	N	指定在備份資料時、不得複製ACL。
非配額樹狀結構	Y 或 N	N	指定在備份資料時、必須忽略qtree中的檔案和目錄。 設定為時 Y，不備份檔案系統變數所指定資料集中 qtree 中的項目。只有檔案系統變數指定整個Volume時、此變數才會生效。非配額樹狀結構變數僅適用於層級0備份、如果指定了多重樹狀結構名稱變數、則無法運作。 如果您將non-quota樹狀結構設為、則不會排除指定要排除備份的檔案或目錄 Y 同時。
NOWRITE	Y 或 N	N	指定還原作業不得將資料寫入磁碟。 此變數用於偵錯。

環境變數	有效值	預設	說明
循環	`Y` 或 `N`	`Y`	指定展開DAR還原期間的目錄項目。 必須啟用直接和強化的 DAR 環境變數（設為 `Y` ）。如果已停用遞迴變數（設為 `N`），只有原始來源路徑中所有目錄的權限和 ACL 會從磁帶還原，而非從目錄的內容還原。如果遞歸變數設為 `N` 或 recover_full 路徑變數設為 `Y`，恢復路徑必須以原始路徑結尾。 如果停用循環變數、且有多個恢復路徑、則所有恢復路徑都必須包含在恢復路徑中最長的路徑內。否則會顯示錯誤訊息。 例如、下列是有效的恢復路徑、因為所有的恢復路徑都在內 `foo/dir1/deepdir/myfile`： • `/foo` • `/foo/dir` • `/foo/dir1/deepdir` • `/foo/dir1/deepdir/myfile` 下列是無效的還原路徑： • `/foo` • `/foo/dir` • `/foo/dir1/myfile` • `/foo/dir2` • `/foo/dir2/myfile`

環境變數	有效值	預設	說明
recover_full路徑	`Y` 或 `N`	`N`	指定完整還原路徑在DAR之後將恢復其權限和ACL。 必須啟用 Direct 和 Enhanced DAR （直接和增強）（設為 `Y`）。如果 recover_full 路徑設為 `Y`，恢復路徑必須以原始路徑結尾。如果目的地磁碟區上已存在目錄、則其權限和ACL將不會從磁帶還原。
更新	`Y` 或 `N`	`Y`	更新中繼資料資訊、以啟用層級式遞增備份。

SMTape支援的環境變數

環境變數	有效值	預設	說明
基準日期	`DUMP_DATE`	`-1`	指定遞增備份的開始日期。 `BASE_DATE`是參考快照識別碼的字串表示。`SMTape` 會使用 `BASE_DATE`字串來尋找參考快照。 `BASE_DATE` 基準備份不需要。對於遞增備份、的值 `DUMP_DATE` 先前基準或遞增備份的變數會指派給 `BASE_DATE` 變動。 備份應用程式會指派 `DUMP_DATE` 來自先前 SMTape 基準或遞增備份的價值。

環境變數	有效值	預設	說明
dump日期	return_value	none	SMTape 備份結束時，dump 日期包含字串識別碼，可識別用於該備份的快照。此快照可作為後續遞增備份的參考快照。 dump日期的結果值將用作後續遞增備份的base日期值。
SMTAPE_backup_Set_ID	string	none	識別與基準備份相關的遞增備份順序。 備份集ID是在基礎備份期間產生的128位元唯一ID。備份應用程式會將此 ID 指派為的輸入 SMTAPE_BACKUP_SET_ID 遞增備份期間的變數。
SMTAPE_snapshot名稱	Volume 中可用的任何有效快照	Invalid	當 SMTAPE_Snapshot_name 變數設定為快照時，該快照及其舊快照會備份到磁帶。 對於增量備份，此變數會指定遞增快照。base_date 變數提供基準快照。
SMTAPE_DELETE快照	Y 或 N	N	對於 SMTape 自動建立的快照，當 SMTAPE_DELETE _snapshot 變數設為 `Y`時，則 SMTape 會在備份作業完成後刪除此快照。不過，由備份應用程式建立的快照將不會刪除。
SMTAPE_中斷 鏡射	Y 或 N	N	當 SMTAPE_BREAT_mirror 變數設為時 Y，類型的 Volume DP 變更為 A RW 磁碟區。

了解常見的**ONTAP NDMP** 磁帶備份拓撲

NDMP支援備份應用程式與儲存系統之間的多種拓撲和組態、或是提供資料（檔案系統）

和磁帶服務的其他NDMP伺服器。

儲存系統對本機磁帶

在最簡單的組態中、備份應用程式會將資料從儲存系統備份到連接至儲存系統的磁帶子系統。NDMP控制連線存在於整個網路邊界。儲存系統內資料與磁帶服務之間的NDMP資料連線稱為NDMP本機組態。

儲存系統與磁帶連接至另一個儲存系統

備份應用程式也可以將資料從儲存系統備份到連接至另一個儲存系統的磁帶庫（具有一或多個磁帶機的媒體交換器）。在此情況下、資料與磁帶服務之間的NDMP資料連線是由TCP或TCP/IP網路連線所提供。這稱為NDMP三向儲存系統對儲存系統組態。

儲存系統對網路附加磁帶庫

支援NDMP的磁帶庫提供三向組態的變化。在此情況下、磁帶庫會直接連接至TCP/IP網路、並透過內部NDMP伺服器與備份應用程式和儲存系統通訊。

儲存系統對資料伺服器對磁帶或資料伺服器對儲存系統對磁帶

NDMP也支援儲存系統對資料伺服器和資料伺服器對儲存系統的三向組態、不過這些變種部署的範圍較少。儲存系統對伺服器可將儲存系統資料備份到附加至備份應用程式主機或其他資料伺服器系統的磁帶庫。伺服器對儲存系統組態可讓伺服器資料備份到儲存系統附加的磁帶庫。

ONTAP支援的 NDMP 身份驗證方法

您可以指定驗證方法來允許NDMP連線要求。支援兩種方法來驗證儲存系統的NDMP存取：純文字和挑戰。ONTAP

在節點範圍的NDMP模式中、挑戰和純文字都預設為啟用。不過、您無法停用挑戰。您可以啟用及停用純文字。在純文字驗證方法中、登入密碼會以純文字傳輸。

在儲存虛擬機器（SVM）範圍的NDMP模式中、驗證方法預設是挑戰。與節點範圍的NDMP模式不同、在此模式中、您可以啟用和停用純文字和挑戰驗證方法。

相關資訊

節點範圍NDMP模式中的使用者驗證

SVM範圍NDMP模式中的使用者驗證

支援NDMP擴充功能ONTAP

NDMP v4提供建立NDMP v4傳輸協定延伸的機制、無需修改核心NDMP v4傳輸協定。您應該注意ONTAP 到支援的NDMP v4副檔名。

下列NDMP v4副檔名受ONTAP 支援：

- 叢集感知備份（CAB）

  此擴充僅在SVM範圍的NDMP模式中受支援。

- 連線位址擴充（CAE）以支援IPv6
- 副檔名類別0x2050

  此擴充支援可重新程式化的備份作業和Snapshot Management Extensions。

  此 `NDMP_SNAP_RECOVER`訊息是 Snapshot Management Extensions 的一部分，用於啟動恢復作業，並將恢復的資料從本機快照傳輸至本機檔案系統位置。在本訊息中、此訊息僅允許恢復磁碟區和一般檔案。ONTAP

  此 `NDMP_SNAP_DIR_LIST`訊息可讓您瀏覽磁碟區的快照。如果在瀏覽作業進行期間執行不中斷營運、則備份應用程式必須重新啟動瀏覽作業。

- NDMP 可重啟備份擴展

  您可以使用NDMP可重新啟動的備份擴充（RBE）功能、在故障發生之前、從資料串流中已知的檢查點重新啟動備份。

了解**ONTAP NDMP** 的增強型 **DAR** 功能

您可以將增強的直接存取還原（DAR）功能用於檔案和NT串流的目錄DAR和DAR。預設會啟用增強的DAR功能。

啟用增強的DAR功能可能會影響備份效能、因為必須建立偏移對應並寫入磁帶。您可以在節點範圍和儲存虛擬機器（SVM）範圍NDMP模式中啟用或停用增強的DAR。

NDMP 會話的**ONTAP**可擴展性限制

您必須注意可在不同系統記憶體容量的儲存系統上同時建立的NDMP工作階段數量上限。此最大值取決於儲存系統的系統記憶體。

下表所述限制適用於NDMP伺服器。「傾印備份與還原工作階段的可調整性限制」一節中提到的限制、適用於傾印與還原工作階段。

傾印備份與還原工作階段的擴充性限制

儲存系統的系統記憶體	**NDMP**工作階段的最大數目
少於16 GB	8.
大於或等於16 GB但小於24 GB	20.
大於或等於24 GB	36.

您可以使用命令（可透過 nodesdeshed 取得）來取得儲存系統的系統記憶體 `sysconfig -a`。如"指令參考資料ONTAP"需詳細 `sysconfig -a`資訊，請參閱。

了解ONTAP FlexGroup卷的 NDMP 支持

從支援支援NDMP的ONTAP 功能到支援FlexGroup 不支援的功能、從功能區9.7開始。

從ONTAP 使用支援的版本為2、7、7、2、5、2 FlexVol 、FlexGroup 5、2、2、5、2、5、2、5、2、5、2、5、2

如果您從ONTAP 還原9.7回復至舊版、先前傳輸的遞增傳輸資訊將不會保留、因此您必須在還原後執行基礎複本。

從功能不完整的9.8開始ONTAP 、FlexGroup 下列NDMP功能在功能不支援的情況下、可在功能不完整的情況下使用：

- 副檔名類別0x2050中的NDMP快照恢復訊息可用於還原FlexGroup 整個卷中的個別檔案。
- 支援NDMP可重新啓動的備份擴充（RBE）以供FlexGroup 支援。
- 支援環境變數exclude、FlexGroup 且支援多個子樹狀結構名稱。

了解帶有ONTAP SnapLock卷的 NDMP

建立多個受管制資料複本可提供備援的還原案例、並透過NDMP傾印與還原、將來源檔案的寫入一次、讀取多次（WORM）特性保留在SnapLock 一個穩定的磁碟區上。

當備份、還原及複製資料時、會保留在一個資料區內檔案上的WORM屬性SnapLock ；不過、只有在還原SnapLock 到一個資料區段時、才會強制執行WORM屬性。如果SnapLock 將從S還原Volume的備份還原至SnapLock 非Some Volume、WORM屬性會保留下來、但會被忽略、ONTAP 而且不會由S還原 強制執行。

管理FlexVol 節點範圍的NDMP模式、以利實現不受限的功能

了解如何管理FlexVol磁碟區的ONTAP節點範圍 NDMP 模式

您可以使用NDMP選項和命令、在節點層級管理NDMP。您可以使用修改 NDMP 選項 `options` 命令。您必須使用NDMP專屬的認證資料來存取儲存系統、才能執行磁帶備份與還原作業。

如"指令參考資料ONTAP"需詳細 `options`資訊，請參閱。

用於管理ONTAP節點範圍 NDMP 模式的命令

您可以使用 `system services ndmp` 用於在節點層級管理 NDMP 的命令。其中有些命令已過時、將在未來的重大版本中移除。

您只能在進階權限層級使用下列NDMP命令：

- `system services ndmp service terminate`
- `system services ndmp service start`
- `system services ndmp service stop`
- `system services ndmp log start`

- `system services ndmp log stop`

如果您想要...	使用此命令...
啟用NDMP服務	`system services ndmp on*`
停用NDMP服務	`system services ndmp off*`
顯示 NDMP 組態	`system services ndmp show*`
修改 NDMP 組態	`system services ndmp modify*`
顯示預設NDMP版本	`system services ndmp version*`
顯示NDMP服務組態	`system services ndmp service show`
修改NDMP服務組態	`system services ndmp service modify`
顯示所有NDMP工作階段	`system services ndmp status`
顯示所有NDMP工作階段的詳細資訊	`system services ndmp probe`
終止指定的NDMP工作階段	`system services ndmp kill`
終止所有NDMP工作階段	`system services ndmp kill-all`
變更NDMP密碼	`system services ndmp password*`
啟用節點範圍的NDMP模式	`system services ndmp node-scope-mode on*`
停用節點範圍的NDMP模式	`system services ndmp node-scope-mode off*`
顯示節點範圍的NDMP模式狀態	`system services ndmp node-scope-mode status*`
強制終止所有NDMP工作階段	`system services ndmp service terminate`
啟動NDMP服務精靈	`system services ndmp service start`
停止NDMP服務精靈	`system services ndmp service stop`
開始記錄指定的NDMP工作階段	`system services ndmp log start*`

如果您想要...	使用此命令...
停止記錄指定的NDMP工作階段	`system services ndmp log stop*`

- 這些命令已過時、將在未來的重大版本中移除。

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

節點範圍NDMP模式中的使用者驗證

在節點範圍的NDMP模式中、您必須使用NDMP專屬認證來存取儲存系統、才能執行磁帶備份與還原作業。

預設使用者ID為「root」。在節點上使用NDMP之前、您必須先確定變更與NDMP使用者相關的預設NDMP密碼。您也可以變更預設的NDMP使用者ID。

相關資訊

管理節點範圍NDMP模式的命令

什麼是節點範圍的NDMP模式

管理SVM範圍內的FlexVol NDMP模式、以利不受限於功能區

了解如何管理FlexVol磁碟區的ONTAP SVM 範圍的 NDMP 模式

您可以使用NDMP選項和命令、以每個SVM為基礎來管理NDMP。您可以使用修改 NDMP 選項 `vserver services ndmp modify` 命令。在SVM範圍的NDMP模式中、使用者驗證會與角色型存取控制機制整合。

您可以使用在允許或不允許的通訊協定清單中新增 NDMP `vserver modify` 命令。根據預設、NDMP位於允許的傳輸協定清單中。如果將NDMP新增至不允許的傳輸協定清單、就無法建立NDMP工作階段。

您可以使用選項來控制 NDMP 資料連線所建立的 LIF 類型 `-preferred-interface-role`。在建立NDMP資料連線期間、NDMP會選擇屬於此選項指定之LIF類型的IP位址。如果IP位址不屬於上述LIF類型、則無法建立NDMP資料連線。如"指令參考資料ONTAP"需詳細 `vserver services ndmp modify`資訊，請參閱。

用於管理ONTAP SVM 範圍的 NDMP 模式的命令

您可以使用 `vserver services ndmp` 管理每個儲存虛擬機器（ SVM 、先前稱為 vserver ）上 NDMP 的命令。

如果您想要...	使用此命令...
啟用NDMP服務	`vserver services ndmp on` 叢集中的所有節點必須一律啟用NDMP服務。您可以使用在節點上啟用 NDMP 服務 `system services ndmp on` 命令。根據預設、NDMP服務一律會在節點上啟用。

如果您想要...	使用此命令...
停用NDMP服務	`vserver services ndmp off`
顯示 NDMP 組態	`vserver services ndmp show`
修改 NDMP 組態	`vserver services ndmp modify`
顯示預設NDMP版本	`vserver services ndmp version`
顯示所有NDMP工作階段	`vserver services ndmp status`
顯示所有NDMP工作階段的詳細資訊	`vserver services ndmp probe`
終止指定的NDMP工作階段	`vserver services ndmp kill`
終止所有NDMP工作階段	`vserver services ndmp kill-all`
產生NDMP密碼	`vserver services ndmp generate-password`
顯示NDMP擴充狀態	`vserver services ndmp extensions show` 此命令可在進階權限層級使用。
修改（啟用或停用）NDMP擴充狀態	`vserver services ndmp extensions modify` 此命令可在進階權限層級使用。
開始記錄指定的NDMP工作階段	`vserver services ndmp log start` 此命令可在進階權限層級使用。
停止記錄指定的NDMP工作階段	`vserver services ndmp log stop` 此命令可在進階權限層級使用。

如"指令參考資料ONTAP"需詳細 `vserver services ndmp`資訊，請參閱。

相關資訊

管理SVM範圍NDMP模式的命令

叢集感知備份擴充的功能

SVM範圍的NDMP模式是什麼

"系統管理"

了解**ONTAP NDMP** 的叢集感知備份擴展

Cab（叢集感知備份）是NDMP v4傳輸協定延伸。此擴充功能可讓NDMP伺服器在擁有磁碟區的節點上建立資料連線。這也可讓備份應用程式判斷磁碟區和磁帶裝置是否位於叢集中的同一個節點上。

若要讓NDMP伺服器識別擁有磁碟區的節點、並在這類節點上建立資料連線、備份應用程式必須支援CAB擴充功能。在建立資料連線之前、駕駛台擴充功能需要備份應用程式通知NDMP伺服器有關要備份或還原的磁碟區。這可讓NDMP伺服器判斷裝載該磁碟區的節點、並適當建立資料連線。

備份應用程式支援的電纜擴充功能、NDMP伺服器可提供有關磁碟區和磁帶裝置的關聯資訊。如果磁碟區和磁帶設備位於叢集中的同一個節點上、備份應用程式可以使用此相似性資訊來執行本機備份、而非三向備份。

ONTAP捲和磁帶設備在不同 **LIF** 類型上備份和還原的可用性

您可以設定備份應用程式、在叢集中的任何LIF類型上建立NDMP控制連線。在儲存虛擬機器（SVM）範圍的NDMP模式中、您可以根據這些LIF類型和駕駛室擴充的狀態、決定用於備份和還原作業的磁碟區和磁帶設備的可用度。

下表顯示NDMP控制連線LIF類型的磁碟區和磁帶設備可用度、以及電纜擴充的狀態：

當備份應用程式不支援駕駛台擴充時、磁碟區和磁帶設備的可用度

NDMP控制連線**LIF**類型	可供備份或還原的磁碟區	可用於備份或還原的磁帶設備
節點管理LIF	由節點託管的所有Volume	連線至裝載節點管理LIF之節點的磁帶設備
資料LIF	只有屬於裝載資料LIF之節點所託管SVM的磁碟區	無
叢集管理LIF	由裝載叢集管理LIF的節點所裝載的所有Volume	無
叢集間 LIF	由裝載叢集間LIF的節點所裝載的所有Volume	連接至裝載叢集間LIF之節點的磁帶設備

當備份應用程式支援駕駛台擴充時、磁碟區和磁帶設備的可用度

NDMP控制連線**LIF**類型	可供備份或還原的磁碟區	可用於備份或還原的磁帶設備
節點管理LIF	由節點託管的所有Volume	連線至裝載節點管理LIF之節點的磁帶設備
資料LIF	所有屬於裝載資料LIF之SVM的磁碟區	無
叢集管理LIF	叢集中的所有磁碟區	叢集中的所有磁帶設備

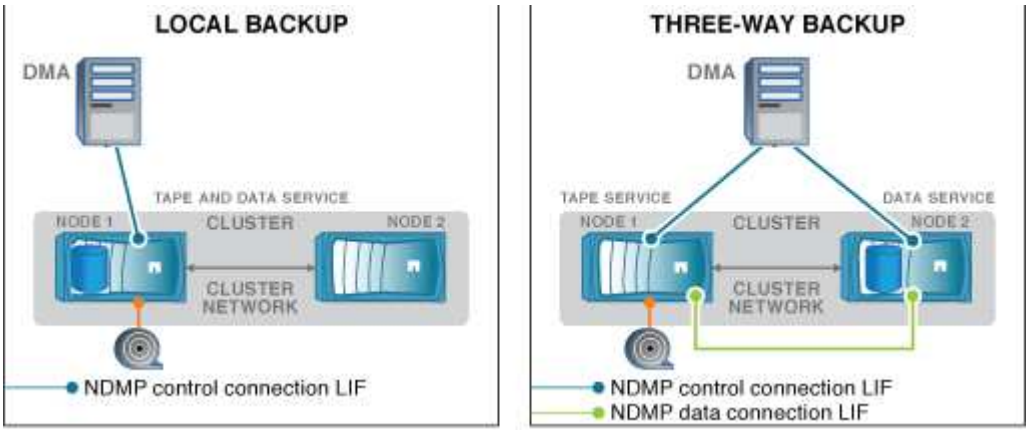
NDMP控制連線LIF類型	可供備份或還原的磁碟區	可用於備份或還原的磁帶設備
叢集間 LIF	叢集中的所有磁碟區	叢集中的所有磁帶設備

了解**ONTAP NDMP** 的親和性訊息

由於備份應用程式可偵測到CA駕駛室、NDMP伺服器可提供有關磁碟區和磁帶裝置的獨特位置資訊。如果磁碟區和磁帶設備共用相同的關聯性、備份應用程式可以使用此關聯性資訊來執行本機備份、而非三向備份。

如果在節點管理LIF上建立NDMP控制連線、叢集管理LIF、 或者叢集間LIF、備份應用程式可以使用關聯性資訊來判斷磁碟區和磁帶設備是否位於同一個節點、然後執行本機或三方備份或還原作業。如果在資料LIF上建立NDMP控制連線、則備份應用程式一律會執行三向備份。

本機**NDMP**備份與三向**NDMP**備份



DMA（備份應用程式）使用有關磁碟區和磁帶裝置的關聯資訊、在位於叢集中節點1的磁碟區和磁帶裝置上執行本機NDMP備份。如果磁碟區從節點1移至節點2、則與磁碟區和磁帶裝置有關的關聯資訊會變更。因此、在後續的備份中、DMA會執行三向NDMP備份作業。如此可確保無論磁碟區移至哪個節點、磁碟區的備份原則都能持續運作。

相關資訊

叢集感知備份擴充的功能

NDMP 伺服器支援 **SVM** 範圍模式下的安全**ONTAP**控制連接

您可以使用安全通訊端（SSL/TLS）作為通訊機制、在資料管理應用程式（DMA）和NDMP伺服器之間建立安全的控制連線。此SSL通訊是以伺服器憑證為基礎。NDMP伺服器會接聽連接埠30000（由IANA指派「ndmps'」服務）。

在這個連接埠上建立用戶端連線之後、伺服器將憑證提交給用戶端的標準SSL交握便會在此發出。當用戶端接受憑證時、SSL交握即告完成。完成此程序之後、用戶端與伺服器之間的所有通訊都會加密。NDMP傳輸協定工作流程維持不變。安全NDMP連線僅需要伺服器端的憑證驗證。DMA可選擇連線至安全NDMP服務或標準NDMP服務來建立連線。

根據預設、儲存虛擬機器（SVM）的安全NDMP服務會停用。您可以使用在指定的 SVM 上啟用或停用安全 NDMP 服務 `vserver services ndmp modify -vserver vserver -is-secure-control`

`-connection-enabled [true|false]` 命令。

NDMP ONTAP資料連線類型

在儲存虛擬機器（SVM）範圍的NDMP模式中、支援的NDMP資料連線類型取決於NDMP控制連線LIF類型和CAB擴充的狀態。此NDMP資料連線類型會指出您可以執行本機或三方NDMP備份或還原作業。

您可以透過TCP或TCP/IP網路執行三向NDMP備份或還原作業。下表顯示NDMP資料連線類型、以NDMP控制連線LIF類型為基礎、以及CAB擴充的狀態。

備份應用程式支援的電纜擴充功能時、即為**NDMP**資料連線類型

NDMP控制連線**LIF**類型	**NDMP**資料連線類型
節點管理LIF	本機、TCP、TCP/IP
資料LIF	TCP、TCP/IP
叢集管理LIF	本機、TCP、TCP/IP
叢集間 LIF	本機、TCP、TCP/IP

備份應用程式不支援的電纜擴充時、即為**NDMP**資料連線類型

NDMP控制連線**LIF**類型	**NDMP**資料連線類型
節點管理LIF	本機、TCP、TCP/IP
資料LIF	TCP、TCP/IP
叢集管理LIF	TCP、TCP/IP
叢集間 LIF	本機、TCP、TCP/IP

相關資訊

叢集感知備份擴充的功能

"網路管理"

SVM 範圍的 NDMP 模式下的ONTAP使用者身份驗證

在儲存虛擬機器（SVM）範圍內的NDMP模式中、NDMP使用者驗證會與角色型存取控制整合。在SVM內容中、NDMP使用者必須具有「vsadmin'」或「vsadmin-Backup」角色。在叢集內容中、NDMP使用者必須具有「admin」或「Backup」角色。

除了這些預先定義的角色之外、只要自訂角色的命令目錄中有「vserver services NDMP」資料夾、而且資料夾的存取層級不是「none"（無）、也可以使用與自訂角色相關的使用者帳戶進行NDMP驗證。在此模式中、您必須為指定的使用者帳戶產生NDMP密碼、此密碼是透過角色型存取控制所建立。管理員或備份角色中的叢集使用者可以存取節點管理LIF、叢集管理LIF或叢集間LIF。vsadmin-backup或vsadmin角色中的使用者只能存取該SVM的資料LIF。因此、視使用者角色而定、備份與還原作業的磁碟區和磁帶設備可用度會有所不同。

此模式也支援NIS和LDAP使用者的使用者驗證。因此、NIS和LDAP使用者可以使用通用的使用者ID和密碼來存取多個SVM。但是、NDMP驗證不支援Active Directory使用者。

在此模式中、使用者帳戶必須與SSH應用程式和「使用者密碼」驗證方法相關聯。

相關資訊

管理SVM範圍NDMP模式的命令

"系統管理"

為**ONTAP NDMP** 使用者產生 **NDMP** 特定密碼

在儲存虛擬機器（SVM）範圍的NDMP模式中、您必須為特定使用者ID產生密碼。產生的密碼是以NDMP使用者的實際登入密碼為基礎。如果實際的登入密碼變更、您必須再次產生NDMP專屬密碼。

步驟

1. 使用 `vserver services ndmp generate-password` 產生 NDMP 特定密碼的命令。

   您可以在任何目前或未來需要輸入密碼的NDMP作業中使用此密碼。

   > 從儲存虛擬機器（SVM、先前稱為Vserver）內容、您可以為僅屬於該SVM的使用者產生NDMP密碼。

   下列範例顯示如何為使用者ID使用者1產生NDMP專屬密碼：

   ```
   cluster1::vserver services ndmp> generate-password -vserver vs1 -user
   user1

   Vserver: vs1
   User: user1
   Password: jWZiNt57huPOoD8d
   ```

2. 如果您將密碼變更為一般儲存系統帳戶、請重複此程序以取得新的NDMP專屬密碼。

在**ONTAP MetroCluster**配置中，災難復原期間磁帶備份和還原作業會受到怎樣的影響

您可以在MetroCluster 災難恢復期間以一套功能組態同時執行磁帶備份與還原作業。您必須瞭解這些作業在災難恢復期間的影響。

如果在災難恢復關係中的某個SVM磁碟區上執行磁帶備份與還原作業、則您可以在切換與切換後繼續執行遞增磁帶備份與還原作業。

關於**FlexVol** 針對資料量的傾印引擎

了解**FlexVol**卷的**ONTAP**轉儲引擎

dump 是 ONTAP 的快照式備份與還原解決方案，可協助您將檔案與目錄從快照備份到磁帶裝置，並將備份的資料還原到儲存系統。

您可以使用傾印備份、將檔案系統資料（例如目錄、檔案及其相關的安全性設定）備份到磁帶設備。您可以備份整個Volume、整個qtree或子樹、而不是整個Volume或整個qtree。

您可以使用NDMP相容的備份應用程式來執行傾印備份或還原。

執行傾印備份時，您可以指定用於備份的快照。如果未指定備份的快照，傾印引擎會建立備份的快照。備份作業完成後，傾印引擎會刪除此快照。

您可以使用傾印引擎、對磁帶執行層級0、遞增或差異備份。

還原至Data ONTAP 版本早於更新版本的版本之後、您必須先執行基礎備份作業、才能執行遞增備份作業。

相關資訊

"升級、回復或降級"

轉儲備份如何與**ONTAP NDMP** 搭配使用

傾印備份會使用預先定義的程序、將檔案系統資料從磁碟寫入磁帶。您可以備份既不是整個Volume、也不是整個qtree的Volume、qtree或子樹。

下表說明ONTAP 了使用哪些程序來備份傾印路徑所指示的物件：

階段	行動
1.	對於容量低於完整磁碟區或完整qtree備份、ONTAP 支援使用者可遍歷目錄來識別要備份的檔案。如果您要備份整個Volume或qtree、ONTAP 則將此階段與第2階段結合在一起。
2.	對於完整Volume或完整qtree備份、ONTAP 支援使用者可在要備份的磁碟區或qtree中識別目錄。
3.	將目錄寫入磁帶。ONTAP
4.	將檔案寫入磁帶。ONTAP
5.	將ACL資訊（若適用）寫入磁帶。ONTAP

傾印備份會使用資料的快照進行備份。因此、您不需要在開始備份之前將磁碟區離線。

dump 備份會將它建立的每個快照命名為 `snapshot_for_backup.n`，其中 `n`是從 0 開始的整數。每次傾印

備份建立快照時，都會將整數增加 1 。在儲存系統重新開機後、會將整數重設為0。備份作業完成後，傾印引擎會刪除此快照。

當 ONTAP 同時執行多個傾印備份時，傾印引擎會建立多個快照。例如，如果 ONTAP 同時執行兩個傾印備份，您可以在備份資料的磁碟區中找到下列快照： `snapshot_for_backup.0`和 `snapshot_for_backup.1`。

當您從快照備份時，傾印引擎不會建立額外的快照。

傾印引擎備份的資料類型

傾印引擎可讓您將資料備份至磁帶、以防止災難或控制器中斷。除了備份檔案、目錄、qtree或整個磁碟區等資料物件之外、傾印引擎也能備份許多類型的每個檔案相關資訊。瞭解傾印引擎可以備份的資料類型、以及需要考量的限制、有助於您規劃災難恢復的方法。

除了備份檔案中的資料外、傾印引擎也可視情況備份每個檔案的下列相關資訊：

- UNIX GID、擁有者唯一識別碼及檔案權限
- UNIX存取、建立及修改時間
- 檔案類型
- 檔案大小
- DOS名稱、DOS屬性及建立時間
- 存取控制清單（ACL）、內含1、024個存取控制項目（ACE）
- qtree資訊
- 交會路徑

交會路徑會備份為符號連結。

- LUN與LUN複製

  您可以備份整個LUN物件、但無法備份LUN物件內的單一檔案。同樣地、您可以還原整個LUN物件、但不能還原LUN內的單一檔案。

  傾印引擎會將LUN複本備份為獨立的LUN。

- VM對齊的檔案

  早於發行版本的版本不支援VM對齊檔案的備份Data ONTAP 。

當快照備援LUN複製作業從Data ONTAP 以7-Mode運作的VMware移轉至ONTAP VMware時、它就會變成不一致的LUN。傾印引擎不會備份不一致的LUN。

當您將資料還原至磁碟區時、所還原的LUN上的用戶端I/O會受到限制。LUN限制只會在傾印還原作業完成時移除。同樣地、在SnapMirror單一檔案或LUN還原作業期間、用戶端I/O也會受到還原檔案和LUN的限制。只有在單一檔案或LUN還原作業完成時、才會移除此限制。如果在執行傾印還原或SnapMirror單一檔案或LUN還原作業的磁碟區上執行傾印備份、則備份中不會包含具有用戶端I/O限制的檔案或LUN。如果移除用戶端I/O限制、這些檔案或LUN會包含在後續的備份作業中。

執行於支援磁帶的LUN僅可還原至8.3版及更新版本、而無法還原至較早版本。Data ONTAP如果LUN還原至較早版本、則LUN會還原為檔案。

當您將SnapVault 某個不支援的次要Volume或Volume SnapMirror目的地備份到磁帶時、只會備份該磁碟區上的資料。不會備份相關的中繼資料。因此、當您嘗試還原磁碟區時、只會還原該磁碟區上的資料。有關Volume SnapMirror關係的資訊無法在備份中取得、因此無法還原。

如果您傾印只有Windows NT權限的檔案、並將其還原至UNIX樣式的qtree或Volume、則該檔案會取得該qtree或Volume的預設UNIX權限。

如果您傾印的檔案只有UNIX權限、並將其還原至NTFS型qtree或Volume、則該檔案會取得該qtree或Volume的預設Windows權限。

其他傾印和還原會保留權限。

您可以備份 VM 對齊的檔案和 `vm-align-sector` 選項。如需VM對齊檔案的詳細資訊、請參閱 "邏輯儲存管理"。

了解增量鍊和ONTAP NDMP

增量鏈是一系列相同路徑的遞增備份。由於您可以隨時指定任何層級的備份、因此您必須瞭解增量鏈、才能有效執行備份與還原。您可以執行31個層級的遞增備份作業。

增量鏈有兩種類型：

- 連續遞增鏈、這是以層級0開始的遞增備份順序、每次後續備份會增加1。
- 不連續的增量鏈、其中遞增備份會跳過層級、或是有順序不連續的層級、例如0、2、3、1、 4、或更常見的0、1、1、1或0、1、 2、1、2。

遞增備份是以最近的較低層級備份為基礎。例如、備份層級0、2、3、1、4的順序提供兩個增量鏈：0、2、3和0、1、4。下表說明遞增備份的基礎：

備份訂單	增量層級	增量鏈	基礎	已備份的檔案
1.	0%	兩者兼具	儲存系統上的檔案	備份路徑中的所有檔案
2.	2.	0 、 2 、 3	層級-0備份	自層級0備份後所建立備份路徑中的檔案
3.	3.	0 、 2 、 3	第2級備份	自層級2備份之後所建立備份路徑中的檔案
4.	1.	0 、 1 、 4	層級0備份、因為這是低於層級1備份的最新層級	從層級0備份建立的備份路徑中的檔案、包括層級2和層級3備份中的檔案

備份訂單	增量層級	增量鏈	基礎	已備份的檔案
5.	4.	0 、 1 、 4	層級1備份、因為它的層級較低、而且比層級0、層級2或層級3備份更新	自層級1備份之後建立的檔案

了解阻塞因素和**ONTAP NDMP**

磁帶區塊為1、024位元組的資料。在磁帶備份或還原期間、您可以指定在每個讀取/寫入作業中傳輸的磁帶區塊數量。此號碼稱為_blocking因素_。

您可以使用4到256之間的封鎖係數。如果您打算將備份還原至備份系統以外的系統、則還原系統必須支援您用於備份的封鎖因素。例如、如果您使用128的封鎖係數、則還原該備份的系統必須支援128的封鎖係數。

在NDMP備份期間、移動者記錄大小決定了封鎖因素。針對「移動者記錄大小」、支援256 KB的最大值。ONTAP

何時重新啟動**ONTAP**轉儲備份

傾印備份有時因為內部或外部錯誤而無法完成、例如磁帶寫入錯誤、停電、使用者意外中斷或儲存系統內部不一致。如果您的備份因為下列其中一項原因而失敗、您可以重新啟動備份。

您可以選擇中斷和重新啟動備份、以避免儲存系統上的流量過大、或避免競爭儲存系統上的其他有限資源、例如磁帶機。如果更緊急的還原（或備份）需要相同的磁帶機、您可以中斷長備份、稍後再重新啟動。重新開機後、可重新啟動的備份會持續存在。只有在符合下列條件時、您才能重新啟動中止的磁帶備份：

- 中止的備份處於第四階段
- 所有已由 dump 命令鎖定的相關快照都可用。
- 必須啟用檔案歷程記錄。

當這類傾印作業中止並留在可重新啟動的狀態時，相關的快照會被鎖定。這些快照會在刪除備份內容之後釋出。您可以使用命令來檢視備份內容清單 `vserver services ndmp restartable backup show`。

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------ -------------------
vserver1 330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1 481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2 5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::> vserver services ndmpd restartable-backup show -vserver
vserver1 -context-id 330e6739-0179-11e6-a299-005056bb4bc9

                      Vserver: vserver1
            Context Identifier: 330e6739-0179-11e6-a299-005056bb4bc9
                   Volume Name: /vserver1/vol1
           Is Cleanup Pending?: false
            Backup Engine Type: dump
Is Snapshot Auto-created?: true
                    Dump Path: /vol/vol1
   Incremental Backup Level ID: 0
                    Dump Name: /vserver1/vol1
     Context Last Updated Time: 1460624875
               Has Offset Map?: true
                 Offset Verify: true
       Is Context Restartable?: true
              Is Context Busy?: false
                  Restart Pass: 4
              Status of Backup: 2
            Snapshot Name: snapshot_for_backup.1
          State of the Context: 7

cluster::>"
```

轉儲還原如何與**ONTAP NDMP** 搭配使用

傾印還原會使用預先定義的程序、將檔案系統資料從磁帶寫入磁碟。

下表中的程序顯示傾印還原的運作方式：

階段	行動
1.	將需要從磁帶中解壓縮的檔案編錄為目錄。ONTAP
2.	可建立目錄和空檔案。ONTAP
3.	從磁帶讀取檔案、將其寫入磁碟、並設定其權限（包括ACL）ONTAP 。

階段	行動
4.	將重複步驟2和3、直到從磁帶複製所有指定的檔案為止。ONTAP

傾印引擎還原的資料類型

當發生災難或控制器中斷時、傾印引擎會提供多種方法、讓您將所有備份的資料、從單一檔案、檔案屬性、還原至整個目錄。瞭解傾印引擎可還原的資料類型、以及何時使用哪種恢復方法、有助於將停機時間降至最低。

您可以將資料還原至線上對應的LUN。不過、在還原作業完成之前、主機應用程式無法存取此LUN。還原作業完成後、應清除LUN資料的主機快取、以提供還原資料的一致性。

傾印引擎可恢復下列資料：

- 檔案和目錄的內容
- UNIX檔案權限
- ACL

  如果您還原的檔案僅具有NTFS qtree或Volume的UNIX檔案權限、則該檔案沒有Windows NT ACL。儲存系統只會使用此檔案的UNIX檔案權限、直到您在該檔案上建立Windows NT ACL為止。

  如果您將從執行Data ONTAP 還原8.2的儲存系統備份的ACL、還原到執行Data ONTAP 速度低於1、024的ACE限制、並執行速度低於1、024的儲存系統、則會還原預設ACL。

- qtree資訊

  僅當qtree還原至磁碟區根目錄時、才會使用qtree資訊。如果 qtree 還原至較低的目錄、例如、則不會使用 qtree 資訊 `/vs1/vol1/subdir/lowerdir`，它不再是 qtree 。

- 所有其他檔案和目錄屬性
- Windows NT串流
- LUN
  - LUN必須還原至磁碟區層級或qtree層級、才能保留為LUN。

    如果將其還原至目錄、則會將其還原為檔案、因為它不包含任何有效的中繼資料。

  - 7-Mode LUN會還原ONTAP 為位於VMware Volume上的LUN。
- 7-Mode Volume可還原ONTAP 為一個不完整的功能。
- 還原至目的地Volume的VM對齊檔案、會繼承目的地Volume的VM對齊屬性。
- 還原作業的目的地Volume可能有具有強制或建議事項鎖定的檔案。

  在對此類目的地Volume執行還原作業時、傾印引擎會忽略這些鎖定。

使用**ONTAP NDMP** 還原資料前的注意事項

您可以將備份的資料還原至其原始路徑或其他目的地。如果您要將備份資料還原至不同目

的地、則必須準備好目的地以進行還原作業。

在將資料還原至原始路徑或其他目的地之前、您必須具備下列資訊、並符合下列需求：

- 還原層級
- 還原資料的路徑
- 備份期間使用的封鎖因素
- 如果您要進行遞增還原、則所有磁帶都必須位於備份鏈中
- 可與要還原之磁帶相容的磁帶機

將資料還原至其他目的地之前、您必須執行下列作業：

- 如果要還原Volume、您必須建立新的Volume。
- 如果您要還原qtree或目錄、則必須重新命名或移動可能與還原檔案名稱相同的檔案。

> 在支援統一碼格式的過程中、qtree名稱可支援ONTAP 使用統一碼格式。舊版ONTAP 的不支援此格式。如果使用將 ONTAP 9 中具有 Unicode 名稱的 qtree 複製到舊版 ONTAP `ndmpcopy` 命令或從磁帶中的備份映像還原、 qtree 會還原為一般目錄、而非以 Unicode 格式還原為 qtree 。

> 如果還原的檔案名稱與現有檔案相同、則現有檔案會被還原的檔案覆寫。不過、目錄不會被覆寫。

若要在還原期間重新命名檔案、目錄或 qtree 而不使用 DAR 、您必須將 Extract 環境變數設為 `E`。

目的地儲存系統上所需的空間

目的地儲存系統所需的空間、比要還原的資料量多出約100 MB。

> 還原作業會在還原作業開始時、檢查目的地磁碟區上的磁碟區空間和inode可用度。將強制環境變數設定為 `Y` 使還原作業略過檢查目的地路徑上的磁碟區空間和 inode 可用度。如果目的地Volume上沒有足夠的磁碟區空間或inode可用、還原作業會恢復目的地Volume空間和inode可用度所允許的資料量。當沒有更多磁碟區空間或inode時、還原作業會停止。

ONTAP轉儲備份和還原會話的可擴展性限制

您必須知道可在不同系統記憶體容量的儲存系統上同時執行的傾印備份與還原工作階段數目上限。此最大值取決於儲存系統的系統記憶體。

下表所述限制適用於傾印或還原引擎。NDMP工作階段的擴充性限制中提到的限制是針對NDMP伺服器、高於引擎限制。

儲存系統的系統記憶體	傾印備份與還原工作階段總數
少於16 GB	4.
大於或等於16 GB但小於24 GB	16.

儲存系統的系統記憶體	傾印備份與還原工作階段總數
大於或等於24 GB	32.

如果您使用 `ndmpcopy` 命令若要在儲存系統內複製資料、會建立兩個 NDMP 工作階段、一個用於傾印備份、另一個用於傾印還原。

您可以使用命令（可透過 nodesdeshed 取得）來取得儲存系統的系統記憶體 `sysconfig -a`。如"指令參考資料ONTAP"需詳細 `sysconfig -a`資訊，請參閱。

相關資訊

NDMP工作階段的擴充性限制

透過提供**ONTAP SVM** 名稱和上下文 **ID** 來刪除可重新啟動的上下文

如果您想要開始備份而非重新啟動內容、可以刪除內容。

關於這項工作

您可以使用刪除可重新啓動的上下文 `vserver services ndmp restartable-backup delete` 命令、提供 SVM 名稱和內容 ID 。

步驟

1. 刪除可重新啓動的上下文：

   `vserver services ndmp restartable-backup delete -vserver *vserver-name* -context-id *context_identifier*`。

```
cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver1    481025c1-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>
cluster::> vserver services ndmp restartable-backup delete -vserver
vserver1 -context-id 481025c1-0179-11e6-a299-005056bb4bc9

cluster::> vserver services ndmpd restartable-backup show
Vserver     Context Identifier                    Is Cleanup Pending?
----------- ------------------------------------- -------------------
vserver1    330e6739-0179-11e6-a299-005056bb4bc9 false
vserver2    5cf10132-0179-11e6-a299-005056bb4bc9 false
3 entries were displayed.

cluster::>"
```

轉儲如何在**ONTAP SnapVault**二級磁碟區上運作

您可以在SnapVault 鏡射到支援鏡射的資料上執行磁帶備份作業。您只能將SnapVault 鏡射在該次要Volume上的資料備份到磁帶、而非SnapVault 還原關係中繼資料。

當您中斷資料保護鏡射關係時 (`snapmirror break`）或 SnapMirror 重新同步發生時，您必須始終執行基準備份。

相關資訊

- "SnapMirror中斷"

轉儲如何與**ONTAP**儲存故障轉移和 **ARL** 操作配合使用

在執行傾印備份或還原作業之前、您應該先瞭解這些作業如何搭配儲存容錯移轉（接管和恢復）或集合重新配置（ARL）作業。。 `-override-vetoes` 選項可決定儲存容錯移轉或 ARL 作業期間傾印引擎的行為。

當執行傾印備份或還原作業時、以及 `-override-vetoes` 選項設定為 `false`、使用者啟動的儲存容錯移轉或 ARL 作業將會停止。不過、如果是 `-override-vetoes` 選項設定為 `true`，則會繼續儲存容錯移轉或 ARL 作業，並中止傾印備份或還原作業。當儲存系統自動啟動儲存容錯移轉或ARL作業時、作用中的傾印備份或還原作業一律會中止。即使在儲存容錯移轉或ARL作業完成之後、也無法重新啟動傾印備份與還原作業。

支援駕駛擴充時的傾印作業

如果備份應用程式支援CAK擴充、您可以在儲存容錯移轉或ARL作業之後、繼續執行遞增傾印備份與還原作業、

而不需重新設定備份原則。

不支援駕駛擴充時的傾印作業

如果備份應用程式不支援CAF擴充、則如果您將備份原則中設定的LIF移轉到裝載目的地Aggregate的節點、就可以繼續執行遞增傾印備份與還原作業。否則、在儲存容錯移轉和ARL作業之後、您必須先執行基礎備份、才能執行遞增備份作業。

對於儲存容錯移轉作業、必須將備份原則中設定的LIF移轉至合作夥伴節點。

相關資訊

"高可用度"

轉儲如何與**ONTAP**卷移動配合使用

磁帶備份與還原作業與Volume搬移可平行執行、直到儲存系統嘗試進行最終轉換階段為止。在此階段之後、將不允許在移動的磁碟區上執行新的磁帶備份與還原作業。不過、目前的作業會持續執行、直到完成為止。

下表說明磁碟區移動作業之後、磁帶備份與還原作業的行為：

如果您在...中執行磁帶備份與還原作業、	然後...
當備份應用程式支援駕駛台擴充時、儲存虛擬機器（SVM）會將NDMP模式範圍內	您可以繼續在讀寫磁碟區和唯讀磁碟區上執行遞增磁帶備份和還原作業、而無需重新設定備份原則。
當備份應用程式不支援駕駛擴充時、SVM範圍的NDMP模式	如果您將備份原則中設定的LIF移轉到裝載目的地Aggregate的節點、則可以繼續在讀取/寫入和唯讀磁碟區上執行遞增磁帶備份和還原作業。否則、在磁碟區移動之後、您必須先執行基礎備份、才能執行遞增備份作業。

發生磁碟區移動時、如果屬於目的地節點上不同SVM的磁碟區名稱與移動的磁碟區名稱相同、則無法對移動的磁碟區執行遞增備份作業。

當**ONTAP FlexVol volume**已滿時轉儲如何運作

在執行遞增傾印備份作業之前、您必須確保FlexVol 在這個卷中有足夠的可用空間。

如果作業失敗，您必須增加 Flex Vol Volume 磁碟區的可用空間，方法是增加其大小或刪除快照。然後再次執行遞增備份作業。

當**ONTAP**磁碟區存取類型發生變化時轉儲如何運作

當SnapMirror目的地Volume或SnapVault 還原次要Volume的狀態從讀取/寫入變更為唯讀或從唯讀變更為讀取/寫入時、您必須執行基礎磁帶備份或還原作業。

SnapMirror目的地SnapVault 和不二級磁碟區是唯讀磁碟區。如果您在這類磁碟區上執行磁帶備份與還原作業、則當磁碟區的狀態從唯讀變更為讀取/寫入、或從讀取/寫入變更為唯讀時、就必須執行基礎備份或還原作業。

轉儲如何與**ONTAP SnapMirror**單一檔案或 **LUN** 還原搭配使用

在使用SnapMirror技術還原單一檔案或LUN的磁碟區上執行傾印備份或還原作業之前、您必須先瞭解傾印作業如何與單一檔案或LUN還原作業搭配運作。

在SnapMirror單一檔案或LUN還原作業期間、用戶端I/O會受限於要還原的檔案或LUN。當單一檔案或LUN還原作業完成時、會移除檔案或LUN的I/O限制。如果在還原單一檔案或LUN的磁碟區上執行傾印備份、則傾印備份中不會包含具有用戶端I/O限制的檔案或LUN。在後續的備份作業中、此檔案或LUN會在移除I/O限制之後備份至磁帶。

您無法在同一個磁碟區上同時執行傾印還原和SnapMirror單一檔案或LUN還原作業。

ONTAP MetroCluster配置對轉儲備份和還原作業有何影響

在執行還原組態的傾印備份與還原作業之前MetroCluster 、您必須先瞭解當發生切換或切換作業時、傾印作業會受到哪些影響。

轉儲備份或還原作業、然後切換

請考慮兩個叢集：叢集1和叢集2。在叢集1上執行傾印備份或還原作業期間、如果從叢集1啟動切換至叢集2、則會發生下列情況：

- 如果的值 `override-vetoes` 選項是 `false`，則會中止此項作業，並繼續進行備份或還原作業。
- 如果選項的值為 `true`，則轉儲備份或還原操作將中止，並繼續進行轉接。

接著是傾印備份或還原作業、接著是切換回復

從叢集1切換至叢集2、並在叢集2上啟動傾印備份或還原作業。傾印作業會備份或還原位於叢集2上的磁碟區。此時、如果從叢集2啟動切換到叢集1、則會發生下列情況：

- 如果的值 `override-vetoes` 選項是 `false`，則會取消切換，並繼續備份或還原作業。
- 如果選項的值為 `true`，則備份或還原作業會中止，並繼續切換。

在切換或切換期間啟動傾印備份或還原作業

從叢集1切換至叢集2期間、如果在叢集1上啟動傾印備份或還原作業、則備份或還原作業會失敗、而且切換會繼續進行。

從叢集2切換回叢集1期間、如果從叢集2啟動傾印備份或還原作業、則備份或還原作業會失敗、而且切換會繼續進行。

關於**FlexVol** 適用於資料量的**SMTape**引擎

了解適用於**FlexVol**磁碟區的**ONTAP SMTape** 引擎

SMtape是一套災難恢復解決方案、可ONTAP 將資料區塊備份到磁帶。您可以使用SMTaper對磁帶執行Volume備份。不過、您無法在qtree或子樹狀結構層級執行備份。SMTape支援基準備份、差異備份和遞增備份。SMTape不需要授權。

您可以使用NDMP相容的備份應用程式來執行SM磁帶 備份與還原作業。您可以選擇SMTape、只在儲存虛擬機器（SVM）指定NDMP模式下執行備份與還原作業。

> 在進行SM磁帶 備份或還原工作階段時、不支援還原程序。您必須等到工作階段完成、否則必須中止NDMP工作階段。

使用 SMTape ，您可以備份 255 個快照。對於後續的基準備份，增量備份或差異備份，您必須刪除較舊的備份快照。

在執行基準還原之前、要還原資料的磁碟區必須是類型 `DP` 而且此磁碟區必須處於受限狀態。成功還原後、此Volume會自動上線。您可以依照執行備份的順序、對此磁碟區執行後續的遞增或差異還原。

了解在 **SMTape** 備份期間使用**ONTAP**快照

您應該瞭解在 SMTape 基準備份和遞增備份期間如何使用快照。在使用SMTape執行備份時、也必須謹記注意事項。

基礎備份

執行基準備份時，您可以指定要備份至磁帶的快照名稱。如果未指定快照，則會根據磁碟區的存取類型（讀取 / 寫入或唯讀）自動建立快照，或使用現有的快照。當您為備份指定快照時，所有比指定快照更舊的快照也會備份到磁帶。

如果您未指定備份的快照，則會發生下列情況：

- 對於讀寫磁碟區，系統會自動建立快照。

  新建立的快照和所有較舊的快照都會備份到磁帶。

- 對於唯讀磁碟區，所有快照（包括最新快照）都會備份到磁帶。

  在備份啟動之後建立的任何新快照都不會備份。

遞增備份

對於 SMTape 遞增或差異備份作業，符合 NDMP 標準的備份應用程式會建立及管理快照。

執行遞增備份作業時，您必須一律指定快照。若要成功執行增量備份作業，在先前備份作業（基準或遞增）期間備份的快照必須位於執行備份的磁碟區上。為了確保您使用此備份快照，您必須在設定備份原則時，考慮在此磁碟區上指派的快照原則。

SnapMirror目的地上的**SMTape**備份考量

- 資料保護鏡射關係會在目的地磁碟區上建立暫時快照以進行複寫。

  請勿將這些快照用於 SMTape 備份。

- 如果在同一磁碟區上執行 SMTape 備份作業期間，目的地磁碟區的資料保護鏡像關係中發生 SnapMirror 更新，則不得刪除來源磁碟區上由 SMTape 備份的快照。

  在備份作業期間， SMTape 會鎖定目的地磁碟區上的快照，如果來源磁碟區上的對應快照已刪除，則後續的 SnapMirror 更新作業將會失敗。

- 增量備份期間不應使用這些快照。

SMTape 功能可最佳化**ONTAP**磁帶備份與復原作業

SMTape 功能，例如快照備份，遞增和差異備份，保留還原磁碟區上的重複資料刪除和壓縮功能，以及磁帶植入，可協助您最佳化磁帶備份和還原作業。

SMTape提供下列功能：

- 提供災難恢復解決方案
- 啟用遞增和差異備份
- 備份快照
- 可備份及還原已刪除重複資料的磁碟區、並在還原的磁碟區上保留重複資料刪除功能
- 備份壓縮磁碟區、並保留還原磁碟區的壓縮
- 啟用磁帶植入

SMTape支援4 KB至256 KB的多倍封鎖係數、範圍介於4 KB至256 KB之間。

您最多ONTAP 只能將資料還原至兩個連續重大發行版本所建立的磁碟區。

SMTape 備份和還原會話的**ONTAP**可擴展性限制

在透過NDMP或CLI（磁帶植入）執行SMTape備份與還原作業時、您必須瞭解可在具有不同系統記憶體容量的儲存系統上同時執行的SM磁帶 備份與還原工作階段數量上限。此最大值取決於儲存系統的系統記憶體。

SM磁帶 備份與還原工作階段擴充性限制與NDMP工作階段限制和傾印工作階段限制不同。

儲存系統的系統記憶體	**SMTape**備份與還原工作階段總數
少於16 GB	6.
大於或等於16 GB但小於24 GB	16.
大於或等於24 GB	32.

您可以使用命令（可透過 nodesdeshed 取得）來取得儲存系統的系統記憶體 `sysconfig -a`。如"指令參考資料ONTAP"需詳細 `sysconfig -a`資訊，請參閱。

相關資訊

- NDMP工作階段的擴充性限制
- 傾印備份與還原工作階段的擴充性限制

了解**ONTAP**磁帶播種

磁帶植入是一項SMTape功能、可協助您在FlexVol 資料保護鏡射關係中初始化目的地的一套。

磁帶植入功能可讓您透過低頻寬連線、在來源系統與目的地系統之間建立資料保護鏡射關係。

透過低頻寬連線，可將快照從來源鏡射到目的地。不過，基礎快照的初始鏡射需要很長時間，而這需要透過低頻寬連線。在這種情況下，您可以將來源磁碟區的 SMTape 備份至磁帶，並使用磁帶將初始基礎快照傳輸至目的地。然後、您可以使用低頻寬連線、將SnapMirror遞增更新設定至目的地系統。

SMTape 如何與**ONTAP**儲存故障轉移和 **ARL** 操作配合使用

在執行SMTape備份或還原作業之前、您應該先瞭解這些作業如何搭配儲存容錯移轉（接管與恢復）或集合重新配置（ARL）作業。。 `-override-vetoes` 選項可決定 SMTape 引擎在儲存容錯移轉或 ARL 作業期間的行為。

當 SMTape 備份或還原作業正在執行時、以及 `-override-vetoes` 選項設定為 `false`、停止使用者啟動的儲存容錯移轉或 ARL 作業、並完成備份或還原作業。如果備份應用程式支援Cab擴充、則您可以繼續執行遞增的SMTape備份與還原作業、而不需重新設定備份原則。不過、如果是 `-override-vetoes` 選項設定為 `true`，然後繼續進行儲存容錯移轉或 ARL 作業，並中止 SMTape 備份或還原作業。

相關資訊

"網路管理"

"高可用度"

SMTape 如何與**ONTAP**磁碟區移動配合使用

SM磁帶 備份作業和Volume Move作業可平行執行、直到儲存系統嘗試最後轉換階段為止。在此階段之後、新的SM磁帶 備份作業無法在要移動的磁碟區上執行。不過、目前的作業會持續執行、直到完成為止。

在開始磁碟區的轉換階段之前、磁碟區移動作業會檢查同一個磁碟區上的有效SMTape備份作業。如果有作用中的SMTape備份作業、則Volume Move作業會移至轉換延後狀態、並允許完成SMTape備份作業。完成這些備份作業之後、您必須手動重新啟動Volume Move作業。

如果備份應用程式支援CAB/EXTENSION、您可以在讀取/寫入和唯讀磁碟區上繼續執行遞增磁帶備份和還原作業、而無需重新設定備份原則。

無法同時執行基礎還原和磁碟區移動作業；不過、遞增還原可與磁碟區移動作業並行執行、其行為類似於磁碟區移動作業期間的SMTape備份作業。

SMTape 如何與**ONTAP**磁碟區重新託管作業搭配使用

在磁碟區上進行磁碟區重新主機作業時、無法開始SMTape作業。當磁碟區涉及到磁碟區重新主機作業時、不應在該磁碟區上啟動SMTape工作階段。

如果正在執行任何磁碟區重新主機作業、則SMTape備份或還原會失敗。如果正在進行SMTape備份或還原、則Volume重新主機作業會失敗、並顯示適當的錯誤訊息。此條件適用於NDMP型和CLI型備份或還原作業。

ONTAP NDMP 備份策略在 ADB 期間會受到怎樣的影響

啟用自動資料平衡器（ADD）時、平衡器會分析Aggregate的使用統計資料、以識別已超過設定的高臨界值使用率百分比的集合體。

在識別出超過臨界值的集合體之後、平衡器會識別出一個磁碟區、該磁碟區可移至位於叢集中其他節點的集合體、並嘗試移動該磁碟區。這種情況會影響為此磁碟區所設定的備份原則、因為如果資料管理應用程式（DMA）無法偵測到、使用者就必須重新設定備份原則、然後執行基礎備份作業。

如果DMA可偵測到CAb、而且備份原則已使用特定介面設定、則不會影響ADb。

ONTAP MetroCluster設定對 SMTape 備援和還原作業有何影響

在MetroCluster 執行以還原組態執行SMTape備份與還原作業之前、您必須先瞭解在發生切換或切換作業時、SMTape作業會受到哪些影響。

SM磁帶 備份或還原作業、然後切換

請考慮兩個叢集：叢集1和叢集2。在叢集1上執行SM磁帶 備份或還原作業期間、如果從叢集1啟動切換至叢集2、則會發生下列情況：

- 如果的值 `-override-vetoes` 選項是 `false`，則會中止轉換程序，並繼續進行備份或還原作業。
- 如果選項的值為 `true`，則 SMTape 備份或還原操作會中止，並繼續進行轉換程序。

SMTape備份或還原作業、接著是切換

從叢集1切換至叢集2、並在叢集2上啟動SMTape備份或還原作業。SMTape作業會備份或還原位於叢集2上的磁碟區。此時、如果從叢集2啟動切換到叢集1、則會發生下列情況：

- 如果的值 `-override-vetoes` 選項是 `false`，則會中止切換程序，並繼續進行備份或還原作業。
- 如果選項的值為 `true`，則備份或還原作業會中止，並繼續切換程序。

SMTape備份或還原作業是在切換或切換期間啟動的

在從叢集1切換至叢集2的過程中、如果在叢集1上啟動SMTape備份或還原作業、則備份或還原作業會失敗、而且切換會繼續進行。

在從叢集2切換到叢集1的過程中、如果從叢集2啟動SM磁帶 備份或還原作業、則備份或還原作業會失敗、而且切換會繼續進行。

監控FlexVol 磁帶備份與還原功能、以利執行各項功能

監控FlexVol磁碟區的ONTAP磁帶備份與復原作業

您可以檢視事件記錄檔、以監控磁帶備份與還原作業。ONTAP 會自動記錄重要的備份與還原事件、以及這些事件發生在名為的記錄檔中的時間 `backup` 控制器的 `/etc/log/` 目錄。依預設、事件記錄設為 `on`。

您可能會因為下列原因而想要檢視事件記錄檔：

- 檢查夜間備份是否成功
- 收集備份作業的統計資料
- 使用過去事件記錄檔中的資訊來協助診斷備份與還原作業的問題

每週會旋轉一次事件記錄檔。。 `/etc/log/backup` 檔案已重新命名為 `/etc/log/backup.0`、`/etc/log/backup.0` 檔案已重新命名為 `/etc/log/backup.1`等等。系統會儲存記錄檔長達六週、因此最多可儲存七個訊息檔案 （/etc/log/backup.[0-5]` 以及目前的 `/etc/log/backup` 檔案）。

存取**ONTAP**事件日誌檔案以進行磁帶備份和還原作業

您可以存取事件記錄檔、以便在中進行磁帶備份與還原作業 `/etc/log/` 使用的目錄 `rdfile` 命令。您可以檢視這些事件記錄檔、以監控磁帶備份與還原作業。

關於這項工作

使用其他組態、例如可存取的存取控制角色 `spi` 使用設定的 Web 服務或使用者帳戶 `http` 存取方法、您也可以使用網頁瀏覽器來存取這些記錄檔。

步驟

1. 若要存取nodesdro解除、請輸入下列命令：

   `node run -node node_name`

   `node_name` 為節點的名稱。

2. 若要存取磁帶備份與還原作業的事件記錄檔、請輸入下列命令：

   `rdfile /etc/log/backup`

相關資訊

"系統管理"

傾印與還原事件記錄訊息格式為何

ONTAP轉儲和復原事件日誌訊息格式

針對每個傾印與還原事件、會有一則訊息寫入備份記錄檔。

傾印與還原事件記錄訊息的格式如下：

`type timestamp identifier event (event_info)`

下列清單說明事件記錄訊息格式的欄位：

- 每則記錄訊息都會以下表所述的其中一種類型指標開頭：

類型	說明
記錄	記錄事件

類型	說明
DMP	傾印事件
RST	還原事件

- `timestamp` 顯示事件的日期和時間。
- 。 `identifier` 傾印事件的欄位包括傾印路徑和傾印的唯一 ID 。。 `identifier` 還原事件欄位僅使用還原目的地路徑名稱做為唯一識別碼。記錄相關的事件訊息不包含 `identifier` 欄位。

了解**ONTAP**日誌記錄事件

以記錄開頭的訊息事件欄位會指定記錄的開頭或記錄的結尾。

其中包含下表所示的其中一個事件：

活動	說明
start_記錄	表示記錄的開始、或記錄功能在停用後重新開啟。
停止記錄	表示記錄功能已關閉。

了解**ONTAP**轉儲事件

傾印事件的事件欄位包含事件類型、並在括弧內加上事件特定資訊。

下表說明可能記錄的傾印作業事件、其說明及相關事件資訊：

活動	說明	活動資訊
開始	NDMP傾印已啟動	傾印層級和傾印類型
結束	成功完成傾印	處理的資料量
中止	作業隨即取消	處理的資料量
選項	會列出指定的選項	所有選項及其相關值、包括NDMP選項
磁帶開啟	磁帶已開啟以供讀取/寫入	新的磁帶設備名稱
磁帶_關閉	磁帶會關閉以供讀取/寫入	磁帶設備名稱
階段變更	傾印正在進入新的處理階段	新階段名稱

活動	說明	活動資訊
錯誤	傾印發生非預期的事件	錯誤訊息
Snapshot	快照即會建立或找到	快照的名稱和時間
base傾印	已在內部中繼檔中找到基礎傾印項目	基礎傾印的層級和時間（僅適用於遞增傾印）

了解**ONTAP**恢復事件

還原事件的事件欄位包含事件類型、後面加上事件特定資訊、並以括弧括住。

下表提供事件的相關資訊、其說明、以及可記錄用於還原作業的相關事件資訊：

活動	說明	活動資訊
開始	NDMP還原已啟動	還原層級和還原類型
結束	還原成功完成	檔案數量和處理的資料量
中止	作業隨即取消	檔案數量和處理的資料量
選項	會列出指定的選項	所有選項及其相關值、包括NDMP選項
磁帶開啟	磁帶已開啟以供讀取/寫入	新的磁帶設備名稱
磁帶_關閉	磁帶會關閉以供讀取/寫入	磁帶設備名稱
階段變更	還原正在進入新的處理階段	新階段名稱
錯誤	還原遇到非預期的事件	錯誤訊息

啟用或停用**ONTAP**磁帶備份和還原作業的事件日誌記錄

您可以開啟或關閉事件記錄。

步驟

1. 若要啟用或停用事件記錄、請在clusterShell輸入下列命令：

   `options -option_name backup.log.enable -option-value {on | off}`

   `on` 開啟事件記錄。

   `off` 關閉事件記錄。

預設會開啟事件記錄。

磁帶備份與FlexVol 還原的錯誤訊息

備份與還原錯誤訊息

資源限制：無可用的執行緒

- 訊息

  ```
  Resource limitation: no available thread
  ```

- 原因

  目前使用中的本機磁帶I/O執行緒數目上限。您最多可以有16個作用中的本機磁帶機。

- 修正行動

  等待部分磁帶工作完成、再開始新的備份或還原工作。

磁帶保留已搶佔

- 訊息

  ```
  Tape reservation preempted
  ```

- 原因

  磁帶機正由其他作業使用、或磁帶已提前關閉。

- 修正行動

  請確定磁帶機未被其他作業使用、且DMA應用程式未中止工作、然後重試。

無法初始化媒體

- 訊息

  ```
  Could not initialize media
  ```

- 原因

  您可能會因為下列原因之一而收到此錯誤：

  - 用於備份的磁帶機毀損或毀損。
  - 磁帶不包含完整備份或毀損。
  - 目前使用中的本機磁帶I/O執行緒數目上限。

    您最多可以有16個作用中的本機磁帶機。

- 修正行動
  - 如果磁帶機毀損或毀損、請使用有效的磁帶機重試此作業。
  - 如果磁帶未包含完整備份或毀損、您將無法執行還原作業。
  - 如果磁帶資源無法使用、請等待部分備份或還原工作完成、然後重試該作業。

進行中的允許傾印或還原數目上限（工作階段上限）

- 訊息

  `Maximum number of allowed dumps or restores` *`(maximum session limit)`* `in progress`

- 原因

  已執行的備份或還原工作數目上限。

- 修正行動

  在某些目前執行中的工作完成後、重試此作業。

磁帶寫入時發生媒體錯誤

- 訊息

  `Media error on tape write`

- 原因

  用於備份的磁帶已毀損。

- 修正行動

  更換磁帶並重試備份工作。

磁帶寫入失敗

- 訊息

  `Tape write failed`

- 原因

  用於備份的磁帶已毀損。

- 修正行動

  更換磁帶並重試備份工作。

磁帶寫入失敗-新磁帶發生媒體錯誤

- 訊息

  ```
  Tape write failed - new tape encountered media error
  ```

- 原因

  用於備份的磁帶已毀損。

- 修正行動

  更換磁帶並重試備份。

磁帶寫入失敗-新磁帶毀損或受到寫入保護

- 訊息

  ```
  Tape write failed - new tape is broken or write protected
  ```

- 原因

  用於備份的磁帶已毀損或受到寫入保護。

- 修正行動

  更換磁帶並重試備份。

磁帶寫入失敗-新磁帶已在媒體結尾

- 訊息

  ```
  Tape write failed - new tape is already at the end of media
  ```

- 原因

  磁帶空間不足、無法完成備份。

- 修正行動

  更換磁帶並重試備份。

磁帶寫入錯誤

- 訊息

  ```
  Tape write error - The previous tape had less than the required minimum
  capacity, size MB, for this tape operation, The operation should be restarted
  from the beginning
  ```

- 原因

磁帶容量不足以容納備份資料。

- 修正行動

  使用容量較大的磁帶、然後重試備份工作。

磁帶讀取時發生媒體錯誤

- 訊息

  ```
  Media error on tape read
  ```

- 原因

  正在從中還原資料的磁帶已毀損、可能不包含完整的備份資料。

- 修正行動

  如果您確定磁帶有完整備份、請重試還原作業。如果磁帶未包含完整備份、您將無法執行還原作業。

磁帶讀取錯誤

- 訊息

  ```
  Tape read error
  ```

- 原因

  磁帶機損壞或磁帶未包含完整備份。

- 修正行動

  如果磁帶機損壞、請使用其他磁帶機。如果磁帶未包含完整備份、您將無法還原資料。

已在磁帶結尾

- 訊息

  ```
  Already at the end of tape
  ```

- 原因

  磁帶不含任何資料、或必須重新繞線。

- 修正行動

  如果磁帶不含資料、請使用包含備份的磁帶、然後重試還原工作。否則、請將磁帶倒帶、然後重試還原工作。

磁帶記錄大小太小。請嘗試使用較大的尺寸。

- 訊息

  `Tape record size is too small. Try a larger size.`

- 原因

  為還原作業指定的封鎖因素小於備份期間使用的封鎖因素。

- 修正行動

  使用備份期間指定的相同封鎖因素。

磁帶記錄大小應為**block_Size1**、而非**block_Size2**

- 訊息

  `Tape record size should be block_size1 and not block_size2`

- 原因

  為本機還原指定的封鎖因素不正確。

- 修正行動

  使用重試還原工作 `block_size1` 成為阻礙因素。

磁帶記錄大小必須介於**4KB**與**256KB**之間

- 訊息

  `Tape record size must be in the range between 4KB and 256KB`

- 原因

  為備份或還原作業指定的封鎖因素不在允許範圍內。

- 修正行動

  指定範圍為4 KB至256 KB的封鎖因素。

NDMP錯誤訊息

網路通訊錯誤

- 訊息

  `Network communication error`

- 原因

透過NDMP三向連線與遠端磁帶的通訊失敗。

- 修正行動

  檢查遠端移動設備的網路連線。

來自讀取套接字的訊息：**error_string**

- 訊息

  ```
  Message from Read Socket: error_string
  ```

- 原因

  以NDMP 3向連線從遠端磁帶還原通訊時發生錯誤。

- 修正行動

  檢查遠端移動設備的網路連線。

來自**Write Dirnet**的訊息：錯誤字串

- 訊息

  ```
  Message from Write Dirnet: error_string
  ```

- 原因

  以NDMP三向連線將通訊備份到遠端磁帶時發生錯誤。

- 修正行動

  檢查遠端移動設備的網路連線。

讀取套接字接收到**EOF**

- 訊息

  ```
  Read Socket received EOF
  ```

- 原因

  嘗試以NDMP三向連線與遠端磁帶通訊已達檔案結尾標記。您可能嘗試從區塊大小較大的備份映像進行三方還原。

- 修正行動

  請指定正確的區塊大小、然後重試還原作業。

ndmpd無效的版本號碼：**VERIN_NUMBER_`**

- 訊息

  ```
  ndmpd invalid version number: version_number
  ```

- 原因

  儲存系統不支援指定的NDMP版本。

- 修正行動

  指定NDMP版本4。

ndmpd工作階段工作階段**_ID**未啟用

- 訊息

  ```
  ndmpd session session_ID not active
  ```

- 原因

  NDMP工作階段可能不存在。

- 修正行動

  使用 `ndmpd status` 用於檢視作用中 NDMP 工作階段的命令。

無法取得**Volume Volume_name**的**vol**參考

- 訊息

  ```
  Could not obtain vol ref for Volume vol_name
  ```

- 原因

  無法取得磁碟區參考、因為其他作業可能正在使用該磁碟區。

- 修正行動

  稍後再重試此作業。

資料連線類型**["NDMP4_ADDR_tcp"|"NDMP4_ADDR_TCP_ipv6"]**不支援使用於**["ipv6"|"ipv4"]**控制連線

- 訊息

  ```
  Data connection type ["NDMP4_ADDR_TCP"|"NDMP4_ADDR_TCP_IPv6"] not supported
  for ["IPv6"|"IPv4"] control connections
  ```

- 原因

  在節點範圍的NDMP模式中、建立的NDMP資料連線必須與NDMP控制連線具有相同的網路位址類型（IPv4

或IPv6）。

- 修正行動

  請聯絡您的備份應用程式廠商。

資料偵聽：**CAB**資料連線準備先決條件錯誤

- 訊息

  ```
  DATA LISTEN: CAB data connection prepare precondition error
  ```

- 原因

  當備份應用程式已與NDMP伺服器交涉CAO擴充功能、且NDMP資料連線位址類型與NDMP _CAP_DATA _CONN_Pare和NDMP資料聆聽訊息不符時、NDMP資料接聽會失敗。

- 修正行動

  請聯絡您的備份應用程式廠商。

資料連線：**CAB**資料連線準備先決條件錯誤

- 訊息

  ```
  DATA CONNECT: CAB data connection prepare precondition error
  ```

- 原因

  當備份應用程式已與NDMP伺服器交涉CAO擴充功能、且NDMP資料連線位址類型與NDMP與NDMP資料連線訊息不符時、NDMP資料連線會失敗。

- 修正行動

  請聯絡您的備份應用程式廠商。

錯誤：顯示失敗：無法取得使用者**'<username>'**的密碼

- 訊息

  ```
  Error: show failed: Cannot get password for user '<username>'
  ```

- 原因

  NDMP的使用者帳戶組態不完整

- 修正行動

  確認使用者帳戶已與SSH存取方法建立關聯、且驗證方法為使用者密碼。

傾印錯誤訊息

目的地**Volume**為唯讀

- 訊息

  `Destination volume is read-only`

- 原因

  嘗試還原作業的路徑為唯讀。

- 修正行動

  請嘗試將資料還原至其他位置。

目的地**qtree**為唯讀

- 訊息

  `Destination qtree is read-only`

- 原因

  嘗試還原的qtree為唯讀。

- 修正行動

  請嘗試將資料還原至其他位置。

傾印在磁碟區上暫時停用、請再試一次

- 訊息

  `Dumps temporarily disabled on volume, try again`

- 原因

  NDMP 傾印備份是在 SnapMirror 目的地磁碟區上執行、而該磁碟區是其中一部分的一部分 `snapmirror break` 或是 `snapmirror resync` 營運。

- 修正行動

  等待 `snapmirror break` 或 `snapmirror resync` 完成作業、然後執行傾印作業。

每當SnapMirror目的地Volume的狀態從讀取/寫入變更為唯讀或從唯讀變更為讀取/寫入時、您必須執行基礎備份。

相關資訊

- "SnapMirror中斷"

- "SnapMirror 重新同步"

無法辨識NFS標籤

- 訊息

  ```
  Error: Aborting: dump encountered NFS security labels in the file system
  ```

- 原因

  啟用NFSv4.2時、NFS安全性標籤會從ONTAP 支援的版本S29開始提供支援。不過、傾印引擎目前無法辨識NFS安全性標籤。如果在任何格式的傾印檔案、目錄或任何特殊檔案上遇到任何NFS安全性標籤、傾印就會失敗。

- 修正行動

  確認沒有檔案或目錄具有NFS安全性標籤。

未建立任何檔案

- 訊息

  ```
  No files were created
  ```

- 原因

  在未啟用增強的DAR功能的情況下、嘗試使用目錄DAR。

- 修正行動

  啟用增強的DAR功能、然後重試DAR。

還原檔案<檔案名稱>失敗

- 訊息

  ```
  Restore of the file file name failed
  ```

- 原因

  當檔案名稱與目的地磁碟區上LUN相同的檔案執行DAR（直接存取還原）時、DAR將會失敗。

- 修正行動

  重試檔案的DAR。

SRC inode <inode number>.....的截短失敗

- 訊息

  ```
  Truncation failed for src inode <inode number>. Error <error number>. Skipping
  ```

inode.

- 原因

  檔案的inode會在還原檔案時刪除。

- 修正行動

  請等待磁碟區上的還原作業完成、然後再使用該磁碟區。

無法鎖定傾印所需的快照

- 訊息

  ```
  Unable to lock a snapshot needed by dump
  ```

- 原因

  指定用於備份的快照不可用。

- 修正行動

  使用不同的快照重試備份。

  使用 `snap list`命令查看可用快照清單。

  如"指令參考資料ONTAP"需詳細 `snap list`資訊，請參閱。

找不到點陣圖檔案

- 訊息

  ```
  Unable to locate bitmap files
  ```

- 原因

  備份作業所需的點陣圖檔案可能已刪除。在此情況下、無法重新啟動備份。

- 修正行動

  再次執行備份。

Volume暫時處於過渡狀態

- 訊息

  ```
  Volume is temporarily in a transitional state
  ```

- 原因

  要備份的磁碟區暫時處於未掛載狀態。

- 修正行動

  等待一段時間、然後再次執行備份。

SMTape錯誤訊息

區塊順序不正常

- 訊息

  ```
  Chunks out of order
  ```

- 原因

  備份磁帶未依正確順序還原。

- 修正行動

  請重試還原作業、並依正確順序載入磁帶。

不支援區塊格式

- 訊息

  ```
  Chunk format not supported
  ```

- 原因

  備份映像不是SMTape。

- 修正行動

  如果備份映像不是SMtape、請使用具有SMtape備份的磁帶重試此作業。

無法分配記憶體

- 訊息

  ```
  Failed to allocate memory
  ```

- 原因

  系統記憶體不足。

- 修正行動

  系統不太忙時、請稍後再重試工作。

無法取得資料緩衝區

- 訊息

  ```
  Failed to get data buffer
  ```

- 原因

  儲存系統的緩衝區已用完。

- 修正行動

  等待部分儲存系統作業完成、然後重試工作。

找不到快照

- 訊息

  ```
  Failed to find snapshot
  ```

- 原因

  指定用於備份的快照不可用。

- 修正行動

  檢查指定的快照是否可用。如果沒有，請使用正確的快照重試。

無法建立快照

- 訊息

  ```
  Failed to create snapshot
  ```

- 原因

  磁碟區已包含快照的最大數量。

- 修正行動

  刪除一些快照，然後重試備份作業。

無法鎖定快照

- 訊息

  ```
  Failed to lock snapshot
  ```

- 原因

  快照正在使用中或已刪除。

- 修正行動

  如果快照正由另一個作業使用，請等待該作業完成，然後重試備份。如果已刪除快照，則無法執行備份。

無法刪除快照

- 訊息

  `Failed to delete snapshot`

- 原因

  無法刪除自動快照，因為其他作業正在使用此快照。

- 修正行動

  使用 `snap`命令來判斷快照的狀態。如果不需要快照，請手動刪除。

無法取得最新的快照

- 訊息

  `Failed to get latest snapshot`

- 原因

  最新的快照可能不存在，因為 SnapMirror 正在初始化該磁碟區。

- 修正行動

  初始化完成後重試。

無法載入新磁帶

- 訊息

  `Failed to load new tape`

- 原因

  磁帶機或媒體發生錯誤。

- 修正行動

  請更換磁帶並重試此作業。

無法初始化磁帶

- 訊息

  `Failed to initialize tape`

- 原因

  您可能會因為下列原因而收到此錯誤訊息：

  - 備份映像不是SMTape。
  - 指定的磁帶封鎖因素不正確。
  - 磁帶毀損或損壞。
  - 載入錯誤的磁帶以進行還原。
- 修正行動
  - 如果備份映像不是SMtape、請使用具有SMtape備份的磁帶重試此作業。
  - 如果封鎖因素不正確、請指定正確的封鎖因素、然後重試此作業。
  - 如果磁帶毀損、您將無法執行還原作業。
  - 如果載入錯誤的磁帶、請使用正確的磁帶重試操作。

無法初始化還原串流

- 訊息

  ```
  Failed to initialize restore stream
  ```
- 原因

  您可能會因為下列原因而收到此錯誤訊息：

  - 備份映像不是SMTape。
  - 指定的磁帶封鎖因素不正確。
  - 磁帶毀損或損壞。
  - 載入錯誤的磁帶以進行還原。
- 修正行動
  - 如果備份映像不是SMtape、請使用具有SMtape備份的磁帶重試此作業。
  - 如果封鎖因素不正確、請指定正確的封鎖因素、然後重試此作業。
  - 如果磁帶毀損、您將無法執行還原作業。
  - 如果載入錯誤的磁帶、請使用正確的磁帶重試操作。

無法讀取備份映像

- 訊息

  ```
  Failed to read backup image
  ```
- 原因

  磁帶毀損。

- 修正行動

  如果磁帶毀損、您將無法執行還原作業。

影像標頭遺失或毀損

- 訊息

  `Image header missing or corrupted`

- 原因

  磁帶不包含有效的SMTape備份。

- 修正行動

  重試含有有效備份的磁帶。

內部聲明

- 訊息

  `Internal assertion`

- 原因

  發生內部SMTape錯誤。

- 修正行動

  回報錯誤並傳送 `etc/log/backup` 歸檔至技術支援。

無效的備份映像幻數

- 訊息

  `Invalid backup image magic number`

- 原因

  備份映像不是SMTape。

- 修正行動

  如果備份映像不是SMtape、請使用具有SMtape備份的磁帶重試此作業。

無效的備份映像**Checksum**

- 訊息

  `Invalid backup image checksum`

- 原因

  磁帶毀損。

- 修正行動

  如果磁帶毀損、您將無法執行還原作業。

無效的輸入磁帶

- 訊息

  ```
  Invalid input tape
  ```

- 原因

  備份映像的簽名在磁帶標頭中無效。磁帶有毀損的資料或不包含有效的備份映像。

- 修正行動

  使用有效的備份映像重試還原工作。

無效的**Volume**路徑

- 訊息

  ```
  Invalid volume path
  ```

- 原因

  找不到用於備份或還原作業的指定磁碟區。

- 修正行動

  以有效的Volume路徑和Volume名稱重試工作。

備份集**ID**不相符

- 訊息

  ```
  Mismatch in backup set ID
  ```

- 原因

  磁帶變更期間載入的磁帶並非備份集的一部分。

- 修正行動

  載入正確的磁帶並重試工作。

備份時間戳記不相符

- 訊息

  `Mismatch in backup time stamp`

- 原因

  磁帶變更期間載入的磁帶並非備份集的一部分。

- 修正行動

  使用 `smtape restore -h` 用於驗證磁帶標頭資訊的命令。

工作因關機而中止

- 訊息

  `Job aborted due to shutdown`

- 原因

  儲存系統正在重新開機。

- 修正行動

  儲存系統重新開機後、請重試工作。

快照自動刪除導致工作中止

- 訊息

  `Job aborted due to snapshot autodelete`

- 原因

  磁碟區沒有足夠的空間，並觸發自動刪除快照。

- 修正行動

  釋放磁碟區中的空間、然後重試工作。

磁帶目前正由其他作業使用中

- 訊息

  `Tape is currently in use by other operations`

- 原因

  磁帶機正在由其他工作使用中。

- 修正行動

  在目前作用中的工作完成後、重試備份。

磁帶順序不正常

- 訊息

  ```
  Tapes out of order
  ```

- 原因

  用於還原作業的磁帶順序第一個磁帶沒有映像標頭。

- 修正行動

  將磁帶與映像標頭一起載入、然後重試工作。

傳輸失敗（**MetroCluster** 因為無法運作而中止）

- 訊息

  ```
  Transfer failed (Aborted due to MetroCluster operation)
  ```

- 原因

  SMTape作業會因切換或切換作業而中止。

- 修正行動

  切換或切換作業完成後、請執行SMTape作業。

傳輸失敗（**ARL**初始中止）

- 訊息

  ```
  Transfer failed (ARL initiated abort)
  ```

- 原因

  如果啟動了Aggregate重新定位、則SMTape作業會在進行中、然後中止。

- 修正行動

  完成Aggregate重新配置作業後、請執行SMTape作業。

傳輸失敗（**CFO**啟動中止）

- 訊息

  ```
  Transfer failed (CFO initiated abort)
  ```

- 原因

  由於CFO Aggregate的儲存容錯移轉（接管和恢復）作業、SMTape作業會中止。

- 修正行動

  CFO Aggregate的儲存容錯移轉完成後、請執行SMTape作業。

傳輸失敗（ **SFO** 起始中止）

- 訊息

  ```
  Transfer failed (SFO initiated abort)
  ```

- 原因

  由於儲存容錯移轉（接管與恢復）作業、SMTape作業會中止。

- 修正行動

  儲存容錯移轉（接管與恢復）作業完成後、請執行SMTape作業。

移轉中的基礎**Aggregate**

- 訊息

  ```
  Underlying aggregate under migration
  ```

- 原因

  如果SMTape作業是在移轉中的集合體上啟動（儲存容錯移轉或集合體重新配置）、則SMTape作業會失敗。

- 修正行動

  完成Aggregate移轉後、請執行SMTape作業。

Volume目前正在移轉中

- 訊息

  ```
  Volume is currently under migration
  ```

- 原因

  Volume移轉與SMTape備份無法同時執行。

- 修正行動

  磁碟區移轉完成後、請重試備份工作。

Volume離線

- 訊息

  `Volume offline`

- 原因

  正在備份的Volume已離線。

- 修正行動

  將磁碟區上線、然後重試備份。

Volume不受限制

- 訊息

  `Volume not restricted`

- 原因

  將資料還原至的目的地Volume並不受限制。

- 修正行動

  限制磁碟區、然後重試還原作業。

NDMP 組態

瞭解 ONTAP NDMP 組態

您可以快速設定ONTAP 一個叢集、使用網路資料管理傳輸協定（NDMP）、使用協力廠商備份應用程式將資料直接備份到磁帶。

如果備份應用程式支援叢集感知備份（Cab）、您可以將NDMP設定為_SVM範圍_或_節點範圍_：

- 叢集（管理SVM）層級的SVM範圍可讓您備份叢集不同節點上裝載的所有Volume。建議盡可能以SVM為範圍的NDMP。
- 節點範圍的NDMP可讓您備份該節點上裝載的所有磁碟區。

如果備份應用程式不支援CAb、您必須使用節點範圍的NDMP。

SVM範圍和節點範圍的NDMP是互不相容的、無法在同一個叢集上設定。

節點範圍的NDMP在ONTAP 支援方面已不再適用。9

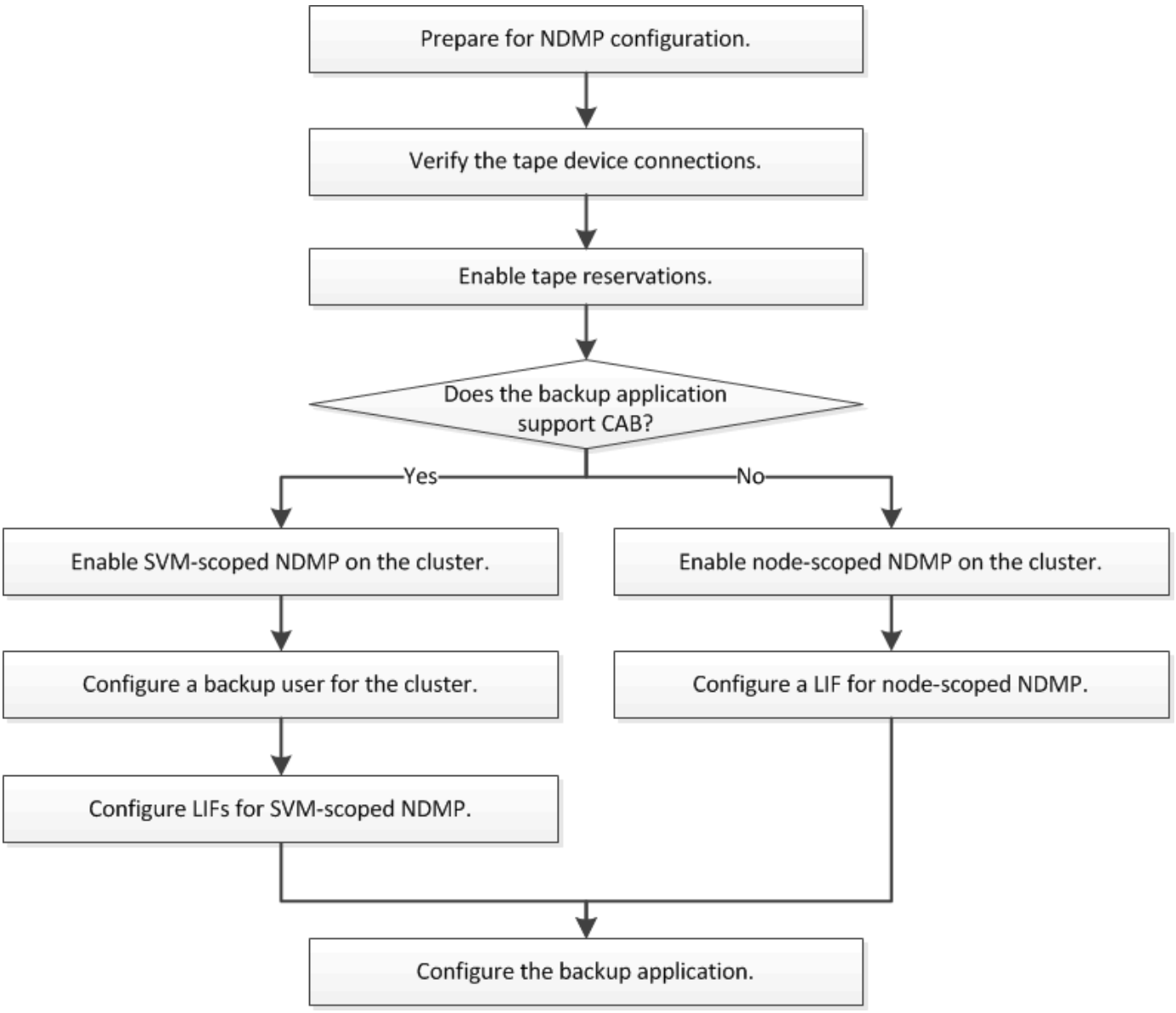
深入瞭解 "叢集感知備份（CAB）"。

在設定NDMP之前、請確認下列事項：

- 您擁有第三方備份應用程式（也稱為資料管理應用程式或DMA）。
- 您是叢集管理員。
- 安裝磁帶設備和可選的媒體服務器。
- 磁帶設備通過光纖通道 (FC) 交換機或本地連接的交換機連接到羣集。
- 至少有一個磁帶設備的邏輯單元號碼（LUN）為0。

了解 **ONTAP NDMP** 設定工作流程

透過NDMP設定磁帶備份涉及準備NDMP組態、驗證磁帶設備連線、啟用磁帶保留、在SVM或節點層級設定NDMP、在叢集上啟用NDMP、設定備份使用者、設定LIF及設定備份應用程式。



準備 ONTAP NDMP 配置

在透過網路資料管理傳輸協定（NDMP）設定磁帶備份存取之前、您必須先確認是否支援所規劃的組態、確認每個節點上的磁帶機均列為合格的磁碟機、確認所有節點都具有叢集間的LIF、 並識別備份應用程式是否支援叢集感知備份（Cab）擴充功能。

步驟

1. 請參閱備份應用程式供應商的ONTAP 支援資訊表以取得支援功能（NetApp不符合ONTAP 使用支援功能的協力廠商備份應用程式要求）。

   您應該確認下列NetApp元件是否相容：

   - 叢集上執行的版本。ONTAP
   - 備份應用程式廠商與版本：例如Veritas NetBackup 8.2或CommVault。
   - 磁帶設備的詳細資料、例如磁帶機的製造商、機型和介面：例如IBM ultrium8或HPE StoreEver ultrium30750 LTO-8。
   - 叢集中節點的平台：例如 FAS8700 或 A400 。

   > ⓘ 您可以在中找到ONTAP 舊版的支援資料、以供備份應用程式使用 "NetApp 互通性對照表工具"。

2. 驗證您的磁帶機是否在每個節點的內建磁帶組態檔中列為合格的磁碟機：

   a. 在命令列介面上、使用檢視內建的磁帶組態檔案 `storage tape show-supported-status` 命令。

   ```
   cluster1::> storage tape show-supported-status

   Node: cluster1-1
                                    Is
   Tape Drives                      Supported  Support Status
   -------------------------------  ---------
   -------------------------------
   Certance Ultrium 2               true       Dynamically Qualified
   Certance Ultrium 3               true       Dynamically Qualified
   Digital DLT2000                  true       Qualified
   ```

   b. 將磁帶機與輸出中的合格磁碟機清單進行比較。

   > ⓘ 輸出中的磁帶設備名稱可能與裝置標籤或互通性對照表中的名稱略有不同。例如、數位DLT2000也稱為「DLT2k」。您可以忽略這些次要的命名差異。

   c. 如果某個裝置未在輸出內容中列為合格裝置，則即使該裝置在互通性對照表中列為合格，仍請依照 NetApp 支援網站上的指示，為該裝置下載並安裝更新的組態檔。

   "NetApp下載：磁帶設備組態檔案"

如果磁帶設備在出貨後符合資格、則內建磁帶組態檔中可能不會列出合格的裝置。

3. 驗證叢集中的每個節點都有叢集間LIF：

   a. 使用檢視節點上的叢集間生命體 `network interface show -role intercluster` 命令。

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
```

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

   b. 如果叢集間 LIF 不存在於任何節點、請使用建立叢集間 LIF `network interface create` 命令。

```
cluster1::> network interface create -vserver cluster1 -lif IC2 -role
intercluster
-home-node cluster1-2 -home-port e0b -address 192.0.2.68 -netmask
255.255.255.0
-status-admin up -failover-policy local-only -firewall-policy
intercluster

cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

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

"網路管理"

4. 使用備份應用程式隨附的文件、識別備份應用程式是否支援叢集感知備份（Cab）。

   在判斷您可以執行的備份類型時、駕駛室內的支援是關鍵因素。

相關資訊

- "儲存磁帶秀"
- "儲存磁帶顯示支援狀態"

驗證 ONTAP NDMP 磁帶設備連接

您必須確保ONTAP 所有的磁碟機和媒體更換器都能在「視覺化」裝置中看到。

步驟

1. 使用檢視所有磁碟機和媒體更換器的相關資訊 `storage tape show` 命令。

```
cluster1::> storage tape show

Node: cluster1-01
Device ID                 Device Type     Description
Status
------------------------  --------------  ------------------------------
--------
sw4:10.11                 tape drive      HP LTO-3
normal
0b.125L1                  media changer   HP MSL G3 Series
normal
0d.4                      tape drive      IBM LTO 5 ULT3580
normal
0d.4L1                    media changer   IBM 3573-TL
normal
...
```

2. 如果未顯示磁帶機、請疑難排解問題。
3. 如果未顯示媒體更換器、請使用檢視媒體更換器的相關資訊 `storage tape show-media-changer` 然後疑難排解問題。

```
cluster1::> storage tape show-media-changer

Media Changer: sw4:10.11L1
  Description: PX70-TL
         WWNN: 2:00a:000e11:10b919
         WWPN: 2:00b:000e11:10b919
Serial Number: 00FRU7800000_LL1

       Errors: -

Paths:
Node                      Initiator  Alias    Device State
Status
------------------------  ---------  -------  ------------------------
--------
cluster1-01               2b         mc0      in-use
normal
...
```

相關資訊

- "儲存磁帶顯示媒體轉換器"

為 ONTAP NDMP 備份作業啟用磁帶預留

您必須確保磁帶機保留供備份應用程式用於NDMP備份作業。

關於這項工作

保留設定在不同的備份應用程式中會有所不同、而且這些設定必須符合備份應用程式、以及使用相同磁碟機的節點或伺服器。如需正確的保留設定、請參閱備份應用程式的廠商文件。

步驟

1. 使用啟用預約 `options -option-name tape.reservations -option-value persistent` 命令。

   下列命令可啟用的保留 `persistent` 價值：

   ```
   cluster1::> options -option-name tape.reservations -option-value
   persistent
   2 entries were modified.
   ```

2. 使用確認已在所有節點上啟用保留 `options tape.reservations` 然後檢閱輸出。

```
cluster1::> options tape.reservations

cluster1-1
    tape.reservations                 persistent

cluster1-2
    tape.reservations                 persistent
2 entries were displayed.
```

設定SVM範圍的NDMP

在 ONTAP 叢集上啟用 SVM 範圍的 NDMP

如果DMA支援叢集感知備份（叢集感知備份）擴充、您可以啟用SVM範圍NDMP、在叢集（管理SVM）上啟用NDMP服務、以及設定資料與控制連線的LIF、來備份叢集中不同節點上託管的所有磁碟區。

開始之前

DMA必須支援駕駛擴充功能。

關於這項工作

關閉節點範圍的NDMP模式可在叢集上啟用SVM範圍的NDMP模式。

步驟

1. 啟用 SVM 範圍的 NDMP 模式：

   ```
   cluster1::> system services ndmp node-scope-mode off
   ```

   已啟用 SVM 範圍的 NDMP 模式。

2. 在管理 SVM 上啟用 NDMP 服務：

   ```
   cluster1::> vserver services ndmp on -vserver cluster1
   ```

   驗證類型設為 `challenge` 預設會停用純文字驗證。

   > 為了安全通訊、您應該停用純文字驗證。

3. 確認 NDMP 服務已啟用：

   ```
   cluster1::> vserver services ndmp show
   ```

```
Vserver       Enabled   Authentication type
------------- --------- -------------------
cluster1      true      challenge
vs1           false     challenge
```

為備份使用者啟用 **ONTAP NDMP** 身份驗證

若要從備份應用程式驗證SVM範圍的NDMP、必須有具有足夠權限和NDMP密碼的管理使用者。

關於這項工作

您必須為備份管理使用者產生NDMP密碼。您可以在叢集或SVM層級啟用備份管理使用者、並視需要建立新的使用者。依預設、具有下列角色的使用者可以驗證NDMP備份：

- 全叢集： `admin` 或 `backup`
- 個別SVM： `vsadmin` 或 `vsadmin-backup`

如果您使用的是NIS或LDAP使用者、則該使用者必須存在於各自的伺服器上。您無法使用Active Directory使用者。

步驟

1. 顯示目前的管理員使用者和權限：

   ```
   security login show
   ```

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

2. 如有需要、請使用建立新的NDMP備份使用者 `security login create` 命令及適當角色、以取得全叢集或個別SVM權限。

   您可以為指定本機備份使用者名稱、或指定 NIS 或 LDAP 使用者名稱 `-user-or-group-name` 參數。

   下列命令會建立備份使用者 `backup_admin1` 使用 `backup` 整個叢集的角色：

   ```
   cluster1::> security login create -user-or-group-name backup_admin1
   -application ssh -authmethod password -role backup
   ```

   下列命令會建立備份使用者 `vsbackup_admin1` 使用 `vsadmin-backup` 個別SVM的角色：

   ```
   cluster1::> security login create -user-or-group-name vsbackup_admin1
   -application ssh -authmethod password -role vsadmin-backup
   ```

   輸入新使用者的密碼並確認。

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

3. 使用為管理 SVM 產生密碼 `vserver services ndmp generate password` 命令。

產生的密碼必須用於驗證備份應用程式的NDMP連線。

```
cluster1::> vserver services ndmp generate-password -vserver cluster1
-user backup_admin1

 Vserver: cluster1
    User: backup_admin1
Password: qG5CqQHYxw7tE57g
```

為 SVM 範圍的 NDMP 設定 ONTAP LIF

您必須識別要用於在資料與磁帶資源之間建立資料連線的生命期、以及用於控制管理SVM與備份應用程式之間的連線。識別出生命之後、您必須確認已設定服務和容錯移轉原則。

> 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需更多資訊、請參閱 "管理支援的流量"。

ONTAP 9 。 10.1 或更新版本

步驟

1. 使用命令搭配 `-service-policy`參數、識別節點上託管的叢集間 `LIF` `network interface show` 。

   ```
   network interface show -service-policy default-intercluster
   ```

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

2. 使用命令搭配 `-service-policy`參數、識別節點上託管的管理 `LIF` `network interface show` 。

   ```
   network interface show -service-policy default-management
   ```

3. 確保叢集間 LIF 包含 `backup-ndmp-control`以下服務：

   ```
   network interface service-policy show
   ```

   如"指令參考資料ONTAP"需詳細 `network interface service-policy show`資訊，請參閱。

4. 請確定已針對所有生命期適當設定容錯移轉原則：

   a. 確認叢集管理 LIF 的容錯移轉原則已設定為 `broadcast-domain-wide`，而叢集間和節點管理階層的原則則設定為 `local-only` 使用 `network interface show -failover` 命令。

      下列命令會顯示叢集管理、叢集間和節點管理生命體的容錯移轉原則：

```
cluster1::> network interface show -failover

           Logical          Home             Failover    Failover
Vserver    Interface        Node:Port        Policy      Group
-------    --------------   --------------   ----------  --------
cluster    cluster1_clus1   cluster1-1:e0a   local-only  cluster
                                                         Failover
Targets:
                                                         .......
cluster1   cluster_mgmt     cluster1-1:e0m   broadcast-  Default
                                                domain-wide
                                                         Failover
Targets:
                                                         .......
           IC1              cluster1-1:e0a   local-only  Default
                                                         Failover
Targets:
           IC2              cluster1-1:e0b   local-only  Default
                                                         Failover
Targets:
                                                         .......
cluster1-1 c1-1_mgmt1       cluster1-1:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
cluster1-2 c1-2_mgmt1       cluster1-2:e0m   local-only  Default
                                                         Failover
Targets:
                                                         ......
```

a. 如果未適當設定容錯移轉原則、請使用修改容錯移轉原則 `network interface modify` 命令 `-failover-policy` 參數。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

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

5. 使用指定資料連線所需的生命 `vserver services ndmp modify` 命令 `preferred-interface-role` 參數。

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

6. 使用確認已為叢集設定偏好的介面角色 `vserver services ndmp show` 命令。

```
cluster1::> vserver services ndmp show -vserver cluster1

                Vserver: cluster1
                NDMP Version: 4
                .......
                .......
Preferred Interface Role: intercluster, cluster-mgmt, node-mgmt
```

ONTAP 9 9 或更早版本

步驟

1. 使用識別叢集間、叢集管理和節點管理階層的生命 `network interface show` 命令 `-role` 參數。

   下列命令會顯示叢集間的LIF：

```
cluster1::> network interface show -role intercluster

            Logical      Status     Network            Current
Current Is
Vserver     Interface    Admin/Oper Address/Mask       Node
Port    Home
----------- ----------   ---------- ------------------ -------------
------- ----
cluster1    IC1          up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2          up/up      192.0.2.68/24      cluster1-2
e0b     true
```

   下列命令會顯示叢集管理LIF：

```
cluster1::> network interface show -role cluster-mgmt

            Logical       Status     Network            Current
Current Is
Vserver     Interface     Admin/Oper Address/Mask       Node
Port    Home
----------- ----------    ---------- ------------------ -----------
------- ----
cluster1    cluster_mgmt  up/up      192.0.2.60/24      cluster1-2
e0M     true
```

   以下命令顯示節點管理生命體：

```
cluster1::> network interface show -role node-mgmt

            Logical           Status     Network          Current
Current Is
Vserver     Interface         Admin/Oper Address/Mask     Node
Port    Home
----------- ----------        ---------- ---------------
------------  ------  ------
cluster1    cluster1-1_mgmt1  up/up      192.0.2.69/24    cluster1-1
e0M     true
            cluster1-2_mgmt1  up/up      192.0.2.70/24    cluster1-2
e0M     true
```

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

2. 確保已爲羣集間 NDMP 、羣集管理(`cluster-mgmt`和節點管理(`node-mgmt`（）生命體上的 NDMP 啓用防火牆策略：

   a. 使用驗證是否已啟用 NDMP 的防火牆原則 `system services firewall policy show` 命令。

      下列命令會顯示叢集管理LIF的防火牆原則：

```
cluster1::> system services firewall policy show -policy cluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -----------------
cluster     cluster      dns        0.0.0.0/0
                         http       0.0.0.0/0
                         https      0.0.0.0/0
                         ndmp       0.0.0.0/0
                         ndmps      0.0.0.0/0
                         ntp        0.0.0.0/0
                         rsh        0.0.0.0/0
                         snmp       0.0.0.0/0
                         ssh        0.0.0.0/0
                         telnet     0.0.0.0/0
10 entries were displayed.
```

      下列命令會顯示叢集間LIF的防火牆原則：

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

下列命令會顯示節點管理LIF的防火牆原則：

```
cluster1::> system services firewall policy show -policy mgmt

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1-1  mgmt         dns        0.0.0.0/0, ::/0
                         http       0.0.0.0/0, ::/0
                         https      0.0.0.0/0, ::/0
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      0.0.0.0/0, ::/0
                         ntp        0.0.0.0/0, ::/0
                         rsh        -
                         snmp       0.0.0.0/0, ::/0
                         ssh        0.0.0.0/0, ::/0
                         telnet     -
10 entries were displayed.
```

b. 如果未啟用防火牆原則、請使用啟用防火牆原則 `system services firewall policy modify` 命令 `-service` 參數。

下列命令可啟用叢集間LIF的防火牆原則：

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 請確定已針對所有生命期適當設定容錯移轉原則：

a. 確認叢集管理 LIF 的容錯移轉原則已設定為 `broadcast-domain-wide`，而叢集間和節點管理階層的原則則設定為 `local-only` 使用 `network interface show -failover` 命令。

   下列命令會顯示叢集管理、叢集間和節點管理生命體的容錯移轉原則：

```
cluster1::> network interface show -failover

          Logical            Home               Failover
Failover
Vserver   Interface          Node:Port          Policy
Group
--------- -----------------  ------------------ --------------------
--------
cluster   cluster1_clus1     cluster1-1:e0a     local-only
cluster
                                                     Failover
Targets:
                                                     .......

cluster1  cluster_mgmt       cluster1-1:e0m     broadcast-domain-
wide Default
                                                     Failover
Targets:
                                                     .......
          IC1                 cluster1-1:e0a     local-only
Default
                                                     Failover
Targets:
          IC2                 cluster1-1:e0b     local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1 cluster1-1_mgmt1  cluster1-1:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
cluster1-2 cluster1-2_mgmt1  cluster1-2:e0m     local-only
Default
                                                     Failover
Targets:
                                                     ......
```

a. 如果未適當設定容錯移轉原則、請使用修改容錯移轉原則 `network interface modify` 命令 `-failover-policy` 參數。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

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

4. 使用指定資料連線所需的生命 `vserver services ndmp modify` 命令 `preferred-interface-role` 參數。

```
cluster1::> vserver services ndmp modify -vserver cluster1
-preferred-interface-role intercluster,cluster-mgmt,node-mgmt
```

5. 使用確認已為叢集設定偏好的介面角色 `vserver services ndmp show` 命令。

```
cluster1::> vserver services ndmp show -vserver cluster1

                            Vserver: cluster1
                       NDMP Version: 4
                       .......
                       .......
            Preferred Interface Role: intercluster, cluster-mgmt,
node-mgmt
```

設定節點範圍的NDMP

在 ONTAP 叢集上啟用節點範圍的 NDMP

您可以啟用節點範圍的NDMP、啟用NDMP服務、以及設定LIF以進行資料和控制連線、來備份單一節點上託管的磁碟區。這可針對叢集的所有節點執行。

節點範圍的NDMP在ONTAP 支援方面已不再適用。9

關於這項工作

在節點範圍模式下使用NDMP時、必須根據節點來設定驗證。如需詳細資訊、請參閱 "知識庫文章「How to configure NDMP authentication in the 'node-sc鏡' mode（如何在「node-sc入 模式」中設定NDMP驗證）」"。

步驟

1. 啟用節點範圍 NDMP 模式：

```
cluster1::> system services ndmp node-scope-mode on
```

NDMP 節點範圍模式已啟用。

2. 在叢集中的所有節點上啟用 NDMP 服務：

   使用萬用字元「*」可同時在所有節點上啟用NDMP服務。

   您必須指定密碼、以便備份應用程式驗證NDMP連線。

```
cluster1::> system services ndmp on -node *
```

```
Please enter password:
Confirm password:
2 entries were modified.
```

3. 停用 `-clear-text` 安全通訊 NDMP 密碼的選項：

   使用萬用字元「」*" disables the `-clear-text 同時在所有節點上執行選項。

```
cluster1::> system services ndmp modify -node * -clear-text false
```

4. 確認 NDMP 服務已啟用、且 `-clear-text` 選項已停用：

```
cluster1::> system services ndmp show
```

```
Node                  Enabled   Clear text  User Id
--------------------- --------- ----------- ---------
cluster1-1            true      false        root
cluster1-2            true      false        root
2 entries were displayed.
```

為節點範圍的 **NDMP** 設定 **ONTAP LIF**

您必須識別LIF、用於建立節點與備份應用程式之間的資料連線和控制連線。識別LIF之後、您必須確認是否已針對LIF設定防火牆和容錯移轉原則。

> 從ONTAP S振 分9.10.1開始、防火牆原則已過時、並完全由LIF服務原則取代。如需更多資訊、請參閱 "管理支援的流量"。

ONTAP 9 。 10.1 或更新版本

步驟

1. 使用命令搭配 `-service-policy`參數、識別節點上託管的叢集間 `LIF` `network interface show` 。

```
network interface show -service-policy default-intercluster
```

2. 確保叢集間 LIF 包含 `backup-ndmp-control`以下服務：

```
network interface service-policy show
```

3. 確保已針對叢集間的生命體設定適當的容錯移轉原則：

   a. 確認叢集間的生命體的容錯移轉原則已設定為 `local-only` 使用 `network interface show -failover` 命令。

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                     Failover
Targets:
                                                     .......
            IC2               cluster1-2:e0b    local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                     Failover
Targets:
                                                     .......
```

   b. 如果未適當設定容錯移轉原則、請使用修改容錯移轉原則 `network interface modify` 命令 `-failover-policy` 參數。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

深入瞭解 `network interface show`，`network interface service-policy show`和 `network interface modify` "指令參考資料ONTAP"。

ONTAP 9 9 或更早版本

步驟

1. 使用識別節點上託管的叢集間 LIF `network interface show` 命令 `-role` 參數。

```
cluster1::> network interface show -role intercluster

            Logical    Status     Network            Current
Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node
Port    Home
----------- ---------- ---------- ------------------ -------------
------- ----
cluster1    IC1        up/up      192.0.2.65/24      cluster1-1
e0a     true
cluster1    IC2        up/up      192.0.2.68/24      cluster1-2
e0b     true
```

2. 確保在叢集間的LIF上啟用NDMP的防火牆原則：

   a. 使用驗證是否已啟用 NDMP 的防火牆原則 `system services firewall policy show` 命令。

      下列命令會顯示叢集間LIF的防火牆原則：

```
cluster1::> system services firewall policy show -policy
intercluster

Vserver     Policy       Service    Allowed
-------     ------------ ---------- -------------------
cluster1    intercluster dns        -
                         http       -
                         https      -
                         ndmp       0.0.0.0/0, ::/0
                         ndmps      -
                         ntp        -
                         rsh        -
                         ssh        -
                         telnet     -
9 entries were displayed.
```

   b. 如果未啟用防火牆原則、請使用啟用防火牆原則 `system services firewall policy modify` 命令 `-service` 參數。

下列命令可啟用叢集間LIF的防火牆原則：

```
cluster1::> system services firewall policy modify -vserver cluster1
-policy intercluster -service ndmp 0.0.0.0/0
```

3. 確保已針對叢集間的生命體設定適當的容錯移轉原則：

   a. 確認叢集間的生命體的容錯移轉原則已設定為 `local-only` 使用 `network interface show -failover` 命令。

```
cluster1::> network interface show -failover
            Logical          Home               Failover
Failover
Vserver     Interface        Node:Port          Policy       Group
--------    ---------------  -----------------  ------------
--------
cluster1    IC1               cluster1-1:e0a    local-only
Default
                                                     Failover
Targets:
                                                     .......
            IC2               cluster1-2:e0b    local-only
Default
                                                     Failover
Targets:
                                                     .......
cluster1-1  cluster1-1_mgmt1 cluster1-1:e0m    local-only
Default
                                                     Failover
Targets:
                                                     .......
```

   b. 如果未適當設定容錯移轉原則、請使用修改容錯移轉原則 `network interface modify` 命令 `-failover-policy` 參數。

```
cluster1::> network interface modify -vserver cluster1 -lif IC1
-failover-policy local-only
```

深入瞭解 `network interface show`及 `network interface modify` "指令參考資料ONTAP"。

為 ONTAP NDMP 配置配置備份應用程式

將叢集設定為可存取NDMP之後、您必須從叢集組態收集資訊、然後在備份應用程式中設定其餘的備份程序。

步驟

1. 收集您先前在ONTAP 《不知何種情況下所設定的下列資訊：
   - 備份應用程式建立NDMP連線所需的使用者名稱和密碼
   - 備份應用程式連線至叢集所需的叢集間生命體IP位址
2. 在 ONTAP 中、使用顯示 ONTAP 指派給每個裝置的別名 `storage tape alias show` 命令。

   別名通常在設定備份應用程式時很有用。

```
cluster1::> storage tape show -alias

  Device ID: 2a.0
Device Type: tape drive
Description: Hewlett-Packard LTO-5

Node                          Alias     Mapping
----------------------------- --------- ------------------------------
stsw-3220-4a-4b-02            st2       SN[HU19497WVR]
...
```

3. 在備份應用程式中、使用備份應用程式的文件來設定其餘的備份程序。

完成後

如果發生資料移動事件（例如磁碟區移動或LIF移轉）、您必須準備好重新初始化任何中斷的備份作業。

相關資訊

- "儲存磁帶別名顯示"

在不同時複寫NetApp Element 功能的軟體與ONTAP 非本性概述之間

您可以使用 SnapMirror 將元素磁碟區的快照複製到 ONTAP 目的地，確保元素系統上的業務持續運作。萬一Element站台發生災難、您可以從ONTAP 該系統將資料提供給用戶端、然後在恢復服務時重新啟動Element系統。

從 ONTAP 9.4 開始，您可以將在 ONTAP 節點上建立的 LUN 快照複寫回元素系統。您可能在Element站台當機期間建立LUN、或是使用LUN將資料從ONTAP 無法修復的軟體移轉至Element軟體。

"設定 NetApp Element 軟體和 ONTAP 的複寫"。

事件、效能和健全狀況監控

使用System Manager監控叢集效能

使用 ONTAP 系統管理器監控叢集效能

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

關於這項工作

此程序適用於 FAS、AFF 和 ASA 系統。如果您擁有 ASA r2 系統（ASA A1K、ASA A90、ASA A70、ASA A50、ASA A30、ASA A20 或 ASA C30），請遵循"這些步驟"監控您的叢集效能。ASA R2 系統提供專為僅限 SAN 的客戶所提供的簡化 ONTAP 體驗。

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

儀表板可讓您判斷下列資訊：

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

在「健全狀況與容量」總覽中、您可以按一下 → 以檢視其他資訊並執行工作。

在「效能」總覽中、您可以根據小時、日、週、月或年來檢視指標。

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

了解如何在 ONTAP System Manager 儀表板上查看叢集

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

使用 System Manager 儀表板、您可以一眼檢視重要警示和通知的相關資訊、儲存層和磁碟區的效率和容量、叢集中可用的節點、高可用度（ HA ）配對中節點的狀態、最活躍的應用程式和物件、 以及叢集或節點的效能指標。

儀表板包含四個面板、如下所述：

健全狀況

「健全狀況」檢視會顯示叢集中所有可搜尋節點整體健全狀況的相關資訊。

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

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

容量

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

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

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

網路

「網路」檢視會顯示屬於網路一部分的實體連接埠、網路介面和儲存 VM 。

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

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

效能

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

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

效能檢視會顯示與延遲、處理量和 IOPS 相關的整體效能指標。

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

效能值每3秒重新整理一次、效能圖表每15秒重新整理一次。如果無法取得叢集效能的相關資訊、將不會顯示圖表。

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

在 ONTAP 系統管理員中辨識熱捲和其他對象

識別經常存取的磁碟區（熱磁碟區）和資料（熱物件）、加速叢集效能。

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

步驟

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

在 ONTAP 系統管理員中修改 QoS

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

步驟

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

在 ONTAP 系統管理員中監控風險

從 ONTAP 9 .10.0 開始、您可以使用系統管理員來監控 Active IQ 數位顧問（也稱為數位顧問）回報的風險。從版本《21》開始ONTAP 、您可以使用System Manager來確認風險。

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

連結至您的數位顧問帳戶

若要從 Digital Advisor 接收風險相關資訊、您應該先從 System Manager 連結至 Digital Advisor 帳戶。

步驟

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

檢視風險數量

從 ONTAP 9 。 10.0 開始、您可以從系統管理員的儀表板檢視數位顧問報告的風險數。

開始之前

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

步驟

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

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

檢視風險詳細資料

從 ONTAP 9 。 10.0 開始、您可以從系統管理員檢視數位顧問報告的風險如何依影響區域分類。您也可以檢視每個已報告風險的詳細資訊、其對系統的潛在影響、以及您可以採取的修正行動。

開始之前

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

步驟

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

瞭解風險

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

步驟

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

> 在您確認風險之後、需要幾分鐘時間才能將變更反映在數位顧問建議清單中。

不承認風險

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

步驟

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

在您不承認風險之後、需要幾分鐘時間才能將變更反映在數位顧問建議清單中。

利用 **ONTAP System Manager** 洞察優化您的系統

有了System Manager、您可以檢視有助於最佳化系統的洞見。

關於這項工作

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

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

- 封鎖延伸可能會導致非預期的結果。 * 從 ONTAP 9.11.1 開始、您可以使用系統管理員為儲存 VM 啟用原生 FPolicy 。您可能會收到 System Manager Insight 的訊息、建議您這樣做 "設定原生 FPolicy" 適用於儲存 VM 。

使用 FPolicy 原生模式、您可以允許或不允許特定的副檔名。System Manager 建議使用超過 3000 個不允許的檔案副檔名、這些副檔名曾在過去的勒索軟體攻擊中使用過。 您環境中的合法檔案可能會使用其中一些副檔名、而封鎖這些副檔名可能會導致非預期的問題。

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

若要深入瞭解原生 FPolicy 、請參閱"Fpolicy 組態類型"。

根據最佳實務做法、這些洞見會顯示在單一頁面上、您可以立即採取行動來最佳化系統。如需更多資訊、請參閱 "System Manager 洞見"。

檢視最佳化洞見

步驟

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

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

- 需要您的注意
- 補救風險

◦ 最佳化您的儲存設備

2. （選用）按一下頁面右上角的這些按鈕、篩選所顯示的洞見：
   - ◦ 顯示安全性相關洞見。
   - ◦ 顯示容量相關洞見。
   - ◦ 顯示與組態相關的洞見。
   - ◦ All 顯示所有洞見。

回應洞見以最佳化您的系統

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

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 將游標停留在深入資訊上、即可顯示可執行下列動作的按鈕：
   - ◦ 解除：從檢視中移除深入見解。若要取消關注，請參閱[customize-settings-insights] 。
   - ◦ 瀏覽：瞭解各種方法、以修正深入見解中提及的問題。 只有在有多種補救方法時、才會顯示此按鈕。
   - ◦ 修正：啟動補救Insight中提及問題的程序。系統會要求您確認是否要採取套用修正程式所需的行動。

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

自訂深入分析的設定

您可以在 System Manager 中自訂要通知的深入資訊。

步驟

1. 在System Manager中、按一下左側導覽欄中的* Insights *。
2. 在頁面右上角、按一下 ⋮、然後選取 * 設定 * 。
3. 在*設定*頁面上、請確認您要收到通知的深入資訊旁的核取方塊有勾選。如果您之前忽略了某個見解，則可以透過確保核取方塊中有勾選來取消忽略它。
4. 按一下「 * 儲存 * 」 。

將洞見匯出成**PDF**檔案

您可以將所有適用的洞見匯出成PDF檔案。

步驟

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

在 ONTAP 系統管理員中設定本機 FPolicy

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

開始之前

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

若要深入瞭解 FPolicy 組態類型、請"FPolicy組態類型"參閱。

步驟

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

   ◦ 封鎖延伸可能會導致非預期的結果。 * 從 ONTAP 9.11.1 開始、您可以使用系統管理員為儲存 VM 啟用原生 FPolicy 。
   使用 FPolicy 原生模式、您可以允許或不允許特定的副檔名。System Manager 建議使用超過 3000 個不允許的檔案副檔名、這些副檔名曾在過去的勒索軟體攻擊中使用過。 您環境中的合法檔案可能會使用其中一些副檔名、而封鎖這些副檔名可能會導致非預期的問題。

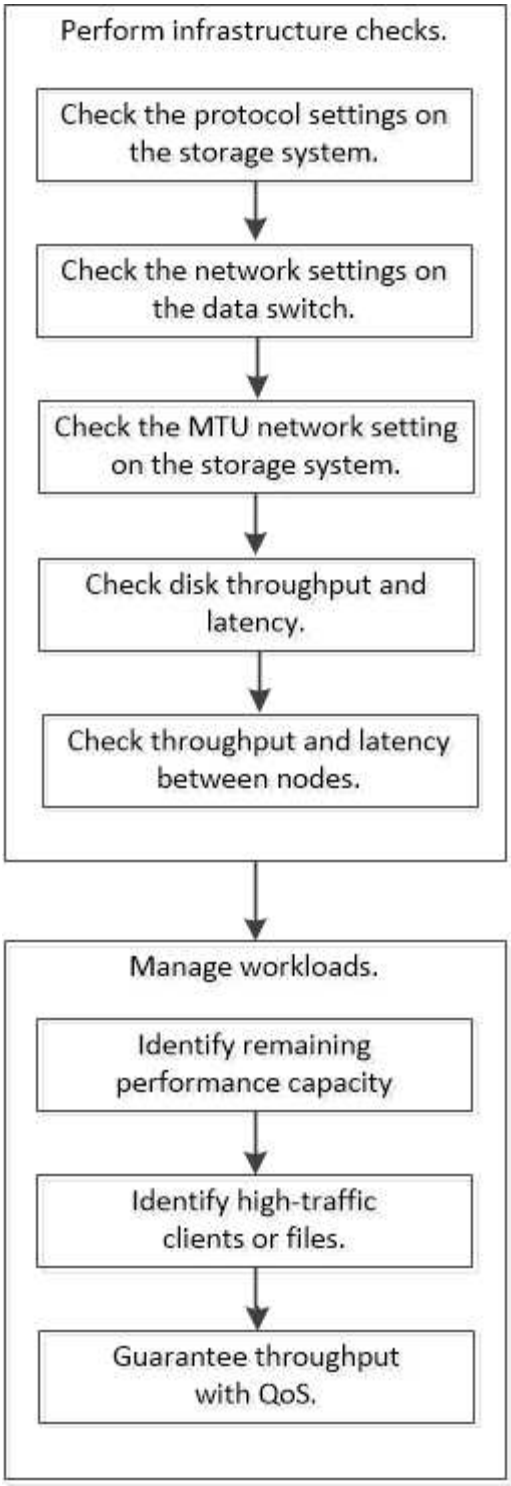
   因此、強烈建議您修改擴充功能清單、以符合您環境的需求。請參閱 "如何從系統管理員使用系統管理員建立的原生 FPolicy 組態中移除副檔名、以重新建立原則"。

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

使用CLI監控及管理叢集效能

ONTAP效能管理工作流程

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



執行基礎架構檢查

檢查儲存系統上的傳輸協定設定

檢查**ONTAP NFS TCP** 最大傳輸大小

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

開始之前

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

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查TCP最大傳輸大小：

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

3. 如果TCP最大傳輸大小太小、請增加大小：

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

4. 返回管理權限層級：

   ```
   set -privilege admin
   ```

範例

下列範例變更的 TCP 傳輸大小上限 `SVM1` 至 1048576 ：

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

檢查**ONTAP iSCSI TCP** 讀取/寫入大小

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

開始之前

此工作需要進階權限層級命令。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查TCP視窗大小設定：

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

3. 修改TCP視窗大小設定：

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

4. 返回管理權限：

```
set -privilege admin
```

範例

下列範例變更的 TCP 視窗大小 SVM1 至 131,400 位元組：

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

檢查ONTAP CIFS/SMB 多工設定

如果CIFS網路效能緩慢導致效能問題、您可以修改多工設定來改善及修正。

步驟

1. 檢查CIFS多工設定：

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

2. 修改CIFS多工設定：

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

範例

下列範例會變更最大多工處理次數 SVM1 至 255 ：

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

檢查ONTAP FC 適配器連接埠速度

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

開始之前

使用此介面卡做為其主連接埠的所有LIF都必須離線。

步驟

1. 使介面卡離線：

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

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

2. 檢查連接埠介面卡的最大速度：

   ```
   fcp adapter show -instance
   ```

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

3. 如有必要、請變更連接埠速度：

   ```
   network fcp adapter modify -node nodename -adapter adapter -speed
   {1|2|4|8|10|16|auto}
   ```

4. 將介面卡上線：

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

5. 將介面卡上的所有生命都上線：

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

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

範例

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

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

檢查資料交換器上的**ONTAP**網路設置

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

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

步驟

1. 對於資料交換器、請檢查MTU大小是否設為9022或更高。

如需詳細資訊、請參閱交換器廠商文件。

檢查儲存系統上的**ONTAP MTU** 網路設置

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

關於這項工作

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

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

步驟

1. 檢查儲存系統上的MTU連接埠設定：

   ```
   network port show -instance
   ```

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

2. 變更連接埠所使用之廣播網域上的MTU：

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

範例

下列範例將MTU連接埠設定變更為9000：

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

檢查**ONTAP**磁碟吞吐量和延遲

您可以檢查叢集節點的磁碟處理量和延遲度量、以協助您進行疑難排解。

關於這項工作

此工作需要進階權限層級命令。

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 檢查磁碟處理量與延遲度量：

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

範例

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

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

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

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

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

相關資訊

- "統計磁碟顯示"

檢查節點之間的**ONTAP**吞吐量和延遲

您可以使用 `network test-path` 用於識別網路瓶頸或預先限定節點之間的網路路徑的命令。您可以在叢集間節點或叢集內節點之間執行命令。

開始之前

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

關於這項工作

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

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

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

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

工作階段類型	說明
同步鏡射位置	SnapMirror在同一叢集中的節點之間使用的設定

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

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 測量節點之間的處理量和延遲：

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

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

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

   ```
   cluster1::> network test-path -source-node node1 -destination-cluster
   cluster2 -destination-node node3 -session-type AsyncMirrorRemote
   ```

   範例輸出（輸出詳細資料可能會因您的 ONTAP 版本而異）：

   ```
   Test Duration:      10.88 secs
   Send Throughput:    18.23 MB/sec
   Receive Throughput: 18.23 MB/sec
   MB sent:            198.31
   MB received:        198.31
   Avg latency in ms:  2301.47
   ```

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

3. 返回管理權限：

   ```
   set -privilege admin
   ```

完成後

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

管理工作負載

識別 ONTAP 中的剩餘效能容量

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

開始之前

此工作需要進階權限層級命令。

關於這項工作

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

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

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

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 開始即時保留空間統計資料收集：

   ```
   statistics start -object resource_headroom_cpu|aggr
   ```

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

3. 顯示即時保留空間統計資訊：

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

4. 返回管理權限：

   ```
   set -privilege admin
   ```

範例

下列範例顯示叢集節點的平均每小時保留空間統計資料。

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

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

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

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

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

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

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

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

識別 **ONTAP** 中的高流量用戶端或檔案

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

題。

開始之前

您必須是叢集管理員才能執行此工作。

步驟

1. 檢視存取叢集的主要用戶端：

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

   下列命令會顯示存取的主要用戶端 `cluster1`：

```
cluster1::> statistics top client show

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


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

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

2. 檢視叢集上存取的主要檔案：

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

   下列命令會顯示在上存取的最上層檔案 `cluster1`：

```
cluster1::> statistics top file show

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

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

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

保證QoS的處理量

透過 ONTAP 中的 QoS 總覽來保證傳輸量

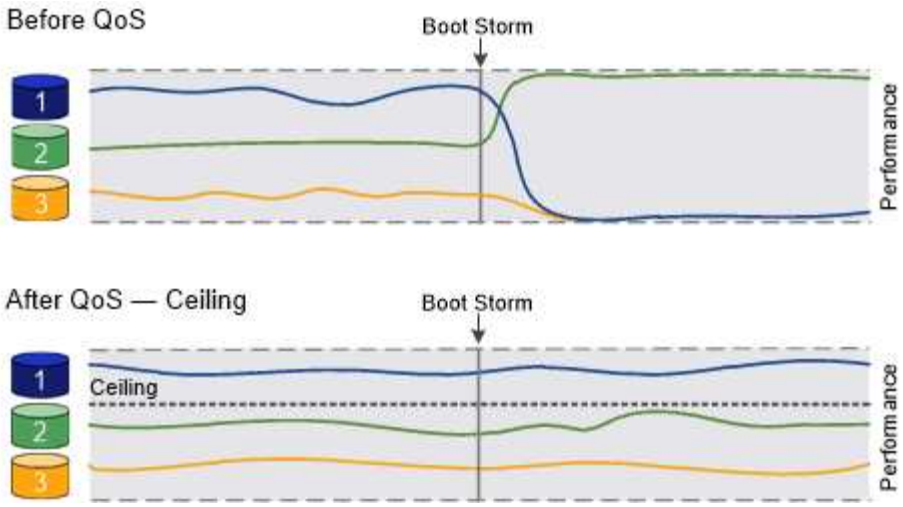
您可以使用儲存服務品質（QoS）來保證關鍵工作負載的效能不會因競爭工作負載而降級。您可以在競爭的工作負載上設定處理量上限、以限制其對系統資源的影響、或為關鍵工作負載設定處理量下限、以確保其符合最低處理量目標、無論競爭的工作負載有何需求。您甚至可以針對相同的工作負載設定上限和樓層。

處理量上限（ QoS 上限）

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

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

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



處理量層（ **QoS** 最低）

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

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

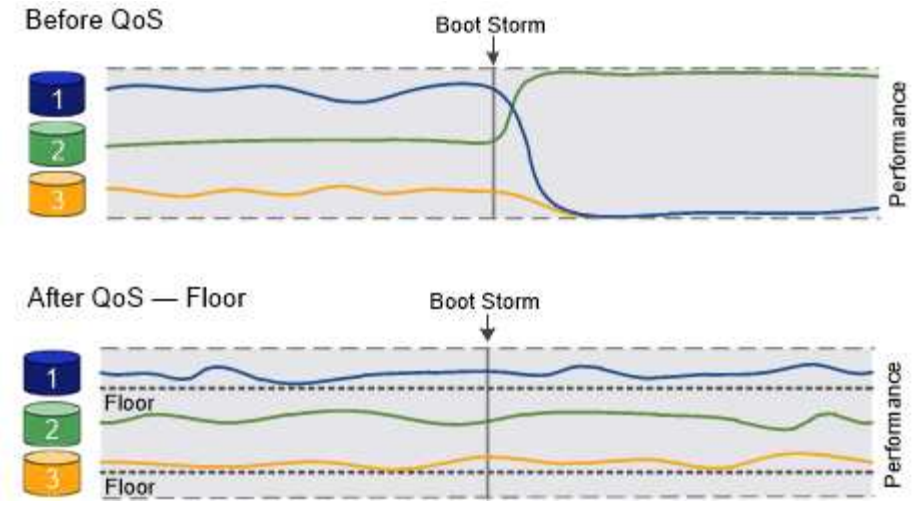
您可以在建立原則群組時指定樓層、也可以等到監控工作負載之後再指定樓層。

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

在更新於ONTAP VMware版本9.7之前的版本中、當有足夠的可用效能容量時、就能保證處理量的樓層數。

在VMware 9.7及更新版本中、即使可用的效能容量不足、也能保證處理量的樓層數。ONTAP這種新的樓層行為稱為Floor v2。為了達成保證、第v2層級可能會導致工作負載延遲更高、而不會出現處理量層或工作環境超過場地設定的情況。第v2層同時適用於QoS和調適性QoS。

ONTAP 9.7P6 及更新版本提供啟用 / 停用第 2 層樓的新行為選項。工作負載在執行關鍵作業時、可能會低於指定的樓層、例如 `volume move trigger-cutover`。即使有足夠的可用容量且未執行關鍵作業、工作負載的處理量仍可能低於指定樓層達5%。如果場地配置過度、而且沒有效能容量、則部分工作負載可能會落在指定樓層以下。



共享和非共享的 **QoS** 原則群組

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

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

調適性**QoS**

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

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

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

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

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

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

處理量上限和樓層的行為如下：

- 當工作負載指派給調適性QoS原則群組時、上限或樓層會立即更新。

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

在進行更新之前、處理量必須增加至少10 IOPS。

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

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

調適性原則群組範本

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

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

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

如需詳細資訊、請參閱 設定調適性原則群組範本。

一般支援

下表顯示支援處理量上限、處理量層和調適性QoS的差異。

資源或功能	處理量上限	處理量最低	處理量層**v2**	調適性**QoS**
版本9 ONTAP	全部	9.2 及更新版本	9.7 及更新版本	9.3 及更新版本
平台	全部	• AFF • C190 [1] • ONTAP Select Premium 搭配 SSD [1]	• AFF • C190 • 搭載SSD的高階版ONTAP Select	全部
通訊協定	全部	全部	全部	全部
FabricPool	是的	是的、如果分層原則設定為「無」、而且雲端中沒有區塊。	是的、如果分層原則設定為「無」、而且雲端中沒有區塊。	否
SnapMirror同步	是的	否	否	是的

[1] C190 與 ONTAP Select 支援從 ONTAP 9.6 版本開始。

處理量上限支援的工作負載

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

工作負載支援	更新版本**ONTAP**	**ONTAP 9.7** 至 **9.4**	**ONTAP 9.3** 及更早版本
Volume	是的	是的	是的
檔案	是的	是的	是的
LUN	是的	是的	是的
SVM	是的	是的	是的
流通量FlexGroup	是的	是的	是（僅限 ONTAP 9.3 ）
qtree [1]	是的	否	否
每個原則群組有多個工作負載	是的	是的	是的
非共用原則群組	是的	是的	否

[1] 從ONTAP 9.9.1 開始，啟用 SMB 的FlexVol和FlexGroup磁碟區中的 qtree 也支援 SMB 存取。從ONTAP 9.8 開始，啟用 NFS 的FlexVol和FlexGroup磁碟區中的 qtree 支援 NFS 存取。

處理量層的支援工作負載

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

工作負載支援	**ONTAP 9.13.1** 及更新版本	零點**9.8**至**9.13.0** **ONTAP**	**ONTAP 9.4** 至 **9.7**	**ONTAP 9.3**
Volume	是的	是的	是的	是的
檔案	是的	是的	是的	是的
LUN	是的	是的	是的	是的
SVM	是的	否	否	否
流通量FlexGroup	是的	是的	是的	否
qtree [1]	是的	是的	否	否
每個原則群組有多個工作負載	是的	是的	是的	否
非共用原則群組	是的	是的	是的	否

[1] 從 ONTAP 9.8 開始， FlexVol 的 qtree 和啟用 NFS 的 FlexGroup 磁碟區都支援 NFS 存取。從ONTAP 推出支

援SMB的支援範圍起、FlexVol 從推出支援SMB的功能、即可從功能支援功能支援使用功能的功能性功能、從功能性功能表中的qtree和FlexGroup 功能表中、存取SMB。

支援調適性**QoS**的工作負載

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

工作負載支援	**ONTAP 9.13.1** 及更新版本	零點**9.4**至**9.13.0 ONTAP**	**ONTAP 9.3**
Volume	是的	是的	是的
檔案	是的	是的	否
LUN	是的	是的	否
SVM	是的	否	否
流通量FlexGroup	是的	是的	否
每個原則群組有多個工作負載	是的	是的	是的
非共用原則群組	是的	是的	是的

工作負載和原則群組的最大數量

下表顯示ONTAP 各個版本的工作負載和原則群組數量上限。

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

啟用或停用**ONTAP**吞吐量底線 **v2**

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

步驟

1. 變更為進階權限層級：

   ```
   set -privilege advanced
   ```

2. 輸入下列其中一個命令：

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

若要在MetroCluster 一個不穩定叢集中停用處理量層v2、您必須執行

`qos settings throughput-floors-v2 -enable false`

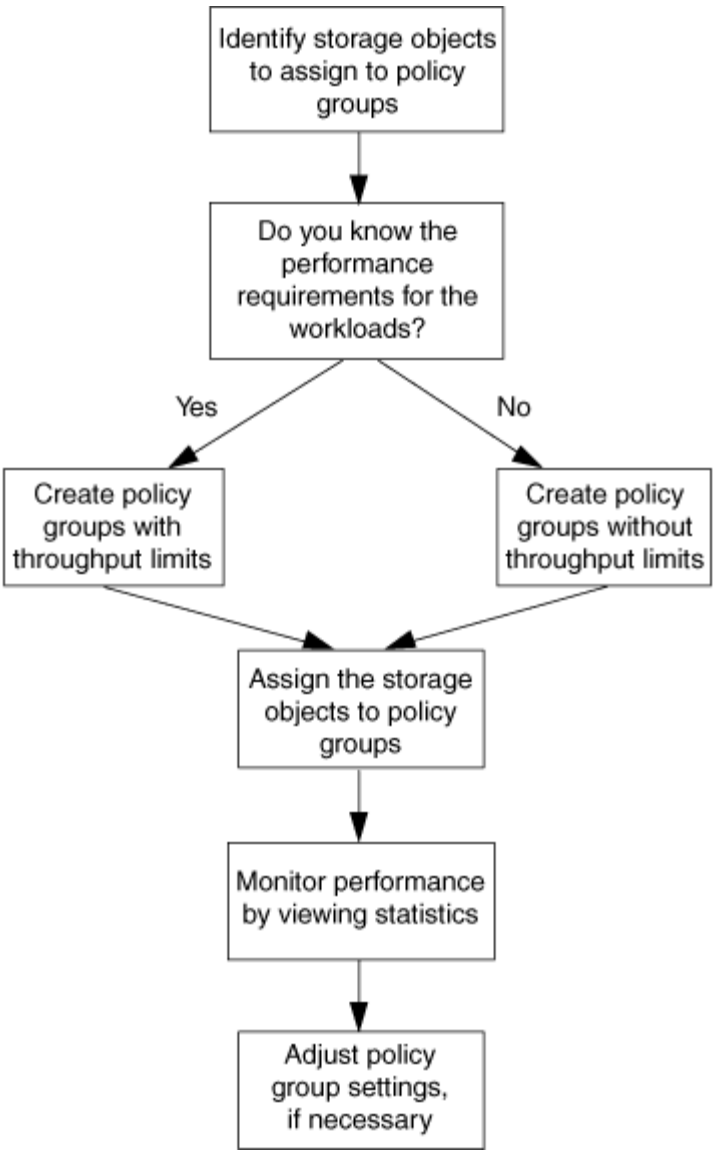
在來源叢集和目的地叢集上執行命令。

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

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

ONTAP儲存 **QoS** 工作流程

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



在 **ONTAP** 中設定 **QoS** 的處理量上限

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

開始之前

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

關於這項工作

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

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

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

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

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

步驟

1. 建立原則群組：

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

   如"指令參考資料ONTAP"需詳細 `qos policy-group create`資訊，請參閱。

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

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

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

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

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

   下列命令會建立非共用原則群組 `pg-vs4` 無處理量限制：

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

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

2. 將原則群組套用至SVM、檔案、磁碟區或LUN：

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

   如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。您可以使用 `*storage_object* modify`命令將不同的原則群組套用至儲存物件。

   下列命令會套用原則群組 `pg-vs1` 至 SVM `vs1`：

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

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

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

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

3. 監控原則群組效能：

   `qos statistics performance show`

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

   監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示原則群組效能：

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

4. 監控工作負載效能：

   `qos statistics workload performance show`

   監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示工作負載效能：

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

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

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

在 **ONTAP** 中設定具有 **QoS** 的處理量層

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

開始之前

- 您必須是叢集管理員、才能建立原則群組。
- 從 ONTAP 9.13.1 開始，您可以使用在 SVM 層級強制執行處理量層級調適性原則群組範本。您無法在具有 QoS 原則群組的 SVM 上設定調適性原則群組範本。

關於這項工作

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

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

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

步驟

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

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

   如"指令參考資料ONTAP"需詳細 `qos policy-group create`資訊，請參閱。

3. 您可以使用 `qos policy-group modify`命令來調整處理量層。

   下列命令會建立最小處理量為 1 ， 000 IOPS 的共用原則群組 `pg-vs2`：

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

   下列命令會建立非共用原則群組 `pg-vs4` 無處理量限制：

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

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

4. 將原則群組套用至磁碟區或LUN：

   `*storage_object* create -vserver *SVM* -qos-policy-group *policy_group*`您可以使用 `_storage_object_modify`命令將不同的策略群組套用到儲存物件。

   下列命令會套用原則群組 `pg-app2` 磁碟區 `app2`：

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

   如需有關本程序中所述命令"指令參考資料ONTAP"的詳細資訊，請參閱。

5. 監控原則群組效能：

   `qos statistics performance show`

   監控叢集的效能。請勿使用主機上的工具來監控效能。

   下列命令顯示原則群組效能：

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

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

6. 監控工作負載效能：

```
qos statistics workload performance show
```

監控叢集的效能。請勿使用主機上的工具來監控效能。

下列命令顯示工作負載效能：

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

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

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

在 **ONTAP** 中使用調適性 **QoS** 原則群組

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

開始之前

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

關於這項工作

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

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

處理量限制與儲存物件大小的比率、取決於下列欄位的互動：

- `expected-iops`是每分配 TB/GB 的最低預期 IOPS。

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

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

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

- peak-iops-allocation 指定是使用分配的空間還是使用的空間（預設） peak-iops。
- absolute-min-iops 為 IOPS 的絕對最小值。您可以將此欄位用於非常小的儲存物件。它會同時取代兩者 peak-iops 和/或 expected-iops 何時 absolute-min-iops 大於計算值 expected-iops。

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

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

預設自適應 **QoS** 策略群組

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

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

儲存物件策略群組分配限制

在某些情況下，如果儲存物件包含的物件或其子物件屬於某個策略群組，則無法將儲存物件指派給該策略群組。

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

以下物件對支援嵌套 QoS 策略：

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

對於嵌套的 QoS 策略，採用最嚴格的適用策略。

下表列出了各項限制。

如果您指派...	那麼你就無法將其指派到策略群組...
SVM到原則群組	SVM 中包含的任何儲存物件。 如果您執行的是ONTAP 9.18.1，則SVM 中所包含的FlexVol和FlexGroup磁碟區_可以_指派給策略群組。
磁碟區至原則群組	包含該磁碟區或任何子 LUN 的 SVM。 如果您執行的是ONTAP 9.18.1 及更高版本，則包含磁碟區的 SVM _可以_指派給策略群組。此外，也可以分配FlexVol或FlexGroup磁碟區中的qtree。
LUN至原則群組	包含 LUN 的磁碟區或 SVM
檔案至原則群組	包含文件的磁碟區或 SVM

步驟

1. 建立可調適的QoS原則群組：

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

   如"指令參考資料ONTAP"需詳細 `qos adaptive-policy-group create`資訊，請參閱。

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

   下列命令會建立調適性 QoS 原則群組 `adpg-app1` 與 `-expected-iops` 設為 300 IOPS / TB 、 `-peak-iops` 設為 1 、 000 IOPS / TB 、 `-peak-iops-allocation` 設定為 `used-space`和 `-absolute-min-iops` 設為 50 IOPS ：

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

2. 將調適性QoS原則群組套用至磁碟區：

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

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

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

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

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

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

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

在 **ONTAP** 中設定調適性原則群組範本

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

關於這項工作

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

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

- 您無法在具有 QoS 原則群組的 SVM 上設定調適性原則群組範本。
- 調適性原則群組範本是專為 AFF 平台所設計。可在其他平台上設定調適性原則群組範本、但原則可能無法強制執行最低處理量。同樣地、您也可以將調適性原則群組範本新增至 FabricPool Aggregate 中的 SVM 、或是新增至不支援最低處理量的 Aggregate 、但不會強制執行處理量層。
- 如果 SVM 是在 MetroCluster 組態或 SnapMirror 關係中、則會在鏡射 SVM 上強制執行調適性原則群組範本。

步驟

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

```
vserver show -fields qos-adaptive-policy-group
```

使用統一管理器監控和管理叢集效能

使用 **ONTAP Unified Manager** 監控叢集效能

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

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

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

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

相關連結：

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

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

您可以設定基本的效能監控與管理工作、並找出並解決常見的效能問題。

如果您的情況符合下列假設、您可以使用這些程序來監控及管理叢集效能：

- 您想要使用最佳實務做法、而非探索每個可用選項。
- 您想要顯示系統狀態和警示、監控叢集效能、以及使用Active IQ Unified Manager 除了OnCommand 使用VMware命令列介面以外的其他功能、使用VMware（前身為VMware Unified Manager）執行根本原因分析ONTAP 。
- 您正在使用 ONTAP 命令列介面來設定儲存服務品質 (QoS) 。QoS 也可透過下列方式取得：
  - 系統管理員
  - 靜態API ONTAP
  - VMware vSphere適用的工具ONTAP
  - NetApp 服務層級經理（ NSLM ）
  - OnCommand Workflow Automation （ WFA ）
- 您想要使用虛擬裝置安裝Active IQ Unified Manager ，而不是基於 Linux 或 Windows 的安裝。
- 您願意使用靜態組態、而非DHCP來安裝軟體。

- 您可以在ONTAP 進階權限層級存取指令檔。
- 您是具有「admin」角色的叢集管理員。

相關資訊

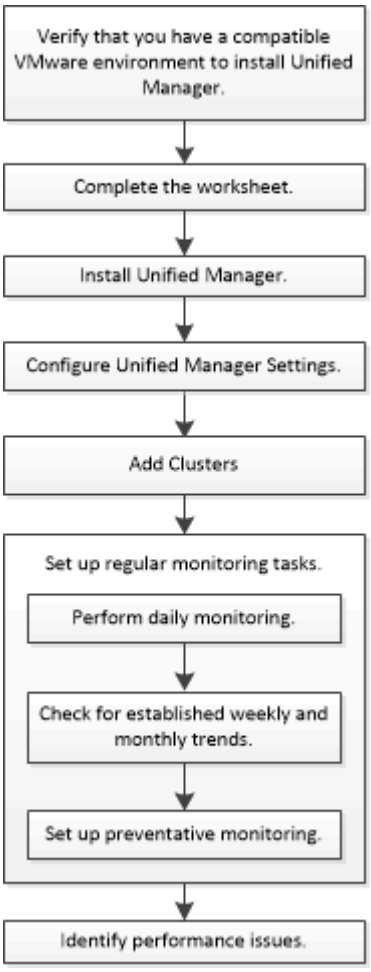
如果這些假設不符合您的情況、您應該看到下列資源：

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

監控效能

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

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



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

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

步驟

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

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

   該組態的詳細資料會顯示在「組態詳細資料」視窗中。
4. 檢閱下列索引標籤中的資訊：
   - 附註

     列出組態專屬的重要警示和資訊。
   - 原則與準則

     提供所有組態的一般準則。

ONTAP Active IQ Unified Manager工作表

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

Unified Manager安裝資訊

部署軟體的虛擬機器	您的價值
ESXi伺服器IP位址	
主機完整網域名稱	
主機IP位址	
網路遮罩	
閘道 IP 位址	
主要DNS位址	

次要DNS位址	
搜尋網域	
維護使用者名稱	
維護使用者密碼	

Unified Manager組態資訊

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

叢集資訊

針對Unified Manager上的每個叢集擷取下列資訊。

第1叢集、共N個	您的價值

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

相關資訊

"系統管理員驗證與RBAC"

安裝Active IQ Unified Manager

下載並部署ONTAP Active IQ Unified Manager

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

步驟

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

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

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

   您可以使用精靈中的*內容*索引標籤來輸入靜態組態資訊。

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

配置初始ONTAP Active IQ Unified Manager設置

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

步驟

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

完成後

初始設定完成後、會顯示「叢集資料來源」頁面、您可以在其中新增叢集詳細資料。

指定要在**Active IQ Unified Manager**中監控的**ONTAP**叢集

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

開始之前

- 您必須具備下列資訊：
  - 主機名稱或叢集管理IP位址

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

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

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

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

關於這項工作

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

步驟

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

   預設會選取HTTPS傳輸協定。

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

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

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

   如果憑證已過期、您就無法新增叢集。您必須更新SSL憑證、然後新增叢集。
6. 選用：檢視叢集探索狀態：
   a. 從「叢集設定」頁面檢閱叢集探索狀態。

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

設定基本監控工作

執行每日**ONTAP Active IQ Unified Manager**監控

您可以執行每日監控、確保不會發生任何需要注意的立即效能問題。

步驟

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

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

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

步驟

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

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

您可以設定效能臨界值來監控關鍵效能問題。使用者定義的臨界值會在系統接近或超過定

義的臨界值時觸發警告或重大事件通知。

步驟

1. 建立「警告」和「重大」事件臨界值：
   a. 選擇*組態*>*效能臨界值*。
   b. 按一下「 * 建立 * 」。
   c. 選取物件類型、然後指定原則的名稱和說明。
   d. 選取物件計數器條件、並指定定義「警告」和「重大」事件的限制值。
   e. 選取要傳送事件時必須違反限制值的持續時間、然後按一下「儲存」。
2. 將臨界值原則指派給儲存物件。
   a. 移至「Inventory」頁面以取得先前選取的相同叢集物件類型、然後從「View」（檢視）選項中選擇「* Performance 」（效能）。
   b. 選取您要指派臨界值原則的物件、然後按一下*指派臨界值原則*。
   c. 選取您先前建立的原則、然後按一下*指派原則*。

範例

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

新增**ONTAP Active IQ Unified Manager**警報

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

您可以設定警報，以便在產生特定事件時通知您。您可以為單一資源、一組資源或特定嚴重性類型的事件設定警報。您可以指定通知頻率，并将脚本与警报相关联。

開始之前

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

關於這項工作

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

步驟

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

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

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

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

   若要選取多個事件、請在選取時按Ctrl鍵。

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

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

   您也可以選擇透過SNMP設陷通知使用者。

7. 按一下「 * 儲存 * 」。

新增警示的範例

本範例說明如何建立符合下列需求的警示：

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

在「新增警示」對話方塊中執行下列步驟：

1. 按一下*名稱*、然後輸入 `HealthTest` 在*警示名稱*欄位中。
2. 按一下「資源」、然後在「包含」索引標籤中、從下拉式清單中選取「磁碟區」。
   a. 輸入 `abc` 在 * 名稱 Contains* 欄位中、顯示名稱包含「 abc 」的磁碟區。
   b. 選取*<<All Volumes whose name contains 'abc'>>「可用資源」區域中的「*」、然後將其移至「選取的資源」區域。
   c. 按一下*排除*、然後輸入 `xyz` 在「名稱包含」欄位中、然後按一下「新增」。
3. 按一下「事件」、然後從「事件嚴重性」欄位中選取「嚴重」。
4. 從「Matching Event（符合事件）」區域中選取* All Critical事件*、然後將其移至「Selected Event（選取的

事件）」區域。

5. 按一下「動作」、然後輸入 `sample@domain.com` 在警示這些使用者欄位中。
6. 選擇*每15分鐘提醒一次*、每15分鐘通知使用者一次。

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

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

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

您可以指定Active IQ Unified Manager 哪些事件來自於「觸發警示」、哪些電子郵件收件者用於這些警示、以及警示的頻率。

開始之前

您必須具有應用程式管理員角色。

關於這項工作

您可以針對下列類型的效能事件、設定獨特的警示設定：

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

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

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

步驟

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

   隨即顯示警示設定頁面。

2. 按一下「新增」、為每種事件類型設定適當的設定。

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

3. 按一下「 * 儲存 * 」。

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

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

步驟

1. 按一下電子郵件通知中的連結、即可直接前往發生效能事件的儲存物件。

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

2. 如果事件已超過系統定義的臨界值、請遵循UI中的建議動作來疑難排解問題。
3. 如果事件已超過使用者定義的臨界值、請分析事件以判斷您是否需要採取行動。
4. 如果問題仍然存在、請檢查下列設定：
   - 儲存系統上的傳輸協定設定
   - 任何乙太網路或光纖交換器上的網路設定
   - 儲存系統上的網路設定
   - 儲存系統上的磁碟配置和Aggregate度量
5. 如果問題持續發生、請聯絡技術支援部門以尋求協助。

使用ONTAP Active IQ Digital Advisor檢視系統效能

對於ONTAP 任何傳送AutoSupport 遙測資料給NetApp的支援系統、您都可以檢視廣泛的效能和容量資料。Digital Advisor 顯示系統效能的時間比 System Manager 長。

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

除了這項效能資料外、 Digital Advisor 還能根據工作負載顯示儲存效率、並將效率與該類型工作負載的預期效率進行比較。您可以檢視容量趨勢、並預估在特定時間範圍內可能需要增加多少儲存容量。

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

相關資訊

- "數位顧問文件"
- "數位顧問影片播放清單"
- "數位顧問Web入口網站"

使用 ONTAP 資料基礎架構洞察監控叢集效能

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

監控、疑難排解及最佳化所有資源

數據基礎設施洞察可協助您大幅減少解決問題的時間並防止問題影響最終用戶。它也能協助您降低雲端基礎架構

成本。透過可據以行動的情報來保護資料、可降低內部威脅的曝險。

資料基礎設施洞察讓您可以在一個地方查看整個混合基礎設施 - 從公有雲到資料中心。您可以立即建立相關的儀表板、以便根據您的特定需求進行自訂。您也可以建立特定且符合組織需求的目標式和條件式警示。

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

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

資料基礎設施洞察可視化您的系統拓撲，以了解您的 Kubernetes 架構。您可以監控Kubernetes叢集的健全狀況、包括發生問題的節點、並在發現問題時放大。

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

資料基礎設施洞察可協助您視覺化 Kubernetes 指標，以便您可以充分了解 pod、節點和叢集之間的關係。您可以評估叢集或正常運作的Pod的健全狀況、以及目前正在處理的負載、讓您能夠掌控K8S叢集、同時控制部署的健全狀況和成本。

相關連結

- "開始使用數據基礎設施洞察"

稽核記錄

瞭解 ONTAP 稽核記錄實作

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

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

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

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

ONTAP中記錄的管理活動

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

管理活動可以是以下類型之一：

- **SET** 請求：
  - 這些請求通常適用於非顯示命令或操作。
  - 這些要求會在您執行時發出 `create`、 `modify`或 `delete` 例如命令。
  - 預設會記錄 SET 請求。

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

審計日誌記錄和輪換

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

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

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

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

瞭解 **ONTAP** 稽核記錄的變更

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

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

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

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

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

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

顯示 **ONTAP** 稽核記錄內容

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

叢集的記錄檔項目包括：

時間

記錄項目時間戳記。

應用程式

用於連線至叢集的應用程式。可能值的範例包括 `internal`， `console`， `ssh` `http` `ontapi`，，， `snmp`，`rsh` `telnet`和 `service-processor`。

使用者

遠端使用者的使用者名稱。

州/省

稽核要求的目前狀態，可以是 `success`， `pending`或 `error`。

訊息

可選欄位、其中可能包含錯誤或命令狀態的其他資訊。

工作階段**ID**

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

儲存 **VM**

使用者連線的SVM。

範圍

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

命令**ID**

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

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

系統管理員

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

CLI

若要顯示從叢集中多個節點合併的稽核項目，請輸入：

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

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

網頁瀏覽器

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

管理 ONTAP 稽核 Get 要求設定

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

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

系統管理員

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

CLI

- 若要指定從 ONTAP CLI 或 API 取得要求應記錄在稽核記錄檔（ audit.log 檔案）中、除了預設的 Set 要求外、請輸入：

```
security audit modify [-cliget {on|off}][-httpget {on|off}][-ontapiget
{on|off}]
```

- 若要顯示目前的設定、請輸入：

```
security audit show
```

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

啟用ONTAP跨叢集審核

從ONTAP 9.17.1 以及ONTAP 9.16.1 P4 和更高版本的 9.16.1 修補程式版本開始，您可以

在ONTAP中啟用跨叢集稽核功能，以記錄從對等叢集發起的操作。這種遠端審計功能在多個ONTAP叢集互動的環境中尤其有用，可以提供遠端操作的可追溯性和責任追究。

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

開始之前

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

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

啟用或停用跨叢集審計

步驟

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

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

2. 透過檢查目前審核狀態來確認叢集對等設定是啟用還是停用：

```
security audit show
```

回覆:

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

啟用 **GET** 稽核的效果

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

管理 ONTAP 稽核記錄目的地

您最多可將稽核記錄轉送至10個目的地。例如、您可以將記錄轉送至Splunk或syslog伺服器、以供監控、分析或備份之用。

關於這項工作

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

您可以使用 `-protocol`參數選取下列其中一個傳輸值：

未加密的**udp**
: 無安全性的使用者資料包傳輸協定（預設）

TCP未加密
: 傳輸控制傳輸協定、無安全性

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

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

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

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

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

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

系統管理員

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

CLI

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

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

cluster1::> cluster log-forwarding create -destination
192.168.123.98
-port 6514 -protocol tcp-encrypted -facility user
```

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

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

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

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

相關資訊

- "叢集記錄轉送顯示"
- "建立叢集記錄轉送"

AutoSupport

瞭解 AutoSupport

瞭解 ONTAP AutoSupport

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

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

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

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

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

相關資訊

- "NetApp支援"
- "指令參考資料ONTAP"

瞭解數位顧問與 ONTAP AutoSupport

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

Digital Advisor可透過雲端型入口網站和行動應用程式、提供可據以行動的預測分析和主動式支援、讓您在全球混合雲中最佳化資料基礎架構。所有擁有有效 SupportEdge 合約的 NetApp 客戶、都能從數位顧問獲得資料導向的洞見和建議（功能因產品和支援層而異）。

以下是數位顧問的一些功能：

- 規劃升級。數位顧問可識別環境中可透過升級至較新版本的 ONTAP 來解決的問題、而升級顧問元件則可協助您規劃成功的升級。
- 檢視系統健全狀況。數位顧問儀表板會回報任何健康問題、並協助您修正這些問題。監控系統容量、確保儲存空間永遠不會耗盡。檢視系統的支援案例。
- 管理效能：Digital Advisor 顯示系統效能的時間比 System Manager 長。找出影響您效能的組態和系統問題。
- 最大化效率。檢視儲存效率指標、找出在更少空間中儲存更多資料的方法。
- 檢視庫存與組態。Digital Advisor 會顯示完整的庫存及軟體與硬體組態資訊。查看服務合約何時到期並續約、以確保您仍享有支援。

相關資訊

"NetApp 文件：數位顧問"

"啟動 Digital Advisor"

"部門服務SupportEdge"

瞭解 **ONTAP AutoSupport** 訊息的傳送時間和位置

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

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

事件觸發的訊息

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

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

排程的訊息

自動定期傳送數則訊息。AutoSupport

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

手動觸發的訊息

您可以手動初始化AutoSupport 或重新傳送一個消息。

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

由技術支援所觸發的訊息

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

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

瞭解 **ONTAP AutoSupport** 事件觸發訊息

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

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

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

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

2. 建立事件觸發的消息。AutoSupport AutoSupport

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

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

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

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

針對特定事件傳送的資料範例

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

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

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

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

ONTAP AutoSupport 訊息類型及其內容

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

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

訊息類型	訊息所包含的資料類型
由AutoSupport NetApp按需觸發	根據需求、可索取新訊息或過去訊息：AutoSupport • 視 AutoSupport 集合類型而定、可以是新訊息 `test`、`all`或 `performance`。 • 過去的訊息取決於重新傳送的訊息類型。 AutoSupport OnDemand 可要求將下列檔案上傳至 NetApp 支援網站的新訊息 "mysupport.netapp.com"、網址為： • 核心傾印 • 效能歸檔

檢視 **ONTAP AutoSupport** 子系統

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

此功能可收集內容相關的內容。AutoSupport

步驟

1. 檢視有關子系統和觸發事件的資訊：

```
system node autosupport trigger show
```

瞭解 **ONTAP AutoSupport** 的規模和時間預算

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

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

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

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

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

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

- 包含哪些子系統

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

- 每個隨附子系統的詳細資料層級

  每個隨附子系統的資料均以基本或疑難排解層級提供。

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

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

以**AutoSupport** 消息形式傳送的記錄檔

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

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

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

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

以每週**AutoSupport** 更新訊息傳送的檔案

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

以下資訊會以每週AutoSupport 的資訊傳送：

- 每個子系統的基本資訊
- 所選內容 `/mroot/etc` 目錄檔案

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

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

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

根據需求提供下列元件：AutoSupport

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

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

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

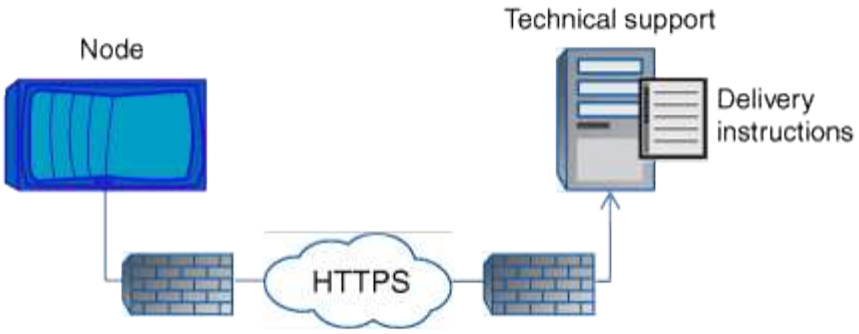
- 啟用了支援。AutoSupport
- 將支援功能設定為傳送訊息給技術支援。AutoSupport
- 將支援使用HTTPS傳輸傳輸傳輸協定。AutoSupport

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

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

如果您想要停用 AutoSupport OnDemand ，但保持 AutoSupport 啟用，請使用命令 `system node autosupport modify -ondemand-state disable`。如"指令參考資料ONTAP"需詳細 `system node autosupport modify -ondemand-state disable`資訊，請參閱。

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



交付指示可包括AutoSupport 要求執行下列事項的申請表：

- 產生新AutoSupport 的消息。

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

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

  技術支援人員可能會要求核心傾印或效能歸檔檔案、以協助分類問題。

- 重新傳輸先前產生AutoSupport 的消息。

  如果由於交付失敗而未收到訊息、則會自動執行此要求。

- 停用針對AutoSupport 特定觸發事件傳送的功能。

  技術支援可能會停用未使用的資料交付。

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

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

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

主旨

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

系統名稱（訊息）_嚴重性_的HA群組通知

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

本文

本文介紹下列資訊：AutoSupport

- 訊息的日期和時間戳記
- 產生訊息的節點上的版本ONTAP

- 產生訊息之節點的系統ID、序號和主機名稱
- 序列號AutoSupport
- SNMP聯絡人名稱與位置（若有指定）
- HA合作夥伴節點的系統ID和主機名稱

附加檔案

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

附件中包含的檔案是特定AutoSupport 於類型的消息。

瞭解 **ONTAP AutoSupport** 嚴重性類型

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

訊息具有下列嚴重性之一：

- 警示：警示訊息指出、如果您未採取任何行動、可能會發生更高層級的事件。

  您必須在24小時內針對警示訊息採取行動。

- 緊急：發生中斷時會顯示緊急訊息。

  您必須立即對緊急訊息採取行動。

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

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

取得 **ONTAP AutoSupport** 訊息說明

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

步驟

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

管理 **ONTAP AutoSupport** 的命令

您可以使用 `system node autosupport` 命令可變更或檢視 AutoSupport 組態、顯示先

前 AutoSupport 訊息的相關資訊、以及傳送、重新傳送或取消 AutoSupport 訊息。

設定**AutoSupport** 功能

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

顯示**AutoSupport** 有關此功能的資訊

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

顯示關於過去**AutoSupport** 的資訊

如果您想要...	使用此命令...
顯示50 AutoSupport 則最新版的一或多則新聞資訊	`system node autosupport history show`
顯示AutoSupport 最近產生的資訊、以將核心傾印或效能歸檔檔案上傳至技術支援網站或指定的URI	`system node autosupport history show-upload-details`

如果您想要...	使用此命令...
檢視AutoSupport 資訊資訊、包括針對訊息收集的每個檔案名稱和大小、以及任何錯誤	`system node autosupport manifest show`

傳送、重新傳送或取消**AutoSupport** 等字訊息

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

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

相關資訊

"指令參考資料ONTAP"

瞭解 **ONTAP AutoSupport** 資訊清單中包含的資訊

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

此資訊清單包含下列資訊：AutoSupport

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

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

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

規劃

準備使用 **ONTAP AutoSupport**

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

將 **AutoSupport** 訊息傳送至 **NetApp**

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

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

另請注意下列事項：

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

HTTPS

這提供最強大的功能。請注意下列事項：

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

SMTP

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

- 不支援 AutoSupport OnDemand 和大型檔案傳輸。

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

使用 **TLS** 改善 **SMTP** 安全性

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

下列連接埠通常用於 SMTPS ：連接埠 587

其他組態考量

在設定 AutoSupport 時、還有一些其他考量。

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

使用電子郵件傳送本機複本

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

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

HTTP Proxy

視您的網路組態而定， HTTPS 傳輸協定可能需要額外的 Proxy URL 組態。如果使用 HTTPS 將 AutoSupport 訊息傳送給技術支援人員、而且您有 Proxy 、則必須識別 Proxy 的 URL 。如果 Proxy 使用的連接埠不是預設的連接埠（連接埠 3128 ），您可以指定該 Proxy 的連接埠。您也可以選擇性地指定 Proxy 驗證的使用者名稱和密碼。

安裝伺服器憑證

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

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

如有需要，請使用下列程序來安裝憑證。您應該在叢集層級安裝所有必要的憑證。

範例 **37.** 步驟

系統管理員

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

CLI

1. 開始安裝：

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

   如"指令參考資料ONTAP"需詳細 `security certificate install`資訊，請參閱。

2. 查看下列主控台訊息：

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

3. 使用文字編輯器開啟憑證檔案。
4. 複製整個憑證、包括下列幾行：

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

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

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

   ```
   security certificate show
   ```

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

相關資訊

- "設定AutoSupport 功能"
- "指令參考資料ONTAP"

設定 ONTAP AutoSupport

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

關於這項工作

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

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

開始之前

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

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

步驟

1. 確保AutoSupport 啟用了功能：

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

2. 如果您想要 NetApp 技術支援人員接收 AutoSupport 訊息、請使用下列命令：

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

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

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

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

您可以從下列選項中選擇：

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

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

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

   b. 使用列出目的地、檢查位址是否正確設定 `system node autosupport destinations show` 命令。
5. 如果您在上一步中為內部支援組織設定收件者位址，或是選擇 SMTP 傳輸訊息給技術支援，請設定命令的下列參數來設定 SMTP `system node autosupport modify` ：
   - 設定 `-mail-hosts` 至一或多個郵件主機、以逗號分隔。

     您最多可以設定五個。

     您可以在郵件主機名稱之後指定一個冒號和連接埠編號、為每個郵件主機設定連接埠值：例如、`mymailhost.example.com:5678`，其中 5678 是郵件主機的連接埠。
   - 設定 `-from` 傳送 AutoSupport 訊息的電子郵件地址。
6. 設定DNS。
7. 或者、如果您想要變更特定設定、請新增命令選項：

如果您想要執行此動作...	然後設定的下列參數 `system node autosupport modify` 命令 ...
移除、遮罩或編碼訊息中的敏感資料、以隱藏私有資料	設定 `-remove-private-data` 至 `true`。如果您從變更 `false` 至 `true`，所有 AutoSupport 歷史記錄和所有相關文件都將被刪除。
停止以週期AutoSupport 性的資訊訊息傳送效能資料	設定 `-perf` 至 `false`。

8. 如果您使用 SMTP 將 AutoSupport 訊息傳送至 NetApp 、您可以選擇性地啟用 TLS 以改善安全性。
   a. 顯示新參數的可用值：

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

   b. 啟用 TLS 以傳輸 SMTP 訊息：

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

   c. 顯示目前的組態：

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

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

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

11. 測試AutoSupport 正在傳送和接收的不實訊息：
    a. 使用 `system node autosupport invoke` 命令 `-type` 參數設為 `test`：

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

    b. 確認NetApp正在接收AutoSupport 您的資訊：

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

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

    c. 您也可以選擇查看您為設定的任何地址的電子郵件、確認 AutoSupport 訊息已傳送至您的內部支援組織

或支援合作夥伴 `-to`、 `-noteto`或 `-partner-address` 的參數 `system node autosupport modify` 命令。

相關資訊

- "準備使用 AutoSupport"
- "指令參考資料ONTAP"

設定

管理 **ONTAP AutoSupport** 設定

您可以使用系統管理員來管理 AutoSupport 帳戶的設定。

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

檢視**AutoSupport** 畫面設定

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

步驟

1. 在System Manager中、按一下*叢集>設定*。

   在* AutoSupport 《》 （《*》）區段中、會顯示下列資訊：

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

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

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

產生並傳送**AutoSupport** 不一樣的資料

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

步驟

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

測試連線**AutoSupport** 至功能不正常的情況

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

步驟

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

啟用或停用**AutoSupport** 功能

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

關於這項工作

停用 AutoSupport 之前，請注意您正在關閉 NetApp 家用電話系統，您將會失去下列好處：

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

步驟

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

抑制支援案例的產生

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

關於這項工作

若要抑制支援案例的產生、請指定您要抑制的節點和小時數。

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

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮、然後選取 * 抑制支援個案產生 * 。
3. 輸入您要進行抑制的時數。

4. 選取您要進行抑制的節點。

恢復產生支援案例

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

步驟

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

編輯**AutoSupport** 功能設定

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

步驟

1. 選擇*叢集>設定*。
2. 在 * AutoSupport * 區段中、選取 ⋮、然後選取 * 更多選項 * 。
3. 在 * 連線 * 區段或 * 電子郵件 * 區段中、選取 Edit 以修改任一區段的設定。

相關資訊

- "準備使用 AutoSupport"
- "設定AutoSupport 功能"

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

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

步驟

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

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

相關資訊

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

使用 **AutoSupport** 上傳檔案

上傳 **ONTAP AutoSupport** 核心傾印檔案

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

開始之前

- 您已使用下列設定來設定 AutoSupport ：
  - 節點上啟用了支援。AutoSupport
  - 將支援功能設定為傳送訊息給技術支援。AutoSupport
  - AutoSupport 設定為使用 HTTPS 傳輸協定。

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

關於這項工作

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

"如何上傳 ONTAP 9 核心檔案進行分析"

步驟

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

   在下列範例中、會顯示本機節點的核心傾印檔案：

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

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

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

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

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

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

上傳 **ONTAP AutoSupport** 效能歸檔檔案

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

開始之前

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

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

關於這項工作

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

步驟

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

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

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

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

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

疑難排解

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

步驟

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

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

3. 執行下列其中一項動作：

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

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

如果系統未傳送預期的 AutoSupport 訊息，而且您使用的是 HTTPS 或自動更新功能無法運作，您可以檢查許多設定來解決問題。

開始之前

您應該已經確認基本的網路連線和DNS查詢：

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

關於這項工作

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

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

步驟

1. 顯示AutoSupport 資訊子系統的詳細狀態：

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

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

2. 驗證節點管理LIF的狀態：

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

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

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

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

5. 解決AutoSupport 由該消息傳回的任何錯誤：

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

如需協助疑難排解任何傳回的錯誤，請參閱"《》（Transport HTTPS和HTTP）解決方案指南ONTAP AutoSupport"。

6. 確認叢集可以成功存取所需的伺服器和網際網路：
   a. `network traceroute -lif node-management_LIF -destination DNS server`
   b. `network traceroute -lif node_management_LIF -destination support.netapp.com`

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

   c. `system node autosupport show -fields proxy-url`
   d. `network traceroute -node node_management_LIF -destination proxy_url`

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

7. 如果AutoSupport 您使用HTTPS作為您的傳輸傳輸協定、請確定HTTPS流量可以離開您的網路：
   a. 在與叢集管理LIF相同的子網路上設定Web用戶端。

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

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

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

8. 從 ONTAP 9.10.1 開始，如果您啟用自動更新，請確保您有 HTTPS 連線功能可連線至下列其他 URL ：
   - https://support-sg-naeast.netapp.com
   - https://support-sg-nawest.netapp.com

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

開始之前

您應該已經確認基本的網路連線和DNS查詢：

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

關於這項工作

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

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

除非ONTAP 另有說明、否則所有命令都會在指令行介面上輸入。

步驟

1. 驗證節點管理LIF的狀態：

   network interface show -home-node local -role node-mgmt -fields vserver,lif,status-oper,status-admin,address,role

   `status-oper`和 `status-admin`字段應返回 `up`
   。如link:https://docs.netapp.com/us-en/ontap-cli/up.html["指令參考資料ONTAP"^]需詳細 `up`資訊，請參閱。

2. 記下SVM名稱、LIF名稱及LIF IP位址以供日後使用。
3. 確認DNS已啟用且設定正確：

   vserver services name-service dns show

4. 顯示AutoSupport 所有設定供下列對象使用的伺服器：

   system node autosupport show -fields mail-hosts

   記錄顯示的所有伺服器名稱。

5. 針對上一步所顯示的每部伺服器、以及 `support.netapp.com`、請確定節點可以連線到伺服器或 URL ：

   network traceroute -node local -destination *server_name*

   如果其中任何一條路由無法運作、請使用大多數協力廠商網路用戶端上的「'traceroute」或「`TRACERT」公用程式、嘗試從與叢集位於同一子網路上的正常運作主機發出相同的路由。這有助於判斷問題是發生在您的網路組態或叢集組態中。

6. 登入指定為郵件主機的主機、並確保它可以處理下列的SMTP要求：

   netstat -aAn|grep 25

   25 是接聽程式 SMTP 連接埠號碼。

   此時會顯示類似下列文字的訊息：

   ```
   ff64878c tcp        0      0  *.25    *.*    LISTEN.
   ```

7. 從其他主機、開啟與郵件主機之SMTP連接埠的遠端登入工作階段：

   telnet *mailhost* 25

   此時會顯示類似下列文字的訊息：

   ```
   220 filer.yourco.com Sendmail 4.1/SMI-4.1 ready at Thu, 30 Nov 2014
   10:49:04 PST
   ```

8. 在登入提示字元時、請確定訊息可以從您的郵件主機轉送：

   HELO *domain_name*

   MAIL FROM: *your_email_address*

   RCPT TO: autosupport@netapp.com

   domain_name 是您網路的網域名稱。

   如果傳回錯誤、指出中繼遭拒、則不會在郵件主機上啟用中繼。請聯絡您的系統管理員。

9. 在登入提示字元下、傳送測試訊息：

   DATA

   SUBJECT: TESTING
   THIS IS A TEST

   .

   > ⓘ 請確定您自己在一行輸入最後一個期間（.）。期間會向郵件主機指出訊息已完成。

   如果傳回錯誤、表示您的郵件主機設定不正確。請聯絡您的系統管理員。

10. 從這個指令行介面、將一份不實的測試訊息傳送到您有權存取的信任電子郵件地址：ONTAP AutoSupport

    system node autosupport invoke -node local -type test

11. 尋找嘗試的順序編號：

    system node autosupport history show -node local -destination smtp

    根據時間戳記尋找嘗試的順序編號。這可能是最近的嘗試。

12. 顯示測試訊息嘗試的錯誤：

    system node autosupport history show -node local -seq-num seq_num -fields error

    如果顯示錯誤 `Login denied`，您的 SMTP 伺服器不接受叢集管理 LIF 的傳送要求。如果您不想變更為使用HTTPS作為傳輸傳輸協定、請聯絡您的站台網路管理員、設定以解決此問題的SMTP閘道。

    如果此測試成功、但傳送至mailto：autosupport@netapp.com的同一訊息卻沒有、請確定所有的SMTP郵件主機都已啟用了SMTP轉送、或使用HTTPS作為傳輸傳輸傳輸傳輸傳輸協定。

    如果連本機管理電子郵件帳戶的訊息都未成功、請確認您的SMTP伺服器已設定為轉送具有下列兩項特性的附件：

    - 「'7z'」字尾
    - 「application/x-7x-compressed」MIME類型。

ONTAP AutoSupport 子系統疑難排解

。 `system node check show` 命令可用於驗證和疑難排解任何與 AutoSupport 組態和交付相關的問題。

步驟

1. 使用下列命令來顯示AutoSupport 資訊子系統的狀態。

使用此命令...	若要這麼做...
`system node autosupport check show`	顯示 AutoSupport 子系統的整體狀態，例如 AutoSupport HTTPS 目的地， AutoSupport SMTP 目的地， AutoSupport 隨選伺服器和 AutoSupport 組態的狀態
`system node autosupport check show-details`	顯示AutoSupport 詳細的資訊、例如錯誤的詳細說明和修正行動

健全狀況監控

瞭解 **ONTAP** 系統健全狀況監控

健全狀況監視器會主動監控叢集中的特定關鍵情況、並在偵測到故障或風險時發出警示。如果有作用中警示、系統健全狀況狀態會報告叢集的降級狀態。這些警示包括回應降級系統健全狀況所需的資訊。

如果狀態為降級、您可以檢視問題的詳細資料、包括可能原因和建議的還原動作。解決問題之後、系統健全狀況狀態會自動返回「OK（確定）」。

系統健全狀況狀態反映多個獨立的健全狀況監視器。個別健全狀況監視器的降級狀態會導致整體系統健全狀況的降級狀態。

如需ONTAP 有關支援叢集交換器以監控叢集內系統健全狀況的詳細資訊、請參閱_E__ Hardware Universe 。

"支援的交換器Hardware Universe"

如需叢集交換器健全狀況監視器（CSHM）AutoSupport 功能介紹訊息的原因、以及解決這些警示所需採取的必要行動、請參閱知識庫文章。

"資訊：Health Monitor Process CSHM AutoSupport"

瞭解 ONTAP 健全狀況監控元件

個別健全狀況監視器有一組原則、可在特定情況發生時觸發警示。瞭解健全狀況監控的運作方式、可協助您回應問題並控制未來警示。

健全狀況監控包含下列元件：

- 特定子系統的個別健全狀況監視器、每個子系統都有自己的健全狀況狀態

  例如、儲存子系統具有節點連線健全狀況監視器。

- 整合個別健全狀況監視器健全狀況狀態的整體系統健全狀況監視器

  任何單一子系統的降級狀態、都會導致整個系統的降級狀態。如果沒有子系統發出警示、則整體系統狀態為「OK（正常）」。

每個健全狀況監視器均由下列關鍵元素組成：

- 警示：健全狀況監視器可能會發出警示

  每個警示都有定義、其中包含警示嚴重性及其可能原因等詳細資料。

- 可識別每個警示觸發時間的健全狀況原則

  每個健全狀況原則都有規則運算式、這是觸發警示的確切條件或變更。

健全狀況監視器會持續監控及驗證其子系統中的資源、以確保狀況或狀態變更。當條件或狀態變更符合健全狀況原則中的規則表示式時、健全狀況監視器會發出警示。警示會使子系統的健全狀況狀態和整體系統健全狀況狀態降級。

瞭解 ONTAP 系統健全狀況警示回應

當系統健全狀況警示發生時、您可以確認該警示、深入瞭解該警示、修復基礎狀況、並防止其再次發生。

當健全狀況監視器發出警示時、您可以使用下列任一方式回應：

- 取得警示的相關資訊、包括受影響的資源、警示嚴重性、可能原因、可能影響及修正行動。
- 取得警示的詳細資訊、例如警示發出時間、以及是否有其他人已確認警示。
- 取得受影響資源或子系統狀態的相關健全狀況資訊、例如特定機櫃或磁碟。
- 確認警示、指出有人正在處理此問題、並將自己識別為「Acknowledger」。
- 請採取警示中提供的修正行動來解決問題、例如修正纜線以解決連線問題。
- 如果系統未自動清除警示、請刪除警示。
- 隱藏警示、以防止其影響子系統的健全狀況狀態。

  當您瞭解問題時、隱藏功能非常實用。隱藏警示之後、仍可能發生、但當發生抑制警示時、子系統健全狀況會顯示為「ok、with -suppressed」（「ok、with -suppressed」）。

瞭解 ONTAP 系統健全狀況警示自訂功能

您可以啟用及停用定義警示觸發時間的系統健全狀況原則、來控制健全狀況監視器產生的警示。這可讓您針對特定環境自訂健全狀況監控系統。

您可以透過顯示所產生警示的詳細資訊、或顯示特定健全狀況監視器、節點或警示ID的原則定義、來學習原則名稱。

停用健全狀況原則與隱藏警示不同。當您隱藏警示時、它不會影響子系統的健全狀況狀態、但仍會發出警示。

如果停用原則、則在原則規則運算式中定義的條件或狀態將不再觸發警示。

您要停用的警示範例

例如、假設發生對您不實用的警示。您可以使用 `system health alert show -instance` 命令以取得警示的原則 ID 。您可以使用中的原則 ID `system health policy definition show` 命令以檢視原則的相關資訊。檢閱規則運算式和原則的其他相關資訊之後、您決定停用原則。您可以使用 `system health policy definition modify` 停用原則的命令。

相關資訊

- "系統健康警報顯示"

瞭解 ONTAP AutoSupport 健全狀況警示觸發程序

系統健全狀況警示會觸發AutoSupport 事件管理系統（EMS）中的訊息和事件、讓您AutoSupport 除了直接使用健全狀況監控系統之外、還能使用消息和EMS來監控系統的健全狀況。

系統AutoSupport 會在發出警示後五分鐘內傳送一則資訊不整訊息。除了複製上一週相同資源的警示和可能原因的警示之外、本資訊還會包含上一次顯示的所有警示。AutoSupport AutoSupport

部分警示不會觸發AutoSupport 資訊不均。如果AutoSupport 健全狀況原則停用AutoSupport 傳送功能、警示不會觸發資訊不全。例如、健全狀況原則AutoSupport 可能預設會停用不含資訊的訊息、因為AutoSupport 當問題發生時、資訊技術已經產生訊息。您可以使用設定原則、使其不會觸發 AutoSupport 訊息 `system health policy definition modify` 命令。

您可以使用檢視上週傳送的所有警示觸發 AutoSupport 訊息清單 `system health autosupport trigger history show` 命令。

警示也會觸發EMS產生事件。每次建立警示及清除警示時、都會產生一個事件。

瞭解可用的 ONTAP 叢集健全狀況監視器

有多個健全狀況監視器可監控叢集的不同部分。健全狀況監視器可ONTAP 偵測事件、傳送警示給您、並在清除事件時刪除事件、協助您從錯誤中恢復。

健全狀況監視器名稱（識別碼）	子系統名稱（識別碼）	目的
乙太網路交換器	交換器（交換器健全狀況）	ONTAP 乙太網路交換器健全狀況監視器（ CSHM ）可監控叢集和儲存網路交換器的狀態，同時收集記錄以供分析。根據預設， CSHM 會每 5 分鐘透過 SNMPv2c 輪詢每個交換器，以更新資源表，其中包含支援性，監控狀態，溫度感測器， CPU 使用率，介面組態和連線，叢集交換器備援，以及風扇和電源供應器作業等資訊。此外，如果已設定， CSHM 會每小時透過 SSH/SCP 收集記錄，並透過 AutoSupport 傳送以供進一步分析。CSHM 也可根據要求，使用 SSH/SCP 執行更詳細的技術支援記錄收集。 如需詳細資訊、請參閱 "交換器健全狀況監控" 。
支援的架構MetroCluster	交換器	監控MetroCluster 支援此功能的後端架構拓撲、並偵測錯誤的組態、例如不正確的佈線和分區、以及ISL故障。
系統健全狀況MetroCluster	互連、RAID和儲存設備	監控FC-VI介面卡、FC啟動器介面卡、左後集合體和磁碟、以及叢集間連接埠
節點連線（節點連線）	CIFS不中斷營運（CIF-NDO）	監控SMB連線、以確保不中斷營運至Hyper-V應用程式。
儲存設備（SAS連線）	在節點層級監控磁碟櫃、磁碟和介面卡、以取得適當的路徑和連線。	系統
不適用	彙總來自其他健全狀況監視器的資訊。	系統連線（系統連線）

自動接收 ONTAP 系統健全狀況警示

您可以使用命令手動檢視系統健全狀況警示 `system health alert show`。不過、您應該訂閱特定的事件管理系統（EMS）訊息、以便在健全狀況監視器產生警示時自動接收通知。

關於這項工作

下列程序說明如何設定所有hm.alert.malled訊息和所有hm.alert.Cleared訊息的通知。

所有hm.alert.malled訊息和所有hm.alert.Cleared訊息均包含SNMP設陷。SNMP 設陷的名稱為 `HealthMonitorAlertRaised`和 `HealthMonitorAlertCleared`。

如"指令參考資料ONTAP"需詳細 `system health alert show`資訊，請參閱。

步驟

1. 使用 `event destination create` 用於定義要將 EMS 訊息傳送至哪個目的地的命令。

```
cluster1::> event destination create -name health_alerts -mail
admin@example.com
```

如"指令參考資料ONTAP"需詳細 `event destination create`資訊，請參閱。

2. 使用 `event route add-destinations` 路由的命令 `hm.alert.raised` 訊息和 `hm.alert.cleared` 傳送至目的地的訊息。

```
cluster1::> event route add-destinations -messagename hm.alert*
-destinations health_alerts
```

如"指令參考資料ONTAP"需詳細 `event route add-destinations`資訊，請參閱。

相關資訊

- "使用系統管理員視覺化 ONTAP 網路"
- "如何在 DATA ONTAP上設定 SNMP 監控"

回應降級的 ONTAP 系統健全狀況

當系統的健全狀況狀態降級時、您可以顯示警示、讀取可能的原因和修正動作、顯示降級子系統的相關資訊、以及解決問題。也會顯示隱藏的警示、以便您修改這些警示、並查看是否已確認。

關於這項工作

您可以透過檢視 AutoSupport 訊息或 EMS 事件、或使用、來發現已產生警示 `system health` 命令。

步驟

1. 使用 `system health alert show` 命令以檢視影響系統健全狀況的警示。
2. 請閱讀警示的可能原因、可能影響及修正行動、以判斷您是否可以解決問題或需要更多資訊。
3. 如果您需要更多資訊、請使用 `system health alert show -instance` 命令以檢視警示可用的其他資訊。
4. 使用 `system health alert modify` 命令 `-acknowledge` 參數、表示您正在處理特定警示。
5. 請採取修正行動、以解決如所述的問題 `Corrective Actions` 警示中的欄位。

   修正行動可能包括重新啟動系統。

   解決問題時、警示會自動清除。如果子系統沒有其他警示、子系統的健全狀況會變更為 `OK`。如果所有子系統的健全狀況均正常、則整體系統健全狀況狀態會變更為 `OK`。

6. 使用 `system health status show` 確認系統健全狀況狀態的命令 `OK`。

   如果系統健全狀況狀態不是 `OK`，請重複此程序。

相關資訊

- "系統健康警報修改"

瞭解如何回應降級的 ONTAP 系統健全狀況

藉由檢閱缺少兩條節點路徑的機櫃所造成的降級系統健全狀況的特定範例、您可以查看當回應警示時CLI顯示的內容。

啟動ONTAP 功能後、您會檢查系統健全狀況、發現狀態已降級：

```
cluster1::>system health status show
  Status
  ---------------
  degraded
```

您會顯示警示、以瞭解問題所在位置、並看到機櫃2沒有兩個節點1路徑：

```
      cluster1::>system health alert show
                 Node: node1
             Resource: Shelf ID 2
             Severity: Major
       Indication Time: Mon Nov 10 16:48:12 2013
     Probable Cause: Disk shelf 2 does not have two paths to controller
                     node1.
    Possible Effect: Access to disk shelf 2 via controller node1 will be
                     lost with a single hardware component failure (e.g.
                     cable, HBA, or IOM failure).
 Corrective Actions: 1. Halt controller node1 and all controllers attached
to disk shelf 2.
                     2. Connect disk shelf 2 to controller node1 via two
paths following the rules in the Universal SAS and ACP Cabling Guide.
                     3. Reboot the halted controllers.
                     4. Contact support personnel if the alert persists.
```

您可以顯示警示的詳細資料、以取得更多資訊、包括警示ID：

```
      cluster1::>system health alert show -monitor node-connect -alert-id
DualPathToDiskShelf_Alert -instance
                  Node: node1
               Monitor: node-connect
              Alert ID: DualPathToDiskShelf_Alert
     Alerting Resource: 50:05:0c:c1:02:00:0f:02
             Subsystem: SAS-connect
       Indication Time: Mon Mar 21 10:26:38 2011
    Perceived Severity: Major
        Probable Cause: Connection_establishment_error
           Description: Disk shelf 2 does not have two paths to controller
node1.
    Corrective Actions: 1. Halt controller node1 and all controllers
attached to disk shelf 2.
                        2. Connect disk shelf 2 to controller node1 via
two paths following the rules in the Universal SAS and ACP Cabling Guide.
                        3. Reboot the halted controllers.
                        4. Contact support personnel if the alert
persists.
       Possible Effect: Access to disk shelf 2 via controller node1 will
be lost with a single
 hardware component failure (e.g. cable, HBA, or IOM failure).
          Acknowledge: false
             Suppress: false
               Policy: DualPathToDiskShelf_Policy
         Acknowledger: -
           Suppressor: -
Additional Information: Shelf uuid: 50:05:0c:c1:02:00:0f:02
                        Shelf id: 2
                        Shelf Name: 4d.shelf2
                        Number of Paths: 1
                        Number of Disks: 6
                        Adapter connected to IOMA:
                        Adapter connected to IOMB: 4d
Alerting Resource Name: Shelf ID 2
```

您認可警示、表示您正在處理警示。

```
      cluster1::>system health alert modify -node node1 -alert-id
DualPathToDiskShelf_Alert -acknowledge true
```

您可以修復機櫃2和節點1之間的纜線、然後重新啟動系統。然後再次檢查系統健全狀況、並查看狀態 OK：

```
cluster1::>system health status show
  Status
  ---------------
  OK
```

相關資訊

- "系統健康警報修改"

用於監控 ONTAP 系統健全狀況的命令

您可以使用 `system health`命令來顯示系統資源健全狀況的相關資訊，回應警示，以及設定未來的警示。使用CLI命令可讓您深入檢視設定健全狀況監控的方式資訊。如"指令參考資料ONTAP"需詳細 `system health`資訊，請參閱。

顯示系統健全狀況的狀態

如果您想要...	使用此命令...
顯示系統的健全狀況狀態、反映個別健全狀況監視器的整體狀態	`system health status show`
顯示子系統的健全狀況狀態、以便進行健全狀況監控	`system health subsystem show`

顯示節點連線狀態

如果您想要...	使用此命令...
顯示從節點連線至儲存櫃的詳細資料、包括連接埠資訊、HBA連接埠速度、I/O處理量、以及每秒I/O作業速率	`storage shelf show -connectivity` 使用 `-instance` 顯示每個機櫃詳細資訊的參數。
顯示磁碟機和陣列LUN的相關資訊、包括可用空間、機櫃和機櫃編號、以及擁有節點名稱	`storage disk show` 使用 `-instance` 參數顯示每個磁碟機的詳細資訊。
顯示儲存櫃連接埠的詳細資訊、包括連接埠類型、速度和狀態	`storage port show` 使用 `-instance` 參數以顯示每個介面卡的詳細資訊。

監控叢集與儲存網路交換器

如果您想要...	使用此命令...（更新版本：**ONTAP**	使用此命令...（更新版本：**9.7**）**ONTAP**
顯示叢集監控的交換器	`system switch ethernet show`	`system cluster-switch show`
顯示叢集目前監控的交換器，包括您刪除的交換器（顯示在命令輸出的「原因」欄中） 此命令可在進階權限層級使用	`system switch ethernet show-all`	`system cluster-switch show-all`
設定對未探索到的交換器的監控	`system switch ethernet create`	`system cluster-switch create`
修改叢集監控的交換器相關資訊（例如、裝置名稱、IP位址、SNMP版本和社群字串）	`system switch ethernet modify`	`system cluster-switch modify`
停用切換器的監控功能	`system switch ethernet modify -disable-monitoring`	`system cluster-switch modify -disable-monitoring`
從監控中刪除交換器	`system switch ethernet delete`	`system cluster-switch delete`
永久移除儲存在資料庫中的交換器組態資訊（如此會重新啟用交換器的自動探索）	`system switch ethernet delete -force`	`system cluster-switch delete -force`
使用交換器執行記錄收集	`system switch ethernet log`	`system cluster-switch log`

如需詳細資訊，請參閱"交換器健全狀況監控"和"設定記錄收集"。

回應產生的警示

如果您想要...	使用此命令...
顯示已產生警示的相關資訊、例如觸發警示的資源和節點、以及警示的嚴重性和可能原因	`system health alert show`
顯示每個產生警示的相關資訊	`system health alert show -instance`
表示有人正在處理警示	`system health alert modify`
確認警示	`system health alert modify -acknowledge`

如果您想要...	使用此命令...
隱藏後續警示、使其不影響子系統的健全狀況	`system health alert modify -suppress`
刪除未自動清除的警示	`system health alert delete`
顯示AutoSupport 上週觸發警示的有關資訊、例如、判斷警示是否觸發AutoSupport 了一個故障訊息	`system health autosupport trigger history show`

設定未來警示

如果您想要...	使用此命令...
啟用或停用控制特定資源狀態是否發出特定警示的原則	`system health policy definition modify`

顯示如何設定健全狀況監控的相關資訊

如果您想要...	使用此命令...
顯示健全狀況監視器的相關資訊、例如其節點、名稱、子系統和狀態	`system health config show` 使用 `-instance` 顯示每個健全狀況監視器的詳細資訊的參數。
顯示健全狀況監視器可能產生之警示的相關資訊	`system health alert definition show` 使用 `-instance` 顯示每個警示定義的詳細資訊的參數。
顯示有關健全狀況監視原則的資訊、以決定何時發出警示	`system health policy definition show` 使用 `-instance` 參數以顯示每個原則的詳細資訊。使用其他參數來篩選警示清單、例如依原則狀態（已啟用或未啟用）、健全狀況監視器、警示等。

相關資訊

- "儲存連接埠顯示"
- "倉儲貨架展示"
- "系統健康警報刪除"

檢視 **ONTAP** 環境資訊

感應器可協助您監控系統的環境元件。您可以檢視的環境感應器相關資訊包括其類型，名稱，狀態，值和臨界值警告。

步驟

1. 若要顯示環境感應器的相關資訊、請使用 `system node environment sensors show` 命令。

檔案系統分析

瞭解 **ONTAP** 檔案系統分析

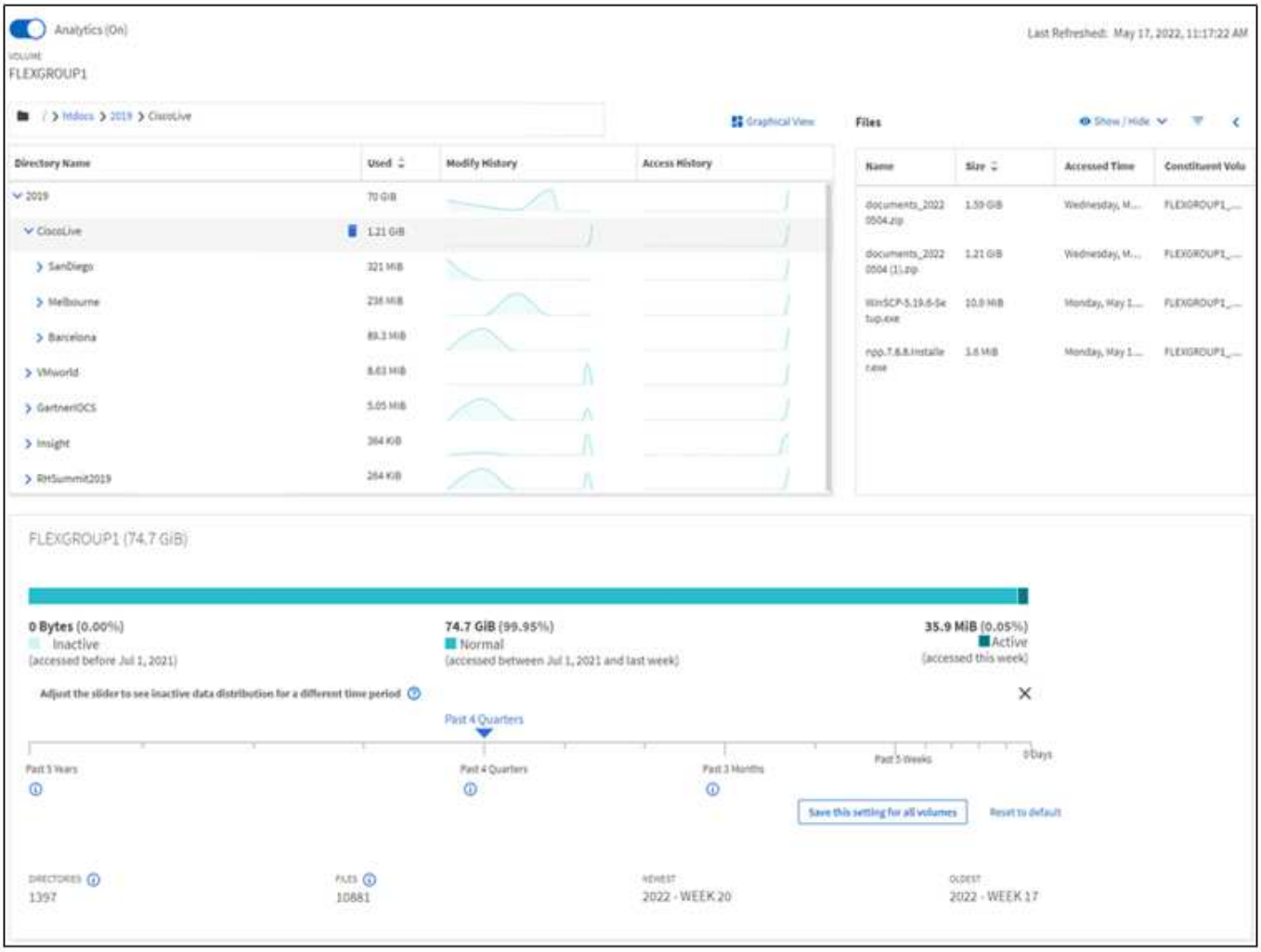
檔案系統分析（FSA）是ONTAP 在更新版本9.8中首次推出、可即時查看ONTAP FlexGroup 檔案使用率及內部的儲存容量趨勢、包括更新版本。FlexVol這項原生功能不需要使用外部工具，並針對儲存設備的使用方式，以及是否有機會針對您的業務需求最佳化儲存設備，提供重要見解。

有了 FSA 、您就能在 NAS 中查看 Volume 檔案系統階層的所有層級。例如、您可以在儲存VM（SVM）、Volume、目錄和檔案層級取得使用量和容量洞見。您可以使用FSA來回答下列問題：

- 我的儲存設備中有哪些空間、還有哪些大型檔案可以移至其他儲存位置？
- 哪些是我最活躍的磁碟區、目錄和檔案？我的儲存效能是否已針對使用者的需求最佳化？
- 上個月新增了多少資料？
- 誰是我最活躍或最不活躍的儲存使用者？
- 我的主要儲存設備上有多少閒置或靜止資料？我可以將資料移至成本較低的冷層嗎？
- 我的計畫性服務品質變更是否會對存取經常存取的重要檔案造成負面影響？

檔案系統分析已整合至ONTAP 《Sytricity System Manager》。System Manager中的檢視可提供：

- 即時可見度、有效管理及營運資料
- 即時資料收集與集合體
- 子目錄和檔案大小與數量、以及相關的效能設定檔
- 修改及存取歷程記錄的檔案保存時間分佈圖



支援的**Volume**類型

檔案系統分析的設計旨在提供使用中NAS資料的磁碟區可見度、FlexCache 但不包括SnapMirror快取和SnapMirror目的地磁碟區。

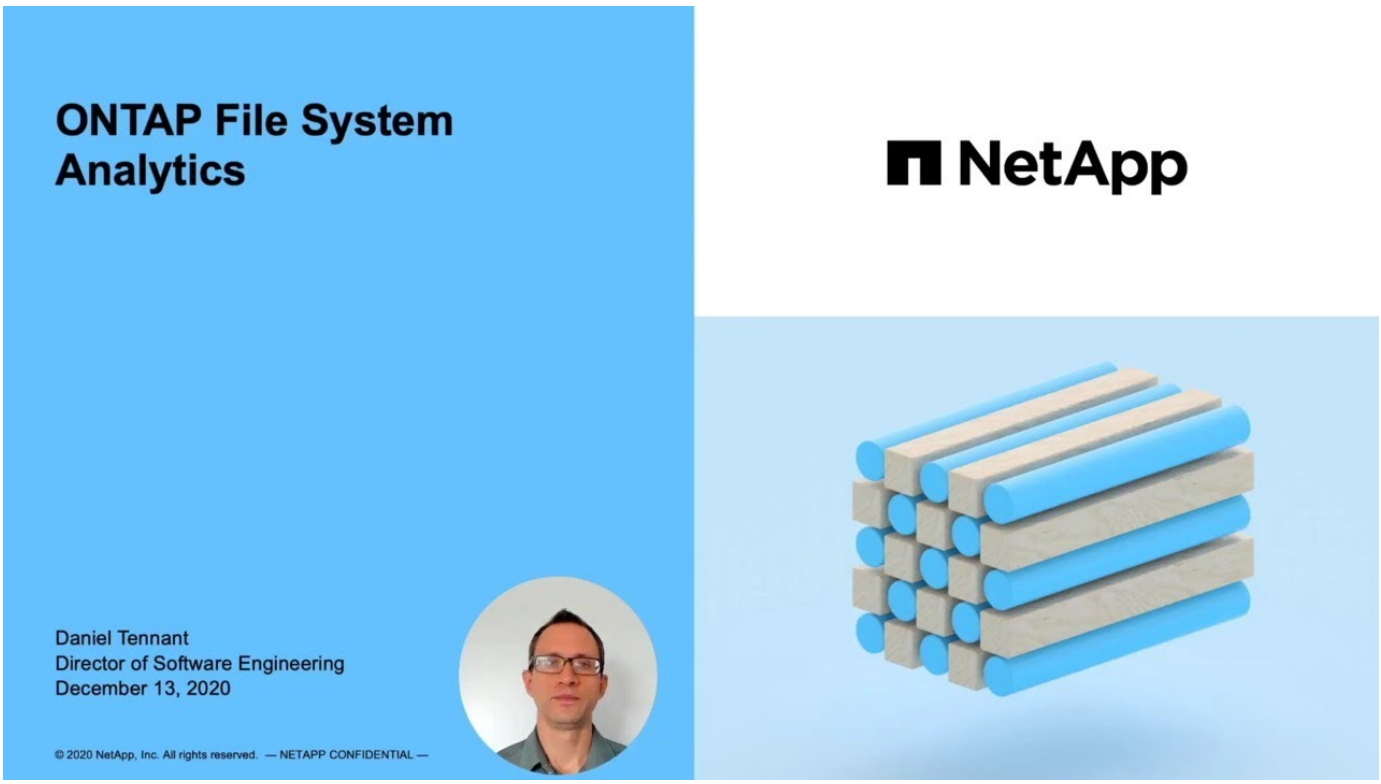
檔案系統分析功能可用度

每個 ONTAP 版本都擴大了檔案系統分析的範圍。

	ONTAP 9.14.1 及更新版本	**ONTAP 9.13.1.12 .9.11.9.1 1.**	**ONTAP 9.12.1**	零點**9.11. 1. ONTAP**	零點**9.10. 1 ONTAP**	部分**9.9.1 ONTAP**	部分**9.8 ONTAP**
系統管理程式中的視覺化功能	是的	是的	是的	是的	是的	是的	是的
容量分析	是的	是的	是的	是的	是的	是的	是的
非作用中資料資訊	是的	是的	是的	是的	是的	是的	是的
支援Data ONTAP 從VMware 7-Mode轉換的Volume	是的	是的	是的	是的	是的	是的	否

	ONTAP 9.14.1 及更新版本	ONTAP 9.13.1.12 .9.11.9.1 1.	ONTAP 9.12.1	零點9.11. 1. ONTAP	零點9.10. 1 ONTAP	部分9.9.1 ONTAP	部分9.8 ONTAP
能夠在System Manager中自訂非作用中期間	是的	是的	是的	是的	是的	是的	否
Volume層級活動追蹤	是的	是的	是的	是的	是的	否	否
將活動追蹤資料下載至CSV	是的	是的	是的	是的	是的	否	否
SVM層級的活動追蹤	是的	是的	是的	是的	否	否	否
時間表	是的	是的	是的	是的	否	否	否
使用分析	是的	是的	是的	否	否	否	否
預設啟用檔案系統分析的選項	是的	是的	否	否	否	否	否
初始化掃描進度監視器	是的	否	否	否	否	否	否

深入瞭解檔案系統分析



相關資訊

- "TR 4687：ONTAP 《關於分析檔案系統的最佳實務準則》"
- "知識庫：開啟NetApp ONTAP 功能的NetApp功能檔系統分析後、延遲時間會大幅或波動"

啟用 ONTAP 檔案系統分析

若要收集及顯示容量分析等使用資料、您必須在磁碟區上啟用檔案系統分析。

從ONTAP 9.17.1 開始，在ONTAP叢集上新建的 SVM 上建立的磁碟區（如果已指派 NAS 協定）現在預設啟用檔案系統分析 (FSA)。 FSA會在磁碟區建立後立即自動激活，無需額外配置即可提供即時分析功能。如果您不想在新磁碟區上啟用檔案系統分析，則必須 "在新磁碟區上停用 FSA" 來自 SVM。

關於這項工作

- 從功能支援的9.8開始ONTAP 、您可以在新的或現有的磁碟區上啟用檔案系統分析功能。如果您將系統升級ONTAP 至支援更新版本的支援版本9.8、請務必先完成所有的升級程序、再啟用檔案系統分析功能。
- 啟用分析所需的時間取決於磁碟區的大小和內容。系統管理程式會顯示進度、並在完成時顯示分析資料。如果您需要更精確的初始化掃描進度資訊、可以使用 ONTAP CLI 命令 `volume analytics show`。
  - 從 ONTAP 9.15.1 開始、您只能在節點上同時執行四次初始化掃描。您必須等待掃描完成、才能開始新的掃描。ONTAP 也會強制磁碟區上有足夠的可用空間、如果沒有、則會顯示錯誤訊息。請確定至少有 5% 至 8% 的磁碟區可用空間可用。如果磁碟區已啟用自動調整大小、請根據最大自動增加大小來計算可用大小。
  - 從 ONTAP 9.14.1 開始、 ONTAP 除了提供影響掃描進度的節流事件通知外、還提供初始化掃描的進度追蹤。
  - 如需初始化掃描的進一步考量、請參閱 掃描考量。
  - 如"指令參考資料ONTAP"需詳細 `volume analytics show`資訊，請參閱。

在現有磁碟區上啟用檔案系統分析

您可以使用ONTAP 支援功能支援檔案系統分析的功能、包括使用支援功能的系統管理程式或CLI。

範例 **38.** 步驟

系統管理員

更新版本**ONTAP**	**ONTAP 9.9.1** 和**ONTAP 9.8**
1. 選擇*儲存>磁碟區*。 2. 選取所需的Volume。從個別Volume功能表中、選取*檔案系統>檔案總管*。 3. 選取 * 啟用分析 * 或 * 停用分析 * 。	1. 選擇*儲存>磁碟區*。 2. 選取所需的磁碟區，然後選取 * 檔案總管 * 。 3. 選取 * 啟用分析 * 或 * 停用分析 * 。

CLI

使用 **CLI** 啟用檔案系統分析

1. 運行以下命令：

```
volume analytics on -vserver <svm_name> -volume <volume_name> [-
foreground {true|false}]
```

預設情況下，此命令在前台運行； ONTAP會在完成後顯示進度並提供分析資料。如果您需要更精確的訊息，可以使用 `-foreground false`選項，然後使用 `volume analytics show`指令在 CLI 中顯示初始化進度。

2. 成功啟用檔案系統分析之後、請使用系統管理員或 ONTAP REST API 來顯示分析資料。

如"指令參考資料ONTAP"需詳細 `volume analytics on`資訊，請參閱。

修改預設檔案系統分析設定

從 ONTAP 9.13.1 開始，您可以修改 SVM 或叢集設定，以在新磁碟區上預設啟用檔案系統分析。

範例 **39.** 步驟

系統管理員

如果您使用的是 System Manager 、您可以修改儲存 VM 或叢集設定、以在建立 Volume 時啟用容量分析和活動追蹤。預設啟用功能僅適用於修改設定後建立的磁碟區、而非現有的磁碟區。

修改叢集上的檔案系統分析設定

1. 在系統管理員中，導航至*集群設定*。
2. 在「叢集設定」中，查看「檔案系統設定」標籤。若要修改設置，請選擇 圖示.
3. 在「活動追蹤」欄位中，輸入預設啟用活動追蹤的 SVM 名稱。如果將此欄位留空，則所有 SVM 上的活動追蹤功能均處於停用狀態。

   取消勾選「在新儲存虛擬機器上啟用」方塊以預設在新儲存虛擬機器上停用活動追蹤。

4. 在「分析」欄位中，輸入您希望預設啟用容量分析的儲存虛擬機器的名稱。如果將此欄位留空，則所有 SVM 上的容量分析均處於停用狀態。

   取消勾選「在新儲存虛擬機器上啟用」方塊以預設在新儲存虛擬機器上停用容量分析。

5. 選擇*保存*。

修改 **SVM** 上的檔案系統分析設定

1. 選擇要修改的 SVM，然後選擇*儲存 VM 設定*。
2. 在*檔案系統分析*卡中，使用切換按鈕啟用或停用儲存虛擬機器上所有新磁碟區的活動追蹤和容量分析。

CLI

您可以使用 ONTAP CLI 將儲存 VM 設定為在新磁碟區上預設啟用檔案系統分析。

依預設、在 **SVM** 上啟用檔案系統分析

1. 修改 SVM 以在所有新建立的磁碟區上預設啟用容量分析和活動追蹤：

   ```
   vserver modify -vserver <svm_name> -auto-enable-activity-tracking
   true -auto-enable-analytics true
   ```

   如"指令參考資料ONTAP"需詳細 `vserver modify`資訊，請參閱。

相關資訊

- "指令參考資料ONTAP"

使用 **FSA** 查看 **ONTAP** 檔案系統活動

啟用檔案系統分析（FSA）之後、您可以檢視所選磁碟區的根目錄內容、並依據每個子樹狀結構中所使用的空間進行排序。

選取任何檔案系統物件以瀏覽檔案系統、並顯示目錄中每個物件的詳細資訊。目錄的相關資訊也可以圖形方式顯示。隨著時間推移、每個子樹狀結構都會顯示歷史資料。如果目錄超過3000個、則不會對已用空間進行排序。

檔案總管

檔案系統分析*檔案總管*畫面包含三個區域：

- 目錄與子目錄的樹狀檢視；可展開的清單、顯示名稱、大小、修改歷程記錄及存取歷程記錄。
- 檔案；顯示目錄清單中所選物件的名稱、大小和存取時間。
- 目錄清單中所選物件的作用中和非作用中資料比較。

  從0到9：9.1開始ONTAP 、您可以自訂要報告的範圍。預設值為一年。根據這些自訂、您可以採取修正行動、例如移動磁碟區和修改分層原則。

預設會顯示存取時間。不過、如果已從 CLI 變更磁碟區預設值（透過設定 `-atime-update` 選項 `false` 使用 `volume modify` 命令）、則只會顯示上次修改的時間。例如：

- 樹狀檢視不會顯示*存取歷程記錄*。
- 檔案檢視畫面將會變更。
- 作用中 / 非作用中的資料檢視將根據修改時間而定 (`mtime`）。

使用這些顯示器、您可以檢查下列項目：

- 檔案系統位置佔用的空間最大
- 目錄樹狀結構的詳細資訊、包括目錄和子目錄內的檔案和子目錄數
- 包含舊資料的檔案系統位置（例如、Scratch、Temp或記錄樹狀結構）

在解讀FSA輸出時、請謹記以下幾點：

- FSA會顯示資料使用的位置和時間、而非處理的資料量。例如、最近存取或修改的檔案佔用大量空間、並不一定表示系統處理負載過高。
- 「* Volume Explorer*」標籤計算FSA空間使用量的方式、可能與其他工具不同。尤其是、如果磁碟區已啟用儲存效率功能、相較於* Volume Overview 所報告的使用量、可能會有顯著差異。這是因為 Volume Explorer’s（磁碟區總管）索引標籤不包含效率節約效益。
- 由於目錄顯示區的空間限制、因此無法在_List View_中檢視大於8層的目錄深度。若要檢視深度超過8層的目錄、您必須切換至_Graphical View_、找到所需的目錄、然後切換回_List View_。如此可在顯示器中增加額外的螢幕空間。

步驟

1. 檢視所選磁碟區的根目錄內容：

從**ONTAP** 功能上開始。**9.10.1**	在**ONTAP 9.9.1** 和 **9.8** 中
選取*儲存>磁碟區*、然後選取所需的磁碟區。從個別Volume功能表中、選取*檔案系統>檔案總管*。	單擊* Storage（儲存設備）> Volumes（磁碟區）、選擇所需的磁碟區、然後單擊 Explorer’s *。

相關資訊

- "Volume修改"

使用 **FSA** 啟用 **ONTAP** 活動追蹤

從 ONTAP 9.10.1 開始、檔案系統分析包含「活動追蹤」功能、可讓您識別常用物件並將資料下載為 CSV 檔案。從《S209.11.1活動ONTAP 追蹤（Activ練習 追蹤）」開始、活動追蹤已擴大至SVM範圍。此外，從 ONTAP 9.11.1 開始， System Manager 也提供活動追蹤時間表，讓您可以查看最多五分鐘的活動追蹤資料。

「活動追蹤」可監控四種類別：

- 目錄
- 檔案
- 用戶端
- 使用者

對於每個受監控的類別、「活動追蹤」會顯示讀取IOPs、寫入IOPs、讀取流量和寫入流量。「活動追蹤」查詢每10到15秒會重新整理一次、以說明系統在前五秒間隔內出現的熱點。

活動追蹤資訊是大約的、資料的準確度取決於傳入I/O流量的分配。

在Volume層級的System Manager中檢視「活動追蹤」時、只有展開Volume的功能表會主動重新整理。如果任何磁碟區的檢視都已收合、則在展開磁碟區顯示之前、這些磁碟區不會重新整理。您可以使用*暫停重新整理*按鈕來停止重新整理。活動資料可以CSV格式下載、以顯示所選磁碟區擷取的所有時間點資料。

從 ONTAP 9.11.1 開始，時間軸功能可讓您在 Volume 或 SVM 上保留熱點活動記錄，並持續每五秒更新一次，並保留前五分鐘的資料。時間軸資料只會保留給頁面可見區域的欄位。如果您摺疊追蹤類別或捲動、使時間表不在檢視範圍內、時間表將停止收集資料。根據預設、當您離開「活動」索引標籤時、時間表會停用、並自動停用。

針對單一**Volume**啟用「活動追蹤」

您可以使用 ONTAP 系統管理員或 CLI 啟用活動追蹤。

關於這項工作

如果您搭配ONTAP 使用RBAC搭配使用REST API或System Manager、則必須建立自訂角色、才能管理「活動追蹤」的存取權限。請參閱 角色型存取控制 此程序。

系統管理員

步驟

1. 選擇*儲存>磁碟區*。選取所需的Volume。從個別Volume功能表中、選取File System（檔案系統）、然後選取「活動」索引標籤。
2. 確保*活動追蹤*已開啟、以檢視熱門目錄、檔案、用戶端和使用者的個別報告。
3. 若要在不重新整理的情況下更深入地分析資料、請選取*暫停重新整理*。您也可以下載資料以取得報告的CSV記錄。

CLI

步驟

1. 啟用活動追蹤：

   ```
   volume activity-tracking on -vserver svm_name -volume volume_name
   ```

2. 使用命令檢查磁碟區的「活動追蹤」狀態是否為開啟或關閉：

   ```
   volume activity-tracking show -vserver svm_name -volume volume_name -state
   ```

3. 啟用後、請使用ONTAP 「靜態系統管理程式」或ONTAP 「靜態API」來顯示「活動追蹤」資料。

啟用多個磁碟區的「活動追蹤」

您可以使用 System Manager 或 CLI 為多個磁碟區啟用「活動追蹤」。

關於這項工作

如果您搭配ONTAP 使用RBAC搭配使用REST API或System Manager、則必須建立自訂角色、才能管理「活動追蹤」的存取權限。請參閱 角色型存取控制 此程序。

系統管理員

針對特定磁碟區啟用

1. 選擇*儲存>磁碟區*。選取所需的Volume。從個別Volume功能表中、選取File System（檔案系統）、然後選取「活動」索引標籤。
2. 選取您要啟用「活動追蹤」的磁碟區。在Volume清單頂端、選取*更多選項*按鈕。選取*啟用活動追蹤*。
3. 若要在SVM層級檢視「活動追蹤」、請從*儲存設備> Volumes *選取您要檢視的特定SVM。導覽至「檔案系統」索引標籤、接著是「活動」、您會看到已啟用「活動追蹤」的磁碟區資料。

為所有磁碟區啟用

1. 選擇*儲存>磁碟區*。從功能表中選取SVM。
2. 瀏覽至*檔案系統*索引標籤、選擇*更多*索引標籤、即可在SVM中的所有磁碟區上啟用「活動追蹤」。

CLI

從 ONTAP 9.13.1 開始，您可以使用 ONTAP CLI 為多個磁碟區啟用「活動追蹤」。

步驟

1. 啟用活動追蹤：

   `volume activity-tracking on -vserver` *`svm_name`* `-volume [*|!`*`volume_names`*`]`

   使用 * 為指定儲存 VM 上的所有磁碟區啟用「活動追蹤」。

   使用 ！接著是 Volume 名稱、以啟用 SVM 上所有磁碟區的「活動追蹤」、但命名磁碟區除外。

2. 確認作業成功：

   `volume show -fields activity-tracking-state`

3. 啟用後、請使用ONTAP 「靜態系統管理程式」或ONTAP 「靜態API」來顯示「活動追蹤」資料。

使用 **FSA** 啟用 **ONTAP** 使用情況分析

從 ONTAP 9.12.1 開始，您可以啟用使用分析功能，查看磁碟區內的哪些目錄使用的空間最大。您可以檢視磁碟區中的目錄總數或磁碟區中的檔案總數。報告僅限於使用最多空間的 25 個目錄。

大型目錄的分析資料會每 15 分鐘重新整理一次。您可以檢查頁面頂端上次重新整理的時間戳記、以監控最近的重新整理。您也可以按一下 [下載] 按鈕，將資料下載至 Excel 活頁簿。下載作業會在背景執行、並顯示所選磁碟區最近回報的資訊。如果掃描傳回時沒有任何結果、請確定磁碟區已上線。例如、事件將導致檔案系統分析重新建立其大型目錄清單。SnapRestore

步驟

1. 選擇*儲存>磁碟區*。選取所需的Volume。
2. 從個別Volume功能表中、選取*檔案系統*。然後選取「使用率」索引標籤。

3. 切換*分析*交換器以啟用使用分析。
4. System Manager會顯示一個長條圖、以遞減順序識別大小最大的目錄。

> 收集熱門目錄清單時、可能會顯示部分資料或根本沒有資料。ONTAP掃描進度可在掃描期間顯示的「使用情況」索引標籤中找到。

若要深入瞭解特定目錄，您可以查看 ONTAP 檔案系統活動。

根據 FSA 中的 ONTAP 分析採取糾正措施

從功能支援的9.9開始ONTAP 、您可以直接從「檔案系統分析」顯示器、根據目前的資料和想要的結果、採取修正行動。

刪除目錄與檔案

在檔案總管畫面中、您可以選取要刪除的目錄或個別檔案。以低延遲的非同步目錄刪除功能刪除目錄。（非同步目錄刪除也可從 ONTAP 9.9.1 開始使用，但不啟用分析功能。）

從**ONTAP** 功能上開始。**9.10.1**	在**ONTAP 9.9.1** 中
1. 選擇“儲存 **>** 磁碟區”並選擇所需的磁碟區名稱。 2. 在單一磁碟區頁面中，選擇「檔案系統」選項卡，然後選擇「資源管理器」標籤。 3. 在*Explorer*視圖中，選擇所需的目錄。 4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除選項出現。 一次只能刪除一個物件。 刪除目錄和檔案時、新的儲存容量值不會立即顯示。	1. 選擇*儲存>磁碟區*。 2. 選取所需的磁碟區，然後選取 * 檔案總管 * 。 3. 在*Explorer*視圖中，選擇所需的目錄。 4. 若要刪除，請將滑鼠懸停在檔案或資料夾上，然後刪除選項出現。

在儲存層中指派媒體成本、以比較非使用中資料儲存位置的成本

媒體成本是您根據儲存成本評估所指派的價值、代表您選擇的每GB貨幣。設定後、System Manager會使用指派的媒體成本、在您移動磁碟區時、將預估的節約成本用於專案。

您設定的媒體成本並非持續性的、只能針對單一瀏覽器工作階段進行設定。

步驟

1. 按一下 * 儲存 > Tiers* 、然後按一下所需的本機層（集合）方塊中的 * 設定媒體成本 * 。

   請務必選取作用中和非作用中的層級、以便進行比較。

2. 輸入貨幣類型和金額。

當您輸入或變更媒體成本時、所有媒體類型都會進行變更。

移動磁碟區以降低儲存成本

根據分析顯示和媒體成本比較、您可以將磁碟區移至本機層中較便宜的儲存設備。

一次只能比較及移動一個Volume。

步驟

1. 啟用媒體成本顯示之後、按一下*儲存設備>層級*、然後按一下*磁碟區*。
2. 若要比較某個 Volume 的目的地選項、請按一下 ⋮ 該 Volume 、然後按一下 * 移動 * 。
3. 在* Select目的地本機層*顯示中、選取目的地層以顯示預估成本差異。
4. 在比較選項之後、選取所需的階層、然後按一下*移動*。

透過 **ONTAP** 檔案系統分析，以角色為基礎的存取控制

從 ONTAP 9.12.1 開始， ONTAP 包含一種預先定義的角色型存取控制（ RBAC ）角色，稱為 `admin-no-fsa`。此 `admin-no-fsa` 角色可授予系統管理員層級的 `Privileges` ，但可防止使用者在 `ONTAP CLI` ， `REST API` 和系統管理員中執行與端點相關的作業 `files`（例如檔案系統分析）。

如需的詳細資訊、請參閱 `admin-no-fsa` 角色、請參閱 叢集管理員的預先定義角色。

如果您使用ONTAP 的是ONTAP 發行版本不低於《支援資訊》9.12.1的版本、則需要建立專屬角色來控制檔案系統分析的存取。在ONTAP 版本的不含ONTAP 更新版本《R129.12.1.1》中、您必須透過ONTAP 《The R1221》或ONTAP 《The R1221 API》來設定RBAC權限。

系統管理員

從 ONTAP 9.12.1 開始，您可以使用系統管理員來設定檔案系統分析的 RBAC 權限。

步驟

1. 選擇*叢集>設定*。在 * 安全 * 下，導航至 * 用戶和角色 * ，然後選擇 → 。
2. 在 * 角色 * 下，選擇 + Add 。
3. 提供角色名稱。在「角色屬性」下、提供適當的權限來設定使用者角色的存取或限制 "API 端點"。請參閱下表、瞭解設定檔案系統分析存取或限制的主要路徑和次要路徑。

限制	主要路徑	次要路徑
Volume活動追蹤	`/api/storage/volumes`	• */:uuid*/top-metrics/directories • */:uuid*/top-metrics/files • */:uuid*/top-metrics/clients • */:uuid*/top-metrics/users
SVM上的活動追蹤	`/api/svm/svms`	• */:uuid*/top-metrics/directories • */:uuid*/top-metrics/files • */:uuid*/top-metrics/clients • */:uuid*/top-metrics/users
所有檔案系統分析作業	`/api/storage/volumes`	*/:uuid*/files

   您可以使用 `/*/` 而非UUID、可在端點設定所有磁碟區或SVM的原則。

   選擇每個端點的存取權限。

4. 選擇*保存*。
5. 若要將角色指派給使用者、請參閱 控制系統管理員存取權。

CLI

如果您使用ONTAP 的是ONTAP 版本不低於《21》的《21》、請使用ONTAP 《21》的《21》CLI建立自訂角色。

步驟

1. 建立預設角色以存取所有功能。

在建立限制角色之前、必須先完成這項作業、以確保「活動追蹤」上的角色僅受到限制：

```
security login role create -cmddirname DEFAULT -access all -role
storageAdmin
```

2. 建立限制角色：

```
security login role create -cmddirname "volume file show-disk-usage"
-access none -role storageAdmin
```

3. 授權角色存取SVM的Web服務：

   - `rest` 用於 REST API 呼叫
   - `security` 提供密碼保護
   - `sysmgr` 供 System Manager 存取

```
vserver services web access create -vserver <svm-name> -name rest -role
storageAdmin

vserver services web access create -vserver <svm-name> -name security
-role storageAdmin
```

```
vserver services web access create -vserver <svm-name> -name sysmgr -role
storageAdmin
```

4. 建立使用者。

   您必須針對要套用至使用者的每個應用程式、發出不同的create命令。在同一位使用者上多次呼叫建立、只會將所有應用程式套用至該位使用者、而不會每次都建立新的使用者。。 `http` 應用程式類型參數適用於 ONTAP REST API 和系統管理員。

```
security login create -user-or-group-name storageUser -authentication
-method password -application http -role storageAdmin
```

5. 有了新的使用者認證資料、您現在可以登入System Manager、或使用ONTAP REST API來存取檔案系統分析資料。

更多資訊

- 叢集管理員的預先定義角色
- 使用 System Manager 控制系統管理員存取
- "深入瞭解RBAC角色和ONTAP REST API"
- "建立安全登入"

ONTAP 檔案系統分析的考量事項

您應該瞭解與實作檔案系統分析相關的特定使用限制和潛在效能影響。

受SVM保護的關係

如果您已在包含SVM的磁碟區上啟用檔案系統分析功能、則分析資料不會複寫到目的地SVM。如果來源SVM必須在還原作業中重新同步、則您必須在還原後手動重新啟用所需磁碟區的分析功能。

效能考量

在某些情況下、啟用檔案系統分析可能會對初始中繼資料收集期間的效能造成負面影響。這是最常出現在使用率最大的系統上。為了避免在這類系統上啟用分析功能、您可以使用ONTAP 《支援系統管理程式》的效能監控工具。

如果您發現延遲明顯增加，請參閱"NetApp知識庫：開啟NetApp ONTAP檔案系統分析後延遲過高或波動"。

掃描考量

當您啟用容量分析時、 ONTAP 會執行容量分析的初始化掃描。掃描會存取已啟用容量分析之 Volume 中所有檔案的中繼資料。掃描期間不會讀取檔案資料。從 ONTAP 9.14.1 開始，您可以使用 REST API ，系統管理員的檔案總管 索引標籤或 CLI 命令來追蹤掃描進度 `volume analytics show`。如果發生節流事件、 ONTAP 會提供通知。

在磁碟區上啟用檔案系統分析時、請確保至少有 5% 至 8% 的磁碟區可用空間可用。如果磁碟區已啟用自動調整大小、請根據最大自動增加大小來計算可用大小。從 ONTAP 9.15.1 開始、如果您在磁碟區上啟用檔案系統分析時沒有足夠的可用空間、 ONTAP 會顯示錯誤訊息。

掃描完成後、檔案系統分析會隨著檔案系統變更而即時更新。

掃描所需時間與磁碟區上的目錄和檔案數量成比例。由於掃描會收集中繼資料、因此檔案大小不會影響掃描時間。

如需初始化掃描的詳細資訊、請參閱 "TR-4867 ：檔案系統分析的最佳實務準則"。

最佳實務做法

您應該在不共用集合體的磁碟區上開始掃描。您可以使用命令查看目前裝載哪些磁碟區的集合體：

```
volume show -volume comma-separated-list_of_volumes -fields aggr-list
```

掃描執行時、磁碟區會繼續處理用戶端流量。建議您在預期用戶端流量較低的期間開始掃描。

如果用戶端流量增加、就會消耗系統資源、導致掃描所需時間較長。

從 ONTAP 9.12.1 開始，您可以在系統管理員和 ONTAP CLI 中暫停資料收集。

- 如果您使用的是 ONTAP CLI ：
  - 您可以使用命令暫停資料收集： `volume analytics initialization pause -vserver svm_name -volume volume_name`
  - 一旦用戶端流量變慢、您就可以使用命令繼續資料收集： `volume analytics initialization resume -vserver svm_name -volume volume_name`
- 如果您使用的是 System Manager 、請在 Volume 功能表的 * 檔案總管 * 檢視中、使用 * 暫停資料收集 * 和 * 恢復資料收集 * 按鈕來管理掃描。

EMS 組態

瞭解 ONTAP EMS 組態

您可以設定ONTAP 支援功能支援功能、將重要的EMS（事件管理系統）事件通知直接傳送至電子郵件地址、syslog伺服器、簡易管理網路傳輸協定（SNMP）traphost或Webhook應用程式、以便立即通知您需要立即注意的系統問題。

由於重要事件通知預設不會啟用、因此您需要設定EMS、將通知傳送至電子郵件地址、syslog伺服器、SNMP traphost或Webhook應用程式。

檢閱的特定版本 "《EMS參考資料》（英文ONTAP ）"。

如果您的EMS事件對應使用過時ONTAP 的支援功能（例如事件目的地、事件路由）、建議您更新對應。"瞭解如何從已過時ONTAP 的等字指令更新EMS對應"。

使用系統管理員設定 ONTAP EMS 事件通知和篩選器

您可以使用System Manager來設定事件管理系統（EMS）傳送事件通知的方式、以便在系統問題需要您立即注意時通知您。

版本ONTAP	有了System Manager、您可以…
更新版本ONTAP	將事件傳送至遠端syslog伺服器時、請指定傳輸層安全性（TLS）傳輸協定。
更新版本ONTAP	設定電子郵件地址、syslog伺服器、Webhook應用程式、以及SNMP traphosts。
ONTAP 9.10.0 至 9.7	僅設定SNMP traphosts。 您可以使用ONTAP CLI設定其他EMS目的地。 請參閱 "EMS 組態概觀"。

新增**EMS**事件通知目的地

您可以使用System Manager來指定要將EMS訊息傳送到何處。

從S廳9.12.1開始ONTAP 、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。如"指令參考資料ONTAP"需詳細 `event notification destination create`資訊，請參閱。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮下、然後按一下 * 檢視事件目的地 * 。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 單擊。 + Add
5. 指定名稱、EMS目的地類型及篩選條件。

如有需要、您可以新增篩選條件。 按一下「新增事件篩選器」。

6. 視您選取的EMS目的地類型而定、請指定下列項目：

若要設定…	指定或選取…
SNMP traphost	• TrapHost名稱
電子郵件 （從9.10.1開始）	• 目的地電子郵件地址 • 郵件伺服器 • 寄件者電子郵件地址
系統記錄伺服器 （從9.10.1開始）	• 伺服器的主機名稱或IP位址 • 系統記錄連接埠（從9.12.1開始） • 系統記錄傳輸（從9.12.1開始） 選取「* TCP Encrypted （ TCP加密*）」可啟用傳輸層安全性（TLS）傳輸協定。如果未輸入* Syslog連接埠*的值、則會根據* Syslog transport*選項使用預設值。
Webhook （從9.10.1開始）	• Webhook URL • 用戶端驗證（選取此選項以指定用戶端憑證）

建立新的**EMS**事件通知篩選器

從ONTAP 《E59.10.1》開始、您可以使用System Manager定義新的自訂篩選條件、以指定處理EMS通知的規則。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮ 下、然後按一下 * 檢視事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 單擊。 + Add
5. 指定名稱、然後選取是要從現有事件篩選器複製規則、還是要新增規則。
6. 視您的選擇而定、請執行下列步驟：

如果您選擇……	然後執行下列步驟…
從現有事件篩選器複製規則	1. 選取現有的事件篩選器。 2. 修改現有規則。 3. 如有需要、請按一下以新增其他規則 + Add 。

新增規則	指定每個新規則的類型、名稱模式、嚴重性及SNMP設陷類型。

編輯**EMS**事件通知目的地

從ONTAP 版本支援的版本起、您可以使用System Manager來變更事件通知目的地資訊。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮ 下、然後按一下 * 檢視事件目的地 * 。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 在事件目的地名稱旁邊，按一下 ⋮ ，然後按一下 * 編輯 * 。
5. 修改事件目的地資訊、然後按一下「儲存」。

編輯**EMS**事件通知篩選器

從ONTAP 功能更新至功能更新至功能更新、您可以使用System Manager修改自訂的篩選條件、以變更事件通知的處理方式。

ⓘ 您無法修改系統定義的篩選條件。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮ 下、然後按一下 * 檢視事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁邊，按一下 ⋮ ，然後按一下 * 編輯 * 。
5. 修改事件篩選器資訊、然後按一下「儲存」。

刪除**EMS**事件通知目的地

從ONTAP 《支援範本》（《支援範本》）9.10.1開始、您可以使用System Manager刪除EMS事件通知目的地。

ⓘ 您無法刪除SNMP目的地。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮ 下、然後按一下 * 檢視事件目的地 * 。
3. 在*通知管理*頁面上、選取*事件目的地*索引標籤。
4. 在事件目的地名稱旁邊，按一下 ⋮ ，然後按一下 * 刪除 * 。

刪除EMS事件通知篩選器

從《軟件及應用程式》（2019）9.10.1開始ONTAP 、您可以使用System Manager刪除自訂的篩選條件。

您無法刪除系統定義的篩選條件。

步驟

1. 按一下*叢集>設定*。
2. 在 * 通知管理 * 區段中、按一 ⋮下、然後按一下 * 檢視事件目的地 * 。
3. 在「通知管理」頁面上、選取「事件篩選器」索引標籤。
4. 在事件篩選器名稱旁邊，按一下 ⋮，然後按一下 * 刪除 * 。

相關資訊

- "《環管系統參考資料》ONTAP"
- "使用CLI設定SNMP traphosts以接收事件通知"

使用CLI設定EMS事件通知

ONTAP EMS 組態工作流程

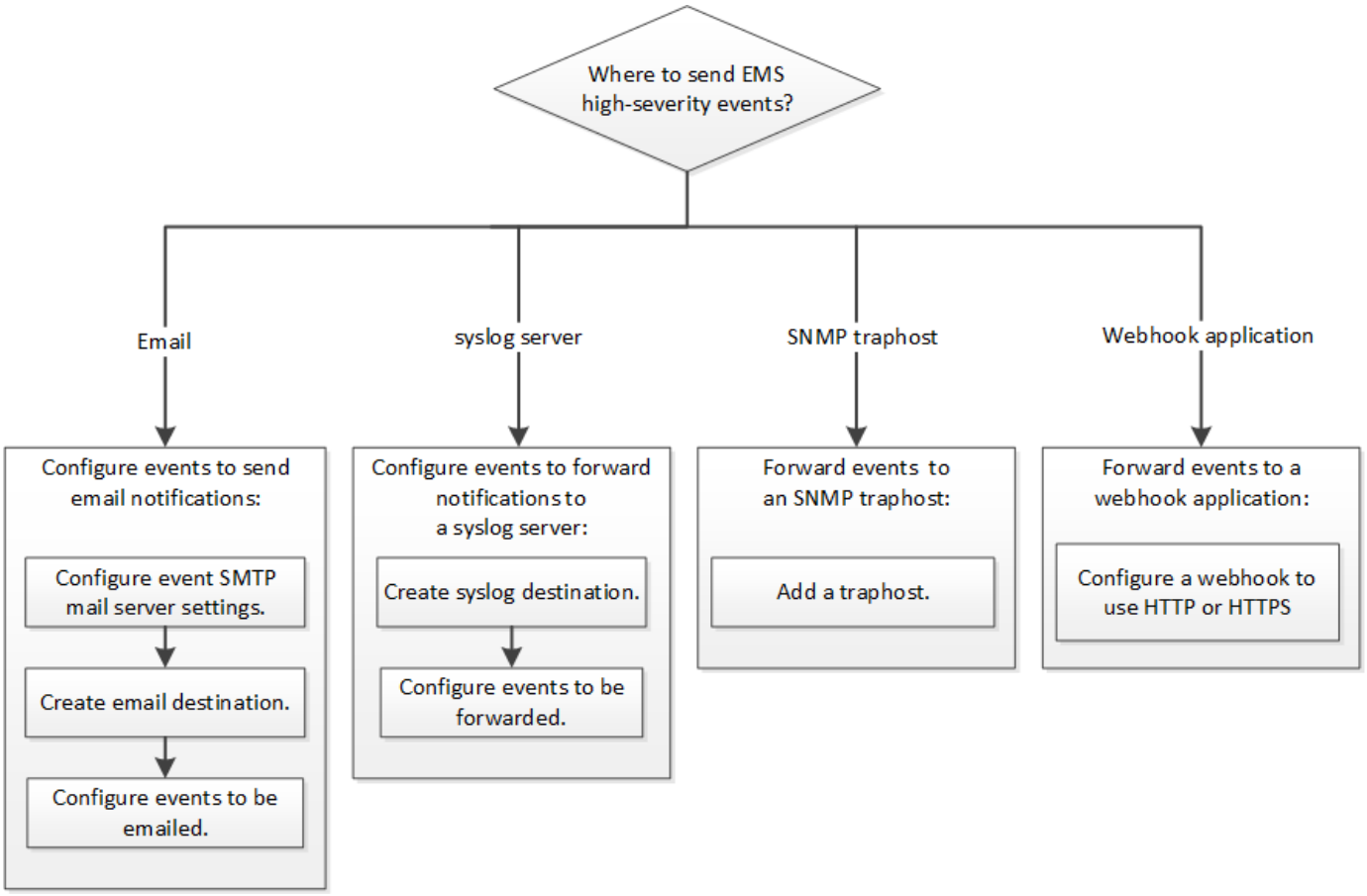
您必須將重要的EMS事件通知設定為以電子郵件傳送、轉送至syslog伺服器、轉送至SNMP traphost、或轉送至Webhook應用程式。這有助於您及時採取修正行動、避免系統中斷。

關於這項工作

如果您的環境已包含syslog伺服器、可用來彙總來自其他系統（例如伺服器和應用程式）的記錄事件、那麼使用syslog伺服器也能更輕鬆地從儲存系統發出重要的事件通知。

如果您的環境尚未包含syslog伺服器、則使用電子郵件進行重要事件通知會更容易。

如果您已將事件通知轉送到SNMP traphost、則可能需要監控該traphost是否有重要事件。



選擇

- 設定EMS以傳送事件通知。

如果您需要…	請參閱此…
將重要事件通知傳送至電子郵件地址的EMS	設定重要的EMS事件以傳送電子郵件通知
EMS可將重要事件通知轉送至syslog伺服器	設定重要的EMS事件、將通知轉送到syslog伺服器
如果您想要EMS將事件通知轉送到SNMP traphost	設定SNMP traphosts以接收事件通知
如果您想要EMS將事件通知轉送到Webhook應用程式	設定重要的EMS事件、將通知轉送到Webhook應用程式

設定重要的 **ONTAP EMS** 事件以傳送電子郵件通知

若要接收最重要事件的電子郵件通知、您必須將EMS設定為針對重要活動的事件傳送電子郵件訊息。

開始之前

必須在叢集上設定DNS、才能解析電子郵件地址。

關於這項工作

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 設定事件的SMTP郵件伺服器設定：

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

   如"指令參考資料ONTAP"需詳細 `event config modify`資訊，請參閱。

2. 建立事件通知的電子郵件目的地：

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

   如"指令參考資料ONTAP"需詳細 `event notification destination create`資訊，請參閱。

3. 設定重要事件以傳送電子郵件通知：

   ```
   event notification create -filter-name important-events -destinations storage-
   admins
   ```

   如"指令參考資料ONTAP"需詳細 `event notification create`資訊，請參閱。

設定重要的 **ONTAP EMS** 事件，將通知轉送到系統記錄伺服器

若要在syslog伺服器上記錄最嚴重事件的通知、您必須將EMS設定為轉送重要活動訊號的事件通知。

開始之前

必須在叢集上設定DNS、才能解析syslog伺服器名稱。

關於這項工作

如果您的環境尚未包含用於事件通知的syslog伺服器、您必須先建立一個。如果您的環境中已包含用於記錄其他系統事件的syslog伺服器、您可能會想要使用該伺服器來處理重要的事件通知。

您可以在ONTAP 叢集執行時、在CLI輸入命令來執行此工作。

從S廳9.12.1開始ONTAP 、可透過傳輸層安全（TLS）傳輸協定、將EMS事件傳送至遠端syslog伺服器上的指定連接埠。有兩個新參數可供使用：

`tcp-encrypted`

何時 `tcp-encrypted` 為指定 `syslog-transport`、ONTAP 驗證目的地主機的憑證來驗證其身分。預設值為 `udp-unencrypted`。

`syslog-port`

預設值 `syslog-port` 參數取決於的設定 `syslog-transport` 參數。如果 `syslog-transport` 設為 `tcp-encrypted`、 `syslog-port` 預設值為6514。

步驟

1. 建立重要事件的syslog伺服器目的地：

   `event notification destination create -name *syslog-ems* -syslog *syslog-server-address* -syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   從ONTAP 功能變數9.12.1開始、可以指定下列值 `syslog-transport`：

   - `udp-unencrypted` 無安全性的使用者資料包傳輸協定
   - `tcp-unencrypted` 無安全性的傳輸控制傳輸協定
   - `tcp-encrypted` -傳輸層安全性（TLS）的傳輸控制傳輸協定

     預設傳輸協定為 `udp-unencrypted`。

   如"指令參考資料ONTAP"需詳細 `event notification destination create`資訊，請參閱。

2. 設定重要事件以將通知轉送到syslog伺服器：

   `event notification create -filter-name *important-events* -destinations *syslog-ems*`

   如"指令參考資料ONTAP"需詳細 `event notification create`資訊，請參閱。

設定 **ONTAP SNMP traphosts** 以接收事件通知

若要在SNMP traphost上接收事件通知、您必須設定traphost。

開始之前

- 必須在叢集上啟用SNMP和SNMP設陷。

  SNMP和SNMP設陷預設為啟用。

- 必須在叢集上設定DNS、才能解析traphost名稱。

關於這項工作

如果您尚未設定SNMP traphost來接收事件通知（SNMP設陷）、則必須新增一個。

您可以在ONTAP 叢集執行時、在指令行輸入命令來執行此工作。

步驟

1. 如果您的環境尚未設定SNMP traphost來接收事件通知、請新增一個：

   `system snmp traphost add -peer-address *snmp_traphost_name*`

   SNMP預設支援的所有事件通知都會轉送到SNMP traphost。

設定重要的 **ONTAP EMS** 事件，將通知轉寄至 **Webhook** 應用程式

您可以設定ONTAP 將重要事件通知轉送至Webhook應用程式。所需的組態步驟取決於您

選擇的安全性層級。

準備設定EMS事件轉送

在設定ONTAP 將事件通知轉送到Webhook應用程式之前、您應該考慮幾個概念和要求。

Webhook應用程式

您需要能夠接收ONTAP 不必要事件通知的Webhook應用程式。Webhook是使用者定義的回撥例行工作、可延伸執行遠端應用程式或伺服器的功能。Webhooks是由用戶端呼叫或啟動（本例ONTAP 為示例）、方法是將HTTP要求傳送至目的地URL。具體而言ONTAP 、將HTTP POST要求傳送至裝載Webhook應用程式的伺服器、以及以XML格式設定的事件通知詳細資料。

安全選項

視傳輸層安全性（TLS）傳輸協定的使用方式而定、有多種安全選項可供選擇。您選擇的選項會決定所需ONTAP 的功能組態。

TLS是一種在網際網路上廣泛使用的密碼編譯傳輸協定。它使用一或多個公開金鑰憑證來提供隱私、資料完整性和驗證。這些憑證由信任的憑證授權單位核發。

HTTP

您可以使用HTTP來傳輸事件通知。使用此組態時、連線不安全。不驗證不驗證ONTAP 客戶端和Webhook應用程式的身分。此外、網路流量並未加密或受到保護。請參閱 "設定Webhook目的地以使用HTTP" 以取得組態詳細資料。

HTTPS

為了提高安全性、您可以在裝載Webhook例行工作的伺服器上安裝憑證。驗證Webhook應用程式伺服器及雙方身分的HTTPS傳輸協定、ONTAP 以確保網路流量的隱私性和完整性。請參閱 "設定 Webhook 目的地以使用 HTTPS" 以取得組態詳細資料。

HTTPS搭配相互驗證

您可以在ONTAP 發出Webbook要求的系統上安裝用戶端憑證、進一步強化HTTPS安全性。除了驗證Webhook應用程式伺服器的身分、並保護網路流量之外、Webhook應用程式還會驗證該客戶端的身分。ONTAP ONTAP這種雙向對等驗證稱為「相互TLS」。請參閱 "設定Webhook目的地使用HTTPS進行相互驗證" 以取得組態詳細資料。

相關資訊

- "傳輸層安全性（TLS）傳輸協定1.3版"

設定Webhook目的地以使用HTTP

您可以設定ONTAP 使用HTTP將事件通知轉送至Webhook應用程式。這是最不安全的選項、但設定起來最簡單。

步驟

1. 建立新目的地 `restapi-ems` 若要接收事件：

```
event notification destination create -name restapi-ems -rest-api-url
http://<webhook-application>
```

在上述命令中、您必須使用* HTTP配置作為目的地。

如"指令參考資料ONTAP"需詳細 `event notification destination create`資訊，請參閱。

2. 建立連結的通知 `important-events` 使用篩選 `restapi-ems` 目的地：

```
event notification create -filter-name important-events -destinations restapi-ems
```

如"指令參考資料ONTAP"需詳細 `event notification create`資訊，請參閱。

設定 **Webhook** 目的地以使用 **HTTPS**

您可以設定 ONTAP 、使用 HTTPS 將事件通知轉寄至 Webhook 應用程式。使用伺服器憑證來確認Webhook應用程式的身分識別、以及保護網路流量。ONTAP

開始之前

- 為Webhook應用程式伺服器產生私密金鑰和憑證
- 讓root憑證可安裝在ONTAP 整個過程中

步驟

1. 在裝載Webhook應用程式的伺服器上安裝適當的伺服器私密金鑰和憑證。具體的組態步驟取決於伺服器。
2. 將伺服器根憑證安裝在ONTAP

```
security certificate install -type server-ca
```

命令會要求提供憑證。

3. 建立 `restapi-ems` 接收事件的目的地：

```
event notification destination create -name restapi-ems -rest-api-url https://<webhook-application>
```

在上述命令中、您必須使用* HTTPS *配置作為目的地。

4. 建立連結的通知 `important-events` 使用新的篩選器 `restapi-ems` 目的地：

```
event notification create -filter-name important-events -destinations restapi-ems
```

設定**Webhook**目的地使用**HTTPS**進行相互驗證

您可以設定ONTAP 將事件通知轉送至Webhook應用程式、使用HTTPS搭配相互驗證。使用此組態有兩個憑證。使用伺服器憑證來確認Webhook應用程式的身分、並保護網路流量。ONTAP此外、裝載Webhook的應用程式會使用用戶端憑證來確認ONTAP 該客戶端的身分。

開始之前

您必須先執行下列步驟、才能設定ONTAP 使用功能：

- 為Webhook應用程式伺服器產生私密金鑰和憑證

- 讓root憑證可安裝在ONTAP 整個過程中
- 為ONTAP 該驗證用戶端產生私密金鑰和憑證

步驟

1. 執行工作的前兩個步驟 "設定 Webhook 目的地以使用 HTTPS" 安裝伺服器憑證、ONTAP 以便驗證伺服器的身分。
2. 在Webhook應用程式中安裝適當的根和中繼憑證、以驗證用戶端憑證。
3. 將用戶端憑證安裝ONTAP 在下列項目中：

   ```
   security certificate install -type client
   ```

   命令會要求提供私密金鑰和憑證。

4. 建立 `restapi-ems` 接收事件的目的地：

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   在上述命令中、您必須使用* HTTPS *配置作為目的地。

5. 建立連結的通知 `important-events` 使用新的篩選器 `restapi-ems` 目的地：

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

相關資訊

- "安全性憑證安裝"

更新過時的**EMS**事件對應

瞭解 **ONTAP EMS** 事件對應模式

在版本不含故障碼的9.0之前ONTAP 、EMS事件只能根據事件名稱模式的相符結果對應至事件目的地。ONTAP 命令集 (`event destination`、 `event route`）使用此模型的 ONTAP 最新版本仍然可用，但從 ONTAP 9.0 開始已被淘汰。

從 ONTAP 9.0 開始、 ONTAP EMS 事件目的地對應的最佳實務做法是使用更具擴充性的事件篩選器模型、在多個欄位上使用進行模式比對 `event filter`、 `event notification`和 `event notification destination` 命令集。

如果您的 EMS 對應是使用過時的命令進行設定，您應該更新對應，以使用 `event filter`， `event notification`和 `event notification destination`命令集。如"指令參考資料ONTAP"需詳細 `event`資訊，請參閱。

事件目的地有兩種類型：

1. 系統產生的目的地：有五個系統產生的事件目的地（預設為建立）

   - `allevents`

- asup
- criticals
- pager
- traphost

  某些系統產生的目的地是為了特殊目的而設計。例如、asup目的地會將CallHome.*事件路由到AutoSupport 位在畫面上的這個動作模組ONTAP 、以產生AutoSupport 各種訊息。

2. * 使用者建立的目的地 * ：這些目的地是使用手動建立的 `event destination create` 命令。

```
cluster-1::event*> destination show
                                                                    Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
traphost          -                 -                  -
false
5 entries were displayed.
+
cluster-1::event*> destination create -name test -mail test@xyz.com
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
+
cluster-1::event*> destination show
+
Hide
Name              Mail Dest.        SNMP Dest.         Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                 -                  -
false
asup              -                 -                  -
false
criticals         -                 -                  -
false
pager             -                 -                  -
false
test              test@xyz.com      -                  -
false
traphost          -                 -                  -
false
6 entries were displayed.
```

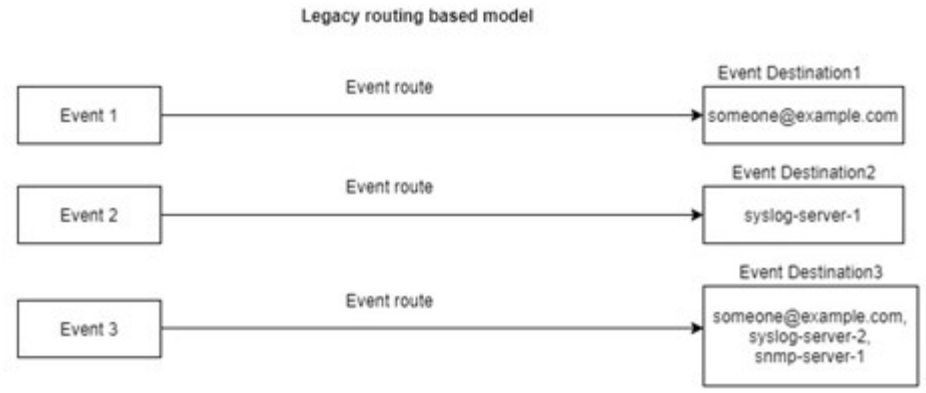
在過時的模型中、 EMS 事件會使用個別對應至目的地 `event route add-destinations` 命令。

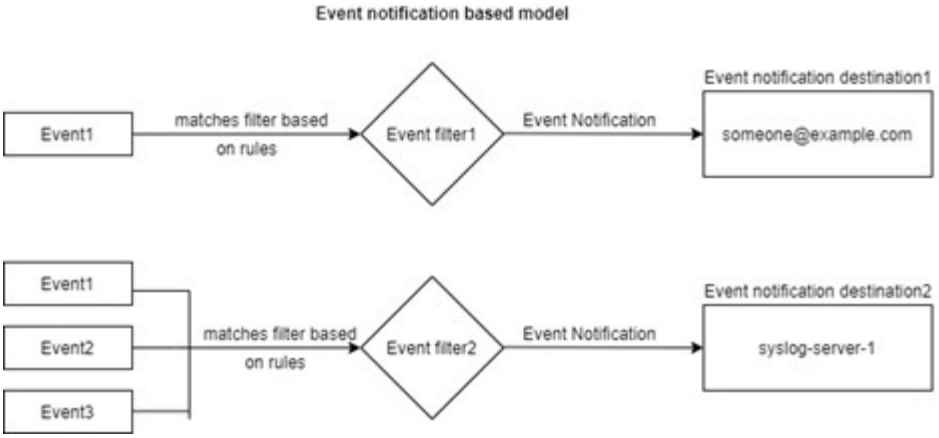
```
cluster-1::event*> route add-destinations -message-name raid.aggr.*
-destinations test
This command is deprecated. Use the "event filter", "event notification
destination" and "event notification" commands, instead.
4 entries were acted on.

cluster-1::event*> route show -message-name raid.aggr.*
                                                                  Freq
Time
Message                          Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort         NOTICE         test           0       0
raid.aggr.autoGrow.success       NOTICE         test           0       0
raid.aggr.lock.conflict          INFORMATIONAL  test           0       0
raid.aggr.log.CP.count           DEBUG          test           0       0
4 entries were displayed.
```

全新且可擴充的EMS事件通知機制、是以事件篩選器和事件通知目的地為基礎。如需新事件通知機制的詳細資訊、請參閱下列知識庫文章：

- "事件管理系統概述ONTAP （適用於）。9."





使用過時的命令更新 **ONTAP EMS** 事件對應

如果您的 EMS 事件對應目前是使用過時的 ONTAP 命令集進行設定 (`event destination`、 `event route`）、您應該遵循此程序來更新對應以使用 `event filter`、 `event notification`和 `event notification destination` 命令集。

步驟

1. 使用列出系統中的所有事件目的地 `event destination show` 命令。

```
cluster-1::event*> destination show

Hide
Name              Mail Dest.         SNMP Dest.          Syslog Dest.
Params
---------------- ----------------- ------------------ ------------------
------
allevents         -                  -                  -
false
asup              -                  -                  -
false
criticals         -                  -                  -
false
pager             -                  -                  -
false
test              test@xyz.com       -                  -
false
traphost          -                  -                  -
false
6 entries were displayed.
```

2. 針對每個目的地、使用列出對應至目的地的事件 `event route show -destinations <destination name>` 命令。

```
cluster-1::event*> route show -destinations test
                                                                    Freq
Time
Message                           Severity       Destinations   Threshd
Threshd
-------------------------------- -------------- -------------- -------
-------
raid.aggr.autoGrow.abort          NOTICE         test           0       0
raid.aggr.autoGrow.success        NOTICE         test           0       0
raid.aggr.lock.conflict           INFORMATIONAL  test           0       0
raid.aggr.log.CP.count            DEBUG          test           0       0
4 entries were displayed.
```

3. 建立對應的 `event filter` 其中包括所有這些事件子集。
例如、如果您只想要包含 `raid.aggr.*` 事件、請使用萬用字元 `message-name` 建立篩選器時的參數。您也可以為單一事件建立篩選器。

   如"指令參考資料ONTAP"需詳細 `event filter`資訊，請參閱。

   > 您最多可以建立50個事件篩選器。

```
cluster-1::event*> filter create -filter-name test_events

cluster-1::event*> filter rule add -filter-name test_events -type
include -message-name raid.aggr.*

cluster-1::event*> filter show -filter-name test_events
Filter Name Rule     Rule      Message Name           SNMP Trap Type
Severity
            Position Type
----------- -------- --------- ---------------------- ---------------
--------
test_events
            1        include   raid.aggr.*            *               *
            2        exclude   *                      *               *
2 entries were displayed.
```

4. 建立 `event notification destination` 針對每個 `event destination` 端點（例如 SMTP/SNMP/Syslog ）

```
cluster-1::event*> notification destination create -name dest1 -email
test@xyz.com

cluster-1::event*> notification destination show
Name            Type        Destination
--------------  ----------  --------------------
dest1           email       test@xyz.com (via "localhost" from
"admin@localhost", configured in "event config")
snmp-traphost   snmp        - (from "system snmp traphost")
2 entries were displayed.
```

深入瞭解 `event notification destination`及 `event destination` "指令參考資料ONTAP"。

5. 將事件篩選器對應至事件通知目的地、以建立事件通知。

```
cluster-1::event*> notification create -filter-name asup_events
-destinations dest1

cluster-1::event*> notification show
ID   Filter Name                    Destinations
---- ------------------------------ -----------------
1    default-trap-events            snmp-traphost
2    asup_events                    dest1
2 entries were displayed.
```

6. 針對每個項目重複步驟 1-5 `event destination` 那有 `event route` 對應：

> 路由至 SNMP 目的地的事件應對應至 `snmp-traphost` 事件通知目的地。SNMP traphost目的地使用系統設定的SNMP traphost。

```
cluster-1::event*> system snmp traphost add 10.234.166.135

cluster-1::event*> system snmp traphost show
        scspr2410142014.gdl.englab.netapp.com
(scspr2410142014.gdl.englab.netapp.com) <10.234.166.135>    Community:
public

cluster-1::event*> notification destination show -name snmp-traphost

                Destination Name: snmp-traphost
            Type of Destination: snmp
                    Destination: 10.234.166.135 (from "system snmp
traphost")
 Server CA Certificates Present?: -
   Client Certificate Issuing CA: -
Client Certificate Serial Number: -
       Client Certificate Valid?: -
```

指令參考資料ONTAP

對於每個主要的ONTAP版本，常用的 CLI 指令（ONTAP手冊頁或手冊頁）都會捆綁到"《指令參考》ONTAP" 。這些命令參考解釋如何使用每個ONTAP版本中的 CLI 命令。

您也可以在ONTAP命令列中使用手冊頁 `man`命令。詳細了解 `man`在"指令參考資料ONTAP" 。

指令參考ONTAP 資料以取得有限支援版本的支援（僅PDF）

- "ONTAP 9.4"

CLI比較工具

您可以使用瞭解ONTAP 有關在各個版本之間變更命令列介面（CLI）命令的資訊 "CLI比較工具" 於 NetApp 支援網站。

相關資訊

- 使用ONTAP 指令行介面
- 瀏覽CLI命令目錄的方法
- "儲存磁碟顯示"

法律聲明

法律聲明提供版權聲明、商標、專利等存取權限。

版權

"https://www.netapp.com/company/legal/copyright/"

商標

NetApp 、 NetApp 標誌及 NetApp 商標頁面上列出的標章均為 NetApp 、 Inc. 的商標。其他公司與產品名稱可能為其各自所有者的商標。

"https://www.netapp.com/company/legal/trademarks/"

專利

如需最新的 NetApp 擁有專利清單、請參閱：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隱私權政策

"https://www.netapp.com/company/legal/privacy-policy/"

開放原始碼

通知檔案提供有關 NetApp 軟體所使用之協力廠商版權與授權的資訊。

ONTAP

"ONTAP 9.18.1 通知" "ONTAP 9.17.1 通知" "ONTAP 9 注意事項。 16.1" "ONTAP 9 .16.0 注意事項" "ONTAP 9.15.1 注意事項" "ONTAP 9.15.0 注意事項" "ONTAP 9.14.1 注意事項" "ONTAP 9.14.0 注意事項" "ONTAP 9.13.1 注意事項" "關於此功能的注意事項ONTAP 9.12.1.1" "關於此功能的注意事項ONTAP 9.12.0" "ONTAP 9.11.1 注意事項" "關於本產品的注意事項ONTAP 9.10.1" "ONTAP 9.10.0 注意事項" "關於此功能的注意事項ONTAP" "關於本產品的注意事項ONTAP 9.8" "關於產品的注意ONTAP 事項9.7" "關於此功能的注意事項ONTAP" "關於本產品的注意事項ONTAP" "關於產品的注意事項ONTAP 9.4" "關於本產品的注意事項ONTAP" "關於此功能的注意事項ONTAP 9.2" "關於此產品的注意事項ONTAP"

適用於 **MetroCluster IP** 組態的 **ONTAP Mediator**

"ONTAP調解員通知 1.11" "ONTAP調解員通知 1.10" "ONTAP Mediator 1.9.1 版通知" "ONTAP調解員1.8通知" "ONTAP調解員1.7通知" "ONTAP調解員1.5通知"

版權資訊

Copyright © 2026 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

此軟體以 NETAPP「原樣」提供，不含任何明示或暗示的擔保，包括但不限於有關適售性或特定目的適用性之擔保，特此聲明。於任何情況下，就任何已造成或基於任何理論上責任之直接性、間接性、附隨性、特殊性、懲罰性或衍生性損害（包括但不限於替代商品或服務之採購；使用、資料或利潤上的損失；或企業營運中斷），無論是在使用此軟體時以任何方式所產生的契約、嚴格責任或侵權行為（包括疏忽或其他）等方面，NetApp 概不負責，即使已被告知有前述損害存在之可能性亦然。

NetApp 保留隨時變更本文所述之任何產品的權利，恕不另行通知。NetApp 不承擔因使用本文所述之產品而產生的責任或義務，除非明確經過 NetApp 書面同意。使用或購買此產品並不會在依據任何專利權、商標權或任何其他 NetApp 智慧財產權的情況下轉讓授權。

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

有限權利說明：政府機關的使用、複製或公開揭露須受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中的「技術資料權利 - 非商業項目」條款 (b)(3) 小段所述之限制。

此處所含屬於商業產品和 / 或商業服務（如 FAR 2.101 所定義）的資料均為 NetApp, Inc. 所有。根據本協議提供的所有 NetApp 技術資料和電腦軟體皆屬於商業性質，並且完全由私人出資開發。 美國政府對於該資料具有非專屬、非轉讓、非轉授權、全球性、有限且不可撤銷的使用權限，僅限於美國政府為傳輸此資料所訂合約所允許之範圍，並基於履行該合約之目的方可使用。除非本文另有規定，否則未經 NetApp Inc. 事前書面許可，不得逕行使用、揭露、重製、修改、履行或展示該資料。美國政府授予國防部之許可權利，僅適用於 DFARS 條款 252.227-7015(b)（2014 年 2 月）所述權利。

商標資訊

NETAPP、NETAPP 標誌及 http://www.netapp.com/TM 所列之標章均為 NetApp, Inc. 的商標。文中所涉及的所有其他公司或產品名稱，均為其各自所有者的商標，不得侵犯。