



SnapCenter software文檔

SnapCenter software

NetApp
September 29, 2025

This PDF was generated from <https://docs.netapp.com/zh-tw/snapcenter-61/index.html> on September 29, 2025. Always check docs.netapp.com for the latest.

目錄

SnapCenter software文檔	1
發行說明	2
發行說明	2
SnapCenter支援的升級路徑	2
開始	3
了解SnapCenter software	3
SnapCenter概述	3
SnapCenter中的安全功能	7
SnapCenter中基於角色的存取控制	8
SnapCenter中的災難復原	13
SnapCenter所需的許可證	13
SnapCenter中的SnapMirror主動同步	16
資料保護的關鍵概念	16
SnapCenter支援的儲存系統和應用程式	18
SnapCenter憑證的驗證方法	18
ASA r2 系統支援的SnapCenter操作	19
SnapCenter software快速入門	20
安裝並設定SnapCenter伺服器	22
準備安裝SnapCenter伺服器	22
安裝SnapCenter伺服器的要求	22
註冊以存取SnapCenter software	27
多重身份驗證 (MFA)	27
安裝SnapCenter伺服器	37
在 Windows 主機上安裝SnapCenter伺服器	37
在 Linux 主機上安裝SnapCenter伺服器	41
註冊SnapCenter	45
使用 RBAC 授權登入SnapCenter	45
配置SnapCenter伺服器	48
新增並配置儲存系統	48
新增基於SnapCenter Standard 控制器的許可證	68
配置高可用性	73
配置基於角色的存取控制 (RBAC)	77
配置審核日誌設定	105
使用SnapCenter Server 設定安全的 MySQL 連接	106
配置基於憑證的身份驗證	111
啟用基於憑證的身份驗證	111
從SnapCenter伺服器匯出憑證授權單位 (CA) 憑證	112
將 CA 憑證匯入 Windows 插件主機	112
將 CA 憑證匯入 UNIX 插件主機	113

匯出SnapCenter證書	114
為 Windows 主機設定 CA 憑證	115
產生CA憑證CSR文件	115
匯入 CA 憑證	115
取得 CA 憑證指紋	116
使用 Windows 主機插件服務設定 CA 憑證	117
使用SnapCenter站點配置 CA 證書	117
為SnapCenter啟用 CA 憑證	118
為Linux主機設定CA憑證	118
設定nginx證書	119
配置審核日誌證書	119
配置SnapCenter服務證書	119
在 Windows 主機上設定並啟用雙向 SSL 通信	120
在 Windows 主機上設定雙向 SSL 通信	120
在 Windows 主機上啟用雙向 SSL 通信	122
在 Linux 主機上設定並啟用雙向 SSL 通信	123
在 Linux 主機上設定雙向 SSL 通信	123
在 Linux 主機上啟用 SSL 通信	125
配置 Active Directory、LDAP 和 LDAPS	125
註冊不受信任的 Active Directory 網域	125
設定 IIS 應用程式集區以啟用 Active Directory 讀取權限	127
為 LDAPS 設定 CA 用戶端憑證	127
保護 Microsoft SQL Server 資料庫	129
適用於 Microsoft SQL Server 的SnapCenter插件	129
適用於 Microsoft SQL Server 的SnapCenter外掛程式概述	129
您可以使用適用於 Microsoft SQL Server 的SnapCenter外掛程式執行哪些操作	129
適用於 Microsoft SQL Server 的SnapCenter外掛功能	130
支援 Windows 群集中的非對稱 LUN 映射	131
SnapCenter Plug-in for Microsoft SQL Server 支援的儲存類型	132
適用於 Microsoft SQL Server 的SnapCenter外掛程式的儲存佈局建議	134
SQL 插件所需的最低ONTAP權限	136
為 SQL Server 外掛程式準備SnapMirror和SnapVault複製的儲存系統	138
SQL Server 資源的備份策略	139
SQL Server 的復原策略	142
定義 SQL Server 的克隆策略	145
準備安裝適用於 Microsoft SQL Server 的SnapCenter插件	146
SnapCenter Plug-in for Microsoft SQL Server 的安裝工作流程	146
新增主機並安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式的先決條件	146
安裝適用於 Windows 的SnapCenter插件包的主機需求	147
為 Windows 的SnapCenter插件包設定憑證	148
為單一 SQL Server 資源配置憑證	149

在 Windows Server 2016 或更高版本上設定 gMSA	151
為 Microsoft SQL Server 安裝SnapCenter插件	152
設定 CA 憑證	157
配置災難復原	161
SnapCenter Plug-in for VMware vSphere	163
部署 CA 憑證	163
配置 CRL 文件	163
做好資料保護準備	163
使用適用於 Microsoft SQL Server 的SnapCenter外掛程式的先決條件	163
如何使用資源、資源群組和原則來保護 SQL Server	164
備份 SQL Server 資料庫、執行個體或可用性群組	164
備份工作流	164
確定資源是否可用於備份	166
將資源遷移到NetApp儲存系統	167
為 SQL Server 資料庫建立備份策略	169
為 SQL Server 建立資源組並附加策略	174
在ASA r2 系統上建立資源組並啟用對 Microsoft SQL Server 資源的二級保護	176
備份 SQL 資源的需求	179
使用 PowerShell cmdlet 建立儲存系統連線和憑證	179
備份 SQL 資源	180
備份 SQL Server 資源組	184
在SnapCenter作業頁面中監控 SQL 資源備份作業	185
取消用於 Microsoft SQL Server 備份作業的SnapCenter插件	186
在拓樸頁面中檢視 SQL Server 備份和克隆	187
使用 PowerShell cmdlet 清理輔助備援計數	189
還原 SQL Server 資源	189
復原工作流程	189
恢復資料庫的要求	190
還原 SQL Server 資料庫備份	191
從輔助儲存還原 SQL Server 資料庫	196
使用 PowerShell cmdlet 還原資源	197
重新設定可用性群組資料庫	199
監視 SQL 資源恢復操作	200
取消SQL資源復原操作	201
克隆 SQL Server 資料庫資源	201
克隆工作流程	201
從 SQL Server 資料庫備份克隆	202
執行複製生命週期	209
監視 SQL 資料庫克隆操作	211
取消 SQL 資源克隆操作	212
分裂克隆	212

保護 SAP HANA 資料庫	214
適用於 SAP HANA 資料庫的SnapCenter插件	214
適用於 SAP HANA 資料庫的SnapCenter插件概述	214
使用適用於 SAP HANA 資料庫的SnapCenter插件可以做什麼	214
適用於 SAP HANA 資料庫的SnapCenter插件功能	214
SnapCenter Plug-in for SAP HANA Database 支援的儲存類型	215
SAP HANA 插件所需的最低ONTAP權限	216
為 SAP HANA 資料庫的SnapMirror和SnapVault複製準備儲存系統	219
SAP HANA 資料庫的備份策略	219
SAP HANA 資料庫的還原與復原策略	222
準備安裝適用於 SAP HANA 資料庫的SnapCenter插件	224
SAP HANA 資料庫的SnapCenter插件安裝工作流程	224
新增主機和安裝適用於 SAP HANA 資料庫的SnapCenter插件的先決條件	225
安裝適用於 Windows 的SnapCenter插件包的主機需求	228
安裝適用於 Linux 的SnapCenter插件包的主機需求	229
為 SAP HANA 資料庫的SnapCenter插件設定憑證	230
在 Windows Server 2016 或更高版本上設定 gMSA	232
為 SAP HANA 資料庫安裝SnapCenter插件	234
設定 CA 憑證	239
SnapCenter Plug-in for VMware vSphere	246
部署 CA 憑證	246
配置 CRL 文件	246
做好資料保護準備	246
使用適用於 SAP HANA 資料庫的SnapCenter插件的先決條件	246
如何使用資源、資源群組和原則來保護 SAP HANA 資料庫	247
備份 SAP HANA 資源	247
備份 SAP HANA 資源	247
為 SAP HANA 資料庫設定 HDB 用戶儲存金鑰和 HDBSQL OS 用戶	248
發現資源並準備多租戶資料庫容器以進行資料保護	249
手動將資源新增至插件主機	251
為 SAP HANA 資料庫建立備份策略	253
建立資源組並附加策略	256
在ASA r2 系統上建立資源組並啟用 SAP HANA 資源的二級保護	260
使用 PowerShell cmdlet 為 SAP HANA 資料庫建立儲存系統連線和憑證	262
備份 SAP HANA 資料庫	264
備份資源組	270
監控 SAP HANA 資料庫備份作業	271
取消 SAP HANA 的備份作業	272
在拓樸頁面中查看 SAP HANA 資料庫備份和克隆	273
還原 SAP HANA 資料庫	274
復原工作流程	274

還原並還原手動新增的資源備份	275
還原和還原自動發現的資料庫備份	279
使用 PowerShell cmdlet 還原資源	283
監控 SAP HANA 資料庫復原操作	285
克隆 SAP HANA 資源備份	286
克隆工作流程	286
克隆 SAP HANA 資料庫備份	287
監控 SAP HANA 資料庫克隆操作	290
分裂克隆	291
升級SnapCenter後刪除或分割 SAP HANA 資料庫克隆	292
保護 Oracle 資料庫	294
Oracle 資料庫的SnapCenter插件概述	294
您可以使用 Oracle 資料庫插件做什麼	294
Oracle 資料庫插件的功能	294
Oracle Database 外掛程式支援的儲存類型	296
為 Oracle 插件準備SnapMirror和SnapVault複製的儲存系統	298
Oracle 插件所需的最低ONTAP權限	298
為 Oracle 資料庫安裝SnapCenter插件	301
Oracle 資料庫的SnapCenter插件安裝工作流程	301
新增主機並安裝 Linux 或 AIX 插件包的先決條件	301
使用 GUI 新增主機並安裝 Linux 或 AIX 插件包	309
安裝 Linux 或 AIX 插件包的其他方法	313
配置SnapCenter插件Loader服務	315
在 Linux 主機上使用SnapCenter插件Loader(SPL) 服務設定 CA 證書	318
為插件啟用 CA 憑證	320
將資料從SnapManager for Oracle 和SnapManager for SAP 匯入到SnapCenter	321
SnapCenter Plug-in for VMware vSphere	326
部署 CA 憑證	326
配置 CRL 文件	326
準備保護 Oracle 資料庫	326
備份 Oracle 資料庫	328
備份過程概述	328
備份配置訊息	329
備份 Oracle 資料庫的要求	340
發現可供備份的 Oracle 資料庫	340
為 Oracle 資料庫建立備份策略	342
為 Oracle 資料庫建立資源組並附加策略	347
在ASA r2 系統上建立資源組並啟用 Oracle 資源的二級保護	349
備份 Oracle 資源	351
備份 Oracle 資料庫資源組	354
監控 Oracle 資料庫備份	355

其他備份操作	356
掛載和卸載資料庫備份	360
裝載資料庫備份	360
卸載資料庫備份	361
還原和還原 Oracle 資料庫	361
復原工作流程	362
定義 Oracle 資料庫的還原與復原策略	362
用於恢復特定處方和後記的預定義環境變量	366
恢復 Oracle 資料庫的要求	367
還原和還原 Oracle 資料庫	368
使用時間點復原來還原和還原表空間	372
使用時間點復原來恢復可插拔資料庫	374
使用 UNIX 指令還原和還原 Oracle 資料庫	376
監視 Oracle 資料庫還原作業	376
取消 Oracle 資料庫還原作業	377
克隆 Oracle 資料庫	378
克隆工作流程	378
定義 Oracle 資料庫的克隆策略	378
克隆特定處方和後記的預定義環境變量	379
克隆 Oracle 資料庫的要求	381
克隆 Oracle 資料庫備份	383
克隆可插入資料庫	390
使用 UNIX 指令克隆 Oracle 資料庫備份	393
拆分 Oracle 資料庫克隆	394
可插拔資料庫的拆分克隆	395
監視 Oracle 資料庫克隆操作	395
刷新克隆	396
刪除可插入資料庫的克隆	397
管理應用程式捲	397
什麼是應用卷	398
新增應用程式捲	398
備份應用程式捲	399
克隆應用程式捲備份	401
保護 Windows 檔案系統	404
適用於 Microsoft Windows 的SnapCenter外掛概念	404
適用於 Microsoft Windows 的SnapCenter外掛程式概述	404
您可以使用適用於 Microsoft Windows 的SnapCenter外掛程式做什麼	404
適用於 Windows 的SnapCenter插件功能	404
SnapCenter如何備份 Windows 檔案系統	405
SnapCenter Plug-in for Microsoft Windows 支援的儲存類型	406
Windows 插件所需的最低ONTAP權限	407

為SnapMirror和SnapVault複製準備儲存系統	410
定義 Windows 檔案系統的備份策略	410
Windows 檔案系統複製的來源和目標	412
安裝適用於 Microsoft Windows 的SnapCenter插件	412
適用於 Microsoft Windows 的SnapCenter外掛程式的安裝工作流程	412
適用於 Microsoft Windows 的SnapCenter外掛程式的安裝需求	412
新增主機並安裝適用於 Microsoft Windows 的SnapCenter插件	416
使用 PowerShell cmdlet 在多個遠端主機上安裝適用於 Microsoft Windows 的SnapCenter插件	419
從命令列靜默安裝適用於 Microsoft Windows 的SnapCenter插件	420
監控SnapCenter插件包安裝狀態	421
設定CA憑證	422
SnapCenter Plug-in for VMware vSphere	425
部署 CA 憑證	425
配置 CRL 文件	425
備份 Windows 檔案系統	425
備份 Windows 檔案系統	425
確定 Windows 檔案系統的資源可用性	427
為 Windows 檔案系統建立備份策略	427
為 Windows 檔案系統建立資源組	430
在ASA r2 系統上建立資源組並為 Windows 檔案系統啟用二級保護	432
使用 PowerShell cmdlet 建立儲存系統連線和憑證	434
按需備份 Windows 檔案系統的單一資源	435
備份 Windows 檔案系統的資源組	439
監視備份作業	440
取消備份作業	441
在拓撲頁面中查看相關備份和克隆	441
使用 PowerShell cmdlet 清理輔助備援計數	443
還原 Windows 檔案系統	444
恢復 Windows 檔案系統備份	444
使用 PowerShell cmdlet 還原資源	447
監視恢復操作	450
取消恢復操作	451
克隆 Windows 檔案系統	452
從 Windows 檔案系統備份克隆	452
監視克隆操作	457
取消克隆操作	458
分裂克隆	458
保護 Microsoft Exchange Server 資料庫	460
適用於 Microsoft Exchange Server 的SnapCenter外掛程式概念	460
適用於 Microsoft Exchange Server 的SnapCenter外掛程式概述	460
SnapCenter外掛程式 for Microsoft Exchange Server 的功能	460

SnapCenter外掛程式（適用於 Microsoft Windows 和 Microsoft Exchange Server）支援的儲存類型	461
Exchange 插件所需的最低ONTAP權限	462
為SnapMirror和SnapVault複製準備儲存系統	464
定義 Exchange Server 資源的備份策略	465
定義 Exchange 資料庫的還原策略	467
為 Microsoft Exchange Server 安裝SnapCenter插件	468
適用於 Microsoft Exchange Server 的SnapCenter插件的安裝工作流程	468
新增主機並安裝適用於 Microsoft Exchange Server 的SnapCenter外掛程式的先決條件	469
為 Windows 版SnapCenter插件設定憑證	472
在 Windows Server 2016 或更高版本上設定 gMSA	473
新增主機並安裝 Exchange 插件	475
使用 PowerShell cmdlet 從SnapCenter伺服器主機安裝 Exchange 插件	479
從命令列靜默安裝適用於 Exchange 的SnapCenter插件	480
監控SnapCenter插件包安裝狀態	481
設定 CA 憑證	482
配置SnapManager 7.x 以使 Exchange 和SnapCenter共存	485
SnapCenter Plug-in for VMware vSphere	486
部署 CA 憑證	486
配置 CRL 文件	487
做好資料保護準備	487
使用適用於 Microsoft Exchange Server 的SnapCenter外掛程式的先決條件	487
如何使用資源、資源群組和原則來保護 Exchange Server	488
備份 Exchange 資源	488
備份工作流	488
Exchange 資料庫和備份驗證	489
確定 Exchange 資源是否可用於備份	489
為 Exchange Server 資料庫建立備份策略	491
為 Exchange 伺服器建立資源組並附加策略	496
使用 PowerShell cmdlet 為 Exchange Server 建立儲存系統連線和憑證	498
備份 Exchange 資料庫	499
備份 Exchange 資源組	504
監視備份作業	505
取消 Exchange 資料庫的備份作業	506
在拓樸頁面中查看 Exchange 備份	507
還原 Exchange 資源	508
復原工作流程	508
還原 Exchange 資料庫的要求	509
還原 Exchange 資料庫	509
郵件和郵箱的粒度恢復	514
從輔助儲存還原 Exchange Server 資料庫	514
重新植入被動 Exchange 節點副本	514

使用 PowerShell cmdlet 為 Exchange 資料庫重新設定副本	515
監視恢復操作	516
取消 Exchange 資料庫的還原操作	517
保護 IBM Db2	518
適用於 IBM Db2 的 SnapCenter 插件	518
適用於 IBM Db2 的 SnapCenter 插件概述	518
使用適用於 IBM Db2 的 SnapCenter 插件可以做什麼	518
適用於 IBM Db2 的 SnapCenter 插件功能	518
SnapCenter Plug-in for IBM Db2 支援的儲存類型	519
IBM Db2 外掛程式所需的最低 ONTAP 權限	520
為 IBM Db2 的 SnapMirror 和 SnapVault 複製準備儲存系統	523
IBM Db2 的備份策略	523
IBM Db2 的還原與復原策略	525
準備安裝適用於 IBM Db2 的 SnapCenter 插件	526
SnapCenter Plug-in for IBM Db2 的安裝工作流程	526
新增主機並安裝 Windows、Linux 或 AIX 插件包的先決條件	527
安裝適用於 Windows 的 SnapCenter 插件包的主機需求	532
安裝適用於 Linux 的 SnapCenter 插件包的主機需求	533
為 IBM Db2 的 SnapCenter 插件設定憑證	534
在 Windows Server 2016 或更高版本上設定 gMSA	536
安裝適用於 IBM Db2 的 SnapCenter 插件	537
設定 CA 憑證	542
做好資料保護準備	549
使用適用於 IBM Db2 的 SnapCenter 插件的先決條件	549
如何使用資源、資源群組和政策來保護 IBM Db2	550
備份 IBM Db2 資源	550
備份 IBM Db2 資源	550
自動發現資料庫	552
手動將資源新增至插件主機	552
為 IBM Db2 建立備份策略	553
建立資源組並附加策略	555
在 ASA r2 系統上建立資源組並為 IBM Db2 資源啟用二級保護	558
使用 PowerShell cmdlet 為 IBM Db2 建立儲存系統連線和憑證	561
備份 Db2 資料庫	562
備份資源組	568
監控 IBM Db2 備份作業	569
取消 IBM Db2 的備份作業	570
在拓樸頁面中查看 IBM Db2 備份和克隆	571
還原 IBM Db2	572
復原工作流程	572
還原手動新增的資源備份	573

還原和還原自動發現的資料庫備份	577
監控 IBM Db2 恢復操作	578
克隆 IBM Db2 資源備份	579
克隆工作流程	579
克隆 IBM Db2 備份	580
監控 IBM Db2 克隆操作	586
分裂克隆	587
升級SnapCenter後刪除或拆分 IBM Db2 資料庫克隆	588
保護 PostgreSQL	589
適用於 PostgreSQL 的SnapCenter插件	589
SnapCenter PostgreSQL 插件概述	589
使用適用於 PostgreSQL 的SnapCenter插件可以做些什麼	589
適用於 PostgreSQL 的SnapCenter插件功能	589
SnapCenter Plug-in for PostgreSQL 支援的儲存類型	590
PostgreSQL 插件所需的最低ONTAP權限	591
為 PostgreSQL 的SnapMirror和SnapVault複製準備儲存系統	594
PostgreSQL 的備份策略	594
PostgreSQL 的還原與復原策略	596
準備安裝適用於 PostgreSQL 的SnapCenter插件	598
SnapCenter Plug-in for PostgreSQL 的安裝工作流程	598
新增主機並安裝 PostgreSQL 的SnapCenter插件的先決條件	598
安裝適用於 Windows 的SnapCenter插件包的主機需求	601
安裝適用於 Linux 的SnapCenter插件包的主機需求	602
為 PostgreSQL 的SnapCenter插件設定憑證	603
在 Windows Server 2016 或更高版本上設定 gMSA	604
安裝適用於 PostgreSQL 的SnapCenter插件	606
設定 CA 憑證	611
做好資料保護準備	618
使用適用於 PostgreSQL 的SnapCenter插件的先決條件	618
如何使用資源、資源群組和策略來保護 PostgreSQL	618
備份 PostgreSQL 資源	619
備份 PostgreSQL 資源	619
自動發現集群	621
手動將資源新增至插件主機	621
為 PostgreSQL 建立備份策略	622
建立資源組並附加策略	625
在ASA r2 系統上建立資源組並為 PostgreSQL 資源啟用二級保護	629
使用 PowerShell cmdlet 為 PostgreSQL 建立儲存系統連線和憑證	631
備份 PostgreSQL	632
備份資源組	638
監控 PostgreSQL 備份操作	638

取消 PostgreSQL 的備份操作	639
在拓模頁面中查看 PostgreSQL 備份和克隆	640
還原 PostgreSQL	641
復原工作流程	641
還原並還原手動新增的資源備份	642
還原和還原自動發現的叢集備份	646
使用 PowerShell cmdlet 還原資源	648
監控 PostgreSQL 復原操作	651
複製 PostgreSQL 資源備份	652
克隆工作流程	652
複製 PostgreSQL 備份	653
監控 PostgreSQL 克隆操作	656
分裂克隆	657
升級SnapCenter後刪除或分割 PostgreSQL 叢集克隆	658
保護 MySQL	659
適用於 MySQL 的SnapCenter插件	659
適用於 MySQL 的SnapCenter插件概述	659
使用適用於 MySQL 的SnapCenter插件可以做什麼	659
適用於 MySQL 的SnapCenter插件功能	659
SnapCenter Plug-in for MySQL 支援的儲存類型	660
MySQL 插件所需的最低ONTAP權限	661
為 MySQL 的SnapMirror和SnapVault複製準備儲存系統	664
MySQL 的備份策略	664
MySQL 的還原與復原策略	666
準備安裝適用於 MySQL 的SnapCenter插件	667
SnapCenter Plug-in for MySQL 的安裝工作流程	667
新增主機並安裝 MySQL 的SnapCenter插件的先決條件	668
安裝適用於 Windows 的SnapCenter插件包的主機需求	671
安裝適用於 Linux 的SnapCenter插件包的主機需求	672
為 MySQL 的SnapCenter插件設定憑證	673
安裝適用於 MySQL 的SnapCenter插件	675
設定 CA 憑證	679
做好資料保護準備	686
使用適用於 MySQL 的SnapCenter插件的先決條件	686
如何使用資源、資源群組和策略來保護 MySQL	687
備份 MySQL 資源	687
備份 MySQL 資源	687
自動發現資料庫	689
手動將資源新增至插件主機	689
為 MySQL 建立備份策略	690
建立資源組並附加策略	693

在ASA r2 系統上建立資源組並啟用 MySQL 資源的二級保護	697
使用 PowerShell cmdlet 為 MySQL 建立儲存系統連線和憑證	699
備份 MySQL	700
備份資源組	706
監控 MySQL 備份作業	706
取消 MySQL 的備份操作	707
在拓樸頁面中查看 MySQL 備份和克隆	708
復原 MySQL	709
復原工作流程	709
還原並還原手動新增的資源備份	710
還原和還原自動發現的資料庫備份	714
使用 PowerShell cmdlet 還原資源	716
監控 MySQL 復原操作	718
克隆 MySQL 資源備份	719
克隆工作流程	719
克隆 MySQL 備份	720
監控 MySQL 複製操作	723
分裂克隆	724
升級SnapCenter後刪除或分割 MySQL 資料庫克隆	725
使用NetApp支援的插件保護應用程式	726
NetApp支援的插件	726
NetApp支援的插件概述	726
NetApp支援的插件可以做什麼	726
NetApp支援的插件功能	727
NetApp支援的插件支援的儲存類型	728
NetApp支援的插件所需的最低ONTAP權限	728
為NetApp支援的插件準備SnapMirror和SnapVault複製的儲存系統	730
定義備份策略	731
NetApp支援的插件的備份策略	731
手動新增的NetApp支援的插件資源支援的復原策略類型	732
準備安裝NetApp支援的插件	732
SnapCenter NetApp支援的插件的安裝工作流程	733
新增主機並安裝 Windows、Linux 或 AIX 插件包的先決條件	733
安裝適用於 Windows 的SnapCenter插件包的主機需求	737
安裝適用於 Linux 和 AIX 的SnapCenter插件包的主機需求	738
為NetApp支援的插件設定憑證	739
在 Windows Server 2016 或更高版本上設定 gMSA	740
安裝NetApp支援的插件	742
設定 CA 憑證	747
做好資料保護準備	755
使用NetApp支援的插件的先決條件	755

如何使用資源、資源群組和策略來保護NetApp支援的插件資源	755
備份NetApp支援的插件資源	756
備份NetApp支援的插件資源	756
為NetApp支援的插件新增資源	756
為NetApp支援的插件資源建立策略	760
建立資源組並附加策略	763
建立資源組並為ASA r2 系統上的資源啟用二級保護	766
使用 PowerShell cmdlet 建立儲存系統連線和憑證	769
備份單一NetApp支援的插件資源	770
備份NetApp支援的插件資源的資源組	775
監控NetApp支援的插件資源備份操作	775
取消NetApp支援的外掛程式的備份操作	776
在拓撲頁面中查看NetApp支援的插件資源相關的備份和克隆	777
恢復NetApp支援的插件資源	778
恢復NetApp支援的插件資源	778
恢復資源備份	779
監控NetApp支援的插件資源復原操作	783
克隆NetApp支援的外掛資源備份	784
克隆NetApp支援的外掛資源備份	784
從備份克隆	785
監控NetApp支援的插件資源克隆操作	790
保護 Unix 檔案系統	792
您可以使用適用於 Unix 檔案系統的SnapCenter插件做什麼	792
支援的配置	792
限制	793
特徵	793
為 Unix 檔案系統安裝SnapCenter插件	793
新增主機並安裝 Linux 插件包的先決條件	793
使用 GUI 新增主機並安裝 Linux 插件包	794
配置SnapCenter插件Loader服務	797
在 Linux 主機上使用SnapCenter插件Loader(SPL) 服務設定 CA 證書	799
為插件啟用 CA 憑證	802
SnapCenter Plug-in for VMware vSphere	802
部署 CA 憑證	803
配置 CRL 文件	803
準備保護 Unix 檔案系統	803
備份 Unix 檔案系統	803
發現可用於備份的 UNIX 檔案系統	803
為 Unix 檔案系統建立備份策略	804
為 Unix 檔案系統建立資源組並附加策略	806
在ASA r2 系統上建立資源組並為 Unix 檔案系統啟用二級保護	808

備份 Unix 檔案系統	810
備份 Unix 檔案系統資源組	811
監控 Unix 檔案系統備份	812
在拓樸頁面中查看受保護的 Unix 檔案系統	813
還原和恢復 Unix 檔案系統	815
恢復 Unix 檔案系統	815
監控 Unix 檔案系統恢復操作	816
克隆 Unix 檔案系統	817
克隆 Unix 檔案系統備份	817
分裂克隆	818
監控 Unix 檔案系統克隆操作	819
保護在 Azure NetApp Files 上運行的應用程式	821
保護在 Azure NetApp Files 上運行的應用程式	821
限制	821
安裝 SnapCenter 並建立憑證	821
在 Azure 虛擬機器上安裝 SnapCenter	821
在 SnapCenter 中建立 Azure 憑證	822
配置 Azure 儲存體帳戶	823
建立憑證以新增插件主機	824
保護 SAP HANA 資料庫	824
為 SAP HANA 資料庫新增主機並安裝 SnapCenter 插件	824
新增 SAP HANA 資料庫	825
為 SAP HANA 資料庫建立備份策略	826
建立資源組並附加 SAP HANA 備份策略	826
備份在 Azure NetApp Files 上執行的 SAP HANA 資料庫	827
備份 SAP HANA 資源組	828
還原和還原 SAP HANA 資料庫	828
克隆 SAP HANA 資料庫備份	829
保護 Microsoft SQL Server 資料庫	830
新增主機並為 SQL Server 資料庫安裝 SnapCenter 插件	830
為 SQL Server 資料庫建立備份策略	831
建立資源組並附加 SQL 備份策略	832
備份在 Azure NetApp Files 上執行的 SQL Server 資料庫	833
備份 SQL Server 資源組	834
還原和還原 SQL Server 資料庫	834
克隆 SQL Server 資料庫備份	835
保護 Oracle 資料庫	837
新增主機並為 Oracle 資料庫安裝 SnapCenter 插件	837
為 Oracle 資料庫建立備份策略	837
建立資源組並附加 Oracle 備份策略	838
備份在 Azure NetApp Files 上執行的 Oracle 資料庫	839

備份 Oracle 資源組	840
還原和還原 Oracle 資料庫	840
克隆 Oracle 資料庫備份	843
管理SnapCenter伺服器 and 插件	845
查看儀表板	845
儀表板概覽	845
如何查看儀表板上的信息	848
從儀表板請求作業的狀態報告	848
從儀表板請求保護狀態報告	849
管理 RBAC	849
修改角色	849
修改使用者和群組	850
管理主機	850
刷新虛擬機器資訊	852
修改插件主機	852
啟動或重新啟動插件服務	853
暫停主機維護計劃	853
資源頁面支援的操作	854
管理政策	854
修改策略	855
分離策略	855
刪除策略	856
管理資源組	856
停止和恢復資源組的操作	856
刪除資源組	857
管理備份	857
重新命名備份	857
刪除備份	858
移除保護	858
刪除克隆	859
監控作業、計畫、事件和日誌	860
監控作業	860
監控時間表	861
監視事件	861
監控日誌	861
從SnapCenter中刪除作業和日誌	862
SnapCenter報告功能概述	863
訪問報告	864
過濾報告	864
匯出或列印報告	865
設定電子郵件通知的 SMTP 伺服器	865

配置透過電子郵件傳送報告的選項	865
管理SnapCenter伺服器儲存庫	866
保護SnapCenter儲存庫的先決條件	866
備份SnapCenter儲存庫	866
查看SnapCenter儲存庫的備份	866
還原SnapCenter資料庫儲存庫	867
遷移SnapCenter儲存庫	867
重置SnapCenter儲存庫密碼	868
管理不受信任域的資源	868
修改不受信任的網域	869
取消註冊不受信任的 Active Directory 網域	869
管理儲存系統	870
修改儲存系統配置	870
刪除儲存系統	871
REST API 支援	872
管理 EMS 資料收集	873
停止 EMS 資料收集	873
開始 EMS 資料收集	873
更改 EMS 資料收集計劃和目標 SVM	873
監控EMS資料收集狀態	873
升級SnapCenter伺服器和插件	875
配置SnapCenter以檢查可用更新	875
升級工作流程	875
支援的升級路徑	875
升級 Windows 主機上的SnapCenter伺服器	876
升級 Linux 主機上的SnapCenter伺服器	878
升級你的插件包	878
技術更新	881
SnapCenter Server 主機的技術更新	881
F5 叢集中節點的技術更新	882
停用舊的SnapCenter Server 主機	882
回滾到舊的SnapCenter Server 主機	882
災難復原	882
SnapCenter插件主機的技術更新	883
儲存系統技術更新	886
更新主儲存的備份	886
更新輔助儲存的備份	888
解除安裝SnapCenter伺服器和插件	889
卸載SnapCenter插件包	889
刪除主機的先決條件	889
刪除主機	890

使用SnapCenter GUI 卸載插件	890
使用 PowerShell cmdlet 解除安裝 Windows 插件	891
在主機本地卸載插件	891
使用 CLI 卸載 Linux 或 AIX 的插件包	892
在 Windows 主機上解除安裝SnapCenter伺服器	892
在 Linux 主機上解除安裝SnapCenter伺服器	893
使用 REST API 實現自動化	894
使用 REST API 實現SnapCenter自動化	894
如何在本機存取SnapCenter REST API	894
REST Web 服務基礎	894
資源和國家代表	894
URI 端點	894
HTTP 郵件	895
JSON 格式	895
基本運作特性	895
請求和回應 API 事務	895
支援 CRUD 操作	895
物件標識符	895
物件實例和集合	896
同步和非同步操作	896
安全	896
控制 API 請求的輸入變數	896
HTTP 方法	896
請求標頭	897
請求正文	897
篩選對象	897
請求特定物件字段	898
對輸出集中的物件進行排序	898
檢索集中的物件時進行分頁	899
尺寸屬性	899
API 回應的解釋	900
HTTP 狀態碼	900
響應標頭	900
回應正文	900
錯誤	901
SnapCenter伺服器和插件支援的 REST API	902
授權	902
域	902
工作	902
設定	902
主機	902

資源	903
備份	905
複製	905
克隆分裂	905
資源組	906
政策	906
儲存	906
分享	907
外掛	907
報告	908
警報	908
RBAC	908
配置	909
證書設定	909
儲存庫	909
版本	909
如何使用 Swagger API 網頁存取 REST API	909
開始使用 REST API	910
你好世界	910
法律聲明	911
版權	911
商標	911
專利	911
隱私權政策	911
開源	911

SnapCenter software 文檔

發行說明

發行說明

了解SnapCenter 6.1 中的新功能和增強功能。

有關新功能和增強功能的完整列表，請參閱["SnapCenter 6.1 中的新增功能"](#)。

有關已知問題、限制、已修復問題以及新命令和更改命令的詳細信息，請參閱 ["SnapCenter軟體 6.1 發行說明"](#)。您必須使用您的NetApp帳戶登入或建立帳戶才能存取發行說明。

SnapCenter支援的升級路徑

升級路徑可協助您了解可以從哪些早期版本的SnapCenter升級至最新版本的SnapCenter以及支援哪些版本的外掛程式。

如果您使用的是 SnapCenter Server 版本...	您可以直接將 SnapCenter Server 升級到...	支援的插件版本
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

有關升級適用SnapCenter Plug-in for VMware vSphere的信息，請參閱 ["升級SnapCenter Plug-in for VMware vSphere"](#)。

開始

了解SnapCenter software

SnapCenter概述

SnapCenter software是一個簡單、集中且可擴展的平台，用於應用程式一致的資料保護。它保護混合雲中ONTAP系統上的應用程式、資料庫、主機檔案系統和虛擬機器。

SnapCenter使用NetApp Snapshot、SnapRestore、FlexClone、SnapMirror和SnapVault技術提供：

- 快速、節省空間、應用程式一致、基於磁碟的備份
- 快速、詳細的恢復和應用程式一致的恢復
- 快速、節省空間的克隆

SnapCenter包括SnapCenter伺服器 and 輕量級插件。您可以自動將外掛程式部署到遠端應用程式主機，安排備份、驗證和複製操作，並監控資料保護操作。

您可以在本機或公有雲上安裝SnapCenter來保護資料。

- 在地保護以下內容：
 - 位於ONTAP FAS、AFF或ASA主系統上並複製到ONTAP FAS、AFF或ASA輔助系統的數據
 - ONTAP Select主系統上的數據
 - 位於ONTAP FAS、AFF或ASA主系統和輔助系統上並受本地StorageGRID物件儲存保護的數據
 - ONTAP ASA r2 主系統和輔助系統上的數據
- 在混合雲中本地保護以下內容：
 - 位於ONTAP FAS、AFF或ASA主系統上並複製到Cloud Volumes ONTAP 的數據
 - 位於ONTAP FAS、AFF或ASA主系統和輔助系統上並受雲端中的物件和歸檔儲存保護的資料（使用BlueXP backup and recovery整合）
- 在公有雲中保護以下內容：
 - Cloud Volumes ONTAP （以前稱為ONTAP Cloud）主系統上的數據
 - Amazon FSX for ONTAP上的數據
 - 主Azure NetApp Files（Oracle、Microsoft SQL 和 SAP HANA）上的數據

主要特點

SnapCenter提供以下主要功能：

- 不同應用程式的集中式、應用程式一致的資料保護

支援在ONTAP系統上執行的 Microsoft Exchange Server、Microsoft SQL Server、Linux 或 AIX 上的 Oracle 資料庫、SAP HANA 資料庫、IBM Db2、PostgreSQL、MySQL 和 Windows 主機檔案系統的資料保護。SnapCenter也支援 MongoDB、Storage、MaxDB、Sybase ASE、ORASCPM 等應用程式的保護。

- 基於策略的備份

基於策略的備份利用NetApp Snapshot 技術來創建快速、節省空間、應用程式一致的基於磁碟的備份。您也可以透過更新現有的保護關係來設定這些備份到二級儲存的自動保護。

- 多種資源的備份

您可以使用SnapCenter資源組一次備份相同類型的多個資源（應用程式、資料庫或主機檔案系統）。

- 還原和復原

SnapCenter提供快速、細粒度的備份還原以及應用程式一致的基於時間的復原。您可以從混合雲中的任何目的地進行恢復。

- 複製

SnapCenter提供快速、節省空間且應用程式一致的克隆。您可以在混合雲中的任何目的地進行複製。

- 單一使用者管理圖形使用者介面

SnapCenter提供單一介面來管理任何混合雲目標中的備份和複製。

- REST API、Windows cmdlet、UNIX 指令

SnapCenter為大多數功能提供了 REST API，以便與任何編排軟體集成，並使用 Windows PowerShell cmdlet 和命令列介面。

- 集中式資料保護儀表板和報告

- 基於角色的存取控制（RBAC）用於安全和授權

- 具有高可用性的內建儲存庫資料庫，用於儲存所有備份元數據

- 自動推送安裝插件

- 高可用性

- 災難復原 (DR)

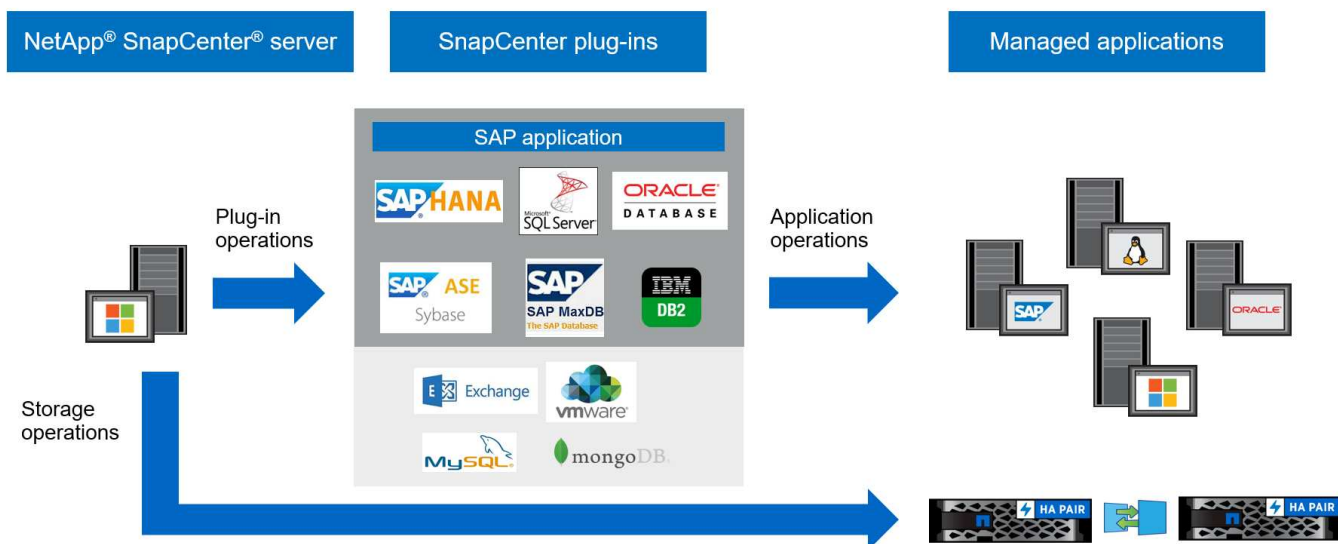
- SnapLock ["了解更多"](#)

- SnapMirror主動同步（最初以SnapMirror業務連續性 [SM-BC] 發行）

- 同步鏡像 ["了解更多"](#)

SnapCenter架構和元件

SnapCenter採用分層設計，包含中央管理伺服器 and 插件主機。伺服器和插件主機可以位於不同的位置。



SnapCenter包含SnapCenter伺服器、適用於 Windows 的SnapCenter插件套件、適用於 Linux 的SnapCenter插件套件。每個包都包含各種應用程式和基礎設施組件的插件。

SnapCenter伺服器

SnapCenter伺服器支援 Microsoft Windows 和 Linux（RHEL 8.x、RHEL 9.x、SLES 15 SP5）作業系統。SnapCenter伺服器包含一個 Web 伺服器、一個基於 HTML5 的集中式使用者介面、PowerShell cmdlet、REST API 和 SnapCenter 儲存庫。

SnapCenter將其操作的相關資訊儲存在 SnapCenter 儲存庫中。

SnapCenter插件

每個 SnapCenter 插件都支援特定的環境、資料庫和應用程式。

插件名稱	包含在安裝包中	需要其他插件	安裝在主機上	支援的平台
適用於 Microsoft SQL Server 的 SnapCenter 插件	Windows 插件包	Windows 外掛	SQL Server 主機	視窗
適用於 Windows 的 SnapCenter 插件	Windows 插件包		Windows 主機	視窗
適用於 Microsoft Exchange Server 的 SnapCenter 插件	Windows 插件包	Windows 外掛	Exchange Server 主機	視窗
適用於 Oracle 資料庫的 SnapCenter 插件	Linux 插件包和 AIX 插件包	UNIX 插件	Oracle 主機	Linux 或 AIX

插件名稱	包含在安裝包中	需要其他插件	安裝在主機上	支援的平台
適用於 SAP HANA 資料庫的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	HDBSQL 用戶端主機	Linux 或 Windows
適用於 IBM Db2 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	Db2 主機	Linux、AIX 或 Windows
適用於 PostgreSQL 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	PostgreSQL 主機	Linux 或 Windows
MySQL 的 SnapCenter 插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	MySQL 主機	Linux 或 Windows
MongoDB 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	MongoDB 主機	Linux 或 Windows
適用於 ORASCPM (Oracle 應用程式) 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	Oracle 主機	Linux 或 Windows
適用於 SAP ASE 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	SAP主機	Linux 或 Windows
適用於 SAP MaxDB 的SnapCenter插件	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	SAP MaxDB 主機	Linux 或 Windows
SnapCenter插件 (用於儲存插件)	Linux 插件包和 Windows 插件包	UNIX 插件或 Windows 插件	儲存主機	Linux 或 Windows

SnapCenter Plug-in for VMware vSphere支援虛擬機器 (VM)、資料儲存庫和虛擬機器磁碟 (VMDK) 的崩潰一致性和 VM 一致性備份和還原作業。它還支援虛擬化資料庫和檔案系統的應用程式一致的備份和復原作業。

若要保護資料庫、檔案系統、虛擬機器或虛擬機器上的資料儲存區，請部署SnapCenter Plug-in for VMware vSphere。欲了解詳細信息，請參閱 "[SnapCenter Plug-in for VMware vSphere文檔](#)"。

SnapCenter儲存庫

SnapCenter儲存庫（有時稱為 NSM 資料庫）儲存每個SnapCenter操作的資訊和元資料。

SnapCenter Server 安裝預設安裝 MySQL Server 儲存庫資料庫。如果您已經安裝了 MySQL Server 並且想要執行SnapCenter Server 的全新安裝，則必須解除安裝 MySQL Server。

SnapCenter支援 MySQL Server 8.0.37 或更高版本作為SnapCenter儲存庫資料庫。如果您將早期版本的 MySQL Server 與早期版本的SnapCenter一起使用，則SnapCenter升級程序會將 MySQL Server 升級至版本 8.0.37 或更高版本。

SnapCenter儲存庫儲存以下資訊和元資料：

- 備份、克隆、還原和驗證元數據
- 報告、工作和事件訊息
- 主機和插件資訊
- 角色、使用者和權限詳細信息
- 儲存系統連接資訊

SnapCenter中的安全功能

SnapCenter採用嚴格的安全性和身份驗證功能，確保您的資料安全。

SnapCenter包含以下安全功能：

- 與SnapCenter的所有通訊都使用 HTTP over SSL (HTTPS)。
- SnapCenter中的所有憑證均使用高級加密標準 (AES) 加密進行保護。
- 支援符合聯邦資訊處理標準 (FIPS) 的安全演算法。
- 支援使用客戶提供的授權CA憑證。
- 支援傳輸層安全性 (TLS) 1.3 以便與ONTAP進行通訊。您也可以使用 TLS 1.2 進行客戶端和伺服器之間的通訊。
- 支援一組特定的 SSL 密碼套件，以提供跨網路通訊的安全性。 ["了解更多"](#)。
- SnapCenter安裝在您公司的防火牆內，以啟用對SnapCenter伺服器的存取並啟用SnapCenter伺服器和插件之間的通訊。
- SnapCenter API 和操作存取使用 AES 加密的令牌，該令牌在 24 小時後過期。
- SnapCenter與 Windows Active Directory 集成，用於登入和基於角色的存取控制 (RBAC) 來管理存取權限。
- 適用於 Windows 和 Linux 主機的ONTAP上的SnapCenter支援 IPsec。 ["了解更多"](#)。
- SnapCenter PowerShell cmdlet 是會話安全性的。
- 預設 15 分鐘不活動時間後，SnapCenter會警告您將在 5 分鐘後被登出。

20 分鐘不活動後，SnapCenter會將您登出，您必須重新登入。您可以修改註銷期限。

- 5 次登入嘗試失敗後，登入將會暫時停用。
- 支援SnapCenter Server 和ONTAP之間的 CA 憑證認證。 ["了解更多"](#)。
- 完整性驗證器被添加到SnapCenter伺服器和插件中，並在全新安裝和升級作業期間驗證所有附帶的二進位檔案。

CA憑證概述

SnapCenter Server 安裝程式在安裝期間啟用集中式 SSL 憑證支援。為了增強伺服器和插件之間的安全通信，SnapCenter支援使用客戶提供的授權 CA 憑證。

安裝SnapCenter伺服器和對應的插件後，您應該部署 CA 憑證。有關更多信息，請參閱["產生CA憑證CSR文件"](#)。

您也可以為 VMware vSphere 的SnapCenter外掛程式部署 CA 憑證。有關更多信息，請參閱 ["建立並匯入證書"](#)

。

雙向 SSL 通信

雙向 SSL 通訊確保SnapCenter伺服器 and 插件之間的相互通訊安全性。

基於憑證的身份驗證概述

基於憑證的身份驗證可驗證嘗試存取SnapCenter插件主機的各個使用者的真實性。使用者應匯出不帶私鑰的SnapCenter伺服器憑證並將其匯入插件主機受信任儲存區。僅當啟用雙向 SSL 功能時，基於憑證的驗證才有效。

多重身份驗證 (MFA)

MFA 透過安全性斷言標記語言 (SAML) 使用第三方身分提供者 (IdP) 來管理使用者會話。此功能透過選擇使用多種因素（例如 TOTP、生物識別、推播通知等）以及現有的使用者名稱和密碼來增強身分驗證的安全性。此外，它還使客戶能夠使用自己的使用者身分提供者在其產品組合中獲得統一的使用者登入 (SSO)。

MFA 僅適用於SnapCenter Server UI 登入。登入透過 IdP Active Directory 聯合驗證服務 (AD FS) 進行驗證。您可以在 AD FS 配置各種身份驗證因素。SnapCenter是服務供應商，您應該將SnapCenter配置為 AD FS 中的依賴方。要在SnapCenter中啟用 MFA，您將需要 AD FS 元資料。

有關啟用 MFA 的信息，請參閱["啟用多重身份驗證"](#)。

SnapCenter中基於角色的存取控制

SnapCenter基於角色的存取控制 (RBAC) 和ONTAP權限使SnapCenter管理員能夠將SnapCenter資源的控制權委託給不同的使用者或使用者群組。這種集中管理的存取使應用程式管理員能夠在委派的环境中安全地工作。

您可以隨時建立和修改角色，並為使用者新增資源存取權。但是，首次設定SnapCenter時，至少應將 Active Directory 使用者或群組新增至角色，然後在這些使用者或群組中新增資源存取權。



您不能使用SnapCenter建立使用者或群組帳戶。您應該在作業系統或資料庫的 Active Directory 中建立使用者或群組帳戶。

SnapCenter中的 RBAC 類型

SnapCenter使用以下類型的角色為基礎的存取控制：

- SnapCenter RBAC
- 應用程式等級 RBAC
- 適用於 VMware vSphere RBAC 的SnapCenter插件
- ONTAP 權限

SnapCenter RBAC

SnapCenter具有預先定義的角色，您可以將使用者或使用者群組指派給這些角色。預定義的角色是：

- SnapCenter管理員角色

- 應用程式備份和克隆管理員角色
- 備份和克隆檢視器角色
- 基礎設施管理員角色

當您為使用者指派角色時，除非您指派了 SnapCenterAdmin 角色，否則只有與該使用者相關的作業才會顯示在「作業」頁面中。

您還可以建立新角色並管理權限和使用者。您可以為使用者或群組指派權限以存取SnapCenter對象，例如主機、儲存連線和資源群組。

您可以將 RBAC 權限指派給同一林內的使用者和群組以及屬於不同林的使用者。您無法將 RBAC 權限指派給屬於跨林嵌套群組的使用者。



如果建立自訂角色，它必須包含 SnapCenterAdmin 角色的所有權限。如果您僅複製部分權限，例如新增主機或刪除主機，則無法執行這些操作。

使用者需要在登入時透過圖形使用者介面 (GUI) 或使用 PowerShell cmdlet 提供身份驗證。如果使用者是多個角色的成員，則在輸入登入憑證後，系統會提示他們指定要使用的角色。用戶還需要提供身份驗證才能運行 API。

應用程式等級 RBAC

SnapCenter使用憑證來驗證授權的SnapCenter使用者是否也具有應用程式層級權限。

例如，如果您想在 SQL Server 環境中執行資料保護操作，則必須使用正確的 Windows 或 SQL 憑證設定憑證。SnapCenter伺服器使用任一方法對設定的憑證進行驗證。如果要在ONTAP儲存上的 Windows 檔案系統環境中執行資料保護操作，SnapCenter管理員角色必須在 Windows 主機上具有管理員權限。

同樣，如果您想在 Oracle 資料庫上執行資料保護操作，並且如果資料庫主機中停用了作業系統 (OS) 驗證，則必須使用 Oracle 資料庫或 Oracle ASM 憑證設定憑證。SnapCenter伺服器根據操作使用其中一種方法對設定的憑證進行身份驗證。

SnapCenter Plug-in for VMware vSphere

如果您使用SnapCenter VMware 外掛程式進行虛擬機器一致的資料保護，則 vCenter Server 會提供額外等級的 RBAC。SnapCenter VMware 外掛程式支援 vCenter Server RBAC 和ONTAP RBAC。"[了解更多](#)"

最佳實務：NetApp建議您為SnapCenter Plug-in for VMware vSphere建立ONTAP角色，並為其指派所有必要的權限。

ONTAP 權限

您應該建立具有存取儲存系統所需權限的 vsadmin 帳戶。"[了解更多](#)"

分配給預定義SnapCenter角色的權限

將使用者新增至角色時，您必須指派 StorageConnection 權限以啟用儲存虛擬機器 (SVM) 通信，或為使用者指派 SVM 以啟用使用 SVM 的權限。儲存連線權限使用戶能夠建立 SVM 連線。

例如，具有SnapCenter管理員角色的用戶可以建立 SVM 連線並將其指派給具有應用程式備份和複製管理員角色的用戶，而該用戶預設情況下沒有建立或編輯 SVM 連線的權限。如果沒有 SVM 連接，使用者就無法完成任何備份、複製或復原作業。

SnapCenter管理員角色

SnapCenter管理員角色已啟用所有權限。您不能修改此角色的權限。您可以將使用者和群組新增至角色或將其刪除。

應用程式備份和克隆管理員角色

應用程式備份和複製管理員角色具有執行應用程式備份和複製相關任務的管理作業所需的權限。此角色沒有主機管理、設定、儲存連線管理或遠端安裝的權限。

權限	已啟用	創造	讀	更新	刪除
資源組	不適用	是的	是的	是的	是的
政策	不適用	是的	是的	是的	是的
備份	不適用	是的	是的	是的	是的
主持人	不適用	是的	是的	是的	是的
儲存連接	不適用	不	是的	不	不
複製	不適用	是的	是的	是的	是的
條款	不適用	不	是的	不	不
儀表板	是的	不適用	不適用	不適用	不適用
報告	是的	不適用	不適用	不適用	不適用
恢復	是的	不適用	不適用	不適用	不適用
資源	是的	是的	是的	是的	是的
插件安裝/解除安裝	不	不適用		不適用	不適用
遷移	不	不適用	不適用	不適用	不適用
山	是的	是的	不適用	不適用	不適用
解除安裝	是的	是的	不適用	不適用	不適用
全卷還原	不	不	不適用	不適用	不適用

權限	已啟用	創造	讀	更新	刪除
二級保護	不	不	不適用	不適用	不適用
作業監視器	是的	不適用	不適用	不適用	不適用

備份和克隆檢視器角色

備份和克隆查看者角色具有所有權限的唯讀檢視。此角色還具有發現、報告和存取儀表板的權限。

權限	已啟用	創造	讀	更新	刪除
資源組	不適用	不	是的	不	不
政策	不適用	不	是的	不	不
備份	不適用	不	是的	不	不
主持人	不適用	不	是的	不	不
儲存連接	不適用	不	是的	不	不
複製	不適用	不	是的	不	不
條款	不適用	不	是的	不	不
儀表板	是的	不適用	不適用	不適用	不適用
報告	是的	不適用	不適用	不適用	不適用
恢復	不	不	不適用	不適用	不適用
資源	不	不	是的	是的	不
插件安裝/解除安裝	不	不適用	不適用	不適用	不適用
遷移	不	不適用	不適用	不適用	不適用
山	是的	不適用	不適用	不適用	不適用
解除安裝	是的	不適用	不適用	不適用	不適用
全卷還原	不	不適用	不適用	不適用	不適用

權限	已啟用	創造	讀	更新	刪除
二級保護	不	不適用	不適用	不適用	不適用
作業監視器	是的	不適用	不適用	不適用	不適用

基礎設施管理員角色

基礎設施管理員角色具有主機管理、儲存管理、配置、資源群組、遠端安裝報告和儀表板存取的權限。

權限	已啟用	創造	讀	更新	刪除
資源組	不適用	是的	是的	是的	是的
政策	不適用	不	是的	是的	是的
備份	不適用	是的	是的	是的	是的
主持人	不適用	是的	是的	是的	是的
儲存連接	不適用	是的	是的	是的	是的
複製	不適用	不	是的	不	不
條款	不適用	是的	是的	是的	是的
儀表板	是的	不適用	不適用	不適用	不適用
報告	是的	不適用	不適用	不適用	不適用
恢復	是的	不適用	不適用	不適用	不適用
資源	是的	是的	是的	是的	是的
插件安裝/解除安裝	是的	不適用	不適用	不適用	不適用
遷移	不	不適用	不適用	不適用	不適用
山	不	不適用	不適用	不適用	不適用
解除安裝	不	不適用	不適用	不適用	不適用
全卷還原	不	不	不適用	不適用	不適用

權限	已啟用	創造	讀	更新	刪除
二級保護	不	不	不適用	不適用	不適用
作業監視器	是的	不適用	不適用	不適用	不適用

SnapCenter中的災難復原

SnapCenter災難復原 (DR) 功能可讓您從資源損壞或伺服器崩潰等災難中復原。它有助於恢復SnapCenter儲存庫、伺服器計劃、配置元件以及 SQL Server 的SnapCenter插件及其儲存。

本節介紹SnapCenter中的兩種 DR 類型：

SnapCenter伺服器災難復原

- SnapCenter Server 資料已備份，無需在SnapCenter Server 上新增或管理任何外掛程式即可復原。
- 輔助SnapCenter伺服器應安裝在與主SnapCenter伺服器相同的安裝目錄和連接埠上。
- 對於多重驗證 (MFA)，在SnapCenter Server DR 期間，關閉所有瀏覽器標籤並重新開啟瀏覽器以再次登入。這將清除現有或活動的會話 cookie 並更新正確的設定資料。
- SnapCenter災難復原功能使用 REST API 來備份SnapCenter伺服器。看["用於SnapCenter Server 災難復原的 REST API 工作流程"](#)。
- 審計設定相關的設定檔未在 DR 備份中備份，還原作業後也不會在 DR 伺服器上備份。您應該手動重複審計日誌設定。

SnapCenter插件與儲存災難復原

DR 僅適用於 SQL Server 的SnapCenter插件。如果外掛程式關閉，請切換到另一個 SQL 主機並按照以下步驟還原資料。看["SnapCenter插件 for SQL Server 的災難復原"](#)。

SnapCenter使用ONTAP SnapMirror複製數據，透過將數據同步到輔助站點，可以用於 DR。若要啟動故障轉移，請中斷SnapMirror複製。在回退期間，逆轉同步以將資料從 DR 站點複製回主位置。

SnapCenter所需的許可證

SnapCenter需要多個許可證才能實現應用程式、資料庫、檔案系統和虛擬機器的資料保護。您安裝的SnapCenter授權類型取決於您的儲存環境和您想要使用的功能。

執照	需要時
SnapCenter標準是基於控制器	FAS、AFF、ASA必需 SnapCenter標準許可證是基於控制器的許可證，是NetApp ONTAP One 的一部分。如果您擁有SnapManager Suite 許可證，您也可以獲得SnapCenter Standard 授權權利。如果您想使用FAS、AFF或ASA儲存試用安裝SnapCenter，您可以聯絡銷售代表以取得NetApp ONTAP One 評估許可證。 有關NetApp ONTAP One 附帶的許可證的信息，請參閱 "NetApp ONTAP One 隨附的許可證"。  SnapCenter也作為資料保護包的一部分提供。如果您購買了 A400 或更高版本，則應該購買資料保護包。
SnapMirror或SnapVault	ONTAP 如果在SnapCenter中啟用了複製，則需要SnapMirror或SnapVault授權。
SnapRestore	需要恢復和驗證備份。 在主儲存系統上 • 需要在SnapVault目標系統上執行遠端驗證並從備份中復原。 • 需要在SnapMirror目標系統上執行遠端驗證。
FlexClone	克隆資料庫和驗證操作所需。 在主儲存系統和輔助儲存系統上 • 需要在SnapVault目標系統上從二級保管庫備份建立複製。 • 需要在SnapMirror目標系統上從二級SnapMirror備份建立複製。

執照	需要時
協議許可證	• LUN 的 iSCSI 或 FC 許可證 • SMB 共享的 CIFS 許可證 • NFS 類型 VMDK 的 NFS 許可證 • VMFS 類型 VMDK 的 iSCSI 或 FC 許可證 如果來源磁碟區不可用，則需要在SnapMirror目標系統上提供資料。
SnapCenter標準許可證（可選）	次要目的地  建議（但不要求）將SnapCenter標準許可證新增至輔助目標。如果未在輔助目標上啟用SnapCenter標準許可證，則執行故障轉移作業後無法使用SnapCenter備份輔助目標上的資源。但是，在輔助目標上需要FlexClone許可證才能執行複製和驗證操作。
單一郵件匣復原 (SMBR) 許可證	如果您使用SnapCenter Plug-in for Exchange 來管理 Microsoft Exchange Server 資料庫和單一郵件匣復原 (SMBR)，則需要額外的 SMBR 許可證，該許可證需要根據使用者信箱單獨購買。 NetApp® 單一信箱復原已於 2023 年 5 月 12 日停止提供 (EOA)。有關詳細信息，請參閱"CPC-00507"。NetApp將在支援期限內繼續為已透過 2020 年 6 月 24 日推出的行銷零件號碼購買郵箱容量、維護和支援的客戶提供支援。 NetApp Single Mailbox Recovery 是 Ontrack 提供的合作夥伴產品。Ontrack PowerControls 提供的功能與NetApp Single Mailbox Recovery 類似。客戶可以從 Ontrack（透過 licenceteam@ontrack.com）購買新的 Ontrack PowerControls 軟體許可證以及 Ontrack PowerControls 維護和支援續約，以便在 2023 年 5 月 12 日 EOA 日期之後進行細粒度的郵箱恢復。



SnapCenter Advanced 和 SnapCenter NAS File Services 授權已棄用，不再可用。Amazon FSx for NetApp ONTAP、ONTAP Select、Cloud Volumes ONTAP 和 Azure NetApp Files 不再需要標準授權和基於容量的授權。

您應該安裝一個或多個 SnapCenter 授權。有關如何添加許可證的信息，請參閱["新增基於 SnapCenter Standard 控制器的許可證"](#)。

SnapCenter中的SnapMirror主動同步

SnapMirror主動同步使業務服務即使在整個站點發生故障時也能繼續運行，支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過SnapMirror主動同步觸發故障轉移。

有關SnapMirror主動同步的更多信息，請參閱 ["SnapMirror主動同步概述"](#)。

對於SnapMirror主動同步，請確保您已滿足各種硬體、軟體和系統配置要求。更多資訊請參閱 ["先決條件"](#)

此功能支援的插件有適用於 SQL Server 的SnapCenter插件、適用於 Windows 的SnapCenter插件、適用於 Oracle 資料庫的SnapCenter插件、適用於 SAP HANA 資料庫的SnapCenter插件、適用於 Microsoft Exchange Server 的SnapCenter插件和適用於 Unix 的SnapCenter插件。



為了支援SnapCenter中的主機啟動器鄰近性，應在ONTAP中設定其值（來源或目標）。

SnapCenter不支援的用例：

- 如果您透過將ONTAP中SnapMirror活動同步關係上的政策從 *automatedfailover* 變更為 *automatedfailoverduplex* 來將現有的非對稱SnapMirror活動同步工作負載轉換為對稱工作負載，則SnapCenter不支援此操作。
- 如果存在資源群組的備份（已在SnapCenter中受到保護），然後在ONTAP中將SnapMirror活動同步關係上的儲存策略從 *automatedfailover* 變更為 *automatedfailoverduplex*，則SnapCenter不支援此操作。

資料保護的關鍵概念

在使用SnapCenter之前，請先了解備份、複製和還原的關鍵概念。

資源

資源包括資料庫、Windows 檔案系統或使用SnapCenter備份或複製的檔案共用。根據您的環境，資源也可能是資料庫執行個體、SQL Server 可用性群組、Oracle 資料庫、RAC 資料庫或自訂應用程式群組。

資源組

資源組是主機或叢集上的資源集合，可能來自多個主機和叢集。對資源組執行的操作將根據指定的計劃應用於其所有資源。您可以對單一資源或群組執行按需或排程備份。



如果共用資源組中的一個主機進入維護模式，則該組的所有主機上的所有排程操作都會暫停。

使用相關外掛程式來備份特定資源：資料庫外掛程式用於資料庫，檔案系統外掛程式用於檔案系統，以及SnapCenter Plug-in for VMware vSphere用於虛擬機器和資料儲存區。

政策

策略指定備份頻率、副本保留、複製、腳本和資料保護作業的其他特徵。

建立資源群組或執行按需備份時可以選擇一個或多個策略。

資源組定義需要保護的內容以及何時（以日期和時間為單位）進行保護。政策描述如何實施保護。例如，如果需要備份主機的所有資料庫或檔案系統，則可以建立包含主機中所有資料庫或檔案系統的資源群組。然後可以將兩個策略附加到資源群組：每日策略和每小時策略。

建立資源群組並附加原則時，可以將其配置為每天執行一次完整備份，並每小時執行一次日誌備份的另一個計畫。

自訂處方和附言可用於資料保護操作。這些腳本允許在資料保護作業之前或之後自動化。例如，腳本可以自動通知資料保護作業失敗或警告。在製定前言和後記之前，了解創建這些腳本的要求至關重要。

前言和後記的使用

自訂的處方和後記可以在作業之前或之後自動執行資料保護任務。例如，您可以新增一個腳本來通知您作業失敗或警告。在設定它們之前，請確保您了解這些腳本的要求。

支援的腳本類型

Windows 支援以下類型的腳本：

- 批次檔
- PowerShell 腳本
- Perl 腳本

UNIX 支援以下類型的腳本：

- Perl 腳本
- Python 腳本
- Shell 腳本



除了預設的 bash shell 之外，還支援其他 shell，如 sh-shell、k-shell 和 c-shell。

腳本路徑

作為非虛擬化和虛擬化儲存系統上的 SnapCenter 操作的一部分運行的所有前腳本和後腳本都在插件主機上執行。

- Windows 腳本應位於插件主機上。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

- UNIX 腳本應位於插件主機上。



腳本路徑在執行時進行驗證。

在哪裡指定腳本

腳本在備份策略中指定。當備份作業開始時，策略會自動將腳本與正在備份的資源關聯起來。建立備份策略時，您可以指定前言和後記參數。



您不能指定多個腳本。

腳本逾時

預設情況下，超時設定為 60 秒。您可以修改超時值。

腳本輸出

Windows 腳本和後記輸出檔案的預設目錄是 Windows\System32。

UNIX 前言和後記沒有預設位置。您可以將輸出檔案重新導向到任何首選位置。

SnapCenter支援的儲存系統和應用程式

您應該了解SnapCenter支援的儲存系統、應用程式和資料庫。

支援的儲存系統

- NetApp ONTAP 9.12.1 及更高版本
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

支援透過傳輸控制協定 (TCP) 的非揮發性記憶體快速 (NVMe)。

有關Amazon FSx for NetApp ONTAP 的信息，請參閱 ["Amazon FSx for NetApp ONTAP文檔"](#)。

- 運行NetApp ONTAP 9.16.1 的NetApp ASA r2 系統。

支援的應用程式和資料庫

SnapCenter支援不同應用程式和資料庫的保護。有關受支援的應用程式和資料庫的詳細信息，請參閱 ["NetApp 互通性表工具"](#)。

SnapCenter支援在 VMware Cloud on Amazon Web Services (AWS) 軟體定義資料中心 (SDDC) 環境中保護 Oracle 和 Microsoft SQL 工作負載。 <https://community.netapp.com/t5/Tech-ONTAP-Blogs/Protect-Oracle-MS-SQL-workloads-using-NetApp-SnapCenter-in-VMware-Cloud-on-AWS/ba-p/449168>["了解更多"^]。

SnapCenter憑證的驗證方法

憑證根據應用程式或環境使用不同的身份驗證方法。憑證對使用者進行身份驗證，以便他們可以執行SnapCenter操作。您應該建立一組用於安裝插件的憑證，並建立另一組用於資料保護操作的憑證。

Windows 驗證

Windows 驗證方法針對 Active Directory 進行驗證。對於 Windows 身份驗證，Active Directory 是在SnapCenter之外設定的。SnapCenter無需額外配置即可進行身份驗證。您需要 Windows 憑證來新增主機、安裝插件包和排程作業。

不受信任的網域身份驗證

SnapCenter允許屬於不受信任網域的使用者和群組建立 Windows 憑證。為了讓身分驗證成功，您應該向SnapCenter註冊不受信任的網域。

本機工作群組身份驗證

SnapCenter允許使用本機工作群組使用者和群組建立 Windows 憑證。本機工作群組使用者和群組的 Windows 驗證不會在 Windows 憑證建立期間發生，而是會延遲到主機註冊和其他主機操作執行時發生。

SQL Server 驗證

SQL 驗證方法針對 SQL Server 執行個體進行驗證。這意味著必須在SnapCenter中發現 SQL Server 執行個體。因此，在新增SQL憑證前，必須先新增主機、安裝外掛程式包、刷新資源。您需要 SQL Server 驗證才能執行 SQL Server 上的排程或發現資源等操作。

Linux 驗證

Linux 驗證方法針對 Linux 主機進行驗證。在從SnapCenter GUI 遠端新增 Linux 主機和安裝適用於 Linux 的SnapCenter插件套件的初步步驟中，您需要進行 Linux 驗證。

AIX 身份驗證

AIX 驗證方法針對 AIX 主機進行驗證。在從SnapCenter GUI 遠端新增 AIX 主機和安裝 AIX的 SnapCenter插件包的初步步驟中，您需要進行 AIX 驗證。

Oracle 資料庫驗證

Oracle 資料庫驗證方法針對 Oracle 資料庫進行驗證。如果資料庫主機上停用了作業系統 (OS) 驗證，則需要 Oracle 資料庫驗證才能在 Oracle 資料庫上執行操作。因此，在新增 Oracle 資料庫憑證之前，您應該在 Oracle 資料庫中建立具有 sysdba 權限的 Oracle 使用者。

Oracle ASM 身份驗證

Oracle ASM 驗證方法針對 Oracle 自動儲存管理 (ASM) 執行個體進行驗證。如果您需要存取 Oracle ASM 執行個體且資料庫主機上停用了 OS 驗證，則需要進行 Oracle ASM 驗證。在新增 Oracle ASM 憑證之前，請在 ASM 實例中建立具有系統權限的 Oracle 使用者。

RMAN 目錄驗證

RMAN 目錄驗證方法針對 Oracle Recovery Manager (RMAN) 目錄資料庫進行驗證。如果您已經設定了外部目錄機制並將您的資料庫註冊到目錄資料庫，則需要新增 RMAN 目錄驗證。

ASA r2 系統支援的SnapCenter操作

從SnapCenter 6.1 開始支援ASA r2 儲存系統。 ["了解有關ASA r2 系統的更多信息"](#)

SnapCenter利用 REST API 在ASA r2 系統上執行所有操作，而 ASA r2 系統不支援 ZAPI。

- SnapCenter for ASA r2 系統支援的操作*

- 透過 VMDK 建立應用程式的主備份
- 將一致性群組快照傳輸到輔助儲存系統
- 將主儲存系統和輔助儲存系統的備份還原到原始主機或備用主機
 - 使用 VMware vMotion 從主儲存系統和輔助儲存系統進行就地恢復
 - 連接主儲存系統和輔助儲存系統並複製復原
- 將備份複製到原始主機或備用主機

SnapCenter可以發現或建立ONTAP一致性組。它還可以為目標叢集提供並初始化SnapMirror關係以提供二次保護。

有關在ASA r2 系統上為您的應用程式啟用二級保護的信息，請參閱：

- "為 Microsoft SQL Server 資源啟用二級保護"
- "為 SAP HANA 資源啟用二級保護"
- "啟用 Oracle 資源的二級保護"
- "為 Windows 檔案系統啟用二級保護"
- "為 IBM Db2 資源啟用二級保護"
- "為 PostgreSQL 資源啟用二級保護"
- "啟用 MySQL 資源的二級保護"
- "為 Unix 檔案系統啟用二級保護"
- SnapCenter不支援ASA r2 系統的操作*
- 原始設備映射 (RDM)
- Oracle 的應用程式捲
- SAP HANA NDV
- LockVault
- 防篡改快照
- FlexGroup卷
- 層次一致性組
- 從ASA、AFF或FAS儲存系統遷移到ASA r2 儲存系統
- 保護混合有ASA、AFF或FAS資源和ASA r2 資源的資料庫
- 重新命名快照
- SQL外掛主機日誌目錄二次配置

SnapCenter software快速入門

快速入門指南概述了安裝和設定SnapCenter software的基本步驟。

1

準備安裝SnapCenter伺服器

您應該確保滿足安裝SnapCenter伺服器的所有要求。

- ["要求"](#)
- ["註冊以存取SnapCenter software"](#)
- ["啟用多因素身份驗證"](#)

2

安裝SnapCenter伺服器

SnapCenter伺服器可以安裝在 Windows 或 Linux 主機上。SnapCenter ["NetApp支援站點"](#)並執行安裝程式。

- ["在 Windows 上安裝SnapCenter伺服器"](#)
- ["在 Linux 上安裝SnapCenter伺服器"](#)

3

配置SnapCenter伺服器

安裝SnapCenter伺服器後，您應該根據您的環境進行設定。

4

為您的應用程式安裝插件

確保根據所使用的應用程式滿足安裝特定於應用程式的插件的所有要求，然後繼續安裝相應的插件。

5

保護您的應用程式

成功安裝SnapCenter伺服器和必要的插件後，您可以啟動應用程式備份的建立。這些備份稍後可以在需要時用於復原和複製目的。

安裝並設定SnapCenter伺服器

準備安裝SnapCenter伺服器

安裝SnapCenter伺服器的要求

在 Windows 或 Linux 主機上安裝SnapCenter Server 之前，您應該檢查並確保滿足您的環境的所有要求。

Windows 主機的網域和工作群組需求

SnapCenter伺服器可以安裝在網域或工作群組中的 Windows 主機上。

具有管理員權限的使用者可以安裝SnapCenter伺服器。

- Active Directory 網域：您必須使用具有本機管理員權限的網域使用者。網域使用者必須是 Windows 主機上本機管理員群組的成員。
- 工作群組：您必須使用具有本機管理員權限的本機帳戶。

雖然支援域信任、多域林和跨域信任，但不支援跨林域。有關 Active Directory 網域和信任的 Microsoft 文件包含更多資訊。



安裝SnapCenter伺服器後，您不應變更SnapCenter主機所在的網域。如果從安裝SnapCenter Server 時所在的網域中移除SnapCenter Server 主機，然後嘗試解除安裝SnapCenter Server，則解除安裝作業將會失敗。

空間和尺寸要求

您應該熟悉空間和尺寸要求。

物品	Windows 主機需求	Linux 主機需求
作業系統	微軟 Windows 僅支援英文、德文、日文和簡體中文版本的作業系統。 有關受支援版本的最新信息，請參閱 https://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT[\"NetApp 互通性表工具\"] 。	• Red Hat Enterprise Linux (RHEL) 8 與 9 • SUSE Linux 企業伺服器 (SLES) 15 有關受支援版本的最新信息，請參閱 https://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT[\"NetApp 互通性表工具\"] 。
最小 CPU 數量	4 核	4 核

物品	Windows 主機需求	Linux 主機需求
最低記憶體	8GB  MySQL 伺服器緩衝池使用了總 RAM 的 20%。	8GB
SnapCenter 伺服器軟體和日誌的最小硬碟空間	7GB  如果 SnapCenter 儲存庫與安裝 SnapCenter Server 的磁碟機位於相同磁碟機中，則建議使用 15 GB。	15GB
SnapCenter 儲存庫的最小硬碟空間	8GB  注意：如果 SnapCenter 伺服器與安裝 SnapCenter 儲存庫的磁碟機相同，建議使用 15 GB。	不適用
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 7.4.2 或更高版本 有關 .NET 特定的故障排除信息，請參閱 "對於沒有 Internet 連線的傳統系統，SnapCenter 升級或安裝失敗"。	• .NET Framework 8.0.12（以及所有後續的 8.0.x 修補程式） • PowerShell 7.4.2 或更高版本 • Nginx 是一個可以用作反向代理的 Web 伺服器 • Pam-devel PAM（可插入式身份驗證模組）是一種系統安全工具，它允許系統管理員設定身份驗證策略，而無需重新編譯執行身份驗證的程式。



ASP.NET 核心需要 IIS_IUSRS 才能存取 Windows 上 SnapCenter Server 中的暫存檔案系統。

SAN 主機需求

SnapCenter 不包括主機實用程式或 DSM。如果 SnapCenter 主機是 SAN（FC/iSCSI）環境的一部分，則可能需要在 SnapCenter Server 主機上安裝和設定其他軟體。

- 主機實用程式：主機實用程式支援 FC 和 iSCSI，它使您能夠在 Windows 伺服器上使用 MPIO。 ["了解更多"](#)

。

- Microsoft DSM for Windows MPIO：軟體與 Windows MPIO 驅動程式搭配使用，以管理NetApp和 Windows 主機之間的多條路徑。高可用性配置需要 DSM。



如果您使用的是ONTAP DSM，則應該遷移到 Microsoft DSM。有關更多信息，請參閱 ["如何從ONTAP DSM 遷移到 Microsoft DSM"](#)。

瀏覽器要求

SnapCenter software支援 Chrome 125 及更高版本以及 Microsoft Edge 110.0.1587.17 及更高版本。

端口要求

SnapCenter software需要不同的連接埠來實現不同元件之間的通訊。

- 應用程式不能共享連接埠。
- 對於可自訂的端口，如果您不想使用預設端口，您可以在安裝期間選擇自訂端口。
- 對於固定端口，您應該接受預設端口號。
- 防火牆
 - 防火牆、代理或其他網路設備不應干擾連線。
 - 如果在安裝SnapCenter時指定自訂端口，則應在插件主機上為SnapCenter插件Loader的該連接埠新增防火牆規則。

下表列出了不同的連接埠及其預設值。

連接埠名稱	連接埠號	協定	方向	描述
SnapCenter端口	8146	HTTPS	雙向	此連接埠用於SnapCenter用戶端（SnapCenter用戶）與SnapCenter伺服器之間的通信，也用於從插件主機到SnapCenter伺服器的通訊。 您可以自訂連接埠號。
SnapCenter SMCORE 通訊端口	8145	HTTPS	雙向	此連接埠用於SnapCenter伺服器與安裝了SnapCenter插件的主機之間的通訊。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
調度程序服務端口	8154	HTTPS		此連接埠用於以集中方式協調SnapCenter伺服器主機內所有託管插件的SnapCenter調度程序工作流程。 您可以自訂連接埠號。
RabbitMQ 端口	5672	TCP		這是 RabbitMQ 監聽的預設端口，用於 Scheduler 服務和SnapCenter之間的發布者-訂閱者模型通訊。
MySQL 連接埠	3306	HTTPS		此連接埠用於與SnapCenter儲存庫資料庫通訊。您可以建立從SnapCenter伺服器到 MySQL 伺服器的安全連線。了解更多
Windows 插件主機	135 , 445	TCP		此連接埠用於SnapCenter伺服器與安裝插件的主機之間的通訊。Microsoft 指定的其他動態連接埠範圍也應開放。
Linux 或 AIX 插件主機	22	SSH	單向	此連接埠用於SnapCenter伺服器和主機之間的通信，從伺服器發起到客戶端主機。
適用於 Windows、Linux 或 AIX 的SnapCenter插件包	8145	HTTPS	雙向	此連接埠用於SMCore與安裝插件包的主機進行通訊。可客製化。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 Oracle 資料庫的SnapCenter插件	27216			Oracle 插件使用預設 JDBC 連接埠來連接 Oracle 資料庫。
適用於 Exchange 資料庫的SnapCenter插件	909			Windows 插件使用預設的 NET.TCP 連接埠來連接 Exchange VSS 回呼。
NetApp支援的SnapCenter插件	9090	HTTPS		這是僅在插件主機上使用的內部連接埠；不需要防火牆例外。 SnapCenter伺服器 and 插件之間的通訊透過連接埠 8145 進行。
ONTAP叢集或 SVM 通訊埠	• 443 (HTTPS) • 80 (HTTP)	• HTTPS • HTTP	雙向	此連接埠由 SAL（儲存抽象層）用於執行SnapCenter Server 的主機和 SVM 之間的通訊。SnapCenter for Windows 插件主機上的 SAL 目前也使用該連接埠來實作SnapCenter插件主機和 SVM 之間的通訊。
適用於 SAP HANA 資料庫的SnapCenter插件	• 3instance_number13 • 3instance_number15	• HTTPS • HTTP	雙向	對於多租戶資料庫容器（MDC）單一租戶，連接埠號碼以13結尾；對於非MDC，連接埠號碼以15結尾。 您可以自訂連接埠號。

連接埠名稱	連接埠號	協定	方向	描述
適用於 PostgreSQL 的 SnapCenter 插件	5432			此連接埠是 PostgreSQL 外掛程式與 PostgreSQL 叢集通訊所使用的預設 PostgreSQL 連接埠。 您可以自訂連接埠號。

註冊以存取 SnapCenter software

如果您是 Amazon FSx for NetApp ONTAP 或 Azure NetApp Files 的新使用者且沒有現有的 NetApp 帳戶，則應該註冊以存取 SnapCenter software。

開始之前

- 您應該可以存取公司電子郵件 ID。
- 如果您使用 Azure NetApp Files，則應該擁有 Azure 訂閱 ID。
- 如果您使用的是 Amazon FSx for NetApp ONTAP，則應該擁有 FSx for ONTAP 檔案系統的檔案系統 ID。

關於此任務

您的註冊需要經過資訊驗證，可能需要一天時間才能確認並將新的 NetApp 支援網站 (NSS) 帳戶從 訪客 存取權限升級為 完全 存取權限。

步驟

1. 點選 <https://mysupport.netapp.com/site/user/registration> 進行註冊。
2. 輸入您的公司電子郵件 ID，完成驗證碼，接受 NetApp 的隱私權政策，然後按一下「提交」。
3. 透過輸入發送到您的電子郵件 ID 的 OTP 來驗證註冊，然後按一下「繼續」*。
4. 在註冊完成頁面，輸入以下詳細資訊以完成註冊。
 - a. 選擇* NetApp 客戶/最終使用者*。
 - b. 在序號欄位中，如果您使用的是 Azure NetApp Files，請輸入 Azure 訂閱 ID；如果您使用的是 Amazon FSx for NetApp ONTAP，請輸入檔案系統 ID。



您可以提交以下票證：<https://mysupport.netapp.com/site/help> 如果您在註冊過程中遇到任何問題或想了解狀態。

多重身份驗證 (MFA)

管理多重身分驗證 (MFA)

您可以管理 Active Directory 聯合驗證服務 (AD FS) 伺服器和 SnapCenter 伺服器中的多重驗證 (MFA) 功能。

啟用多重身份驗證 (MFA)

您可以使用 PowerShell 指令為 SnapCenter Server 啟用 MFA 功能。

關於此任務

- 當在相同 AD FS 中設定其他應用程式時，SnapCenter 支援基於 SSO 的登入。在某些 AD FS 配置中，SnapCenter 可能會出於安全性原因要求使用者進行身份驗證，具體取決於 AD FS 會話持久性。
- 可以透過執行以下命令來取得有關可與 cmdlet 一起使用的參數及其描述的信息 `Get-Help command_name`。或者，您也可以查看 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

開始之前

- Windows Active Directory 聯合驗證服務 (AD FS) 應該會在對應的網域中啟動並執行。
- 您應該擁有 AD FS 支援的多重驗證服務，例如 Azure MFA、Cisco Duo 等。
- 無論時區為何，SnapCenter 和 AD FS 伺服器時間戳記都應該相同。
- 為 SnapCenter Server 採購並配置授權 CA 憑證。

由於以下原因，CA 證書是強制性的：

- 確保 ADFS-F5 通訊不會中斷，因為自簽名憑證在節點層級是唯一的。
- 確保在獨立或高可用性配置中的升級、修復或災難復原 (DR) 期間，不會重新建立自簽名證書，從而避免重新配置 MFA。
- 確保 IP-FQDN 解析。

有關 CA 憑證的信息，請參閱 "[產生 CA 憑證 CSR 文件](#)"。

步驟

1. 連線至 Active Directory 聯合驗證服務 (AD FS) 主機。
2. 從下列位置下載 AD FS 聯合元資料文件 "<https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"。
3. 將下載的檔案複製到 SnapCenter Server 以啟用 MFA 功能。
4. 透過 PowerShell 以 SnapCenter 管理員使用者身分登入 SnapCenter 伺服器。
5. 使用 PowerShell 會話，使用 `New-SmMultifactorAuthenticationMetadata -path` cmdlet 產生 SnapCenter MFA 元資料檔。

`path` 參數指定在 SnapCenter Server 主機中儲存 MFA 元資料檔案的路徑。

6. 將產生的檔案複製到 AD FS 主機以將 SnapCenter 配置為客戶端實體。
7. SnapCenter ``Set-SmMultiFactorAuthentication`` 命令。
8. (可選) 使用以下方式檢查 MFA 配置狀態和設置 ``Get-SmMultiFactorAuthentication`` 命令。
9. 前往 Microsoft 管理控制台 (MMC) 並執行下列步驟：
 - a. 按一下“檔案”>“新增/刪除管理單元”。
 - b. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
 - c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

- d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
- e. 右鍵點選綁定到SnapCenter 的CA 證書，然後選擇 所有任務 > 管理私密金鑰。
- f. 在權限精靈上執行下列步驟：
 - i. 按一下“新增”。
 - ii. 點擊*位置*並選擇相關主機（層次結構的頂部）。
 - iii. 在「位置」彈出視窗中按一下「確定」。
 - iv. 在物件名稱欄位中，輸入“IIS_IUSRS”，然後按一下“檢查名稱”，然後按一下“確定”。

如果檢查成功，請按一下「確定」。

10. 在 AD FS 主機中，開啟 AD FS 管理精靈並執行下列步驟：
 - a. 右鍵點選*依賴方信任*>*新增依賴方信任*>*開始*。
 - b. 選擇第二個選項並瀏覽SnapCenter MFA 元資料文件，然後按一下「下一步」。
 - c. 指定顯示名稱並按一下“下一步”。
 - d. 根據需要選擇存取控制策略，然後按一下「下一步」。
 - e. 在下一個選項卡中選擇預設設定。
 - f. 按一下“完成”。

SnapCenter現在反映為具有所提供顯示名稱的依賴方。

11. 選擇名稱並執行以下步驟：
 - a. 按一下「編輯索賠簽發政策」。
 - b. 按一下“新增規則”，然後按一下“下一步”。
 - c. 指定聲明規則的名稱。
 - d. 選擇*Active Directory*作為屬性儲存。
 - e. 選擇屬性為 **User-Principal-Name**，傳出宣告類型為 **Name-ID**。
 - f. 按一下“完成”。

12. 在 ADFS 伺服器上執行下列 PowerShell 命令。

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-SigningCertificateRevocationCheck None
```

```
Set-AdfsRelyingPartyTrust -TargetName '<Display name of relying party >'  
-EncryptionCertificateRevocationCheck None
```

13. 執行下列步驟以確認元資料已成功匯入。
 - a. 右鍵點選信賴方信任並選擇“屬性”。
 - b. 確保端點、標識符和簽名欄位已填入。
14. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

SnapCenter MFA 功能也可以使用 REST API 啟用。

有關故障排除信息，請參閱 "[在多個選項卡中同時嘗試登入時顯示 MFA 錯誤](#)"。

更新 AD FS MFA 元數據

每當 AD FS 伺服器發生任何修改（例如昇級、CA 憑證續約、DR 等）時，您都應該更新 SnapCenter 中的 AD FS MFA 元資料。

步驟

1. 從下列位置下載 AD FS 聯合元資料文件"<https://<hostFQDN>/FederationMetadata/2007-06/FederationMetadata.xml>"
2. 將下載的檔案複製到 SnapCenter Server 以更新 MFA 設定。
3. 透過執行以下 cmdlet 更新 SnapCenter 中的 AD FS 元資料：

```
Set-SmMultiFactorAuthentication -Path <location of ADFS MFA metadata xml file>
```

4. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

更新 SnapCenter MFA 元數據

每當 ADFS 伺服器發生任何修改（例如修復、CA 憑證續約、DR 等）時，您都應該更新 AD FS 中的 SnapCenter MFA 元資料。

步驟

1. 在 AD FS 主機中，開啟 AD FS 管理精靈並執行下列步驟：
 - a. 選擇*依賴方信任*。
 - b. 右鍵點選為 SnapCenter 建立的信賴方信任並選擇「刪除」。

將顯示依賴方信任的使用者定義名稱。

- c. 啟用多重身份驗證 (MFA)。

看"[啟用多重身份驗證](#)"。

2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

停用多重身份驗證 (MFA)

步驟

1. 停用 MFA 並清理啟用 MFA 時建立的設定文件，方法是使用 `Set-SmMultiFactorAuthentication` 命令。
2. 關閉所有瀏覽器標籤並重新開啟瀏覽器以清除現有或活動的會話 cookie，然後再次登入。

使用 Rest API、PowerShell 和 SCCLI 管理多重驗證 (MFA)

支援透過瀏覽器、REST API、PowerShell 和 SCCLI 進行 MFA 登入。MFA 透過 AD FS 身份管理器支援。您可以從 GUI、REST API、PowerShell 和 SCCLI 啟用 MFA、停用 MFA 和設定 MFA。

將 AD FS 設定為 OAuth/OIDC

使用 Windows GUI 精靈設定 AD FS

1. 導覽至 伺服器管理員儀表板 > 工具 > **ADFS** 管理。
2. 導覽至 **ADFS** > 應用程式群組。
 - a. 右鍵點選“應用程式群組”。
 - b. 選擇*新增應用程式群組*並輸入*應用程式名稱*。
 - c. 選擇*伺服器應用程式*。
 - d. 按一下“下一步”。
3. 複製*客戶端識別碼*。

這是客戶端 ID。..在重新導向 URL 中新增回呼 URL（SnapCenter伺服器 URL）。..按一下“下一步”。

4. 選擇*產生共享金鑰*。

複製秘密值。這是客戶的秘密。..按一下“下一步”。

5. 在「摘要」頁面上，按一下「下一步」。
 - a. 在*完成*頁面上，按一下*關閉*。
6. 右鍵點選新新增的*應用程式群組*並選擇*屬性*。
7. 從應用程式屬性中選擇*新增應用程式*。
8. 點擊“新增應用程式”。

選擇 Web API 並按一下「下一步」。

9. 在設定 Web API 頁面上，將上一個步驟建立的SnapCenter伺服器 URL 和用戶端識別碼輸入到識別碼部分。
 - a. 按一下“新增”。
 - b. 按一下“下一步”。
10. 在*選擇存取控制策略*頁面上，根據您的要求選擇控制策略（例如，允許所有人並要求 MFA），然後按一下*下一步*。
11. 在*配置應用程式權限*頁面，預設選擇openid作為範圍，點擊*下一步*。
12. 在「摘要」頁面上，按一下「下一步」。

在*完成*頁面上，按一下*關閉*。

13. 在「範例應用程式屬性」頁面上，按一下「確定」。
14. JWT 令牌由授權伺服器（AD FS）頒發，供資源使用。

此令牌的「aud」或受眾聲明必須與資源或 Web API 的識別碼相符。

15. 編輯選定的 WebAPI 並檢查回呼 URL（SnapCenter伺服器 URL）和用戶端識別碼是否正確新增。

配置 OpenID Connect 以提供使用者名稱作為聲明。

16. 開啟位於伺服器管理員右上角*工具*選單下的*AD FS 管理*工具。
 - a. 從左側邊欄中選擇“應用程式群組”資料夾。
 - b. 選擇 Web API 並點選 **EDIT**。
 - c. 前往發行轉換規則標籤
17. 按一下“新增規則”。
 - a. 在聲明規則範本下拉選單中選擇*將 LDAP 屬性作為聲明傳送*。
 - b. 按一下“下一步”。
18. 輸入*聲明規則*名稱。
 - a. 在屬性儲存下拉選單中選擇*Active Directory*。
 - b. 在 **LDAP Attribute** 下拉選單中選擇 **User-Principal-Name**，在 O*utgoing Claim Type* 下拉選單中選擇 **UPN**。
 - c. 按一下“完成”。

使用 **PowerShell** 命令建立應用程式群組

您可以使用 PowerShell 命令建立應用程式群組、Web API 並新增範圍和聲明。這些命令以自動腳本格式提供。欲了解更多信息，請參閱<連結至知識庫文章>。

1. 使用以下命令在 AD FS 中建立新的應用程式組。

```
New-AdfsApplicationGroup -Name $ClientRoleIdentifier
-ApplicationGroupIdentifier $ClientRoleIdentifier
```

`ClientRoleIdentifier`您的應用程式群組的名稱

`redirectURL`授權後重定向的有效 URL

2. 建立 AD FS 伺服器應用程式並產生客戶端機密。

```
Add-AdfsServerApplication -Name "$ClientRoleIdentifier - Server app"
-ApplicationGroupIdentifier $ClientRoleIdentifier -RedirectUri $redirectURL
-Identifier $identifier -GenerateClientSecret
```

3. 建立 ADFS Web API 應用程式並配置其應使用的策略名稱。

```
$identifier = (New-Guid).Guid
```

```
Add-AdfsWebApiApplication -ApplicationGroupIdentifier $ClientRoleIdentifier
-Name "App Web API"
```

```
-Identifier $identifier -AccessControlPolicyName "Permit everyone"
```

4. 從以下命令的輸出中取得客戶端 ID 和客戶端金鑰，因為它只顯示一次。

```
"client_id = $identifier"
```

```
"client_secret: "$($ADFSApp.ClientSecret)
```

5. 授予 AD FS 應用程式 allatclaims 和 openid 權限。

```
Grant-AdfsApplicationPermission -ClientRoleIdentifier $identifier
-ServerRoleIdentifier $identifier -ScopeNames @('openid')

$transformrule = @"

@RuleTemplate = "LdapClaims"

@RuleName = "AD User properties and Groups"

c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname",
Issuer ==

"AD AUTHORITY"]

⇒ issue(store = "Active Directory", types =
("http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn"), query =
";userPrincipalName;{0}", param = c.Value);

"@
```

6. 寫出轉換規則檔。

```
$transformrule | Out-File -FilePath .\issueancetransformrules.tmp -force
-Encoding ascii
$relativePath = Get-Item .\issueancetransformrules.tmp
```

7. 命名 Web API 應用程式並使用外部文件定義其頒發轉換規則。

```
Set-AdfsWebApiApplication -Name "$ClientRoleIdentifier - Web API"
-TargetIdentifier

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

更新訪問令牌到期時間

您可以使用 PowerShell 指令更新存取權杖的到期時間。

關於此任務

- 存取令牌只能用於使用者、用戶端和資源的特定組合。存取令牌不能被撤銷，並且在到期前有效。
- 預設情況下，存取令牌的有效期為 60 分鐘。此最短到期時間足夠且可擴充。您必須提供足夠的價值以避免任何正在進行的關鍵業務工作。

步

若要更新應用程式群組 WebApi 的存取權杖到期時間，請在 AD FS 伺服器中使用下列命令。

+

```
Set-AdfsWebApiApplication -TokenLifetime 3600 -TargetName "<Web API>"
```

從 **AD FS** 取得持有者令牌

您應該在任何 REST 用戶端（如 Postman）中填寫下面提到的參數，它會提示您填寫使用者憑證。此外，您應該輸入第二因素身份驗證（您擁有的東西和您是的东西）來獲取承載令牌。

+ 持有者令牌的有效性可根據應用程式從 AD FS 伺服器進行配置，預設有效期為 60 分鐘。

場地	價值
資助類型	授權碼
回調URL	如果您沒有回調 URL，請輸入應用程式的基本 URL。
授權網址	[adfs 網域]/adfs/oauth2/授權
訪問令牌 URL	[adfs 網域]/adfs/oauth2/token
客戶端 ID	輸入 AD FS 用戶端 ID
客戶端機密	輸入 AD FS 用戶端機密
範圍	OpenID
客戶端身份驗證	作為基本 AUTH 標頭發送
資源	在「進階選項」標籤中，新增與回呼 URL 具有相同值的資源字段，該字段會作為 JWT 令牌中的「aud」值出現。

使用 **PowerShell**、**SCCLI** 和 **REST API** 在 **SnapCenter Server** 中設定 **MFA**

您可以使用 PowerShell、SCCLI 和 REST API 在 SnapCenter Server 中設定 MFA。

SnapCenter MFA CLI 身份驗證

在 PowerShell 和 SCCLI 中，現有的 cmdlet（Open-SmConnection）擴展了一個名為「AccessToken」的字段，以使用承載令牌對使用者進行身份驗證。

```
Open-SmConnection -Credential <PSCredential> [-SMSbaseUrl <String>] [-Port <String>] [-RoleName <String>] [-AccessToken <string>]
```

執行上述 cmdlet 後，將為對應使用者建立一個會話以執行進一步的 SnapCenter cmdlet。

SnapCenter MFA Rest API 驗證

在 REST API 用戶端（如 Postman 或 swagger）中使用格式為 *Authorization=Bearer <access token>* 的承載令牌，並在標頭中提及使用者 RoleName 以從 SnapCenter 獲得成功回應。

MFA Rest API 工作流程

當使用 AD FS 設定 MFA 時，您應該使用存取（承載）令牌進行身份驗證，以透過任何 Rest API 存取 SnapCenter 應用程式。

關於此任務

- 您可以使用任何 REST 用戶端，例如 Postman、Swagger UI 或 FireCamp。
- 取得存取權杖並使用它來驗證後續請求（SnapCenter Rest API）以執行任何操作。

步驟

透過 AD FS MFA 進行身份驗證

1. 配置 REST 用戶端以呼叫 AD FS 端點來取得存取權杖。

當您點擊按鈕以取得應用程式的存取權杖時，您將被重新導向至 AD FS SSO 頁面，您必須在該頁面提供您的 AD 憑證並使用 MFA 進行驗證。1. 在 AD FS SSO 頁面中，在使用者名稱文字方塊中輸入您的使用者名稱或電子郵件。

+ 使用者名稱必須格式化為 user@domain 或 domain\user。

2. 在密碼文字方塊中，輸入您的密碼。
3. 點選“登入”。
4. 從*登入選項*部分，選擇一個身份驗證選項並進行身份驗證（取決於您的配置）。
 - 推播：批准發送到您手機的推播通知。
 - 二維碼：使用 AUTH Point 手機應用程式掃描二維碼，然後輸入應用程式中顯示的驗證碼
 - 一次性密碼：輸入您的令牌的一次性密碼。

5. 身份驗證成功後，將開啟一個彈出窗口，其中包含存取、ID 和刷新令牌。

複製存取權杖並在 SnapCenter Rest API 中使用它來執行操作。

6. 在 Rest API 中，您應該在標題部分傳遞存取權杖和角色名稱。
7. SnapCenter 從 AD FS 驗證此存取權杖。

如果它是有效令牌，SnapCenter 會對其進行解碼並取得使用者名稱。

8. SnapCenter 使用使用者名稱和角色名稱對使用者進行身份驗證以執行 API。

如果驗證成功，SnapCenter 將傳回結果，否則將顯示錯誤訊息。

為 **Rest API**、**CLI** 和 **GUI** 啟用或停用**SnapCenter MFA** 功能

圖形使用者介面

步驟

- 1. 以SnapCenter管理員身分登入SnapCenter伺服器。
- 2. 點擊“設定”>“全域設定”>“多重身份驗證 (MFA) 設定”
- 3. 選擇介面（GUI/RST API/CLI）以啟用或停用 MFA 登入。

PowerShell 介面

步驟

- 1. 執行 PowerShell 或 CLI 命令以啟用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

```
Set-SmMultiFactorAuthentication -IsGuiMFAEnabled -IsRestApiMFAEnabled  
-IsCliMFAEnabled -Path
```

路徑參數指定 AD FS MFA 元資料 xml 檔案的位置。

使用指定的 AD FS 元資料檔案路徑配置的SnapCenter GUI、Rest API、PowerShell 和 SCCLI 啟用 MFA。

- 2. 使用 `Get-SmMultiFactorAuthentication` 命令。

SCCLI 介面

步驟

- 1. # sccli Set-SmMultiFactorAuthentication -IsGuiMFAEnabled true
-IsRESTAPIMFAEnabled true -IsCliMFAEnabled true -Path
"C:\ADFS_metadata\abc.xml"
- 2. # sccli Get-SmMultiFactorAuthentication

REST API

- 1. 執行以下文章 API 以啟用 GUI、Rest API、PowerShell 和 SCCLI 的 MFA。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	郵政
請求正文	{ "IsGuiMFAEnabled" : false ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSSConfigFilePath」 : 「C:\ADFS_metadata\abc.xml」 }

回應主體	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false ， "ADFSSConfigFilePath" : "C : \\ADFS_metadata \\abc.xml" ， 「SCConfigFilePath」 : null ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSHostName」 : 「win-adfs- sc49.winscedom2.com」 } }

2. 使用以下 API 檢查 MFA 配置狀態和設定。

範圍	價值
請求的 URL	/api/4.9/settings/multifactorauthentication
HTTP 方法	得到
回應主體	{ "MFAConfiguration" : { "IsGuiMFAEnabled" : false ， "ADFSSConfigFilePath" : "C : \\ADFS_metadata \\abc.xml" ， 「SCConfigFilePath」 : null ， 「IsRestApiMFAEnabled」 : true ， 「IsCliMFAEnabled」 : false ， 「ADFSHostName」 : 「win-adfs- sc49.winscedom2.com」 } }

安裝SnapCenter伺服器

在 Windows 主機上安裝SnapCenter伺服器

您可以執行SnapCenter Server 安裝程式執行檔來安裝SnapCenter Server。

您可以選擇使用 PowerShell cmdlet 執行多個安裝和設定程序。您應該使用 PowerShell 7.4.2 或更高版本。



不支援從命令列靜默安裝SnapCenter伺服器。

開始之前

- SnapCenter伺服器主機必須保持最新的 Windows 更新，且無需重新啟動系統。
- 您應該確保計劃安裝SnapCenter伺服器的主機上未安裝 MySQL 伺服器。
- 您應該啟用 Windows 安裝程式偵錯。

有關啟用 ["Windows 安裝程式日誌記錄"](#)。



您不應在具有 Microsoft Exchange Server、Active Directory 或網域名稱伺服器的主機上安裝SnapCenter Server。

步驟

1. 從下列位置下載SnapCenter Server 安裝包 ["NetApp支援站點"](#)。

2. 雙擊下載的 .exe 檔案啟動SnapCenter Server 安裝。

啟動安裝後，將執行所有預檢查，如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

您可以忽略警告訊息並繼續安裝；但是，錯誤應該得到修復。

3. 查看SnapCenter伺服器安裝所需的預先填入值並根據需要進行修改。

您不必指定 MySQL 伺服器儲存庫資料庫的密碼。在SnapCenter Server 安裝期間，密碼會自動產生。



特殊字元“%`” is not supported in the custom path for the repository database. If you include " %`”，則安裝失敗。

4. 按一下“立即安裝”。

如果您指定的任何值無效，則會顯示相應的錯誤訊息。您應該重新輸入這些值，然後啟動安裝。



如果點選*取消*按鈕，正在執行的步驟將會完成，然後開始回溯操作。 SnapCenter伺服器將從主機中完全刪除。

但是，如果在執行“SnapCenter Server 網站重新啟動”或“等待SnapCenter Server 啟動”操作時按一下“取消”，則安裝將繼續進行而不會取消操作。

日誌檔案始終列在管理員使用者的 %temp% 資料夾中（最早的在前）。如果要重新導向日誌位置，請透過執行下列命令從命令提示字元啟動SnapCenter Server 安裝

```
:C:\installer_location\installer_name.exe /log"C:\\"
```

安裝期間在 **Windows** 主機上啟用的功能

SnapCenter Server 安裝程式在安裝期間在 Windows 主機上啟用 Windows 功能和角色。這些可能對故障排除和維護主機系統有用。

類別	特徵
Web 伺服器	• 網路資訊服務 • 萬維網服務 • 常見 HTTP 功能 ◦ 預設文檔 ◦ 目錄瀏覽 ◦ HTTP 錯誤 ◦ HTTP 重新導向 ◦ 靜態內容 ◦ WebDAV 發布 • 健康與診斷 ◦ 自訂日誌 ◦ HTTP 日誌記錄 ◦ 測井工具 ◦ 請求監控 ◦ 追蹤 • 性能特點 ◦ 靜態內容壓縮 • 安全 ◦ IP 安全 ◦ 基本驗證 ◦ 集中式 SSL 憑證支持 ◦ 用戶端憑證對應認證 ◦ IIS 用戶端憑證對應驗證 ◦ IP 和網域限制 ◦ 請求過濾 ◦ URL 授權 ◦ Windows 驗證 • 應用程式開發功能 ◦ .NET 擴充性 4.5 ◦ 應用程式初始化 ◦ ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 ◦ 伺服器端包含 ◦ WebSocket 協議 管理工具

類別	特徵
IIS 管理腳本和工具	• IIS 管理服務 • Web管理工具
.NET Framework 8.0.12 功能	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • Windows Communication Foundation (WCF) HTTP 啟動45 ◦ TCP 啟用設定 ◦ HTTP 啟用設定 有關 .NET 特定的故障排除信息，請參閱 "對於沒有 Internet 連線的傳統系統，SnapCenter升級或安裝失敗"。
訊息佇列	• 訊息隊列服務  確保沒有其他應用程式使用 SnapCenter 建立和管理的 MSMQ 服務。 • RabbitMQ • Erlang
Windows 進程啟動服務	• 流程模型
配置 API	全部

在 Linux 主機上安裝 SnapCenter 伺服器

您可以執行 SnapCenter Server 安裝程式執行檔來安裝 SnapCenter Server。

開始之前

- 如果您想要使用沒有足夠權限安裝 SnapCenter 的非 root 使用者安裝 SnapCenter 伺服器，請從 NetApp 支援網站取得 sudoers 校驗和檔案。您應該根據 Linux 版本使用適當的校驗和檔案。
- 如果 SUSE Linux 中沒有 sudo 套件，請安裝 sudo 套件以避免身份驗證失敗。
- 對於 SUSE Linux，請配置主機名稱以避免安裝失敗。
- 透過執行以下命令檢查 Linux 的安全狀態 `sestatus`。如果 `_SELinux 狀態_` 為“已啟用”且 `_當前模式_` 為“強制”，請執行下列操作：
 - 運行以下命令：`sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT>`

`WEBAPP_EXTERNAL_PORT` 的預設值為 8146

- 如果防火牆阻止了端口，請運行 `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

`WEBAPP_EXTERNAL_PORT` 的預設值為 8146

- 從您具有讀寫權限的目錄執行以下命令：

- `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

如果命令返回“無事可做”，請在安裝 SnapCenter Server 後重新執行該命令。

- 如果命令建立了 `_my-nginx.pp_`，則執行命令使策略包處於活動狀態：`sudo semodule -i my-nginx.pp`

- MySQL PID 目錄所使用的路徑是 `/var/opt/mysqld`。執行以下命令設定 MySQL 安裝的權限。

- `mkdir /var/opt/mysqld`

- `sudo semanage fcontext -a -t mysqld_var_run_t "/var/opt/mysqld(/.*)?"`

- `sudo restorecon -Rv /var/opt/mysqld`

- MySQL 資料目錄所使用的路徑是 `/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/`。執行以下命令設定 MySQL 資料目錄的權限。

- `mkdir -p /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

- `sudo semanage fcontext -a -t mysqld_db_t "/INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL(/.*)?"`

- `sudo restorecon -Rv /INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL`

關於此任務

- 當 SnapCenter Server 安裝在 Linux 主機上時，就會安裝 MySQL、RabbitMq、Erlang 等第三方服務。您不應該卸載它們。
- Linux 主機上安裝的 SnapCenter 伺服器不支援：
 - 高可用性
 - Windows 外掛
 - Active Directory（僅支援本機用戶，包括具有憑證的 root 用戶和非 root 用戶）
 - 基於金鑰的身份驗證以登入 SnapCenter
- 在安裝 .NET 執行時期期間，如果安裝無法解析 `libicu` 庫的依賴關係，則透過執行以下命令安裝 `libicu`：`yum install -y libicu`
- 如果由於 `_Perl_` 不可用而導致 SnapCenter Server 安裝失敗，則透過執行下列命令安裝 `_Perl_`：`yum install -y perl`

步驟

1. 從以下位置下載 "[NetApp 支援站點](#)" 到 `/home` 目錄。
 - SnapCenter 伺服器安裝套件 - `* SnapCenter-linux-server-(el8/el9/sles15).bin*`
 - 公鑰檔案 - `snapcenter_public_key.pub`

。對應的簽章檔案 - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**

2. 驗證簽名文件。

```
$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>
```

3. 對於非 root 使用者安裝，請新增 .bin 安裝程式隨附的 **snapcenter_server_checksum_(el8/el9/sles15).txt** 中指定的 visudo 內容。

4. 為 .bin 安裝程式分配執行權限。

```
chmod +x snapcenter-linux-server-(el8/el9/sles15).bin
```

5. 執行其中一項操作來安裝 SnapCenter Server。

如果你想表演...	這樣做...
互動式安裝	<pre>./snapcenter-linux-server-(el8/el9/sles15).bin</pre> 系統將提示您輸入以下詳細資訊： • 用於存取 Linux 主機外部的 SnapCenter 伺服器的 webapp 外部連接埠。預設值為 8146。 • 將安裝 SnapCenter Server 的 SnapCenter Server 使用者。 • 將安裝軟體包的安裝目錄。

如果你想表演...	這樣做...
非互動式安裝	<pre> sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DWEBAPP_EXTERNAL_PORT=<port> -DWEBAPP_INTERNAL_PORT=<port> -DSMCORE_PORT=<port> -DSCHEDULER_PORT=<port> -DSNAPCENTER_SERVER_USER=<user> -DUSER_INSTALL_DIR=<dir> -DINSTALL_LOG_NAME=<filename> </pre> 範例：sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLoglog 日誌將儲存在 <code>/var/opt/snapcenter/logs</code>。 安裝SnapCenter Server 時要傳遞的參數： • DWEBAPP_EXTERNAL_PORT：用於存取 Linux 主機外部的SnapCenter伺服器的 Webapp 外部連接埠。預設值為 8146。 • DWEBAPP_INTERNAL_PORT：用於存取 Linux 主機內的SnapCenter伺服器的 Webapp 內部連接埠。預設值為 8147。 • DSMCORE_PORT：smcore 服務正在執行的 SMCORE 連接埠。預設值為 8145。 • DSCHEDULER_PORT：執行調度程序服務的調度程序連接埠。預設值為 8154。 • DSNAPCENTER_SERVER_USER：將安裝SnapCenter Server 的SnapCenter Server 使用者。對於 <code>DSNAPCENTER_SERVER_USER</code>，預設值是執行安裝程式的使用者。 • DUSER_INSTALL_DIR：將安裝套件的安裝目錄。對於 <code>_DUSER_INSTALL_DIR_</code>，預設安裝目錄是 <code>_opt_</code>。 • DINSTALL_LOG_NAME：儲存安裝日誌的日誌檔案名稱。這是一個可選參數，如果指定，則控制台上不會顯示任何日誌。如果不指定此參數，則日誌將顯示在控制台上，並儲存在預設日誌檔案中。 • DSELINUX：如果 <code>_SELinux_</code> 狀態為“啟用”，<code>_當前模式_</code> 為“強制”，並且您已執行“開始之前”部分中提到的命令，則應指定此參數並將其值指定為 1。預設值為 0。 • DUPGRADE：預設值為 0。指定此參數及其值為 0 以外的任何整數來升級SnapCenter伺服器。

下一步是什麼？

- 如果 `_SELinux` 狀態_為“啟用”且 `_當前模式_` 為“強制”，則 **nginx** 服務無法啟動。您應該執行以下命令：
 - a. 前往主目錄。
 - b. 運行以下命令：`journalctl -x|grep nginx`。
 - c. 如果不允許Webapp內部連接埠（8147）監聽，則執行下列命令：
 - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
 - `semodule -i my-nginx.pp`
 - d. 跑步 `setsebool -P httpd_can_network_connect on`

安裝期間在 **Linux** 主機上啟用的功能

SnapCenter伺服器安裝以下軟體包，可協助排除故障和維護主機系統。

- RabbitMQ
- Erlang

註冊**SnapCenter**

如果您是NetApp產品的新用戶且沒有現有的NetApp帳戶，則應該註冊SnapCenter以獲得支援。

步驟

1. 安裝SnapCenter後，導覽至 幫助 > 關於。
2. 在「關於 SnapCenter」對話方塊中，記下SnapCenter實例，這是一個以 971 開頭的 20 位數。
3. 點選 <https://register.netapp.com>。
4. 點擊“我不是註冊的**NetApp**客戶”。
5. 指定您的詳細資料以進行註冊。
6. 將NetApp參考 SN 欄位留空。
7. 從產品線下拉式選單中選擇* SnapCenter*。
8. 選擇計費提供者。
9. 輸入 20 位元SnapCenter執行個體 ID。
10. 點選“提交”。

使用 **RBAC** 授權登入**SnapCenter**

SnapCenter支援基於角色的存取控制 (RBAC)。SnapCenter管理員透過SnapCenter RBAC 將角色和資源分配給工作群組或活動目錄中的用戶，或活動目錄中的群組。RBAC 使用者現在可以使用指派的角色登入SnapCenter。

開始之前

- 您應該在 Windows 伺服器管理員中啟用 Windows 進程啟動服務 (WAS)。

- 如果您想要使用 Internet Explorer 作為瀏覽器登入 SnapCenter 伺服器，則應確保 Internet Explorer 中的保護模式已停用。
- 如果 SnapCenter Server 安裝在 Linux 主機上，則應使用用於安裝 SnapCenter Server 的使用者帳號登入。

關於此任務

在安裝過程中，SnapCenter 伺服器安裝精靈會建立一個捷徑並將其放在桌面上和安裝 SnapCenter 的主機的「開始」功能表中。此外，在安裝結束時，安裝精靈會根據您在安裝期間提供的資訊顯示 SnapCenter URL，如果您想從遠端系統登錄，可以複製該 URL。



如果您在 Web 瀏覽器中開啟了多個選項卡，則僅關閉 SnapCenter 瀏覽器標籤並不會將您登出 SnapCenter。若要結束與 SnapCenter 的連接，您必須透過點擊「退出」按鈕或關閉整個 Web 瀏覽器來退出 SnapCenter。

最佳實務：出於安全原因，建議您不要啟用瀏覽器來儲存您的 SnapCenter 密碼。

預設 GUI URL 是與安裝 SnapCenter Server 的伺服器上的預設連接埠 8146 的安全連線 (<https://server:8146>)。如果您在 SnapCenter 安裝期間提供了不同的伺服器端口，則將使用該端口。

對於高可用性 (HA) 部署，您必須使用虛擬叢集 IP https://Virtual_Cluster_IP_or_FQDN:8146 存取 SnapCenter。如果在 Internet Explorer (IE) 中導覽至 https://Virtual_Cluster_IP_or_FQDN:8146 時沒有看到 SnapCenter UI，則必須在每個外掛程式主機上的 IE 中將虛擬叢集 IP 位址或 FQDN 新增為受信任的網站，或者必須在每個外掛程式主機上停用 IE 增強性。有關更多信息，請參閱 ["無法從外部網路存取群集 IP 位址"](#)。

除了使用 SnapCenter GUI 之外，您還可以使用 PowerShell cmdlet 建立腳本來執行設定、備份和復原作業。每次發布 SnapCenter 時，某些 cmdlet 可能會發生變化。這 ["SnapCenter 軟體 Cmdlet 參考指南"](#) 有詳細資料。



如果您是第一次登入 SnapCenter，則必須使用安裝過程中提供的憑證登入。

步驟

1. 從本機主機桌面上的捷徑、安裝結束時提供的 URL 或 SnapCenter 管理員提供的 URL 啟動 SnapCenter。
2. 輸入使用者憑證。

若要指定以下內容...	使用以下格式之一...
網域管理員	• NetBIOS\使用者名 • 使用者名稱@UPN後綴 例如，username@netapp.com • 網域 FQDN\用戶名
本機管理員	使用者名稱

3. 如果您被指派了多個角色，請從角色方塊中選擇要用於此登入工作階段的角色。

登入後，您目前的使用者和相關角色將顯示在 SnapCenter 的右上角。

結果

將顯示“儀表板”頁面。

如果日誌記錄失敗並出現無法存取網站的錯誤，則應將 SSL 憑證對應到 SnapCenter。"了解更多"

完成後

首次以 RBAC 使用者登入 SnapCenter Server 後，重新整理資源清單。

如果您有不受信任的 Active Directory 網域並且希望 SnapCenter 支援這些網域，則必須先向 SnapCenter 註冊這些網域，然後再為不受信任網域上的使用者設定角色。"了解更多"。

如果要在 Linux 主機上執行的 SnapCenter 中新增插件主機，則應從下列位置取得校驗和檔案：`/opt/NetApp/snapcenter/SnapManagerWeb/Repository`。

從 6.0 版本開始，桌面上會建立 SnapCenter PowerShell 的捷徑。您可以使用捷徑直接存取 SnapCenter PowerShell cmdlet。

使用多重身份驗證 (MFA) 登入 SnapCenter

SnapCenter Server 支援網域帳戶的 MFA，它是活動目錄的一部分。

開始之前

您應該啟用 MFA。有關如何啟用 MFA 的信息，請參閱"啟用多重身份驗證"

關於此任務

- 僅支援 FQDN
- 工作群組和跨網域使用者無法使用 MFA 登入

步驟

1. 從本機主機桌面上的捷徑、安裝結束時提供的 URL 或 SnapCenter 管理員提供的 URL 啟動 SnapCenter。
2. 在 AD FS 登入頁面，輸入使用者名稱和密碼。

當 AD FS 頁面上顯示使用者名稱或密碼無效錯誤訊息時，您應該檢查以下內容：

- 使用者名稱或密碼是否有效
- 使用者帳戶應該存在於 Active Directory (AD) 中
- 您是否超出了 AD 中設定的最大允許嘗試次數
- AD 和 AD FS 是否已啟動並執行

修改 SnapCenter 預設 GUI 會話逾時

您可以修改 SnapCenter GUI 會話逾時期限，使其小於或大於預設逾時期限 20 分鐘。

作為一項安全功能，在預設 15 分鐘不活動時間後，SnapCenter 會警告您將在 5 分鐘內退出 GUI 工作階段。預設情況下，SnapCenter 會在 20 分鐘不活動後將您從 GUI 工作階段中登出，您必須重新登入。

步驟

1. 在左側導覽窗格中，按一下「設定」>「全域設定」。
2. 在全域設定頁面中，按一下*配置設定*。
3. 在會話逾時欄位中，輸入新的會話逾時時間（分鐘），然後按一下「儲存」。

透過停用 **SSL 3.0** 來保護**SnapCenter Web** 伺服器

出於安全目的，如果您的SnapCenter Web 伺服器上啟用了安全通訊端層 (SSL) 3.0 協議，則應在 Microsoft IIS 中停用該協定。

SSL 3.0 協定有缺陷，攻擊者可以利用這些缺陷導致連線失敗，或進行中間人攻擊並觀察您的網站與其訪客之間的加密流量。

步驟

1. 若要在SnapCenter Web 伺服器主機上啟動登錄編輯器，請按一下“開始”>“執行”，然後輸入 regedit。
2. 在登錄編輯器中，導覽至
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\。
 - 如果伺服器金鑰已經存在：
 - i. 選擇已啟用的 DWORD，然後按一下 編輯 > 修改。
 - ii. 將值變更為 0，然後按一下“確定”。
 - 如果伺服器金鑰不存在：
 - i. 按一下“編輯”>“新建”>“金鑰”，然後將金鑰命名為“伺服器”。
 - ii. 選擇新的伺服器金鑰後，按一下*編輯* > 新建 > **DWORD**。
 - iii. 將新的 DWORD 命名為 Enabled，然後輸入 0 作為值。
3. 關閉登錄編輯程式。

配置**SnapCenter**伺服器

新增並配置儲存系統

新增儲存系統

您應該設定儲存系統，使SnapCenter能夠存取ONTAP儲存、ASA r2 系統或Amazon FSx for NetApp ONTAP來執行資料保護和設定作業。

您可以新增獨立的 SVM 或由多個 SVM 組成的叢集。如果您使用的是Amazon FSx for NetApp ONTAP，則可以使用 fsxadmin 帳戶新增由多個 SVM 組成的 FSx 管理 LIF，或在SnapCenter中新增 FSx SVM。

開始之前

- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在SnapCenter GUI 中顯示為「不可用於備份」或「不在NetApp儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter不支援不同叢集上具有相同名稱的多個儲存系統。 SnapCenter支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

關於此任務

- 配置儲存系統時，您還可以啟用事件管理系統 (EMS) 和AutoSupport功能。 AutoSupport工具收集有關係統健康狀況的數據，並自動將數據發送給NetApp技術支持，使他們能夠排除系統故障。

如果啟用這些功能，當資源受到保護、還原或複製作業成功完成或操作失敗時， SnapCenter會將AutoSupport資訊傳送至儲存系統，並將 EMS 訊息傳送至儲存系統系統日誌。

- 如果您打算將快照複製到SnapMirror目標或SnapVault目標，則必須為目標 SVM 或叢集以及來源 SVM 或叢集設定儲存系統連線。



如果變更儲存系統密碼，排程作業、按需備份和復原作業可能會失敗。更改儲存系統密碼後，您可以透過點擊「儲存」標籤中的「修改」來更新密碼。

步驟

1. 在左側導覽窗格中，按一下「儲存系統」。
2. 在儲存系統頁面中，按一下*新建*。
3. 在新增儲存系統頁面中，提供以下資訊：

對於這個領域...	這樣做...
儲存系統	輸入儲存系統名稱或IP位址。  儲存系統名稱（不包括網域名稱）必須包含 15 個或更少的字符，且名稱必須可解析。若要建立名稱超過 15 個字元的儲存系統連接，可以使用 Add-SmStorageConnectionPowerShell cmdlet。  對於具有MetroCluster配置 (MCC) 的儲存系統，建議同時註冊本地集群和對等集群，以實現無中斷操作。 SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。SnapCenter支援的每個 SVM 都必須具有唯一的名稱。  將儲存連線新增至SnapCenter後，不應使用ONTAP重命名 SVM 或叢集。  如果使用短名稱或 FQDN 新增了 SVM，則它必須能夠從SnapCenter和外掛程式主機解析。
使用者名稱/密碼	輸入具有存取儲存系統所需權限的儲存使用者的憑證。
事件管理系統 (EMS) 和AutoSupport設置	如果您想要將 EMS 訊息傳送到儲存系統 syslog，或想要將AutoSupport訊息傳送到儲存系統以套用保護、完成還原作業或失敗操作，請選取對應的核取方塊。 當您勾選 向儲存系統發送失敗操作的AutoSupport通知 複選框時，也會選取 將SnapCenter伺服器事件記錄到 syslog 複選框，因為啟用AutoSupport通知需要 EMS 訊息傳遞。

4. 如果要修改指派給平台、協定、連接埠和逾時的預設值，請按一下「更多選項」。

a. 在平台中，從下拉清單中選擇一個選項。

如果 SVM 是備份關係中的輔助儲存系統，請選取 輔助 複選框。當選擇“**Secondary**”選項時，SnapCenter不會立即執行許可證檢查。

如果您已在SnapCenter中新增了 SVM，則使用者需要從下拉清單中手動選擇平台類型。

a. 在協定中，選擇在 SVM 或叢集設定期間配置的協議，通常是 HTTPS。

b. 輸入儲存系統接受的連接埠。

預設連接埠 443 通常有效。

c. 輸入停止通訊嘗試前應經過的時間（以秒為單位）。

預設值為 60 秒。

d. 如果 SVM 有多個管理接口，請勾選「首選 IP」複選框，然後輸入 SVM 連接的首選 IP 位址。

e. 點選“儲存”。

5. 點選“提交”。

結果

在儲存系統頁面中，從*類型*下拉式選單中執行下列其中一項：

- 如果要查看已新增的所有 SVM，請選擇 * ONTAP SVM *。

如果您已新增 FSx SVM，則 FSx SVM 將在此處列出。

- 如果要查看所有已新增的集群，請選擇* ONTAP集群*。

如果您已使用 fsxadmin 新增了 FSx 集群，則 FSx 集群將在此處列出。

當您按一下叢集名稱時，叢集中的所有 SVM 都會顯示在儲存虛擬機器部分。

如果使用ONTAP GUI 將新的 SVM 新增至ONTAP集群，請按一下 重新發現 查看新新增的 SVM。

完成後

叢集管理員必須在每個儲存系統節點上啟用AutoSupport，以便從SnapCenter有權存取的所有儲存系統發送電子郵件通知，方法是從儲存系統命令列執行下列命令：

```
autosupport trigger modify -node nodename -autosupport-message client.app.info  
-to enable -noteto enable
```



儲存虛擬機器 (SVM) 管理員無法存取AutoSupport。

儲存連接和憑證

在執行資料保護操作之前，您應該設定儲存連線並新增SnapCenter伺服器 and SnapCenter 插件將使用的憑證。

儲存連接

儲存連接使SnapCenter伺服器和SnapCenter插件能夠存取ONTAP儲存。設定這些連線也涉及設定AutoSupport 和事件管理系統 (EMS) 功能。

- 網域管理員或管理員群組的任何成員

指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為：

- *NetBIOS*\使用者名稱
- 域 *FQDN*\用戶名
- 用戶名@*upn*

- 本機管理員（僅適用於工作群組）

對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。

使用者名字段的有效格式為：*UserName*

- 各資源組的憑證

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

在 **Windows** 主機上設定儲存

建立和管理 **igroup**

您可以建立啟動器群組 (**igroup**) 來指定哪些主機可以存取儲存系統上的給定 LUN。您可以使用SnapCenter在 Windows 主機上建立、重新命名、修改或刪除 **igroup**。

建立 **igroup**

您可以使用SnapCenter在 Windows 主機上建立 **igroup**。當您將 **igroup** 對應到 LUN 時，**igroup** 將在建立磁碟或連線磁碟精靈中可用。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下 **Igroup**。
3. 在「啟動器群組」頁面中，按一下「新建」。
4. 在建立 **Igroup** 對話方塊中，定義 **igroup**：

在這個領域...	這樣做...
儲存系統	選擇要對應到 igroup 的 LUN 的 SVM。
主持人	選擇要在其上建立 igroup 的主機。

在這個領域...	這樣做...
群組名稱	輸入 igroup 的名稱。
發起者	選擇發起者。
類型	選擇啟動器類型：iSCSI、FCP 或混合（FCP 和 iSCSI）。

5. 如果您對輸入的內容滿意，請按一下「確定」。

SnapCenter在儲存系統上建立 igroup。

重命名 igroup

您可以使用SnapCenter重新命名現有的 igroup。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下 **Igroup**。
3. 在啟動器群組頁面中，按一下 **Storage Virtual Machine** 欄位以顯示可用 SVM 的列表，然後選擇要重新命名的 igroup 的 SVM。
4. 在 SVM 的 igroup 清單中，選擇要重新命名的 igroup，然後按一下「重新命名」。
5. 在「重新命名 igroup」對話方塊中，輸入 igroup 的新名稱，然後按一下「重新命名」。

修改 igroup

您可以使用SnapCenter將 igroup 啟動器新增至現有 igroup。建立 igroup 時，您只能新增一個主機。如果要為叢集建立 igroup，則可以修改 igroup 以將其他節點新增至該 igroup。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下 **Igroup**。
3. 在「啟動器群組」頁面中，按一下「**Storage Virtual Machine**」欄位以顯示可用 SVM 的下拉列表，然後選擇要修改的 igroup 的 SVM。
4. 在 igroup 清單中，選擇一個 igroup 並按一下「將啟動器新增至 igroup」。
5. 選擇主機。
6. 選擇啟動器並按一下“確定”。

刪除 igroup

當您不再需要某個 igroup 時，可以使用SnapCenter將其刪除。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下 **Igroup**。
3. 在「啟動器群組」頁面中，按一下「**Storage Virtual Machine**」欄位以顯示可用 SVM 的下拉列表，然後選取要刪除的 igroup 的 SVM。
4. 在 SVM 的 igroup 清單中，選擇要刪除的 igroup，然後按一下「刪除」。
5. 在「刪除 igroup」對話方塊中，按一下「確定」。

SnapCenter刪除 igroup。

建立和管理磁碟

Windows 主機將儲存系統上的 LUN 視為虛擬磁碟。您可以使用SnapCenter建立和設定 FC 連線或 iSCSI 連線的 LUN。

- SnapCenter僅支援基本磁碟。不支援動態磁碟。
- 對於 GPT，只允許一個資料分割區，對於 MBR，只允許一個主分割區，該主分割區具有一個使用 NTFS 或 CSVFS 格式化的磁碟區和一個掛載路徑。
- 支援的分割區樣式：GPT、MBR；在 VMware UEFI VM 中，僅支援 iSCSI 磁碟



SnapCenter不支援重新命名磁碟。如果重新命名由SnapCenter管理的磁碟，SnapCenter作業將不會成功。

查看主機上的磁碟

您可以使用SnapCenter檢視管理的每個 Windows 主機上的磁碟。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從*主機*下拉清單中選擇主機。

磁碟已列出。

查看叢集磁碟

您可以查看使用SnapCenter管理的叢集上的叢集磁碟。僅當您從主機下拉式選單中選擇叢集時才會顯示叢集磁碟。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。

3. 從*主機*下拉清單中選擇叢集。

磁碟已列出。

建立 iSCSI 會話

如果您使用 iSCSI 連線至 LUN，則必須在建立 LUN 之前建立 iSCSI 會話以啟用通訊。

開始之前

- 您必須已將儲存系統節點定義為 iSCSI 目標。
- 您必須已經在儲存系統上啟動了 iSCSI 服務。 ["了解更多"](#)

關於此任務

您只能在相同的 IP 版本之間建立 iSCSI 會話，無論是從 IPv6 到 IPv6，還是從 IPv4 到 IPv4。

只有當主機和目標位於相同子網路中時，才可以使用連結本機 IPv6 位址進行 iSCSI 會話管理以及主機和目標之間的通訊。

如果變更 iSCSI 啟動器的名稱，則對 iSCSI 目標的存取會受到影響。更改名稱後，您可能需要重新配置啟動器存取的目標，以便它們能夠識別新名稱。變更 iSCSI 啟動器的名稱後，必須確保重新啟動主機。

如果您的主機有多個 iSCSI 接口，一旦您使用第一個介面上的 IP 位址建立了與 SnapCenter 的 iSCSI 會話，您就無法從具有不同 IP 位址的另一個介面建立 iSCSI 會話。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「iSCSI 會話」。
3. 從「儲存虛擬機器」下拉清單中，選擇 iSCSI 目標的儲存虛擬機器 (SVM)。
4. 從「主機」下拉清單中，選擇會話的主機。
5. 點選*建立會話*。

將顯示「建立會話」精靈。

6. 在建立會話精靈中，確定目標：

在這個領域...	進入...
目標節點名稱	iSCSI 目標的節點名稱 如果存在現有的目標節點名稱，則以唯讀格式顯示該名稱。
目標入口網站位址	目標網路入口網站的IP位址
目標入口網站連接埠	目標網路入口網站的TCP端口

在這個領域...	進入...
發起者入口網站位址	發起者網路入口網站的 IP 位址

7. 當您對輸入的內容滿意時，請按一下「連線」。

SnapCenter建立 iSCSI 會話。

8. 重複此程序為每個目標建立會話。

建立 FC 連線或 iSCSI 連線的 LUN 或磁碟

Windows 主機將儲存系統上的 LUN 視為虛擬磁碟。您可以使用SnapCenter建立和設定 FC 連線或 iSCSI 連線的 LUN。

如果您想在SnapCenter之外建立和格式化磁碟，則僅支援 NTFS 和 CSVFS 檔案系統。

開始之前

- 您必須已經在儲存系統上為 LUN 建立了一個磁碟區。

該磁碟區應該僅保存 LUN，並且僅保存使用SnapCenter建立的 LUN。



除非克隆已拆分，否則您無法在SnapCenter建立的複製磁碟區上建立 LUN。

- 您必須已在儲存系統上啟動 FC 或 iSCSI 服務。
- 如果您正在使用 iSCSI，則必須與儲存系統建立 iSCSI 會話。
- 適用於 Windows 的SnapCenter插件包必須僅安裝在要建立磁碟的主機上。

關於此任務

- 除非 Windows Server 故障轉移叢集中的主機共用 LUN，否則您無法將 LUN 連線至多個主機。
- 如果使用 CSV（叢集共用磁碟區）的 Windows Server 故障轉移叢集中的主機共用 LUN，則必須在擁有該叢集群組的主機上建立磁碟。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從*主機*下拉清單中選擇主機。
4. 點選“新建”。

將開啟建立磁碟精靈。

5. 在 LUN 名稱頁面中，識別 LUN：

在這個領域...	這樣做...
儲存系統	選擇 LUN 的 SVM。
LUN 路徑	按一下「瀏覽」以選擇包含 LUN 的資料夾的完整路徑。
LUN 名稱	輸入 LUN 的名稱。
簇大小	選擇叢集的 LUN 區塊分配大小。 叢集大小取決於作業系統和應用程式。
LUN 標籤	或者，輸入 LUN 的描述性文字。

6. 在磁碟類型頁面中，選擇磁碟類型：

選擇...	如果...
專用磁碟	該 LUN 只能被一個主機存取。 忽略*資源組*欄位。
共享磁碟	LUN 由 Windows Server 故障轉移叢集中的主機共用。 在「資源組」欄位中輸入群集資源組的名稱。您只需在故障轉移群集中的一個主機上建立磁碟。
叢集共用磁碟區 (CSV)	此 LUN 由使用 CSV 的 Windows Server 故障轉移群集中的主機共用。 在「資源組」欄位中輸入群集資源組的名稱。確保在其上建立磁碟的主機是叢集群組的擁有者。

7. 在磁碟機屬性頁面中，指定磁碟機屬性：

財產	描述
自動分配掛載點	SnapCenter根據系統磁碟機自動分配磁碟區掛載點。 例如，如果您的系統磁碟機是 C:，則自動指派會在您的 C: 磁碟機下方建立磁碟區裝入點 (C:\scmnt)。共享磁碟不支援自動分配。
分配磁碟機號	將磁碟安裝到您在相鄰下拉清單中選擇的磁碟機。

財產	描述
使用卷掛載點	將磁碟安裝到您在相鄰欄位中指定的磁碟機路徑。 磁碟區安裝點的根目錄必須由您正在建立磁碟的主機擁有。
不要分配磁碟機號或磁碟區安裝點	如果您希望在 Windows 中手動安裝磁碟，請選擇此選項。
LUN大小	指定 LUN 大小；最小 150 MB。 在相鄰的下拉清單中選擇 MB、GB 或 TB。
託管此 LUN 的磁碟區使用精簡配置	精簡配置 LUN。 精簡配置一次僅分配所需的儲存空間，使 LUN 能夠有效率地成長到最大可用容量。 確保磁碟區上有足夠的可用空間來容納您認為需要的所有 LUN 儲存。
選擇分割區類型	為 GUID 分割區表選擇 GPT 分割區，或為主開機記錄選擇 MBR 分割區。 MBR 分割區可能會導致 Windows Server 故障轉移叢集中發生錯位問題。  不支援統一可擴充韌體介面 (UEFI) 分割區磁碟。

8. 在映射 LUN 頁面中，選擇主機上的 iSCSI 或 FC 啟動器：

在這個領域...	這樣做...
主持人	雙擊群集組名稱，顯示屬於該群集的主機的下拉列表，然後選擇啟動器的主機。 只有當 LUN 由 Windows Server 故障轉移叢集中的主機共用時，才會顯示此欄位。
選擇主機發起者	選擇“光纖通道”或“ iSCSI ”，然後選擇主機上的啟動器。 如果您使用具有多路徑 I/O (MPIO) 的 FC，則可以選擇多個 FC 啟動器。

9. 在「群組類型」頁面中，指定是否要將現有 igroup 對應到 LUN，還是建立新的 igroup：

選擇...	如果...
為選定的啟動器建立新的 igroup	您想要為選定的啟動器建立一個新的 igroup。
為選定的啟動器選擇現有的 igroup 或指定新的 igroup	您想要為選定的啟動器指定現有的 igroup，或使用您指定的名稱建立新的 igroup。 在 igroup name 欄位中輸入 igroup 名稱。輸入現有 igroup 名稱的前幾個字母以自動完成該欄位。

10. 在「摘要」頁面中，檢查您的選擇，然後按一下「完成」。

SnapCenter 建立 LUN 並將其連接到主機上的指定磁碟機或磁碟機路徑。

調整磁碟大小

您可以根據儲存系統需求的變化增加或減少磁碟的大小。

關於此任務

- 對於精簡配置的 LUN，ONTAP LUN 幾何大小顯示為最大大小。
- 對於厚置備 LUN，可擴充大小（磁碟區中的可用大小）顯示為最大大小。
- 具有 MBR 樣式分割的 LUN 的大小限制為 2 TB。
- 具有 GPT 樣式分割區的 LUN 的儲存系統大小限制為 16 TB。
- 在調整 LUN 大小之前製作快照是一個好主意。
- 如果您需要從調整 LUN 大小之前建立的快照中還原 LUN，SnapCenter 會自動將 LUN 調整為快照的大小。

復原操作後，必須從調整大小後建立的快照中復原調整大小後新增至 LUN 的資料。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從主機下拉清單中選擇主機。

磁碟已列出。

4. 選擇要調整大小的磁碟，然後按一下「調整大小」。
5. 在「調整磁碟大小」對話方塊中，使用滑桿工具指定磁碟的新大小，或在「大小」欄位中輸入新大小。



如果您手動輸入尺寸，則需要按一下「尺寸」欄位外部，然後才能正確啟用「收縮」或「擴充」按鈕。此外，您必須按一下 MB、GB 或 TB 來指定測量單位。

6. 當您對輸入的內容滿意時，請根據需要按一下「收縮」或「擴充」。

SnapCenter 調整磁碟大小。

連接磁碟

您可以使用連線磁碟精靈將現有 LUN 連線到主機，或重新連線已中斷連線的 LUN。

開始之前

- 您必須已在儲存系統上啟動 FC 或 iSCSI 服務。
- 如果您正在使用 iSCSI，則必須與儲存系統建立 iSCSI 會話。
- 除非 Windows Server 故障轉移叢集中的主機共用 LUN，否則您無法將 LUN 連線至多個主機。
- 如果 LUN 由使用 CSV（叢集共用磁碟區）的 Windows Server 故障轉移叢集中的主機共用，則必須連接擁有叢集群組的主機上的磁碟。
- 只需在連接磁碟的主機上安裝適用於 Windows 的插件。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從*主機*下拉清單中選擇主機。
4. 按一下“連接”。

將開啟連接磁碟精靈。

5. 在 LUN 名稱頁面中，確定要連接的 LUN：

在這個領域...	這樣做...
儲存系統	選擇 LUN 的 SVM。
LUN 路徑	按一下「瀏覽」以選擇包含 LUN 的磁碟區的完整路徑。
LUN 名稱	輸入 LUN 的名稱。
簇大小	選擇叢集的 LUN 區塊分配大小。 叢集大小取決於作業系統和應用程式。
LUN 標籤	或者，輸入 LUN 的描述性文字。

6. 在磁碟類型頁面中，選擇磁碟類型：

選擇...	如果...
專用磁碟	該 LUN 只能被一個主機存取。

選擇...	如果...
共享磁碟	LUN 由 Windows Server 故障轉移叢集中的主機共用。 您只需將磁碟連接到故障轉移群集中的一台主機。
叢集共用磁碟區 (CSV)	此 LUN 由使用 CSV 的 Windows Server 故障轉移群集中的主機共用。 確保連接到磁碟的主機是叢集群組的擁有者。

7. 在磁碟機屬性頁面中，指定磁碟機屬性：

財產	描述
自動分配	讓 SnapCenter 根據系統磁碟機自動分配磁碟區掛載點。 例如，如果您的系統磁碟機是 C:，則自動指派屬性會在您的 C: 磁碟機下方建立磁碟區裝入點 (C:\scmnt\)。共享磁碟不支援自動分配屬性。
分配磁碟機號	將磁碟安裝到您在相鄰下拉清單中選擇的磁碟機。
使用卷掛載點	將磁碟安裝到您在相鄰欄位中指定的磁碟機路徑。 磁碟區安裝點的根目錄必須由您正在建立磁碟的主機擁有。
不要分配磁碟機號或磁碟區安裝點	如果您希望在 Windows 中手動安裝磁碟，請選擇此選項。

8. 在映射 LUN 頁面中，選擇主機上的 iSCSI 或 FC 啟動器：

在這個領域...	這樣做...
主持人	雙擊叢集群組名稱，顯示屬於該叢集的主機的下拉列表，然後選擇啟動器的主機。 只有當 LUN 由 Windows Server 故障轉移叢集中的主機共用時，才會顯示此欄位。
選擇主機發起者	選擇“光纖通道”或“iSCSI”，然後選擇主機上的啟動器。 如果您使用具有 MPIO 的 FC，則可以選擇多個 FC 啟動器。

9. 在「群組類型」頁面中，指定是否要將現有 igroup 對應到 LUN 或建立新的 igroup：

選擇...	如果...
為選定的啟動器建立新的 igroup	您想要為選定的啟動器建立一個新的 igroup。
為選定的啟動器選擇現有的 igroup 或指定新的 igroup	您想要為選定的啟動器指定現有的 igroup，或使用您指定的名稱建立新的 igroup。 在 igroup name 欄位中輸入 igroup 名稱。輸入現有 igroup 名稱的前幾個字母以自動完成該欄位。

10. 在「摘要」頁面中，檢查您的選擇並按一下「完成」。

SnapCenter將 LUN 連接到主機上的指定磁碟機或磁碟機路徑。

斷開磁碟

您可以將 LUN 與主機斷開連接，而不會影響 LUN 的內容，但有一個例外：如果在克隆分離之前斷開連接，則會丟失克隆的內容。

開始之前

- 確保 LUN 未被任何應用程式使用。
- 確保 LUN 未被監控軟體監控。
- 如果 LUN 是共享的，請確保從 LUN 中刪除叢集資源相依性，並驗證叢集中的所有節點是否都已開啟電源、正常運作且可供SnapCenter使用。

關於此任務

如果中斷SnapCenter建立的FlexClone磁碟區中的某個 LUN 且該磁碟區上沒有連接任何其他 LUN，SnapCenter會刪除該磁碟區。在斷開 LUN 之前，SnapCenter會顯示一則訊息，警告您FlexClone磁碟區可能會被刪除。

為避免自動刪除FlexClone磁碟區，您應該在斷開最後一個 LUN 之前重新命名該磁碟區。重命名卷時，請確保更改多個字符，而不僅僅是名稱中的最後一個字符。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從*主機*下拉清單中選擇主機。

磁碟已列出。

4. 選擇要斷開的磁碟，然後按一下“斷開連接”。
5. 在「斷開磁碟」對話方塊中，按一下「確定」。

SnapCenter斷開磁碟連線。

刪除磁碟

當您不再需要磁碟時，可以將其刪除。刪除磁碟後，將無法復原。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「磁碟」。
3. 從*主機*下拉清單中選擇主機。

磁碟已列出。

4. 選擇要刪除的磁碟，然後按一下“刪除”。
5. 在「刪除磁碟」對話方塊中，按一下「確定」。

SnapCenter刪除磁碟。

建立和管理 SMB 共享

若要在儲存虛擬機器 (SVM) 上設定 SMB3 共用，您可以使用SnapCenter使用者介面或 PowerShell cmdlet。

*最佳實踐：*建議使用 cmdlet，因為它使您能夠利用SnapCenter提供的範本來自動化共享配置。

模板概括了磁碟區和共享配置的最佳實踐。您可以在 Windows 版SnapCenter插件包的安裝資料夾中的 Templates 資料夾中找到這些範本。



如果您願意，您可以按照提供的模型建立自己的模板。在建立自訂範本之前，您應該查看 cmdlet 文件中的參數。

建立 SMB 共享

您可以使用SnapCenter共用頁面在儲存虛擬機器 (SVM) 上建立 SMB3 共用。

您不能使用SnapCenter備份 SMB 共用上的資料庫。SMB 支援僅限於設定。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「共享」。
3. 從「儲存虛擬機器」下拉清單中選擇 SVM。
4. 點選“新建”。

“新共享”對話方塊開啟。

5. 在新共享對話方塊中，定義共享：

在這個領域...	這樣做...
描述	輸入共享的描述性文字。
共享名稱	輸入共享名稱，例如 test_share。 您輸入的共享名稱也將用作磁碟區名稱。 共享名稱： • 必須是 UTF-8 字串。 • 不得包含以下字符：從 0x00 到 0x1F（含）的控製字符、0x22（雙引號）以及特殊字符 \ / [] : (vertical bar) < > + = ; , ?
分享路徑	• 按一下該欄位以輸入新的檔案系統路徑，例如 /。 • 雙擊該欄位以從現有檔案系統路徑清單中進行選擇。

6. 如果您對輸入的內容滿意，請按一下「確定」。

SnapCenter在 SVM 上建立 SMB 共用。

刪除 **SMB** 共享

當您不再需要 SMB 共用時，可以將其刪除。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「共享」。
3. 在共用頁面中，按一下「儲存虛擬機器」欄位以顯示下拉式選單，其中包含可用儲存虛擬機器 (SVM) 的列表，然後選擇要刪除的共用的 SVM。
4. 從 SVM 上的共享清單中，選擇要刪除的共享，然後按一下「刪除」。
5. 在「刪除共享」對話方塊中，按一下「確定」。

SnapCenter從 SVM 中刪除 SMB 共用。

回收儲存系統上的空間

儘管 NTFS 在檔案被刪除或修改時會追蹤 LUN 上的可用空間，但它不會將新資訊報告給儲存系統。您可以在適用於 Windows 主機的插件上執行空間回收 PowerShell cmdlet，以確保新釋放的區塊在儲存中標記為可用。

如果您在遠端插件主機上執行 cmdlet，則必須執行 SnapCenterOpen-SMConnection cmdlet 才能開啟

與SnapCenter伺服器的連線。

開始之前

- 您必須確保在執行復原作業之前空間回收過程已完成。
- 如果 LUN 由 Windows Server 故障轉移叢集中的主機共用，則必須在擁有該叢集群組的主機上執行空間回收。
- 為了獲得最佳儲存效能，您應該盡可能頻繁地執行空間回收。

您應該確保已掃描整個 NTFS 檔案系統。

關於此任務

- 空間回收非常耗時且佔用大量 CPU 資源，因此最好在儲存系統和 Windows 主機使用率較低時執行此操作。
- 空間回收幾乎可以回收所有可用空間，但並非 100%。
- 您不應在執行空間回收的同時執行磁碟碎片整理。

這樣做會減慢回收過程。

步

在應用程式伺服器 PowerShell 命令提示字元下，輸入以下命令：

```
Invoke-SdHostVolumeSpaceReclaim -Path drive_path
```

drive_path 是對應到 LUN 的磁碟機路徑。

使用 **PowerShell cmdlet** 設定存儲

如果您不想使用SnapCenter GUI 執行主機設定和空間回收作業，則可以使用 PowerShell cmdlet。您可以直接使用 cmdlet 或將其新增至腳本。

如果您在遠端插件主機上執行 cmdlet，則必須執行SnapCenter Open-SMConnection cmdlet 來開啟與SnapCenter伺服器的連線。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

如果因為從伺服器移除SnapDrive for Windows 而導致SnapCenter PowerShell cmdlet 損壞，請參閱 ["卸載SnapDrive for Windows 時SnapCenter cmdlet 損壞"](#)。

在 **VMware** 環境中設定存儲

您可以在 VMware 環境中使用適用於 Microsoft Windows 的SnapCenter外掛程式來建立和管理 LUN 以及管理快照。

支援的 **VMware** 客戶作業系統平台

- 支援的 Windows Server 版本

- Microsoft 群集配置

使用 Microsoft iSCSI Software Initiator 時，VMware 上最多支援 16 個節點，使用 FC 時最多支援兩個節點

- RDM LUN

對於普通 RDMS，最多支援 56 個 RDM LUN，配備四個 LSI Logic SCSI 控制器；對於 Windows 配置，VMware VM MSCS 盒對盒插件最多支援 42 個 RDM LUN，配備三個 LSI Logic SCSI 控制器

支援 VMware ParaVirtual SCSI 控制器。RDM 磁碟上可支援 256 個磁碟。

有關受支援版本的最新信息，請參閱 ["NetApp互通性表工具"](#)。

VMware ESXi 伺服器相關限制

- 不支援使用 ESXi 憑證在虛擬機器上的 Microsoft 叢集上安裝適用於 Windows 的插件。

在叢集虛擬機器上安裝適用於 Windows 的插件時，您應該使用 vCenter 憑證。

- 所有叢集節點必須對同一個叢集磁碟使用相同的目標 ID（在虛擬 SCSI 適配器上）。
- 當您在適用於 Windows 的插件之外建立 RDM LUN 時，必須重新啟動插件服務以使其能夠識別新建立的磁碟。
- 您無法在 VMware 客戶作業系統上同時使用 iSCSI 和 FC 啟動器。

SnapCenter RDM 操作所需的最低 vCenter 權限

您應該在主機上擁有下列 vCenter 權限才能在來賓作業系統中執行 RDM 操作：

- 資料儲存：刪除文件
- 主機：配置 > 儲存分區配置
- 虛擬機器：配置

您必須將這些權限指派給 Virtual Center Server 等級的角色。您指派了這些權限的角色不能指派給沒有 root 權限的任何使用者。

指派這些權限後，您可以在來賓作業系統上安裝適用於 Windows 的插件。

管理 Microsoft 叢集中的 FC RDM LUN

您可以使用適用於 Windows 的插件來管理使用 FC RDM LUN 的 Microsoft 群集，但必須先在插件外部建立共用 RDM 仲裁和共用存儲，然後將磁碟新增至叢集中的虛擬機器。

從 ESXi 5.5 開始，您也可以使用 ESX iSCSI 和 FCoE 硬體來管理 Microsoft 叢集。Windows 外掛程式包含對 Microsoft 叢集的開箱即用支援。

要求

當您滿足特定的配置要求時，適用於 Windows 的插件可為 Microsoft 群集提供支持，這些群集使用屬於兩個不同 ESX 或 ESXi 伺服器的兩個不同虛擬機器上的 FC RDM LUN，也稱為跨箱群集。

- 虛擬機器 (VM) 必須執行相同的 Windows Server 版本。
- 每個 VMware 父主機的 ESX 或 ESXi 伺服器版本必須相同。
- 每個父主機必須至少有兩個網路介面卡。
- 兩個 ESX 或 ESXi 伺服器之間必須共用至少一個 VMware 虛擬機器檔案系統 (VMFS) 資料儲存。
- VMware 建議在 FC SAN 上建立共用資料儲存。

如果需要，也可以透過 iSCSI 建立共享資料儲存。

- 共享 RDM LUN 必須處於實體相容模式。
- 必須在 Windows 外掛程式之外手動建立共享 RDM LUN。

您不能將虛擬磁碟用於共享儲存。

- 必須在實體相容模式下在叢集中的每個虛擬機器上設定 SCSI 控制器：

Windows Server 2008 R2 要求您在每個虛擬機器上設定 LSI Logic SAS SCSI 控制器。如果僅存在一個相同類型的控制器且該控制器已連接到 C: 驅動器，則共用 LUN 無法使用現有的 LSI Logic SAS 控制器。

VMware Microsoft 叢集不支援半虛擬化類型的 SCSI 控制器。



當您在實體相容模式下將 SCSI 控制器新增至虛擬機器上的共用 LUN 時，您必須在 VMware Infrastructure Client 中選擇 原始裝置對應 (RDM) 選項，而不是 建立新磁碟 選項。

- Microsoft 虛擬機器叢集不能成為 VMware 叢集的一部分。
- 在屬於 Microsoft 叢集的虛擬機器上安裝適用於 Windows 的插件時，必須使用 vCenter 憑證，而非 ESX 或 ESXi 憑證。
- Windows 外掛程式無法使用來自多個主機的啟動器建立單一 igroup。

在建立將用作共用叢集磁碟的 RDM LUN 之前，必須在儲存控制器上建立包含所有 ESXi 主機的啟動器的 igroup。

- 確保使用 FC 啟動器在 ESXi 5.0 上建立 RDM LUN。

建立 RDM LUN 時，將使用 ALUA 建立啟動器群組。

限制

Windows 外掛程式支援在屬於不同 ESX 或 ESXi 伺服器的不同虛擬機器上使用 FC/iSCSI RDM LUN 的 Microsoft 叢集。



ESX 5.5i 之前的版本不支援此功能。

- Windows 插件不支援 ESX iSCSI 和 NFS 資料儲存上的叢集。
- Windows 外掛程式不支援叢集環境中的混合啟動器。

啟動器必須是 FC 或 Microsoft iSCSI，但不能同時是兩者。

- Microsoft 叢集中的共用磁碟不支援 ESX iSCSI 啟動器和 HBA。
- 如果虛擬機器是 Microsoft 叢集的一部分，則適用於 Windows 的外掛程式不支援使用 vMotion 進行虛擬機器遷移。
- Windows 外掛程式不支援 Microsoft 群集中虛擬機器上的 MPIO。

建立共享 FC RDM LUN

在使用 FC RDM LUN 在 Microsoft 叢集中的節點之間共用儲存體之前，您必須先建立共用仲裁磁碟和共用儲存磁碟，然後將它們新增至叢集中的兩個虛擬機器。

共享磁碟不是使用 Windows 插件建立的。您應該建立共用 LUN，然後將其新增至叢集中的每個虛擬機器。有關信息，請參閱 ["跨實體主機叢集虛擬機"](#)。

新增基於 SnapCenter Standard 控制器的許可證

如果您使用 FAS、AFF 或 ASA 儲存控制器，則需要基於 SnapCenter Standard 控制器的授權。

基於控制器的授權具有以下特點：

- 購買 Premium 或 Flash Bundle 即可獲得 SnapCenter Standard 權利（不包含在基礎包中）
- 無限儲存使用
- 使用 ONTAP 系統管理器或 ONTAP CLI 直接加入到 FAS、AFF 或 ASA 儲存控制器。



您無需在 SnapCenter 使用者介面中輸入基於 SnapCenter 控制器的授權的任何授權資訊。

- 鎖定到控制器的序號

有關所需許可證的信息，請參閱 ["SnapCenter 許可證"](#)。

步驟 1：驗證是否安裝了 SnapManager Suite 許可證

您可以使用 SnapCenter 使用者介面檢查 FAS、AFF 或 ASA 主儲存系統上是否安裝了 SnapManager Suite 許可證，並確定哪些系統需要許可證。SnapManager Suite 授權僅適用於主儲存系統上的 FAS、AFF 和 ASA SVM 或叢集。



如果您的控制器上已有 SnapManager Suite 許可證，SnapCenter 會自動提供基於標準控制器的授權授權。SnapManager Suite 授權和基於 SnapCenter Standard 控制器的授權這兩個名稱可以互換使用，但它們指的是同一個授權。

步驟

1. 在左側導覽窗格中，選擇 ***儲存系統***。
2. 在「儲存系統」頁面中，從「類型」下拉式選單中選擇是否要查看已新增的所有 SVM 或叢集：
 - 若要查看已新增的所有 SVM，請選擇 *** ONTAP SVM***。
 - 若要查看已新增的所有集群，請選擇 **「ONTAP 集群」**。

當您選擇叢集名稱時，叢集中的所有 SVM 都會顯示在 Storage Virtual Machines 部分。

3. 在儲存連接清單中，找到控制器許可證列。

控制器許可證列顯示以下狀態：

-  表示SnapManager Suite 許可證已安裝在FAS、AFF或ASA主儲存系統上。
-  表示FAS、AFF或ASA主儲存系統上未安裝SnapManager Suite 授權。
- 不適用表示SnapManager Suite 授權不適用，因為儲存控制器位於Amazon FSx for NetApp ONTAP、Cloud Volumes ONTAP、ONTAP Select或輔助儲存平台。

第 2 步：識別控制器上安裝的許可證

您可以使用ONTAP命令列查看控制器上安裝的所有授權。您應該是FAS、AFF或ASA系統上的叢集管理員。



控制器將基於SnapCenter Standard 控制器的授權顯示為 SnapManagerSuite 授權。

步驟

1. 使用ONTAP命令列登入NetApp控制器。
2. 輸入 license show 命令，然後查看輸出以查看是否已安裝 SnapManagerSuite 授權。

範例輸出

```
cluster1::> license show
(system license show)

Serial Number: 1-80-0000xx
Owner: cluster1
Package          Type      Description          Expiration
-----
Base             site     Cluster Base License -

Serial Number: 1-81-000000000000000000000000xx
Owner: cluster1-01
Package          Type      Description          Expiration
-----
NFS              license   NFS License         -
CIFS             license   CIFS License        -
iSCSI            license   iSCSI License       -
FCP              license   FCP License         -
SnapRestore      license   SnapRestore License -
SnapMirror       license   SnapMirror License  -
FlexClone        license   FlexClone License   -
SnapVault        license   SnapVault License   -
SnapManagerSuite license   SnapManagerSuite License -
```

在範例中，已安裝 SnapManagerSuite 許可證，因此不需要額外的SnapCenter許可操作。

步驟 3：檢索控制器序號

使用ONTAP命令列取得控制器序號。您必須是FAS、AFF或ASA系統上的叢集管理員才能取得基於控制器的許可證序號。

步驟

1. 使用ONTAP命令列登入控制器。
2. 輸入 `system show -instance` 命令，然後查看輸出以找到控制器序號。

範例輸出

```
cluster1::> system show -instance
```

```
Node: fasxxxx-xx-xx-xx
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234511
Asset Tag: -
Uptime: 143 days 23:46
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false

Node: fas8080-41-42-02
Owner:
Location: RTP 1.5
Model: FAS8080
Serial Number: 123451234512
Asset Tag: -
Uptime: 144 days 00:08
NVRAM System ID: xxxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. 記錄序號。

步驟 4：檢索基於控制器的許可證的序號

如果您使用的是FAS、ASA或AFF存儲，則可以先從NetApp支援站點擷取基於SnapCenter控制器的許可證，然後再使用ONTAP命令列進行安裝。

開始之前

- 您應該擁有有效的NetApp支援網站登入憑證。

如果您沒有輸入有效的憑證，系統將不會傳回任何有關您搜尋的資訊。

- 您應該有控制器序號。

步驟

1. 登入 ["NetApp支援站點"](#)。
2. 導覽至*系統* > 軟體許可證。
3. 在選擇標準區域，確保選擇了序號（位於裝置背面），輸入控制器序號，然後選擇*Go!*。

Software Licenses

Selection Criteria

Choose a method by which to search

► Enter Value:

Enter the Cluster Serial Number value without dashes.

- OR -

► Show Me All: For Company:

顯示指定控制器的許可證清單。

4. 找到並記錄SnapCenter Standard 或 SnapManagerSuite 許可證。

步驟 5：新增基於控制器的許可證

當您使用FAS、AFF或ASA系統並且擁有SnapCenter Standard 或 SnapManagerSuite 授權時，您可以使用ONTAP命令列新增基於SnapCenter控制器的授權。

開始之前

- 您應該是FAS、AFF或ASA系統上的叢集管理員。
- 您應該擁有SnapCenter Standard 或 SnapManagerSuite 授權。

關於此任務

如果您想使用FAS、AFF或ASA儲存試用安裝SnapCenter，您可以取得 Premium Bundle 評估授權以安裝在控制器上。

如果您想嘗試安裝SnapCenter，您應該聯絡您的銷售代表以取得 Premium Bundle 評估授權以安裝在您的控制器上。

步驟

1. 使用ONTAP命令列登入NetApp叢集。
2. 新增 SnapManagerSuite 許可證金鑰：

```
system license add -license-code license_key
```

此命令在管理員權限層級可用。

3. 驗證是否已安裝 SnapManagerSuite 授權：

```
license show
```

步驟 6：刪除試用許可證

如果您正在使用基於控制器的SnapCenter標準許可證，並且需要刪除基於容量的試用許可證（序號以「50」結尾），則應使用 MySQL 命令手動刪除試用許可證。無法使用SnapCenter使用者介面刪除試用許可證。



只有當您使用基於SnapCenter Standard 控制器的授權時才需要手動刪除試用授權。

步驟

1. 在SnapCenter伺服器上，開啟 PowerShell 視窗以重設 MySQL 密碼。
 - a. 執行 Open-SmConnection cmdlet 為 SnapCenterAdmin 帳戶與SnapCenter伺服器建立連線。
 - b. 執行 Set-SmRepositoryPassword 重設 MySQL 密碼。

有關 cmdlet 的信息，請參閱 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

2. 開啟命令提示字元並執行mysql -u root -p登入MySQL。

MySQL 提示您輸入密碼。輸入您在重設密碼時提供的憑證。

3. 從資料庫中刪除試用許可證：

```
use nsm;DELETE FROM nsm_License WHERE nsm_License_Serial_Number='510000050';
```

配置高可用性

配置SnapCenter伺服器以實現高可用性

為了支援在 Windows 或 Linux 上執行的SnapCenter中的高可用性 (HA)，您可以安裝 F5 負載平衡器。F5 使SnapCenter伺服器能夠支援位於相同位置的最多兩台主機的主動-被動配置。若要在SnapCenter中使用 F5 負載平衡器，您應該設定SnapCenter伺服器並設定 F5 負載平衡器。

您也可以設定網路負載平衡 (NLB) 來設定SnapCenter高可用性。您應該在SnapCenter安裝之外手動配置 NLB 以實現高可用性。

對於雲端環境，您可以使用 Amazon Web Services (AWS) 彈性負載平衡 (ELB) 和 Azure 負載平衡器來設定高可用性。

使用 F5 配置高可用性

有關使用 F5 負載平衡器設定 SnapCenter 伺服器以實現高可用性的說明，請參閱 ["如何使用 F5 負載平衡器配置 SnapCenter 伺服器以實現高可用性"](#)。

您必須是 SnapCenter 伺服器上本機管理員群組的成員（除了指派 SnapCenterAdmin 角色），才能使用下列 cmdlet 新增和刪除 F5 叢集：

- 新增 SmServerCluster
- 新增 SmServer
- 刪除-SmServerCluster

有關更多信息，請參閱 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

附加資訊

- 安裝並配置 SnapCenter 以實現高可用性後，編輯 SnapCenter 桌面捷徑以指向 F5 叢集 IP。
- 如果 SnapCenter 伺服器之間發生故障轉移，並且還存在現有的 SnapCenter 會話，則必須關閉瀏覽器並再次登入 SnapCenter。
- 在負載平衡器設定（NLB 或 F5）中，如果新增由 NLB 或 F5 主機部分解析的主機，如果 SnapCenter 主機無法連線到該主機，則 SnapCenter 主機頁面會在主機關閉和運作狀態之間經常切換。要解決此問題，您應該確保兩個 SnapCenter 主機都能夠解析 NLB 或 F5 主機中的主機。
- 應在所有主機上執行 MFA 設定的 SnapCenter 指令。依賴方設定應使用 F5 叢集詳細資訊在 Active Directory 聯合驗證服務 (AD FS) 伺服器中完成。啟用 MFA 後，主機級 SnapCenter UI 存取將被阻止。
- 在故障轉移期間，稽核日誌設定不會反映在第二台主機上。因此，當 F5 被動主機變成主動主機時，您應該手動重複稽核日誌設定。

使用網路負載平衡 (NLB) 配置高可用性

您可以設定網路負載平衡 (NLB) 來設定 SnapCenter 高可用性。您應該在 SnapCenter 安裝之外手動配置 NLB 以實現高可用性。

有關如何使用 SnapCenter 配置網路負載平衡 (NLB) 的信息，請參閱 ["如何使用 SnapCenter 配置 NLB"](#)。

使用 AWS Elastic Load Balancing (ELB) 配置高可用性

您可以在 Amazon Web Services (AWS) 中設定高可用性 SnapCenter 環境，方法是在不同的可用區域 (AZ) 中設定兩個 SnapCenter 伺服器並對其進行設定以實現自動故障轉移。此架構包括虛擬專用 IP 位址、路由表以及主備 MySQL 資料庫之間的同步。

步驟

1. 在 AWS 中配置虛擬專用覆蓋 IP。有關信息，請參閱 ["配置虛擬專用覆蓋 IP"](#)。
2. 準備 Windows 主機
 - a. 強制 IPv4 優先權高於 IPv6：
 - 位置：HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
 - 鍵：DisabledComponents
 - 類型：REG_DWORD

- 值：0x20
 - b. 確保完全限定網域名稱可以透過 DNS 或本機設定解析為 IPv4 位址。
 - c. 確保您沒有配置系統代理程式。
 - d. 當使用沒有 Active Directory 的設定且伺服器不在一個網域中時，請確保兩個 Windows Server 上的管理員密碼相同。
 - e. 在兩個 Windows 伺服器上新增虛擬 IP。
3. 建立 SnapCenter 叢集。
 - a. 啟動 Powershell 並連線到 SnapCenter。
`Open-SmConnection`
 - b. 建立集群。
`Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip> -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator`
 - c. 新增輔助伺服器。
`Add-SmServer -ServerName <server_name> -ServerIP <server_ip> -CleanUpSecondaryServer -Verbose -Credential administrator`
 - d. 取得高可用性詳細資訊。
`Get-SmServerConfig`
 4. 建立 Lambda 函數以在虛擬私人 IP 端點不可用時調整路由表，並由 AWS CloudWatch 監控。有關信息，請參閱 ["建立 Lambda 函數"](#)。
 5. 在 CloudWatch 中建立一個監視器來監控 SnapCenter 端點的可用性。如果端點無法訪問，則配置警報以觸發 Lambda 函數。Lambda 函數會調整路由表以將流量重新導向至活動的 SnapCenter 伺服器。有關信息，請參閱 ["創建合成金絲雀"](#)。
 6. 使用步驟函數實作工作流程作為 CloudWatch 監控的替代方案，從而提供更短的故障轉移時間。此工作流程包括一個用於測試 SnapCenter URL 的 Lambda 探測函數、一個用於儲存故障計數的 DynamoDB 表以及 Step Function 本身。
 - a. 使用 lambda 函數探測 SnapCenter URL。有關信息，請參閱 ["建立 Lambda 函數"](#)。
 - b. 建立一個 DynamoDB 表來儲存兩次 Step Function 迭代之間的失敗計數。有關信息，請參閱 ["DynamoDB 表格入門"](#)。
 - c. 建立步進函數。有關信息，請參閱 ["Step Function 文檔"](#)。
 - d. 測試單一步驟。
 - e. 測試完整功能。
 - f. 建立 IAM 角色並調整權限以允許執行 Lambda 函數。
 - g. 建立計劃以觸發 Step Function。有關信息，請參閱 ["使用 Amazon EventBridge Scheduler 啟動 Step Functions"](#)。

使用 **Azure** 負載平衡器配置高可用性

您可以使用 Azure 負載平衡器設定高可用性 SnapCenter 環境。

步驟

1. 使用 Azure 入口網站在規模集中建立虛擬機器。Azure 虛擬機器規模集可讓您建立和管理一組負載平衡的虛擬機器。虛擬機器實例的數量可以根據需求或定義的時間表自動增加或減少。有關信息，請參閱 ["使用 Azure 入口網站在規模集中建立虛擬機"](#)。

2. 配置虛擬機器後，登入 VM 集中的每個虛擬機器並在兩個節點上安裝 SnapCenter Server。
3. 在主機 1 中建立叢集。
`Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>`
4. 新增輔助伺服器。
`Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>`
5. 取得高可用性詳細資訊。
`Get-SmServerConfig`
6. 如果需要，重建輔助主機。
`Set-SmRepositoryConfig -RebuildSlave -Verbose`
7. 故障轉移到第二台主機。
`Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose`

== 從 NLB 切換到 F5 以實現高可用性

您可以將 SnapCenter HA 設定從網路負載平衡 (NLB) 變更為使用 F5 負載平衡器。

步驟

1. 使用 F5 設定 SnapCenter 伺服器以實現高可用性。 ["了解更多"](#)。
2. 在 SnapCenter 伺服器主機上，啟動 PowerShell。
3. 使用 `Open-SmConnection` cmdlet 啟動會話，然後輸入您的憑證。
4. 使用 `Update-SmServerCluster` cmdlet 更新 SnapCenter 伺服器以指向 F5 叢集 IP 位址。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

SnapCenter MySQL 儲存庫的高可用性

MySQL 複製是 MySQL 伺服器的功能，它可讓您將資料從一個 MySQL 資料庫伺服器（主伺服器）複製到另一個 MySQL 資料庫伺服器（從伺服器）。SnapCenter 僅在兩個啟用網路負載平衡 (NLB) 的節點上支援 MySQL 複製以實現高可用性。

SnapCenter 在主儲存庫上執行讀取或寫入操作，並在主儲存庫發生故障時將其連接路由至從屬儲存庫。然後從屬儲存庫將成為主儲存庫。SnapCenter 還支援反向複製，該功能僅在故障轉移期間啟用。

如果要使用 MySQL 高可用性 (HA) 功能，則必須在第一個節點上設定網路負載平衡器 (NLB)。MySQL 儲存庫會作為安裝的一部分安裝在此節點上。在第二個節點上安裝 SnapCenter 時，您必須加入第一個節點的 F5 並在第二個節點上建立 MySQL 儲存庫的副本。

SnapCenter 提供 `Get-SmRepositoryConfig` 和 `Set-SmRepositoryConfig` PowerShell cmdlet 來管理 MySQL 複製。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您

也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

您必須了解與 MySQL HA 功能相關的限制：

- 兩個節點以上不支援 NLB 和 MySQL HA。
- 不支援從 SnapCenter 獨立安裝切換到 NLB 安裝或反之亦然，也不支援從 MySQL 獨立安裝切換到 MySQL HA。
- 如果從屬儲存庫資料與主儲存庫資料不同步，則不支援自動故障轉移。

您可以使用 `Set-SmRepositoryConfig` cmdlet 啟動強制故障轉移。

- 當啟動故障轉移時，正在執行的作業可能會失敗。

如果由於 MySQL 伺服器或 SnapCenter 伺服器關閉而發生故障轉移，則任何正在執行的作業都可能失敗。故障轉移到第二個節點後，所有後續作業均成功運作。

有關配置高可用性的信息，請參閱 ["如何使用 SnapCenter 配置 NLB 和 ARR"](#)。

配置基於角色的存取控制 (RBAC)

創建角色

除了使用現有的 SnapCenter 角色之外，您還可以建立自己的角色並自訂權限。

若要建立自己的角色，必須以「SnapCenterAdmin」角色登入。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「角色」。
3. 點選 .
4. 為新角色指定名稱和描述。



使用者名稱和群組名稱中只能使用以下特殊字元：空格（ ）、連字號（-）、底線（_）和冒號（:）。

5. 選擇“此角色的所有成員都可以看到其他成員的物件”，使該角色的其他成員在刷新資源清單後可以看到磁碟區和主機等資源。

如果您不希望該角色的成員看到指派給其他成員的對象，則應取消選取此選項。



啟用此選項後，如果使用者與建立物件或資源的使用者屬於相同角色，則無需為使用者指派對物件或資源的存取權限。

6. 在「權限」頁面中，選擇要指派給角色的權限，或按一下「全選」將所有權限授予角色。
7. 點選“提交”。

使用安全登入指令新增NetApp ONTAP RBAC 角色

當您的儲存系統執行叢集ONTAP時，您可以使用安全登入指令新增NetApp ONTAP RBAC 角色。

開始之前

- 確定您要執行的任務以及執行這些任務所需的權限。
- 授予命令和/或命令目錄權限。

每個命令/命令目錄有兩種存取等級：全部存取和唯讀。

您必須始終先指派所有存取權限。

- 為使用者指派角色。
- 根據您的SnapCenter插件是連接到整個叢集的叢集管理員 IP 還是直接連接到叢集內的 SVM 來確定您的配置。

關於此任務

為了簡化儲存系統上這些角色的配置，您可以使用NetApp ONTAP工具的 RBAC 使用者建立器，該工具發佈在NetApp社群論壇上。

該工具會自動正確設定ONTAP權限。例如，NetApp ONTAP的 RBAC User Creator 工具會自動以正確的順序新增權限，以便所有存取權限會先出現。如果您先新增唯讀權限，然後新增所有存取權限，ONTAP會將所有存取權限標記為重複並忽略它們。



如果您稍後升級SnapCenter或ONTAP，則應重新執行NetApp ONTAP的 RBAC User Creator 工具來更新您先前建立的使用者角色。為早期版本的SnapCenter或ONTAP所建立的使用者角色無法與升級後的版本正常搭配使用。當您重新運行該工具時，它會自動處理升級。您不需要重新建立角色。

有關設定ONTAP RBAC 角色的更多信息，請參閱 ["ONTAP 9 管理員驗證和 RBAC 電源指南"](#)。

步驟

1. 在儲存系統上，輸入以下指令以建立新角色：

```
security login role create <role_name> -cmddirname "command" -access all  
-vserver <svm_name>
```

- svm_name 是 SVM 的名稱。如果將其留空，則預設為叢集管理員。
- role_name 是您為角色指定的名稱。
- 指令是ONTAP功能。



您必須對每個權限重複此命令。請記住，全訪問命令必須在只讀命令之前列出。

有關權限清單的信息，請參閱["用於建立角色和分配權限的ONTAP CLI 命令"](#)。

2. 輸入以下命令建立使用者名稱：

```
security login create -username <user_name\> -application ontapi -authmethod  
<password\> -role <name_of_role_in_step_1\> -vserver <svm_name\> -comment  
"user_description"
```

- `user_name` 是您正在建立的使用者的名稱。
- `<password>` 是您的密碼。如果您未指定密碼，系統會提示您輸入密碼。
- `svm_name` 是 SVM 的名稱。

3. 透過輸入以下命令將角色指派給使用者：

```
security login modify username <user_name\> -vserver <svm_name\> -role  
<role_name\> -application ontapi -application console -authmethod <password\>
```

- `<user_name>` 是您在步驟 2 中建立的使用者的名稱。此命令允許您修改使用者以將其與角色關聯。
- `<svm_name>` 是 SVM 的名稱。
- `<role_name>` 是您在步驟 1 中建立的角色的名稱。
- `<password>` 是您的密碼。如果您未指定密碼，系統會提示您輸入密碼。

4. 輸入以下命令驗證使用者是否已正確建立：

```
security login show -vserver <svm_name\> -user-or-group-name <user_name\>
```

`user_name` 是您在步驟 3 中建立的使用者的名稱。

建立具有最低權限的 **SVM** 角色

在 ONTAP 中為新的 SVM 使用者建立角色時，必須執行幾個 ONTAP CLI 指令。如果您在 ONTAP 中設定 SVM 以與 SnapCenter 一起使用且不想使用 `vsadmin` 角色，則需要此角色。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

```
security login role create -vserver <svm_name\> - role <SVM_Role_Name\>  
-cmddirname <permission\>
```



您應該對每個權限重複此命令。

2. 建立一個使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <svm_name\> -application  
ontapi -authmethod password -role <SVM_Role_Name\>
```

3. 解除用戶鎖定。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

您應該執行幾個ONTAP CLI 命令來建立 SVM 角色並指派權限。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "network interface" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "version" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume clone split stop" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume snapshot restore-file" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver" -access readonly
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver export-policy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "vserver iscsi" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume clone split status" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume managed-feature" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem map" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname

```
"nvme subsystem delete" -access all
```

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all

為ASA r2 系統建立 SVM 角色

您必須執行幾個ONTAP CLI 命令才能在ASA r2 系統中為新的 SVM 使用者建立角色。如果您在ASA r2 系統中設定 SVM 以與SnapCenter一起使用且不想使用 vsadmin 角色，則需要此角色。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

```
security login role create -vserver <svm_name\>- role <SVM_Role_Name\>
-cmddirname <permission\>
```



您應該對每個權限重複此命令。

2. 建立一個使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <svm_name\> -application
http -authmethod password -role <SVM_Role_Name\>
```

3. 解除用戶鎖定。

```
security login unlock -user <user_name\> -vserver <svm_name\>
```

用於建立 SVM 角色和分配權限的ONTAP CLI 命令

您應該執行幾個ONTAP CLI 命令來建立 SVM 角色並指派權限。

- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror list-destinations" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job history show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "job show" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "job stop" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname


```

"lun offline" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun online" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun resize" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun serial" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "lun show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "network interface" -access readonly

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy add-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy modify-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy remove-rule" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror policy show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror restore" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "snapmirror show-history" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror update" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "snapmirror update-ls-set" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "version" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume create" -access all

```

- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file clone create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume file show-disk-usage" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume offline" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume online" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree modify" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume qtree show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume restrict" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume snapshot modify-snaplock-expiry-time" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname

```

"volume snapshot show-delta" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume unmount" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs share create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs share delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs share show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver cifs show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy delete" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy rule create" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy rule show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy show" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "vserver iscsi connection show" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver" -access readonly

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver export-policy" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "vserver iscsi" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "volume clone split status" -access all

• security login role create -vserver SVM_name -role SVM_Role_Name -cmddirname
  "volume managed-feature" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem map" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem create" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem delete" -access all

• security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname
  "nvme subsystem modify" -access all

```

- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem host" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem controller" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme subsystem show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace create" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace delete" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace modify" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "nvme namespace show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "storage-unit show" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "consistency-group" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "snapmirror protect" -access all`
- `security login role create -vserver SVM_Name -role SVM_Role_Name -cmddirname "volume delete" -access all`
- `security login create -user-or-group-name user_name -application http -authentication-method password -role SVM_Role_Name -vserver SVM_Name`
- `security login create -user-or-group-name user_name -application ssh -authentication-method password -role SVM_Role_Name -vserver SVM_Name`

建立具有最低權限的ONTAP叢集角色

您應該建立具有最小權限的ONTAP叢集角色，這樣您就不必使用ONTAP管理員角色在SnapCenter中執行操作。您可以執行多個ONTAP CLI 命令來建立ONTAP叢集角色並指派最低權限。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

```
security login role create -vserver <cluster_name>- role <role_name>-
-cmddirname <permission>
```



您應該對每個權限重複此命令。

2. 建立一個使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
ontapi http -authmethod password -role <role_name\>
```

3. 解除用戶鎖定。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

用於建立叢集角色和分配權限的**ONTAP CLI** 命令

您應該執行幾個ONTAP CLI 命令來建立叢集角色並指派權限。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun online" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun persistent-reservation clear" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun resize" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun serial" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface create" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface delete" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface modify" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "network interface show" -access readonly
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"nvme subsystem map" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem host" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem controller" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme subsystem show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "nvme namespace show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "security login" -access readonly
- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "version" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split start" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume clone split stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume destroy" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname


```

"volume file clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot promote" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot rename" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot restore-file" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot show-delta" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy rule show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver export-policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver iscsi connection show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```
"vserver modify" -access all
```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver show" -access all

為ASA r2 系統建立ONTAP叢集角色

您應該建立具有最小權限的ONTAP叢集角色，這樣您就不必使用ONTAP管理員角色在SnapCenter中執行操作。您可以執行多個ONTAP CLI 命令來建立ONTAP叢集角色並指派最低權限。

步驟

1. 在儲存系統上建立一個角色，並為該角色賦予所有權限。

```
security login role create -vserver <cluster_name\>- role <role_name\>  
-cmddirname <permission\>
```



您應該對每個權限重複此命令。

2. 建立一個使用者並將角色指派給該使用者。

```
security login create -user <user_name\> -vserver <cluster_name\> -application  
http -authmethod password -role <role_name\>
```

3. 解除用戶鎖定。

```
security login unlock -user <user_name\> -vserver <cluster_name\>
```

用於建立叢集角色和分配權限的ONTAP CLI 命令

您應該執行幾個ONTAP CLI 命令來建立叢集角色並指派權限。

- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "metrocluster show" -access readonly
- security login role create -vserver Cluster_name or cluster_name -role Role_Name -cmddirname "cluster identity modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster identity show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster peer show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "cluster show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "event generate-autosupport-log" -access all

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job history show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "job stop" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun igroup show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping add-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping remove-reporting-nodes" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun mapping show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun move-in-volume" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "lun offline" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"lun online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun persistent-reservation clear" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun resize" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun serial" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "lun show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface create" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface delete" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface modify" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "network interface show" -access readonly

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem map" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem host" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem controller" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme subsystem show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "nvme namespace show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "security login" -access readonly

```

- security login role create -role Role_Name -cmddirname "snapmirror create" -vserver Cluster_name -access all
- security login role create -role Role_Name -cmddirname "snapmirror list-destinations" -vserver Cluster_name -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy add-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy modify-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy remove-rule" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror policy show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror show-history" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "snapmirror update-ls-set" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license add" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license clean-up" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system license status show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "system node modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname

```

"system node show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "system status show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "version" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split start" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume clone split stop" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume destroy" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file clone create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume file show-disk-usage" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume snapshot modify-snaplock-expiry-time" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume offline" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume online" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree create" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree delete" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree modify" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume qtree show" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume restrict" -access all

• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume show" -access all

```

- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot promote" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot rename" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot restore-file" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume snapshot show-delta" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "volume unmount" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share create" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share delete" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share modify" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs share show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname "vserver cifs show" -access all
- security login role create -vserver Cluster_name -role Role_Name -cmddirname


```

"vserver create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule create" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule delete" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy rule show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver export-policy show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver iscsi connection show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver modify" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "vserver show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "storage-unit show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "consistency-group" show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "snapmirror protect" show" -access all
• security login role create -vserver Cluster_name -role Role_Name -cmddirname
  "volume delete" show" -access all

```

新增使用者或群組並分配角色和資產

若要為SnapCenter使用者配置基於角色的存取控制，您可以新增使用者或群組並指派角色。角色決定了SnapCenter用戶可以存取的選項。

開始之前

- 您必須以「SnapCenterAdmin」角色登入。
- 您必須已經在作業系統或資料庫的 Active Directory 中建立了使用者或群組帳戶。您不能使用SnapCenter建立這些帳戶。



使用者名稱和群組名稱中只能包含以下特殊字元：空格 ()、連字號 (-)、底線 () 和冒號 (:)。

- SnapCenter包含幾個預先定義的角色。

您可以將這些角色指派給使用者或建立新角色。

- 新增至SnapCenter RBAC 的 AD 使用者和 AD 群組必須對 Active Directory 中的使用者容器和電腦容器具有讀取權限。
- 將角色指派給包含適當權限的使用者或群組後，必須為該使用者指派對SnapCenter資產（例如主機和儲存連線）的存取權。

這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

- 您應該在某個時候為使用者或群組分配一個角色，以利用 RBAC 權限和效率。
- 您可以在建立使用者或群組時為使用者指派主機、資源群組、政策、儲存連線、外掛程式和憑證等資產。
- 您應指派給使用者執行某些操作的最低資產如下：

手術	資產轉讓
保護資源	主機、策略
備份	主機、資源群組、策略
恢復	主機、資源組
複製	主機、資源群組、策略
複製生命週期	主持人
建立資源組	主持人

- 當將新節點新增至 Windows 叢集或 DAG（Exchange Server 資料庫可用性群組）資產時，如果將此新節點指派給用戶，則必須將資產重新指派給使用者或群組，以將新節點包含至使用者或群組。

您應該將 RBAC 使用者或群組重新指派給群集或 DAG，以將新節點包含到 RBAC 使用者或群組。例如，您有一個雙節點集群，並且已為該集群分配了 RBAC 使用者或群組。當您向集群新增另一個節點時，您應該將 RBAC 使用者或群組重新指派給集群，以便為 RBAC 使用者或群組包含新節點。

- 如果您計劃複製快照，則必須將來源磁碟區和目標磁碟區的儲存連線指派給執行操作的使用者。

您應該在向使用者分配存取權限之前新增資產。



如果您使用適用SnapCenter Plug-in for VMware vSphere功能來保護虛擬機器、VMDK 或資料儲存區，則應使用 VMware vSphere GUI 將 vCenter 使用者新增至SnapCenter Plug-in for VMware vSphere角色。有關 VMware vSphere 角色的信息，請參閱 "[SnapCenter Plug-in for VMware vSphere隨附的預先定義角色](#)"。

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「使用者和造訪」 > 「**」。
3. 在「從 Active Directory 或工作群組新增使用者/群組」頁面中：

對於這個領域...	這樣做...
訪問類型	選擇網域或工作群組 對於網域身份驗證類型，您應該指定要將使用者新增至角色的使用者或群組的網域名稱。 預設情況下，它預先填入了登入的網域。  您必須在*設定* > 全域設定 > *網域設定*頁面中註冊不受信任的網域。
類型	選擇使用者或群組  SnapCenter僅支援安全群組，不支援分發組。
使用者名稱	a. 輸入部分用戶名，然後按一下「新增」。  使用者名稱區分大小寫。 b. 從搜尋清單中選擇使用者名稱。  當您從不同的網域或不受信任的網域新增使用者時，您應該完整地輸入使用者名，因為沒有跨網域使用者的搜尋清單。 重複此步驟以將其他使用者或群組新增至所選角色。
角色	選擇您想要新增使用者的角色。

4. 按一下“分配”，然後在“分配資產”頁面中：
 - a. 從*資產*下拉清單中選擇資產類型。
 - b. 在資產表中，選擇資產。

只有當使用者將資產新增至SnapCenter時，才會列出資產。

- c. 對所有所需資產重複此程序。
 - d. 點選“儲存”。
5. 點選“提交”。

新增使用者或群組並指派角色後，刷新資源清單。

配置審核日誌設定

SnapCenter 伺服器的每個活動都會產生審計日誌。預設情況下，稽核日誌會儲存在預設安裝位置 `C:\Program Files\NetApp\SnapCenter WebApp\audit\`。

透過為每個稽核事件產生數位簽章摘要來保護稽核日誌，以防止未經授權的修改。產生的摘要保存在單獨的審計校驗和文件中，並進行定期的完整性檢查以確保內容的完整性。

您應該以「SnapCenterAdmin」角色登入。

關於此任務

- 在以下情況下會發送警報：
 - 審計日誌完整性檢查計劃或 Syslog 伺服器已啟用或停用
 - 稽核日誌完整性檢查、稽核日誌或 Syslog 伺服器日誌故障
 - 磁碟空間不足
- 僅當完整性檢查失敗時才發送電子郵件。
- 您應該同時修改稽核日誌目錄和稽核校驗和日誌目錄路徑。您不能只修改其中一個。
- 當稽核日誌目錄和稽核校驗和日誌目錄路徑被修改時，無法對先前位置的稽核日誌執行完整性檢查。
- 稽核日誌目錄和稽核校驗和日誌目錄路徑應位於 SnapCenter Server 的本機磁碟機上。

不支援共用或網路安裝的磁碟機。

- 如果在 Syslog 伺服器設定中使用 UDP 協議，則由於連接埠關閉或不可用而導致的錯誤無法在 SnapCenter 中擷取為錯誤或警報。
- 您可以使用 `Set-SmAuditSettings` 和 `Get-SmAuditSettings` 指令來設定稽核日誌。

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

步驟

1. 在*設定*頁面中，導覽至*設定*>*全域設定*>*稽核日誌設定*。
2. 在審計日誌部分，輸入詳細資訊。
3. 進入*審計日誌目錄*和*審計校驗和日誌目錄*
 - a. 輸入最大檔案大小
 - b. 輸入最大日誌檔數
 - c. 輸入磁碟空間使用率百分比以發送警報
4. (可選) 啟用*記錄 UTC 時間*。
5. (選用) 啟用*稽核日誌完整性檢查計畫*並點選*開始完整性檢查*進行按需完整性檢查。

您也可以執行*`Start-SmAuditIntegrityCheck`*指令來啟動按需完整性檢查。

6. (可選) 啟用轉發審計日誌到遠端系統日誌伺服器並輸入系統日誌伺服器詳細資訊。

您應該將 Syslog 伺服器中的憑證匯入 TLS 1.2 協定的「受信任的根」。

- a. 輸入 Syslog 伺服器主機
 - b. 輸入 Syslog 伺服器端口
 - c. 輸入 Syslog 伺服器協議
 - d. 輸入 RFC 格式
7. 點選“儲存”。
 8. 您可以透過點選「監視」>「作業」查看稽核完整性檢查和磁碟空間檢查。

使用 SnapCenter Server 設定安全的 MySQL 連接

如果您想在獨立配置或網路負載平衡 (NLB) 配置中保護 SnapCenter 伺服器和 MySQL 伺服器之間的通信，則可以產生安全通訊端層 (SSL) 憑證和金鑰檔案。

為獨立 SnapCenter 伺服器設定配置安全的 MySQL 連接

如果您想要確保 SnapCenter 伺服器和 MySQL 伺服器之間的通訊安全，可以產生安全通訊端層 (SSL) 憑證和金鑰檔案。您必須在 MySQL 伺服器和 SnapCenter 伺服器中設定憑證和金鑰檔案。

產生以下證書：

- CA 憑證
- 伺服器公鑰和私鑰文件
- 客戶端公鑰和私鑰文件

步驟

1. 使用 openssl 指令為 Windows 上的 MySQL 伺服器和用戶端設定 SSL 憑證和金鑰檔案。

有關信息，請參閱 ["MySQL 版本 5.7：使用 openssl 建立 SSL 憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。如果通用名稱值相同，則使用 OpenSSL 編譯的伺服器的憑證和金鑰檔案將會失敗。

最佳實務：您應該使用伺服器完全限定網域名稱 (FQDN) 作為伺服器憑證的通用名稱。

2. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。

預設的 MySQL 資料夾路徑是 C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\。

3. 更新 MySQL 伺服器設定檔 (my.ini) 中的 CA 憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。

預設的 MySQL 伺服器設定檔 (my.ini) 路徑是 C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini。



您必須在 MySQL 伺服器設定檔 (my.ini) 的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔 (my.ini) 的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰文件

C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. 停止 Internet 資訊伺服器 (IIS) 中的 SnapCenter Server Web 應用程式。
5. 重新啟動 MySQL 服務。
6. 更新 SnapManager 檔中 MySQLProtocol 鍵的值。

以下範例顯示了 SnapManager 檔案中更新的 MySQLProtocol 鍵的值。

```
<add key="MySQLProtocol" value="SSL" />
```

7. 使用 my.ini 檔案的 [client] 部分中提供的路徑更新 SnapManager.Web.UI.dll.config 檔案。

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL
Data/Data/ca.pem" />
```

8. 在 IIS 中啟動 SnapCenter Server Web 應用程式。

為 HA 設定配置安全的 MySQL 連接

如果您想要確保 SnapCenter 伺服器 and MySQL 伺服器之間的通訊安全，您可以為高可用性 (HA) 節點產生安全通訊端層 (SSL) 憑證和金鑰檔案。您必須在 MySQL 伺服器和 HA 節點上設定憑證和金鑰檔案。

產生以下證書：

- CA 憑證

在其中一個 HA 節點上產生 CA 證書，並將此 CA 證書複製到另一個 HA 節點。

- 兩個 HA 節點的伺服器公共憑證和伺服器私鑰文件
- 兩個 HA 節點的客戶端公共憑證和客戶端私鑰文件

步驟

1. 對於第一個 HA 節點，使用 openssl 指令為 Windows 上的 MySQL 伺服器和用戶端設定 SSL 憑證和金鑰檔案。

有關信息，請參閱 ["MySQL 版本 5.7：使用 openssl 建立 SSL 憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。如果通用名稱值相同，則使用 OpenSSL 編譯的伺服器的憑證和金鑰檔案將會失敗。

最佳實務：您應該使用伺服器完全限定網域名稱 (FQDN) 作為伺服器憑證的通用名稱。

2. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。

預設 MySQL 資料夾路徑為 C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\。

3. 更新 MySQL 伺服器設定檔 (my.ini) 中的 CA 憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。

預設 MySQL 伺服器設定檔 (my.ini) 路徑為 C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini。



您必須在 MySQL 伺服器設定檔 (my.ini) 的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔 (my.ini) 的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾 C:/ProgramData/ NetApp/ SnapCenter/MySQL Data/Data 中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰檔案。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/client-  
key.pem"
```

4. 對於第二個 HA 節點，複製 CA 憑證並產生伺服器公鑰憑證、伺服器私鑰檔案、用戶端公鑰憑證和用戶端私鑰檔案。執行以下步驟：

- a. 將第一個 HA 節點上產生的 CA 憑證複製到第二個 NLB 節點的 MySQL Data 資料夾中。

預設 MySQL 資料夾路徑為 C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\。



您不能再次建立 CA 憑證。您應該只建立伺服器公共憑證、客戶端公共憑證、伺服器私鑰檔案和客戶端私鑰檔案。

- b. 對於第一個 HA 節點，使用 openssl 指令為 Windows 上的 MySQL 伺服器 and 用戶端設定 SSL 憑證和金鑰檔案。

["MySQL 版本 5.7：使用 openssl 建立 SSL 憑證和金鑰"](#)



用於伺服器憑證、用戶端憑證和金鑰檔案的通用名稱值必須與用於 CA 憑證的通用名稱值不同。如果通用名稱值相同，則使用 OpenSSL 編譯的伺服器的憑證和金鑰檔案將會失敗。

建議使用伺服器 FQDN 作為伺服器憑證的通用名稱。

- c. 將 SSL 憑證和金鑰檔案複製到 MySQL 資料夾。
- d. 更新MySQL伺服器設定檔（my.ini）中的CA憑證、伺服器公鑰、用戶端公鑰、伺服器私鑰、用戶端私鑰路徑。



您必須在 MySQL 伺服器設定檔（my.ini）的 [mysqld] 部分中指定 CA 憑證、伺服器公用憑證和伺服器私密金鑰路徑。

您必須在 MySQL 伺服器設定檔（my.ini）的 [client] 部分中指定 CA 憑證、用戶端公用憑證和用戶端私鑰路徑。

以下範例顯示複製到預設資料夾 C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data 中 my.ini 檔案的 [mysqld] 部分的憑證和金鑰檔案。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
ssl-ca="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/ca.pem"
```

+

```
ssl-cert="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
cert.pem"
```

+

```
ssl-key="C:/ProgramData/NetApp/SnapCenter/MySQL Data/Data/server-  
key.pem"
```

5. 停止兩個 HA 節點上的 Internet 資訊伺服器 (IIS) 中的 SnapCenter Server Web 應用程式。
6. 在兩個 HA 節點上重新啟動 MySQL 服務。
7. 更新兩個 HA 節點的 SnapManager.Web.UI.dll.config 檔案中 MySQLProtocol 鍵的值。

以下範例顯示了 SnapManager 檔案中更新的 MySQLProtocol 鍵的值。

```
<add key="MySQLProtocol" value="SSL" />
```

8. 使用您在 my.ini 檔案的 [client] 部分中為兩個 HA 節點指定的路徑更新 SnapManager.Web.UI.dll.config 檔案。

以下範例顯示了 my.ini 檔案的 [client] 部分中更新的路徑。

```
<add key="ssl-client-cert" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-cert.pem" />
```

```
<add key="ssl-client-key" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/client-key.pem" />
```

```
<add key="ssl-ca" value="C:/ProgramData/NetApp/SnapCenter/MySQL  
Data/Data/ca.pem" />
```

9. 在兩個 HA 節點上的 IIS 中啟動 SnapCenter Server Web 應用程式。
10. 在其中一個 HA 節點上使用帶有 -Force 選項的 Set-SmRepositoryConfig -RebuildSlave -Force PowerShell cmdlet 在兩個 HA 節點上建立安全的 MySQL 複製。

即使複製狀態良好，-Force 選項也允許您重建從屬儲存庫。

配置基於憑證的身份驗證

基於憑證的身份驗證透過驗證 SnapCenter 伺服器和插件主機的身份來增強安全性，確保安全 and 加密的通訊。

啟用基於憑證的身份驗證

若要為 SnapCenter Server 和 Windows 外掛程式主機啟用基於憑證的驗證，請執行下列 PowerShell cmdlet。對於 Linux 外掛主機，啟用雙向 SSL 時將啟用基於憑證的驗證。

- 若要啟用基於用戶端憑證的身份驗證：

```
Set-SmConfigSettings -Agent -configSettings  
@{"EnableClientCertificateAuthentication"="true"} -HostName[hostname]
```

- 若要停用基於客戶端憑證的身份驗證：

```
Set-SmConfigSettings -Agent -configSettings
@{"EnableClientCertificateAuthentication"="false"} -HostName [hostname]`
```

從SnapCenter伺服器匯出憑證授權單位 (CA) 憑證

您應該使用 Microsoft 管理主控台 (MMC) 將 CA 憑證從SnapCenter伺服器匯出到外掛程式主機。

開始之前

您應該已經配置了雙向 SSL。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
5. 右鍵點選用於SnapCenter Server 的採購 CA 證書，然後選擇 所有任務 > 匯出 以啟動匯出精靈。
6. 在精靈中執行下列操作。

對於此選項...	執行以下操作...
匯出私鑰	選擇*否，不匯出私鑰*，然後按一下*下一步*。
匯出文件格式	按一下“下一步”。
檔案名稱	點選*瀏覽*並指定儲存憑證的檔案路徑，然後點選*下一步*。
完成憑證匯出精靈	查看摘要，然後按一下「完成」開始匯出。



SnapCenter HA 設定和SnapCenter Plug-in for VMware vSphere不支援基於憑證的驗證。

將 CA 憑證匯入 Windows 插件主機

若要使用匯出的SnapCenter Server CA 證書，您應該使用 Microsoft 管理主控台 (MMC) 將相關憑證匯入至SnapCenter Windows 外掛程式主機。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。

4. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
5. 右鍵單擊資料夾“個人”，然後選擇*所有任務* > *導入*以啟動導入精靈。
6. 在精靈中執行下列操作。

對於此選項...	執行以下操作...
商店位置	按一下“下一步”。
要導入的文件	選擇以 .cer 副檔名結尾的SnapCenter伺服器憑證。
證書存儲	按一下“下一步”。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

將 CA 憑證匯入 UNIX 插件主機

您應該將 CA 憑證匯入到 UNIX 插件主機。

關於此任務

- 您可以管理 SPL 金鑰庫的密碼，以及正在使用的 CA 簽章金鑰對的別名。
- SPL 金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

步驟

1. 您可以從 SPL 屬性檔案中檢索 SPL 金鑰庫預設密碼。它是鍵對應的值 `SPL_KEYSTORE_PASS`。
2. 更改密鑰庫密碼：

```
$ keytool -storepasswd -keystore keystore.jks
```
3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```
4. 對金鑰 `SPL_KEYSTORE_PASS` 進行相同的更新 ``spl.properties`` 文件。
5. 修改密碼後重啟服務。

將根憑證或中繼憑證設定到 **SPL** 信任庫

您應該將根憑證或中間憑證設定到 SPL 信任庫。您應該新增根 CA 證書，然後新增中間 CA 證書。

步驟

1. 導航至包含 SPL 金鑰庫的資料夾：`/var/opt/snapcenter/spl/etc`。
2. 找到文件 `keystore.jks`。
3. 列出密鑰庫中新增的憑證：

```
$ keytool -list -v -keystore keystore.jks
```
4. 新增根證書或中間證書：

```
$ keytool -import -trustcacerts -alias <AliasNameForCertificateToBeImported>
-file /<CertificatePath> -keystore keystore.jks
```

5. 將根憑證或中間憑證配置到 SPL 信任庫後重新啟動服務。

將 **CA** 簽章金鑰對配置到 **SPL** 信任庫

您應該將 CA 簽署的金鑰對配置到 SPL 信任庫。

步驟

1. 導航至包含 SPL 金鑰庫的資料夾 /var/opt/snapcenter/spl/etc。
2. 找到文件 keystore.jks。
3. 列出密鑰庫中新增的憑證：

```
$ keytool -list -v -keystore keystore.jks
```
4. 新增具有私鑰和公鑰的 CA 憑證。

```
$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype
pkcs12 -destkeystore keystore.jks -deststoretype JKS
```
5. 列出密鑰庫中新增的憑證。

```
$ keytool -list -v -keystore keystore.jks
```
6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設 SPL 金鑰庫密碼是金鑰 SPL_KEYSTORE_PASS 的值 `spl.properties` 文件。

```
$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks`
```

8. 如果CA憑證中的別名較長，且包含空格或特殊字元（“*”，“，”），請將別名修改為簡單名稱：

```
$ keytool -changealias -alias "<OriginalAliasName>" -destalias "<NewAliasName>"
-keystore keystore.jks`
```
9. 從位於的金鑰庫配置別名 `spl.properties` 文件。根據鍵 SPL_CERTIFICATE_ALIAS 更新此值。
10. 將 CA 簽署金鑰對配置到 SPL 信任庫後重新啟動服務。

匯出SnapCenter證書

您應該以 .pfx 格式匯出SnapCenter憑證。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「我的使用者帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 目前使用者 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵點選具有SnapCenter友善名稱的證書，然後選擇 所有任務 > 匯出 以啟動匯出精靈。

6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
匯出私鑰	選擇選項*是，匯出私鑰*，然後按一下*下一步*。
匯出文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
要匯出的文件	指定匯出憑證的檔案名稱（必須使用.pfx），然後按一下「下一步」。
完成憑證匯出精靈	查看摘要，然後按一下「完成」開始匯出。

為 Windows 主機設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。

3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在SnapCenter伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

2. 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

使用SnapCenter站點配置 CA 證書

您應該在 Windows 主機上使用SnapCenter網站設定 CA 憑證。

步驟

1. 在安裝了SnapCenter的 Windows Server 上開啟 IIS 管理員。
2. 在左側導覽窗格中，按一下「連線」。
3. 展開伺服器的名稱和*網站*。
4. 選擇要安裝 SSL 憑證的SnapCenter網站。
5. 導覽至*操作* > 編輯網站，按一下*綁定*。
6. 在綁定頁面中，選擇「https 綁定」。
7. 按一下“編輯”。

8. 從 SSL 憑證下拉清單中，選擇最近匯入的 SSL 憑證。

9. 按一下“確定”。



SnapCenter Scheduler 網站（預設連接埠：8154，HTTPS）配置了自簽名憑證。此連接埠在 SnapCenter Server 主機內進行通信，且不需要使用 CA 憑證進行設定。但是，如果您的環境要求您使用 CA 證書，請使用 SnapCenter Scheduler 網站重複步驟 5 到 9。



如果下拉式選單中未列出最近部署的 CA 證書，請檢查該 CA 證書是否與私鑰相關聯。



確保使用下列路徑新增憑證：控制台根 > 憑證 - 本機 > 受信任的根憑證授權單位 > 憑證。

為 SnapCenter 啟用 CA 憑證

您應該設定 CA 憑證並為 SnapCenter 伺服器啟用 CA 憑證驗證。

開始之前

- 您可以使用 Set-SmCertificateSettings cmdlet 啟用或停用 CA 憑證。
- 您可以使用 Get-SmCertificateSettings cmdlet 顯示 SnapCenter 伺服器的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「CA 憑證設定」。
2. 選擇*啟用憑證驗證*。
3. 按一下“應用”。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器和插件主機之間的連線狀態。

- * * 表示沒有啟用或指派給插件主機的 CA 憑證。
- * * 表示 CA 憑證驗證成功。
- * * 表示無法驗證 CA 憑證。
- * * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

為 Linux 主機設定 CA 憑證

在 Linux 上安裝 SnapCenter 伺服器後，安裝程式會建立自簽名憑證。如果要使用 CA 證書，則應為 nginx 反向代理、稽核日誌記錄和 SnapCenter 服務設定證書。

設定nginx證書

步驟

1. 導航至 `/etc/nginx/conf.d`：`cd /etc/nginx/conf.d`
2. 使用 `vi` 或任何文字編輯器開啟 **snapcenter.conf**。
3. 導航到設定檔中的伺服器部分。
4. 修改 `_ssl_certificate` 和 `_ssl_certificate_key` 的路徑以指向CA憑證。
5. 儲存並關閉文件。
6. 重新載入 `nginx`：`$nginx -s reload`

配置審核日誌證書

步驟

1. 使用 `vi` 或任何文字編輯器開啟 `_INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager`。

INSTALL_DIR 的預設值是 */opt*。
2. 編輯 **AUDILOG_CERTIFICATE_PATH** 和 **AUDILOG_CERTIFICATE_PASSWORD** 鍵以分別包含 CA 憑證路徑和密碼。

稽核日誌憑證僅支援 *.pfx* 格式。
3. 儲存並關閉文件。
4. 重新啟動 **snapmanagerweb** 服務：`$ systemctl restart snapmanagerweb`

配置SnapCenter服務證書

步驟

1. 使用 `vi` 或任何文字編輯器開啟以下設定檔。
 - `INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config`
 - 安裝目錄NetApp
 - 安裝目錄NetApp
INSTALL_DIR 的預設值是 */opt*。
2. 編輯 **SERVICE_CERTIFICATE_PATH** 和 **SERVICE_CERTIFICATE_PASSWORD** 鍵以分別包含 CA 憑證路徑和密碼。

SnapCenter服務憑證僅支援 *.pfx* 格式。
3. 儲存並關閉文件。
4. 重新啟動所有服務。
 - `$ systemctl restart snapmanagerweb`
 - `$ systemctl restart smcore`

◦ `$ systemctl restart scheduler`

在 Windows 主機上設定並啟用雙向 SSL 通信

在 Windows 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

- 您應該已經產生了具有最小支援金鑰長度 3072 的 CA 憑證 CSR 檔案。
- CA憑證應支援伺服器認證和用戶端認證。
- 您應該擁有一份包含私鑰和指紋詳細資訊的 CA 憑證。
- 您應該已經啟用單向 SSL 設定。

有關詳細信息，請參閱 ["配置CA憑證部分。"](#)

- 您必須在所有插件主機和SnapCenter伺服器上啟用雙向 SSL 通訊。

不支援某些主機或伺服器未啟用雙向 SSL 通訊的環境。

步驟

1. 若要綁定端口，請使用 PowerShell 命令在SnapCenter Server 主機上對SnapCenter IIS Web 伺服器連接埠 8146（預設）執行下列步驟，並再次對 SMCore 連接埠 8145（預設）執行下列步驟。

- a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
```

例如，

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

```
> netsh http delete sslcert ipport=0.0.0.0:8146
```

- b. 將新購買的 CA 憑證與SnapCenter伺服器和 SMCore 連接埠綁定。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port/IIS port>  
certhash=$cert appid="$guid" clientcertnegotiation=enable  
verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port/IIS port>
```

例如，

```

> $cert = "abc123abc123abc123abc123"

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8146 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> $guid = [guid]::NewGuid().ToString("B")

> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"
clientcertnegotiation=enable verifyclientcertrevocation=disable

> netsh http show sslcert ipport=0.0.0.0:8146

> netsh http show sslcert ipport=0.0.0.0:8145

```

2. 若要存取 CA 憑證的權限，請透過執行下列步驟在憑證權限清單中新增 SnapCenter 的預設 IIS Web 伺服器使用者「**IIS AppPool\ SnapCenter**」來存取新購買的 CA 憑證。
 - a. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
 - b. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
 - c. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
 - d. 按一下 控制台根 > 憑證 - 本機 > 個人 > 憑證。
 - e. 選擇 SnapCenter 證書。
 - f. 若要啟動新增使用者權限精靈，請以滑鼠右鍵按一下 CA 憑證並選擇 所有任務 > 管理私密金鑰。
 - g. 按一下“新增”，在“選取使用者和群組”精靈中將位置變更為本機電腦名稱（層次結構中的最頂層）
 - h. 新增 IIS AppPool\ SnapCenter 用戶，授予完全控制權限。

3. 對於 **CA 憑證 IIS** 權限，從下列路徑在 SnapCenter Server 中新增新的 DWORD 登錄項目項目：

在 Windows 登錄編輯器中，遍歷下面提到的路徑，

```
HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityPro
viders\SCHANNEL
```

4. 在 SCHANNEL 註冊表配置上下文中建立新的 DWORD 註冊表項條目。

```
SendTrustedIssuerList = 0
```

```
ClientAuthTrustMode = 2
```

配置 SnapCenter Windows 插件以進行雙向 SSL 通信

您應該使用 PowerShell 命令設定 SnapCenter Windows 插件以進行雙向 SSL 通訊。

開始之前

確保 CA 憑證指紋可用。

步驟

1. 若要綁定端口，請在 Windows 插件主機上對 SMCore 連接埠 8145（預設）執行下列操作。

a. 使用下列 PowerShell 指令刪除現有的SnapCenter自簽章憑證連接埠綁定。

```
> netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
```

例如，

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

b. 將新購買的CA憑證與SMCore連接埠綁定。

```
> $cert = "<CA_certificate_thumbprint>"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0: <SMCore Port> certhash=$cert  
appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:<SMCore Port>
```

例如，

```
> $cert = "abc123abc123abc123abc123"
```

```
> $guid = [guid]::NewGuid().ToString("B")
```

```
> netsh http add sslcert ipport=0.0.0.0:8145 certhash=$cert appid="$guid"  
clientcertnegotiation=enable verifyclientcertrevocation=disable
```

```
> netsh http show sslcert ipport=0.0.0.0:8145
```

在 Windows 主機上啟用雙向 SSL 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Windows 主機上的SnapCenter伺服器與插件之間的相互通訊。

開始之前

首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。

步驟

1. 若要啟用雙向 SSL 通信，請在SnapCenter伺服器上執行下列命令，用於插件、伺服器以及需要雙向 SSL 通訊的每個代理程式。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
```

```
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. 使用下列命令執行 IIS SnapCenter應用程式集區回收作業。

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. 對於 Windows 插件，透過執行下列 PowerShell 命令重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

禁用雙向 SSL 通信

您可以使用 PowerShell 指令停用雙向 SSL 通訊。

關於此任務

- 首先執行所有插件和 SMCore 代理的命令，然後執行伺服器的命令。
- 當您停用雙向 SSL 通訊時，CA 憑證及其配置不會被刪除。
- 若要為 SnapCenter Server 新增主機，必須停用所有插件主機的雙向 SSL。
- 不支援 NLB 和 F5。

步驟

1. 若要停用雙向 SSL 通信，請在 SnapCenter Server 上對所有插件主機和 SnapCenter 主機執行下列命令。

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName <Agent_HostName>
```

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}  
-HostName localhost
```

```
> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. 使用下列命令執行 IIS SnapCenter應用程式集區回收作業。

```
> Restart-WebAppPool -Name "SnapCenter"
```

3. 對於 Windows 插件，透過執行下列 PowerShell 命令重新啟動 SMCore 服務：

```
> Restart-Service -Name SnapManagerCoreService
```

在 Linux 主機上設定並啟用雙向 SSL 通信

在 Linux 主機上設定雙向 SSL 通信

您應該配置雙向 SSL 通訊以保護 Linux 主機上的 SnapCenter 伺服器與插件之間的相互通訊。

開始之前

- 您應該已經為 Linux 主機設定了 CA 憑證。
- 您必須在所有插件主機和SnapCenter伺服器上啟用雙向 SSL 通訊。

步驟

1. 將 **certificate.pem** 複製到 `/etc/pki/ca-trust/source/anchors/`。
 - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
 - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
 - `update-ca-trust extract`
2. 將憑證新增到 Linux 主機的信任清單中。


```
trust list | grep "<CN of your certificate>"
```
3. 驗證證書是否已新增至信任清單。
4. 更新SnapCenter **nginx** 檔案中的 **ssl_certificate** 和 **ssl_certificate_key** 並重新啟動。
 - `vim /etc/nginx/conf.d/snapcenter.conf`
 - `systemctl restart nginx`
5. 刷新SnapCenter伺服器 GUI 連結。
6. 更新位於 `/<安裝路徑>/NetApp/snapcenter/SnapManagerWeb_` 的 `* SnapManager.Web.UI.dll.config*` 和位於 `/<安裝路徑>/NetApp/snapcenter/SMCore` 的 **SMCoreServiceHost.dll.config** 中的下列登錄項目的值。
 - `<add key="SERVICE_CERTIFICATE_PATH" value="<證書.pfx 的路徑>" />`
 - `<新增鍵="SERVICE_CERTIFICATE_PASSWORD"值="<密碼>"/>`
7. 重新啟動以下服務。
 - `systemctl restart smcore.service`
 - `systemctl restart snapmanagerweb.service`
8. 驗證憑證是否已附加至SnapManager Web 連接埠。


```
openssl s_client -connect localhost:8146 -brief
```
9. 驗證憑證是否已附加到 smcore 連接埠。


```
openssl s_client -connect localhost:8145 -brief
```
10. 管理 SPL 金鑰庫和別名的密碼。
 - a. 檢索指派給 SPL 屬性檔案中的 **SPL_KEYSTORE_PASS** 鍵的 SPL 金鑰庫預設密碼。
 - b. 更改密鑰庫密碼。


```
keytool -storepasswd -keystore keystore.jks
```
 - c. 更改所有私鑰條目別名的密碼。


```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```
 - d. 為 `spl.properties` 中的金鑰 **SPL_KEYSTORE_PASS** 更新相同的密碼。
 - e. 重新啟動服務。
11. 在插件 Linux 主機上，在 SPL 插件的金鑰庫中新增根憑證和中間憑證。
 - `keytool -import -trustcacerts -alias <any preferred alias name> -file <path of root-ca.pem> -keystore <path of keystore.jks mentioned in spl.properties`

file>

```
° keytool -importkeystore -srckeystore <path of certificate.pfx> -srcstoretype pkcs12 -destkeystore <path of keystore.jks mentioned in spl.properties file> -deststoretype JKS
```

i. 檢查 keystore.jks 中的條目。

```
keytool -list -v -keystore <path to keystore.jks>
```

ii. 如果需要，請重新命名任何別名。

```
keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass  
keypass -keystore </path/to/keystore> -storepass storepas
```

12. 使用儲存在 *keystore.jks* 中的 **certificate.pfx** 的別名更新 *spl.properties* 檔案中的 **SPL_CERTIFICATE_ALIAS** 的值，然後重新啟動 SPL 服務：systemctl restart spl

13. 驗證憑證是否已附加到 smcore 連接埠。

```
openssl s_client -connect localhost:8145 -brief
```

在 Linux 主機上啟用 SSL 通信

您可以啟用雙向 SSL 通信，以使用 PowerShell 命令保護 Linux 主機上的 SnapCenter 伺服器與插件之間的相互通訊。

步

1. 執行以下操作以啟用單向 SSL 通訊。

a. 登入 SnapCenter GUI。

b. 按一下“設定”>“全域設定”，然後選擇“在 SnapCenter 伺服器上啟用憑證驗證”。

c. 按一下“主機”>“託管主機”，然後選擇要啟用單向 SSL 的插件主機。

d. 點選  圖標，然後按一下*啟用憑證驗證*。

2. 從 SnapCenter Server Linux 主機啟用雙向 SSL 通訊。

```
° Open-SmConnection
```

```
° Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName <Plugin Host Name>
```

```
° Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}  
-HostName localhost
```

```
° Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

配置 Active Directory、LDAP 和 LDAPS

註冊不受信任的 Active Directory 網域

您應該向 SnapCenter Server 註冊 Active Directory，以管理來自多個不受信任的 Active Directory 網域的主機、使用者和群組。

開始之前

LDAP 和 LDAPS 協議

- 您可以使用 LDAP 或 LDAPS 協定註冊不受信任的活動目錄網域。
- 您應該已經啟用插件主機和SnapCenter伺服器之間的雙向通訊。
- 應設定從SnapCenter伺服器到插件主機的 DNS 解析，反之亦然。

LDAP 協定

- 完全限定網域名稱 (FQDN) 應該可以從SnapCenter Server 解析。

您可以使用 FQDN 註冊不受信任的網域。如果無法從SnapCenter伺服器解析 FQDN，則可以使用網域控制器 IP 位址進行註冊，並且該位址應該可以從SnapCenter伺服器解析。

LDAPS 協定

- LDAPS 需要 CA 憑證來在活動目錄通訊期間提供端對端加密。

["為 LDAPS 設定 CA 用戶端憑證"](#)

- 網域控制器主機名稱 (DCHostName) 應該可以從SnapCenter伺服器存取。

關於此任務

- 您可以使用SnapCenter使用者介面、PowerShell cmdlet 或 REST API 來註冊不受信任的網域。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「全域設定」。
3. 在全域設定頁面中，按一下「網域設定」。
4. 點選  註冊一個新網域。
5. 在註冊新網域頁面中，選擇 **LDAP** 或 **LDAPS**。
 - a. 如果選擇 **LDAP**，請指定為 LDAP 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN 並按一下 解析。
網域控制器 IP 位址	如果無法從SnapCenter伺服器解析網域 FQDN，請指定一個或多個網域控制器 IP 位址。 有關更多信息，請參閱 "從 GUI 為不受信任的網域新增網域控制器 IP"。

b. 如果選擇 **LDAPS**，請指定為 LDAPS 註冊不受信任網域所需的資訊：

對於這個領域...	這樣做...
網域	指定網域的 NetBIOS 名稱。
域 FQDN	指定 FQDN。
網域控制器名稱	指定一個或多個網域控制站名稱，然後按一下「解析」。
網域控制器 IP 位址	如果網域控制站名稱無法從 SnapCenter Server 解析，則應修正 DNS 解析。

6. 按一下“確定”。

設定 IIS 應用程式集區以啟用 **Active Directory** 讀取權限

當您需要為 SnapCenter 啟用 Active Directory 讀取權限時，您可以在 Windows Server 上設定 Internet 資訊服務 (IIS) 來建立自訂應用程式集區帳戶。

步驟

1. 在安裝了 SnapCenter 的 Windows Server 上開啟 IIS 管理員。
2. 在左側導覽窗格中，按一下「應用程式集區」。
3. 在應用程式集區清單中選擇 SnapCenter，然後按一下操作窗格中的「進階設定」。
4. 選擇“身分”，然後按一下“...”以編輯 SnapCenter 應用程式集區身分。
5. 在自訂帳戶欄位中，輸入具有 Active Directory 讀取權限的網域使用者或網域管理員帳戶名稱。
6. 按一下“確定”。

自訂帳戶取代了 SnapCenter 應用程式集區的內建 ApplicationPoolIdentity 帳戶。

為 **LDAPS** 設定 **CA** 用戶端憑證

當 Windows Active Directory LDAPS 配置了 CA 憑證時，您應該在 SnapCenter 伺服器上為 LDAPS 設定 CA 用戶端憑證。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇“所有任務” > “匯入”以啟動匯入精靈。

6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
在嚮導的第二頁	按一下“瀏覽”，選擇“根憑證”，然後按一下“下一步”。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。

7. 對中間證書重複步驟 5 和 6。

保護 Microsoft SQL Server 資料庫

適用於 Microsoft SQL Server 的SnapCenter插件

適用於 Microsoft SQL Server 的SnapCenter外掛程式概述

適用於 Microsoft SQL Server 的SnapCenter外掛程式是NetApp SnapCenter軟體的主機端元件，可實現 Microsoft SQL Server 資料庫的應用程式感知資料保護管理。SQL Server 外掛程式可在您的SnapCenter環境中自動執行 SQL Server 資料庫備份、驗證、復原和複製作業。

安裝 SQL Server 外掛程式後，您可以將SnapCenter與NetApp SnapMirror技術結合使用，在另一個磁碟區上建立備份集的鏡像副本，並使用NetApp SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性或存檔目的。

- 自動執行SnapCenter環境中 Microsoft SQL Server 資料庫的應用程式感知備份、還原和複製作業。
- 當您部署SnapCenter Plug-in for VMware vSphere並在SnapCenter中註冊外掛程式時，支援 VMDK 和原始裝置對應 (RDM) LUN 上的 Microsoft SQL Server 資料庫
- 僅支援配置 SMB 共享。不支援在 SMB 共用上備份 SQL Server 資料庫。
- 支援將備份從SnapManager for Microsoft SQL Server 匯入到SnapCenter。

您可以使用適用於 Microsoft SQL Server 的SnapCenter外掛程式執行哪些操作

當您的環境中安裝了適用於 Microsoft SQL Server 的SnapCenter外掛程式後，您可以使用SnapCenter備份、還原和複製 SQL Server 資料庫。

您可以執行下列支援 SQL Server 資料庫和資料庫資源的備份作業、還原作業和複製作業的任務：

- 備份 SQL Server 資料庫和相關交易日誌

您不能為 master 和 msdb 系統資料庫建立日誌備份。但是，您可以為模型系統資料庫建立日誌備份。

- 恢復資料庫資源
 - 您可以還原主系統資料庫、msdb 系統資料庫和模型系統資料庫。
 - 您無法還原多個資料庫、執行個體和可用性群組。
 - 您無法將系統資料庫還原到備用路徑。

- 建立生產資料庫的時間點克隆

您無法對 tempdb 系統資料庫執行備份、還原、複製和複製生命週期作業。

- 立即驗證備份作業或延遲驗證

不支援驗證 SQL Server 系統資料庫。SnapCenter克隆資料庫以執行驗證操作。SnapCenter無法克隆 SQL Server 系統資料庫，因此不支援驗證這些資料庫。

- 安排備份作業和克隆作業
- 監控備份作業、復原作業和複製操作



SQL Server 外掛程式不支援在 SMB 共用上備份和還原 SQL Server 資料庫。

適用於 Microsoft SQL Server 的SnapCenter外掛功能

SQL Server 外掛程式與 Windows 主機上的 Microsoft SQL Server 以及儲存系統上的NetApp Snapshot 技術整合。若要使用 SQL Server 插件，您需要使用SnapCenter介面。

SQL Server 外掛程式包含以下主要功能：

- 由**SnapCenter**提供支援的統一圖形使用者介面

SnapCenter介面為您提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份和復原流程、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以及監控所有外掛程式中的作業。SnapCenter還提供集中調度和策略管理以支援備份和複製作業。

- 自動化中央管理

您可以安排例行 SQL Server 備份、設定基於政策的備份保留以及設定時間點和最新的復原作業。您也可以透過設定SnapCenter傳送電子郵件警報來主動監控您的 SQL Server 環境。

- 無中斷**NetApp Snapshot** 技術

SQL Server 外掛程式將NetApp Snapshot 技術與 Microsoft Windows 的NetApp SnapCenter插件結合使用。這使您能夠在幾秒鐘內備份資料庫並快速還原它們，而無需使 SQL Server 離線。快照佔用最少的儲存空間。

除了這些主要功能外，SQL Server 外掛程式還提供以下優點：

- 備份、還原、複製和驗證工作流程支持
- RBAC 支援的安全性和集中角色委派
- 使用NetApp FlexClone技術建立生產資料庫的空間高效時間點副本，用於測試或資料擷取

保存克隆的儲存系統需要FlexClone許可證。

- 無中斷和自動化備份驗證
- 能夠在多台伺服器上同時執行多個備份
- 用於編寫備份、驗證、還原和複製作業腳本的 PowerShell cmdlet
- 支援 SQL Server 中的 AlwaysOn 可用性群組 (AG)，以加速 AG 設定、備份和復原作業
- 記憶體資料庫和緩衝池擴展 (BPE) 是 SQL Server 2014 的一部分
- 支援 LUN 和虛擬機器磁碟 (VMDK) 的備份
- 支援實體和虛擬化基礎設施

- 支援 iSCSI、光纖通道、FCoE、原始設備對映 (RDM) 以及 NFS 和 VMFS 上的 VMDK



NAS 磁碟區應該在儲存虛擬機器 (SVM) 中具有預設匯出策略。

- 支援 SQL Server 獨立資料庫中的 FileStream 和檔案群組。
- Windows Server 2022 支援非揮發性記憶體快速 (NVMe)
 - 在 TCP/IP 上的 NVMe 上建立的 VMDK 佈局的備份、復原、複製和驗證工作流程。
 - 從 ESX 8.0 update 2 開始支援 NVMe 韌體版本 1.3，並且需要虛擬硬體版本 21。
 - NVMe over TCP/IP 上的 VMDK 應用程式不支援 Windows Server 故障轉移叢集 (WSFC)。
- 支援 SnapMirror 主動同步（最初作為 SnapMirror 業務連續性 [SM-BC] 發布），即使整個網站發生故障，也能使業務服務繼續運行，支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過 SnapMirror 主動同步觸發故障轉移。

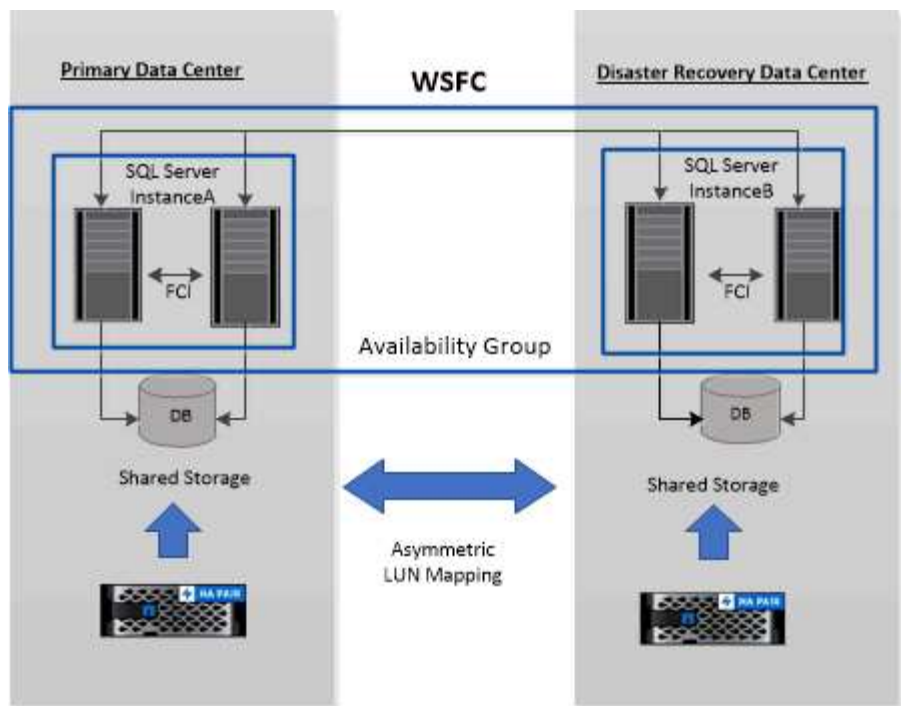
支援 Windows 群集中的非對稱 LUN 映射

適用於 Microsoft SQL Server 的 SnapCenter 外掛程式支援 SQL Server 2012 及更高版本中的發現、用於高可用性的非對稱 LUN 對應 (ALM) 配置以及用於災難復原的可用性群組。在發現資源時，SnapCenter 會在 ALM 設定中發現本機主機和遠端主機上的資料庫。

ALM 配置是單一 Windows 伺服器故障轉移群集，其中包含主資料中心中的一個或多個節點以及災難復原中心中的一個或多個節點。

以下是 ALM 配置的範例：

- 多站點資料中心中的兩個故障轉移群集實例 (FCI)
- FCI 用於本地高可用性 (HA) 和可用性群組 (AG)，用於在災難復原站點使用獨立實例進行災難復原



WSFC----Windows Server Failover Cluster

主資料中心中的儲存空間在主資料中心中的 FCI 節點之間共用。災難復原資料中心中的儲存空間在災難復原資料中心中的 FCI 節點之間共用。

主資料中心上的儲存空間對於災難復原資料中心上的節點是不可見的，反之亦然。

ALM 架構結合了 FCI 使用的兩種共用儲存解決方案以及 SQL AG 使用的非共用或專用儲存解決方案。AG 解決方案使用相同的磁碟機號碼來跨資料中心共用磁碟資源。這種儲存安排，即叢集磁碟在 WSFC 內的節點子集之間共用，稱為 ALM。

SnapCenter Plug-in for Microsoft SQL Server 支援的儲存類型

SnapCenter 支援實體機器和虛擬機器上的多種儲存類型。在為您的主機安裝軟體包之前，您必須驗證您的儲存類型是否受支援。

Windows Server 上提供 SnapCenter 設定和資料保護支援。有關受支援版本的最新信息，請參閱 [https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp 互通性表工具\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\)。

機器	儲存類型	使用配置	支援說明
實體伺服器	FC 連接的 LUN	SnapCenter 圖形使用者介面 (GUI) 或 PowerShell cmdlet	
實體伺服器	iSCSI 連接的 LUN	SnapCenter GUI 或 PowerShell cmdlet	

機器	儲存類型	使用配置	支援說明
實體伺服器	駐留在儲存虛擬機器 (SVM) 上的 SMB3 (CIFS) 共用	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。
VMware VM	透過 FC 或 iSCSI HBA 連接的 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	
VMware VM	虛擬機器檔案系統 (VMFS) 或 NFS 資料存儲	VMware vSphere	
VMware VM	連接到 SVM 上的 SMB3 共享的客戶系統	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。
VMware VM	NFS 和 SAN 上的 vVol 資料存儲	適用於 VMware vSphere 的 ONTAP 工具	
Hyper-V 虛擬機	透過虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN	SnapCenter GUI 或 PowerShell cmdlet	您必須使用 Hyper-V 管理員來設定由虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN。  不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。
Hyper-V 虛擬機	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	 不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。

機器	儲存類型	使用配置	支援說明
Hyper-V 虛擬機	連接到 SVM 上的 SMB3 共享的客戶系統	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。  不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。

適用於 Microsoft SQL Server 的 SnapCenter 外掛程式的儲存佈局建議

精心設計的儲存佈局可讓 SnapCenter Server 備份您的資料庫以滿足您的復原目標。在定義儲存佈局時，您應該考慮幾個因素，包括資料庫的大小、資料庫的變化率以及執行備份的頻率。

以下部分定義了在您的環境中安裝了適用於 Microsoft SQL Server 的 SnapCenter 插件的 LUN 和虛擬機器磁碟 (VMDK) 的儲存佈局建議和限制。

在這種情況下，LUN 可以包括映射到來賓的 VMware RDM 磁碟和 iSCSI 直連 LUN。

LUN 和 VMDK 要求

您可以選擇使用專用 LUN 或 VMDK 來實現以下資料庫的最佳效能和管理：

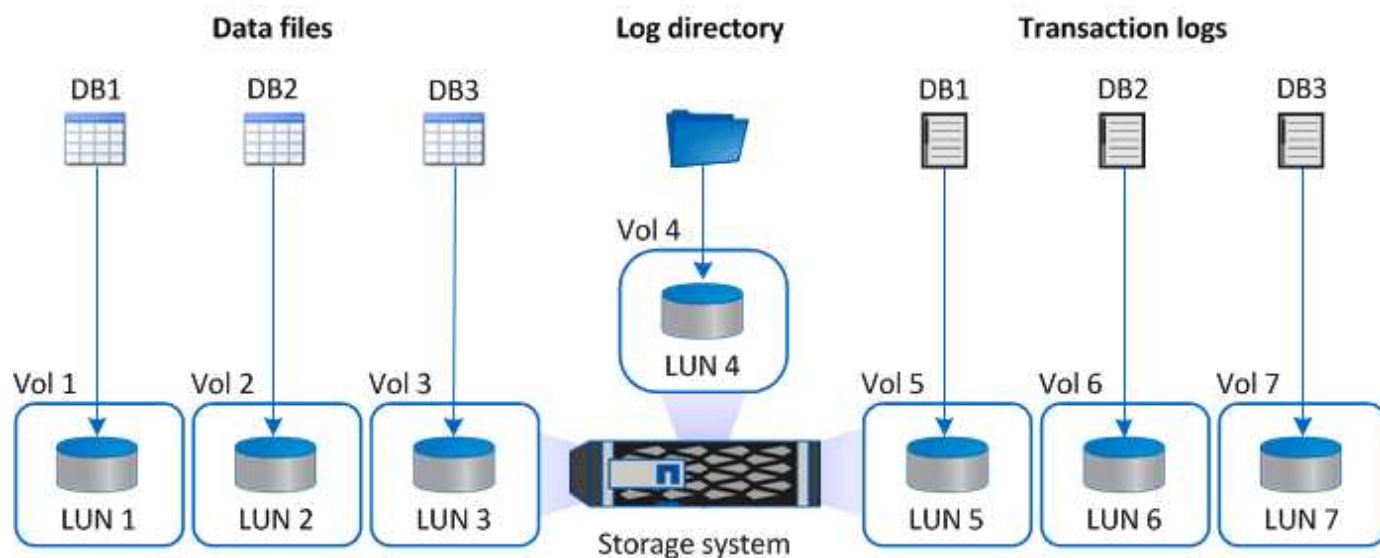
- 主系統資料庫和模型系統資料庫
- 臨時資料庫
- 使用者資料庫檔案 (.mdf 和 .ndf)
- 使用者資料庫事務日誌檔 (.ldf)
- 日誌目錄

要恢復大型資料庫，最佳做法是使用專用 LUN 或 VMDK。恢復完整的 LUN 或 VMDK 所需的時間少於恢復儲存在 LUN 或 VMDK 中的單一檔案所需的時間。

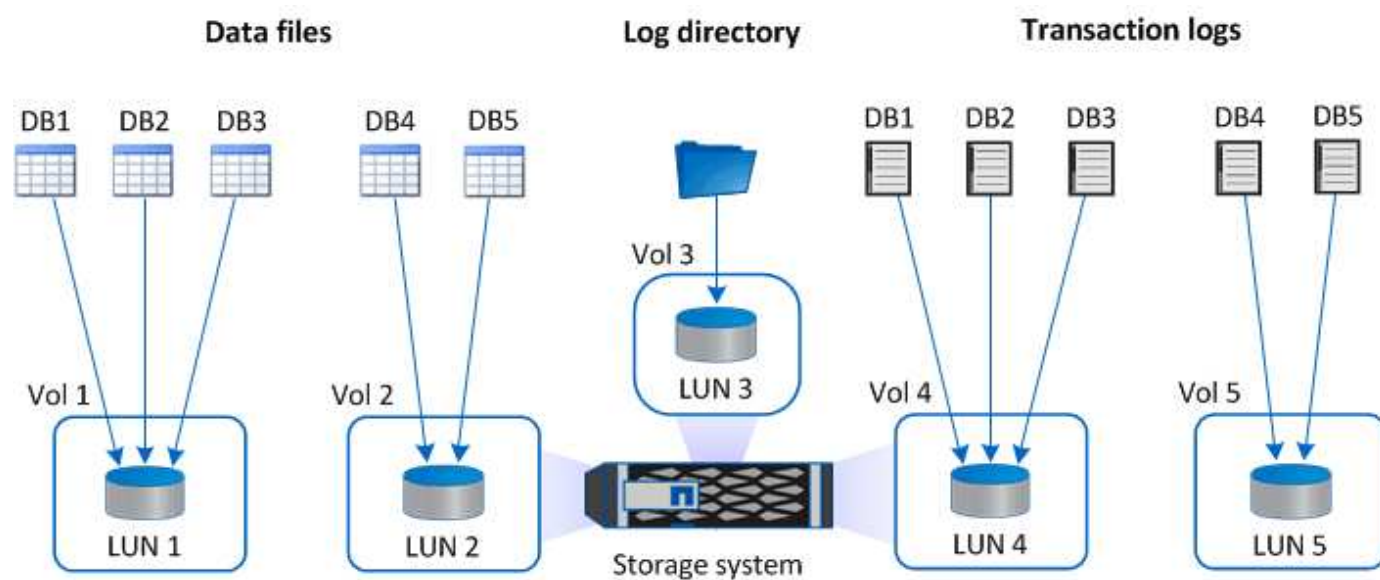
對於日誌目錄，您應該建立一個單獨的 LUN 或 VMDK，以便在資料或日誌檔案磁碟中有足夠的可用空間。

LUN 和 VMDK 範例佈局

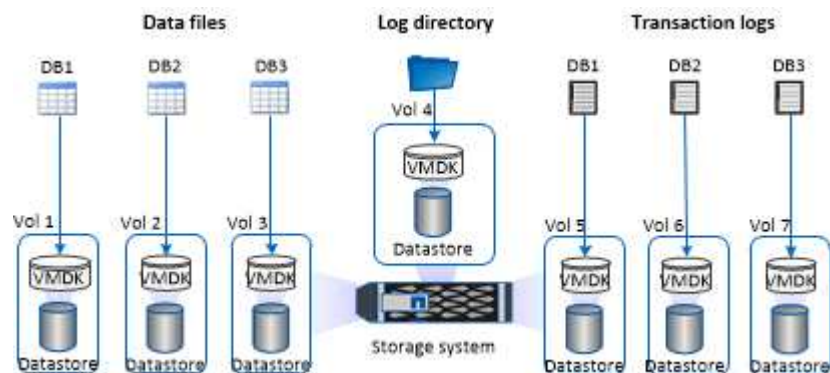
下圖顯示如何在 LUN 上設定大型資料庫的儲存佈局：



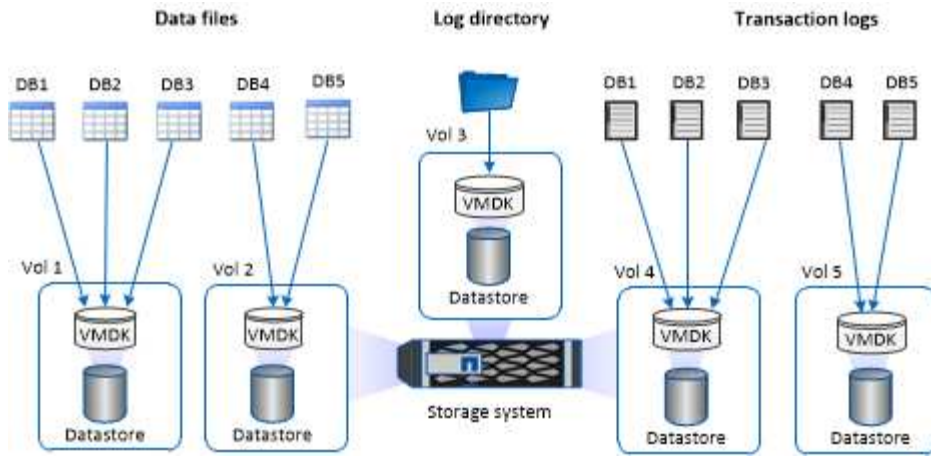
下圖顯示如何在 LUN 上配置中型或小型資料庫的儲存佈局：



下圖顯示如何在 VMDK 上配置大型資料庫的儲存佈局：



下圖顯示如何在 VMDK 上配置中型或小型資料庫的儲存佈局：



SQL 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令： ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - 倫
 - lun 創建
 - lun 刪除
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 秀
 - lun 映射新增報告節點
 - lun 映射創建
 - lun映射刪除
 - lun 映射刪除報告節點
 - 倫圖秀
 - lun修改
 - lun 移入磁碟區
 - lun 離線
 - 倫在線
 - lun 大小調整

- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線
- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照重命名

- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 網路介面
- 網路介面顯示
- 虛擬伺服器
- 大都會集群秀

為 SQL Server 外掛程式準備SnapMirror和SnapVault複製的儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

SQL Server 資源的備份策略

定義 SQL Server 資源的備份策略

在建立備份作業之前定義備份策略有助於確保您擁有成功還原或複製資料庫所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是指服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於備份策略。

支援的備份類型

使用SnapCenter備份 SQL Server 系統和使用者資料庫需要您選擇資源類型，例如資料庫、SQL 伺服器執行個體和可用性群組 (AG)。利用快照技術來建立資源所在磁碟區的線上、唯讀副本。

您可以選擇僅複製選項來指定 SQL Server 不截斷交易日誌。當您使用其他備份應用程式管理 SQL Server 時，應使用此選項。保持交易日誌完整可使任何備份應用程式還原系統資料庫。僅複製備份與排程備份的順序無關，且不會影響資料庫的備份和還原過程。

備份類型	描述	具有備份類型的僅複製選項
完整備份和日誌備份	備份系統資料庫並截斷交易日誌。 SQL Server 透過刪除已提交至資料庫的項目來截斷交易日誌。 完整備份完成後，此選項會建立一個擷取交易資訊的交易日誌。通常，您應該選擇此選項。但是，如果您的備份時間很短，您可以選擇不執行交易日誌備份，而是進行完整備份。 您不能為 master 和 msdb 系統資料庫建立日誌備份。但是，您可以為模型系統資料庫建立日誌備份。	備份系統資料庫檔案和交易日誌而不截斷日誌。 僅複製備份不能作為差異基準或差異備份，且不會影響差異基準。恢復僅複製完整備份與恢復任何其他完整備份相同。

備份類型	描述	具有備份類型的僅複製選項
完整資料庫備份	備份系統資料庫檔案。 您可以為主資料庫、模型資料庫和 msdb 系統資料庫建立完整的資料庫備份。	備份系統資料庫檔案。
交易日誌備份	備份截斷的交易日誌，僅複製自最近的交易日誌備份以來提交的交易。 如果您安排頻繁的交易日誌備份和完整的資料庫備份，則可以選擇粒度復原點。	備份交易日誌而不截斷它們。 此備份類型不會影響常規日誌備份的順序。僅複製日誌備份對於執行線上復原作業很有用。

SQL 伺服器外掛程式的備份計劃

備份頻率（計畫類型）在策略中指定；備份計畫在資源組配置中指定。確定備份頻率或計畫的最關鍵因素是資源的變化率和資料的重要性。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA 和 RPO 有助於資料保護策略。

即使是使用頻繁的資源，也不需要每天執行一次或兩次以上的完整備份。例如，定期的交易日誌備份可能足以確保您擁有所需的備份。備份資料庫的頻率越高，SnapCenter 在復原時需要使用的交易日誌就越少，因此可以加快復原作業的速度。

備份計畫分為兩部分，如下所示：

- 備份頻率

備份頻率（執行備份的頻率），對於某些外掛程式來說稱為 計畫類型，是策略配置的一部分。您可以選擇每小時、每天、每週或每月作為策略的備份頻率。如果您未選擇任何頻率，則建立的策略是僅按需策略。您可以透過點選「設定」>「策略」來存取策略。

- 備份計畫

備份計畫（確切地指定執行備份的時間）是資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份。您可以透過點選「資源」>「資源群組」來存取資源組計畫。

資料庫所需的備份作業數量

決定所需備份作業數量的因素包括資料庫的大小、使用的捲數、資料庫的變化率以及服務等級協定 (SLA)。

對於資料庫備份，您選擇的備份作業的數量通常取決於放置資料庫的磁碟區的數量。例如，如果將一組小型資料

庫放在一個磁碟區上，將一個大型資料庫放在另一個磁碟區上，則可以為小型資料庫建立備份作業，為大型資料庫建立一個備份作業。

SQL 伺服器外掛程式的備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

```
resourcegroupname_hostname_timestamp
```

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳後綴會加入到快照名稱中。

SQL Server 外掛程式的備份保留選項

您可以選擇保留備份副本的天數，或指定要保留的備份副本數量，ONTAP 最多可保留 255 份。例如，您的組織可能要求您保留 10 天的備份副本或 130 份備份副本。

建立策略時，您可以指定備份類型和計畫類型的保留選項。

如果您設定了 SnapMirror 複製，則保留政策將在目標磁碟區上鏡像。

SnapCenter 會刪除具有與計劃類型相符的保留標籤的保留備份。如果資源或資源群組的計劃類型發生更改，則具有舊計劃類型標籤的備份可能仍保留在系統中。



為了長期保留備份副本，您應該使用 SnapVault 備份。

在來源儲存系統上保留交易日誌備份多長時間

適用於 Microsoft SQL Server 的 SnapCenter 外掛程式需要交易日誌備份來執行最新的還原作業，將資料庫還原到兩次完整備份之間的時間。

例如，如果 Plug-in for SQL Server 在上午 8:00 進行了一次完整備份，並在下午 5:00 進行了另一次完整備份，則它可以使用最新的交易日誌備份將資料庫還原到上午 8:00 至下午 5:00 之間的任何時間。如果沒有交易日誌，則 Plug-in for SQL Server 只能執行時間點還原作業，即將資料庫還原到 Plug-in for SQL Server 完成完整備份

的時間。

通常，您只需要一兩天的最新恢復操作。預設情況下， SnapCenter至少保留兩天。

同一卷上的多個資料庫

您可以將所有資料庫放在同一磁碟區上，因為備份策略有一個選項可以設定每個備份的最大資料庫數量（預設值為 100）。

例如，如果同一磁碟區中有 200 個資料庫，則會建立兩個快照，每個快照包含 100 個資料庫。

使用 **Plug-in for SQL Server** 的主儲存磁碟區或輔助儲存磁碟區進行備份副本驗證

您可以驗證主儲存磁碟區或SnapMirror或SnapVault二級儲存磁碟區上的備份副本。使用輔助儲存磁碟區進行驗證可減少主儲存磁碟區的負載。

當您驗證主儲存磁碟區或輔助儲存磁碟區上的備份時，所有主快照和輔助快照都會被標記為已驗證。

需要SnapRestore授權來驗證SnapMirror和SnapVault二級儲存磁碟區上的備份副本。

何時安排驗證工作

儘管SnapCenter可以在建立備份後立即驗證備份，但這樣做會顯著增加完成備份作業所需的時間，並且耗費大量資源。因此，最好將驗證安排在以後的單獨工作中。例如，如果您每天下午 5:00 備份資料庫，則可以安排驗證在一小時後的下午 6:00 進行

基於相同的原因，通常不需要在每次執行備份時都執行備份驗證。定期但頻率較低的驗證通常足以確保備份的完整性。單一驗證作業可以同時驗證多個備份。

SQL Server 的復原策略

還原操作的來源和目標

您可以從主儲存或輔助儲存體上的備份副本還原 SQL Server 資料庫。除了原始位置之外，您還可以將資料庫還原到不同的目標位置，從而可以選擇支援您要求的目標位置。

恢復操作的來源

您可以從主儲存或輔助儲存還原資料庫。

恢復操作的目標

您可以將資料庫還原到各種目標：

目的地	描述
原址	預設情況下， SnapCenter將資料庫還原到相同 SQL Server 執行個體上的相同位置。

目的地	描述
不同地點	您可以將資料庫還原到同一主機內任何 SQL Server 執行個體上的不同位置。
原始位置或不同位置使用不同的資料庫名稱	您可以將具有不同名稱的資料庫還原到建立備份的相同主機上的任何 SQL Server 執行個體。



不支援跨 ESX 伺服器將 VMDK（NFS 和 VMFS 資料儲存區）上的 SQL 資料庫還原到備用主機。

SnapCenter 支援的 SQL Server 復原模型

預設情況下，每個資料庫類型都會指派特定的復原模型。SQL Server 資料庫管理員可以將每個資料庫重新指派到不同的復原模型。

SnapCenter 支援三種類型的 SQL Server 復原模型：

- 簡單恢復模型

當您使用簡單還原模型時，您無法備份交易日誌。

- 完全恢復模型

當您使用完整復原模型時，您可以將資料庫從故障點還原到先前的狀態。

- 批次日誌復原模型

當您使用批次日誌復原模型時，您必須手動重新執行批次日誌操作。如果在還原之前尚未備份包含作業提交記錄的交易日誌，則必須執行批次記錄作業。如果批次日誌作業在資料庫中插入了 1000 萬行數據，而資料庫在交易日誌備份之前發生故障，則還原的資料庫將不包含批次日誌作業插入的行。

恢復操作的類型

您可以使用 SnapCenter 對 SQL Server 資源執行不同類型的還原作業。

- 恢復最新狀態
- 恢復到之前的時間點

在以下情況下，您可以恢復到最新時間點或恢復到先前的時間點：

- 從 SnapMirror 或 SnapVault 二級儲存恢復
- 恢復到備用路徑（位置）



SnapCenter 不支援基於磁碟區的 SnapRestore。

在最新的復原操作（預設選擇）中，資料庫將恢復到故障點。 SnapCenter透過執行以下序列來實現此目的：

1. 在還原資料庫之前備份最後一個活動交易日誌。
2. 從您選擇的完整資料庫備份還原資料庫。
3. 套用所有未提交到資料庫的交易日誌（包括從備份建立時到目前時間的備份交易日誌）。

交易日誌被向前移動並應用於任何選定的資料庫。

最新的復原操作需要一組連續的交易日誌。

由於SnapCenter無法從日誌傳送備份檔案還原 SQL Server 資料庫交易日誌（日誌傳送可讓您自動將交易日誌備份從主伺服器執行個體上的主資料庫傳送至單獨的輔助伺服器執行個體上的一個或多個輔助資料庫），因此您無法從交易日誌備份執行最新的還原作業。因此，您應該使用SnapCenter來備份 SQL Server 資料庫交易記錄檔。

如果您不需要為所有備份保留最新的還原功能，則可以透過備份原則設定系統的交易日誌備份保留。

最新恢復操作的範例

假設您每天中午執行 SQL Server 備份，並且星期三下午 4:00 需要從備份中還原。由於某種原因，週三中午的備份未能驗證，因此您決定從週二中午的備份進行還原。此後，如果還原了備份，則所有交易日誌都會向前移動並應用於還原的資料庫，從建立星期二備份時未提交的交易日誌開始，一直到星期三下午 4:00 寫入的最新交易日誌（如果交易日誌已備份）。

恢復到之前的時間點

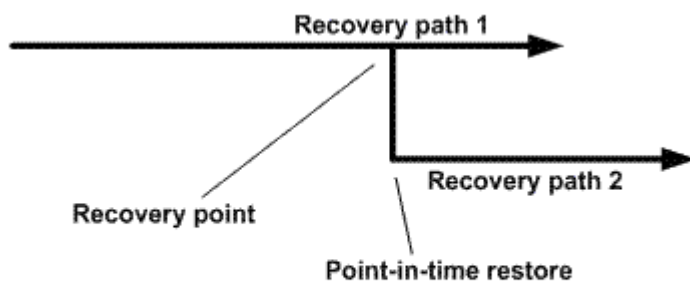
在時間點還原作業中，資料庫僅還原到過去的特定時間。時間點還原操作發生在下列還原情況：

- 資料庫還原到備份交易日誌中的給定時間。
- 資料庫已恢復，並且僅將備份交易日誌的子集套用至該資料庫。



將資料庫還原到某個時間點會產生新的復原路徑。

下圖說明了執行時間點還原作業時出現的問題：



在影像中，復原路徑 1 由完整備份和隨後的幾個交易日誌備份組成。您將資料庫還原到某個時間點。時間點還

原作業後會建立新的交易日誌備份，產生復原路徑 2。新的交易日誌備份是在沒有建立新的完整備份的情況下建立的。由於資料損壞或其他問題，您無法還原目前資料庫，直到建立新的完整備份。此外，無法將在復原路徑 2 中建立的交易日誌套用至屬於復原路徑 1 的完整備份。

如果您套用交易日誌備份，您也可以指定停止套用備份交易的特定日期和時間。為此，您需要指定可用範圍內的日期和時間，SnapCenter 將刪除該時間點之前未提交的任何交易。您可以使用此方法將資料庫還原到發生損壞之前的時間點，或從意外的資料庫或資料表刪除中復原。

時間點還原操作範例

假設您在午夜進行一次完整資料庫備份，並每小時進行一次交易日誌備份。資料庫在上午 9:45 崩潰，但您仍然備份了故障資料庫的交易日誌。您可以從以下時間點還原場景中進行選擇：

- 恢復午夜所做的完整資料庫備份，並接受隨後所做的資料庫變更的遺失。（選項：無）
- 還原完整的資料庫備份並套用所有交易日誌備份直到上午 9:45（選項：記錄到）
- 還原完整的資料庫備份並套用交易日誌備份，指定您希望交易從最後一組交易日誌備份還原的時間。（選項：按具體時間）

在這種情況下，您需要計算報告某個錯誤的日期和時間。任何未在指定日期和時間之前提交的事務都將被刪除。

定義 SQL Server 的克隆策略

定義克隆策略使您能夠成功克隆資料庫。

1. 查看與克隆操作相關的限制。
2. 確定您需要的克隆類型。

克隆操作的限制

在克隆資料庫之前，您應該了解克隆操作的限制。

- 如果您使用的是 Oracle 11.2.0.4 至 12.1.0.1 中的任何版本，則執行 *renamedg* 指令時複製操作將處於暫停狀態。您可以套用 Oracle 補丁 19544733 來修復此問題。
- 不支援將資料庫從直接連接到主機的 LUN（例如，透過在 Windows 主機上使用 Microsoft iSCSI Initiator）複製到同一 Windows 主機或另一個 Windows 主機上的 VMDK 或 RDM LUN，反之亦然。
- 卷掛載點的根目錄不能是共享目錄。
- 如果將包含複製的 LUN 移至新磁碟區，則無法刪除該複製。

克隆操作的類型

您可以使用 SnapCenter 克隆 SQL Server 資料庫備份或生產資料庫。

- 從資料庫備份克隆

克隆的資料庫可以作為開發新應用程式的基準，並有助於隔離生產環境中發生的應用程式錯誤。克隆的資料庫也可用於從軟資料庫錯誤中復原。

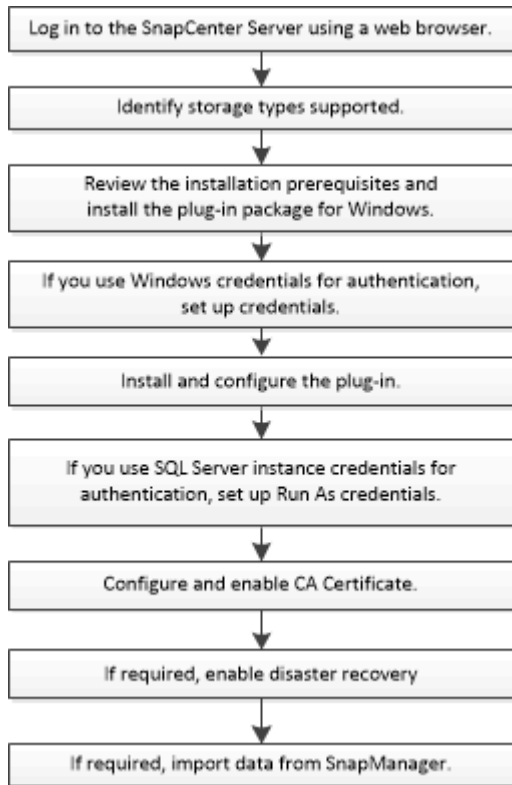
- 複製生命週期

您可以使用SnapCenter來安排在生產資料庫不忙碌時發生的重複克隆作業。

準備安裝適用於 **Microsoft SQL Server** 的SnapCenter插件

SnapCenter Plug-in for Microsoft SQL Server 的安裝工作流程

如果您想要保護 SQL Server 資料庫，則應該安裝並設定適用於 Microsoft SQL Server 的SnapCenter外掛程式。



新增主機並安裝適用於 **Microsoft SQL Server** 的SnapCenter外掛程式的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。

- 如果您正在使用 iSCSI，則 iSCSI 服務必須正在執行。
- 您必須擁有具有本機管理員權限的用戶，且該用戶在遠端主機上具有本機登入權限。
- 如果您在SnapCenter中管理叢集節點，則必須擁有對叢集中所有節點具有管理權限的使用者。
- 您必須擁有在 SQL Server 上具有 sysadmin 權限的使用者。

適用於 Microsoft SQL Server 的SnapCenter外掛程式使用 Microsoft VDI 框架，該框架需要系統管理員存取權。

"[Microsoft 支援文章 2926557：SQL Server VDI 備份與還原作業需要 Sysadmin 權限](#)"

- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。

- 如果安裝了SnapManager for Microsoft SQL Server，則必須停止或停用該服務和計畫。

如果您打算將備份或複製作業匯入SnapCenter，請不要解除安裝SnapManager for Microsoft SQL Server。

- 主機必須能夠解析為伺服器的完全限定網域名稱 (FQDN)。

如果修改了 hosts 檔案以使其可解析，並且在 hosts 檔案中指定了短名稱和 FQDN，則在SnapCenter hosts 檔案中建立一個項目，格式如下：<ip_address> <host_fqdn> <host_name>

安裝適用於 Windows 的SnapCenter插件包的主機需求

在安裝適用於 Windows 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

為 Windows 的SnapCenter插件包設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

開始之前

- 在安裝插件之前，您必須設定 Windows 憑證。
- 您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。
- Windows 主機上的 SQL 驗證

安裝插件後，您必須設定 SQL 憑證。

如果您正在為 Microsoft SQL Server 部署SnapCenter插件，則必須在安裝插件後設定 SQL 憑證。為具有 SQL Server sysadmin 權限的使用者設定憑證。

SQL 驗證方法針對 SQL Server 執行個體進行驗證。這意味著必須在SnapCenter中發現 SQL Server 執行個體。因此，在新增SQL憑證前，必須先新增主機、安裝外掛程式包、刷新資源。您需要 SQL Server 驗證才能執行諸如調度或發現資源之類的操作。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。

對於這個領域...	這樣做...
使用者名稱/密碼	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員 指定要安裝SnapCenter插件的系統上的網域管理員。用戶名字段的有效格式為： ◦ NetBIOS\UserName ◦ Domain FQDN\UserName • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。用戶名字段的有效格式為：UserName 請勿在密碼中使用雙引號 (") 或反引號 (`) 。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，lessthan<!10、lessthan10<!、backtick`12。
認證模式	選擇您想要使用的身份驗證模式。如果選擇SQL驗證模式，也必須指定SQL伺服器執行個體以及SQL實例所在的主機。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

為單一 **SQL Server** 資源配置憑證

您可以設定憑證來為每個使用者在單獨的 SQL Server 資源上執行資料保護作業。雖然您可以全域設定憑證，但您可能只想針對特定資源執行此操作。

關於此任務

- 如果您使用 Windows 憑證進行驗證，則必須在安裝外掛程式之前設定您的憑證。

但是，如果您使用 SQL Server 執行個體進行驗證，則必須在安裝外掛程式後新增憑證。

- 如果您在設定憑證時啟用了 SQL 驗證，則發現的執行個體或資料庫將顯示紅色掛鎖圖示。

如果出現掛鎖圖標，則必須指定實例或資料庫憑證才能成功將實例或資料庫新增至資源組。

- 當滿足下列條件時，您必須將憑證指派給沒有 sysadmin 存取權限的基於角色的存取控制 (RBAC) 使用者：

- 憑證已指派給 SQL 實例。
- SQL 實例或主機被指派給 RBAC 使用者。

使用者必須同時擁有資源群組和備份權限。

步驟 1：新增並設定憑證

1. 在左側導覽窗格中，選擇「設定」。
2. 在設定頁面中，選擇*憑證*。
 - a. 若要新增憑證，請選擇「新建」。
 - b. 在憑證頁面中，設定憑證：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱	輸入用於 SQL Server 驗證的使用者名稱。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter外掛程式的系統上的網域管理員或管理員群組的任何成員。「使用者名稱」欄位的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 • 本機管理員（僅限工作群組）對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名稱 欄位的有效格式為：<i>UserName</i>
密碼	輸入用於身份驗證的密碼。
認證方式	選擇 SQL Server 驗證模式。如果 Windows 使用者在 SQL 伺服器上具有 sysadmin 權限，您也可以選擇 Windows 驗證。
主持人	選擇主機。
SQL Server 執行個體	選擇 SQL Server 執行個體。

- c. 選擇“確定”新增憑證。

步驟 2：設定實例

1. 在左側導覽窗格中，選擇「資源」。
2. 在資源頁面中，從*檢視*清單中選擇*實例*。

- a. 選擇 image:.../media/filter_icon.png[過濾器圖示]，然後選擇主機名稱來過濾實例。
 - b. 選擇 image:.../media/filter_icon.png[filter icon] 以關閉過濾器窗格。
3. 在實例保護頁面中，保護實例，如果需要，選擇*配置憑證*。

如果登入 SnapCenter 伺服器的使用者無法存取 Microsoft SQL Server 的 SnapCenter 插件，則使用者必須設定憑證。



憑證選項不適用於資料庫和可用性群組。

4. 選擇*刷新資源*。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
 - b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA：Install-AdServiceAccount <gMSA>
 - c. 透過執行以下命令驗證你的 gMSA 帳戶：Test-AdServiceAccount <gMSA>
5. 將管理權限指派給主機上配置的 gMSA。
6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

為 Microsoft SQL Server 安裝 SnapCenter 插件

新增主機並安裝適用於 **Windows** 的 SnapCenter 插件包

您必須使用 SnapCenter *新增主機* 頁面來新增主機並安裝插件包。插件會自動安裝在遠端主機上。

開始之前

- 如果 SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 在 Windows 主機上安裝外掛程式時，如果指定非內建的憑證，則應在主機上停用 UAC。
- 您應該確保訊息佇列服務處於運行狀態。

- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

["在 Windows Server 2016 或更高版本上為 SQL 設定組託管服務帳戶"](#)

關於此任務

您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。

您可以新增主機並為單一主機或叢集安裝插件包。如果您在叢集或 Windows Server 故障轉移叢集 (WSFC) 上安裝插件，則插件將安裝在叢集的所有節點上。

有關管理主機的信息，請參閱["管理主機"](#)。

步驟

1. 在左側導覽窗格中，選擇*主機*。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 選擇“新增”。
4. 在「主機」頁面中執行以下操作：

對於這個領域...	這樣做...
主機類型	選擇 Windows 作為主機類型。SnapCenter伺服器會新增主機，然後安裝適用於 Windows 的插件（如果主機上尚未安裝該插件）。 如果您在「外掛程式」頁面上選擇「Microsoft SQL Server」選項，SnapCenter伺服器將安裝 SQL Server 外掛程式。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。只有當 IP 位址解析為 FQDN 時，不受信任的網域主機才支援該 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • WSFC 如果您使用SnapCenter新增主機且該主機是子網域的一部分，則必須提供 FQDN。

對於這個領域...	這樣做...
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標置於指定的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在*選擇要安裝的插件*部分中，選擇要安裝的插件。

6. 選擇*更多選項*。

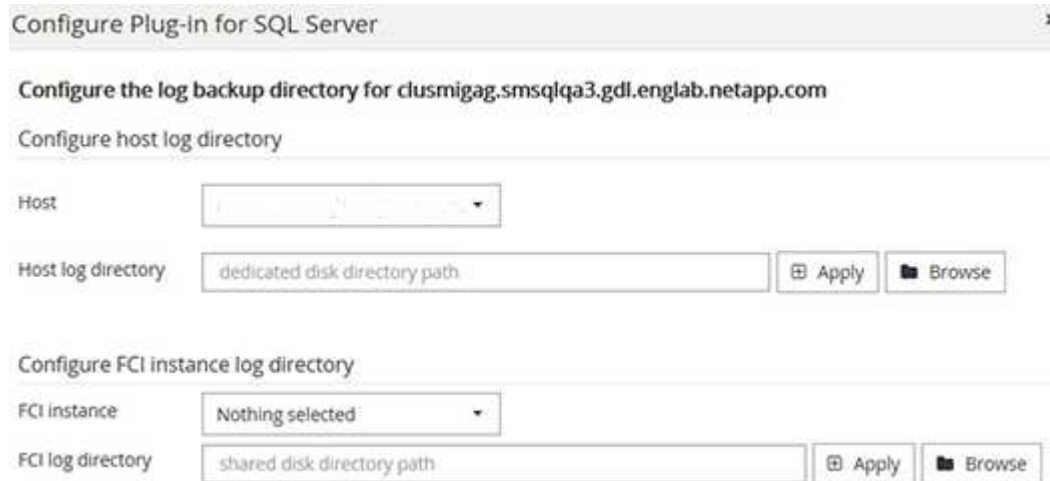
對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您可以選擇自訂路徑。
新增叢集中的所有主機	選取此核取方塊可新增 WSFC 或 SQL 可用性群組中的所有叢集節點。如果您想要管理和識別叢集內的多個可用的 SQL 可用性群組，則應該透過選擇 GUI 中的對應叢集複選框來新增所有叢集節點。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	如果要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。 以以下格式提供 gMSA 名稱 ：domainName\accountName\$。  如果主機新增了 gMSA，且 gMSA 具有登入和系統管理員權限，則 gMSA 將用於連線到 SQL 實例。

7. 選擇*提交*。

8. 對於SQL插件，選擇主機來設定日誌目錄。

a. 選擇*設定日誌目錄*，在設定主機日誌目錄頁面中選擇*瀏覽*並完成下列步驟：

僅列出NetApp LUN（驅動器）可供選擇。 SnapCenter在備份作業過程中備份並複製主機日誌目錄。



i. 選擇主機上將儲存主機日誌的磁碟機號碼或掛載點。

ii. 如果需要，請選擇一個子目錄。

iii. 選擇*儲存*。

9. 選擇*提交*。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）和 Java 版本（適用於 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 檔案以修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

10. 監控安裝進度。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Microsoft SQL Server** 的SnapCenter插件

您可以使用 Install-SmHostPackage PowerShell cmdlet 同時在多個主機上安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式。

開始之前

您必須以網域使用者身分登入SnapCenter，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，使用 Open-SmConnection cmdlet 建立會話，然後輸入您的憑證。
3. 使用 Install-SmHostPackage cmdlet 和所需參數在多個遠端主機上安裝適用於 Microsoft SQL Server

的SnapCenter外掛程式。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

當您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

從命令列靜默安裝適用於 **Microsoft SQL Server** 的SnapCenter插件

您應該從SnapCenter使用者介面安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式。但是，如果您因為某些原因無法這樣做，您可以從 Windows 命令列以靜默模式無人值守執行 SQL Server 外掛程式安裝程式。

開始之前

- 在安裝之前，您必須刪除適用於 Microsoft SQL Server 的早期版本的SnapCenter外掛程式。

有關更多信息，請參閱 ["如何從插件主機手動直接安裝SnapCenter插件"](#)。

步驟

1. 驗證插件主機上是否存在 `C:\temp` 資料夾以及登入使用者是否對該資料夾具有完全存取權限。
2. 從 `C:\ProgramData\NetApp\SnapCenter\Package Repository` 下載 SQL Server 軟體插件。

可以從安裝SnapCenter伺服器的主機存取此路徑。

3. 將安裝檔案複製到要安裝插件的主機上。
4. 從本機上的 Windows 命令提示符，導覽至儲存插件安裝檔案的目錄。
5. 安裝 SQL Server 軟體插件：

```
"snapcenter_windows_host_plugin.exe"/silent /debuglog"Debug_Log_Path"  
/log"Log_Path" BI_SNAPCENTER_PORT=Num  
SUITE_INSTALLDIR="Install_Directory_Path"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```

用您的資料替換佔位符值

- `Debug_Log_Path` 是套件安裝程式日誌檔案的名稱和位置。
- `Log_Path` 是插件元件（SCW、SCSQL 和 SMCore）的安裝日誌的位置。
- `Num` 是SnapCenter與 SMCore 通訊的端口
- `Install_Directory_Path`是主機插件包安裝目錄。
- `domain\administrator` 是 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式。
- `password` 是 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式的密碼。+
`"snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145
SUITE_INSTALLDIR="C:\Program Files\NetApp\SnapCenter"`

```
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW,SCSQL
```



安裝 SQL Server 外掛程式期間傳遞的所有參數都區分大小寫。

6. 監視 Windows 工作排程器、主安裝記錄檔 C:\Installdebug.log 以及 C:\Temp 中的附加安裝檔。
7. 監控 %temp% 目錄以驗證 msie.exe 安裝程式是否正在無錯誤地安裝軟體。



SQL Server 插件的安裝在主機上註冊該插件，而不是在 SnapCenter 伺服器上註冊。您可以透過使用 SnapCenter GUI 或 PowerShell cmdlet 新增主機在 SnapCenter 伺服器上註冊插件。新增主機後，會自動發現插件。

監控 SQL Server 插件的安裝狀態

您可以使用「作業」頁面監控 SnapCenter 插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

- 進行中
- 成功完成
- 失敗的
- 已完成但有警告，或因警告而無法啟動
- 排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾「受信任的根憑證授權單位」，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-Childitem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 **Windows** 主機插件服務設定 **CA** 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- ．透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

為插件啟用 CA 憑證

您應該設定 CA 憑證並在 SnapCenter 伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器和插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

配置災難復原

SnapCenter 插件 for SQL Server 的災難復原

當 SQL Server 的 SnapCenter 外掛程式關閉時，請使用下列步驟切換到其他 SQL 主機並還原資料。

開始之前

- 輔助主機應具有與主主機相同的作業系統、應用程式和主機名稱。
- 使用「新增主機」或「修改主機」頁面將 SQL Server 的 SnapCenter 外掛程式推送到備用主機。看["管理主機"](#)了解更多。

步驟

1. 從「主機」頁面中選擇主機來修改並安裝 SQL Server 的 SnapCenter 插件。
2. （可選）將 SQL Server 設定檔的 SnapCenter 插件從災難復原 (DR) 備份取代到新電腦。
3. 從 DR 備份中的 SQL Server 資料夾的 SnapCenter 插件匯入 Windows 和 SQL 計畫。

相關資訊

查看["災難復原 API"](#)影片。

SnapCenter Plug-in for SQL Server 的儲存災難復原 (DR)

您可以透過在「全域設定」頁面中啟用儲存的 DR 模式來還原用於 SQL Server 儲存的 SnapCenter 插件。

開始之前

- 確保插件處於維護模式。
- 中斷 SnapMirror/ SnapVault 關係。["中斷 SnapMirror 關係"](#)
- 將從屬磁碟的 LUN 連接到具有相同磁碟機號碼的主機。
- 確保所有磁碟都使用 DR 之前使用的相同磁碟機號碼進行連接。
- 重新啟動 MSSQL 伺服器服務。
- 確保 SQL 資源重新連線。

關於此任務

VMDK 和 RDM 配置不支援災難復原 (DR)。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「災難復原」。
2. 選擇“啟用災難復原”。
3. 按一下“應用”。
4. 按一下「監控」>「作業」來驗證 DR 作業是否已啟用。

完成後

- 如果故障轉移後建立了新的資料庫，則資料庫將處於非 DR 模式。

新的資料庫將像故障轉移之前一樣繼續運作。

- 在 DR 模式下建立的新備份將在拓樸頁面中的SnapMirror或SnapVault（輔助）下列出。

新備份旁邊會顯示一個「i」圖標，表示這些備份是在 DR 模式期間建立的。

- 您可以使用 UI 或以下 cmdlet 刪除故障轉移期間建立的 SQL Server 備份的SnapCenter插件：Remove-SmBackup
- 故障轉移後，如果您希望某些資源處於非 DR 模式，請使用下列 cmdlet：Remove-SmResourceDRMode

更多資訊請參閱 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

- SnapCenter Server 將管理處於 DR 或非 DR 模式的單一儲存資源（SQL 資料庫），但不管理處於 DR 模式或非 DR 模式的儲存資源的資源群組。

從適用於 **SQL Server** 二級儲存的**SnapCenter**插件故障還原到主儲存

在 SQL Server 主儲存的SnapCenter外掛程式還原連線後，您應該故障還原到主儲存。

開始之前

- 從託管主機頁面將 SQL Server 的SnapCenter插件置於*維護*模式。
- 中斷輔助儲存與主機的連線並從主儲存進行連線。
- 若要故障恢復到主儲存，請透過執行反向重新同步操作確保關係方向與故障轉移之前保持相同。

為了在反向重新同步操作後保留主儲存和輔助儲存的角色，請再次執行反向重新同步操作。

更多資訊請參見"[反向重新同步鏡像關係](#)"

- 重新啟動 MSSQL 伺服器服務。
- 確保 SQL 資源重新連線。



在插件故障轉移或故障回復期間，插件整體狀態不會立即刷新。主機和插件的整體狀態在後續的主機刷新操作中更新。

步驟

1. 在「設定」頁面中，導覽至「設定」>「全域設定」>「災難復原」。
2. 取消選擇“啟用災難復原”。
3. 按一下“應用”。
4. 按一下「監控」>「作業」來驗證 DR 作業是否已啟用。

完成後

您可以使用 UI 或以下 cmdlet 刪除故障轉移期間建立的 SQL Server 備份的SnapCenter插件：Remove-SmDRFailoverBackups

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 `/opt/netapp/config/crl`。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

做好資料保護準備

使用適用於 **Microsoft SQL Server** 的SnapCenter外掛程式的先決條件

在開始使用 SQL Server 外掛程式之前，SnapCenter管理員必須安裝和設定SnapCenter Server 並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。
- 登入SnapCenter。
- 透過新增或指派儲存系統連線並建立憑證來配置SnapCenter環境。



SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。SnapCenter支援的每個 SVM 都必須具有唯一的名稱。

- 新增主機、安裝插件、發現（刷新）資源、配置插件。
- 透過執行 `Invoke-SmConfigureResources` 將現有的 Microsoft SQL Server 資料庫從本機磁碟移至NetApp LUN 或反之亦然。

有關運行 cmdlet 的信息，請參閱 ["SnapCenter軟體 Cmdlet 參考指南"](#)

- 如果您使用SnapCenter Server 保護駐留在 VMware RDM LUN 或 VMDK 上的 SQL 資料庫，則必須部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊外掛程式。SnapCenter Plug-in for VMware vSphere文件包含更多資訊。

["SnapCenter Plug-in for VMware vSphere文檔"](#)

- 使用適用於 Microsoft Windows 的SnapCenter外掛程式執行主機端儲存配置。
- 如果您想要備份複製，請設定SnapMirror和SnapVault關係。

有關詳細信息，請參閱SnapCenter安裝資訊。

對於SnapCenter 4.1.1 用戶，SnapCenter Plug-in for VMware vSphere包含有關保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.2.x 用戶，NetApp Data Broker 1.0 和 1.0.1 文件包含有關使用基於 Linux 的NetApp Data Broker 虛擬設備（開放虛擬設備格式）提供的適用SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.3.x 用戶，SnapCenter Plug-in for VMware vSphere文件包含有關使用基於 Linux 的SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。

"SnapCenter Plug-in for VMware vSphere文檔"

如何使用資源、資源群組和原則來保護 **SQL Server**

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的資料庫、資料庫執行個體或 Microsoft SQL Server 可用性群組。
- SnapCenter資源群組是主機或叢集上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

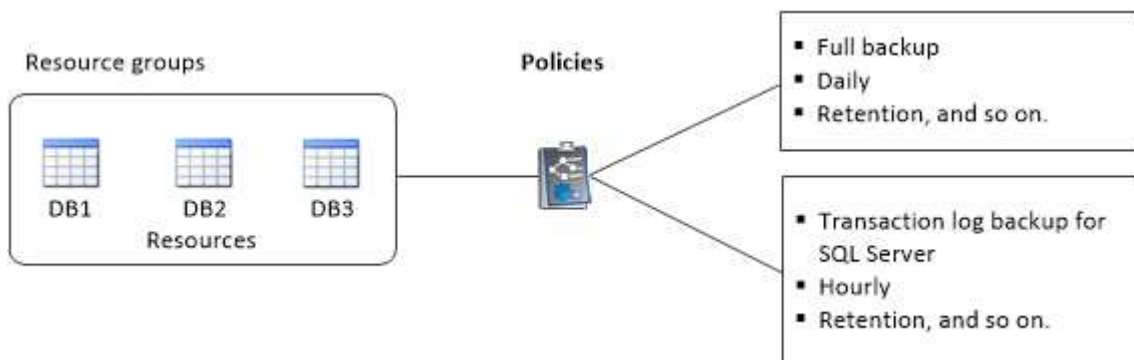
您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、副本保留、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

可以將資源群組視為定義您想要保護的內容以及您想要在日期和時間方面保護的內容。把政策想像成定義你想如何保護它。例如，如果要備份主機的所有資料庫或所有檔案系統，則可以建立包含主機中的所有資料庫或所有檔案系統的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加策略時，您可以設定資源組以每天執行一次完整備份，並配置另一個每小時執行一次日誌備份的計畫。

下圖說明了資料庫的資源、資源群組和策略之間的關係：



備份 **SQL Server** 資料庫、執行個體或可用性群組

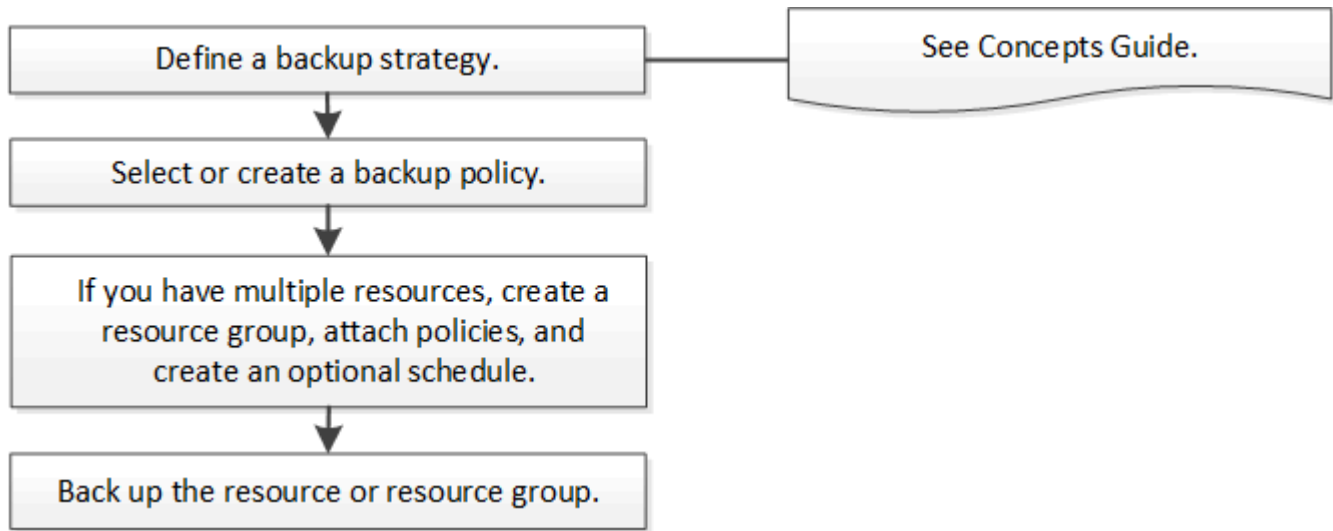
備份工作流

在您的環境中安裝適用於 Microsoft SQL Server 的SnapCenter外掛程式時，您可以使用SnapCenter備份 SQL Server 資源。

您可以安排多個備份同時在伺服器之間執行。

不能對相同資源同時執行備份和復原作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



如果您選擇非NetApp LUN、已損壞的資料庫或正在復原的資料庫，則「資源」頁面上的「立即備份」、「復原」、「管理備份」和「複製」選項將會停用。

您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原、還原、驗證和複製作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 ["SnapCenter 軟體 Cmdlet 參考指南"](#)

SnapCenter 如何備份資料庫

SnapCenter 使用 Snapshot 技術來備份駐留在 LUN 或 VMDK 上的 SQL Server 資料庫。SnapCenter 透過建立資料庫快照來建立備份。

當您從資源頁面選擇一個資料庫進行完整資料庫備份時，SnapCenter 會自動選擇駐留在同一儲存磁碟區上的所有其他資料庫。如果 LUN 或 VMDK 僅儲存單一資料庫，則可以單獨清除或重新選擇該資料庫。如果 LUN 或 VMDK 包含多個資料庫，則必須清除或重新選擇資料庫作為一個群組。

駐留在單一磁碟區上的所有資料庫都使用快照同時備份。如果並發備份資料庫的最大數量為 35，且儲存磁碟區中駐留的資料庫超過 35 個，則建立的快照總數等於資料庫數量除以 35。



您可以在備份策略中配置每個快照的最大資料庫數量。

當 SnapCenter 建立快照時，整個儲存系統磁碟區都會被擷取到快照中。但是，備份僅對建立備份的 SQL 主機伺服器有效。

如果其他 SQL 主機伺服器的資料駐留在同一磁碟區上，則無法從快照還原該資料。

查找更多資訊

["靜默或分組資源操作失敗"](#)

確定資源是否可用於備份

資源是由您安裝的外掛程式維護的資料庫、應用程式執行個體、可用性群組和類似元件。您可以將這些資源新增至資源組中，以便執行資料保護作業，但首先必須確定您有哪些可用資源。確定可用資源也可以驗證插件安裝是否已成功完成。

開始之前

- 您必須已經完成安裝SnapCenter Server、新增主機、建立儲存系統連線和新增憑證等任務。
- 要發現 Microsoft SQL 資料庫，應滿足以下條件之一。
 - 用於將插件主機新增至SnapCenter Server 的使用者應具有 Microsoft SQL Server 上所需的權限 (sysadmin)。
 - 如果不符合上述條件，則應在SnapCenter伺服器中設定在 Microsoft SQL Server 上具有所需權限 (sysadmin) 的使用者。使用者應在 Microsoft SQL Server 執行個體層級進行配置，並且可以是 SQL 或 Windows 使用者。
- 若要發現 Windows 群集中的 Microsoft SQL 資料庫，必須解除故障轉移群集執行個體 (FCI) TCP/IP 連接埠的封鎖。
- 如果資料庫駐留在 VMware RDM LUN 或 VMDK 上，則必須部署SnapCenter Plug-in for VMware vSphere 並向SnapCenter註冊外掛程式。

有關詳細信息，請參閱 ["SnapCenter Plug-in for VMware vSphere"](#)

- 如果主機新增了 gMSA，且 gMSA 具有登入和系統管理員權限，則 gMSA 將用於連線到 SQL 實例。

關於此任務

當「詳細資料」頁面中的「整體狀態」選項設定為「無法用於備份」時，您無法備份資料庫。當下列任一情況為真時，「總體狀態」選項將設定為「不可用於備份」：

- 資料庫不在NetApp LUN 上。
- 資料庫狀態不正常。

當資料庫處於離線、復原、復原待定、可疑等狀態時，它們就不處於正常狀態。

- 資料庫權限不足。

例如，如果使用者僅具有資料庫的檢視權限，則無法識別資料庫的檔案和屬性，因此無法備份。



如果您在 SQL Server 標準版上具有可用性群組配置，則SnapCenter只能備份主資料庫。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*、實例*或*可用性群組。

點選  並選擇主機名稱和SQL Server執行個體來過濾資源。然後您可以點選  關閉篩選器窗格。

3. 按一下“刷新資源”。

新新增、重新命名或刪除的資源將更新至SnapCenter伺服器清單。



如果資料庫在SnapCenter之外重新命名，則必須刷新資源。

資源與資源類型、主機或叢集名稱、相關資源群組、備份類型、政策和總體狀態等資訊一起顯示。

- 如果資料庫位於非NetApp儲存上，`Not available for backup`顯示在*總體狀態*列中。

您無法對非NetApp儲存裝置上的資料庫執行資料保護操作。

- 如果資料庫位於NetApp儲存空間且未受保護，`Not protected`顯示在*總體狀態*列中。
- 如果資料庫位於NetApp儲存系統上並受到保護，則使用者介面顯示 Backup not run總體狀態 列中的消息。
- 如果資料庫位於NetApp儲存系統上並受到保護，並且觸發了資料庫備份，則使用者介面會顯示 Backup succeeded總體狀態 列中的消息。



如果您在設定憑證時啟用了 SQL 驗證，則發現的執行個體或資料庫將顯示紅色掛鎖圖示。如果出現掛鎖圖標，則必須指定實例或資料庫憑證才能成功將實例或資料庫新增至資源組。

1. SnapCenter管理員將資源指派給 RBAC 使用者後，RBAC 使用者必須登入並點選 刷新資源 才能查看資源的最新 整體狀態。

將資源遷移到NetApp儲存系統

使用適用於 Microsoft Windows 的SnapCenter外掛程式設定NetApp儲存系統後，您可以使用SnapCenter圖形使用者介面 (GUI) 或使用 PowerShell cmdlet 將資源移轉到NetApp儲存系統或從一個NetApp LUN 移轉到另一個NetApp LUN。

開始之前

- 您必須已將儲存系統新增至SnapCenter Server。
- 您必須刷新（發現）SQL Server 資源。

這些嚮導頁面上的大多數欄位都是不言自明的。以下資訊描述了您可能需要指導的一些欄位。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*或*實例*。
3. 從清單中選擇資料庫或實例，然後按一下*遷移*。
4. 在資源頁面中，執行以下操作：

對於這個領域...	這樣做...
資料庫名稱（可選）	如果您已選擇要遷移的實例，則必須從*資料庫*下拉清單中選擇該實例的資料庫。

對於這個領域...	這樣做...
選擇目的地	選擇資料和日誌檔案的目標位置。 資料和日誌檔案分別移動到所選NetApp磁碟機下的資料和日誌資料夾。如果資料夾結構中不存在任何資料夾，則建立一個資料夾並遷移資源。
顯示資料庫檔案詳細資料（可選）	當您想要遷移單一資料庫的多個檔案時，請選擇此選項。  當您選擇*實例*資源時，不會顯示此選項。
選項	選擇“刪除原始位置的遷移資料庫副本”以從來源中刪除資料庫副本。 可選：分離資料庫之前在表上運行更新統計資料。

5. 在驗證頁面中執行以下操作：

對於這個領域...	這樣做...
資料庫一致性檢查選項	選擇*運行前*以在遷移之前檢查資料庫的完整性。選擇*運行後*來檢查遷移後資料庫的完整性。
DBCC CHECKDB 選項	- 選擇 PHYSICAL_ONLY 選項將完整性檢查限制在資料庫的實體結構內，並偵測影響資料庫的頁面撕裂、校驗和失敗以及常見硬體故障。 - 選擇 NO_INFOMSGS 選項來抑制所有資訊訊息。 - 選擇 ALL_ERRORMSG 選項來顯示每個物件報告的所有錯誤。 - 如果您不想檢查非聚集索引，請選擇 NOINDEX 選項。 SQL Server 資料庫使用 Microsoft SQL Server 資料庫一致性檢查器 (DBCC) 來檢查資料庫中物件的邏輯和實體完整性。  您可能希望選擇此選項來減少執行時間。 - 選擇TABLOCK選項來限制檢查並取得鎖定，而不是使用內部資料庫快照。

6. 查看摘要，然後按一下完成。

為 SQL Server 資料庫建立備份策略

您可以在使用SnapCenter備份 SQL Server 資源之前為資源或資源群組建立備份策略，也可以在建立資源群組或備份單一資源時建立備份原則。

開始之前

- 您必須已經定義了您的資料保護策略。
- 您必須透過完成安裝SnapCenter、新增主機、識別資源和建立儲存系統連線等任務來為資料保護做好準備。
- 您必須已設定主機日誌目錄以進行日誌備份。
- 您必須刷新（發現）SQL Server 資源。
- 如果您要將快照複製到映像或保管庫，SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的儲存虛擬機器 (SVM)。

有關管理員如何向使用者指派資源的信息，請參閱SnapCenter安裝資訊。

- 如果您想要在前腳本和後腳本中執行 PowerShell 腳本，則應在 web.config 檔案中將 usePowershellProcessforScripts 參數的值設為 true。

預設值為 false。

- 查看SnapMirror主動同步特定的先決條件和限制。欲了解詳細信息，請參閱 ["SnapMirror主動同步的物件限制"](#)。

關於此任務

- 備份策略是一組規則，用於控制如何管理和保留備份以及資源或資源群組的備份頻率。此外，您還可以指定複製和腳本設定。當您想要將策略重新用於另一個資源群組時，在策略中指定選項可以節省時間。

SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
 - 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。

對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟 1：建立策略名稱

1. 在左側導覽窗格中，選擇「設定」。

2. 在設定頁面中，選擇*策略*。
3. 選擇“新建”。
4. 在*名稱*頁面中，輸入策略名稱和詳細資訊。

步驟 2：設定策略選項

1. 在「策略類型」頁面中，執行下列步驟：
 - a. 選擇您的儲存類型。
 - b. 選擇您的保單範圍。

完整備份和日誌備份

備份資料庫檔案和交易日誌並截斷交易日誌。

- i. 選擇*完整備份和日誌備份*。
- ii. 輸入每個快照應備份的最大資料庫數量。



如果要同時執行多個備份操作，則必須增加此值。

完整備份

備份資料庫檔案。

- i. 選擇*完整備份*。
- ii. 輸入每個快照應備份的資料庫的最大數量。預設值為 100



如果要同時執行多個備份操作，則必須增加此值。

日誌備份

- i. 備份交易日誌。
- ii. 選擇*日誌備份*。

僅複製備份

- i. 如果您使用其他備份應用程式備份資源，請選擇*僅複製備份*。

保持交易日誌完整允許任何備份應用程式還原資料庫。通常，您不應在任何其他情況下使用僅複製選項。



Microsoft SQL 不支援將「僅複製備份」選項與「完整備份和記錄備份」選項一起用於輔助儲存。

步驟 3：設定可用性群組設定

1. 在可用性群組設定部分中，執行以下操作：

- a. 僅在首選備份副本上備份。

選擇此選項僅在首選備份副本上備份。首選備份副本由 SQL Server 中為 AG 配置的備份首選項決定。

- b. 選擇要備份的副本。

選擇主 AG 副本或輔助 AG 副本進行備份。

- c. 選擇備份優先權（最小和最大備份優先權）

指定最小備份優先權數和最大備份優先權數，以決定要備份的 AG 副本。例如，最小優先權可以為 10，最大優先權可以為 50。在這種情況下，所有優先權大於 10 且小於 50 的 AG 副本都被視為備份。

預設情況下，最小優先權為 1，最大優先權為 100。



在叢集配置中，備份會根據策略中設定的保留設定保留在叢集的每個節點上。如果 AG 的擁有者節點發生變化，則根據保留設定進行備份，並且將保留前一個所有者節點的備份。AG 的保留僅適用於節點層級。

步驟 4：設定快照和複製設定

1. 在「快照和複製」頁面中，執行下列步驟：

- a. 透過選擇*按需*、*每小時*、*每日*、*每週*或*每月*來指定方案類型。

一個策略只能選擇一種計劃類型。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，但允許您為每個策略指派不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

步驟 5：配置最新的保留設置

1. 在「最新保留設定」部分中，根據備份類型頁面中所選的備份類型，執行下列操作中的一項或多項：

具體份數

僅保留特定數量的快照。

1. 選擇*保留適用於最近<number>天的日誌備份*選項，並指定要保留的天數。如果接近此限制，您可能需要刪除舊副本。

具體天數

將備份副本保留特定天數。

1. 選擇*保留適用於最後<number>天完整備份的日誌備份*選項，並指定保留日誌備份副本的天數。

步驟 6：配置快照設定

1. 對於完整備份保留設置，請執行以下操作：

a. 指定要保留的快照總數

- i. 若要指定要保留的快照數量，請選擇*要保留的副本*。
- ii. 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。



預設情況下，保留計數的值設定為 2。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。



最大保留值為 1018。如果保留設定的值高於底層NetApp ONTAP版本支援的值，則備份將會失敗。

2. 保留快照的時間長度

- a. 如果您想要指定在刪除快照之前保留快照的天數，請選擇「保留副本」**。

3. 選擇*Snapshot 副本鎖定期限*並指定天、月或年的持續時間。

Snaplock 保留期應少於 100 年。

4. 選擇一個策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

步驟 7：配置輔助複製選項

1. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

更新SnapMirror

建立本機 Snapshot 副本後更新SnapMirror。

1. 選擇此選項可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror）。

應為SnapMirror主動同步啟用此選項。

在二次複製期間，SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。

看["在拓撲頁面中檢視 SQL Server 備份和克隆"](#)。

更新SnapVault

建立 Snapshot 副本後更新SnapVault。

1. 選擇此選項可執行磁碟到磁碟的備份複製。

在二次複製期間，SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。

當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。

有關SnapLock Vault 的更多信息，請參閱 ["將 Snapshot 副本提交到保管庫目標上的 WORM"](#)

看["在拓撲頁面中檢視 SQL Server 備份和克隆"](#)。

錯誤重試次數

1. 輸入進程停止之前應發生的複製嘗試次數。

步驟 8：配置腳本設定

1. 在腳本頁面中，分別輸入應在備份作業之前或之後執行的前置腳本或後置腳本的路徑和參數。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報和傳送日誌。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。



您必須在ONTAP中設定SnapMirror保留策略，以便二級儲存不會達到快照的最大限制。

步驟 9：配置驗證設定

在驗證頁面中，執行以下步驟：

1. 在「執行以下備份計畫的驗證」部分中，選擇計畫頻率。
2. 在資料庫一致性檢查選項部分中，執行下列操作：

- a. 將完整性結構限制為資料庫的物理結構 (PHYSICAL_ONLY)
 - i. 選擇*將完整性結構限制為資料庫的實體結構 (PHYSICAL_ONLY)*以將完整性檢查限制為資料庫的實體結構，並偵測影響資料庫的頁面撕裂、校驗和失敗以及常見硬體故障。
 - b. 抑制所有資訊訊息 (NO_INFOMSGS)
 - i. 選擇*抑制所有訊息訊息 (NO_INFOMSGS)*以抑制所有訊息訊息。預設選擇。
 - c. 顯示每個物件報告的所有錯誤訊息 (ALL_ERRORMSGs)
 - i. 選擇*顯示每個物件報告的所有錯誤訊息 (ALL_ERRORMSGs)*以顯示每個物件報告的所有錯誤。
 - d. 不檢查非聚集索引 (NOINDEX)
 - i. 如果不想檢查非聚集索引，請選擇「不檢查非聚集索引 (NOINDEX)」。SQL Server 資料庫使用 Microsoft SQL Server 資料庫一致性檢查器 (DBCC) 來檢查資料庫中物件的邏輯和實體完整性。
 - e. 限制檢查並取得鎖，而不是使用內部資料庫快照 (TABLOCK)
 - i. 選擇*限制檢查並取得鎖定而不是使用內部資料庫快照副本 (TABLOCK)*來限制檢查並取得鎖定而不是使用內部資料庫快照。
3. 在*日誌備份*部分中，選擇*完成後驗證日誌備份*以在完成後驗證日誌備份。
 4. 在*驗證腳本設定*部分中，分別輸入在驗證操作之前或之後應執行的腳本或後腳本的路徑和參數。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

步驟 10：審核摘要

1. 查看摘要，然後選擇*完成*。

為 SQL Server 建立資源組並附加策略

資源組是一個容器，您可以將想要一起備份和保護的資源新增到其中。資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

您可以單獨保護資源，而無需建立新的資源組。您可以對受保護的資源進行備份。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新資料庫新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下將新資料庫新增至現有資源組。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。



如果您最近為SnapCenter新增了資源，請按一下「刷新資源」以查看新新增的資源。

3. 按一下“新建資源組”。
4. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組名稱。  資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
對 Snapshot 副本使用自訂名稱格式	可選：輸入自訂快照名稱和格式。例如，customtext_resourcegroup_policy_hostname 或 resourcegroup_hostname。預設情況下，時間戳記會附加到快照名稱。

5. 在資源頁面中，執行以下步驟：

- a. 從下拉清單中選擇主機名稱、資源類型和 SQL Server 執行個體來過濾資源清單。

 如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

- b. 若要將資源從「可用資源」部分移至「選取資源」部分，請執行下列步驟之一：

- 選擇「自動選擇相同儲存磁碟區上的所有資源」以將同一磁碟區上的所有資源移至「選取資源」部分。
- 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。

 您也可以透過點擊 * 來建立策略  *.

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 在「配置所選策略的計畫」部分中，按一下 *  * 在您想要設定計畫的政策的政策設定計畫列中。
- c. 在「為策略_policy_name_新增計畫」對話方塊中，透過指定開始日期、到期日和頻率來配置計畫，然後按一下「確定」。

您必須對策略中列出的每個頻率執行此操作。配置的計畫列在「為選定的策略配置計畫」部分的「已套用的計畫」列中。

- d. 選擇 Microsoft SQL Server 排程器。

您還必須選擇一個調度程序實例來與調度策略關聯。

如果不選擇 Microsoft SQL Server 排程程序，則預設為 Microsoft Windows 排程器。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。您不應修改排程並重新命名在 Windows 排程器或 SQL Server 代理程式中建立的備份作業。

7. 在驗證頁面中，執行以下步驟：

- a. 從*驗證伺服器*下拉清單中選擇驗證伺服器。

此清單包括在SnapCenter中新增的所有 SQL Server。您可以選擇多個驗證伺服器（本機主機或遠端主機）。



驗證伺服器版本應與託管主資料庫的 SQL 伺服器的版本和版本相符。

- a. 按一下「載入定位器」以載入SnapMirror和SnapVault卷，對二級儲存執行驗證。

- b. 選擇您要設定驗證計畫的策略，然後按一下*  *.

- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*運行計劃驗證*。

- d. 按一下“確定”。

配置的計畫列在「已套用的計畫」欄位中。您可以透過點擊 *  * 進行檢視和編輯 * 或點選 * 刪除  *.

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtptServer 指定 SMTP 伺服器詳細資訊。

9. 查看摘要，然後按一下「完成」。

相關資訊

["為 SQL Server 資料庫建立備份策略"](#)

在**ASA r2** 系統上建立資源組並啟用對 **Microsoft SQL Server** 資源的二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建​​立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

- a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtServer` 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

備份 SQL 資源的需求

在備份 SQL 資源之前，您必須確保滿足幾個要求。

- 您必須已將資源從非NetApp儲存系統移轉到NetApp儲存系統。
- 您必須已經建立了備份策略。
- 如果要將具有SnapMirror關係的資源備份到二級存儲，則分配給儲存使用者的ONTAP角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。
- 如果未將 SQL 執行個體憑證指派給 AD 使用者或群組，則由活動目錄 (AD) 使用者啟動的備份作業將會失敗。您必須從*設定* > *使用者存取*頁面將 SQL 實例憑證指派給 AD 使用者或群組。
- 您必須已建立附加有策略的資源群組。
- 如果資源組有來自不同主機的多個資料庫，則由於網路問題，某些主機上的備份操作可能會延遲觸發。您應該使用 `Set-SmConfigSettings` PS cmdlet 在 `web.config` 中設定 `FMaxRetryForUninitializedHosts` 的值。

使用 PowerShell cmdlet 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 執行資料保護作業之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的管理 LIF IP 位址。

步驟

1. 使用 `Open-SmConnection` cmdlet 啟動 PowerShell Core 連線會話。

此範例開啟一個 PowerShell 會話：

```
PS C:\> Open-SmConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

此範例建立一個新的儲存系統連線：

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例使用 Windows 憑證建立一個名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

備份 SQL 資源

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

關於此任務

- 為了優化備份操作，您應該在 DNS 伺服器中建立 Windows 叢集名稱和 IP 位址的反向查找記錄。
- 對於 Windows 憑證驗證，您必須在安裝外掛程式之前設定您的憑證。
- 對於 SQL Server 執行個體驗證，您必須在安裝外掛程式後新增憑證。
- 對於 gMSA 驗證，您必須在 新增主機 或 修改主機 頁面中向 SnapCenter 註冊主機時設定 gMSA，以啟用和使用 gMSA。
- 如果主機新增了 gMSA，且 gMSA 具有登入和系統管理員權限，則允許 gMSA 連線到 SQL 實例。
 - SnapCenter 將驗證是否配置了 SQL 執行個體的驗證。如果配置了身份驗證，則將使用此憑證存取 SQL 實例。
 - 如果未配置身份驗證，請使用 gMSA 查看 SQL 插件目前是否正在運行。如果插件正在運行，它將用於建立與 SQL 實例的連接。
 - 當未配置 SQL 執行個體的驗證且外掛程式無法執行時，將透過 Windows 憑證驗證存取 SQL 執行個體。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*、*實例*或*可用性群組*。
 - a. 選擇要備份的資料庫、執行個體或可用性群組。

當您備份實例時，有關該實例的最後備份狀態或時間戳記的資訊將不會在資源頁面中提供。

在拓樸視圖中，您無法區分備份狀態、時間戳記或備份是針對實例還是資料庫。

3. 在資源頁面中，選取*Snapshot 副本的自訂名稱格式*複選框，然後輸入要用於 Snapshot 名稱的自訂名稱格式。

例如，customtext_policy_hostname 或 resource_hostname。預設情況下，時間戳記會附加到快照名稱。

4. 在「策略」頁面中，執行以下任務：
 - a. 在「策略」部分中，從下拉清單中選擇一個或多個策略。

您可以透過選擇 *  * 啟動策略精靈。

在「為選定的策略配置計畫」部分中，列出了選定的策略。

- b. 選擇 *  * 在您想要設定計畫的政策的政策設定計畫列中。
- c. 在*新增政策時間表* `policy\_name`對話方塊中，配置計畫，然後選擇*確定*。

這裡 `policy\_name`是您選擇的策略的名稱。

配置的計畫列在「已套用的計畫」欄位中。

- a. 選擇“使用 Microsoft SQL Server 排程器”，然後從與排程原則關聯的“排程器實例”下拉清單中選擇排程器實例。
5. 在驗證頁面中，執行以下步驟：
 - a. 從*驗證伺服器*下拉清單中選擇驗證伺服器。

您可以選擇多個驗證伺服器（本機主機或遠端主機）。



驗證伺服器版本應等於或高於託管主資料庫的 SQL 伺服器的版本。

- a. 選擇*載入輔助定位器以驗證輔助備份*以驗證輔助儲存系統上的備份。
- b. 選擇您要設定驗證計畫的策略，然後選擇 *  *.
- c. 在新增驗證計畫_policy_name_對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*運行計劃驗證*。



如果驗證伺服器沒有儲存連接，驗證操作將失敗並出現錯誤：無法掛載磁碟。

d. 選擇“確定”。

配置的計劃列在「已套用的計劃」欄位中。

6. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

7. 查看摘要，然後選擇*完成*。

進入資料庫拓撲頁面。

8. 選擇*立即備份*。

9. 在備份頁面中，執行以下步驟：

a. 如果您已對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

b. 選擇*備份後驗證*來驗證您的備份。

c. 選擇*備份*。



您不應重新命名在 Windows 排程器或 SQL Server 代理程式中建立的備份作業。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

建立隱式資源組。您可以從「使用者造訪」頁面選擇相應的使用者或群組來查看。隱式資源組類型是“Resource”。

10. 透過選擇 **Monitor > Jobs** 來監控操作進度。

完成後

- 在MetroCluster配置中，SnapCenter可能無法在故障轉移後偵測到保護關係。

"MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"

- 如果您正在備份 VMDK 上的應用程式數據，並且 SnapCenter Plug-in for VMware vSphere 的 Java 堆大小不夠大，則備份可能會失敗。若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method`` 命令啟動 SnapCenter VMware 插件服務。將該命令更新為以下內容：``Java -jar -Xmx8192M -Xms4096M`。

相關資訊

"為 SQL Server 資料庫建立備份策略"

"由於 TCP_TIMEOUT 延遲，備份操作失敗，並出現 MySQL 連線錯誤"

"備份會因 Windows 排程器錯誤而失敗"

"靜默或分組資源操作失敗"

PowerShell cmdlet

步驟

1. 使用 `Open-SmConnection` cmdlet 為指定使用者啟動與 SnapCenter 伺服器的連線會話。

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

顯示使用者名稱和密碼提示。

2. 使用 `Add-SmPolicy` cmdlet 建立備份策略。

此範例建立一個 SQL 備份類型為 `FullBackup` 的新備份策略：

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy  
-PluginPolicyType SCSQL -PolicyType Backup  
-SqlBackupType FullBackup -Verbose
```

此範例建立一個新的備份策略，其 Windows 檔案系統備份類型為 `CrashConsistent`：

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy  
-PluginPolicyType SCW -PolicyType Backup  
-ScwBackupType CrashConsistent -Verbose
```

3. 使用 `Get-SmResources` cmdlet 來發現主機資源。

此範例發現指定主機上的 Microsoft SQL 外掛程式的資源：

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCSQL
```

此範例發現指定主機上的 Windows 檔案系統的資源：

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com  
-PluginCode SCW
```

4. 使用 Add-SmResourceGroup cmdlet 為SnapCenter新增新的資源組。

此範例使用指定的策略和資源建立一個新的 SQL 資料庫備份資源組：

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource  
-Resources @{"Host"="visef6.org.com";  
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}  
-Policies "BackupPolicy"
```

此範例使用指定的策略和資源建立一個新的 Windows 檔案系統備份資源群組：

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource  
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";  
"Type"="Windows Filesystem";"Names"="E:\"}  
-Policies "EngineeringBackupPolicy"
```

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy  
FinancePolicy
```

6. 使用 Get-SmBackupReport cmdlet 查看備份作業的狀態。

此範例顯示在指定日期執行的所有作業的作業摘要報表：

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

備份 SQL Server 資源組

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或選擇，然後選擇標籤。然後您可以選擇關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：
 - a. 如果您已將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 備份後，選擇*驗證*來驗證按需備份。

政策中的 驗證 選項僅適用於排程作業。

- c. 選擇*備份*。

5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

相關資訊

["為 SQL Server 資料庫建立備份策略"](#)

["為 SQL Server 建立資源組並附加策略"](#)

["由於 TCP_TIMEOUT 延遲，備份操作失敗，並出現 MySQL 連線錯誤"](#)

["備份會因 Windows 排程器錯誤而失敗"](#)

在SnapCenter作業頁面中監控 SQL 資源備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。

2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監視 **SQL** 資源上的資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消用於 **Microsoft SQL Server** 備份作業的**SnapCenter**插件

您可以取消正在執行、排隊或無回應的備份作業。當您取消備份作業時，如果已建立的備份未在SnapCenter Server 中註冊， SnapCenter Server 將停止該作業並從儲存體中刪除所有快照。如果備份已在SnapCenter Server 中註冊，則即使觸發取消，也不會回溯已建立的快照。

開始之前

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消還原作業。
- 您只能取消排隊或正在執行的日誌或完整備份作業。
- 驗證開始後，您無法取消操作。

如果在驗證前取消操作，則操作被取消，並且不會執行驗證操作。

- 您可以從「監視」頁面或「活動」窗格取消備份作業。

- 除了使用 SnapCenter GUI 之外，您還可以使用 PowerShell cmdlet 來取消操作。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，選擇「監控」>「作業」。 2. 選擇作業並選擇*取消作業*。
活動窗格	1. 啟動備份作業後，選擇在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，選擇「取消工作」。

結果

操作被取消，資源恢復到之前的狀態。如果您取消的操作在取消或運作狀態下無回應，則應執行 `Cancel-SmJob -JobID <int> -Force` cmdlet 強制停止備份作業。

在拓樸頁面中檢視 SQL Server 備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保險庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
 -  顯示使用 SnapMirror 技術在二級儲存上鏡像的備份和克隆的數量。
 -  顯示使用 SnapVault 技術在二級儲存上複製的備份和克隆的數量。
- 顯示的備份數量包括從輔助儲存中刪除的備份。

例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。
-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果選擇的資源是克隆的資料庫，則保護克隆的資料庫，克隆的來源顯示在拓撲頁面中。按一下「詳細資料」以查看用於複製的備份。

如果資源受到保護，則會顯示所選資源的拓撲頁面。

4. 查看摘要卡以了解主儲存和輔助儲存上可用的備份和複製數量的摘要。

*摘要卡*部分顯示備份和克隆的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 會自動配置為新的主目標。

- 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製、重新命名和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

7. 從表中選擇一個克隆，然後按一下「克隆拆分」。
8. 如果要刪除克隆，請從表中選擇克隆，然後按一下 。

使用 PowerShell cmdlet 清理輔助備援計數

您可以使用 Remove-SmBackup cmdlet 清理沒有快照的輔助備份的備份計數。當管理副本拓撲中顯示的快照總數與輔助儲存快照保留設定不符時，您可能需要使用此 cmdlet。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

可以透過執行 `_Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. 使用 -CleanupSecondaryBackups 參數清理輔助備援計數。

此範例清理沒有快照的輔助備份的備份計數：

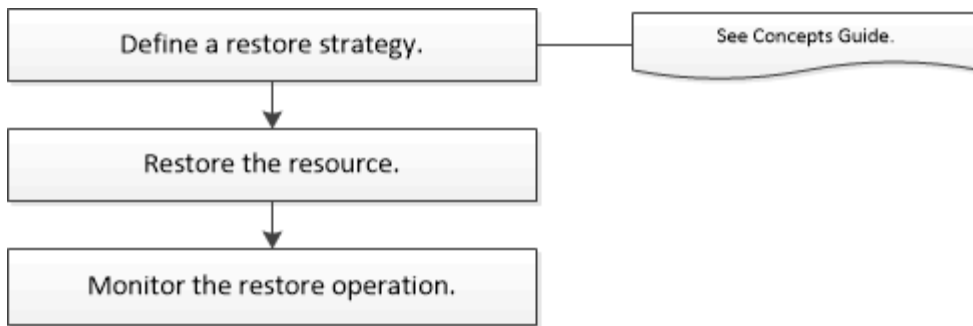
```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):
```

還原 SQL Server 資源

復原工作流程

您可以使用SnapCenter透過將一個或多個備份中的資料還原到活動檔案系統，然後還原資料庫來還原 SQL Server 資料庫。您也可以還原可用性群組中的資料庫，然後將還原的資料庫新增至可用性群組。在還原 SQL Server 資料庫之前，您必須執行幾項準備任務。

以下工作流程顯示了執行資料庫還原作業的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原、還原、驗證和複製作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 ["SnapCenter 軟體 Cmdlet 參考指南"](#)

查找更多資訊

["從輔助儲存還原 SQL Server 資料庫"](#)

["使用 PowerShell cmdlet 還原和復原資源"](#)

["在 Windows 2008 R2 上還原作業可能會失敗"](#)

恢復資料庫的要求

從 SnapCenter Plug-in for Microsoft SQL Server 備份還原 SQL Server 資料庫之前，必須確保符合幾個要求。

- 在復原資料庫之前，目標 SQL Server 執行個體必須處於線上且正在執行的狀態。

這適用於使用者資料庫還原操作和系統資料庫還原操作。

- 必須停用針對您正在還原的 SQL Server 資料執行的 SnapCenter 操作，包括在遠端管理或遠端驗證伺服器上排程的任何作業。
- 如果系統資料庫不起作用，則必須先使用 SQL Server 公用程式重建系統資料庫。
- 如果您正在安裝插件，請確保授予其他角色恢復可用性群組 (AG) 備份的權限。

當滿足以下條件之一時，恢復 AG 會失敗：

- 如果外掛程式由 RBAC 使用者安裝，且管理員嘗試還原 AG 備份
- 如果外掛程式由管理員安裝，且 RBAC 使用者嘗試還原 AG 備份
- 如果要將自訂日誌目錄備份還原到備用主機，則 SnapCenter 伺服器和插件主機必須安裝相同的 SnapCenter 版本。
- 您必須安裝 Microsoft 修補程式 KB2887595。Microsoft 支援網站包含有關 KB2887595 的更多資訊。

["Microsoft 支援文章 2887595：Windows RT 8.1、Windows 8.1 與 Windows Server 2012 R2 更新總表：2013 年 11 月"](#)

- 您必須已備份資源組或資料庫。
- 如果您要將快照複製到映像或保管庫，SnapCenter 管理員必須已為來源磁碟區和目標磁碟區指派儲存虛擬機器 (SVM)。

有關管理員如何向使用者指派資源的信息，請參閱SnapCenter安裝資訊。

- 恢復資料庫之前必須停止所有備份和克隆作業。
- 如果資料庫大小為數以 TB 為單位，則還原作業可能會逾時。

您必須透過執行下列指令將SnapCenter Server 的 RESTTimeout 參數值增加到 20000000 毫秒：Set-SmConfigSettings -Agent -configSettings @"{\"RESTTimeout\" = \"20000000\"}。根據資料庫的大小，可以變更逾時值，可以設定的最大值為 86400000 毫秒。

如果您想在資料庫上線上時進行恢復，則應在「恢復」頁面中啟用線上復原選項。

還原 SQL Server 資料庫備份

您可以使用SnapCenter來還原備份的 SQL Server 資料庫。資料庫復原是一個多階段過程，將所有資料和日誌頁從指定的 SQL Server 備份複製到指定的資料庫。

關於此任務

- 您可以將備份的 SQL Server 資料庫還原到建立備份的相同主機上的不同 SQL Server 執行個體。

您可以使用SnapCenter將備份的 SQL Server 資料庫還原到備用路徑，這樣就不會替換生產版本。

- SnapCenter可以在不使 SQL Server 叢集群組離線的情況下還原 Windows 叢集中的資料庫。
- 如果在還原作業期間發生群集故障（群集組移動操作）（例如，如果擁有資源的節點發生故障），則必須重新連線到 SQL Server 實例，然後重新啟動還原作業。
- 當使用者或 SQL Server 代理作業正在存取資料庫時，您無法還原資料庫。
- 您無法將系統資料庫還原到備用路徑。
- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 恢復精靈頁面上的大多數欄位都是不言自明的。以下資訊描述了您可能需要指導的欄位。
- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。
- 對於啟用SnapLock的策略、對於ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從清單中選擇資料庫或資源組。

進入拓樸頁面。

4. 從管理副本檢視中，從儲存系統中選擇*備份*。
5. 從表中選擇備份，然後按一下  圖示。



6. 在「還原範圍」頁面中，選擇下列選項之一：

選項	描述
將資料庫還原到建立備份的相同主機	如果您想要將資料庫還原到進行備份的相同 SQL 伺服器，請選擇此選項。
將資料庫還原到備用主機	如果您希望將資料庫還原到與備份相同的或不同的主機上的其他 SQL 伺服器，請選擇此選項。 選擇主機名，提供資料庫名稱（可選），選擇實例，並指定還原路徑。  備用路徑中提供的檔案副檔名必須與原始資料庫檔案的檔案副檔名相同。 如果「還原範圍」頁面中未顯示「將資料庫還原到備用主機」選項，請清除瀏覽器快取。
使用現有資料庫檔案還原資料庫	如果您希望將資料庫還原到與備份相同的或不同的主機上的備用 SQL Server，請選擇此選項。 資料庫檔案應該已經存在於給定的現有檔案路徑上。選擇主機名，提供資料庫名稱（可選），選擇實例，並指定還原路徑。

7. 在「恢復範圍」頁面中，選擇以下選項之一：

選項	描述
沒有任何	當您只需要還原完整備份而不還原任何日誌時，請選擇「無」。
所有日誌備份	選擇*所有日誌備份*最新備份還原作業，在完整備份後還原所有可用的日誌備份。
通過日誌備份直到	選擇「按日誌備份」執行時間點還原作業，該操作會根據備份日誌還原資料庫，直到選定日期的備份日誌。
按特定日期直至	選擇「以特定日期直到」來指定交易日誌不應用於復原資料庫的日期和時間。 此時間點還原作業將暫停在指定日期和時間之後記錄的交易日誌條目的還原。
使用自訂日誌目錄	如果您選擇了“所有日誌備份”、“按日誌備份”或“按特定日期直到”並且日誌位於自訂位置，請選擇“使用自訂日誌目錄”，然後指定日誌位置。 只有當您選擇了「將資料庫還原到備用主機」或「使用現有資料庫檔案還原資料庫」時，「使用自訂日誌目錄」選項才可用。您也可以使用共用路徑，但請確保 SQL 使用者可以存取該路徑。  可用性群組資料庫不支援自訂日誌目錄。

8. 在「Pre Ops」頁面中，執行下列步驟：

a. 在「預還原選項」頁面中，選擇下列選項之一：

- 選擇*還原時覆寫同名資料庫*以還原同名資料庫。
- 選擇*保留 SQL 資料庫複製設定*以還原資料庫並保留現有的複製設定。
- 選擇「還原前建立交易日誌備份」以在還原作業開始之前建立交易日誌。
- 如果交易日誌備份失敗，請選擇「如果還原前的交易日誌備份失敗則退出還原」以中止還原作業。

b. 指定在執行還原作業之前要執行的選用腳本。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報、傳送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

9. 在 Post Ops 頁面中，執行以下步驟：

a. 在還原完成後選擇資料庫狀態部分中，選擇下列選項之一：

- 如果您現在要還原所有必要的備份，請選擇*可操作，但無法還原其他交易日誌*。

這是預設行為，透過回滾未提交的事務使資料庫可供使用。在建立備份之前，您無法還原其他交易日誌。

- 選擇*不可操作，但可用於還原其他交易日誌*以使資料庫不可操作，而不回滾未提交的交易。

可以還原額外的交易日誌。在資料庫恢復之前您無法使用它。

- 選擇*唯讀模式，可用於還原額外的交易日誌*以使資料庫處於唯讀模式。

此選項撤銷未提交的事務，但將撤銷的操作保存在備用檔案中，以便可以恢復復原效果。

如果啟用了撤銷目錄選項，則會還原更多的交易日誌。如果交易日誌的復原操作不成功，則可以回溯變更。SQL Server 文件包含更多資訊。

b. 指定執行還原作業後執行的選用腳本。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報、傳送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

10. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

11. 查看摘要，然後按一下「完成」。

12. 使用「監控」>「作業」頁面監控復原過程。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269  
-Confirm:$false  
output:  
Name                : Restore  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'  
Id                  : 2368  
StartTime           : 10/4/2016 11:22:02 PM  
EndTime            :  
IsCancellable       : False  
IsRestartable       : False  
IsCompleted         : False  
IsVisible           : True  
IsScheduled         : False  
PercentageCompleted : 0  
Description         :  
Status              : Queued  
Owner                :  
Error                :  
Priority             : None  
Tasks               : {}  
ParentJobID         : 0  
EventId             : 0  
JobTypeId           :  
ApisJobKey          :  
ObjectId            : 0  
PluginCode          : NONE  
PluginName          :
```

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

從輔助儲存還原 **SQL Server** 資料庫

您可以從輔助儲存系統上的實體 LUN（RDM、iSCSI 或 FCP）還原備份的 SQL Server 資料庫。復原功能是一個多階段過程，它將所有資料和日誌頁從駐留在輔助儲存系統上的指定 SQL Server 備份複製到指定的資料庫。

開始之前

- 您必須已將快照從主儲存系統複製到輔助儲存系統。
- 您必須確保 SnapCenter 伺服器 and 插件主機能夠連接到輔助儲存系統。

- 恢復精靈頁面上的大多數欄位都在基本恢復過程中進行了解釋。以下資訊描述了您可能需要指導的一些欄位。

關於此任務

對於啟用SnapLock的策略、對於ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“適用於 SQL Server 的SnapCenter外掛程式”。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*或*資源組*。
3. 選擇資料庫或資源組。

進入資料庫或資源組拓撲頁面。

4. 在「管理副本」部分，從輔助儲存系統（鏡像或保險庫）中選擇「備份」。
5. 從清單中選擇備份，然後按一下 。
6. 在位置頁面中，選擇還原所選資源的目標磁碟區。
7. 完成還原精靈，查看摘要，然後按一下「完成」。

如果將資料庫還原到其他資料庫共用的不同路徑，則應執行完整備份和備份驗證，以確認還原的資料庫沒有實體級損壞。

使用 PowerShell cmdlet 還原資源

恢復資源備份包括啟動與SnapCenter伺服器的連線會話、列出備份並檢索備份資訊以及恢復備份。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：


```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

SmBackupId	: 113
SmJobId	: 2032
StartDateTime	: 2/2/2015 6:57:03 AM
EndDateTime	: 2/2/2015 6:57:11 AM
Duration	: 00:00:07.3060000
CreatedDateTime	: 2/2/2015 6:57:23 AM
Status	: Completed
ProtectionGroupName	: Clone
SmProtectionGroupId	: 34
PolicyName	: Vault
SmPolicyId	: 18
BackupName	: Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus	: NotVerified
SmBackupId	: 114
SmJobId	: 2183
StartDateTime	: 2/2/2015 1:02:41 PM
EndDateTime	: 2/2/2015 1:02:38 PM
Duration	: -00:00:03.2300000
CreatedDateTime	: 2/2/2015 1:02:53 PM
Status	: Completed
ProtectionGroupName	: Clone
SmProtectionGroupId	: 34
PolicyName	: Vault
SmPolicyId	: 18
BackupName	: Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus	: NotVerified

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

重新設定可用性群組資料庫

重新播種是復原可用性群組 (AG) 資料庫的選項。如果輔助資料庫與 AG 中的主資料庫不同步，則可以重新設定輔助資料庫的種子。

開始之前

- 您必須已經建立了要還原的輔助 AG 資料庫的備份。
- SnapCenter 伺服器 and 插件主機必須安裝相同的 SnapCenter 版本。

關於此任務

- 您無法在主資料庫上執行重新設定種子操作。
- 如果副本資料庫已從可用性群組中刪除，則您無法執行重新設定種子操作。當副本被刪除時，重新播種操作

會失敗。

- 在 SQL 可用性群組資料庫上執行重新設定種子作業時，不應在該可用性群組資料庫的副本資料庫上觸發日誌備份。如果在重新設定種子操作期間觸發日誌備份，則重新設定種子操作將失敗，並顯示「鏡像資料庫「database_name」的交易日誌資料不足以保存主體資料庫的日誌備份鏈」錯誤訊息。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“適用於 SQL Server 的 SnapCenter 外掛程式”。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。
3. 從清單中選擇輔助 AG 資料庫。
4. 按一下“重新播種”。
5. 透過點選「監視」>「作業」來監視操作進度。

監視 SQL 資源恢復操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從*狀態*下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

取消SQL資源復原操作

您可以取消排隊的還原作業。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消恢復操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的復原操作。
- 您無法取消正在執行的復原操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的還原作業。
- 對於無法取消的復原操作，「取消作業」按鈕將被停用。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊復原作業。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇作業並點選「取消作業」。
活動窗格	1. 啟動恢復操作後，按一下在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

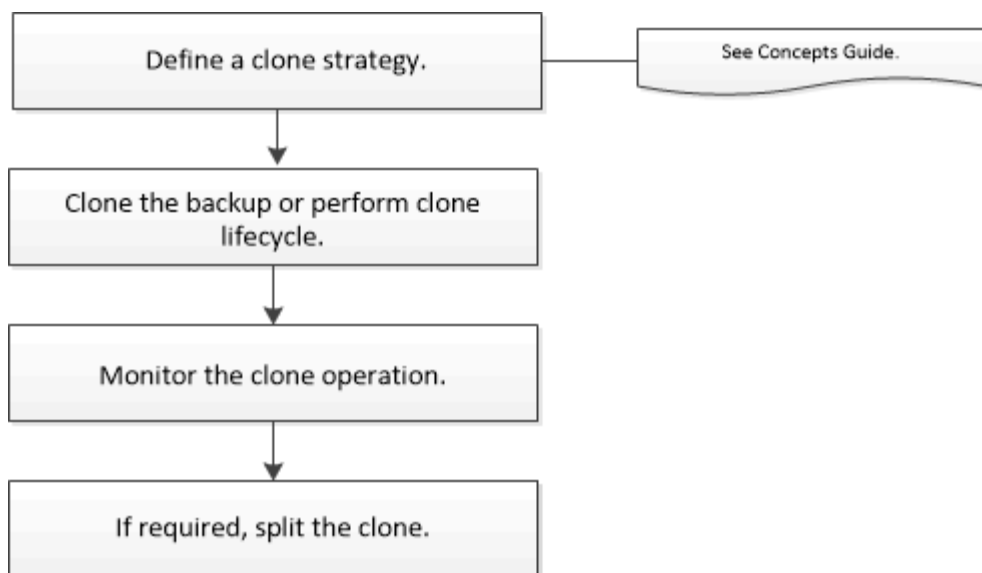
克隆 SQL Server 資料庫資源

克隆工作流程

在從備份複製資料庫資源之前，您必須使用SnapCenter Server 執行幾項任務。資料庫克隆是建立生產資料庫或其備份集的時間點副本的過程。您可以複製資料庫來測試在應用程式開發週期中必須使用目前資料庫結構和內容實現的功能，在填充資料倉儲時使用資料擷取和操作工具，或還原被錯誤刪除或變更的資料。

資料庫克隆操作根據作業 ID 產生報告。

以下工作流程顯示了執行複製操作的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原、還原、驗證和複製作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 "[SnapCenter 軟體 Cmdlet 參考指南](#)"

查找更多資訊

["從 SQL Server 資料庫備份克隆"](#)

["執行複製生命週期"](#)

["克隆操作可能失敗或需要更長時間才能完成，且使用預設 TCP_TIMEOUT 值"](#)

從 SQL Server 資料庫備份克隆

您可以使用 SnapCenter 克隆 SQL Server 資料庫備份。如果您想存取或還原舊版本的數據，您可以根據需要克隆資料庫備份。

開始之前

- 您應該已經透過完成新增主機、識別資源和建立儲存系統連線等任務為資料保護做好了準備。
- 您應該已經備份資料庫或資源組。
- 資料 LUN 和日誌 LUN 的保護類型（例如鏡像、保管庫或鏡像保管庫）應該相同，以便在使用日誌備份複製到備用主機期間發現輔助定位器。
- 如果在 SnapCenter 複製作業期間找不到已安裝的複製驅動器，則應將 SnapCenter Server 的 CloneRetryTimeout 參數變更為 300。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。

關於此任務

- 複製到獨立資料庫執行個體時，請確保掛載點路徑存在且是專用磁碟。
- 當複製到故障轉移群集實例 (FCI) 時，請確保掛載點存在、它是共用磁碟，且路徑和 FCI 應該屬於同一個 SQL 資源組。
- 確保每個主機僅連接一個 vFC 或 FC 啟動器。這是因為，SnapCenter 每個主機只支援一個啟動器。

- 如果來源資料庫或目標執行個體位於叢集共用磁碟區（csv）上，則複製的資料庫將位於 csv 上。
- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：[API /4.7/configsettings](#)

您可以使用 GET API 來顯示鍵的值。不支援 SET API。



對於虛擬環境（VMDK/RDM），請確保掛載點是專用磁碟。

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇“適用於 SQL Server 的SnapCenter外掛程式*”。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。



不支援克隆實例的備份。

3. 選擇資料庫或資源組。
4. 從*管理副本*檢視頁面中，選擇來自主或輔助（鏡像或保管）儲存系統的備份。
5. 選擇備份，然後選擇**。
6. 在「複製選項」頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	選擇要建立克隆的主機。
克隆實例	選擇要將資料庫備份複製到的克隆實例。 此 SQL 實例必須位於指定的克隆伺服器中。
克隆後綴	輸入將附加到克隆檔案名稱的後綴，以標識該資料庫是克隆的。 例如， <i>db1_clone</i> 。如果要複製到與原始資料庫相同的位置，則必須提供後綴以區分複製的資料庫和原始資料庫。否則，操作失敗。
自動分配掛載點或自動分配路徑下的磁碟區掛載點	選擇是否自動指派掛載點或路徑下的磁碟區掛載點。 自動分配路徑下的磁碟區掛載點：路徑下的掛載點可讓您提供特定的目錄。掛載點將在該目錄內建立。在選擇此選項之前，您必須確保目錄為空。如果目錄中存在資料庫，則掛載操作後資料庫將處於無效狀態。

7. 在日誌頁面中，選擇以下選項之一：

對於這個領域...	這樣做...
沒有任何	當您只想克隆完整備份而不克隆任何日誌時，請選擇此選項。
所有日誌備份	選擇此選項可以複製完整備份之後的所有可用日誌備份。

對於這個領域...	這樣做...
通過日誌備份直到	選擇此選項可根據所選日期的備份日誌建立的備份日誌複製資料庫。
按特定日期直至	指定交易日誌不再應用於複製資料庫的日期和時間。 此時間點複製會停止指定日期和時間之後記錄的交易日誌條目的複製。

8. 在*腳本*頁面中，分別輸入腳本逾時、路徑以及複製操作之前或之後應執行的預腳本或後腳本的參數。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報、傳送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

預設腳本超時為 60 秒。

9. 在*通知*頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

對於 EMS，您可以參考 ["管理 EMS 資料收集"](#)

10. 查看摘要，然後選擇*完成*。

11. 透過選擇 **Monitor > Jobs** 來監控操作進度。

完成後

創建克隆後，您永遠不應對其進行重命名。

相關資訊

["克隆操作可能失敗或需要更長時間才能完成，且使用預設 TCP_TIMEOUT 值"](#)

["故障轉移群集實例資料庫克隆失敗"](#)

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. 列出可以使用 Get-SmBackup 或 Get-SmResourceGroup cmdlet 克隆的備份。

此範例顯示有關所有可用備份的資訊：

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

此範例顯示有關指定資源組、其資源和相關策略的資訊：

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
```

Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}

```

SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. 使用 New-SmClone cmdlet 從現有備援啟動複製作業。

此範例從包含所有日誌的指定備份建立複製：

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

此範例建立指定 Microsoft SQL Server 執行個體的複製：

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. 使用 Get-SmCloneReport cmdlet 查看複製作業的狀態。

此範例顯示指定作業 ID 的複製報表：

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

執行複製生命週期

使用 SnapCenter，您可以從資源組或資料庫建立克隆。您可以執行按需克隆，也可以安排資源群組或資料庫的重複克隆操作。如果您定期複製備份，則可以使用該複製來開發應用程式、填充資料或還原資料。

SnapCenter 可讓您安排多個複製作業在多個伺服器上同時執行。

開始之前

- 複製到獨立資料庫執行個體時，請確保掛載點路徑存在且是專用磁碟。
- 當複製到故障轉移群集實例 (FCI) 時，請確保掛載點存在、它是共用磁碟，且路徑和 FCI 應該屬於同一個 SQL 資源組。
- 如果來源資料庫或目標執行個體位於叢集共用磁碟區 (csv) 上，則複製的資料庫將位於 csv 上。



對於虛擬環境 (VMDK/RDM)，請確保掛載點是專用磁碟。

關於此任務

- `SCRIPTS_PATH` 是使用插件主機的 `SMCoreServiceHost.exe.Config` 檔案中的 `PredefinedWindowsScriptsDirectory` 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 複製生命週期精靈頁面上的大多數欄位都是不言自明的。以下資訊描述了您可能需要指導的欄位。
- 對於ONTAP 9.12.1 及以下版本，如果指定 Snapshot 鎖定期限，則從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 選擇資源群組或資料庫，然後按一下「克隆生命週期」。
4. 在「選項」頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆作業名稱	指定複製生命週期作業名稱，以協助監控和修改複製生命週期作業。
克隆伺服器	選擇要放置克隆的主機。
克隆實例	選擇要將資料庫克隆到的克隆實例。此 SQL 實例必須位於指定的克隆伺服器中。
克隆後綴	輸入將附加到克隆資料庫的後綴，以標識它是一個克隆。用於建立克隆資源組的每個 SQL 實例都必須具有唯一的資料庫名稱。例如，如果克隆資源組包含來自 SQL 實例“inst1”的來源資料庫“db1”，並且如果“db1”被複製到“inst1”，則克隆資料庫名稱應該是“db1clone”。“clone”是強制的使用者定義後綴，因為資料庫被複製到同一個實例。如果將“db1”複製到 SQL 執行個體“inst2”，則複製資料庫名稱可以保留為“db1”（後綴是可選的），因為資料庫被複製到不同的執行個體。
自動分配掛載點或自動分配路徑下的磁碟區掛載點	選擇是否自動分配路徑下的掛載點或磁碟區掛載點。選擇自動分配路徑下的磁碟區掛載點可讓您提供特定的目錄。掛載點將在該目錄內建立。在選擇此選項之前，您必須確保目錄為空。如果目錄中存在資料庫，則掛載操作後資料庫將處於無效狀態。

5. 在位置頁面中，選擇用於建立複製的儲存位置。
6. 在腳本頁面中，分別輸入複製操作之前或之後應執行的前置腳本或後置腳本的路徑和參數。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報、傳送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 `SCRIPTS_PATH`。

預設腳本超時為 60 秒。

7. 在「計劃」頁面中，執行下列其中一項操作：

- 如果您想立即執行複製作業，請選擇*立即執行*。
- 當您想要確定克隆操作發生的頻率、克隆計劃的開始時間、克隆操作發生的日期、計劃的到期時間以及計劃到期後是否必須刪除克隆時，請選擇*配置計劃*。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtServer` 指定 SMTP 伺服器詳細資訊。

對於 EMS，您可以參考 ["管理 EMS 資料收集"](#)

9. 查看摘要，然後按一下「完成」。

您應該使用*Monitor* > *Jobs*頁面來監控複製過程。

監視 SQL 資料庫克隆操作

您可以使用「作業」頁面監控SnapCenter複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

- 進行中
- 成功完成
- 失敗的
- 已完成但有警告，或因警告而無法啟動
- 排隊
- 取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選 過濾列表以便僅列出克隆操作。

- b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從*狀態*下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
 5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

取消 SQL 資源克隆操作

您可以取消排隊的複製操作。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消複製操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的複製操作。
- 您無法取消正在執行的克隆操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的複製作業。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊複製操作。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇操作，然後按一下「取消作業」。
活動窗格	1. 啟動克隆操作後，按一下在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2 後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“”。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCore 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定SMCore輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為5分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter克隆或驗證失敗，聚合不存在"](#)

保護 SAP HANA 資料庫

適用於 SAP HANA 資料庫的SnapCenter插件

適用於 SAP HANA 資料庫的SnapCenter插件概述

SAP HANA 資料庫的SnapCenter插件是NetApp SnapCenter software的主機端元件，可實現 SAP HANA 資料庫的應用程式感知資料保護管理。SAP HANA 資料庫外掛程式可自動在SnapCenter環境中備份、復原和複製 SAP HANA 資料庫。

SnapCenter支援單容器和多租戶資料庫容器 (MDC)。您可以在 Windows 和 Linux 環境中使用 SAP HANA 資料庫插件。未安裝在 HANA 資料庫主機上的插件稱為集中式主機插件。集中式主機插件可以管理跨不同主機的多個 HANA 資料庫。

安裝 SAP HANA 資料庫外掛程式後，您可以使用具有NetApp SnapMirror技術的SnapCenter在另一個磁碟區上建立備份集的鏡像副本。您也可以使用具有NetApp SnapVault技術的插件來執行磁碟到磁碟的備份複製，以符合標準。

SAP HANA 資料庫外掛程式支援SnapMirror主動同步（最初是作為SnapMirror業務連續性 [SM-BC] 發布），即使整個網站發生故障，該外掛程式也能使業務服務繼續運行，支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過SnapMirror主動同步觸發故障轉移。

使用適用於 SAP HANA 資料庫的SnapCenter插件可以做什麼

在您的環境中安裝 SAP HANA 資料庫插件時，您可以使用SnapCenter備份、還原和複製 SAP HANA 資料庫及其資源。您也可以執行支援這些操作的任務。

- 新增資料庫。
- 建立備份。
- 從備份中復原。
- 克隆備份。
- 安排備份作業。
- 監控備份、復原和克隆作業。
- 查看備份、復原和克隆作業的報告。

適用於 SAP HANA 資料庫的SnapCenter插件功能

SnapCenter與插件應用程式以及儲存系統上的NetApp技術整合。若要使用 SAP HANA 資料庫插件，您需要使用SnapCenter圖形使用者介面。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份、復原和複製作業、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以及監控所有外掛程式中的作業。

- 自動化中央管理

您可以安排備份作業、設定基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷**NetApp Snapshot** 複製技術

SnapCenter使用NetApp Snapshot 技術和 SAP HANA 資料庫插件來備份資源。

使用 SAP HANA 資料庫插件還可帶來以下好處：

- 支援備份、復原和複製工作流程
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 使用NetApp FlexClone技術建立節省空間的資源時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 支援ONTAP的一致性群組 (CG) 快照功能作為建立備份的一部分。
- 能夠跨多個資源主機同時執行多個備份

在單一操作中，當單一主機中的資源共用同一磁碟區時，快照就會合併。

- 能夠使用外部命令建立快照。
- 支援基於檔案的備份。
- 支援 XFS 檔案系統上的 Linux LVM。

SnapCenter Plug-in for SAP HANA Database 支援的儲存類型

SnapCenter支援實體機器和虛擬機器 (VM) 上的多種儲存類型。在安裝適用於 SAP HANA 資料庫的SnapCenter插件之前，您必須驗證對您的儲存類型的支援。

機器	儲存類型
實體伺服器	• FC 連接的 LUN • iSCSI 連接的 LUN • NFS 連結卷

機器	儲存類型
VMware ESXi	- 透過 FC 或 iSCSI ESXi HBA 連線的 RDM LUN 主機匯流排適配器 (HBA) 掃描可能需要很長時間才能完成，因為SnapCenter會掃描主機中存在的所有主機匯流排適配器。 您可以編輯位於 <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> 的 LinuxConfig.pm 文件，將 SCSI_HOSTS_OPTIMIZED_RESCAN 參數的值設定為 1，以僅重新掃描 HBA_DRI VBA 中列出的那些參數的值。 - iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統 - NFS 資料儲存上的 VMDK - VMFS 上的 VMDK 已建立 - NFS 磁碟區直接連接到客戶系統 - NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

SAP HANA 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - 倫
 - lun 創建
 - lun 創建
 - lun 創建
 - lun 刪除
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 重新命名

- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun 映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun 修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線

- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照修改-快照鎖定到期時間
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面

- 網路介面顯示
- 虛擬伺服器

為 SAP HANA 資料庫的SnapMirror和SnapVault複製準備儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

SAP HANA 資料庫的備份策略

定義 SAP HANA 資料庫的備份策略

在建立備份作業之前定義備份策略有助於您獲得成功復原或複製資源所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

關於此任務

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

步驟

1. 確定何時應該備份資源。
2. 確定您需要多少個備份作業。
3. 決定如何命名您的備份。
4. 決定是否要建立基於 Snapshot 副本的策略來備份資料庫的應用程式一致的快照。
5. 決定是否要驗證資料庫的完整性。
6. 決定是否要使用NetApp SnapMirror技術進行複製或使用NetApp SnapVault技術進行長期保留。

7. 確定來源儲存系統和SnapMirror目標上的快照的保留期限。
8. 確定是否要在備份作業之前或之後執行任何命令，並提供前言或後記。

Linux主機上的資源自動發現

資源是 Linux 主機上由SnapCenter管理的 SAP HANA 資料庫和非資料磁碟區。安裝適用於 SAP HANA 資料庫的SnapCenter外掛程式後，該 Linux 主機上的 SAP HANA 資料庫將自動發現並顯示在資源頁面中。

以下 SAP HANA 資源支援自動發現：

- 單一容器

安裝或升級插件後，位於集中式主機插件上的單一容器資源將作為手動新增的資源繼續使用。

安裝或升級插件後，僅在直接註冊到SnapCenter的 SAP HANA Linux 主機上自動發現 SAP HANA 資料庫。

- 多租戶資料庫容器（MDC）

安裝或升級插件後，位於集中主機插件上的MDC資源將繼續作為手動新增的資源。

升級到SnapCenter 4.3 後，您必須繼續在集中式主機插件上手動新增 MDC 資源。

對於直接在SnapCenter中註冊的 SAP HANA Linux 主機，安裝或升級外掛程式將觸發主機上資源的自動發現。升級插件後，對於位於插件主機上的每個 MDC 資源，將自動發現具有不同 GUID 格式的另一個 MDC 資源並在SnapCenter中註冊。新的資源將處於鎖定狀態。

例如，在SnapCenter 4.2 中，如果 E90 MDC 資源位於插件主機上並手動註冊，則升級到SnapCenter 4.3 後，將在SnapCenter中發現並註冊另一個具有不同 GUID 的 E90 MDC 資源。

以下配置不支援自動發現：

- RDM 和 VMDK 佈局



一旦發現上述資源，則不支援對這些資源進行資料保護操作。

- HANA 多主機配置
- 同一主機上的多個實例
- 多層橫向擴展 HANA 系統複製
- 系統複製模式下的級聯複製環境

支援的備份類型

備份類型指定您要建立的備份類型。 SnapCenter支援 SAP HANA 資料庫的基於檔案的備份和基於快照副本的備份類型。

基於檔案的備份

基於檔案的備份驗證資料庫的完整性。您可以安排基於檔案的備份作業以特定的時間間隔進行。僅備份活躍租戶。您無法從SnapCenter還原和複製基於檔案的備份。

基於快照副本的備份

基於快照副本的備份利用NetApp Snapshot 技術建立 SAP HANA 資料庫所在磁碟區的線上只讀副本。

SAP HANA 資料庫的SnapCenter插件如何使用一致性群組快照

您可以使用該外掛程式為資源組建立一致性組快照。一致性群組是一個可以容納多個磁碟區的容器，以便您可以將它們作為一個實體進行管理。一致性組是多個磁碟區的同時快照，提供一組磁碟區的一致副本。

您也可以指定儲存控制器對快照進行一致分組的等待時間。可用的等待時間選項有*緊急*、中等*和*寬鬆。您也可以在一致的群組快照操作期間啟用或停用隨處寫入檔案佈局 (WAFL) 同步。WAFL同步提高了一致性組快照的效能。

SnapCenter如何管理日誌和資料備份

SnapCenter管理儲存系統和檔案系統層級以及 SAP HANA 備份目錄中的日誌和資料備份。

根據保留設定刪除主儲存或輔助儲存上的快照及其在 SAP HANA 目錄中的對應項目。在備份和資源群組刪除期間，SAP HANA 目錄條目也會被刪除。

確定 SAP HANA 資料庫備份計畫的注意事項

確定備份計畫的最關鍵因素是資源的變化率。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

備份計畫分為兩部分，如下所示：

- 備份頻率（執行備份的頻率）

備份頻率（對於某些外掛程式也稱為計畫類型）是策略配置的一部分。例如，您可以將備份頻率設定為每小時、每天、每週或每月。

- 備份計畫（確切的備份執行時間）

備份計畫是資源或資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份

SAP HANA 資料庫所需的備份作業數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

SAP HANA 資料庫插件的備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

resourcegroupname_hostname_timestamp

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，customtext_resourcegroup_policy_hostname 或 resourcegroup_hostname。預設情況下，時間戳後綴會加入到快照名稱中。

SAP HANA 資料庫的還原與復原策略

定義 **SAP HANA** 資源的還原與復原策略

您必須在還原和復原資料庫之前定義一個策略，以便能夠成功執行還原和復原作業。

步驟

1. 確定手動新增的 SAP HANA 資源支援的還原策略
2. 確定自動發現的 SAP HANA 資料庫支援的還原策略
3. 確定要執行的復原操作的類型。

手動新增的 **SAP HANA** 資源支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。手動新增的 SAP HANA 資源的復原策略有兩種。您無法復原手動新增的 SAP HANA 資源。



您無法復原手動新增的 SAP HANA 資源。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

檔案級恢復

- 從磁碟區、qtree 或目錄還原文件
- 僅恢復選定的 LUN

自動發現的 **SAP HANA** 資料庫支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。自動發現的 SAP HANA 資料庫有兩種類型的復原策略。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN
 - 應選擇“**Volume Revert**”選項來恢復整個磁碟區。



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

租戶資料庫

- 恢復租戶資料庫

如果選擇了「租用戶資料庫」選項，則必須使用 SnapCenter 外部的 HANA 工作室或 HANA 復原腳本來執行復原作業。

自動發現的 **SAP HANA** 資料庫的還原操作類型

SnapCenter 支援基於磁碟區的 SnapRestore (VBSR)、單一檔案 SnapRestore 以及自動發現的 SAP HANA 資料庫的連線和複製還原類型。

基於磁碟區的 **SnapRestore (VBSR)** 在 **NFS** 環境中針對以下場景執行：

- 當選擇要還原的備份是在 SnapCenter 4.3 之前的版本上執行時，並且僅當選擇了「完整資源」選項時
- 當在 SnapCenter 4.3 中建立選擇用於還原的備份時，如果選擇了「磁碟區還原」選項

單檔 **SnapRestore** 在 **NFS** 環境中針對以下場景執行：

- 當在 SnapCenter 4.3 中建立選擇用於還原的備份時，如果僅選擇了「完整資源」選項
- 對於多租用戶資料庫容器 (MDC)，當選擇在 SnapCenter 4.3 上進行還原的備份，並且選擇了「租用戶資料庫」選項時
- 當選擇的備份來自 SnapMirror 或 SnapVault 二級位置，並且選擇了「完整資源」選項時

單一檔案SnapRestore在 SAN 環境中針對下列場景執行：

- 在SnapCenter 4.3 之前的版本上進行備份時，僅當選擇了「完整資源」選項時
- 在SnapCenter 4.3 中進行備份時，僅當選擇了「完整資源」選項時
- 從SnapMirror或SnapVault二級位置選擇備份，並選擇「完整資源」選項時

在 SAN 環境中針對下列情境執行基於連線和複製的還原：

- 對於 MDC，當在SnapCenter 4.3 中執行選擇用於還原的備份時，並選擇「租用戶資料庫」選項



復原範圍頁面上提供了*完整資源*、*磁碟區復原*和*租戶資料庫*選項。

SAP HANA 資料庫支援的復原操作類型

SnapCenter可讓您對 SAP HANA 資料庫執行不同類型的復原操作。

- 將資料庫還原到最新狀態
- 將資料庫還原到特定時間點

您必須指定恢復的日期和時間。

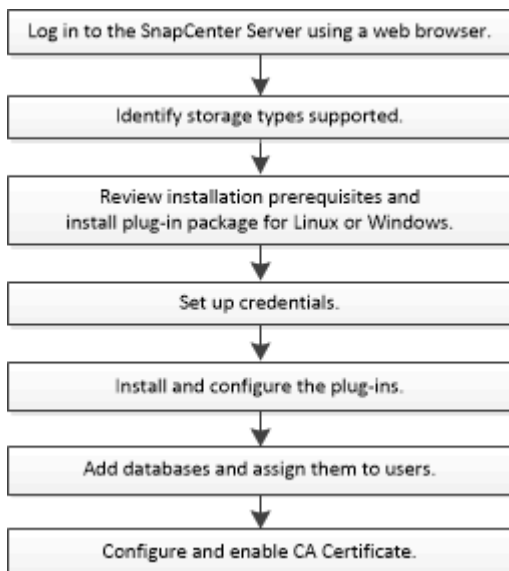
- 將資料庫還原到特定的資料備份

SnapCenter也為 SAP HANA 資料庫提供了無復原選項。

準備安裝適用於 SAP HANA 資料庫的SnapCenter插件

SAP HANA 資料庫的SnapCenter插件安裝工作流程

如果您想要保護 SAP HANA 資料庫，則應該安裝並設定適用於 SAP HANA 資料庫的SnapCenter插件。



新增主機和安裝適用於 **SAP HANA** 資料庫的**SnapCenter**插件的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。適用於 SAP HANA 資料庫的SnapCenter插件可在 Windows 和 Linux 環境中使用。

- 您必須在主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 主機上必須安裝有SAP HANA資料庫互動終端機（HDBSQL客戶端）。
- 對於 Windows，插件建立者服務應該使用「LocalSystem」Windows 使用者執行，這是以網域管理員身分安裝 SAP HANA 資料庫插件時的預設行為。
- 對於 Windows，應以 SYSTEM 使用者身分建立使用者儲存金鑰。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。適用於 Microsoft Windows 的SnapCenter插件將預設與 Windows 主機上的 SAP HANA 插件一起部署。
- 對於 Linux 主機，HDB 安全性使用者儲存金鑰以 HDBSQL OS 使用者身分存取。
- SnapCenter伺服器應該可以存取 SAP HANA 資料庫主機插件的 8145 或自訂連接埠。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 在 Windows 主機上安裝適用於 SAP HANA 資料庫的插件時，適用於 Microsoft Windows 的SnapCenter外掛程式會自動安裝。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Windows 主機上安裝 Java 11。

["下載適用於所有作業系統的 JAVA"](#)

["NetApp互通性表工具"](#)

Linux 主機

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Linux 主機上安裝 Java 11。

["下載適用於所有作業系統的 JAVA"](#)

["NetApp互通性表工具"](#)

- 對於在 Linux 主機上執行的 SAP HANA 資料庫，在安裝 SAP HANA 資料庫插件時，會自動安裝適用於 UNIX 的SnapCenter插件。
- 您應該將 **bash** 作為插件安裝的預設 shell。

補充命令

若要在 SAP HANA 的 SnapCenter 插件上執行補充命令，必須將其包含在 `allowed_commands.config` 檔案中。

- Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 主機上的預設位置：`/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`

若要允許插件主機上的補充命令，請在編輯器中開啟 `_allowed_commands.config` 檔案。每個命令在單獨的行上輸入，並且命令不區分大小寫。確保指定完全限定的路徑名，並且如果路徑名包含空格，則將其括在引號 (") 中。

例如：

命令：`mount`

命令：`umount`

指令：`"C:\Program Files\ NetApp\ SnapCreator 指令\ sdcli.exe"`

指令：`myscript.bat`

如果不存在 `allowed_commands.config` 文件，命令或腳本執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行`[/mnt/mount -a]`。透過在插件主機上的檔案 `%s` 中新增命令來授權。」

如果命令或腳本不在 `_allowed_commands.config` 中，則命令或腳本的執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行`[/mnt/mount -a]`。透過在插件主機上的檔案 `%s` 中新增命令來授權。」



您不應使用通配符 (*) 來允許所有命令。

為 Linux 主機的非 root 使用者配置 sudo 權限

SnapCenter 2.0 及更高版本允許非 root 用戶安裝適用於 Linux 的 SnapCenter 插件套件並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 `umask` 為 0027，請確保 `java` 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `_etc/ssh/ssh_config` 文件，設定訊息認證碼演算法：MACs `hmac-sha2-256`、MACs `hmac-sha2-512`。

更新設定檔後重新啟動 `sshd` 服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載
- /custom_location/ NetApp/snapcenter/spl/bin/spl

步驟

1. 登入要安裝適用於 Linux 的 SnapCenter 插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 /etc/sudoers 檔案。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`LINUX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 Windows 的 SnapCenter 插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

安裝適用於 Linux 的SnapCenter插件包的主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間和大小需求。

物品	要求
作業系統	• 紅帽企業 Linux • SUSE Linux 企業伺服器 (SLES) 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

物品	要求
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間有所不同，取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 與 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

為 SAP HANA 資料庫的SnapCenter插件設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

關於此任務

- Linux 主機

您必須設定在 Linux 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

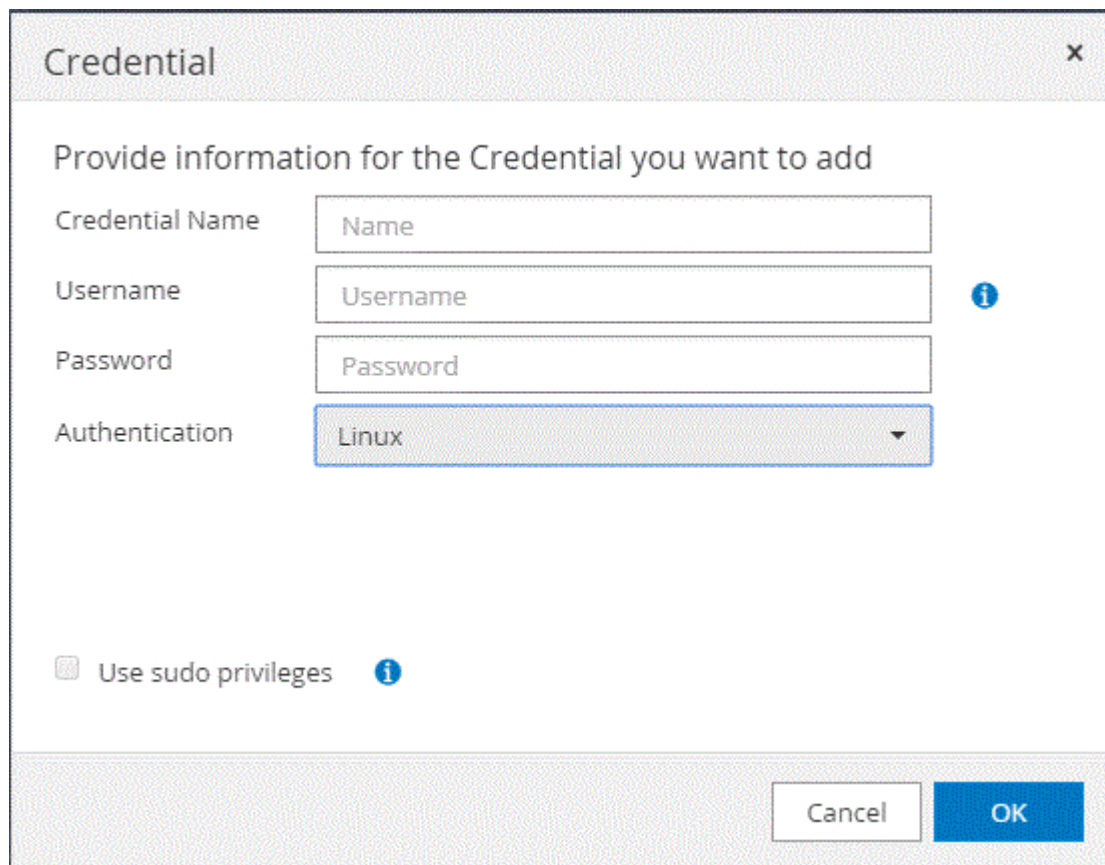
在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。



The image shows a 'Credential' dialog box with a title bar containing a close button (X). The main content area is titled 'Provide information for the Credential you want to add'. It contains four input fields: 'Credential Name' with a placeholder 'Name', 'Username' with a placeholder 'Username', 'Password' with a placeholder 'Password', and 'Authentication' with a dropdown menu showing 'Linux'. To the right of the 'Username' field is a blue information icon (i). Below the input fields is a checkbox labeled 'Use sudo privileges' with a blue information icon (i) to its right. At the bottom right of the dialog are two buttons: 'Cancel' and 'OK'.

4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。

對於這個領域...	這樣做...
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 - 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 - 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i> 請勿在密碼中使用雙引號（"）或反引號（`）。密碼中不應同時使用小於號（<）和驚嘆號（!）符號。例如，lessthan<!10、lessthan10<!、backtick`12。
密碼	輸入用於身份驗證的密碼。
認證模式	選擇您想要使用的身份驗證模式。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。
- 為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
- b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA：Install-AdServiceAccount

<gMSA>

c. 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`

5. 將管理權限指派給主機上配置的 gMSA。
6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

為 SAP HANA 資料庫安裝 SnapCenter 插件

新增主機並在遠端主機上安裝插件包

您必須使用 SnapCenter 新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以為單一主機或叢集新增主機並安裝插件包。

開始之前

- 如果 SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 您應該確保訊息佇列服務正在運行。
- 管理文件包含有關管理主機的資訊。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

["在 Windows Server 2016 或更高版本上為 SAP HANA 配置群組託管服務帳戶"](#)

關於此任務

- 您不能將 SnapCenter 伺服器作為插件主機新增至另一個 SnapCenter 伺服器。
- 為了讓 SAP HANA 系統複製發現主系統和輔助系統上的資源，建議使用 root 或 sudo 使用者新增主系統和輔助系統。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下「新增」。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux  SAP HANA插件安裝在HDBSQL客戶端主機上，該主機可以是Windows系統，也可以是Linux系統。
主機名稱	輸入通訊主機名稱。輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 您必須在此主機上設定 HDBSQL 用戶端和 HDBUserStore。
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標放在您提供的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。

對於這個領域...	這樣做...
安裝路徑	SAP HANA插件安裝在HDBSQL客戶端主機上，該主機可以是Windows系統，也可以是Linux系統。 - 對於適用於 Windows 的SnapCenter插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您也可以選擇自訂路徑。 - 對於適用於 Linux 的SnapCenter插件包，預設路徑為 /opt/ NetApp/snapcenter。您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	對於 Windows 主機，如果您要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。  以以下格式提供 gMSA 名稱： ：domainName\accountName\$。  gMSA 將僅用作 Windows 服務的SnapCenter插件的登入服務帳戶。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）和 Java 版本（適用於 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 檔案以修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 如果主機類型為Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

特定於安裝的日誌檔案位於 /custom_location/snapcenter/logs。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux** 或 **Windows** 的**SnapCenter**插件包

您可以使用 **Install-SmHostPackage PowerShell cmdlet** 同時在多個主機上安裝適用於 **Linux** 或 **Windows** 的**SnapCenter**插件套件。

開始之前

您必須以網域使用者身分登入**SnapCenter**，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 **PowerShell**。
2. 在**SnapCenter Server** 主機上，使用 **Open-SmConnection cmdlet** 建立會話，然後輸入您的憑證。
3. 使用 **Install-SmHostPackage cmdlet** 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 **cmdlet** 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 **-skipprecheck** 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝適用於 **SAP HANA** 資料庫的**SnapCenter**插件

您應該使用**SnapCenter**使用者介面 (UI) 安裝適用於 **SAP HANA** 資料庫的**SnapCenter**插件。如果您的環境不允許從**SnapCenter** UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控制台模式或靜默模式安裝 **SAP HANA** 資料庫插件。

開始之前

- 您應該在 **HDBSQL** 用戶端所在的每個 **Linux** 主機上安裝 **SAP HANA** 資料庫插件。
- 要安裝適用於 **SAP HANA** 資料庫的**SnapCenter**插件的 **Linux** 主機必須符合相關軟體、資料庫和作業系統的要求。

互通性矩陣工具 (IMT) 包含受支援配置的最新資訊。

<https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT>

- **SAP HANA** 資料庫的**SnapCenter**插件是 **Linux** 的**SnapCenter**插件包的一部分。在安裝適用於 **Linux** 的**SnapCenter**插件包之前，您應該已經在 **Windows** 主機上安裝了**SnapCenter**。

步驟

1. 將 **Linux** 安裝檔案 (**snapcenter_linux_host_plugin.bin**) 的**SnapCenter**插件包從 **C:\ProgramData\NetApp\SnapCenter\Package Repository** 複製到要安裝 **SAP HANA** 資料庫插件的主機。

您可以從安裝了**SnapCenter**伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。
3. 安裝插件：
`path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i
silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address
-DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT 指定 SMCORE HTTPS 通訊連接埠。
- -DSERVER_IP 指定 SnapCenter 伺服器 IP 位址。
- -DSERVER_HTTPS_PORT 指定 SnapCenter 伺服器 HTTPS 連接埠。
- -DUSER_INSTALL_DIR 指定要安裝 Linux 版 SnapCenter 插件包的目錄。
- DINSTALL_LOG_NAME 指定日誌檔案的名稱。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. 編輯 /<安裝目錄> NetApp 文件，然後新增 PLUGINS_ENABLED = hana:3.0 參數。
5. 使用 Add-Smhost cmdlet 和所需參數將主機新增至 SnapCenter 伺服器。

可以透過執行 `_Get-Help command_name_` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 SAP HANA 插件安裝狀態

您可以使用「作業」頁面監控 SnapCenter 插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。

- e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。

在此精靈視窗中...	執行以下操作...
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。


```
Get-Childitem -Path 憑證:\LocalMachine\My
```
 - b. 複製指紋。

使用 **Windows** 主機插件服務設定 **CA** 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

．透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

為 Linux 主機上的**SnapCenter SAP HANA** 插件服務設定 **CA** 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

插件使用位於 `/opt/NetApp/snapcenter/scc/etc` 的檔案「keystore.jks」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與密鑰“KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks  
．將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

對 `agent.properties` 檔案中的金鑰 `KEYSTORE_PASS` 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/ NetApp/snapcenter/scc/etc`。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。
```



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導航至包含插件金鑰庫 `/opt/ NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 `agent.properties` 檔案中密鑰 `KEYSTORE_PASS` 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

． 如果CA憑證中的別名較長，且包含空格或特殊字元（"*"，"，"，"），請將別名修改為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

． 在 `agent.properties` 檔案中配置來自 CA 憑證的別名。

根據鍵 `SCC_CERTIFICATE_ALIAS` 更新此值。

8. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於此任務

- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter插件的 CRL 檔案的預設目錄是「`opt/NetApp/snapcenter/scc/etc/crl`」。

步驟

1. 您可以根據鍵 `CRL_PATH` 修改和更新 `agent.properties` 檔案中的預設目錄。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

為 **Windows** 主機上的**SnapCenter SAP HANA** 插件服務設定 **CA** 證書

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

外掛程式使用位於 `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc` 的檔案 `keystore.jks` 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與金鑰 `_KEYSTORE_PASS` 對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore 金鑰庫.jks
```



如果 Windows 命令提示字元無法辨識「keytool」命令，請將 keytool 命令替換為其完整路徑。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe"-storepasswd -keystore keystore.jks
```

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks
```

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案 *_keystore.jks_*。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增加的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在_agent.properties_檔案中配置來自CA憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenterSnapCenter的 CRL 檔案的預設目錄是 'C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl'。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 agent.properties 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行_Set-SmCertificateSettings_ cmdlet 來啟用或停用 CA 憑證。
- 您可以使用_Get-SmCertificateSettings_顯示插件的憑證狀態。

可以透過執行_Get-Help command_name_來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。

2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 `/opt/netapp/config/crl`。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

做好資料保護準備

使用適用於 SAP HANA 資料庫的SnapCenter插件的先決條件

在使用適用於 SAP HANA 資料庫的SnapCenter外掛程式之前，SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。
- 登入SnapCenter伺服器。
- 透過新增儲存系統連接和建立憑證（如果適用）來配置SnapCenter環境。

- 在您的 Linux 或 Windows 主機上安裝 Java 11。

您必須在主機的環境路徑變數中設定 Java 路徑。

- 如果您想要備份複製，請設定SnapMirror和SnapVault。
- 在將安裝 SAP HANA 資料庫插件的主機上安裝 HDBSQL 用戶端。

為您將透過此主機管理的 SAP HANA 節點設定使用者儲存金鑰。

- 對於 SAP HANA 資料庫 2.0SPS05，如果您使用 SAP HANA 資料庫使用者帳戶，請確保您具有下列權限以在SnapCenter Server 中執行備份、還原和複製作業：
 - 備份管理員
 - 目錄閱讀
 - 資料庫備份管理員
 - 資料庫復原操作員

如何使用資源、資源群組和原則來保護 **SAP HANA** 資料庫

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的 SAP HANA 資料庫。
- SnapCenter資源組是主機上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

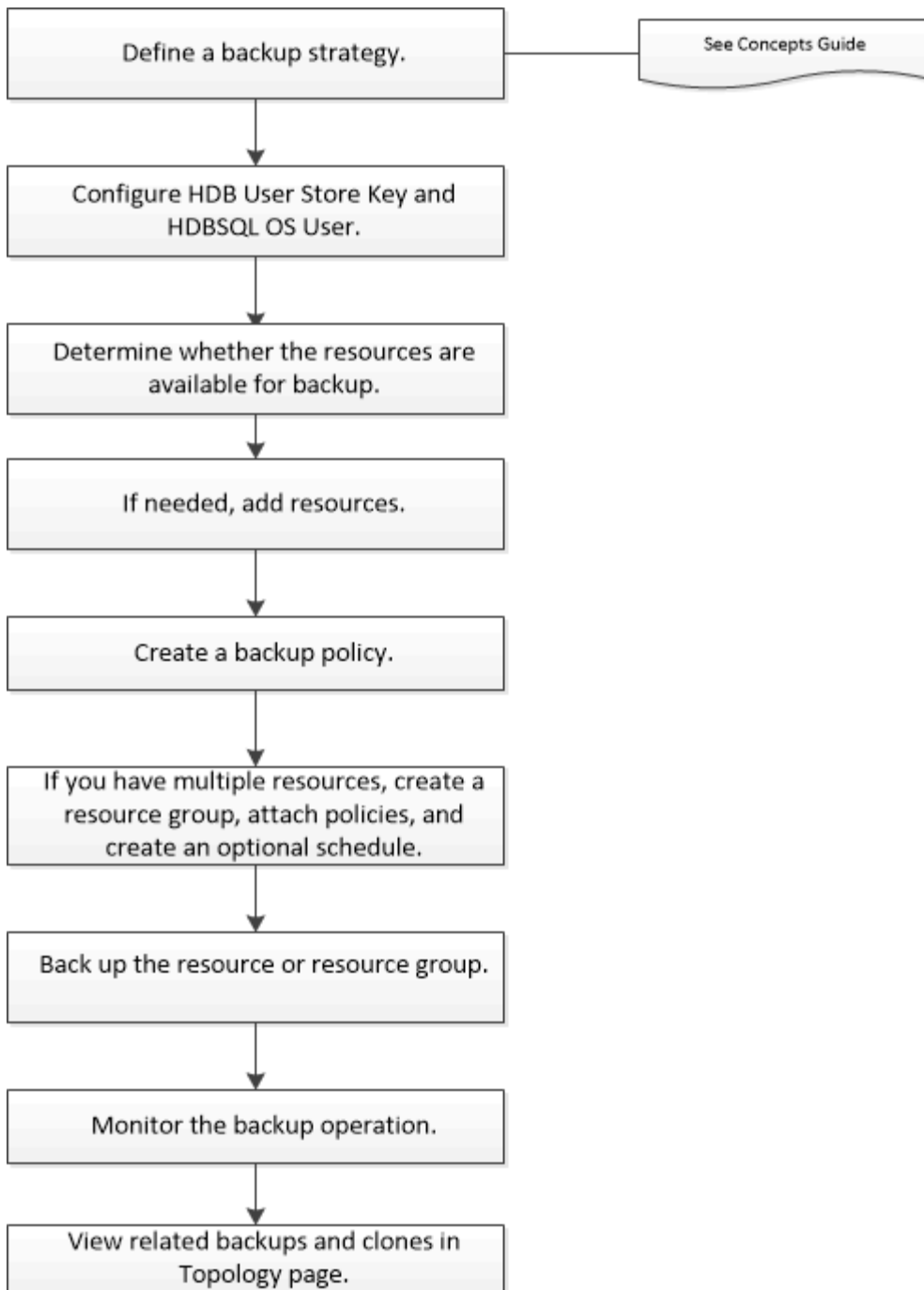
資源群組可以視為定義您想要保護的內容以及何時以日期和時間進行保護。把政策看作是定義你想如何保護它。例如，如果要備份所有資料庫，則可以建立一個包含主機中所有資料庫的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加原則時，您可以配置資源組以每天執行完整備份。

備份 **SAP HANA** 資源

備份 **SAP HANA** 資源

您可以建立資源（資料庫）或資源組的備份。備份工作流程包括規劃、識別要備份的資料庫、管理備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含更多有關 PowerShell cmdlet 的資訊。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenter軟體 Cmdlet 參考指南"]。

為 SAP HANA 資料庫設定 HDB 用戶儲存金鑰和 HDBSQL OS 用戶

您必須設定 HDB User Store Key 和 HDBSQL OS User 才能對 SAP HANA 資料庫執行資料保護作業。

開始之前

- 如果 SAP HANA 資料庫未配置 HDB 安全用戶儲存金鑰和 HDB SQL OS 用戶，則只有自動發現的資源才會出現紅色掛鎖圖示。如果在後續的發現操作中發現配置的 HDB 安全使用者儲存金鑰不正確或未提供對資料

庫本身的存取權限，則紅色掛鎖圖示將重新出現。

- 您必須設定 HDB 安全使用者儲存金鑰和 HDB SQL OS 使用者才能保護資料庫或將其新增至資源群組以執行資料保護操作。
- 您必須設定 HDB SQL OS 使用者才能存取系統資料庫。如果 HDB SQL OS 使用者配置為僅存取租用戶資料庫，則發現操作將會失敗。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“適用於 SAP HANA 資料庫的SnapCenter外掛程式”。
2. 在資源頁面中，從*檢視*清單中選擇資源類型。
3. （可選）點擊並選擇主機名稱。

然後您可以點擊關閉篩選器窗格。

4. 選擇資料庫，然後按一下*配置資料庫*。
5. 在設定資料庫設定部分，輸入 HDB 安全使用者儲存金鑰。



顯示插件主機名，並且 HDB SQL OS 用戶自動填入 <sid>adm。

6. 按一下“確定”。

您可以從拓樸頁面修改資料庫配置。

發現資源並準備多租戶資料庫容器以進行資料保護

自動發現資料庫

資源是 Linux 主機上由SnapCenter管理的 SAP HANA 資料庫和非資料磁碟區。發現可用的 SAP HANA 資料庫後，您可以將這些資源新增至資源組以執行資料保護操作。

開始之前

- 您必須已經完成安裝SnapCenter伺服器、新增 HDB 使用者儲存金鑰、新增主機和設定儲存系統連線等任務。
- 您必須已在 Linux 主機上設定 HDB 安全使用者儲存金鑰和 HDB SQL OS 使用者。
 - 您必須使用 SID adm user 設定 HDB 使用者儲存金鑰。例如，對於SID為A22的HANA系統，HDB User Store Key必須配置為a22adm。
- SAP HANA 資料庫的SnapCenter插件不支援自動發現駐留在 RDM/VMDK 虛擬環境中的資源。手動新增資料庫時必須提供虛擬環境的儲存資訊。

關於此任務

安裝外掛程式後，該Linux主機上的所有資源都會自動發現並顯示在資源頁面上。

自動發現的資源不能被修改或刪除。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“SAP HANA 資料庫外掛程式”。

2. 在資源頁面中，從視圖清單中選擇資源類型。

3. (可選) 點擊**，然後選擇主機名稱。

然後您可以點擊** 關閉篩選窗格。

4. 按一下「刷新資源」以發現主機上可用的資源。

資源與資源類型、主機名稱、關聯資源群組、備份類型、政策和總體狀態等資訊一起顯示。

- 如果資料庫位於NetApp儲存空間且未受保護，則「整體狀態」欄位中顯示「未受保護」。
- 如果資料庫位於NetApp儲存系統上並受到保護，且沒有執行備份操作，則「整體狀態」欄位中會顯示「備份未執行」。否則，狀態將根據上次備份狀態變更為備份失敗或備份成功。



如果 SAP HANA 資料庫未配置 HDB 安全使用者儲存金鑰，則資源旁邊會出現紅色掛鎖圖示。如果在後續的發現操作中發現配置的 HDB 安全使用者儲存金鑰不正確或未提供對資料庫本身的存取權限，則紅色掛鎖圖示將重新出現。



如果資料庫在SnapCenter之外重新命名，則必須刷新資源。

完成後

您必須設定 HDB 安全使用者儲存金鑰和 HDBSQL OS 使用者才能保護資料庫或將其新增至資源群組以執行資料保護作業。

"為 SAP HANA 資料庫設定 HDB 用戶儲存金鑰和 HDBSQL OS 用戶"

準備多租戶資料庫容器以進行資料保護

直接在SnapCenter中註冊的 SAP HANA 主機，安裝或升級 SAP HANA 資料庫的SnapCenter插件將觸發主機上資源的自動發現。安裝或升級插件後，對於位於插件主機上的每個多租戶資料庫容器 (MDC) 資源，將自動發現具有不同 GUID 格式的另一個 MDC 資源並在SnapCenter中註冊。新資源將處於「鎖定」狀態。

關於此任務

例如，在SnapCenter 4.2 中，如果 E90 MDC 資源位於插件主機上並手動註冊，則升級到SnapCenter 4.3 後，將在SnapCenter中發現並註冊另一個具有不同 GUID 的 E90 MDC 資源。



與SnapCenter 4.2 及更早版本的資源相關的備份必須保留，直到保留期到期。保留期到期後，您可以刪除舊的 MDC 資源並繼續管理新的自動發現的 MDC 資源。

`Old MDC resource`是SnapCenter 4.2 或更早版本中手動新增的插件主機的 MDC 資源。

執行下列步驟開始使用SnapCenter 4.3 中發現的新資源進行資料保護作業：

步驟

1. 在「資源」頁面中，選擇已將備份新增至早期SnapCenter版本的舊 MDC 資源，然後從「拓撲」頁面將其置於「維護模式」。

如果資源是資源組的一部分，則將資源組置於「維護模式」。

2. 透過從「資源」頁面中選擇新資源來配置升級到SnapCenter 4.3 後發現的新 MDC 資源。

「新 MDC 資源」是SnapCenter伺服器 and 插件主機升級到 4.3 後發現的新 MDC 資源。對於給定主機，新的 MDC 資源可以被識別為與舊 MDC 資源具有相同 SID 的資源，並且在資源頁面中旁邊帶有紅色掛鎖圖示。

3. 透過選擇保護策略、計劃和通知設定來保護升級到SnapCenter 4.3 後發現的新 MDC 資源。
4. 根據保留設定刪除在SnapCenter 4.2 或更早版本中建立的備份。
5. 從拓樸頁面中刪除資源組。
6. 從資源頁面中刪除舊的 MDC 資源。

例如，如果主快照保留期為 7 天，次要快照保留期為 45 天，則 45 天結束後，刪除所有備份後，必須刪除資源組和舊的 MDC 資源。

相關資訊

["為 SAP HANA 資料庫設定 HDB 用戶儲存金鑰和 HDBSQL OS 用戶"](#)

["在拓樸頁面中查看 SAP HANA 資料庫備份和克隆"](#)

手動將資源新增至插件主機

某些 HANA 實例不支援自動發現。您必須手動新增這些資源。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機、設定儲存系統連線以及新增 HDB 使用者儲存金鑰等任務。
- 對於 SAP HANA 系統複製，建議將該 HANA 系統的所有資源新增至一個資源組中，並進行資源組備份。這可確保接管故障復原模式期間的無縫備份。

["建立資源組並附加策略"](#)。

關於此任務

以下配置不支援自動發現：

- RDM 和 VMDK 佈局



一旦發現上述資源，則不支援對這些資源進行資料保護操作。

- HANA 多主機配置
- 同一主機上的多個實例
- 多層橫向擴展 HANA 系統複製
- 系統複製模式下的級聯複製環境

步驟

1. 在左側導覽窗格中，從下拉清單中選擇適用於 SAP HANA 資料庫的SnapCenter插件，然後按一下「資源」。
2. 在資源頁面中，按一下*新增 SAP HANA 資料庫*。

3. 在提供資源詳細資訊頁面中，執行以下操作：

對於這個領域...	這樣做...
資源類型	輸入資源類型。資源類型包括單容器、多租戶資料庫容器 (MDC) 和非資料磁碟區。
HANA 系統名稱	輸入描述性的 SAP HANA 系統名稱。僅當您選擇了單容器或 MDC 資源類型時，此選項才可用。
SID	輸入系統 ID (SID)。已安裝的 SAP HANA 系統由單一 SID 識別。
插件主機	選擇插件主機。
HDB 安全用戶儲存金鑰	輸入密鑰以連接到 SAP HANA 系統。 此密鑰包含連接資料庫的登入資訊。 對於 SAP HANA 系統複製，未驗證輔助使用者金鑰。這將在接管期間使用。
HDBSQL 作業系統用戶	輸入配置了 HDB 安全用戶儲存金鑰的使用者名稱。對於 Windows，HDBSQL OS 使用者必須是 SYSTEM 使用者。因此，您必須為 SYSTEM 使用者配置 HDB 安全性使用者儲存金鑰。

4. 在「提供儲存佔用空間」頁面中，選擇儲存系統並選擇一個或多個磁碟區、LUN 和 qtree，然後按一下「儲存」。

可選：您可以點擊 *  * 圖示用於從其他儲存系統新增更多磁碟區、LUN 和 qtree。

5. 查看摘要，然後按一下「完成」。

資料庫與 SID、插件主機、相關資源群組和策略以及總體狀態等資訊一起顯示

如果您想讓使用者存取資源，您必須將資源指派給使用者。這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

"新增使用者或群組並分配角色和資產"

新增資料庫後，您可以修改 SAP HANA 資料庫詳細資訊。

如果存在與 SAP HANA 資源關聯的備份，則您無法修改以下內容：

- 多租用戶資料庫容器 (MDC)：SID 或 HDBSQL 用戶端（外掛程式）主機
- 單容器：SID 或 HDBSQL 用戶端（外掛程式）主機
- 非資料磁碟區：資源名稱、關聯 SID 或插件主機

為 SAP HANA 資料庫建立備份策略

在使用SnapCenter備份 SAP HANA 資料庫資源之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。

開始之前

- 您必須已經定義了您的備份策略。

有關詳細信息，請參閱有關定義 SAP HANA 資料庫的資料保護策略的資訊。

- 您必須已完成安裝SnapCenter、新增主機、設定儲存系統連線和新增資源等任務，為資料保護做好準備。
- 如果您要將快照複製到映像或保管庫，SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。

此外，您還可以在策略中指定複製、腳本和應用程式設定。當您想要將該策略重新用於另一個資源群組時，這些選項可以節省時間。

- 查看SnapMirror主動同步特定的先決條件和限制。更多資訊請參閱 ["SnapMirror主動同步的物件限制"](#)。

關於此任務

- SAP HANA 系統複製
 - 您可以保護主 SAP HANA 系統，並且可以執行所有資料保護操作。
 - 您可以保護輔助 SAP HANA 系統，但無法建立備份。

故障轉移後，當輔助 SAP HANA 系統成為主 SAP HANA 系統時，可以執行所有資料保護操作。

您無法為 SAP HANA 資料卷建立備份，但SnapCenter會繼續保護非資料磁碟區 (NDV)。

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
 - 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。
 - 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選「新建」。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「策略類型」頁面中，執行下列步驟：
 - 選擇儲存類型
 - 選擇備份類型：

如果你想...	這樣做...
使用快照技術建立備份	選擇*基於快照*。
執行資料庫完整性檢查	選擇*基於檔案的備份*。僅備份活躍租戶。

6. 在「快照和複製」頁面中，執行下列步驟：

- 透過選擇*按需*、每小時、每日、*每週*或*每月*來指定方案類型。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，還使您能夠為每個策略分配不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

7. 在「快照和複製」頁面中，指定備份類型和在「備份類型」頁面中選擇的計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則先刪除最舊的快照。  最大保留值為 1018。如果保留設定的值高於ONTAP版本支援的值，則備份將會失敗。  對於基於 Snapshot 副本的備份，如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。  對於 SAP HANA 系統複製，建議將 SAP HANA 系統的所有資源新增至一個資源組。這可確保保留正確數量的備份。  對於 SAP HANA 系統複製，拍攝的快照總數將等於資源組的保留設定。最舊 Snapshot 的刪除取決於最舊 Snapshot 位於哪個節點。例如，對於具有 SAP HANA 系統複製主伺服器 and SAP HANA 系統複製輔助伺服器的資源群組，保留設定為 7。您一次最多可以拍攝 7 張快照，包含 SAP HANA 系統複製主快照和 SAP HANA 系統複製輔助快照。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*，並指定天、月或年。 SnapLock保留期應少於 100 年。

8. 選擇快照標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

9. 對於基於 Snapshot 副本的備份，在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
*建立本機 Snapshot 副本後更新SnapMirror *	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 應為SnapMirror主動同步啟用此選項。 如果ONTAP中的保護關係屬於鏡像和保險庫類型，並且您僅選擇此選項，則在主伺服器上建立的快照將不會傳輸到目標伺服器，但會在目標伺服器中列出。如果從目標中選擇此快照來執行復原操作，則會顯示所選保管/鏡像備份的輔助位置不可用的錯誤訊息。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓撲頁面中查看 SAP HANA 資料庫備份和克隆"。
*建立本機 Snapshot 副本後更新SnapVault *	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。 有關SnapLock Vault 的更多信息，請參閱 "將 Snapshot 副本提交到保管庫目標上的 WORM" 看"在拓撲頁面中查看 SAP HANA 資料庫備份和克隆"。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

10. 查看摘要，然後按一下「完成」。

建立資源組並附加策略

資源組是您必須新增要備份和保護的資源的容器。資源組可讓您同時備份與給定應用程式

相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

關於此任務

- 若要建立 SAP HANA 系統複製備份，建議將 SAP HANA 系統的所有資源新增至一個資源組。這可確保接管故障復原模式期間的無縫備份。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新資料庫新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下將新資料庫新增至現有資源組。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。  資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

4. 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。

這有助於過濾螢幕上的信息。
5. 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
6. 在應用程式設定頁面中，執行以下操作：

- a. 按一下“備份”箭頭以設定其他備份選項：

啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+

- 點擊“腳本”箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- 按一下「自訂配置」箭頭並輸入使用此資源的所有資料保護操作所需的自訂鍵值對。

範圍	環境	描述
歸檔日誌啟用	(是/否)	啟用存檔日誌管理以刪除存檔日誌。
歸檔日誌保留	天數	指定存檔日誌保留的天數。 此設定必須等於或大於 NTAP_SNAPSHOT_RETENTIONS。
歸檔日誌目錄	更改訊息目錄/日誌	指定包含存檔日誌的目錄的路徑。

範圍	環境	描述
ARCHIVE_LOG_EXT	檔案副檔名	指定存檔日誌檔案擴充長度。 例如，如果歸檔日誌為log_backup_0_0_0.161518551942 9，且file_extension值為5，則日誌的副檔名將保留5位數，即16151。
ARCHIVE_LOG_RECURSIVE_SEARCH	(是/否)	啟用子目錄內的存檔日誌管理。 如果存檔日誌位於子目錄下，則應使用此參數。



SAP HANA Linux 外掛系統支援自訂鍵值對，但註冊為集中式 Windows 外掛程式的 SAP HANA 資料庫不支援自訂鍵值對。

c. 點選*Snapshot Copy Tool*箭頭選擇建立快照的工具：

如果你想...	然後...
SnapCenter使用適用於 Windows 的插件並在建立快照之前將檔案系統置於一致狀態。對於 Linux 資源，此選項不適用。	選擇*具有檔案系統一致性的SnapCenter *。 此選項不適用於 SAP HANA 資料庫的SnapCenter 插件。
SnapCenter建立儲存等級 Snapshot	選擇“* 不具有檔案系統一致性的SnapCenter *”。
輸入要在主機上執行的命令來建立 Snapshot 副本。	選擇*其他*，然後輸入要在主機上執行的指令來建立Snapshot。

7. 在「策略」頁面中，執行以下步驟：

a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 * 來建立策略 *.

這些策略列在「為選定的策略配置計劃」部分中。

b. 在配置計劃列中，按一下 * * 您想要配置的策略。

c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。

其中，policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。必須在*設定* > *全域設定*中設定SMTP 伺服器。

9. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並啟用 **SAP HANA** 資源的二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建​​立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計畫的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：
 - a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：
 - a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
 - b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
 - c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtptServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 為 SAP HANA 資料庫建立儲存系統連線和憑證

在使用 PowerShell cmdlet 備份、還原或複製 SAP HANA 資料庫之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

步驟

1. 使用 Open-SmConnection cmdlet 啟動 PowerShell 連線會話。

```
PS C:\> Open-SmStorageConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例顯示如何使用 Windows 憑證建立名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. 將 SAP HANA 通訊主機新增至 SnapCenter 伺服器。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName  
FinanceAdmin -PluginCode hana
```

5. 在主機上安裝軟體套件和適用於 SAP HANA 資料庫的 SnapCenter 插件。

對於 Linux：

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode  
hana
```

對於 Windows：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana  
-FileSystemCode scw -RunAsName FinanceAdmin
```

6. 設定 HDBSQL 客戶端的路徑。

對於 Windows：

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode  
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program  
Files\sap\hdbclient\hdbsql.exe"}
```

對於 Linux：

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com  
-PluginCode hana -configSettings  
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

可以透過執行 `_Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

備份 SAP HANA 資料庫

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

開始之前

- 您必須已經建立了備份策略。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。
- 對於基於 Snapshot 副本的備份作業，請確保所有租用戶資料庫均有效且處於活動狀態。
- 若要建立 SAP HANA 系統複製備份，建議將 SAP HANA 系統的所有資源新增至一個資源組。這可確保接管故障復原模式期間的無縫備份。

["建立資源組並附加策略"](#)。

"備份資源組"

- 如果要在一個或多個租用戶資料庫關閉時建立基於檔案的備份，請在 HANA 屬性檔案中將 `ALLOW_FILE_BASED_BACKUP_IF_INACTIVE_TENANTS_PRESENT` 參數設定為 **YES**，使用 ``Set-SmConfigSettings`` 命令。

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)

- 對於靜默、快照和取消靜默操作的預先命令和後命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

選擇  *，然後選擇主機名稱和資源類型來過濾資源。然後您可以選擇  關閉篩選器窗格。

3. 選擇要備份的資源。
4. 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。

例如，*customtext_policy_hostname* 或 *resource_hostname*。預設情況下，時間戳記會附加到快照名稱。

5. 在應用程式設定頁面中，執行以下操作：

- 選擇“備份”箭頭來設定其他備份選項：

如果需要，請啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待「一致性組快照」操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

- 選擇「腳本」箭頭來執行靜默、快照和取消靜默操作的前置和後置命令。

您也可以在退出備份作業之前執行預命令。前言和後記在SnapCenter伺服器中運作。

- 選擇自訂配置箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
- 選擇*Snapshot Copy Tool*箭頭來選擇建立快照的工具：

如果你想...	然後...
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
SnapCenter使用適用於 Windows 的插件將檔案系統置於一致狀態，然後建立快照	選擇*具有檔案系統一致性的SnapCenter *。
輸入建立快照的命令	選擇*其他*，然後輸入建立快照的命令。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊  來建立策略 .

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 選擇  在您想要設定計畫的政策的政策設定計畫列中。
- c. 在為政策_policy_name_新增計劃對話方塊中，配置計畫，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後選擇*完成*。

進入資源拓樸頁面。

9. 選擇*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行

保留。

b. 選擇*備份*。

11. 透過點選「監視」>「作業」來監視操作進度。

- 在MetroCluster配置中， SnapCenter可能無法在故障轉移後偵測到保護關係。

有關信息，請參閱：["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java堆大小不夠大，則備份可能會失敗。

若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method` 命令啟動SnapCenter VMware 插件服務。將此指令更新為以下內容：`Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmResources cmdlet 新增資源。

此範例顯示如何新增 SingleContainer 類型的 SAP HANA 資料庫：

```
C:\PS> Add-SmResource -HostName '10.232.204.42' -PluginCode 'HANA'  
-DatabaseName H10 -ResourceType SingleContainer -StorageFootPrint  
(@{"VolumeName"="HanaData10";"StorageSystem"="vserver_scauto_primary"  
"}) -SID 'H10' -filebackuppath '/tmp/HanaFileLog' -userstorekeys  
'HS10' -osdbuser 'h10adm' -filebackupprefix 'H10_'
```

此範例顯示如何新增 MultipleContainers 類型的 SAP HANA 資料庫：

```
C:\PS> Add-SmResource -HostName 'vp-hana2.gdl.englab.netapp.com'  
-PluginCode 'HANA' -DatabaseName MDC_MT -ResourceType  
MultipleContainers -StorageFootPrint  
(@{"VolumeName"="VP_HANA2_data";"StorageSystem"="buck.gdl.englab.net  
app.com"}) -sid 'A12' -userstorekeys 'A12KEY' -TenantType  
'MultiTenant'
```

此範例顯示如何建立非資料卷資源：

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sscore.test.com'  
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType  
NonDataVolume -StorageFootPrint  
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})  
-sid 'S10'
```

3. 使用 Add-SmPolicy cmdlet 建立備份策略。

此範例為基於 Snapshot 副本的備份建立備份策略：

```
C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType  
Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
```

此範例為基於檔案的備份建立備份策略：

```
C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup  
-PluginPolicyType hana -BackupType FileBasedBackup
```

4. 使用 Add-SmResourceGroup cmdlet 保護資源或為SnapCenter新增資源組。

此範例保護單一容器資源：

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies  
hana_snapshotbased,hana_Filebased  
-Resources @{"Host"="host.example.com";"UID"="SID"} -Description  
test -usesnapcenterwithoutfilesystemconsistency
```

此範例保護多個容器資源：

```
C:\PS> Add-SmProtectResource -PluginCode HANA -Policies  
hana_snapshotbased,hana_Filebased  
-Resources @{"Host"="host.example.com";"UID"="MDC\SID"}  
-Description test -usesnapcenterwithoutfilesystemconsistency
```

此範例使用指定的策略和資源建立一個新的資源組：

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sscore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sscore.test.com";"Uid"="MDC\SID"})
-Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency -plugincode 'HANA'
```

此範例建立非資料卷資源組：

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sscore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

此範例顯示如何備份資源組：

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

此範例備份受保護的資源：

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. 使用 Get-smJobSummaryReport cmdlet 監視作業狀態（正在執行、已完成或失敗）。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. 使用 Get-SmBackupReport cmdlet 監視備份作業詳細資料（如備份 ID、備份名稱）以執行還原或複製作業。


```

PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId                : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime               : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                 : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                 : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :

```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份資源組

資源組是主機上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用「vsadmin」角色，則不需要「snapmirror all」權限。

關於此任務

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。

2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或選擇，然後選擇標籤。然後您可以選擇關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。

4. 在備份頁面中，執行以下步驟：

a. 如果您將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

b. 選擇*備份*。

5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

監控 SAP HANA 資料庫備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。

2. 在「監控」頁面中，按一下「作業」。

3. 在「作業」頁面中，執行下列步驟：

- a. 點選過濾清單以便僅列出備份操作。
- b. 指定開始和結束日期。
- c. 從「類型」下拉清單中，選擇「備份」。
- d. 從*狀態*下拉式選單中，選擇備份狀態。
- e. 點擊“應用”即可查看操作是否已成功完成。

4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監控 **SAP HANA** 資料庫上的資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消 **SAP HANA** 的備份作業

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	a. 在左側導覽窗格中，按一下「監控」>「作業」。 b. 選擇操作，然後按一下「取消作業」。

從...	行動
活動窗格	- 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 - 選擇操作。 - 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓撲頁面中查看 **SAP HANA** 資料庫備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。



顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

在拓撲頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。
-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓樸頁面。

4. 查看*摘要卡*以了解主儲存和輔助儲存上可用的備份和克隆數量的摘要。

*摘要卡*部分顯示基於檔案的備份、基於快照副本的備份和複製的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 會自動配置為新的主目標。
 - 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。
5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

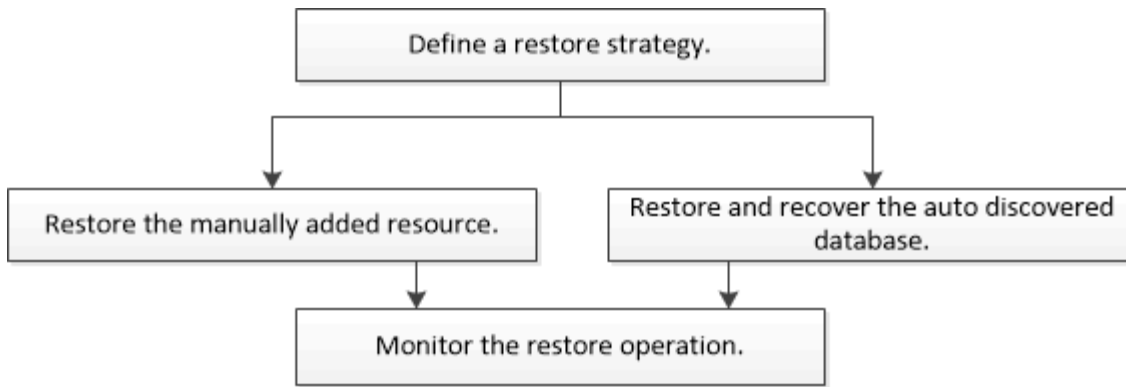
7. 如果要刪除克隆，請從表中選擇克隆，然後按一下 。
8. 如果要拆分克隆，請從表中選擇克隆，然後按一下 。

還原 SAP HANA 資料庫

復原工作流程

還原和復原工作流程包括規劃、執行還原操作和監視操作。

以下工作流程顯示了執行還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

["SnapCenter軟體 Cmdlet 參考指南"](#)。

還原並還原手動新增的資源備份

您可以使用SnapCenter從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 無法從SnapCenter還原基於檔案的備份副本。
- 升級到SnapCenter 4.3 後，可以還原在SnapCenter 4.2 中建立的備份，但無法復原。您必須使用SnapCenter外部的 HANA 工作室或 HANA 復原腳本來還原在SnapCenter 4.2 中建立的備份。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 在「復原範圍」頁面中，選擇「完整資源」或「檔案層級」。
 - a. 如果選擇“完整資源”，則會還原 SAP HANA 資料庫的所有已配置資料磁碟區。

如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果在相同的磁碟區或 qtree 上託管任何其他資源，則該資源也會被刪除。

- b. 如果選擇“檔案等級”，則可以選擇“全部”或選擇特定的磁碟區或 qtree，然後輸入與這些磁碟區或 qtree 相關的路徑（以逗號分隔）
 - 您可以選擇多個磁碟區和 qtree。
 - 如果資源類型為LUN，則還原整個LUN。

您可以選擇多個 LUN。



如果選擇“全部”，則會還原磁碟區、qtree 或 LUN 上的所有檔案。

7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

10. 查看摘要，然後按一下「完成」。

11. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：


```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

還原和還原自動發現的資料庫備份

您可以使用 SnapCenter 從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 無法從SnapCenter還原基於檔案的備份副本。
- 升級到SnapCenter 4.3 後，可以還原在SnapCenter 4.2 中建立的備份，但無法復原。您必須使用SnapCenter外部的 HANA 工作室或 HANA 復原腳本來還原在SnapCenter 4.2 中建立的備份。
- 對於ONTAP 9.12.1 及更早版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



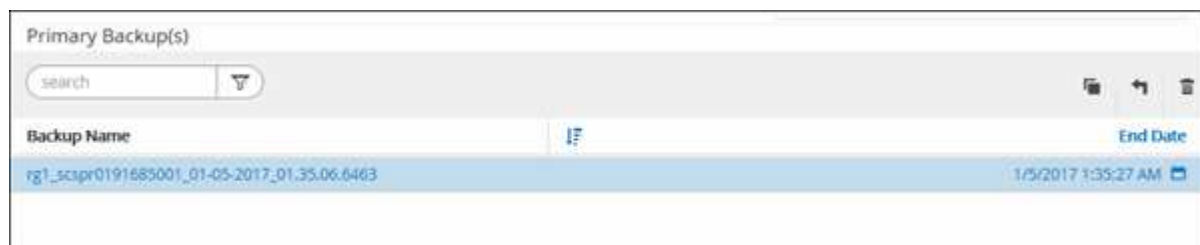
儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.



6. 在「復原範圍」頁面中，選擇「完整資源」以還原 SAP HANA 資料庫的已設定資料磁碟區。



您可以選擇*完整資源*（帶或不帶*卷恢復*）或*租戶資料庫*。

當使用者選擇「租用戶資料庫」或「完全還原」選項時，SnapCenter Server 不支援對多個租用戶執行復原作業。您必須使用 HANA 工作室或 HANA python 腳本來執行復原操作。

- a. 如果您想恢復整個卷，請選擇*卷恢復*。

此選項適用於在 NFS 環境中使用SnapCenter 4.3 進行的備份。

如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。當選擇帶有 **Volume Revert** 選項的 **Complete Resource** 進行復原時，這適用。

b. 選擇*租戶資料庫*。

此選項僅適用於 MDC 資源。

確保在執行復原操作之前停止租戶資料庫。

如果選擇「租用戶資料庫」選項，則必須使用 HANA 工作室或使用SnapCenter外部的 HANA 復原腳本來執行復原作業。

7. 在「恢復範圍」頁面中，選擇以下選項之一：

如果你...	這樣做...
希望恢復到盡可能接近當前時間	選擇*恢復到最近的狀態*。對於單一容器資源，指定一個或多個日誌和目錄備份位置。 對於多租用戶資料庫容器 (MDC) 資源，指定一個或多個日誌備份位置和備份目錄位置。 對於 MDC 資源，路徑應包含系統資料庫和租用戶資料庫日誌。

如果你...	這樣做...
想要恢復到指定的時間點	選擇*恢復到時間點*。 a. 選擇時區。 瀏覽器時區預設填滿。 所選時區以及輸入時間將轉換為絕對格林威治標準時間。 b. 輸入日期和時間。例如，HANA Linux 主機位於加州桑尼維爾，而北卡羅來納州羅利的用戶正在將日誌還原到SnapCenter。 這兩個地點之間的時差為 3 小時，由於用戶從北卡羅來納州羅利市登錄，因此 GUI 中選擇的預設瀏覽器時區為 GMT-04:00。 如果使用者想要恢復到凌晨 5 點，則使用者必須將瀏覽器時區設定為 HANA Linux 主機時區，即 GMT-07:00，並將日期和時間指定為凌晨 5:00 對於單一容器資源，指定一個或多個日誌和目錄備份位置。 對於 MDC 資源，指定一個或多個日誌備份位置和備份目錄位置。 對於 MDC 資源，路徑應包含系統資料庫和租用戶資料庫日誌。
想要還原到特定的資料備份	選擇*恢復到指定的資料備份*。
不想恢復	選擇*不恢復*。您必須從 HANA 工作室手動執行復原操作。

您只能恢復升級到SnapCenter 4.3 後建立的備份，前提是主機和外掛程式都升級到SnapCenter 4.3，並且選擇用於還原的備份是在資源轉換或發現為自動發現的資源後建立的。

- 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

- 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

- 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設

定 SMTP。

11. 查看摘要，然後按一下「完成」。
12. 透過點選「監視」>「作業」來監視操作進度。

使用 PowerShell cmdlet 還原資源

恢復資源備份包括啟動與SnapCenter伺服器的連線會話、列出備份並檢索備份資訊以及恢復備份。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 SAP HANA 資料庫復原操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成

-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

克隆 SAP HANA 資源備份

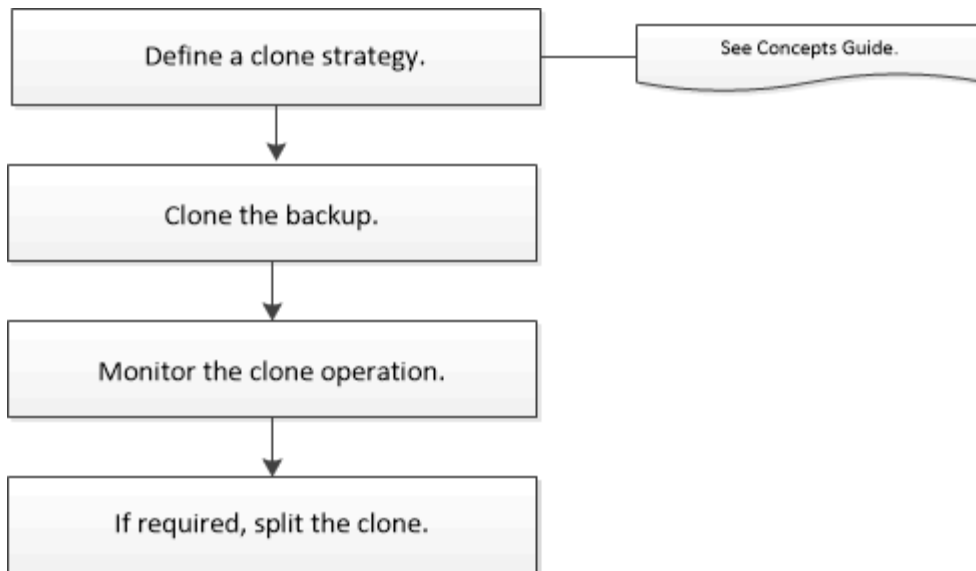
克隆工作流程

克隆工作流程包括執行克隆操作和監視操作。

關於此任務

- 您可以在來源 SAP HANA 伺服器上進行複製。
- 您可能會因為以下原因而複製資源備份：
 - 在應用程式開發週期中測試必須使用目前資源結構和內容實現的功能
 - 用於填充資料倉儲時的資料擷取和操作工具
 - 恢復被錯誤刪除或更改的數據

以下工作流程顯示了執行複製操作必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

克隆 SAP HANA 資料庫備份

您可以使用 SnapCenter 克隆備份。您可以從主備份或輔助備份複製。

開始之前

- 您應該已經備份資源或資源組。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 您無法克隆基於檔案的備份。
- 目標複製伺服器應具有與目標複製 SID 欄位中提供的相同的 SAP HANA 實例 SID。
- 對於克隆前或克隆後命令，您應該從以下路徑檢查這些命令是否存在於插件主機上可用的命令清單中：
 - 對於 Windows：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - 對於 Linux：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 有關克隆拆分操作限制的信息，請參閱 ["ONTAP 9 邏輯儲存管理指南"](#)。
- 對於 ONTAP 9.12.1 及更早版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和策略以及狀態等資訊一起顯示。

3. 選擇資源或資源組。

如果選擇資源組，則必須選擇資源。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
插件主機	選擇要掛載克隆並安裝插件的主機。
目標複製 SID	輸入要從現有備份中複製的 SAP HANA 實例 ID。
NFS 匯出 IP 位址	輸入將會匯出複製磁碟區的 IP 位址或主機名稱。
iSCSI 發起程序	輸入 LUN 匯出到的主機 iSCSI 啟動器名稱。只有當您選擇了 LUN 資源類型時，此選項才可用。
協定	輸入 LUN 協定。只有當您選擇了 LUN 資源類型時，此選項才可用。

如果選擇的資源是 LUN 並且您正在從輔助備份進行克隆，則會列出目標磁碟區。單一來源可以有多個目標磁碟區。



在複製之前，您必須確保 iSCSI 啟動器或 FCP 存在並且已設定並登入備用主機。

7. 在腳本頁面中，執行以下步驟：



腳本在插件主機上運行。

- a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。

- 克隆前指令：刪除現有的同名資料庫
- 克隆後指令：驗證資料庫或啟動資料庫。

b. 輸入 mount 指令將檔案系統掛載到主機。

Linux 電腦上磁碟區或 qtree 的掛載指令：

NFS 範例：mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

9. 查看摘要，然後按一下「完成」。

10. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146/
```

2. 使用 Get-SmBackup cmdlet 檢索備份以執行複製作業。

此範例顯示有兩個備份可供複製：

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 從現有備份啟動複製操作，並指定複製磁碟區匯出到的 NFS 匯出 IP 位址。

此範例顯示要複製的備份具有 NFSExportIPs 位址 10.232.206.169：

```
New-SmClone -AppPluginCode hana -BackupName
scsccore1_sccore_test_com_hana_H73_scsccore1_06-07-
2017_02.54.29.3817 -Resources
@{"Host"="scsccore1.sccore.test.com";"Uid"="H73"} -CloneToInstance
shivsc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```



如果沒有指定NFSExportIPs，則預設匯出至複製目標主機。

4. 使用 Get-SmCloneReport cmdlet 查看複製作業詳細信息，以驗證備份是否已成功複製。

您可以查看複製 ID、開始日期和時間、結束日期和時間等詳細資訊。

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration              : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName      : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

監控 SAP HANA 資料庫克隆操作

您可以使用「作業」頁面監控SnapCenter複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2 後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。

2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“”。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCore 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定 SMCore 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為 5 分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter 克隆或驗證失敗，聚合不存在"](#)

升級 SnapCenter 後刪除或分割 SAP HANA 資料庫克隆

升級到 SnapCenter 4.3 後，您將不再看到克隆。您可以從建立克隆的資源的拓樸頁面中刪除克隆或分割克隆。

關於此任務

如果您要找到隱藏複製的儲存空間，請執行以下命令：Get-SmClone -ListStorageFootprint

步驟

1. 使用 remove-smbbackup cmdlet 刪除克隆資源的備份。
2. 使用 remove-smresourcegroup cmdlet 刪除克隆資源的資源群組。
3. 使用 remove-smprotectresource cmdlet 刪除克隆資源的保護。

4. 從資源頁面中選擇父資源。

進入資源拓樸頁面。

5. 從「管理副本」檢視中，選擇來自主或輔助（鏡像或複製）儲存系統的複製。

6. 選擇克隆，然後按一下  刪除克隆或點擊  分裂克隆。

7. 按一下“確定”。

保護 Oracle 資料庫

Oracle 資料庫的SnapCenter插件概述

您可以使用 **Oracle** 資料庫插件做什麼

Oracle 資料庫的SnapCenter插件是NetApp SnapCenter軟體的主機端元件，可實現 Oracle 資料庫的應用程式感知資料保護管理。

Oracle 資料庫外掛程式可使用 Oracle Recovery Manager (RMAN) 自動執行備份、編目和取消編目，以及在SnapCenter環境中驗證、掛載、解除安裝、還原、還原和複製 Oracle 資料庫。Oracle 資料庫插件安裝適用於 UNIX 的SnapCenter插件來執行所有資料保護操作。

您可以使用 Oracle 資料庫外掛程式來管理執行 SAP 應用程式的 Oracle 資料庫的備份。但是，不支援 SAP BR*Tools 整合。

- 備份資料檔案、控制檔案和存檔日誌檔案。

僅在容器資料庫 (CDB) 層級支援備份。

- 資料庫、CDB 和可插拔資料庫 (PDB) 的還原和復原。

不支援 PDB 的不完全恢復。

- 建立某個時間點的生產資料庫克隆。

僅 CDB 等級支援克隆。

- 立即驗證備份。
- 為復原作業掛載和卸載資料和日誌備份。
- 安排備份和驗證作業。
- 監控所有操作。
- 查看備份、復原和克隆作業的報告。
- 自動執行SnapCenter環境中 Oracle 資料庫的應用程式感知備份、還原、復原、驗證、掛載、解除安裝和複製作業
- 支援 SAP 的 Oracle 資料庫，但不提供 SAP BR*Tools 集成

Oracle 資料庫插件的功能

Oracle 資料庫外掛程式可與 Linux 或 AIX 主機上的 Oracle 資料庫以及儲存系統上的NetApp技術整合。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨插件完成一致的備份、還原、還原和複製操作，使用集中式報告，使用一目了然的儀表板視圖，設定基於角色的存取控制 (RBAC)，

並監控所有插件中的作業。

- 自動化中央管理

您可以安排備份和複製作業、配置基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷NetApp Snapshot 技術

SnapCenter使用NetApp Snapshot 技術以及 Oracle Database 插件和 UNIX 插件來備份資料庫。快照佔用的儲存空間極小。

Oracle 資料庫外掛程式還具有以下優點：

- 支援備份、復原、複製、掛載、卸載和驗證工作流程
- 自動發現主機上配置的 Oracle 資料庫
- 支援使用 Oracle Recovery Manager (RMAN) 進行編目和取消編目
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 支援用於復原和複製操作的存檔日誌管理 (ALM)
- 使用NetApp FlexClone技術建立生產資料庫的空間高效和時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 在 SAN 和 ASM 環境中建立備份時支援ONTAP的一致性群組 (CG) 功能
- 無中斷和自動化備份驗證
- 能夠跨多個資料庫主機同時執行多個備份

在單一操作中，當單一主機中的資料庫共用同一磁碟區時，快照就會合併。

- 支援實體和虛擬化基礎設施
- 支援 NFS、iSCSI、光纖通道 (FC)、RDM、NFS 和 VMFS 上的 VMDK 以及 NFS、SAN、RDM 和 VMDK 上的 ASM
- 支援ONTAP的選擇性 LUN 映射 (SLM) 功能

SLM 功能預設為啟用，它會定期發現沒有最佳化路徑的 LUN 並進行修復。您可以透過修改位於 `/var/opt/snapcenter/scu/etc` 的 `scu.properties` 檔案中的參數來配置 SLM。

- 您可以將 `ENABLE_LUNPATH_MONITORING` 參數的值設為 `false` 來停用此功能。
- 您可以透過為 `LUNPATH_MONITORING_INTERVAL` 參數指派值（以小時為單位）來指定自動修復 LUN 路徑的頻率。有關 SLM 的信息，請參閱 ["ONTAP 9 SAN 管理部分"](#)。

- Linux 上對非揮發性記憶體標準 (NVMe) 的支持
 - 主機上應安裝 NVMe util。

您必須安裝 NVMe util 才能複製或安裝到備用主機。

- 除 RDM 等虛擬化環境外，NVMe 硬體支援備份、復原、複製、掛載、卸載、編目、取消編目和驗證作業。

以上操作在無分區或單分區的設備上均支援。



您可以透過在核心中設定本機多路徑選項來為 NVMe 裝置配置多路徑解決方案。不支援裝置映射器 (DM) 多路徑。

- NVMe over TCP/IP 支援備份、復原、複製、掛載、卸載、編目、取消編目和驗證工作流程。
- 在 NVMe over TCP/IP 上建立的 VMDK 佈局支援備份、復原、複製、掛載、卸載、編目、取消編目和驗證工作流程。
- 支援 SnapMirror 主動同步（最初作為 SnapMirror 業務連續性 [SM-BC] 發布），即使整個網站發生故障，也能使業務服務繼續運行，支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過 SnapMirror 主動同步觸發故障轉移。
- 支援任何非預設用戶，而不是 oracle 和 grid。

為了支援非預設用戶，您應該透過修改位於 `file /var/opt/snapcenter/sco/etc/` 的 **sco.properties** 檔案中的參數值來設定非預設用戶。

參數的預設值設定為 oracle 和 grid。

- DB_USER=oracle
- DB_GROUP=安裝
- GI_USER=網格
- GI_GROUP=安裝

Oracle Database 外掛程式支援的儲存類型

SnapCenter 支援實體機器和虛擬機器上的多種儲存類型。在安裝適用於 Linux 的 SnapCenter 插件包或適用於 AIX 的 SnapCenter 插件包之前，您必須驗證對您的儲存類型的支援。

SnapCenter 不支援 Linux 和 AIX 的儲存配置。

Linux 支援的儲存類型

下表列出了 Linux 上支援的儲存類型。

機器	儲存類型
實體伺服器	• FC 連接的 LUN • iSCSI 連接的 LUN • NFS 連結卷 • NVMe光纖通道 • NVMe/TCP
VMware ESXi	• 透過 FC 或 iSCSI ESXi HBA 連線的 RDM LUN 主機匯流排適配器 (HBA) 掃描可能需要很長時間才能完成，因為SnapCenter會掃描主機中存在的所有主機匯流排適配器。 您可以編輯位於 <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> 的 LinuxConfig.pm 文件，將 SCSI_HOSTS_OPTIMIZED_RESCAN 參數的值設定為 1，以僅重新掃描 HBA_DRI VBA 中列出的那些參數的值。 • iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統 • NFS 資料儲存上的 VMDK • 透過 NVMe/TCP 建立的 VMFS 上的 VMDK  ESX 8.0U2 支援 RAC，並支援共享 VMDK • NFS 磁碟區直接連接到客戶系統 • NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

AIX 上支援的儲存類型

下表列出了 AIX 上支援的儲存類型。

機器	儲存類型
實體伺服器	- FC 連線和 iSCSI 連線的 LUN。 在 SAN 環境中，支援 ASM、LVM 和 SAN 檔案系統。  不支援 AIX 和檔案系統上的 NFS。 - 增強型日誌檔案系統 (JFS2) 支援 SAN 檔案系統和 LVM 佈局上的內聯日誌記錄。

這 ["NetApp互通性表工具"](#) 包含受支援版本的最新資訊。

為 Oracle 插件準備 SnapMirror 和 SnapVault 複製的儲存系統

您可以使用具有 ONTAP SnapMirror 技術的 SnapCenter 插件在另一個磁碟區上建立備份集的鏡像副本，並使用 ONTAP SnapVault 技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter 完成 Snapshot 作業後對 SnapMirror 和 SnapVault 執行更新。SnapMirror 和 SnapVault 更新作為 SnapCenter 作業的一部分執行；不要建立單獨的 ONTAP 計畫。



如果您從 NetApp SnapManager 產品前往 SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP 會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter 不支援 SnapMirror 和 SnapVault 磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter 支援版本靈活的 SnapMirror 關係的管理。有關版本靈活的 SnapMirror 關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

Oracle 插件所需的最低 ONTAP 權限

所需的最低 ONTAP 權限會根據您用於資料保護的 SnapCenter 插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止

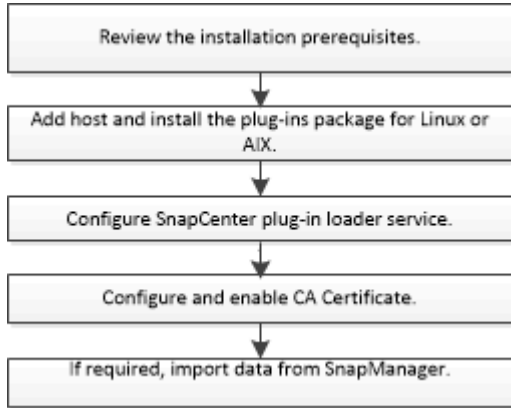
- 倫
- lun 屬性顯示
- lun 創建
- lun 刪除
- 倫幾何
- lun igroup 新增
- lun igroup 創建
- lun igroup 刪除
- lun igroup 重新命名
- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本

- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線
- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器
- 虛擬伺服器 CIFS
- vservers cifs 影子複製顯示
- 虛擬伺服器顯示
- 網路介面
- 網路介面顯示
- 大都會集群秀

為 Oracle 資料庫安裝 SnapCenter 插件

Oracle 資料庫的 SnapCenter 插件安裝工作流程

如果您想要保護 Oracle 資料庫，則應該安裝並設定適用於 Oracle 資料庫的 SnapCenter 插件。



新增主機並安裝 Linux 或 AIX 插件包的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。

- 如果您正在使用 iSCSI，則 iSCSI 服務必須正在執行。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。

非 root 使用者可以安裝適用於 Oracle 資料庫的 SnapCenter 插件。但是，您應該為非 root 使用者配置 sudo 權限來安裝和啟動插件進程。安裝插件後，進程將作為有效的非 root 用戶運行。

- 如果您正在 AIX 主機上安裝適用於 AIX 的 SnapCenter 插件包，則應該手動解析目錄級符號連結。

AIX 的 SnapCenter 插件包會自動解析文件級符號鏈接，但不解析目錄級符號鏈接以獲取 JAVA_HOME 絕對路徑。

- 為安裝使用者建立驗證模式為 Linux 或 AIX 的憑證。
- 您必須在 Linux 或 AIX 主機上安裝 Java 11。
 - Linux 支援 Oracle 和 OpenJDK 的 Java
 - 適用於 AIX 的 IBM Java。您可以從下載 ["IBM Semeru 執行階段下載"](#)



確保您在 Linux 主機上僅安裝了 JAVA 11 的認證版本。

- 對於在 Linux 或 AIX 主機上執行的 Oracle 資料庫，您應該同時安裝適用於 Oracle 資料庫的 SnapCenter 插件和適用於 UNIX 的 SnapCenter 插件。



您也可以使用 Oracle 資料庫外掛程式來管理 SAP 的 Oracle 資料庫。但是，不支援 SAP BR*Tools 整合。

- 如果您使用的是 Oracle 資料庫 11.2.0.3 或更高版本，則必須安裝 13366202 Oracle 修補程式。



SnapCenter不支援 /etc/fstab 檔案中的 UUID 對映。

- 您應該將 **bash** 作為插件安裝的預設 shell。

Linux 主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該確保主機符合要求。

物品	要求
作業系統	• 紅帽企業 Linux • Oracle Linux 如果您在 Oracle Linux 或 Red Hat Enterprise Linux 6.6 或 7.0 作業系統中的 LVM 上使用 Oracle 資料庫，則必須安裝最新版本的邏輯磁碟區管理器 (LVM)。 • SUSE Linux 企業伺服器 (SLES)
主機上SnapCenter插件的最小 RAM	2GB
主機上SnapCenter插件的最小安裝和日誌空間	2GB 您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle 和 OpenJDK 確保您在 Linux 主機上僅安裝了 JAVA 11 的認證版本。 如果您已將 JAVA 升級至最新版本，則必須確保位於 /var/opt/snapcenter/spl/etc/spl.properties 的 JAVA_HOME 選項設定為正確的 JAVA 版本和正確的路徑。

有關受支援版本的最新信息，請參閱 ["NetApp互通性表工具"](#)。

為 Linux 主機的非 root 使用者配置 **sudo** 權限

SnapCenter 2.0 及更高版本允許非 root 用戶安裝適用於 Linux 的SnapCenter插件套件並啟動插件進程。插件進

程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 為 0027，請確保 java 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 Linux 的SnapCenter插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`LINUX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

AIX 主機需求

在安裝適用於 AIX 的 SnapCenter 插件包之前，您應該確保主機符合要求。



SnapCenter Plug-in for UNIX 是 SnapCenter Plug-ins Package for AIX 的一部分，不支援並發磁碟區組。

物品	要求
作業系統	AIX 7.1 或更高版本
主機上SnapCenter插件的最小 RAM	4GB
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 IBM Java 如果您已將 JAVA 升級至最新版本，則必須確保位於 /var/opt/snapcenter/spl/etc/spl.properties 的 JAVA_HOME 選項設定為正確的 JAVA 版本和正確的路徑。

有關受支援版本的最新信息，請參閱 ["NetApp互通性表工具"](#)。

為 AIX 主機的非 root 使用者配置 sudo 權限

SnapCenter 4.4 及更高版本允許非 root 用戶安裝適用於 AIX 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 為 0027，請確保 java 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- /home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載
- /custom_location/ NetApp/snapcenter/spl/bin/spl

步驟

1. 登入要安裝適用於 AIX 的 SnapCenter 插件包的 AIX 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 /etc/sudoers 檔案。

```
Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty
```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
“`/<crs_home>/bin/olsnodes`”

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`AIX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

設定憑證

SnapCenter 使用憑證對 SnapCenter 操作的使用者進行身份驗證。您應該建立用於在 Linux 或 AIX 主機上安裝插件包的憑證。

關於此任務

憑證是為 root 使用者或具有 sudo 權限的非 root 使用者建立的，用於安裝和啟動插件進程。

有關信息，請參閱：[為 Linux 主機的非 root 使用者配置 sudo 權限](#) 或者 [為 AIX 主機的非 root 使用者配置 sudo 權限](#)

*最佳實務：*雖然您可以在部署主機和安裝外掛程式後建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在憑證頁面中，輸入憑證資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。

對於這個領域...	這樣做...
使用者名稱/密碼	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員 指定要安裝SnapCenter插件的系統上的網域管理員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i>
認證模式	選擇您想要使用的身份驗證模式。 根據插件主機的作業系統，選擇 Linux 或 AIX。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。

5. 按一下“確定”。

完成憑證設定後，您可能想要在*使用者和存取*頁面上將憑證維護指派給使用者或使用者群組。

配置 Oracle 資料庫的憑證

您必須設定用於在 Oracle 資料庫上執行資料保護作業的憑證。

關於此任務

您應該查看 Oracle 資料庫支援的不同身份驗證方法。有關信息，請參閱["您的憑證的身份驗證方法"](#)。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則該使用者名稱至少必須具有資源群組和備份權限。

如果您啟用了 Oracle 資料庫驗證，資源視圖中會顯示一個紅色掛鎖圖示。您必須配置資料庫憑證才能保護資料庫或將其新增至資源組以執行資料保護操作。



如果您在建立憑證時指定了不正確的詳細信息，則會顯示錯誤訊息。您必須按一下“取消”，然後重試。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。
3. 點選，然後選擇主機名稱和資料庫類型來過濾資源。

然後您可以點選關閉篩選器窗格。

4. 選擇資料庫，然後按一下*資料庫設定*>*配置資料庫*。
5. 在設定資料庫設定部分中，從*使用現有憑證*下拉清單中，選擇套用於在 Oracle 資料庫上執行資料保護作業的憑證。



Oracle 使用者應具有 sysdba 權限。

您也可以透過點選建立憑證。

6. 在設定 ASM 設定部分中，從*使用現有憑證*下拉清單中，選擇套用於在 ASM 實例上執行資料保護作業的憑證。



ASM 使用者應該具有 sysasm 權限。

您也可以透過點選建立憑證。

7. 在設定 RMAN 目錄設定部分中，從 使用現有憑證 下拉清單中，選擇套用於在 Oracle Recovery Manager (RMAN) 目錄資料庫上執行資料保護作業的憑證。

您也可以透過點選建立憑證。

在 **TNSName** 欄位中，輸入SnapCenter伺服器將用於與資料庫通訊的透明網路底層 (TNS) 檔案名稱。

8. 在「首選 **RAC** 節點」欄位中，指定備份所需的 Real Application Cluster (RAC) 節點。

首選節點可能是 RAC 資料庫實例所在的一個或所有叢集節點。備份操作僅在這些優先節點上按優先順序觸發。

在 RAC One Node 中，首選節點中僅列出一個節點，該節點是資料庫目前所在的節點。

在 RAC One Node 資料庫故障轉移或重新定位後，刷新SnapCenter資源頁面中的資源將從資料庫先前託管的首選 **RAC** 節點 清單中刪除該主機。資料庫重新定位的 RAC 節點將在 **RAC** 節點 中列出，並且需要手動配置為首選 RAC 節點。

有關更多信息，請參閱["RAC 設定中的首選節點"](#)。

9. 按一下“確定”。

使用 GUI 新增主機並安裝 Linux 或 AIX 插件包

您可以使用「新增主機」頁面新增主機，然後安裝適用於 Linux 的SnapCenter插件套件或適用於 AIX 的SnapCenter插件套件。插件會自動安裝在遠端主機上。

關於此任務

您可以為單一主機或叢集新增主機並安裝插件包。如果在叢集（Oracle RAC）上安裝該插件，則該插件將安裝在叢集的所有節點上。對於 Oracle RAC One Node，您應該在主動節點和被動節點上安裝該插件。



在 Oracle RAC 上安裝插件時僅支援基於密碼的身份驗證。不支援基於 SSH 金鑰的身份驗證。

您應該被指派一個具有插件安裝和卸載權限的角色，例如SnapCenter管理員角色。



您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。

步驟

- 1. 在左側導覽窗格中，按一下「主機」。
- 2. 驗證頂部的「託管主機」標籤是否已選取。
- 3. 按一下“新增”。
- 4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇 Linux 或 AIX 作為主機類型。 SnapCenter伺服器新增主機，然後安裝適用於 Oracle 資料庫的插件和適用於 UNIX 的插件（如果主機上尚未安裝這些插件）。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • Oracle Real Application Clusters (RAC) 環境中的任意節點  不支援節點 VIP 或掃描 IP 如果您使用SnapCenter新增主機且該主機是子網域的一部分，則必須提供 FQDN。

對於這個領域...	這樣做...
證書	選擇您建立的憑證名稱或建立新的憑證。 該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標置於指定的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。 預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑為 <code>/opt/NetApp/snapcenter</code>。 您可以選擇自訂路徑。
新增 Oracle RAC 中的所有主機	選取此複選框可新增 Oracle RAC 中的所有叢集節點。 在 Flex ASM 設定中，所有節點（無論是 Hub 節點或 Leaf 節點）都會被新增。
跳過可選的預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。

7. 點選“提交”。

如果您沒有選取「跳過預檢查」複選框，則會對主機進行驗證，以驗證主機是否符合安裝外掛程式的要求。



如果防火牆拒絕規則中指定了插件連接埠防火牆狀態，則預先檢查腳本不會驗證該狀態。

如果未滿足最低要求，則會顯示適當的錯誤或警告訊息。如果錯誤與磁碟空間或 RAM 有關，您可以更新位

於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 檔案以修改預設值。如果錯誤與其他參數有關，則應修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



SnapCenter不支援 ECDSA 演算法。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

特定於安裝的日誌檔案位於 /custom_location/snapcenter/logs。

結果

主機上的所有資料庫都會自動發現並顯示在資源頁面中。如果沒有顯示任何內容，請按一下「刷新資源」。

監控安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。

- e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

安裝 Linux 或 AIX 插件包的其他方法

您也可以使用 cmdlet 或 CLI 手動安裝適用於 Linux 或 AIX 的插件套件。

在手動安裝插件之前，您應該使用位於 `C:\ProgramData\NetApp\SnapCenter\Package Repository` 的金鑰 `snapcenter_public_key.pub` 和 `snapcenter_linux_host_plugin.bin.sig` 驗證二進位套件的簽章。



確保要安裝插件的主機上安裝了 **OpenSSL 1.0.2g**。

透過執行以下命令驗證二進位套件的簽章：

- 對於 Linux 主機：`openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- 對於 AIX 主機：`openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

使用 cmdlet 在多個遠端主機上安裝

您應該使用 *Install-SmHostPackage* PowerShell cmdlet 在多個主機上安裝適用於 Linux 的 SnapCenter 插件包或適用於 AIX 的 SnapCenter 插件包。

您需要什麼

您應該以網域使用者身分登入 SnapCenter，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在 SnapCenter Server 主機上，使用 *Open-SmConnection* cmdlet 建立會話，然後輸入您的憑證。
3. 使用 *Install-SmHostPackage* cmdlet 和所需參數安裝適用於 Linux 的 SnapCenter 插件包或適用於 AIX 的 SnapCenter 插件包。

當您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `_skipprecheck_` 選項。



如果防火牆拒絕規則中指定了插件連接埠防火牆狀態，則預先檢查腳本不會驗證該狀態。

4. 輸入您的遠端安裝憑證。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

在叢集主機上安裝

您應該在叢集主機的兩個節點上安裝適用於 Linux 的 SnapCenter 插件包或適用於 AIX 的 SnapCenter 插件包。

叢集主機的每個節點都有兩個IP。其中一個 IP 將是各個節點的公共 IP，第二個 IP 將是兩個節點之間共享的叢集 IP。

步驟

1. 在叢集主機的兩個節點上安裝適用於 Linux 的 SnapCenter 插件包或適用於 AIX 的 SnapCenter 插件包。
2. 驗證位於 `/var/opt/snapcenter/spl/etc/` 的 `spl.properties` 檔案中指定了 `SNAPCENTER_SERVER_HOST`、`SPL_PORT`、`SNAPCENTER_SERVER_PORT` 和 `SPL_ENABLED_PLUGINS` 參數的正確值。

如果 `spl.properties` 中未指定 `SPL_ENABLED_PLUGINS`，則可以新增它並指派值 `SCO,SCU`。

3. 在 SnapCenter Server 主機上，使用 `Open-SmConnection` cmdlet 建立會話，然後輸入您的憑證。
4. 在每個節點中，使用 `Set-PreferredHostIPsInStorageExportPolicy` sccli 指令和所需參數設定節點的首選 IP。
5. 在 SnapCenter Server 主機中，在 `C:\Windows\System32\drivers\etc\hosts` 中新增叢集 IP 和對應 DNS 名稱的項目。
6. 透過指定主機名稱的叢集 IP，使用 `Add-SmHost` cmdlet 將節點新增至 SnapCenter 伺服器。

發現節點 1 上的 Oracle 資料庫（假設叢集 IP 託管在節點 1 上）並建立資料庫的備份。如果發生故障轉移，您可以使用在節點 1 上建立的備份來還原節點 2 上的資料庫。您也可以使用在節點 1 上建立的備份在節點 2 上建立克隆。



如果在執行任何其他 SnapCenter 作業時發生故障轉移，則會出現過時的磁碟區、目錄和鎖定檔案。

靜默模式下安裝 Linux 插件包

您可以使用命令列介面 (CLI) 以靜默模式安裝適用於 Linux 的 SnapCenter 插件包。

您需要什麼

- 您應該查看安裝插件包的先決條件。
- 您應該確保未設定 `DISPLAY` 環境變數。

如果設定了 `DISPLAY` 環境變量，則應執行 `unset DISPLAY`，然後嘗試手動安裝插件。

關於此任務

在控制台模式下安裝時，您需要提供必要的安裝信息，而在靜默模式下安裝時，您不必提供任何安裝信息。

步驟

1. 從 SnapCenter 伺服器安裝位置下載適用於 Linux 的 SnapCenter 插件套件。

預設安裝路徑為 `_C:\ProgramData\ NetApp\ SnapCenter\PackageRepository_`。可以從安裝 SnapCenter 伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至下載安裝檔案的目錄。
3. 跑步

```
./SnapCenter_linux_host_plugin.bin-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom_path
```

4. 編輯位於 `/var/opt/snapcenter/spl/etc/` 的 `spl.properties` 檔案以新增 `SPL_ENABLED_PLUGINS=SCO,SCU`，然後重新啟動SnapCenter插件Loader服務。



插件包的安裝會在主機上註冊插件，而不是在SnapCenter伺服器上註冊。您應該透過使用SnapCenter GUI 或 PowerShell cmdlet 新增主機在SnapCenter伺服器上註冊插件。新增主機時，選擇“無”作為憑證。新增主機後，會自動發現已安裝的插件。

靜默模式下安裝 AIX 插件包

您可以使用命令列介面 (CLI) 以靜默模式安裝適用於 AIX 的SnapCenter插件包。

您需要什麼

- 您應該查看安裝插件包的先決條件。
- 您應該確保未設定 `DISPLAY` 環境變數。

如果設定了 `DISPLAY` 環境變量，則應執行 `unset DISPLAY`，然後嘗試手動安裝插件。

步驟

1. 從SnapCenter伺服器安裝位置下載適用於 AIX 的SnapCenter插件包。

預設安裝路徑為 `C:\ProgramData\ NetApp\ SnapCenter\PackageRepository_`。可以從安裝SnapCenter伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至下載安裝檔案的目錄。
3. 跑步

```
./snapcenter_aix_host_plugin.bsx-i silent-DPORT=8145-  
DSERVER_IP=SnapCenter_Server_FQDN-DSERVER_HTTPS_PORT=SnapCenter_Server_Port-  
DUSER_INSTALL_DIR==/opt/custom_path-  
DINSTALL_LOG_NAME=SnapCenter_AIX_Host_Plug-in_Install_MANUAL.log-  
DCHOSEN_FEATURE_LIST=CUSTOMDSPL_USER=install_user
```

4. 編輯位於 `/var/opt/snapcenter/spl/etc/` 的 `spl.properties` 檔案以新增 `SPL_ENABLED_PLUGINS=SCO,SCU`，然後重新啟動SnapCenter插件Loader服務。



插件包的安裝會在主機上註冊插件，而不是在SnapCenter伺服器上註冊。您應該透過使用SnapCenter GUI 或 PowerShell cmdlet 新增主機在SnapCenter伺服器上註冊插件。新增主機時，選擇“無”作為憑證。新增主機後，會自動發現已安裝的插件。

配置SnapCenter插件Loader服務

SnapCenter插件Loader服務會載入 Linux 或 AIX 的插件包以與SnapCenter伺服器互動。安裝適用於 Linux 的SnapCenter插件包或適用於 AIX 的SnapCenter插件包時，也會安

裝SnapCenter插件載入Loader服務。

關於此任務

安裝適用於 Linux 的SnapCenter插件包或適用於 AIX 的SnapCenter插件包後， SnapCenter插件Loader服務將自動啟動。如果SnapCenter插件Loader服務無法自動啟動，您應該：

- 確保插件運行的目錄沒有被刪除
- 增加分配給 Java 虛擬機器的記憶體空間

spl.properties 檔案位於 `/custom_location/ NetApp/snapcenter/spl/etc/`，包含下列參數。這些參數被分配了預設值。

參數名稱	描述
日誌等級	顯示支援的日誌等級。 可能的值是 TRACE、DEBUG、INFO、WARN、ERROR 和 FATAL。
SPL_協定	顯示SnapCenter插件Loader程式支援的協定。 僅支援HTTPS協定。如果缺少預設值，您可以新增該值。
SNAPCENTER_SERVER_協議	顯示SnapCenter Server 支援的協定。 僅支援HTTPS協定。如果缺少預設值，您可以新增該值。
跳過JAVAHOME更新	預設情況下，SPL 服務會偵測 java 路徑並更新 JAVA_HOME 參數。 因此預設值設定為 FALSE。如果您想要停用預設行為並手動修復 java 路徑，可以將其設定為 TRUE。
SPL_KEYSTORE_PASS	顯示密鑰庫檔案的密碼。 僅當您變更密碼或建立新的金鑰庫檔案時才可以變更此值。
SPL_埠	顯示SnapCenter插件Loader服務正在執行的連接埠號碼。 如果缺少預設值，您可以新增該值。  安裝插件後您不應更改該值。
SNAPCENTER_SERVER_HOST	顯示SnapCenter伺服器的 IP 位址或主機名稱。

參數名稱	描述
SPL_KEYSTORE_PATH	顯示密鑰庫檔案的絕對路徑。
SNAPCENTER_SERVER_PORT	顯示SnapCenter伺服器正在執行的連接埠號碼。
日誌最大數量	顯示保留在 <code>/custom_location/snapcenter/spl/logs</code> 資料夾中的SnapCenter插件Loader日誌檔案的數量。 預設值設定為 5000。如果計數超過指定值，則保留最後 5000 個修改的檔案。從SnapCenter插件Loader服務啟動時起，每 24 小時自動檢查一次檔案數量。  如果手動刪除 <code>spl.properties</code> 文件，則要保留的文件數將設定為 9999。
JAVA_HOME	顯示用於啟動 SPL 服務的 JAVA_HOME 的絕對目錄路徑。 此路徑是在安裝期間和啟動 SPL 的過程中確定的。
日誌最大大小	顯示作業日誌檔案的最大大小。 一旦達到最大大小，日誌檔案就會被壓縮，並且日誌會被寫入該作業的新檔案中。
保留最近幾天的日誌	顯示日誌最多保留的天數。
啟用憑證驗證	當主機啟用 CA 憑證驗證時顯示 true。 您可以透過編輯 <code>spl.properties</code> 或使用SnapCenter GUI 或 cmdlet 來啟用或停用此參數。

如果這些參數中的任何一個沒有分配預設值或您想要分配或更改值，那麼您可以修改 `spl.properties` 檔案。您也可以驗證 `spl.properties` 檔案並編輯該檔案以解決與指派給參數的值相關的任何問題。修改 `spl.properties` 檔案後，您應該重新啟動SnapCenter插件Loader服務。

步驟

1. 根據需要執行以下操作之一：

◦ 啟動SnapCenter插件Loader服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl start`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ 停止SnapCenter插件Loader服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl stop`

- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



您可以將 `-force` 選項與 `stop` 命令結合使用來強制停止 SnapCenter 插件 Loader 服務。但是，在執行此操作之前應謹慎，因為它也會終止現有操作。

◦ 重新啟動 SnapCenter 插件 Loader 服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ 尋找 SnapCenter 插件 Loader 服務的狀態：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl status`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ 尋找 SnapCenter 插件 Loader 服務中的變更：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl change`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

在 Linux 主機上使用 SnapCenter 插件 Loader (SPL) 服務設定 CA 證書

您應該管理 SPL 金鑰庫及其憑證的密碼，配置 CA 證書，將根憑證或中間憑證配置到 SPL 信任庫，並使用 SnapCenter 插件 Loader 服務將 CA 簽章金鑰對配置到 SPL 信任庫以啟動已安裝的數位憑證。



SPL 使用位於「`/var/opt/snapcenter/spl/etc`」的檔案「`keystore.jks`」作為其信任庫和金鑰庫。

管理 **SPL** 金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從 SPL 屬性檔案中檢索 SPL 金鑰庫預設密碼。

它是與鍵“`SPL_KEYSTORE_PASS`”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks
```

- 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

對 spl.properties 檔案中的金鑰 SPL_KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



SPL 金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

將根憑證或中繼憑證設定到 **SPL** 信任庫

您應該將沒有私鑰的根憑證或中間憑證設定到 SPL 信任庫。

步驟

1. 導覽至包含 SPL 金鑰庫的資料夾：`/var/opt/snapcenter/spl/etc`。
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

． 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

． 將根憑證或中間憑證配置到 SPL 信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

將 **CA** 簽章金鑰對配置到 **SPL** 信任庫

您應該將 CA 簽署的金鑰對配置到 SPL 信任庫。

步驟

1. 導航至包含 SPL 金鑰庫 `/var/opt/snapcenter/spl/etc` 的資料夾。
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

． 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

- 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

- 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
- 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設 SPL 金鑰庫密碼是 spl.properties 檔案中金鑰 SPL_KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
```

- 如果CA憑證中的別名較長，且包含空格或特殊字元（"*"，"，"，"），請將別名修改為簡單名稱：

```
keytool -changealias -alias "<OriginalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
```

- 從位於 spl.properties 檔案中的金鑰庫配置別名。

根據鍵 SPL_CERTIFICATE_ALIAS 更新此值。

4. 將 CA 簽署金鑰對配置到 SPL 信任庫後重新啟動服務。

為 SPL 設定憑證撤銷清單 (CRL)

您應該為 SPL 配置 CRL

關於此任務

- SPL 將在預先配置的目錄中尋找 CRL 檔案。
- SPL 的 CRL 檔案的預設目錄是 `/var/opt/snapcenter/spl/etc/crl`。

步驟

1. 您可以根據鍵 SPL_CRL_PATH 修改和更新 spl.properties 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器和對應的插件主機中部署 CA 憑證。您應該為

插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

將資料從 SnapManager for Oracle 和 SnapManager for SAP 匯入到 SnapCenter

將資料從 SnapManager for Oracle 和 SnapManager for SAP 匯入 SnapCenter 可讓您繼續使用先前版本的資料。

您可以透過從命令列介面（Linux 主機 CLI）執行導入工具，將資料從 SnapManager for Oracle 和 SnapManager for SAP 匯入到 SnapCenter。

導入工具在 SnapCenter 中建立政策和資源組。SnapCenter 中建立的政策和資源群組與 SnapManager for Oracle 和 SnapManager for SAP 中的設定檔以及使用這些設定檔執行的操作相對應。SnapCenter 導入工具與 SnapManager for Oracle 和 SnapManager for SAP 儲存庫資料庫以及您要匯入的資料庫進行互動。

- 檢索所有設定檔、計劃以及使用設定檔執行的操作。
- 為每個唯一操作和附加到設定檔的每個計劃建立 SnapCenter 備份策略。
- 為每個目標資料庫建立一個資源組。

您可以透過執行位於 `/opt/NetApp/snapcenter/spl/bin` 的 `sc-migrate` 腳本來執行匯入工具。在要匯入的資料庫主機上安裝適用於 Linux 的 SnapCenter 外掛程式套件時，`sc-migrate` 腳本將會複製到 `/opt/NetApp/snapcenter/spl/bin`。



SnapCenter圖形使用者介面 (GUI) 不支援匯入資料。

SnapCenter不支援以 7 模式運作的Data ONTAP 。您可以使用 7-模式過渡工具將儲存在運行以 7-模式運行的Data ONTAP 的系統上的資料和配置遷移到ONTAP系統。

支援導入資料的配置

在將資料從SnapManager 3.4.x for Oracle 和SnapManager 3.4.x for SAP 匯入到SnapCenter之前，您應該了解SnapCenter Plug-in for Oracle Database 支援的配置。

SnapCenter插件支援的 Oracle Database 配置列在 "[NetApp互通性表工具](#)"。

匯入到SnapCenter 的內容

您可以匯入設定檔、計畫以及使用設定檔執行的操作。

從 SnapManager for Oracle 和 SnapManager for SAP	至 SnapCenter
沒有任何操作和時間表的配置文件	建立的策略預設備份類型為“線上”，備份範圍為“完整”。
具有一個或多個操作的配置文件	根據設定檔和使用該設定檔執行的操作的唯一組合來建立多個策略。 SnapCenter中建立的政策包含從設定檔和對應操作中檢索的存檔日誌修剪和保留詳細資訊。
具有 Oracle 復原管理器 (RMAN) 配置的設定文件	政策是在啟用「使用 Oracle Recovery Manager 進行目錄備份」選項的情況下建立的。 如果在SnapManager中使用了外部 RMAN 編目，則必須在SnapCenter中設定 RMAN 目錄設定。您可以選擇現有憑證或建立新憑證。 如果 RMAN 是透過SnapManager中的控制檔配置的，則無需在SnapCenter中設定 RMAN。
附於個人資料的時間表	僅為了時間表而創建一項政策。
資料庫	為每個匯入的資料庫建立一個資源組。 在 Real Application Clusters (RAC) 設定中，執行匯入工具的節點在匯入後將成為首選節點，並為該節點建立資源群組。



匯入設定檔時，會與備份策略一起建立驗證策略。

當SnapManager for Oracle 和SnapManager for SAP 設定檔、計畫以及使用設定檔執行的任何操作匯入

到SnapCenter時，不同的參數值也會被匯入。

SnapManager for Oracle 和SnapManager for SAP 參數和值	SnapCenter參數和值	筆記
備份範圍 • 滿的 • 數據 • 紀錄	備份範圍 • 滿的 • 數據 • 紀錄	
備份模式 • 汽車 • 在線的 • 離線	備份類型 • 在線的 • 離線關機	如果備份模式為自動，則匯入工具會在執行操作時檢查資料庫狀態，並適當地將備份類型設定為線上或離線關閉。
保留 • 天 • 計數	保留 • 天 • 計數	SnapManager for Oracle 和SnapManager for SAP 使用天數和計數來設定保留。 在SnapCenter中，有天數或數數。因此，保留是根據天數設定的，因為在SnapManager for Oracle 和SnapManager for SAP 中，天數優先於計數。
修剪時間表 • 全部 • 系統變更號碼 (SCN) • 日期 • 在指定小時、天、週和月之前建立的日誌	修剪時間表 • 全部 • 在指定小時和日期之前建立的日誌	SnapCenter不支援基於 SCN、日期、週和月的修剪。
通知 • 僅對成功操作發送電子郵件 • 僅針對失敗的操作發送電子郵件 • 操作成功和失敗時均發送電子郵件	通知 • 總是 • 失敗時 • 警告 • 錯誤	電子郵件通知已匯入。 但是，您必須使用SnapCenter GUI 手動更新 SMTP 伺服器。電子郵件的主題留空，供您設定。

哪些內容未匯入SnapCenter

導入工具不會將所有內容匯入到SnapCenter。

您無法將以下內容匯入SnapCenter：

- 備份元數據
- 部分備份
- 原始設備映射 (RDM) 和虛擬儲存控制台 (VSC) 相關備份
- SnapManager for Oracle 和SnapManager for SAP 儲存庫中可用的角色或任何憑證
- 與驗證、恢復和克隆操作相關的數據
- 修剪操作
- SnapManager for Oracle 和SnapManager for SAP 設定檔中指定的複製詳細資訊

匯入後，您必須手動編輯在SnapCenter中建立的相應原則以包含複製詳細資訊。

- 已編目的備份訊息

準備導入數據

在將資料匯入SnapCenter之前，您必須執行某些任務才能成功執行匯入操作。

步驟

1. 確定要匯入的資料庫。
2. 使用SnapCenter新增資料庫主機並安裝適用於 Linux 的SnapCenter插件包。
3. 使用SnapCenter設定主機上資料庫使用的儲存虛擬機器 (SVM) 的連線。
4. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
5. 在資源頁面中，確保要匯入的資料庫已被發現並顯示。

當您想要運行導入工具時，資料庫必須可訪問，否則資源組創建將失敗。

如果資料庫已配置憑證，則必須在SnapCenter中建立對應的憑證，將憑證指派給資料庫，然後重新執行資料庫的發現。如果資料庫駐留在自動儲存管理 (ASM) 上，則必須為 ASM 實例建立憑證，並將該憑證指派給資料庫。

6. 確保執行導入工具的使用者俱有足夠的權限從SnapManager for Oracle 或SnapManager for SAP 主機執行SnapManager for Oracle 或SnapManager for SAP CLI 命令（例如暫停計劃的命令）。
7. 在SnapManager for Oracle 或SnapManager for SAP 主機上執行以下命令以暫停計劃：

- a. 如果要暫停SnapManager for Oracle 主機上的計劃，請執行：

- `smo credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smo profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smo credential set -profile -name profile_name`



您必須對主機上的每個設定檔執行 `smo credential set` 命令。

b. 如果要暫停 SnapManager for SAP 主機上的計劃，請執行：

- `smoap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
- `smoap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
- `smoap credential set -profile -name profile_name`



您必須為主機上的每個設定檔執行 `smoap credential set` 指令。

8. 確保在執行 `hostname -f` 時顯示資料庫主機的完全限定網域名稱 (FQDN)。

如果沒有顯示 FQDN，則必須修改 `/etc/hosts` 以指定主機的 FQDN。

導入數據

您可以從資料庫主機執行導入工具來匯入資料。

關於此任務

匯入後建立的 SnapCenter 備份策略具有不同的命名格式：

- 為沒有任何操作和計劃的設定檔建立的策略具有 `SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED` 格式。
- 當未使用設定檔執行任何操作時，將建立相應的策略，其預設備份類型為在線，備份範圍為完整。
- 為具有一個或多個操作的設定檔建立的策略具有 `SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` 格式。
- 為附加到設定檔的計劃所建立的策略具有 `SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED` 格式。

步驟

1. 登入要匯入的資料庫主機。
2. 透過執行位於 `/opt/NetApp/snapcenter/spl/bin` 的 `sc-migrate` 腳本來執行導入工具。
3. 輸入 SnapCenter 伺服器使用者名稱和密碼。

驗證憑證後，將與 SnapCenter 建立連線。

4. 輸入 SnapManager for Oracle 或 SnapManager for SAP 儲存庫資料庫詳細資訊。

儲存庫資料庫列出了主機上可用的資料庫。

5. 輸入目標資料庫詳細資訊。

如果要匯入主機上的所有資料庫，則輸入all。

6. 如果您想要產生系統日誌或傳送失敗操作的 ASUP 訊息，則必須透過執行 *Add-SmStorageConnection* 或 *Set-SmStorageConnection* 命令來啟用它們。



如果要取消匯入操作（無論是在執行匯入工具時還是匯入後），都必須手動刪除作為匯入作業的一部分所建立的SnapCenter原則、憑證和資源群組。

結果

SnapCenter備份策略是針對設定檔、計劃以及使用設定檔執行的操作所建立的。也為每個目標資料庫建立資源組。

成功匯入資料後，與匯入的資料庫關聯的計畫將在SnapManager for Oracle 和SnapManager for SAP 中暫停。



匯入後，您必須使用SnapCenter管理匯入的資料庫或檔案系統。

每次執行匯入工具的日誌都會儲存在 */var/opt/snapcenter/spl/logs* 目錄中，名稱為 *spl_migration_timestamp.log*。您可以參考此日誌來查看匯入錯誤並進行故障排除。

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 */opt/netapp/config/crl*。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

準備保護 Oracle 資料庫

在執行任何資料保護操作（例如備份、複製或復原作業）之前，您必須定義策略並設定環境。您也可以設定SnapCenter伺服器以使用SnapMirror和SnapVault技術。

若要利用SnapVault和SnapMirror技術，您必須在儲存裝置上設定並初始化來源磁碟區和目標磁碟區之間的資料保護關係。您可以使用 NetAppSystem Manager 或儲存控制台命令列來執行這些任務。

在使用 Oracle 資料庫插件之前，SnapCenter管理員應安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。["了解更多"](#)
- 透過新增儲存系統連接來配置SnapCenter環境。["了解更多"](#)



SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。使用 SVM 註冊或叢集註冊向SnapCenter註冊的每個 SVM 都必須是唯一的。

- 為安裝使用者建立驗證模式為 Linux 或 AIX 的憑證。["了解更多"](#)
- 新增主機、安裝插件、發現資源。
- 如果您使用SnapCenter Server 保護駐留在 VMware RDM LUN 或 VMDK 上的 Oracle 資料庫，則必須部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊外掛程式。
- 在您的 Linux 或 AIX 主機上安裝 Java。

看["Linux 主機需求"](#)或者["AIX 主機需求"](#)了解更多。

- 您應該將應用程式防火牆的逾時值設為3小時或更長。
- 如果您在 NFS 環境中有 Oracle 資料庫，則必須為主儲存或輔助儲存配置至少一個 NFS 資料 LIF 來執行掛載、複製、驗證和還原作業。
- 如果您有多個資料路徑 (LIF) 或 dNFS 配置，則可以使用資料庫主機上的SnapCenter CLI 執行下列操作：
 - 預設情況下，資料庫主機的所有 IP 位址都會新增至複製磁碟區的儲存虛擬機器 (SVM) 中的 NFS 儲存匯出原則。如果您想要特定的 IP 位址或限制為 IP 位址的子集，請執行 Set-PreferredHostIPsInStorageExportPolicy CLI。
 - 如果 SVM 中有多個資料路徑 (LIF)，SnapCenter會選擇適當的資料路徑 (LIF) 來掛載 NFS 複製磁碟區。但是，如果要指定特定的資料路徑 (LIF)，則必須執行 Set-SvmPreferredDataPath CLI。命令參考指南有更多資訊。
- 如果您在 SAN 環境中有 Oracle 資料庫，請確保依照下列指南中所提及的建議設定 SAN 環境：
 - ["使用具有ONTAP儲存的 Linux 主機"](#)
 - ["受 AIX 主機實用程式影響的主機設置"](#)
- 如果您在 Oracle Linux 或 RHEL 作業系統中的 LVM 上有 Oracle 資料庫，請安裝最新版本的邏輯磁碟區管理 (LVM)。
- 如果您正在使用SnapManager for Oracle 並希望遷移到SnapCenter Plug-in for Oracle Database，則可以使用 sccli 命令 sc-migrate 將設定檔遷移到SnapCenter的政策和資源群組。
- 如果您需要備份複製，請在ONTAP上設定SnapMirror和SnapVault

對於SnapCenter 4.1.1 用戶，SnapCenter Plug-in for VMware vSphere包含有關保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.2.x 用戶，NetApp Data Broker 1.0 和 1.0.1 文件包含有關使用基於 Linux 的NetApp Data Broker 虛擬設備（開放虛擬設備格式）提供的適用SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.3.x 用戶，SnapCenter Plug-in for VMware vSphere文件包含有關使用基於 Linux 的SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。

查找更多資訊

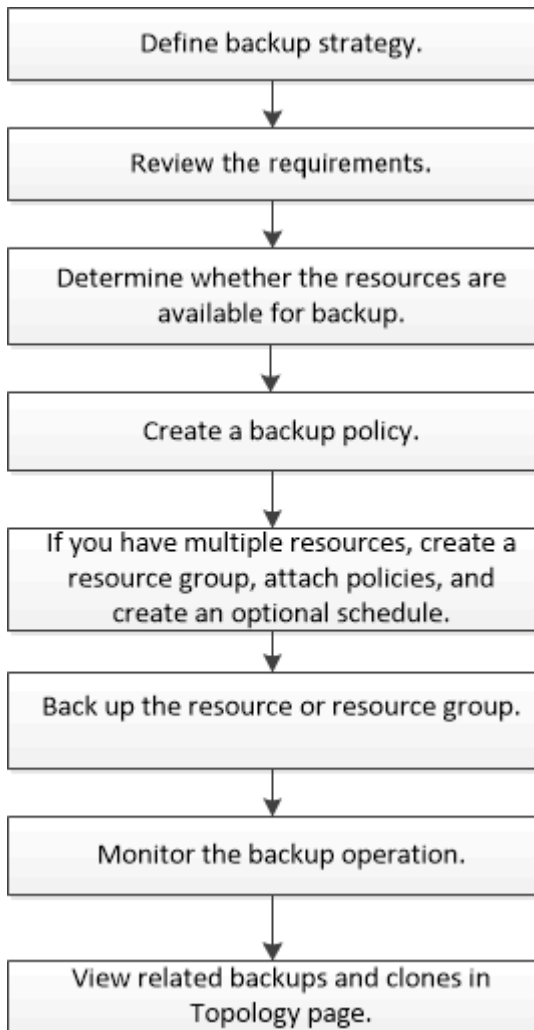
- ["互通性矩陣工具"](#)
- ["SnapCenter Plug-in for VMware vSphere文檔"](#)
- ["在 RHEL 7 及更高版本中的非多路徑環境中，資料保護操作失敗"](#)

備份 Oracle 資料庫

備份過程概述

您可以建立資源（資料庫）或資源組的備份。備份過程包括規劃、確定備份資源、建立備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



在為 Oracle 資料庫建立備份時，會在 Oracle 資料庫主機的 `/var/opt/snapcenter/sco/lock` 目錄中建立一個操作鎖定檔案 (`.sm_lock_dbsid`)，以避免在資料庫上執行多個操作。資料庫備份完成後，操作鎖定檔案將自動刪除。

但是，如果上一次備份完成時出現警告，則操作鎖定檔案可能不會被刪除，並且下一個備份作業將進入等待佇列。如果不刪除 `.sm_lock_dbsid` 文件，它最終可能會被取消。在這種情況下，您必須透過執行下列步驟手動刪除操作鎖定檔案：

1. 從命令提示字元處，導覽至 `/var/opt/snapcenter/sco/lock`。
2. 刪除操作鎖：`rm -rf .sm_lock_dbsid`。

備份配置訊息

支援的 **Oracle** 資料庫備份配置

SnapCenter支援不同 Oracle 資料庫配置的備份。

- Oracle 獨立版
- Oracle 真正應用叢集 (RAC)
- Oracle 獨立舊版
- Oracle 獨立容器資料庫 (CDB)
- Oracle Data Guard 備用

您只能建立 Data Guard 備用資料庫的離線安裝備份。不支援離線關閉備份、僅存檔日誌備份和完整備份。

- Oracle Active Data Guard 備用

您只能建立 Active Data Guard 備用資料庫的線上備份。不支援僅存檔日誌備份和完整備份。

在建立 Data Guard 備用資料庫或 Active Data Guard 備用資料庫的備份之前，託管復原程序 (MRP) 將停止，一旦建立備份，MRP 就會啟動。

- 自動儲存管理 (ASM)
 - 虛擬機器磁碟 (VMDK) 上的 ASM 獨立和 ASM RAC

在 Oracle 資料庫支援的所有還原方法中，您只能在 VMDK 上執行 ASM RAC 資料庫的連線和複製還原。

- ASM 獨立版和原始設備映射 (RDM) 上的 ASM RAC + 您可以在 ASM 上對 Oracle 資料庫執行備份、復原和複製操作，無論是否使用 ASMLib。
- Oracle ASM 過濾驅動程式 (ASMFD)

不支援 PDB 遷移和 PDB 克隆操作。

- Oracle Flex ASM

有關支援的 Oracle 版本的最新信息，請參閱 ["NetApp互通性表工具"](#)。

Oracle 資料庫支援的備份類型

備份類型指定您要建立的備份類型。SnapCenter支援 Oracle 資料庫的線上和離線備份類型。

線上備份

當資料庫處於線上狀態時所建立的備份稱為線上備份。線上備份也稱為熱備份，它使您無需關閉資料庫即可建立資料庫的備份。

作為線上備份的一部分，您可以建立以下文件的備份：

- 僅限資料檔案和控制文件
- 僅存檔日誌檔案（在這種情況下資料庫不會進入備份模式）
- 包含資料檔案、控制檔案和存檔日誌檔案的完整資料庫

離線備份

當資料庫處於安裝或關閉狀態時所建立的備份稱為離線備份。離線備份也稱為冷備份。離線備份中只能包含資料檔案和控制檔。您可以建立離線安裝或離線關機備份。

- 建立離線掛載備份時，必須確保資料庫處於掛載狀態。

如果資料庫處於任何其他狀態，則備份操作會失敗。

- 建立離線關閉備份時，資料庫可以處於任何狀態。

資料庫狀態變更為建立備份所需的狀態。建立備份後，資料庫狀態將恢復到原始狀態。

SnapCenter如何發現 Oracle 資料庫

資源是主機上由SnapCenter維護的 Oracle 資料庫。發現可用的資料庫後，您可以將這些資料庫新增至資源組以執行資料保護操作。

以下部分介紹了SnapCenter用於發現不同類型和版本的 Oracle 資料庫的過程。

對於 **Oracle** 版本 **11g** 至 **12cR1**

RAC 資料庫

RAC 資料庫僅根據 `/etc/oratab` 條目來發現。您應該在 `/etc/oratab` 檔案中擁有資料庫條目。

獨立

僅根據 `/etc/oratab` 條目才能發現獨立資料庫。

自動化管理

ASM 實例條目應該在 `/etc/oratab` 檔案中可用。

RAC 單節點

RAC One Node 資料庫僅根據 `/etc/oratab` 條目來發現。資料庫應處於 `nomount`、`mount` 或 `open` 狀態。您應該在 `/etc/oratab` 檔案中擁有資料庫條目。

如果資料庫已被發現且備份與資料庫相關聯，則 RAC One Node 資料庫狀態將被標記為重新命名或刪除。

如果資料庫被重新定位，則應執行下列步驟：

1. 在故障轉移 RAC 節點上的 `/etc/oratab` 檔案中手動新增重定位的資料庫項目。
2. 手動刷新資源。
3. 從資源頁面中選擇 RAC One Node 資料庫，然後按一下資料庫設定。
4. 配置資料庫以將首選叢集節點設定為目前託管資料庫的 RAC 節點。

5. 執行SnapCenter操作。
6. 如果您已將資料庫從一個節點重新定位到另一個節點，且先前節點中的 `oratab` 條目未被刪除，請手動刪除 `oratab` 條目以避免同一個資料庫顯示兩次。

適用於 **Oracle 版本 12cR2 至 18c、19c 或 21c**

RAC 資料庫

使用 `srvctl config` 指令發現 RAC 資料庫。您應該在 `/etc/oratab` 檔案中擁有資料庫條目。

獨立

獨立資料庫是根據 `/etc/oratab` 檔案中的條目和 `srvctl config` 命令的輸出發現的。

自動化管理

ASM 實例條目不需要位於 `/etc/oratab` 檔案中。

RAC 單節點

僅使用 `srvctl config` 指令即可發現 RAC One Node 資料庫。資料庫應處於 `nomount`、`mount` 或 `open` 狀態。如果資料庫已被發現且備份與資料庫相關聯，則 RAC One Node 資料庫狀態將被標記為重新命名或刪除。

如果資料庫被重新定位，您應該執行以下步驟：
。手動刷新資源。
。從資源頁面中選擇 RAC One Node 資料庫，然後按一下資料庫設定。
。配置資料庫以將首選叢集節點設定為目前託管資料庫的 RAC 節點。
。執行SnapCenter操作。



如果 `/etc/oratab` 檔案中有任何 Oracle 12cR2 和 18c 資料庫條目，並且使用 `srvctl config` 指令註冊了相同的資料庫，則SnapCenter將消除重複的資料庫條目。如果存在過時的資料庫條目，則會發現該資料庫，但該資料庫將無法存取且狀態將為離線。

RAC 設定中的首選節點

在 Oracle Real Application Clusters (RAC) 設定中，您可以指定SnapCenter用於執行備份作業的首選節點。如果您未指定首選節點，SnapCenter會自動指派節點作為首選節點，並在該節點上建立備份。

首選節點可能是 RAC 資料庫執行個體所在的叢集節點之一或所有叢集節點。備份操作僅在這些優先節點上按照優先順序觸發。

例子

RAC 資料庫 `cdbrac` 有三個實例：節點 1 上的 `cdbrac1`、節點 2 上的 `cdbrac2` 和節點 3 上的 `cdbrac3`。

`node1` 和 `node2` 實例被配置為首選節點，其中 `node2` 為第一首選，`node1` 為第二首選。執行備份作業時，首先在 `node2` 上嘗試執行該操作，因為它是第一個首選節點。

如果 `node2` 未處於備份狀態，這可能是由於多種原因造成的，例如插件代理未在主機上執行、主機上的資料庫執行個體未處於指定備份類型所需的狀態，或 FlexASM 配置中 `node2` 上的資料庫執行個體未由本機 ASM 執行個體提供服務；然後將在 `node1` 上嘗試執行該操作。

由於 `node3` 不在首選節點清單中，因此不會用於備份。

Flex ASM 設定

在 Flex ASM 設定中，如果基數小於 RAC 叢集中的節點數，則葉節點將不會被列為首選節點。如果 Flex ASM 叢集節點角色有任何變化，您應該手動發現以便刷新首選節點。

所需的資料庫狀態

首選節點上的 RAC 資料庫執行個體必須處於所需狀態才能成功完成備份：

- 配置的首選節點中的一個 RAC 資料庫執行個體必須處於開啟狀態才能建立線上備份。
- 配置的首選節點中的一個 RAC 資料庫執行個體必須處於掛載狀態，且所有其他執行個體（包括其他首選節點）必須處於掛載狀態或更低狀態才能建立離線掛載備份。
- RAC 資料庫實例可以處於任何狀態，但必須指定首選節點來建立離線關閉備份。

如何使用 Oracle Recovery Manager 對備份進行編目

您可以使用 Oracle Recovery Manager (RMAN) 對 Oracle 資料庫的備份進行分類，以將備份資訊儲存在 Oracle RMAN 儲存庫中。

編目備份稍後可用於區塊級復原或表空間時間點復原作業。當您不需要這些編目備份時，您可以刪除目錄資訊。

資料庫必須處於已安裝或更高狀態才能進行編目。您可以對資料備份、存檔日誌備份和完整備份執行編目。如果對具有多個資料庫的資源組的備份啟用了編目，則會對每個資料庫執行編目。對於 Oracle RAC 資料庫，將在資料庫至少處於安裝狀態的首選節點上執行編目。

如果要對 RAC 資料庫的備份進行編目，請確保沒有針對該資料庫執行其他作業。如果另一個作業正在運行，則編目操作將失敗而不是排隊。

外部目錄資料庫

預設情況下，使用目標資料庫控制檔進行編目。如果要新增外部目錄資料庫，可以使用 SnapCenter 圖形使用者介面 (GUI) 中的資料庫設定精靈指定外部目錄的憑證和透明網路底層 (TNS) 名稱來設定它。您也可以透過執行帶有 `-OracleRmanCatalogCredentialName` 和 `-OracleRmanCatalogTnsName` 選項的 `Configure-SmOracleDatabase` 命令從 CLI 配置外部目錄資料庫。

RMAN 命令

如果在從 SnapCenter GUI 建立 Oracle 備份原則時啟用了編目選項，則備份將使用 Oracle RMAN 作為備份作業的一部分進行編目。您也可以透過運行 ``Catalog-SmBackupWithOracleRMAN`` 命令。

對備份進行編目後，您可以運行 ``Get-SmBackupDetails`` 命令取得編目備份訊息，例如編目資料檔案的標籤、控制檔案編目路徑和編目存檔日誌位置。

命名格式

如果 ASM 磁碟組名稱大於或等於 16 個字符，從 SnapCenter 3.0 開始，備份使用的命名格式為 `SC_HASHCODEofDISKGROUP_DBSID_BACKUPID`。但是，如果磁碟組名稱少於 16 個字符，則備份使用的命名格式為 `DISKGROUPNAME_DBSID_BACKUPID`，這與 SnapCenter 2.0 中使用的格式相同。

`HASHCODEofDISKGROUP` 是自動產生的每個 ASM 磁碟組獨有的數字（2 到 10 位數）。

交叉檢查操作

您可以執行交叉檢查來更新有關儲存庫記錄與其物理狀態不符的備份的過時 RMAN 儲存庫資訊。例如，如果使用者使用作業系統指令從磁碟中刪除存檔日誌，則控制檔案仍指示日誌在磁碟上，但實際上並不在。

交叉檢查操作可讓您使用資訊更新控制檔。您可以透過執行 `Set-SmConfigSettings` 指令並將值 `TRUE` 指派給 `ENABLE_CROSSCHECK` 參數來啟用交叉檢查。預設值設定為 `FALSE`。

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings  
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

刪除目錄訊息

您可以透過執行 `Uncatalog-SmBackupWithOracleRMAN` 指令來刪除目錄資訊。您無法使用 SnapCenter GUI 刪除目錄資訊。但是，在刪除備份或刪除與該編目備份相關的保留和資源群組時，編目備份的資訊將會被刪除。



當您強制刪除 SnapCenter 主機時，與該主機關聯的編目備份的資訊不會被刪除。在強制刪除主機之前，您必須刪除該主機的所有編目備份的資訊。

如果由於操作時間超出了 `ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT` 參數指定的逾時值而導致編目和取消編目失敗，則應透過執行下列命令來修改該參數的值：

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType  
Plugin -PluginCode SCO-ConfigSettings  
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

修改參數值後，透過執行以下命令重新啟動 SnapCenter 插件 Loader (SPL) 服務：

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您可以參考 ["SnapCenter 軟體命令參考指南"](#)。

用於備份特定處方和後記的預定義環境變量

SnapCenter 可讓您在建立備份原則時執行前腳本和後腳本時使用預先定義的環境變數。除 VMDK 之外的所有 Oracle 配置都支援此功能。

SnapCenter 預先定義了可在執行 shell 腳本的環境中直接存取的參數值。執行腳本時，您不必手動指定這些參數的值。

支援建立備份策略的預定義環境變數

- **SC_JOB_ID** 指定操作的作業 ID。

例如：256

- **SC_ORACLE_SID** 指定資料庫的系統識別碼。

如果操作涉及多個資料庫，則參數將包含以管道分隔的資料庫名稱。

此參數將填入應用程式磁碟區。

例如：NFSB32|NFSB31

- **SC_HOST** 指定資料庫的主機名稱。

對於 RAC，主機名稱將是執行備份的主機的名稱。

此參數將填入應用程式磁碟區。

範例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** 指定資料庫的作業系統擁有者。

資料將會格式化為 <db1>@<osuser1>|<db2>@<osuser2>。

範例：NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** 指定資料庫的作業系統群組。

資料將被格式化為 <db1>@<osgroup1>|<db2>@<osgroup2>。

範例：NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE** 指定備份類型（線上完整備份、線上資料備份、線上日誌備份、離線關機備份、離線掛載備份）

例子：

- 對於完整備份：ONLINEFULL
- 僅資料備份：ONLINEDATA
- 對於僅日誌備份：ONLINELOG

- **SC_BACKUP_NAME** 指定備份的名稱。

此參數將填入應用程式磁碟區。

範例：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1|AV@RG2_scspr2417819002_07-20-2021_12.16.48.9267

- **SC_BACKUP_ID** 指定備份 ID。

此參數將填入應用程式磁碟區。

範例：DATA@203|LOG@205|AV@207

- **SC_ORACLE_HOME** 指定 Oracle 主目錄的路徑。

範例：NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_RETENTION** 指定政策中定義的保留期。

例子：

- 對於完整備份：每小時|DATA@DAYS:3|LOG@COUNT:4
- 對於按需資料備份：Ondemand|DATA@COUNT:2
- 對於僅按需日誌備份：Ondemand|LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** 指定資源組的名稱。

例如：RG1

- **SC_BACKUP_POLICY_NAME** 指定備份策略的名稱。

範例：backup_policy

- **SC_AV_NAME** 指定應用程式磁碟區的名稱。

範例：AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** 指定 SVM 到資料檔案目錄磁碟區的儲存對應。它將是 lun 和 qtree 的父卷的名稱。

資料格式為 <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>。

例子：

- 對於同一資源組中的 2 個資料庫
：NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA
- 對於資料檔案分佈在多個磁碟區上的單一資料庫
：buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS

- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** 指定 SVM 到日誌檔案目錄磁碟區的儲存對映。它將是 lun 和 qtree 的父卷的名稱。

例子：

- 對於單一資料庫實例：buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
- 對於多個資料庫實例
：NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO

- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** 指定包含儲存系統名稱和磁碟區名稱的快照清單。

例子：

- 對於單一資料庫實例
：buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3
973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 對於多個資料庫實例
：NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-

2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-
2021_02.28.26.39
73_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-
2021_02.28.26.3973_1

- **SC_PRIMARY_SNAPSHOT_NAMES** 指定備份期間建立的主快照的名稱。

例子：

- 對於單一資料庫實例：RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- 對於多個資料庫實例：NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.
- 對於涉及 2 個磁碟區的一致性群組快照：cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_5838

- **SC_PRIMARY_MOUNT_POINTS** 指定作為備份一部分的掛載點詳細資料。

詳細資訊包括磁碟區的安裝目錄，而不是備份檔案的直接父目錄。對於 ASM 配置，它是磁碟組的名稱。

資料將被格式化為 <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>。

例子：

- 對於單一資料庫實例：/mnt/nfsdb3_data、/mnt/nfsdb3_log、/mnt/nfsdb3_data1
- 對於多個資料庫實例：NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
- 對於 ASM：+DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** 指定在每個掛載點備份期間所建立的快照的名稱。

例子：

- 對於單一資料庫實例：RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_scspr2417819002_07-21-2021_scspr2417819002_07-21-2021_02123135130000100021-20210021-202102109830021-202102109830021-2021021-2021021.
- 對於多個資料庫實例：NFSB32@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb32_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb31_log|NFSB31@RG2_scspr2417819002_07-21-2021_02.28.26.3973_0:/mnt/nfsb31_data,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1:/mnt/nfsb32_log

- **SC_ARCHIVELOGS_LOCATIONS** 指定存檔日誌目錄的位置。

目錄名稱將是存檔日誌檔案的直接父級。如果存檔日誌放置在多個位置，那麼所有位置都會被捕獲。這也包括 FRA 場景。如果目錄使用軟鏈接，則將填充相同的內容。

例子：

- 對於 NFS 上的單一資料庫：/mnt/nfsdb2_log
- 對於 NFS 上的多個資料庫以及放置在兩個不同位置的 NFSB31 資料庫存檔日誌：
NFSB31@/mnt/nfsdb31_log1、/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
- 對於 ASM：+LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15

• **SC_REDO_LOGS_LOCATIONS** 指定重做日誌目錄的位置。

目錄名稱將是重做日誌檔案的直接父級。如果目錄使用軟鏈接，則將填充相同的內容。

例子：

- 對於 NFS 上的單一資料庫：/mnt/nfsdb2_data/newdb1
- 對於 NFS 上的多個資料庫：
NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
- 對於 ASM：+LOG2DG/ASMDB2/ONLINELOG

• **SC_CONTROL_FILES_LOCATIONS** 指定控制檔目錄的位置。

目錄名稱將是控制檔案的直接父級。如果目錄使用軟鏈接，則將填充相同的內容。

例子：

- 對於 NFS 上的單一資料庫：/mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
- 對於 NFS 上的多個資料庫：
NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/fra/newdb32,/mnt/nfsdb32_data/new32_data/fra/newdb32,/mnt/nfsdb32_data/new32
- 對於 ASM：+LOG2DG/ASMDB2/CONTROLFILE

• **SC_DATA_FILES_LOCATIONS** 指定資料檔案目錄的位置。

目錄名稱將是資料檔案的直接父級。如果目錄使用軟鏈接，則將填充相同的內容。

例子：

- 對於 NFS 上的單一資料庫：/mnt/nfsdb3_data1、/mnt/nfsdb3_data/NEWDB3/datafile
- 對於 NFS 上的多個資料庫：
NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
- 對於 ASM：+DATA2DG/ASMDB2/DATAFILE、+DATA2DG/ASMDB2/TEMPFILE

• **SC_SNAPSHOT_LABEL** 指定二級標籤的名稱。

範例：每小時、每天、每週、每月或自訂標籤。

支援的分隔符

- : 用來分隔 SVM 名稱和磁碟區名稱

範例：buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_

0,buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- @ 用於將資料與其資料庫名稱分開，並將值與其鍵分開。

例子：

- NFSB32 @ buck : /vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0 , buck
: /vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
- NFSB31@oracle|NFSB32@oracle
- | 用於分隔兩個不同資料庫之間的數據，以及分隔 SC_BACKUP_ID、SC_BACKUP_RETENTION 和 SC_BACKUP_NAME 參數的兩個不同實體之間的資料。

例子：

- 資料@203|日誌@205
- 每小時|資料@天數:3|日誌@計數:4
- 資料@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|日誌@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
- / 用於將磁碟區名稱與 SC_PRIMARY_SNAPSHOT_NAMES 和 SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG 參數的快照分開。

範例：NFSB32 @ buck : /vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0 , buck
: /vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

- , 用來分隔相同 DB 的變數集。

範例：NFSB32 @ buck : /vol/scspr2417819002_NFS_CDB_NFSB32_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0 , buck
: /vol/scspr2417819002_NFS_CDB_NFSB32_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA/RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO/RG2_scspr2417819002_07-21-2021_02.28.26.3973_1

備份保留選項

您可以選擇保留備份副本的天數，或指定要保留的備份副本數量，ONTAP最多可保留 255 份。例如，您的組織可能要求您保留 10 天的備份副本或 130 份備份副本。

建立策略時，您可以指定備份類型和計畫類型的保留選項。

如果您設定了SnapMirror複製，則保留政策將在目標磁碟區上鏡像。

SnapCenter會刪除具有與計劃類型相符的保留標籤的保留備份。如果資源或資源群組的計劃類型發生更改，則具有舊計劃類型標籤的備份可能仍保留在系統中。



為了長期保留備份副本，您應該使用SnapVault備份。

備份計劃

備份頻率（計畫類型）在策略中指定；備份計畫在資源組配置中指定。確定備份頻率或計劃的最關鍵因素是資源的變化率和資料的重要性。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA 和 RPO 有助於資料保護策略。

即使是使用頻繁的資源，也不需要每天執行一次或兩次以上的完整備份。例如，定期的交易日誌備份可能足以確保您擁有所需的備份。備份資料庫的頻率越高，SnapCenter在復原時需要使用的交易日誌就越少，因此可以加快復原作業的速度。

備份計畫分為兩部分，如下所示：

- 備份頻率

備份頻率（執行備份的頻率），對於某些外掛程式來說稱為計畫類型，是策略配置的一部分。您可以選擇每小時、每天、每週或每月作為策略的備份頻率。如果您未選擇任何頻率，則建立的策略是僅按需策略。您可以透過點選「設定」>「策略」來存取策略。

- 備份計畫

備份計畫（確切地指定執行備份的時間）是資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份。您可以透過點選「資源」>「資源群組」來存取資源組計畫。

備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

```
resourcegroupname_hostname_timestamp
```

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- `dts1` 是資源組名稱。
- `mach1x88` 是主機名稱。
- `03-12-2015_23.17.26` 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳後綴會加入到快照名稱中。

備份 Oracle 資料庫的要求

在備份 Oracle 資料庫之前，您應該確保先決條件已滿足。

- 您必須已建立附加有策略的資源群組。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「`snapmirror all`」權限。但是，如果您使用“`vsadmin`”角色，則不需要“`snapmirror all`”權限。
- 您必須已將備份作業正在使用的聚合指派給資料庫使用的儲存虛擬機器 (SVM)。
- 如果為該資料庫啟用了二級保護，您應該已經驗證了屬於該資料庫的所有資料磁碟區和存檔日誌磁碟區都受到保護。
- 您應該已經驗證了 ASM 磁碟組上有檔案的資料庫應該處於「MOUNT」或「OPEN」狀態，以便使用 Oracle DBVERIFY 公用程式驗證其備份。
- 您應該已經驗證卷裝入點長度不超過 240 個字元。
- 如果要備份的資料庫很大（以 TB 為單位），則應將 SnapCenter Server 主機中的 `C:\Program Files\NetApp\SMCore\SMCoreServiceHost.exe.config` 檔案中的 `RESTTimeout` 值增加到 86400000 毫秒。

修改值時，請確保沒有正在執行的作業，並在增加值後重新啟動 SnapCenter SMCore 服務。

發現可供備份的 Oracle 資料庫

資源是主機上由 SnapCenter 管理的 Oracle 資料庫。發現可用的資料庫後，您可以將這些資料庫新增至資源組以執行資料保護操作。

開始之前

- 您必須完成安裝 SnapCenter 伺服器、新增主機、建立儲存系統連線和新增憑證等任務。
- 如果資料庫駐留在虛擬機器磁碟 (VMDK) 或原始裝置對映 (RDM) 上，則必須部署 SnapCenter Plug-in for VMware vSphere 並向 SnapCenter 註冊外掛程式。

有關更多信息，請參閱 ["SnapCenter Plug-in for VMware vSphere"](#)。

- 如果資料庫駐留在 VMDK 檔案系統上，則必須登入 vCenter 並導覽至 **VM** 選項 > 進階 > 編輯設定，將 VM 的 `disk.enableUUID` 值設為 `true`。
- 您必須已經查看了 SnapCenter 遵循的流程來發現不同類型和版本的 Oracle 資料庫。

步驟 1：防止 SnapCenter 發現非資料庫條目

您可以阻止 SnapCenter 發現 `oratab` 檔案中新增的非資料庫條目。

步驟

1. 安裝 Oracle 外掛後，root 使用者應在目錄 `/var/opt/snapcenter/sco/etc/` 下建立 **sc_oratab.config** 檔案。
授予 Oracle 二進位檔案擁有者和群組寫入權限，以便將來可以維護該檔案。
2. 資料庫管理員應在 **sc_oratab.config** 檔案中新增非資料庫條目。

建議維護 `/etc/oratab` 檔案中非資料庫條目定義的相同格式，或者使用者可以只新增非資料庫實體字串。



該字串區分大小寫。任何以 # 開頭的文字都被視為註釋。註釋可以附加在非資料庫名稱後面。

```
For example:
-----
# Sample entries
# Each line can have only one non-database name
# These are non-database name
oratar # Added by the admin group -1
#Added by the script team
NEWSPT
DBAGNT:/ora01/app/oracle/product/agent:N
-----
```

3. 發現資源。

sc_oratab.config 中新增的非資料庫項目將不會在資源頁面中列出。



始終建議在升級SnapCenter插件之前備份 **sc_oratab.config** 檔案。

第 2 步：發現資源

安裝外掛程式後，該主機上的所有資料庫都會自動發現並顯示在資源頁面中。

資料庫至少應處於已安裝狀態或更高狀態，才能成功發現資料庫。在 Oracle 真正應用叢集 (RAC) 環境中，執行發現的主機中的 RAC 資料庫執行個體應至少處於已安裝狀態或更高狀態，資料庫執行個體的發現才能成功。只有成功發現的資料庫才能加入資源組。

如果您刪除了主機上的 Oracle 資料庫，SnapCenter Server 將不會意識到並會列出已刪除的資料庫。您應該手動刷新資源以更新SnapCenter資源清單。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。

點選按一下[過濾圖示]，然後選擇主機名稱和資料庫類型來過濾資源。然後，您可以按一下[過濾圖示]_icon.png 圖示來關閉篩選器窗格。

3. 按一下“刷新資源”。

在 RAC One Node 場景中，資料庫被發現為其目前所在節點上的 RAC 資料庫。

結果

資料庫與資料庫類型、主機或叢集名稱、相關資源群組和策略以及狀態等資訊一起顯示。



如果資料庫在SnapCenter之外重新命名，則必須刷新資源。

- 如果資料庫位於非NetApp儲存系統上，則使用者介面將在「整體狀態」欄位中顯示「不可用於備份」訊息。

您無法對非NetApp儲存系統上的資料庫執行資料保護操作。

- 如果資料庫位於NetApp儲存系統且未受保護，則使用者介面將在「整體狀態」欄位中顯示「未受保護」訊息。
- 如果資料庫位於NetApp儲存系統上並且受到保護，則使用者介面會在「整體狀態」欄位中顯示「可供備份」訊息。



如果您啟用了 Oracle 資料庫驗證，資源檢視中會顯示一個紅色掛鎖圖示。您必須配置資料庫憑證才能保護資料庫或將其新增至資源組以執行資料保護操作。

為 Oracle 資料庫建立備份策略

在使用SnapCenter備份 Oracle 資料庫資源之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。您也可以指定複製、腳本和備份類型設定。當您想要在另一個資源或資源群組上重複使用策略時，建立策略可以節省時間。

開始之前

- 您必須已經定義了您的備份策略。
- 您必須已完成安裝SnapCenter、新增主機、發現資料庫和建立儲存系統連線等任務，為資料保護做好準備。
- 如果您要將快照複製到映像或保管庫二級存儲， SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。
- 如果您以非 root 使用者身分安裝了該插件，則應手動為 prescript 和 postscript 目錄指派執行權限。
- 查看SnapMirror主動同步特定的先決條件和限制。欲了解詳細信息，請參閱 ["SnapMirror主動同步的物件限制"](#)。

關於此任務

如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。

+ 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。

+ 對於ONTAP 9.12.1 及以下版本，作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 從下拉清單中選擇“**Oracle** 資料庫”。
4. 點選“新建”。
5. 在名稱頁面中，輸入策略名稱和詳細資訊。
6. 在「策略類型」頁面中，執行下列步驟：

a. 選擇您的儲存類型。

b. 選擇政策範圍：

- 如果您想*建立線上備份*，請選擇*線上備份*。

您必須指定是否要備份所有資料文件、控制文件和存檔日誌文件，還是僅備份資料檔案和控制文件，或僅備份存檔日誌文件。

- 如果您想*建立離線備份*，請選擇*離線備份*，然後選擇以下選項之一：

- 如果要在資料庫處於安裝狀態時建立離線備份，請選擇*安裝*。
- 如果要透過將資料庫變更為關閉狀態來建立離線關閉備份，請選擇*關閉*。

如果您有可插拔資料庫 (PDB)，並且想要在建立備份之前儲存 PDB 的狀態，則必須選擇 **儲存 PDB** 的狀態。這使您能夠在建立備份後將 PDB 還原到其原始狀態。

- c. 如果要使用 Oracle Recovery Manager (RMAN) 進行目錄備份，請選擇*使用 Oracle Recovery Manager (RMAN) 進行目錄備份*。

您可以使用 GUI 或使用 SnapCenter CLI 指令 `Catalog-SmBackupWithOracleRMAN` 一次對一個備份執行延遲編目。



如果要對 RAC 資料庫的備份進行編目，請確保沒有針對該資料庫執行其他作業。如果另一個作業正在運行，則編目操作將失敗而不是排隊。

- d. 如果要在備份後修剪存檔日誌，請選擇*備份後修剪存檔日誌*。



將跳過從資料庫中未配置的存檔日誌目標中修剪存檔日誌的操作。



如果您使用的是 Oracle 標準版，則可以在執行存檔日誌備份時使用 `LOG_ARCHIVE_DEST` 和 `LOG_ARCHIVE_DUPLEX_DEST` 參數。

- 只有當您選擇存檔日誌檔案作為備份的一部分時，您才可以刪除存檔日誌。



您必須確保 RAC 環境中的所有節點都可以存取所有存檔日誌位置，才能成功執行刪除操作。

如果你想...	然後...
刪除所有存檔日誌	選擇*刪除所有存檔日誌*。
刪除較舊的存檔日誌	選擇*刪除早於此時間的存檔日誌*，然後以天數和小時數指定要刪除的存檔日誌的使用期限。
從所有目的地刪除存檔日誌	選擇*從所有目的地刪除存檔日誌*。
從作為備份一部分的日誌目標中刪除存檔日誌	選擇*從備份目的地刪除存檔日誌*。

+

☒ Prune archive logs after backup

Prune log retention setting

☐ Delete all archive logs

☒ Delete archive logs older than

Prune log destination setting

☐ Delete archive logs from all the destinations

☒ Delete archive logs from the destinations which are part of backup

7. 在「快照和複製」頁面中，執行下列步驟：

- a. 透過選擇*按需*、每小時、每天、*每週*或*每月*來指定計畫頻率。



您可以在建立資源組時指定備份作業的計畫（開始日期和結束日期）。這使您能夠建立共享相同策略和備份頻率的資源群組，但允許您為每個策略指派不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- a. 在資料快照保留設定部分中，指定備份類型和在備份類型頁面中選擇的計畫類型的保留設定：

如果你想...	然後...

保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*並指定天、月或年的持續時間。 SnapLock保留期應少於 100 年。

b. 在存檔日誌快照保留設定部分中，指定備份類型和備份類型頁面中選擇的計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。

快照副本鎖定期	選擇*Snapshot 副本鎖定期限*並指定天、月或年的持續時間。 SnapLock保留期應少於 100 年。

c. 選擇策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

8. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：



您必須選擇輔助複製選項才能使*輔助快照副本鎖定期*生效。

對於這個領域...	這樣做...
建立本地快照後更新SnapMirror	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 應為SnapMirror主動同步啟用此選項。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。
建立本機快照後更新SnapVault	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。 有關SnapLock Vault 的更多信息，請參閱 " 將 Snapshot 副本提交到保管庫目標上的 WORM " 看"在拓撲頁面中查看 Oracle 資料庫備份和克隆" 。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

9. 在腳本頁面中，分別輸入要在備份作業之前或之後執行的前置腳本或後置腳本的路徑和參數。

您必須將腳本和後記儲存在 `/var/opt/snapcenter/spl/scripts` 或此路徑內的任何資料夾中。預設情況下，填入

`/var/opt/snapcenter/spl/scripts` 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。

您也可以指定腳本超時值。預設值為 60 秒。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

10. 在驗證頁面中，執行以下步驟：

- a. 選擇要執行驗證作業的備份計畫。
- b. 在驗證腳本指令部分，分別輸入要在驗證作業之前或之後執行的腳本或後腳本的路徑和參數。

您必須將腳本和後記儲存在 `/var/opt/snapcenter/spl/scripts` 或此路徑內的任何資料夾中。預設情況下，填入 `/var/opt/snapcenter/spl/scripts` 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。

您也可以指定腳本超時值。預設值為 60 秒。

11. 查看摘要，然後按一下「完成」。

為 Oracle 資料庫建立資源組並附加策略

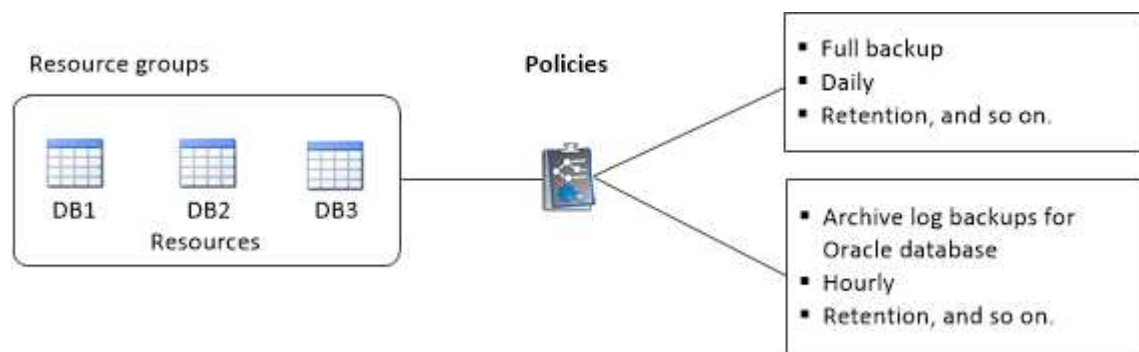
資源組是一個容器，您可以在其中新增想要備份和保護的資源。資源組可讓您同時備份與給定應用程式相關的所有資料。

關於此任務

- 具有 ASM 磁碟組中檔案的資料庫必須處於「MOUNT」或「OPEN」狀態才能使用 Oracle DBVERIFY 公用程式驗證其備份。

將一個或多個策略附加到資源組以定義要執行的資料保護作業的類型。

下圖說明了資料庫的資源、資源群組和策略之間的關係：



- 對於啟用SnapLock的策略、對於ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新資料庫新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下將新資料庫新增至現有資源組。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，`customtext_resource group_policy_hostname` 或 `resource group_hostname`。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



您應該使用與 Oracle 中設定的完全相同的目標，包括前綴（如果需要）。

4. 在資源頁面中，從*主機*下拉清單中選擇 Oracle 資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從“可用資源”部分中選擇資源並將其移至“選定資源”部分。



您可以在單一資源組中新增來自 Linux 和 AIX 主機的資料庫。

6. 在應用程式設定頁面中，選擇備份選項。

7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計畫的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtptServer 指定 SMTP 伺服器詳細資訊。

10. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並啟用 Oracle 資源的二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。

2. 在資源頁面中，按一下「新資源組」。

3. 在名稱頁面中，執行以下操作：

a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，`customtext_resource group_policy_hostname` 或 `resource group_hostname`。預設情況下，時間戳記會附加到快照名稱。

d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。

6. 在應用程式設定頁面中，選擇備份選項。

7. 在「策略」頁面中，執行以下步驟：

a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

b.

點選  在要設定計畫的策略的配置計畫列中。

c. 在為政策_policy_name_新增計畫視窗中，配置計畫，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：
 - a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
 - b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
 - c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

備份 Oracle 資源

如果資源不屬於任何資源群組，您可以從資源頁面備份該資源。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，從視圖清單中選擇*資料庫*。

3. 點選，然後選擇主機名稱和資料庫類型來過濾資源。

然後您可以點選關閉篩選器窗格。

4. 選擇要備份的資料庫。

進入「資料庫保護」頁面。

5. 在資源頁面中，執行以下步驟：

- a. 選取複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，`customtext_policy_hostname``或者 ``resource_hostname`。預設情況下，時間戳記會附加到快照名稱。

- b. 指定您不想備份的存檔日誌檔案的目標。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。

您可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在配置時間表列中為您想要的策略配置時間表。

- c. 在「為政策_policy_name_新增計劃」視窗中，配置計劃，然後選擇 OK。

policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

7. 在驗證頁面中，執行以下步驟：

- a. 點擊“載入定位器”以載入SnapMirror或SnapVault磁碟區來驗證二級儲存。

- b. 點選  在配置時間表列中為策略的所有時間表類型配置驗證時間表。+ 在新增驗證計畫_policy_name_對話方塊中，您可以執行下列步驟：

- c. 選擇*備份後執行驗證*。

- d. 選擇*執行計劃驗證*，並從下拉清單中選擇計劃類型。



在 Flex ASM 設定中，如果基數小於 RAC 叢集中的節點數，則無法對 Leaf 節點執行驗證操作。

- e. 選擇*在輔助位置驗證*以驗證輔助儲存上的備份。

- f. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中選擇您想要傳送電子郵件的場景。

您必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源執行的備份作業的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令指定 SMTP 伺服器詳細資訊 `Set-SmSmtServer`。

9. 查看摘要，然後按一下「完成」。

進入資料庫拓撲頁面。

10. 點選*立即備份*。

11. 在備份頁面中，執行以下步驟：

a. 如果您已對資源套用了多個策略，請從策略下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

b. 按一下“備份”。

12. 透過點選「監視」>「作業」來監視操作進度。

完成後

- 在 AIX 設定中，您可以使用 ``lkdev`` 命令鎖定和 ``rendev`` 指令重新命名備份資料庫所在的磁碟。

當您使用該備份進行還原時，鎖定或重新命名裝置不會影響復原作業。

- 如果由於資料庫查詢執行時間超過逾時值而導致備份操作失敗，則應透過執行下列命令來變更 `ORACLE_SQL_QUERY_TIMEOUT` 和 `ORACLE_PLUGIN_SQL_QUERY_TIMEOUT` 參數的值 ``Set-SmConfigSettings`` 命令：

修改參數值後，透過執行以下命令重新啟動SnapCenter插件Loader(SPL) 服務

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

- 如果在驗證過程中無法存取該檔案且掛載點不可用，則操作可能會失敗，並出現錯誤代碼 DBV-00100 指定檔案。您應該修改 `sco.properties` 中的 `VERIFICATION_DELAY` 和 `VERIFICATION_RETRY_COUNT` 參數的值。

修改參數值後，透過執行以下命令重新啟動SnapCenter插件Loader(SPL) 服務

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

- 在 MetroCluster 配置中，SnapCenter 可能無法在故障轉移後偵測到保護關係。
- 如果您正在備份 VMDK 上的應用程式數據，並且 SnapCenter Plug-in for VMware vSphere 的 Java 堆大小不夠大，則備份可能會失敗。

若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method`` 命令啟動 SnapCenter VMware 插件服務。將該命令更新為以下內容：``Java -jar -Xmx8192M -Xms4096M`。

查找更多信息

- ["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

- "跳過 Oracle RAC One Node 資料庫來執行SnapCenter操作"
- "無法變更 Oracle 12c ASM 資料庫的狀態"
- "AIX 系統上備份、還原和克隆作業的可自訂參數" (需要登入)

備份 Oracle 資料庫資源組

資源組是主機或叢集上的資源的集合。備份操作針對資源組中定義的所有資源執行。

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則會根據計劃建立備份。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 在搜尋框中輸入資源組名稱，或按一下，然後選擇標籤。

點選關閉篩選器窗格。

4. 在資源組頁面中，選擇要備份的資源組。



如果您有一個包含兩個資料庫的聯合資源群組，而其中一個資料庫的資料位於非NetApp儲存體上，則即使另一個資料庫位於NetApp儲存體上，備份作業也會中止。

5. 在備份頁面中，執行以下步驟：

- a. 如果您有多個與資源群組關聯的策略，請從「策略」下拉清單中選擇要使用的備份策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 選擇*備份*。

6. 透過選擇「監控」>「作業」來監控進度。

完成後

- 在 AIX 設定中，您可以使用 `lkdev` 命令鎖定和 `rendev` 指令重新命名備份資料庫所在的磁碟。

當您使用該備份進行還原時，鎖定或重新命名裝置不會影響復原作業。

- 如果由於資料庫查詢執行時間超過逾時值而導致備份操作失敗，則應透過執行下列命令來變更 ORACLE_SQL_QUERY_TIMEOUT 和 ORACLE_PLUGIN_SQL_QUERY_TIMEOUT 參數的值 `Set-SmConfigSettings` 命令：

修改參數值後，透過執行以下命令重新啟動SnapCenter插件Loader(SPL) 服務
`/opt/NetApp/snapcenter/spl/bin/spl restart`

- 如果在驗證過程中無法存取該檔案且掛載點不可用，則操作可能會失敗，並出現錯誤代碼 DBV-00100 指定檔案。您應該修改sco.properties中VERIFICATION_DELAY_和VERIFICATION_RETRY_COUNT參數的值。

修改參數值後，透過執行以下命令重新啟動SnapCenter插件Loader(SPL) 服務

監控 Oracle 資料庫備份

了解如何監控備份作業和資料保護作業的進度。

監視 Oracle 資料庫備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監視資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

其他備份操作

使用 **UNIX** 指令備份 **Oracle** 資料庫

備份工作流包括規劃、確定備份資源、建立備份策略、建立資源群組和附加策略、建立備份以及監控作業。

您需要什麼

- 您應該已經使用命令 `_Add-SmStorageConnection_` 和 `_Add-SmCredential_` 新增了儲存系統連線並建立了憑證。
- 您應該已經使用命令 `_Open-SmConnection_` 與 SnapCenter 伺服器建立連線會話。

您只能有一個 SnapCenter 帳戶登入會話，並且令牌儲存在使用者主目錄中。



連線會話僅在 24 小時內有效。但是，您可以使用 `TokenNeverExpires` 選項建立令牌，以建立永不過期的令牌，並且會話將始終有效。

關於此任務

您應該執行以下命令來與 SnapCenter 伺服器建立連接，發現 Oracle 資料庫實例，新增策略和資源群組，備份並驗證備份。

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體命令參考指南](#)"。

步驟

1. 為指定使用者啟動與 SnapCenter 伺服器的連線會話：`Open-SmConnection`
2. 執行主機資源發現操作：`Get-SmResources`
3. 為 Real Application Cluster (RAC) 資料庫的備份作業設定 Oracle 資料庫憑證和優先節點：`Configure-SmOracleDatabase`
4. 建立備份策略：`Add-SmPolicy`
5. 檢索有關二級（SnapVault 或 SnapMirror）儲存位置的資訊：`Get-SmSecondaryDetails`

此命令檢索指定資源的主儲存到輔助儲存映射詳細資訊。您可以在建立備份資源組時使用映射詳細資訊來設定二次驗證設定。

6. 為SnapCenter新增資源組：*Add-SmResourceGroup*

7. 建立備份：*New-SmBackup*

您可以使用 *WaitForCompletion* 選項輪詢作業。如果指定了此選項，則命令將繼續輪詢伺服器，直到備份作業完成。

8. 從SnapCenter檢索日誌：*Get-SmLogs*

取消 **Oracle** 資料庫的備份作業

您可以取消正在執行、排隊或無回應的備份作業。

您必須以SnapCenter管理員或作業所有者的身分登入才能取消備份作業。

關於此任務

當您取消備份作業時，如果已建立的備份未在SnapCenter Server 中註冊， SnapCenter Server 將停止該作業並從儲存體中刪除所有快照。如果備份已在SnapCenter Server 中註冊，則即使觸發取消，也不會回溯已建立的快照。

- 您只能取消排隊或正在執行的日誌或完整備份作業。
- 驗證開始後，您無法取消操作。

如果在驗證前取消操作，則操作被取消，並且不會執行驗證操作。

- 目錄操作開始後，您無法取消備份作業。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 除了使用SnapCenter GUI 之外，您還可以使用 CLI 命令來取消操作。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇操作並按一下「取消作業」。

從...	行動
活動窗格	1. 啟動備份作業後，按一下  在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

結果

操作被取消，資源恢復到原始狀態。

如果您取消的作業在取消或運作狀態下無回應，則應執行 `Cancel-SmJob -JobID <int> -Force` 強制停止備份作業。

在拓撲頁面中查看 **Oracle** 資料庫備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

在拓撲頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。

顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。

-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受到保護，則會顯示所選資源的拓樸頁面。

4. 查看摘要卡以了解主儲存和輔助儲存上可用的備份和複製數量的摘要。

摘要卡部分顯示備份和克隆的總數以及日誌備份的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 會自動配置為新的主目標。
- 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示來執行還原、複製、掛載、卸載、重新命名、編目、取消編目和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

- 如果選擇了日誌備份，則只能執行重新命名、掛載、卸載、編目、取消編目和刪除作業。
- 如果您已使用 Oracle Recovery Manager (RMAN) 對備份進行分類，則無法重新命名這些已分類的備份。

7. 如果要刪除克隆，請從表中選擇克隆，然後按一下 。

如果指派給 SnapmirrorStatusUpdateWaitTime 的值較小，則即使資料和日誌磁碟區成功受到保護，鏡像和保管庫備份副本也不會列在拓樸頁面上。您應該使用 `Set-SmConfigSettings PowerShell cmdlet` 來增加指派給 SnapmirrorStatusUpdateWaitTime 的值。

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。

或者，您也可以參考 "[SnapCenter軟體命令參考指南](#)" 或者 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

掛載和卸載資料庫備份

如果您想存取備份中的文件，您可以安裝單一或多個資料並僅記錄備份。您可以將備份安裝到已建立備份的相同主機，也可以安裝到具有相同類型的 Oracle 和主機配置的遠端主機。如果您已手動安裝了備份，則應在完成作業後手動卸載備份。在任何給定實例中，資料庫的備份都可以安裝到任何一個主機上。執行操作時，您只能安裝一個備份。



在 Flex ASM 設定中，如果基數小於 RAC 叢集中的節點數，則無法在 Leaf 節點上執行掛載操作。

裝載資料庫備份

如果您想存取備份中的文件，則應該手動安裝資料庫備份。

您需要什麼

- 如果您在 NFS 環境中有一個自動儲存管理 (ASM) 資料庫實例並且想要掛載 ASM 備份，則應該將 ASM 磁碟路徑 `/var/opt/snapcenter/sco/backup*/**/*/*` 新增至 `asm_diskstring` 參數中定義的現有路徑。
- 如果您在 NFS 環境中有一個 ASM 資料庫實例，並且想要將 ASM 日誌備份作為復原作業的一部分掛載，則應該將 ASM 磁碟路徑 `/var/opt/snapcenter/scu/clones*/**/*` 新增至 `asm_diskstring` 參數中定義的現有路徑。
- 在 `asm_diskstring` 參數中，如果使用 ASMFD，則應配置 `AFD:*`；如果使用 ASMLIB，則應配置 `ORCL:*`。



有關如何編輯 `asm_diskstring` 參數的信息，請參閱 "[如何將磁碟路徑新增至 asm_diskstring](#)"。

- 如果 ASM 憑證和 ASM 連接埠與來源資料庫主機的不同，則在裝載備份時應配置 ASM 憑證和 ASM 連接埠。
- 如果要掛載到備用主機，則必須驗證備用主機是否符合以下要求：
 - 與原始主機相同的 UID 和 GID
 - 與原始主機相同的 Oracle 版本
 - 與原始主機相同的作業系統發行版和版本
 - 對於 NVMe，應安裝 NVMe util
- 您應該確保 LUN 沒有使用由混合協定 iSCSI 和 FC 組成的 iGroup 對應到 AIX 主機。有關更多信息，請參閱 "[操作失敗，錯誤：無法發現 LUN 的設備](#)"。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從資料庫詳細資訊檢視或資源組詳細資料檢視中選擇資料庫。

進入資料庫拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或複製）中選擇「備份」。
5. 從表中選擇備份，然後按一下 。

6. 在「掛載備份」頁面中，從*選擇要掛載備份的主機*下拉清單中選擇要掛載備份的主機。

顯示掛載路徑 `/var/opt/snapcenter/sco/backup_mount/backup_name/database_name`。

如果正在掛載 ASM 資料庫的備份，則會顯示掛載路徑 `+diskgroupname_SID_backupid`。

7. 按一下“安裝”。

完成後

- 您可以執行以下命令來檢索與已掛載備份相關的資訊：

```
./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
```

- 如果您已經安裝了 ASM 資料庫，則可以執行下列命令來擷取與已安裝備份相關的資訊：

```
./sccli Get-Smbbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
```

- 若要檢索備份 ID，請執行下列命令：

```
./sccli Get-Smbbackup-BackupNamebackup_name
```

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體命令參考指南"](#)。

卸載資料庫備份

當您不再想存取備份上的檔案時，可以手動卸載已安裝的資料庫備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從資料庫詳細資訊檢視或資源組詳細資料檢視中選擇資料庫。

進入資料庫拓撲頁面。

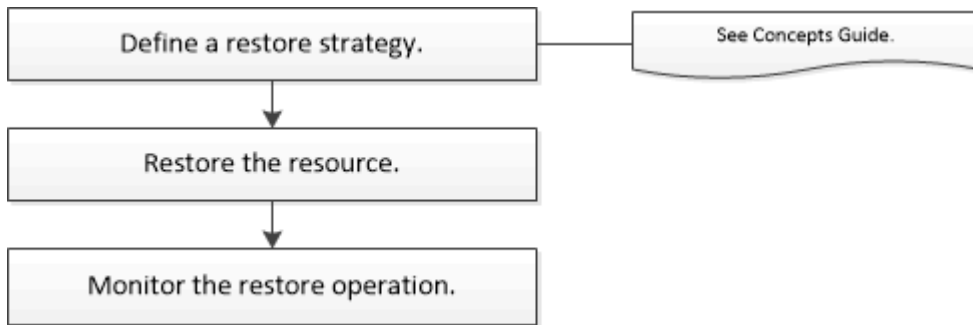
4. 選擇已裝載的備份，然後按一下 。
5. 按一下“確定”。

還原和還原 Oracle 資料庫

復原工作流程

復原工作流程包括規劃、執行復原操作和監控操作。

以下工作流程顯示了執行還原作業必須遵循的順序：



定義 **Oracle** 資料庫的還原與復原策略

您必須在還原和復原資料庫之前定義一個策略，以便能夠成功執行還原和復原作業。

還原和復原作業支援的備份類型

SnapCenter支援不同類型的 **Oracle** 資料庫備份的還原和還原。

- 線上資料備份
- 離線關機資料備份
- 離線掛載資料備份



如果您正在恢復離線關閉或離線掛載資料備份，SnapCenter會使資料庫處於離線狀態。您應該手動恢復資料庫並重置日誌。

- 完整備份
- Data Guard 備用資料庫的離線備份
- Active Data Guard 備用資料庫的僅資料線上備份



您無法執行 Active Data Guard 備用資料庫的復原。

- 真實應用叢集 (RAC) 設定中的線上資料備份、線上完整備份、離線掛載備份和離線關機備份
- 自動儲存管理 (ASM) 設定中的線上資料備份、線上完整備份、離線掛載備份和離線關機備份

Oracle 資料庫支援的還原方法類型

SnapCenter支援 **Oracle** 資料庫的連線和複製或就地還原。在還原作業期間，SnapCenter會決定適合檔案系統的還原方法，以使用於還原而不會遺失任何資料。



SnapCenter不支援基於磁碟區的SnapRestore。

如果資料庫佈局與備份不同，或在建立備份後有任何新文件，則執行連線和複製還原。在連線和複製還原方法中，執行下列任務：

步驟

1. 該磁碟區是從快照克隆的，並且使用克隆的 LUN 或磁碟區在主機上建立檔案系統堆疊。
2. 文件從克隆的檔案系統複製到原始檔案系統。
3. 然後從主機上卸載克隆的檔案系統，並從ONTAP中刪除克隆的磁碟區。



對於 Flex ASM 設定（基數小於 RAC 叢集中的節點數）或 VMDK 或 RDM 上的 ASM RAC 資料庫，僅支援連接和複製復原方法。

即使您已強制啟用就地還原， SnapCenter也會在下列情況下執行連線和複製還原：

- 從輔助儲存系統復原
- 還原未配置資料庫實例的 Oracle RAC 設定節點上的 ASM 磁碟組
- 在 Oracle RAC 設定中，如果 ASM 實例或叢集實例未執行，或對等節點已關閉，則在任何對等節點上
- 僅恢復控制文件
- 復原位於 ASM 磁碟組上的表空間子集
- 資料檔案、sp檔案、密碼檔案共享磁碟組
- SnapCenter插件Loader(SPL) 服務未安裝或未在 RAC 環境中的遠端節點上執行
- 新節點已新增至 Oracle RAC，但SnapCenter伺服器不知道新新增的節點

就地還原

如果資料庫佈局與備份類似，且在儲存體和資料庫堆疊上沒有發生任何設定更改，則執行就地還原，其中在ONTAP上執行檔案或 LUN 的還原。 SnapCenter僅支援單一檔案SnapRestore (SFSR) 作為就地復原方法的一部分。



NetApp ONTAP支援從輔助位置進行就地復原。

如果要在資料庫上執行就地恢復，請確保 ASM 磁碟組上只有資料檔案。對 ASM 磁碟組或資料庫的實體結構進行任何變更後，都必須建立備份。執行就地復原後，磁碟組將包含與備份時相同數量的資料檔案。

當磁碟組或掛載點符合下列條件時，將自動套用就地還原：

- 備份後沒有新增新的資料檔案（外部檔案檢查）
- 備份後不新增、刪除或重新建立 ASM 磁碟或 LUN（ASM 磁碟組結構變化檢查）
- 不向 LVM 磁碟組新增、刪除或重新建立 LUN（LVM 磁碟組結構變化檢查）



您也可以使用 GUI、 SnapCenter CLI 或 PowerShell cmdlet 強制啟用就地還原，以覆寫外部檔案檢查和 LVM 磁碟組結構變更檢查。

在 ASM RAC 上執行就地恢復

在 SnapCenter 中，執行還原的節點稱為主節點，而 ASM 磁碟組所在的 RAC 的所有其他節點稱為對等節點。在執行儲存還原作業之前，SnapCenter 會在 ASM 磁碟組處於掛載狀態的所有節點上將 ASM 磁碟組的狀態變更為卸載。儲存恢復完成後，SnapCenter 會將 ASM 磁碟組的狀態變更為復原作業之前的狀態。

在 SAN 環境中，SnapCenter 會從所有對等節點中刪除設備，並在儲存復原作業之前執行 LUN 取消對映操作。儲存復原作業後，SnapCenter 執行 LUN 對映操作並在所有對等節點上建置裝置。在 SAN 環境中，如果 Oracle RAC ASM 佈局駐留在 LUN 上，則在還原 SnapCenter 時，會在 ASM 磁碟組所在的 RAC 叢集的所有節點上執行 LUN 取消對應、LUN 還原和 LUN 對應操作。即使在還原之前 RAC 節點的所有啟動器都沒有用於 LUN，還原之後 SnapCenter 也會使用所有 RAC 節點的所有啟動器建立新的 iGroup。

- 如果對等節點上的預還原活動期間發生任何故障，SnapCenter 會自動將 ASM 磁碟組狀態回滾到在預還原作業成功的對等節點上執行還原之前的狀態。主節點和操作失敗的對等節點不支援回滾。在嘗試另一次復原之前，您必須手動修復對等節點上的問題，並將主節點上的 ASM 磁碟組還原為安裝狀態。
- 如果在復原活動期間出現任何故障，則復原操作失敗且不會執行回溯。在嘗試另一次復原之前，您必須手動修復儲存復原問題並使主節點上的 ASM 磁碟組還原到安裝狀態。
- 如果任何對等節點上的復原後活動期間出現任何故障，SnapCenter 將繼續在其他對等節點上執行復原作業。您必須手動修復對等節點上的復原後問題。

Oracle 資料庫支援的還原作業類型

SnapCenter 可讓您對 Oracle 資料庫執行不同類型的復原作業。

在還原資料庫之前，將驗證備份以確定與實際資料庫檔案相比是否缺少任何檔案。

完全恢復

- 僅恢復資料檔案
- 僅恢復控制文件
- 恢復資料檔案和控制文件
- 還原 Data Guard 備用資料庫和 Active Data Guard 備用資料庫中的資料檔案、控制檔案和重做日誌文件

部分恢復

- 僅恢復選定的表空間
- 僅恢復選定的可插拔資料庫 (PDB)
- 僅恢復 PDB 的選定表空間

Oracle 資料庫支援的復原作業類型

SnapCenter 可讓您對 Oracle 資料庫執行不同類型的復原作業。

- 資料庫直到最後事務（所有日誌）
- 資料庫達到特定的系統變更號碼（SCN）
- 資料庫直到特定的日期和時間

您必須根據資料庫主機の時區指定復原的日期和時間。

SnapCenter也為 Oracle 資料庫提供了無復原選項。



如果您使用以資料庫角色作為備用建立的備份進行恢復，則 Oracle 資料庫外掛程式不支援恢復。您必須始終對實體備用資料庫執行手動復原。

與 Oracle 資料庫還原和復原相關的限制

在執行還原和復原操作之前，您必須了解其限制。

如果您使用的是 Oracle 11.2.0.4 至 12.1.0.1 中的任何版本，則執行 *renamedg* 指令時還原作業將處於暫停狀態。您可以套用 Oracle 補丁 19544733 來修復此問題。

不支援以下還原和復原操作：

- 根容器資料庫 (CDB) 表空間的還原和恢復
- 恢復臨時表空間和與 PDB 關聯的臨時表空間
- 同時從多個 PDB 還原和還原表空間
- 復原日誌備份
- 將備份還原到其他位置
- 在 Data Guard 備用資料庫或 Active Data Guard 備用資料庫以外的任何設定中還原重做記錄檔
- 恢復 SPFILE 和密碼文件
- 當您對使用相同主機上預先存在的資料庫名稱重新建立、由 SnapCenter 管理且具有有效備份的資料庫執行還原作業時，還原作業會覆寫新建立的資料庫文件，即使 DBID 不同。

可以透過執行以下操作之一來避免這種情況：

- 重新建立資料庫後發現 SnapCenter 資源
- 建立重新建立的資料庫的備份

與表空間的時間點恢復相關的限制

- 不支援 SYSTEM、SYSAUX 和 UNDO 表空間的時間點復原 (PITR)
- 表空間的 PITR 不能與其他類型的復原一起執行
- 如果表空間被重新命名，並且您想要將其還原到重新命名之前的某個時間點，則應指定表空間的早期名稱
- 如果一個表空間中的表的限制包含在另一個表空間中，則應該恢復這兩個表空間
- 如果表及其索引儲存在不同的表空間中，則應在執行 PITR 之前刪除索引
- PITR 不能用於恢復目前預設表空間
- PITR 不能用於復原包含下列任何物件的表空間：
 - 具有底層物件（例如物化視圖）或包含物件（例如分區表）的對象，除非所有底層物件或包含物件都在復原集中

此外，如果分割表的分割區儲存在不同的表空間中，那麼您應該在執行 PITR 之前刪除該表，或者在執行 PITR 之前將所有分割區移動到同一個表空間。

- 撤銷或回滾段
- 具有多個接收者的 Oracle 8 相容高階佇列
- SYS 使用者擁有的對象

這些類型的物件的範例有 PL/SQL、Java 類別、呼叫程式、檢視、同義詞、使用者、權限、維度、目錄和序列。

還原 Oracle 資料庫的來源和目標

您可以從主儲存或輔助儲存上的備份副本還原 Oracle 資料庫。您只能將資料庫還原到同一資料庫執行個體上的相同位置。但是，在 Real Application Cluster (RAC) 設定中，您可以將資料庫還原到其他節點。

恢復操作的來源

您可以從主儲存或輔助儲存上的備份還原資料庫。如果要從多鏡像配置中的輔助儲存上的備份進行恢復，則可以選擇輔助儲存鏡像作為來源。

恢復操作的目標

您只能將資料庫還原到同一資料庫執行個體上的相同位置。

在 RAC 設定中，您可以從叢集中的任何節點還原 RAC 資料庫。

用於恢復特定處方和後記的預定義環境變量

SnapCenter可讓您在還原資料庫時執行前腳本和後腳本時使用預先定義的環境變數。

支援用於復原資料庫的預定義環境變數

- **SC_JOB_ID** 指定操作的作業 ID。

例如：257

- **SC_ORACLE_SID** 指定資料庫的系統識別碼。

如果操作涉及多個資料庫，這將包含以管道分隔的資料庫名稱。

例如：NFSB31

- **SC_HOST** 指定資料庫的主機名稱。

此參數將填入應用程式磁碟區。

範例：scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** 指定資料庫的作業系統擁有者。

範例：oracle

- **SC_OS_GROUP** 指定資料庫的作業系統群組。

範例：oinstall

- **SC_BACKUP_NAME** 指定備份的名稱。

此參數將填入應用程式磁碟區。

例子：

- 如果資料庫未以 ARCHIVELOG 模式運作：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_scspr2417819002_07-20-2021_12.
- 如果資料庫以 ARCHIVELOG 模式運作：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_8.9

- **SC_BACKUP_ID** 指定備份的 ID。

此參數將填入應用程式磁碟區。

例子：

- 如果資料庫未以 ARCHIVELOG 模式運作：DATA@203|LOG@205
- 如果資料庫以 ARCHIVELOG 模式運作：DATA@203|LOG@205,206,207

- **SC_RESOURCE_GROUP_NAME** 指定資源組的名稱。

例如：RG1

- **SC_ORACLE_HOME** 指定 Oracle 主目錄的路徑。

範例：/ora01/app/oracle/product/18.1.0/db_1

- **SC_RECOVERY_TYPE** 指定要復原的檔案以及復原範圍。

範例

：RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false。

有關分隔符號的信息，請參閱["支援的分隔符"](#)。

恢復 Oracle 資料庫的要求

在還原 Oracle 資料庫之前，您應該確保先決條件已滿足。

- 您應該已經定義了您的復原和復原策略。
- 如果您要將快照複製到映像或保管庫，SnapCenter 管理員應該已經為來源磁碟區和目標磁碟區指派了儲存虛擬機器 (SVM)。
- 如果將存檔日誌作為備份的一部分被修剪，則您應該手動安裝所需的存檔日誌備份。
- 如果要復原駐留在虛擬機器磁碟 (VMDK) 上的 Oracle 資料庫，則應確保用戶端具有所需數量的可用插槽來

指派複製的 VMDK。

- 如果為該資料庫啟用了二級保護，則應確保屬於該資料庫的所有資料磁碟區和存檔日誌磁碟區都受到保護。
- 您應該確保 RAC One Node 資料庫處於“nomount”狀態以執行控制文件或完整資料庫還原。
- 如果您在 NFS 環境中有一個 ASM 資料庫實例，則應將 ASM 磁碟路徑 `/var/opt/snapcenter/scu/clones/*/*` 新增至 `asm_diskstring` 參數中定義的現有路徑，以便成功掛載 ASM 日誌備份作為復原作業的一部分。
- 在 `asm_diskstring` 參數中，如果使用 ASMFD，則應配置 `AFD:*`；如果使用 ASMLIB，則應配置 `ORCL:*`。



有關如何編輯 `asm_diskstring` 參數的信息，請參閱 ["如何將磁碟路徑新增至 `asm\_diskstring`"](#)

- 如果您已停用 OS 驗證並啟用 Oracle 資料庫驗證，並且想要還原該資料庫的資料檔案和控制文件，則應在 `listener.ora` 檔案中設定靜態偵聽器，對於非 ASM 資料庫，該檔案位於 `$ORACLE_HOME/network/admin`，對於 ASM 資料庫，該檔案位於 `$ORACLE_HOME/network/admin`，對於 ASM 資料庫，該檔案位於 `_`\$
- 如果資料庫大小以 TB 為單位，則應透過執行 `Set-SmConfigSettings` 指令來增加 `SCORestoreTimeout` 參數的值。
- 您應該確保 vCenter 所需的所有授權都已安裝且是最新的。

如果許可證未安裝或不是最新的，則會顯示警告訊息。如果您忽略警告並繼續，從 RDM 復原將會失敗。

- 您應該確保 LUN 沒有使用由混合協定 iSCSI 和 FC 組成的 iGroup 對應到 AIX 主機。有關更多信息，請參閱 ["操作失敗，錯誤：無法發現 LUN 的設備"](#)。

還原和還原 Oracle 資料庫

如果發生資料遺失，您可以使用 SnapCenter 將資料從一個或多個備份還原到活動檔案系統，然後還原資料庫。

開始之前

如果您以非 root 使用者身分安裝了該插件，則應手動為 `prescript` 和 `postscript` 目錄指派執行權限。

關於此任務

- 復原是使用設定的存檔日誌位置處可用的存檔日誌執行的。如果資料庫在 ARCHIVELOG 模式下執行，Oracle 資料庫會將已填入的重做日誌檔案組儲存到一個或多個離線目標，統稱為歸檔重做日誌。SnapCenter 根據指定的 SCN、選定的日期和時間或所有日誌選項識別並安裝最佳數量的日誌備份。如果復原所需的存檔日誌在配置的位置不可用，則應掛載包含日誌的快照並將路徑指定為外部存檔日誌。

如果將 ASM 資料庫從 ASMLIB 遷移到 ASMFD，則使用 ASMLIB 建立的備份不能用於還原資料庫。您應該在 ASMFD 配置中建立備份並使用這些備份進行還原。同樣，如果 ASM 資料庫從 ASMFD 遷移到 ASMLIB，則應在 ASMLIB 配置中建立備份以便復原。

還原資料庫時，會在 Oracle 資料庫主機的 `/var/opt/snapcenter/sco/lock` 目錄中建立一個操作鎖定檔案 (`.sm_lock_dbsid`)，以避免在資料庫上執行多個操作。資料庫復原後，操作鎖定檔案將自動刪除。



不支援恢復 SPFILE 和密碼檔案。

- 對於啟用 SnapLock 的策略、對於 ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承 SnapLock 到期時間。儲存管理員應在 SnapLock 到期後手動清理克

隆。

步驟

- 1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
- 3. 從資料庫詳細資訊檢視或資源組詳細資料檢視中選擇資料庫。

進入資料庫拓撲頁面。

- 4. 從「管理副本」檢視中，從主儲存系統或輔助（鏡像或複製）儲存系統中選擇「備份」。
- 5. 從表格中選擇備份，然後按一下**。
- 6. 在「還原範圍」頁面中，執行下列任務：
 - a. 如果您選擇了 Real Application Clusters (RAC) 環境中的資料庫備份，請選擇 RAC 節點。
 - b. 當您選擇鏡像或保管資料時：
 - 如果鏡像或保險庫中沒有日誌備份，則不會選擇任何內容，且定位器為空。
 - 如果鏡像或保管庫中存在日誌備份，則選擇最新的日誌備份並顯示相應的定位器。



如果選定的日誌備份同時存在於鏡像和保管庫位置，則會顯示兩個定位器。

- c. 執行以下操作：

如果您想恢復...	這樣做...
資料庫的所有資料文件	選擇*所有資料檔*。 僅恢復資料庫的資料檔。控制檔案、存檔日誌或重做日誌檔案未復原。
表空間	選擇*表空間*。 您可以指定要復原的表空間。
控制文件	選擇*控制檔*。  恢復控制檔案時，請確保目錄結構存在或應使用正確的使用者和群組所有權（如果有）創建，以允許復原過程將檔案複製到目標位置。如果該目錄不存在，則還原作業將會失敗。

如果您想恢復...	這樣做...
重做日誌文件	選擇*重做日誌檔*。 此選項僅適用於 Data Guard 備用資料庫或 Active Data Guard 備用資料庫。  非 Data Guard 資料庫不會備份重做日誌檔。對於非 Data Guard 資料庫，使用存檔日誌執行復原。
可插拔資料庫 (PDB)	選擇*可插入資料庫*，然後指定要復原的 PDB。
可插拔資料庫 (PDB) 表空間	選擇*可插入資料庫 (PDB) 表空間*，然後指定要復原的 PDB 和該 PDB 的表空間。 只有當您選擇了要還原的 PDB 時，此選項才可用。

- d. 選擇*如果需要還原和復原則變更資料庫狀態*將資料庫的狀態變更為執行還原和復原作業所需的狀態。

資料庫的各種狀態從高到低依序為open、mounted、started、shutdown。如果資料庫處於較高狀態，則必須選取此複選框，但必須將狀態變更為較低狀態才能執行還原操作。如果資料庫處於較低狀態，但必須將狀態變更為較高狀態才能執行還原操作，則即使您未選取該複選框，資料庫狀態也會自動變更。

如果資料庫處於開啟狀態，並且為了恢復資料庫需要處於安裝狀態，則只有選取此核取方塊才會變更資料庫狀態。

- a. 如果要在備份後新增資料檔案或在 LVM 磁碟組中新增、刪除或重新建立 LUN 的情況下執行就地還原，請選擇「強制就地還原」。

7. 在「恢復範圍」頁面中，執行以下操作：

如果你...	這樣做...
想要恢復到最後一筆交易	選擇“所有日誌”。
想要恢復到特定的系統變更號碼 (SCN)	選擇*直到 SCN（系統變更號碼）*。
想要恢復到特定的資料和時間	選擇*日期和時間*。 您必須指定資料庫主機時區的日期和時間。
不想恢復	選擇*不恢復*。

如果你...	這樣做...
想要指定任何外部歸檔日誌位置	如果資料庫在 ARCHIVELOG 模式下執行，SnapCenter會根據指定的 SCN、選取的日期和時間或所有日誌選項識別並安裝最佳數量的日誌備份。 如果您仍想指定外部存檔日誌檔案的位置，請選擇*指定外部存檔日誌位置*。 如果將存檔日誌作為備份的一部分被修剪，且您已手動安裝了所需的存檔日誌備份，則必須指定已安裝的備份路徑作為還原的外部存檔日誌位置。  在將掛載路徑列為外部日誌位置之前，您應該驗證其路徑和內容。 • "使用ONTAP進行 Oracle 資料保護" • "操作失敗，出現 ORA-00308 錯誤"

如果存檔日誌磁碟區未受保護但資料磁碟區受到保護，則無法透過從輔助備份還原來執行還原。您只能透過選擇“不恢復”來恢復。

如果您在選擇開啟資料庫選項的情況下還原 RAC 資料庫，則只有啟動復原作業的 RAC 執行個體才會還原為開啟狀態。



Data Guard 備用資料庫和 Active Data Guard 備用資料庫不支援復原。

8. 在 PreOps 頁面中，輸入要在復原作業之前執行的處方的路徑和參數。

您必須將處方儲存在 `/var/opt/snapcenter/spl/scripts` 路徑或此路徑內的任何資料夾中。預設情況下，填入 `/var/opt/snapcenter/spl/scripts` 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。

您也可以指定腳本超時值。預設值為 60 秒。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

9. 在 PostOps 頁面中，執行下列步驟：

- a. 輸入要在恢復操作後運行的後記的路徑和參數。

您必須將後記儲存在 `/var/opt/snapcenter/spl/scripts` 或此路徑內的任何資料夾中。預設情況下，填入 `/var/opt/snapcenter/spl/scripts` 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。



如果復原操作失敗，則不會執行後記，而是直接觸發清理活動。

- b. 如果要在復原後開啟資料庫，請選取該複選框。

在恢復具有或不帶有控制檔案的容器資料庫 (CDB) 後，或在僅還原 CDB 控制檔案後，如果指定在復原

後開啟資料庫，則僅開啟 CDB，而不是開啟該 CDB 中的可插拔資料庫 (PDB)。

在 RAC 設定中，恢復後僅開啟用於復原的 RAC 實例。



恢復具有控制檔的使用者表空間、有或沒有控制檔的系統表空間、有或沒有控制檔的 PDB 後，只有與復原操作相關的 PDB 的狀態會變成原始狀態。未用於復原的其他 PDB 的狀態不會變更為原始狀態，因為這些 PDB 的狀態未儲存。您必須手動變更未用於還原的 PDB 的狀態。

10. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件通知的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的復原作業的報告，您必須選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

11. 查看摘要，然後按一下「完成」。

12. 透過點選「監視」>「作業」來監視操作進度。

更多資訊

- ["跳過 Oracle RAC One Node 資料庫來執行 SnapCenter 操作"](#)
- ["無法從輔助 SnapMirror 或 SnapVault 位置還原"](#)
- ["無法從孤立化身的備份中恢復"](#)
- ["AIX 系統上備份、還原和克隆作業的可自訂參數"](#)

使用時間點復原來還原和還原表空間

您可以還原已損壞或刪除的表空間子集，而不會影響資料庫中的其他表空間。SnapCenter 使用 RMAN 執行表空間的時間點復原 (PITR)。

開始之前

- 執行表空間 PITR 所需的備份應該被編目和掛載。
- 如果您以非 root 使用者身分安裝了該插件，則應手動為 prescript 和 postscript 目錄指派執行權限。

關於此任務

在 PITR 操作期間，RMAN 在指定的輔助目的地建立一個輔助實例。輔助目標可以是掛載點或 ASM 磁碟組。如果掛載位置有足夠的空間，則可以重複使用其中一個掛載位置，而不是專用掛載點。

您應該指定日期和時間或 SCN，並在來源資料庫上還原表空間。

您可以選擇並還原駐留在 ASM、NFS 和 SAN 環境中的多個表空間。例如，如果表空間 TS2 和 TS3 位於 NFS 上，而 TS4 位於 SAN 上，則可以執行單一 PITR 作業來還原所有表空間。



在 RAC 設定中，您可以從 RAC 的任何節點執行表格空間的 PITR。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從資料庫詳細資料檢視或資源群組詳細資料檢視中選擇單一實例（多租用戶）類型的資料庫。

進入資料庫拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助（鏡像或複製）儲存系統中選擇「備份」。

如果備份未編入目錄，您應該選擇該備份並點擊*目錄*。

5. 選擇已編目的備份，然後按一下 *。
選擇已編目的備份，然後按一下 *。
6. 在「還原範圍」頁面中，執行下列任務：
 - a. 如果您選擇了 Real Application Clusters (RAC) 環境中的資料庫備份，請選擇 RAC 節點。
 - b. 選擇*表空間*，然後指定要還原的表空間。



您無法在 SYSAUX、SYSTEM 和 UNDO 表空間上執行 PITR。

- c. 選擇*如果需要還原和復原則變更資料庫狀態*將資料庫的狀態變更為執行還原和復原作業所需的狀態。
7. 在「復原範圍」頁面中，執行下列其中一項操作：
 - 如果要還原到特定的系統變更號碼 (SCN)，請選擇 直到 **SCN** 並指定 SCN 和輔助目標。
 - 如果要恢復到特定的日期和時間，請選擇*日期和時間*並指定日期和時間以及輔助目的地。

SnapCenter根據指定的 SCN 或選定的日期和時間識別、然後掛載和編錄執行 PITR 所需的最佳數量的資料和日誌備份。

8. 在 PreOps 頁面中，輸入要在復原作業之前執行的處方的路徑和參數。

您應該將處方儲存在 /var/opt/snapcenter/spl/scripts 路徑中或此路徑內的任何資料夾中。預設情況下，填入 /var/opt/snapcenter/spl/scripts 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。

您也可以指定腳本超時值。預設值為 60 秒。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

9. 在 PostOps 頁面中，執行下列步驟：
 - a. 輸入要在恢復操作後運行的後記的路徑和參數。



如果復原操作失敗，則不會執行後記，而是直接觸發清理活動。

- b. 如果要在復原後開啟資料庫，請選取該複選框。

10. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件通知的場景。
11. 查看摘要，然後按一下「完成」。

12. 透過點選「監視」>「作業」來監視操作進度。

使用時間點復原來恢復可插拔資料庫

您可以還原和還原已損壞或刪除的可插拔資料庫 (PDB)，而不會影響容器資料庫 (CDB) 中的其他 PDB。SnapCenter 使用 RMAN 執行 PDB 的時間點復原 (PITR)。

開始之前

- 執行 PDB PITR 所需的備份應該被編目和掛載。



在 RAC 設定中，您應該在 RAC 設定的所有節點上手動關閉 PDB（將狀態變更為 MOUNTED）。

- 如果您以非 root 使用者身分安裝了該插件，則應手動為 prescript 和 postscript 目錄指派執行權限。

關於此任務

在 PITR 操作期間，RMAN 在指定的輔助目的地建立一個輔助實例。輔助目標可以是掛載點或 ASM 磁碟組。如果掛載位置有足夠的空間，則可以重複使用其中一個掛載位置，而不是專用掛載點。

您應該指定日期和時間或 SCN 來執行 PDB 的 PITR。RMAN 可以還原讀寫、唯讀或刪除的 PDB，包括資料檔。

您只能還原和復原：

- 一次一個 PDB
- PDB 中的一個表空間
- 同一 PDB 的多個表空間



在 RAC 設定中，您可以從 RAC 的任何節點執行表格空間的 PITR。

步驟

- 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
- 從資料庫詳細資料檢視或資源群組詳細資料檢視中選擇單一實例（多租用戶）類型的資料庫。

進入資料庫拓撲頁面。

- 從「管理副本」檢視中，從主儲存系統或輔助（鏡像或複製）儲存系統中選擇「備份」。

如果備份未編入目錄，您應該選擇該備份並點擊*目錄*。

- 選擇已編目的備份，然後按一下 **。
- 在「還原範圍」頁面中，執行下列任務：

- 如果您選擇了 Real Application Clusters (RAC) 環境中的資料庫備份，請選擇 RAC 節點。

b. 根據您是否要還原 PDB 或 PDB 中的表空間，執行下列其中一項操作：

如果你想...	步驟...
恢復 PDB	i. 選擇*可插拔資料庫 (PDB)*。 ii. 指定要恢復的 PDB。  您不能在 PDB\$SEED 資料庫上執行 PITR。
恢復 PDB 中的表空間	i. 選擇*可插入資料庫 (PDB) 表空間*。 ii. 指定 PDB。 iii. 指定要復原的單一表空間或多個表空間。  您無法在 SYSAUX、SYSTEM 和 UNDO 表空間上執行 PITR。

c. 選擇*如果需要還原和復原則變更資料庫狀態*將資料庫的狀態變更為執行還原和復原作業所需的狀態。

7. 在「復原範圍」頁面中，執行下列其中一項操作：

- 如果要還原到特定的系統變更號碼 (SCN)，請選擇 直到 **SCN** 並指定 SCN 和輔助目標。
- 如果要恢復到特定的日期和時間，請選擇*日期和時間*並指定日期和時間以及輔助目的地。

SnapCenter根據指定的 SCN 或選定的日期和時間識別、然後掛載和編錄執行 PITR 所需的最佳數量的資料和日誌備份。

8. 在 PreOps 頁面中，輸入要在復原作業之前執行的處方的路徑和參數。

您應該將處方儲存在 /var/opt/snapcenter/spl/scripts 路徑中或此路徑內的任何資料夾中。預設情況下，填入 /var/opt/snapcenter/spl/scripts 路徑。如果您在此路徑內建立了任何資料夾來儲存腳本，則必須在路徑中指定這些資料夾。

您也可以指定腳本超時值。預設值為 60 秒。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

9. 在 PostOps 頁面中，執行下列步驟：

a. 輸入要在恢復操作後運行的後記的路徑和參數。



如果復原操作失敗，則不會執行後記，而是直接觸發清理活動。

b. 如果要在復原後開啟資料庫，請選取該複選框。

在 RAC 設定中，PDB 將僅在復原資料庫的節點上開啟。您應該在 RAC 設定的所有其他節點上手動開啟復原的 PDB。

10. 在通知頁面上，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件通知的場景。
11. 查看摘要，然後按一下「完成」。
12. 透過點選「監視」>「作業」來監視操作進度。

使用 UNIX 指令還原和還原 Oracle 資料庫

還原和復原工作流程包括規劃、執行還原和復原作業以及監視操作。

關於此任務

- 您應該執行以下命令來與SnapCenter伺服器建立連接，列出備份並檢索其訊息，以及恢復備份。

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體命令參考指南](#)"。

- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。

步驟

1. 為指定使用者啟動與SnapCenter伺服器的連線會話：*Open-SmConnection*
2. 檢索有關要還原的備份的資訊：*Get-SmBackup*
3. 檢索指定備份的詳細資訊：*Get-SmBackupDetails*

此命令檢索具有給定備份 ID 的指定資源的備份的詳細資訊。資訊包括資料庫名稱、版本、主目錄、起始和結束 SCN、表空間、可插拔資料庫及其表空間。

4. 從備份中還原資料：*Restore-SmBackup*

監視 Oracle 資料庫還原作業

您可以使用「作業」頁面監控不同SnapCenter還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

取消 Oracle 資料庫還原作業

您可以取消排隊的還原作業。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消恢復操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的復原操作。
- 您無法取消正在執行的復原操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的還原作業。
- 對於無法取消的復原操作，「取消作業」按鈕將被停用。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊復原作業。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇作業並點選「取消作業」。
活動窗格	1. 啟動恢復操作後，按一下  在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

克隆 Oracle 資料庫

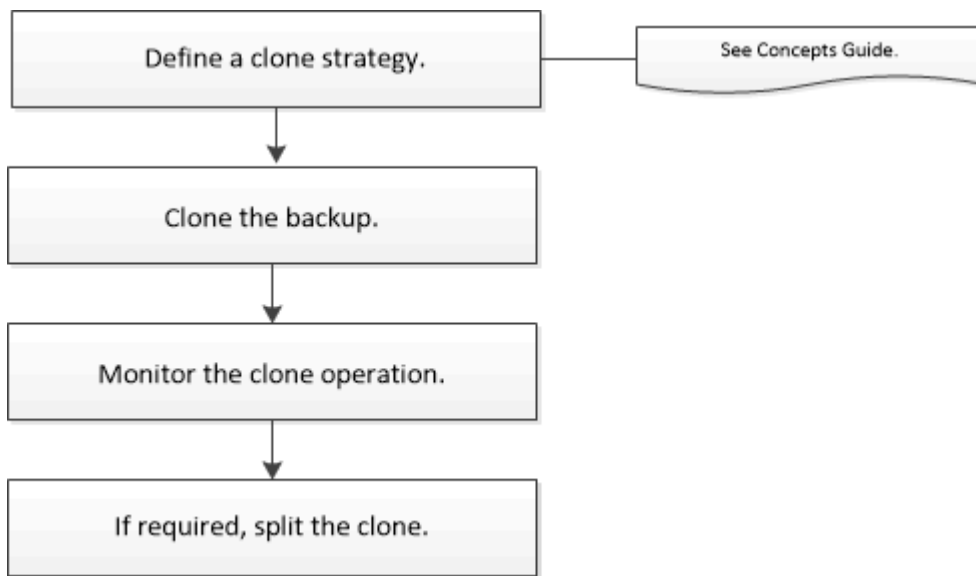
克隆工作流程

克隆工作流程包括規劃、執行複製操作和監控操作。

您可能由於以下原因而克隆資料庫：

- 在應用程式開發週期中測試必須使用目前資料庫結構和內容實現的功能。
- 使用資料擷取和操作工具填充資料倉儲。
- 恢復被錯誤刪除或更改的資料。

以下工作流程顯示了執行複製操作必須遵循的順序：



定義 Oracle 資料庫的克隆策略

在克隆資料庫之前定義策略可確保克隆操作成功。

克隆支援的備份類型

SnapCenter支援克隆不同類型的 Oracle 資料庫備份。

- 線上資料備份
- 線上完整備份
- 離線掛載備份
- 離線關機備份
- Data Guard 備用資料庫和 Active Data Guard 備用資料庫的備份
- 真實應用叢集 (RAC) 設定中的線上資料備份、線上完整備份、離線掛載備份和離線關機備份
- 自動儲存管理 (ASM) 設定中的線上資料備份、線上完整備份、離線掛載備份和離線關機備份



如果多路徑設定檔中的 `user_friendly_names` 選項設定為 `yes`，則不支援 SAN 設定。



不支援克隆存檔日誌備份。

Oracle 資料庫支援的克隆類型

在 Oracle 資料庫環境中，SnapCenter 支援克隆資料庫備份。您可以從主儲存系統和輔助儲存系統複製備份。

SnapCenter 伺服器使用 NetApp FlexClone 技術來複製備份。

您可以透過執行“Refresh-SmClone”命令來刷新克隆。此命令會建立資料庫的備份，刪除現有的克隆，並建立同名的克隆。



克隆刷新操作只能使用 UNIX 指令執行。

Oracle 資料庫的克隆命名約定

從 SnapCenter 3.0 開始，檔案系統複製所使用的命名約定與 ASM 磁碟組的複製不同。

- SAN 或 NFS 檔案系統的命名約定是 `FileSystemNameofsourcedatabase_CLONESID`。
- ASM 磁碟組的命名約定是 `SC_HASHCODEofDISKGROUP_CLONESID`。

`HASHCODEofDISKGROUP` 是自動產生的數字（2 到 10 位數），每個 ASM 磁碟組都有唯一的 `HASHCODE`。

克隆 Oracle 資料庫的局限性

在克隆資料庫之前，您應該了解克隆操作的限制。

- 如果您使用的是 Oracle 11.2.0.4 至 12.1.0.1 中的任何版本，則執行 `renamedg` 指令時複製操作將處於暫停狀態。您可以套用 Oracle 補丁 19544733 來修復此問題。
- 不支援將資料庫從直接連接到主機의 LUN（例如，透過在 Windows 主機上使用 Microsoft iSCSI Initiator）複製到同一 Windows 主機或另一個 Windows 主機上的 VMDK 或 RDM LUN，反之亦然。
- 卷掛載點的根目錄不能是共享目錄。
- 如果將包含複製的 LUN 移至新磁碟區，則無法刪除該複製。

克隆特定處方和後記的預定義環境變量

SnapCenter 可讓您在複製資料庫時執行前腳本和後腳本時使用預先定義的環境變數。

支援用於克隆資料庫的預定義環境變數

- `SC_ORIGINAL_SID` 指定來源資料庫的 SID。

此參數將填入應用程式磁碟區。

例如：NFSB32

- **SC_ORIGINAL_HOST** 指定來源主機的名稱。

此參數將填入應用程式磁碟區。

例如：asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** 指定目標資料庫的 Oracle 主目錄的路徑。

範例：/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME** 指定備份的名稱。

此參數將填入應用程式磁碟區。

例子：

- 如果資料庫未以 ARCHIVELOG 模式運作：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_scspr2417819002_07-20-2021_12.
- 如果資料庫以 ARCHIVELOG 模式運作：DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG:RG2_scspr2417819002_07-20-2021_12.16.48.9267_1, RG2_scspr2417819002_07-21-2021_12.16.48.9267_1, RG2_scspr2417819002_07-22-2021_12.16.48.9267_8.9

- **SC_AV_NAME** 指定應用程式磁碟區的名稱。

範例：AV1|AV2

- **SC_ORIGINAL_OS_USER** 指定來源資料庫的作業系統擁有者。

範例：oracle

- **SC_ORIGINAL_OS_GROUP** 指定來源資料庫的作業系統群組。

範例：oinstall

- **SC_TARGET_SID** 指定複製資料庫的 SID。

對於 PDB 克隆工作流程，此參數的值將不會預先定義。

此參數將填入應用程式磁碟區。

範例：clonedb

- **SC_TARGET_HOST** 指定將複製資料庫的主機的名稱。

此參數將填入應用程式磁碟區。

例如：asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** 指定複製資料庫的作業系統擁有者。

對於 PDB 克隆工作流程，此參數的值將不會預先定義。

範例：oracle

- **SC_TARGET_OS_GROUP** 指定複製資料庫的作業系統群組。

對於 PDB 克隆工作流程，此參數的值將不會預先定義。

範例：oinstall

- **SC_TARGET_DB_PORT** 指定克隆資料庫的資料庫連接埠。

對於 PDB 克隆工作流程，此參數的值將不會預先定義。

例如：1521

有關分隔符號的信息，請參閱["支援的分隔符"](#)。

克隆 Oracle 資料庫的要求

在複製 Oracle 資料庫之前，您應該確保先決條件已完成。

- 您應該已經使用 SnapCenter 建立了資料庫的備份。

您應該已經成功建立了線上資料和日誌備份或離線（安裝或關閉）備份，複製操作才能成功。

- 如果要自訂控制檔或重做日誌檔案路徑，則應預先配置所需的檔案系統或自動儲存管理 (ASM) 磁碟組。

預設情況下，克隆資料庫的重做日誌和控制檔案會在 ASM 磁碟組或 SnapCenter 為克隆資料庫的資料檔案配置的檔案系統上建立。

- 如果您使用 NFS 上的 ASM，則應將 `/var/opt/snapcenter/scu/clones/*/*` 新增至 `asm_diskstring` 參數中定義的現有路徑。
- 在 `asm_diskstring` 參數中，如果使用 ASMFD，則應配置 `AFD:*`；如果使用 ASMLIB，則應配置 `ORCL:*`。

有關如何編輯 `asm_diskstring` 參數的信息，請參閱 ["如何將磁碟路徑新增至 `asm\_diskstring`"](#)。

- 如果要在備用主機上建立克隆，則備用主機應符合下列要求：
 - 應在備用主機上安裝適用於 Oracle 資料庫的 SnapCenter 插件。
 - 克隆主機應該能夠從主儲存或輔助儲存中發現 LUN。
 - 如果您要從主儲存或輔助（Vault 或映像）儲存複製到備用主機，請確保在輔助儲存和備用主機之間建立 iSCSI 會話，或針對 FC 正確劃分區域。
 - 如果要從 Vault 或映像儲存複製到相同主機，請確保在 Vault 或映像儲存與主機之間建立 iSCSI 會話，或針對 FC 正確劃分區域。
 - 如果在虛擬化環境中進行克隆，請確保在主儲存或輔助儲存與託管備用主機的 ESX 伺服器之間建立 iSCSI 會話，或針對 FC 進行正確分區。

有關信息，請參閱 ["主機實用程式文檔"](#)。

- 如果來源資料庫是 ASM 資料庫：

- ASM 執行個體應該會在將執行複製的主機上啟動並執行。
- 如果要將複製資料庫的存檔日誌檔案放置在專用 ASM 磁碟組中，則應在複製作業之前設定 ASM 磁碟組。
- 可以配置資料磁碟組的名稱，但請確保該名稱未被執行複製的主機上的任何其他 ASM 磁碟組使用。

駐留在 ASM 磁碟組上的資料檔案會作為 SnapCenter 克隆工作流程的一部分進行設定。

◦ 對於 NVMe，應安裝 NVMe util

- 資料 LUN 和日誌 LUN 的保護類型（例如鏡像、保管庫或鏡像保管庫）應該相同，以便在使用日誌備份複製到備用主機期間發現輔助定位器。
- 您應該在來源資料庫參數檔案中將 `exclude_seed_cdb_view` 的值設為 `FALSE`，以檢索用於複製 12_c_ 資料庫備份的種子 PDB 相關資訊。

種子 PDB 是系統提供的模板，CDB 可以使用它來建立 PDB。種子 PDB 名為 `PDB$SEED`。有關 `PDB$SEED` 的信息，請參閱 Oracle Doc ID 1940806.1。



您應該在備份 12_c_ 資料庫之前設定該值。

- SnapCenter 支援由 `autofs` 子系統管理的檔案系統的備份。如果要複製資料庫，請確保資料掛載點不在 `autofs` 掛載點的根目錄下，因為插件主機的根使用者沒有權限在 `autofs` 掛載點的根目錄下建立目錄。

如果控制和重做日誌檔案位於資料掛載點下，則應修改控制檔案路徑，然後相應地修改重做日誌檔案路徑。



您可以手動向 `autofs` 子系統註冊新的克隆掛載點。新克隆的掛載點不會自動註冊。

- 如果您有 TDE（自動登入）並希望在同一台或備用主機上複製資料庫，則應將 `/etc/ORACLE/WALLET/$ORACLE_SID` 下的錢包（金鑰檔案）從來源資料庫複製到複製的資料庫。
- 您應該在 `/etc/lvm/lvm.conf` 中設定 `use_lvmetad = 0` 的值並停止 `lvmetad` 服務，以便在 Oracle Linux 7 或更高版本或 Red Hat Enterprise Linux (RHEL) 7 或更高版本上的儲存區域網路 (SAN) 環境中成功執行複製。
- 如果您使用的是 Oracle 資料庫 11.2.0.3 或更高版本，並且使用 `NID` 腳本變更了輔助執行個體的資料庫 ID，則應安裝 13366202 Oracle 修補程式。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 對於 NVMe，如果必須排除任何目標連接埠的連接，則應在 `/var/opt/snapcenter/scu/etc/nvme.conf` 檔案中新增目標節點名稱和連接埠名稱。

如果該文件不存在，您應該按照以下範例所示建立該文件：

```
blacklist {
  nn-0x<target_node_name_1>:pn-0x<target_port_name_1>
  nn-0x<target_node_name_2>:pn-0x<target_port_name_2>
}
```

- 您應該確保 LUN 沒有使用由混合協定 iSCSI 和 FC 組成的 iGroup 對應到 AIX 主機。有關更多信息，請參閱 ["操作失敗，錯誤：無法發現 LUN 的設備"](#)。

克隆 Oracle 資料庫備份

您可以使用SnapCenter透過資料庫備份來克隆 Oracle 資料庫。

開始之前

如果您以非 root 使用者身分安裝了該插件，則應手動為 prescript 和 postscript 目錄指派執行權限。

關於此任務

- 複製操作會建立資料庫資料檔案的副本，並建立新的線上重做日誌檔案和控制檔。根據指定的復原選項，資料庫可以選擇性地還原到指定的時間。



如果您嘗試將在 Linux 主機上建立的備份複製到 AIX 主機或反之亦然，克隆將會失敗。

SnapCenter從 Oracle RAC 資料庫備份克隆時會建立一個獨立資料庫。SnapCenter支援從 Data Guard 備用資料庫和 Active Data Guard 備用資料庫的備份建立複製。

在複製期間，SnapCenter會根據 SCN 或日期和時間裝載最佳數量的日誌備份以進行復原作業。恢復後，日誌備份將被卸載。所有這些克隆都安裝在 `/var/opt/snapcenter/scu/clones/` 下。如果您使用 NFS 上的 ASM，則應將 `/var/opt/snapcenter/scu/clones/*/*` 新增至 `asm_diskstring` 參數中定義的現有路徑。

在 SAN 環境中複製 ASM 資料庫的備份時，將在 `/etc/udev/rules.d/999-scu-netapp.rules` 處建立複製主機裝置的 udev 規則。當您刪除複製時，與複製主機裝置關聯的這些 udev 規則也會被刪除。



在 Flex ASM 設定中，如果基數小於 RAC 叢集中的節點數，則無法在 Leaf 節點上執行複製操作。

- 對於啟用SnapLock的策略、對於ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從資料庫詳細資訊檢視或資源組詳細資料檢視中選擇資料庫。

進入資料庫拓撲頁面。

4. 從管理副本檢視中，從本機副本（主副本）、鏡像副本（次副本）或保管庫副本（次副本）中選擇備份。
5. 從表中選擇資料備份，然後按一下 。
6. 在名稱頁面中，執行下列其中一項操作：

如果你想...	步驟...
克隆資料庫（CDB 或非 CDB）	a. 指定克隆的 SID。 克隆SID預設不可用，SID最大長度為8個字元。  您應該確保將要建立克隆的主機上不存在具有相同 SID 的資料庫。
克隆可插拔資料庫（PDB）	a. 選擇*PDB 克隆*。 b. 指定要克隆的 PDB。 c. 指定克隆的 PDB 的名稱。有關克隆 PDB 的詳細步驟，請參閱"克隆可插入資料庫"。

當您選擇鏡像或保管資料時：

- 如果鏡像或保管庫中沒有日誌備份，則不會選擇任何內容，且定位器為空。
- 如果鏡像或保管庫中存在日誌備份，則選擇最新的日誌備份並顯示相應的定位器。



如果選定的日誌備份同時存在於鏡像和保管庫位置，則會顯示兩個定位器。

7. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
複製主機	預設情況下，來源資料庫主機已填入。 如果要在備用主機上建立克隆，請選擇與來源資料庫主機具有相同 Oracle 版本和作業系統的主機。

對於這個領域...	這樣做...
資料檔案位置	預設情況下，資料檔案位置已填入。 SnapCenter對 SAN 或 NFS 檔案系統的預設命名約定是 <code>FileSystemNameofsourcedatabase_CLONESID</code>。 SnapCenter 的ASM 磁碟組的預設命名約定是 <code>SC_HASHCODEofDISKGROUP_CLONESID</code>。 <code>HASHCODEofDISKGROUP</code> 是自動產生的數字（2 到 10 位數），每個 ASM 磁碟組都有其唯一性。  如果您要自訂 ASM 磁碟組名稱，請確保名稱長度符合 Oracle 支援的最大長度。 如果要指定不同的路徑，則必須輸入用於複製資料庫的資料檔案掛載點或 ASM 磁碟組名稱。自訂資料檔案路徑時，也必須將控制檔案和重做日誌檔案 ASM 磁碟群組名稱或檔案系統變更為與資料檔案相同的名稱，或變更為現有的 ASM 磁碟群組或檔案系統。
控制文件	預設情況下，控制檔案路徑被填入。 控制檔案與資料檔案放在同一個 ASM 磁碟組或檔案系統中。如果要覆寫控制檔路徑，可以提供不同的控制檔路徑。  檔案系統或 ASM 磁碟組應該存在於主機上。 預設情況下，控制文件的數量與來源資料庫的數量相同。您可以修改控制文件的數量，但克隆資料庫至少需要一個控制文件。 您可以將控制檔案路徑自訂為與來源資料庫不同的檔案系統（現有）。

對於這個領域...	這樣做...
重做日誌	預設情況下，重做日誌檔案群組、路徑及其大小均已填入。 重做日誌與複製資料庫的資料檔案放在同一個 ASM 磁碟組或檔案系統中。如果要覆寫重做日誌檔案路徑，則可以將重做日誌檔案路徑自訂為與來源資料庫不同的檔案系統。  新的檔案系統或 ASM 磁碟組應該存在於主機上。 預設情況下，重做日誌組、重做日誌檔案的數量及其大小與來源資料庫相同。您可以修改以下參數： - 重做日誌組的數量  克隆資料庫至少需要兩個重做日誌組。 - 各組重做日誌檔及其路徑 您可以將重做日誌檔案路徑自訂為與來源資料庫不同的檔案系統（現有）。  重做日誌組中至少需要一個重做日誌檔來克隆資料庫。 - 重做日誌檔的大小

8. 在「憑證」頁面上，執行以下操作：

對於這個領域...	這樣做...
sys 使用者的憑證名稱	選擇用於定義克隆資料庫的系統使用者密碼的憑證。 如果目標主機上的 sqlnet.ora 檔案中的 SQLNET.AUTHENTICATION_SERVICES 設定為 NONE，則不應在 SnapCenter GUI 中選擇 None 作為憑證。
ASM 實例憑證名稱	如果啟用了 OS 驗證來連線到複製主機上的 ASM 實例，請選擇 無。 否則，請選擇使用「sys」使用者或具有適用於複製主機的「sysasm」權限的使用者配置的 Oracle ASM 憑證。

Oracle 主目錄、使用者名稱和群組詳細資訊將從來源資料庫自動填入。您可以根據將建立複製的主機的 Oracle 環境變更這些值。

9. 在 PreOps 頁面中，執行下列步驟：

- a. 輸入要在克隆操作之前運行的處方的路徑和參數。

您必須將處方儲存在 `/var/opt/snapcenter/spl/scripts` 或此路徑內的任何資料夾中。預設情況下，填入 `/var/opt/snapcenter/spl/scripts` 路徑。如果您已將腳本放在此路徑內的任何資料夾中，則需要提供放置腳本的資料夾的完整路徑。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

- b. 在資料庫參數設定部分，修改用於初始化資料庫的預填資料庫參數的值。

您可以透過點擊 * 新增其他參數  *。

如果您使用的是 Oracle 標準版，且資料庫在存檔日誌模式下執行，或者您想要從存檔重做日誌還原資料庫，請新增參數並指定路徑。

- 日誌歸檔目標
- LOG_ARCHIVE_DUPLEX_DEST



預先填入的資料庫參數中未定義快速恢復區 (FRA)。您可以透過新增相關參數來配置 FRA。



`log_archive_dest_1` 的預設值是 `$ORACLE_HOME/clone_sid`，克隆資料庫的存檔日誌將在此位置建立。如果您刪除了 `log_archive_dest_1` 參數，則存檔日誌位置由 Oracle 決定。您可以透過編輯 `log_archive_dest_1` 來定義存檔日誌的新位置，但請確保檔案系統或磁碟組存在並在主機上可用。

- a. 按一下“重設”以取得預設資料庫參數設定。

10. 在 PostOps 頁面中，預設選擇 *Recover database* 和 *Until Cancel* 來執行克隆資料庫的復原。

SnapCenter 透過在選擇進行複製的資料備份之後安裝具有完整存檔日誌序列的最新日誌備份來執行復原。日誌和資料備份應在主儲存體上以便在主儲存體上執行克隆，且日誌和資料備份應在輔助儲存體上以便在輔助儲存體上執行複製。

如果 SnapCenter 無法找到適當的日誌備份，則不會選擇「還原資料庫」和「直到取消」選項。如果「指定外部存檔日誌位置」中沒有日誌備份，您可以提供外部存檔日誌位置。您可以指定多個日誌位置。



如果要複製配置為支援閃回復原區 (FRA) 和 Oracle 管理檔案 (OMF) 的來源資料庫，則復原的日誌目標也必須遵循 OMF 目錄結構。

如果來源資料庫是 Data Guard 備用資料庫或 Active Data Guard 備用資料庫，則不會顯示 PostOps 頁面。對於 Data Guard 備用資料庫或活動 Data Guard 備用資料庫，SnapCenter 不提供在 SnapCenter GUI 中選擇恢復類型的選項，但資料庫使用「直到取消」恢復類型進行恢復，而不套用任何日誌。

欄位名稱	描述
直到取消	SnapCenter透過在選擇進行複製的資料備份之後安裝具有完整存檔日誌序列的最新日誌備份來執行復原。克隆的資料庫恢復到遺失或損壞的日誌檔案。
日期和時間	SnapCenter將資料庫還原到指定的日期和時間。接受的格式是 mm/dd/yyyy hh:mm:ss。  時間可以 24 小時格式指定。
直到 SCN（系統變更號）	SnapCenter將資料庫還原到指定的系統變更號碼 (SCN)。
指定外部歸檔日誌位置	如果資料庫在 ARCHIVELOG 模式下執行，SnapCenter會根據指定的 SCN 或選取的日期和時間識別並安裝最佳數量的日誌備份。 您也可以指定外部存檔日誌位置。  如果您選擇了“直到取消”，SnapCenter將不會自動識別和安裝日誌備份。
建立新的 DBID	預設情況下，勾選「建立新 DBID」複選框，為複製的資料庫產生一個唯一的編號 (DBID)，以區別於來源資料庫。 如果要將來源資料庫的 DBID 指派給複製的資料庫，請清除該核取方塊。在這種情況下，如果您想將複製的資料庫註冊到來源資料庫已註冊的外部 RMAN 目錄，則操作會失敗。
為臨時表空間建立臨時文件	如果要為克隆資料庫的預設臨時表空間建立臨時文件，請選取該複選框。 如果未選取該複選框，則將建立不含臨時檔案的資料庫克隆。
輸入建立複製時要套用的 SQL 條目	新增建立克隆時要套用的 SQL 條目。

欄位名稱	描述
輸入克隆操作後運行的腳本	指定克隆操作後要運行的後記的路徑和參數。 您應該將後記儲存在 <code>/var/opt/snapcenter/spl/scripts</code> 中或此路徑內的任何資料夾中。預設情況下，填入 <code>/var/opt/snapcenter/spl/scripts</code> 路徑。 如果您已將腳本放在此路徑內的任何資料夾中，則需要提供放置腳本的資料夾的完整路徑。  如果克隆操作失敗，則不會執行後記，直接觸發清理活動。

11. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtptServer` 指定 SMTP 伺服器詳細資訊。

12. 查看摘要，然後按一下「完成」。



在執行複製建立作業中的復原時，即使復原失敗，也會建立複製並發出警告。您可以對此克隆執行手動恢復，以使克隆資料庫達到一致狀態。

13. 透過點選「監視」>「作業」來監視操作進度。

結果

複製資料庫後，您可以刷新資源頁面，將複製的資料庫列為可供備份的資源之一。複製的資料庫可以像任何其他資料庫一樣使用標準備份工作流進行保護，也可以包含在資源組（新建或現有）中。克隆的資料庫可以進一步克隆（克隆的克隆）。

克隆後，您永遠不應重命名克隆的資料庫。



如果在克隆時沒有執行恢復，則克隆資料庫的備份可能會因恢復不當而失敗，並且您可能必須執行手動恢復。如果存檔日誌的預設位置位於非NetApp儲存體上，或儲存系統未配置SnapCenter，則日誌備份也可能會失敗。

在 AIX 設定中，您可以使用 `lkdev` 指令鎖定並使用 `rendev` 指令重命名複製資料庫所在的磁碟。

鎖定或重新命名裝置不會影響複製刪除操作。對於在 SAN 設備上建置的 AIX LVM 佈局，不支援對克隆的 SAN 設備進行設備重新命名。

查找更多資訊

- ["恢復或複製失敗並出現 ORA-00308 錯誤訊息"](#)

- "無法恢復克隆的資料庫"
- "AIX 系統上備份、還原和克隆作業的可自訂參數"

更新主機上的首選 IP

複製作業完成後，儲存存取層 (SAL) 提供給複製的路徑將採用 `<nfs_lif_IP>:<JunctionPath>` 格式。若要提供首選 IP，您必須使用 SCCLI 命令在主機上對其進行設定。

步驟

1. 登入資料庫主機。
2. 為指定使用者啟動與 SnapCenter 的 PowerShell 連線會話。

開放簡訊連接

3. 建立一個空文件。

觸摸 `/var/opt/snapcenter/scu/etc/storagepreference.properties`

4. 為 SVM 配置首選資料 LIF。

`Add-SvmPreferredDataPath -SVM <SVM 名稱> -DataPath <IP 位址或 FQDN>`

5. 驗證首選路徑。

取得 `SvmPreferredDataPath`

克隆可插入資料庫

您可以將可插拔資料庫 (PDB) 複製到同一主機或備用主機上不同或相同的目標 CDB。您也可以將克隆的 PDB 還原到所需的 SCN 或日期和時間。

開始之前

如果您以非 root 使用者身分安裝了該插件，則應手動為 `prescript` 和 `postscript` 目錄指派執行權限。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 從資料庫詳細資料檢視或資源群組詳細資料檢視中選擇單一實例（多租用戶）類型的資料庫。

進入資料庫拓撲頁面。

4. 從管理副本檢視中，從本機副本（主副本）、鏡像副本（次副本）或保管庫副本（次副本）中選擇備份。
5. 從表格中選擇備份，然後按一下**。
6. 在名稱頁面中，執行以下操作：
 - a. 選擇*PDB 克隆*。

b. 指定要克隆的 PDB。



一次只能克隆一個 PDB。

c. 指定克隆 PDB 的名稱。

7. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
複製主機	預設情況下，來源資料庫主機已填入。 如果要在備用主機上建立克隆，請選擇與來源資料庫主機具有相同 Oracle 版本和作業系統的主機。
目標 CDB	選擇要包含克隆的 PDB 的 CDB。 您應該確保目標 CDB 正在運作。
資料庫狀態	如果您想以讀寫模式開啟 PDB，請選取*以讀寫模式開啟複製的 PDB*複選框。
資料檔案位置	預設情況下，資料檔案位置已填入。 SnapCenter對 SAN 或 NFS 檔案系統的預設命名約定是 FileSystemNameofsourcedatabase_SCJOBID。 SnapCenter 的ASM 磁碟組預設命名約定是 SC_HASHCODEofDISKGROUP_SCJOBID。 HASHCODEofDISKGROUP 是自動產生的數字（2 到 10 位數），每個 ASM 磁碟組都有其唯一性。  如果您要自訂 ASM 磁碟組名稱，請確保名稱長度符合 Oracle 支援的最大長度。 如果要指定不同的路徑，則必須輸入用於複製資料庫的資料檔案掛載點或 ASM 磁碟組名稱。

Oracle 主目錄、使用者名稱和群組詳細資訊將從來源資料庫自動填入。您可以根據將建立複製的主機的 Oracle 環境變更這些值。

8. 在 PreOps 頁面中，執行下列步驟：

a. 輸入要在克隆操作之前運行的處方的路徑和參數。

您應該將處方儲存在 /var/opt/snapcenter/spl/scripts 或此路徑內的任何資料夾中。預設情況下，填入 /var/opt/snapcenter/spl/scripts 路徑。如果您已將腳本放在此路徑內的任何資料夾中，則需要提供放置腳本的資料夾的完整路徑。

SnapCenter可讓您在執行前腳本和後腳本時使用預先定義的環境變數。["了解更多"](#)

- a. 在輔助 CDB 克隆資料庫參數設定部分，修改用於初始化資料庫的預先填入資料庫參數的值。
9. 按一下“重設”以取得預設資料庫參數設定。
10. 在 PostOps 頁面中，預設選擇 **Until Cancel** 來執行複製資料庫的復原。

如果SnapCenter無法找到適當的日誌備份，則不會選擇「直到取消」選項。如果「指定外部存檔日誌位置」中沒有日誌備份，您可以提供外部存檔日誌位置。您可以指定多個日誌位置。



如果要複製配置為支援閃回復原區 (FRA) 和 Oracle 管理檔案 (OMF) 的來源資料庫，則復原的日誌目標也必須遵循 OMF 目錄結構。

欄位名稱	描述
直到取消	SnapCenter透過在選擇進行複製的資料備份之後安裝具有完整存檔日誌序列的最新日誌備份來執行復原。 日誌和資料備份應在主儲存體上以便在主儲存體上執行克隆，且日誌和資料備份應在輔助儲存體上以便在輔助儲存體上執行複製。克隆的資料庫恢復到遺失或損壞的日誌檔案。
日期和時間	SnapCenter將資料庫還原到指定的日期和時間。  時間可以 24 小時格式指定。
直到 SCN（系統變更號）	SnapCenter將資料庫還原到指定的系統變更號碼 (SCN)。
指定外部歸檔日誌位置	指定外部存檔日誌位置。
建立新的 DBID	預設情況下，輔助複製資料庫的「建立新 DBID」複選框未選取。 如果要為輔助複製資料庫產生一個唯一編號（DBID）以區別於來源資料庫，請選取此核取方塊。
為臨時表空間建立臨時文件	如果要為克隆資料庫的預設臨時表空間建立臨時文件，請選取該複選框。 如果未選取該複選框，則將建立不含臨時檔案的資料庫克隆。
輸入建立複製時要套用的 SQL 條目	新增建立克隆時要套用的 SQL 條目。

欄位名稱	描述
輸入克隆操作後運行的腳本	指定克隆操作後要運行的後記的路徑和參數。 您應該將後記儲存在 <code>/var/opt/snapcenter/spl/scripts</code> 中或此路徑內的任何資料夾中。 預設情況下，填入 <code>/var/opt/snapcenter/spl/scripts</code> 路徑。如果您已將腳本放在此路徑內的任何資料夾中，則需要提供放置腳本的資料夾的完整路徑。  如果克隆操作失敗，則不會執行後記，直接觸發清理活動。

11. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtServer` 指定 SMTP 伺服器詳細資訊。

12. 查看摘要，然後按一下「完成」。
13. 透過點選「監視」>「作業」來監視操作進度。

完成後

如果要建立克隆的 PDB 的備份，則應該備份克隆 PDB 的目標 CDB，因為僅備份克隆的 PDB 是不可能的。如果您想要建立具有輔助關係的備份，則應該為目標 CDB 建立輔助關係。

在 RAC 設定中，克隆 PDB 的儲存僅附加到執行 PDB 克隆的節點。RAC 其他節點上的 PDB 處於 MOUNT 狀態。如果您希望克隆的 PDB 可從其他節點訪問，則應手動將儲存空間附加到其他節點。

查找更多資訊

- ["恢復或複製失敗並出現 ORA-00308 錯誤訊息"](#)
- ["AIX 系統上備份、還原和克隆作業的可自訂參數"](#)

使用 UNIX 指令克隆 Oracle 資料庫備份

克隆工作流程包括規劃、執行複製操作和監控操作。

關於此任務

您應該執行以下命令來建立 Oracle 資料庫克隆規範檔案並啟動克隆操作。

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體命令參考指南"](#)。

步驟

1. 從指定備份建立 Oracle 資料庫複製規格：*New-SmOracleCloneSpecification*



如果二級資料保護策略是統一鏡像保管庫，則僅指定 `-IncludeSecondaryDetails`。您不必指定 `-SecondaryStorageType`。

此命令會自動為指定的來源資料庫及其備份建立 Oracle 資料庫克隆規範檔案。您還必須提供複製資料庫 SID，以便建立的規格文件具有您將要建立的複製資料庫的自動產生的值。



克隆規範檔案在 `/var/opt/snapcenter/sco/clone_specs` 處建立。

2. 從複製資源群組或現有備份啟動複製作業：*New-SmClone*

此命令啟動克隆操作。您還必須為克隆操作提供 Oracle 克隆規範文件路徑。您還可以指定復原選項、要執行複製操作的主機、處方、後記和其他詳細資訊。

預設情況下，複製資料庫的存檔日誌目標檔案會自動填入 `$_ORACLE_HOME/CLONE_SIDs_`。

拆分 Oracle 資料庫克隆

您可以使用 SnapCenter 將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建 clone2 後，clone1 為中間克隆，無法對 clone1 進行克隆分裂操作。但是可以對 clone2 進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您分割複製時，複製的備份副本將會被刪除。
- 有關 FlexClone 磁碟區拆分操作的信息，請參閱 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> [將 FlexClone 磁碟區從其父卷中拆分出來]
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。
3. 選擇克隆的資源（例如資料庫或 LUN），然後按一下 .
4. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
5. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCORE 服務重新啟動且執行複製分割作業的資料庫在資源頁面中列為克隆，則複製分割作業將停止回應。您應該執行 `Stop-SmJob` cmdlet 來停止複製分割操作，然後重試複製分割操作。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 `SMCoreServiceHost.exe.config` 檔案中 `CloneSplitStatusCheckPollTime` 參數的值來設定 `SMCore` 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為5分鐘。

例如，

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```



如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

可插拔資料庫的拆分克隆

您可以使用 SnapCenter 拆分克隆的可插拔資料庫 (PDB)。

關於此任務

如果您建立了複製 PDB 的目標 CDB 的備份，則當您分割 PDB 複製時，複製的 PDB 也會從包含複製 PDB 的目標 CDB 的所有備份中刪除。



PDB 克隆未顯示在庫存或資源視圖中。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 從資源或資源組視圖中選擇來源容器資料庫 (CDB)。
3. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或複製）中選擇「複製」。
4. 選擇 PDB 克隆（targetCDB：PDBClone），然後按一下 。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

監視 Oracle 資料庫克隆操作

您可以使用「作業」頁面監控 SnapCenter 複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-

 已完成但有警告，或因警告而無法啟動

-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

刷新克隆

您可以透過執行 `_Refresh-SmClone_` 命令來刷新克隆。此命令會建立資料庫的備份，刪除現有的克隆，並建立同名的克隆。



您無法刷新 PDB 克隆。

您需要什麼

- 建立線上完整備份或離線資料備份策略，不啟用任何排程備份。
- 僅為備份失敗配置策略中的電子郵件通知。
- 適當定義按需備份的保留計數，以確保沒有不必要的備份。
- 確保只有線上完整備份或離線資料備份策略與已確定用於刷新克隆作業的資源群組相關聯。
- 建立只有一個資料庫的資源組。
- 如果為複製刷新指令建立了 cron 作業，請確保 SnapCenter 計畫和 cron 計畫與資料庫資源組不重疊。

對於為克隆刷新命令建立的 cron 作業，請確保每 24 小時執行一次 `Open-SmConnection`。

- 確保克隆 SID 對於主機來說是唯一的。

如果多個刷新克隆操作使用相同的克隆規範文件或使用具有相同克隆 SID 的克隆規範文件，則主機上具有該 SID 的現有克隆將被刪除，然後創建克隆。

- 確保備份策略啟用了二級保護，並使用“-IncludeSecondaryDetails”建立克隆規範文件，以使用二級備份建立克隆。

- 如果指定了主克隆規範文件，但策略選擇了輔助更新選項，則將建立備份，並將更新傳輸到輔助。但是，克隆將從主備份建立。
- 如果指定了主複製規範文件，且策略未選擇輔助更新選項，則會在主伺服器上建立備份，並從主伺服器建立複製。

步驟

1. 為指定使用者啟動與SnapCenter伺服器的連線會話：*Open-SmConnection*
2. 從指定備份建立 Oracle 資料庫複製規格：*New-SmOracleCloneSpecification*



如果二級資料保護策略是統一鏡像保管庫，則僅指定-IncludeSecondaryDetails。您不必指定-SecondaryStorageType。

此命令會自動為指定的來源資料庫及其備份建立 Oracle 資料庫克隆規範檔案。您還必須提供複製資料庫 SID，以便建立的規格文件具有您將要建立的複製資料庫的自動產生的值。



克隆規範檔案在 `/var/opt/snapcenter/sco/clone_specs` 處建立。

3. 運行 `_Refresh-SmClone_`。

如果操作失敗並出現「PL-SCO-20032：canExecute 操作失敗，錯誤：PL-SCO-30031：重做日誌檔案 +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log 存在」錯誤訊息，請為 `rig-WaitTT` 為 `rig-WaitToTger` 指定更高的值。

有關 UNIX 命令的詳細信息，請參閱 "[SnapCenter軟體命令參考指南](#)"。

刪除可插入資料庫的克隆

如果不再需要可插拔資料庫 (PDB) 的克隆，您可以刪除它。

如果您建立了複製 PDB 的目標 CDB 的備份，則當您刪除 PDB 複製時，複製的 PDB 也會從目標 CDB 的備份中刪除。



PDB 克隆未顯示在庫存或資源視圖中。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 從資源或資源組視圖中選擇來源容器資料庫 (CDB)。
3. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或複製）中選擇「複製」。
4. 選擇 PDB 克隆（`targetCDB`：PDBClone），然後按一下 。
5. 按一下“確定”。

管理應用程式捲

什麼是應用卷

應用程式磁碟區是儲存配置、安裝程式和其他與 Oracle 資料庫相關的非資料檔案等資訊的儲存空間。

Oracle 資料庫的 SnapCenter 插件可讓您與 Oracle 資料庫一起建立應用程式磁碟區（非資料磁碟區）的一致備份。

該外掛程式可自動執行應用程式磁碟區的備份和複製。

- 在單一資源群組中保護應用程式磁碟區以及 Oracle 資料庫磁碟區。
- 建立應用程式捲的備份。
- 建立 Oracle 資料庫以及應用程式磁碟區的備份。
- 建立資料庫的克隆以及某個時間點的應用程式磁碟區。
- 安排備份作業。
- 監控所有操作。
- 查看備份和克隆作業的報告。

新增應用程式捲

SnapCenter 支援 Oracle 資料庫應用程式磁碟區的備份和複製。您應該手動新增應用程式捲。不支援自動發現應用程式捲。



應用程式磁碟區僅支援直接 NFS 和直接 iSCSI 連線。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 按一下“新增應用程式磁碟區”。
3. 在名稱頁面中，執行以下操作：
 - 在名稱欄位中，輸入應用程式磁碟區的名稱。
 - 在主機名字段中，輸入主機的名稱。
4. 在「儲存佔用空間」頁面中，輸入儲存系統名稱，選擇一個或多個磁碟區，並指定關聯的 LUN 或 qtree。

您可以新增多個儲存系統。

5. 查看摘要，然後按一下「完成」。
6. 在資源頁面中，從*查看*清單中選擇*應用程式磁碟區*，查看已新增的所有應用程式磁碟區。

修改應用程式音量

如果沒有建立備份，您可以修改新增應用程式磁碟區時指定的所有值。如果建立了備份，則只能修改儲存系統詳細資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3.  點選  修改值。
4.  點選  修改值。

刪除應用程式捲

當您刪除應用程式磁碟區時，如果有任何與該應用程式磁碟區關聯的備份，則該應用程式磁碟區將進入維護模式，不會建立新的備份，也不會保留任何早期的備份。如果沒有相關備份，所有元資料將被刪除。

如果需要，SnapCenter允許您撤銷刪除操作。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3. 點選  選擇圖示]來修改值。

備份應用程式捲

備份應用程式捲

如果應用程式磁碟區不屬於任何資源群組，您可以從資源頁面備份該應用程式磁碟區。

關於此任務

預設情況下，會建立一致性群組 (CG) 備份。如果您想要建立基於磁碟區的備份，您應該在 *web.config* 檔案中將 **EnableOracleNdvVolumeBasedBackup** 的值設為 true。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3. 點擊  *，然後選擇主機名稱和資料庫類型來過濾資源。

然後您可以點擊  * 關閉篩選窗格。

4. 選擇要備份的應用程式磁碟區。

將顯示應用程式磁碟區保護頁面。

5. 在資源頁面中，執行以下操作：

對於這個領域...	這樣做...
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如，customtext__policy_hostname 或 resource_hostname。預設情況下，時間戳記會附加到快照名稱。
從備份中排除存檔日誌目標	指定您不想備份的存檔日誌檔案的目標。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊  來建立策略。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計畫的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源執行的備份作業的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

8. 查看摘要，然後按一下「完成」。

進入應用程式捲拓撲頁面。

9. 點選*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您已對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。
- b. 按一下“備份”。

11. 透過點選「監視」>「作業」來監視操作進度。

備份應用程式捲資源組

您可以備份僅包含應用程式磁碟區或包含應用程式磁碟區和資料庫的混合的資源群組。資源組上的備份作業會針對資源組中定義的所有資源執行。

如果資源組有多個應用程式捲，則所有應用程式磁碟區都應具有SnapMirror或SnapVault複製策略。

關於此任務

預設情況下，會建立一致性群組 (CG) 備份。如果您想要建立基於磁碟區的備份，您應該在 `web.config` 檔案中將 **EnableOracleNdvVolumeBasedBackup** 的值設為 `true`。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或按一下 * 來搜尋資源組  *，然後選擇標籤。然後您可以點擊 *  * 關閉篩選窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後按一下「立即備份」。
4. 在備份頁面中，執行以下步驟：
 - a. 如果您已將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。
5. 透過點選「監視」>「作業」來監視操作進度。



驗證操作僅針對資料庫執行，而不是針對應用程式磁碟區執行。

克隆應用程式捲備份

您可以使用SnapCenter克隆應用程式磁碟區備份。

開始之前

如果您以非 root 使用者身分安裝了該插件，則應手動為 `prescript` 和 `postscript` 目錄指派執行權限。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3. 從應用程式磁碟區詳細資料檢視或資源群組詳細資料檢視中選擇應用程式磁碟區。

進入應用程式捲拓撲頁面。

4. 從管理副本檢視中，從本機副本（主副本）、鏡像副本（次副本）或保管庫副本（次副本）中選擇備份。
5. 從表格中選擇備份，然後按一下*  *。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
插件主機	選擇要建立克隆的主機。
目標資源名稱	指定資源名稱。

7. 在腳本頁面中，指定複製前要執行的腳本的名稱、掛載檔案系統的命令、複製後要執行的腳本的名稱。
8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

9. 查看摘要，然後按一下「完成」。

拆分應用程式捲克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3. 選擇克隆的資源並點擊 。
4. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
5. 透過點選「監視」>「作業」來監視操作進度。

刪除應用程式捲克隆

如果您發現克隆不再需要，您可以刪除它們。您無法刪除充當其他克隆來源的克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Oracle 資料庫外掛程式。
2. 在資源頁面中，從*檢視*清單中選擇*應用程式磁碟區*。
3. 從清單中選擇資源或資源組。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或複製）中選擇「複製」。
5. 選擇克隆，然後按一下 。
6. 在刪除克隆頁面中，執行以下操作：
 - a. 在*Pre clone delete*欄位中，輸入在刪除複製之前要執行的腳本的名稱。
 - b. 在 **Unmount** 欄位中，輸入刪除克隆之前卸載克隆的命令。
7. 按一下“確定”。

保護 Windows 檔案系統

適用於 Microsoft Windows 的SnapCenter外掛概念

適用於 Microsoft Windows 的SnapCenter外掛程式概述

適用於 Microsoft Windows 的SnapCenter外掛程式是NetApp SnapCenter軟體的主機端元件，可實現 Microsoft 檔案系統資源的應用程式感知資料保護管理。此外，它還為 Windows 檔案系統提供儲存配置、快照一致性和空間回收。適用於 Windows 的外掛程式可在您的SnapCenter環境中自動執行檔案系統備份、復原和複製作業。

安裝適用於 Windows 的插件後，您可以將SnapCenter與NetApp SnapMirror技術結合使用，在另一個磁碟區上建立備份集的鏡像副本，並使用NetApp SnapVault技術執行磁碟到磁碟的備份複製，以滿足存檔或標準合規性。

- 為SnapCenter環境中 Windows 主機中執行的其他外掛程式啟用應用程式感知資料保護
- 自動執行SnapCenter環境中 Microsoft 檔案系統的應用程式感知備份、還原和複製作業
- 支援 Windows 主機的儲存配置、快照一致性和空間回收



Windows 外掛程式在實體和 RDM LUN 上設定 SMB 共用和 Windows 檔案系統，但不支援對 SMB 共用上的 Windows 檔案系統進行備份作業。

您可以使用適用於 Microsoft Windows 的SnapCenter外掛程式做什麼

當您的環境中安裝了適用於 Windows 的插件後，您可以使用SnapCenter備份、還原和複製 Windows 檔案系統。您也可以執行支援這些操作的任務。

- 發現資源
- 備份 Windows 檔案系統
- 安排備份作業
- 恢復檔案系統備份
- 克隆檔案系統備份
- 監控備份、復原和複製操作



Windows 外掛程式不支援 SMB 共用上的檔案系統的備份和還原。

適用於 Windows 的SnapCenter插件功能

Windows 插件與儲存系統上的NetApp Snapshot 技術整合。若要使用適用於 Windows 的插件，您需要使用SnapCenter介面。

Windows 外掛程式包括以下主要功能：

- 由**SnapCenter**提供支援的統一圖形使用者介面

SnapCenter介面為您提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份和復原流程、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以及監控所有外掛程式中的作業。SnapCenter還提供集中調度和策略管理以支援備份和複製作業。

- 自動化中央管理

您可以安排例行檔案系統備份、設定基於政策的備份保留以及設定復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的檔案系統環境。

- 無中斷**NetApp Snapshot** 技術

Windows 插件使用NetApp Snapshot 技術。這使您能夠在幾秒鐘內備份檔案系統並快速恢復它們，而無需使主機離線。快照佔用的儲存空間極小。

除了這些主要功能外，Windows 外掛還提供以下優點：

- 備份、還原和克隆工作流程支持
- RBAC 支援的安全性和集中角色委派
- 使用NetApp FlexClone技術建立生產檔案系統的空間高效副本，用於測試或資料擷取

有關FlexClone許可信息，請參閱["SnapCenter許可證"](#)。

- 能夠在多台伺服器上同時執行多個備份
- 用於編寫備份、還原和複製作業腳本的 PowerShell cmdlet
- 支援檔案系統和虛擬機器磁碟 (VMDK) 的備份
- 支援實體和虛擬化基礎設施
- 支援 iSCSI、光纖通道、FCoE、原始裝置對映 (RDM)、非對稱 LUN 對映 (ALM)、NFS 和 VMFS 上的 VMDK 以及虛擬 FC
- Windows Server 2022 支援非揮發性記憶體快速 (NVMe)
 - 在 TCP/IP 上的 NVMe 上建立的 VMDK 佈局的備份、復原、複製和驗證工作流程。
 - 從 ESX 8.0 update 2 開始支援 NVMe 韌體版本 1.3，並且需要虛擬硬體版本 21。
 - NVMe over TCP/IP 上的 VMDK 應用程式不支援 Windows Server 故障轉移叢集 (WSFC)。
- 支援SnapMirror主動同步（最初作為SnapMirror業務連續性 [SM-BC] 發布），即使整個網站發生故障，也能使業務服務繼續運行，支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過SnapMirror主動同步觸發故障轉移。

SnapCenter如何備份 Windows 檔案系統

SnapCenter使用 Snapshot 技術備份駐留在 LUN、CSV（叢集共用磁碟區）、RDM（原始裝置對應）磁碟區、Windows 叢集中的 ALM（非對稱 LUN 對應）以及基於 VMFS/NFS（使用 NFS 的 VMware 虛擬機器檔案系統）的 VMDK 上的 Windows 檔案系統資源。

SnapCenter透過建立檔案系統的快照來建立備份。聯合備份（其中一個磁碟區包含來自多個主機的 LUN）比每個單獨的 LUN 的備份更快、更有效率，因為與每個檔案系統的單獨快照相比，只建立磁碟區的一個快照。

當SnapCenter建立快照時，整個儲存系統磁碟區都會被擷取到快照中。但是，備份僅對建立備份的主機伺服器有效。

如果其他主機伺服器的資料駐留在同一磁碟區上，則無法從快照還原該資料。



如果 Windows 檔案系統包含資料庫，那麼備份檔案系統與備份資料庫不同。要備份資料庫，您必須使用其中一個資料庫外掛程式。

SnapCenter Plug-in for Microsoft Windows 支援的儲存類型

SnapCenter支援實體機器和虛擬機器上的多種儲存類型。在為您的主機安裝軟體包之前，您必須驗證您的儲存類型是否受支援。

Windows Server 上提供SnapCenter設定和資料保護支援。有關受支援版本的最新信息，請參閱[https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT\[\"NetApp互通性表工具\"\]](https://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT[\)。

機器	儲存類型	使用配置	支援說明
實體伺服器	FC 連接的 LUN	SnapCenter圖形使用者介面 (GUI) 或 PowerShell cmdlet	
實體伺服器	iSCSI 連接的 LUN	SnapCenter GUI 或 PowerShell cmdlet	
實體伺服器	駐留在儲存虛擬機器 (SVM) 上的 SMB3 (CIFS) 共用	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。
VMware VM	透過 FC 或 iSCSI HBA 連接的 RDM LUN	PowerShell cmdlet	
VMware VM	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	
VMware VM	虛擬機器檔案系統 (VMFS) 或 NFS 資料存儲	VMware vSphere	
VMware VM	連接到 SVM 上的 SMB3 共享的客戶系統	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。
VMware VM	NFS 和 SAN 上的 vVol 資料存儲	適用於 VMware vSphere 的ONTAP工具	

機器	儲存類型	使用配置	支援說明
Hyper-V 虛擬機	透過虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN	SnapCenter GUI 或 PowerShell cmdlet	您必須使用 Hyper-V 管理員來設定由虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN。  不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。
Hyper-V 虛擬機	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	 不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。
Hyper-V 虛擬機	連接到 SVM 上的 SMB3 共享的客戶系統	SnapCenter GUI 或 PowerShell cmdlet	僅支援配置。  不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。

Windows 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止

- 倫
- lun 創建
- lun 刪除
- lun igroup 新增
- lun igroup 創建
- lun igroup 刪除
- lun igroup 重新命名
- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun 映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun 修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始

- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線
- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示

- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面
 - 網路介面顯示
 - 虛擬伺服器

為SnapMirror和SnapVault複製準備儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

定義 Windows 檔案系統的備份策略

在建立備份之前定義備份策略可為您提供成功復原或複製檔案系統所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

Windows 檔案系統的備份計劃

備份頻率在策略中指定；備份計畫在資源組配置中指定。確定備份頻率或計劃的最關鍵因素是資源的變化率和資料的重要性。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次不常用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA 和 RPO 有助於資料保護策略。

即使是使用頻繁的資源，也不需要每天執行一次或兩次以上的完整備份。

備份計畫分為兩部分，如下所示：

- 備份頻率

備份頻率（執行備份的頻率），對於某些外掛程式來說稱為 *計畫類型*，是策略配置的一部分。例如，您可以將備份頻率配置為每小時、每天、每週或每月，或者您可以指定 **None**，這使該策略成為僅按需策略。您可以透過點選「設定」>「策略」來存取策略。

- 備份計畫

備份計畫（確切地指定執行備份的時間）是資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份。您可以透過點選「資源」>「資源群組」來存取資源組計畫。

Windows 檔案系統所需的備份數量

決定所需備份數量的因素包括 Windows 檔案系統的大小、使用的磁碟區數、檔案系統的變化率以及您的服務等級協定 (SLA)。

Windows 檔案系統的備份命名約定

Windows 檔案系統備份使用預設的快照命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：`resourcegroupname_hostname_timestamp`

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- ``dts1`` 是資源組名稱。
- ``mach1x88`` 是主機名稱。
- ``03-12-2016_23.17.26`` 是日期和時間戳。

建立備份時，您也可以新增描述性標籤來協助識別備份。相反，如果您想使用自訂的備份命名約定，則需要在備份作業完成後重新命名備份。

備份保留選項

您可以選擇保留備份副本的天數，或指定要保留的備份副本數量，ONTAP 最多可保留 255 份。例如，您的組織可能要求您保留 10 天的備份副本或 130 份備份副本。

建立策略時，您可以指定備份類型和計畫類型的保留選項。

如果您設定了SnapMirror複製，則保留政策將在目標磁碟區上鏡像。

SnapCenter會刪除具有與計劃類型相符的保留標籤的保留備份。如果資源或資源群組的計劃類型發生更改，則具有舊計劃類型標籤的備份可能仍保留在系統中。



為了長期保留備份副本，您應該使用SnapVault備份。

Windows 檔案系統複製的來源和目標

您可以從主儲存或輔助儲存複製檔案系統備份。您也可以選擇支援您要求的目的地；原始備份位置或同一主機或不同主機上的其他目的地。目標必須與克隆來源備份位於同一磁碟區上。

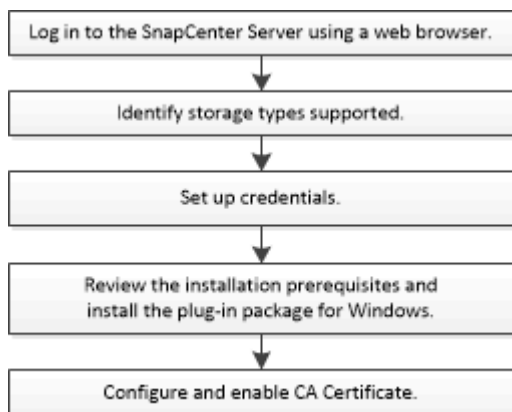
克隆目標	描述
原文、來源、地點	預設情況下， SnapCenter將克隆儲存在與被複製的備份相同的位置和主機上。
不同位置	您可以將複製儲存在同一主機或不同主機的不同位置。主機必須具有與儲存虛擬機器 (SVM) 的設定連線。

克隆操作完成後，您可以重新命名克隆。

安裝適用於 Microsoft Windows 的SnapCenter插件

適用於 Microsoft Windows 的SnapCenter外掛程式的安裝工作流程

如果要保護非資料庫文件的 Windows 文件，則必須安裝並設定適用於 Microsoft Windows 的SnapCenter外掛程式。



適用於 Microsoft Windows 的SnapCenter外掛程式的安裝需求

在安裝適用於 Windows 的插件之前，您應該了解某些安裝要求。

在開始使用適用於 Windows 的插件之前，SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 您必須具有SnapCenter管理員權限才能安裝適用於 Windows 的插件。

SnapCenter管理員角色必須具有管理員權限。

- 您必須已安裝並設定SnapCenter伺服器。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 如果您想要備份複製，則必須設定SnapMirror和SnapVault。

安裝適用於 Windows 的SnapCenter插件包的主機需求

在安裝適用於 Windows 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 如果您使用的是 Windows 叢集設置，您還應該安裝和設定 Windows 遠端管理 (WinRM)。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

設定 Windows 插件的憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證，以及用於在 Windows 檔案系統上執行資料保護作業的附加憑證。

您需要什麼

- 在安裝插件之前，您必須設定 Windows 憑證。
- 您必須在遠端主機上設定具有管理員權限（包括管理員權利）的憑證。
- 如果您為單一資源群組設定了憑證，且使用者沒有完全管理權限，則必須至少為該使用者指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，執行下列操作：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱/密碼	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式如下： ◦ NetBIOS\UserName ◦ Domain FQDN\UserName ◦ UserName@upn • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。用戶名字段的有效格式如下： UserName 請勿在密碼中使用雙引號 (") 或反引號 (` )。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，less<than<!10、less<than10<!、backtick`12。

對於這個領域...	這樣做...
密碼	輸入用於身份驗證的密碼。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面上將憑證維護指派給使用者或使用者群組。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$
.. 將電腦物件新增至群組。
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,...>
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
 - b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA： `Install-AdServiceAccount <gMSA>`
 - c. 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`
5. 將管理權限指派給主機上配置的 gMSA。
 6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

新增主機並安裝適用於 Microsoft Windows 的 SnapCenter 插件

您可以使用 SnapCenter 新增主機頁面來新增 Windows 主機。適用於 Microsoft Windows 的 SnapCenter 外掛程式會自動安裝在指定主機上。這是安裝插件的推薦方法。您可以新增主機並為單一主機或叢集安裝插件。

開始之前

- 如果 SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 應將 SnapCenter 使用者新增至 Windows Server 的「作為服務登入」角色。

- 您應該確保訊息佇列服務處於運行狀態。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

"在 Windows Server 2016 或更高版本上為 Windows 檔案系統設定群組託管服務帳戶"

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。
- Windows 外掛
 - 微軟 Windows
 - Microsoft Exchange 伺服器
 - 微軟 SQL 伺服器
 - SAP HANA
- 在集群上安裝插件

如果在叢集（WSFC、Oracle RAC 或 Exchange DAG）上安裝插件，則它們將安裝在叢集的所有節點上。

- E系列儲存

您無法在連接到 E 系列儲存的 Windows 主機上安裝適用於 Windows 的插件。



如果主機已經是工作群組的一部分並變更為另一個網域或反之亦然，則SnapCenter不支援將相同主機（插件主機）新增至SnapCenter。如果要新增相同的主機，則應從SnapCenter中刪除該主機，然後重新新增。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 確保在頂部選擇了*託管主機*。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇 Windows 類型的主機。 SnapCenter Server 新增主機，然後安裝適用於 Windows 的插件（如果主機上尚未安裝）。

對於這個領域...	這樣做...
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter 依賴 DNS 的正確配置。因此，最佳做法是輸入完全限定網域名稱 (FQDN)。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • Windows Server 故障轉移叢集 (WSFC) 如果您使用 SnapCenter 新增主機且它是子網域的一部分，則必須提供 FQDN。
證書	選擇您建立的憑證名稱或建立新的憑證。 該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 將遊標放在您提供的憑證名稱上即可顯示有關憑證的詳細信息，包括使用者名稱、網域和主機類型。  驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

對於新部署，沒有列出插件包。

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。 預設連接埠號碼為 8145。如果 SnapCenter 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。

對於這個領域...	這樣做...
安裝路徑	預設路徑為 C:\Program Files\ NetApp\ SnapCenter 。 您可以選擇自訂路徑。對於適用於 Windows 的 SnapCenter 插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。但是，如果您願意，您可以自訂預設路徑。
新增叢集中的所有主機	選取此複選框可新增 WSFC 中的所有叢集節點。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	如果要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。 以以下格式提供 gMSA 名稱： : domainName\accountName\$。  gMSA 將僅用作 Windows 服務的 SnapCenter 插件的登入服務帳戶。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本和位置。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\NetApp\SnapCenter\WebApp` 修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 監控安裝進度。

使用 PowerShell cmdlet 在多個遠端主機上安裝適用於 Microsoft Windows 的 SnapCenter 插件

如果要同時在多個主機上安裝適用於 Microsoft Windows 的 SnapCenter 插件，可以使用 `Install-SmHostPackage` PowerShell 指令。

您必須以網域使用者身分登入 SnapCenter，並在要安裝插件的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在 SnapCenter 伺服器主機上，使用 `Open-SmConnection` cmdlet，然後輸入您的憑證。

3. SnapCenter `Add-SmHost`cmdlet 和所需的參數。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

4. 使用 `Install-SmHostPackage`cmdlet 和所需的參數。

您可以使用 `-skipprecheck`` 當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以選擇此選項。

從命令列靜默安裝適用於 **Microsoft Windows** 的SnapCenter插件

如果您無法從SnapCenter GUI 遠端安裝插件，則可以在 Windows 主機上本機安裝適用於 Microsoft Windows 的SnapCenter插件。您可以從 Windows 命令列以靜默模式無人值守執行適用於 Microsoft Windows 的SnapCenter外掛程式安裝程式。

開始之前

- 您必須安裝 ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管套件。
- 您必須安裝 PowerShell 7.4.2 或更高版本。
- 您必須是主機上的本機管理員。

步驟

1. 從安裝位置下載適用於 Microsoft Windows 的SnapCenter外掛程式。

例如，預設安裝路徑為 `C:\ProgramData\NetApp\SnapCenter\Package Repository`。

可以從安裝SnapCenter伺服器的主機存取此路徑。

2. 將安裝檔案複製到要安裝插件的主機上。

3. 從命令提示字元處，導覽至下載安裝檔案的目錄。

4. 輸入以下命令，用您的資料取代變數：

```
"snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""  
BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=  
ISFeatureInstall=SCW
```

例如：

```
`"C:\ProgramData\NetApp\SnapCenter\Package Repository  
\  
snapcenter_windows_host_plugin.exe"/silent /debuglog"C:  
\  
HPPW_SCW_Install.log" /log"C:\ " BI_SNAPCENTER_PORT=8145  
SUITE_INSTALLDIR="C: \Program Files\NetApp\SnapCenter"  
BI_SERVICEACCOUNT=domain\administrator BI_SERVICEPWD=password  
ISFeatureInstall=SCW`
```



安裝 Windows 插件期間傳遞的所有參數均區分大小寫。

輸入以下變數的值：

多變的	價值
/debuglog"<偵錯日誌路徑>	指定套件安裝程式日誌檔案的名稱和位置，如下例所示：Setup.exe /debuglog"C:\PathToLog\setupexe.log"。
BI_SNAPCENTER_連接埠	指定SnapCenter與 SMCore 通訊的連接埠。
套件安裝目錄	指定主機插件包安裝目錄。
BI_服務帳戶	為 Microsoft Windows Web 服務帳戶指定SnapCenter外掛程式。
BI_SERVICEPWD	指定 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式的密碼。
ISFeature安裝	指定SnapCenter在遠端主機上部署的解決方案。

debuglog 參數包含SnapCenter日誌檔案的路徑。寫入此日誌檔案是取得故障排除資訊的首選方法，因為該檔案包含安裝對插件先決條件執行的檢查結果。

如有必要，您可以在SnapCenter for Windows 套件的日誌檔案中找到其他故障排除資訊。套件的日誌檔案列在 %Temp% 資料夾中（最早的在前），例如 C:\temp\。



Windows 插件的安裝在主機上註冊該插件，而不是在SnapCenter伺服器上註冊。您可以透過使用SnapCenter GUI 或 PowerShell cmdlet 新增主機在SnapCenter伺服器上註冊插件。新增主機後，會自動發現插件。

監控SnapCenter插件包安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動

- 排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定CA憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。

3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在SnapCenter伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器和對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。

3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 `/opt/netapp/config/crl`。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

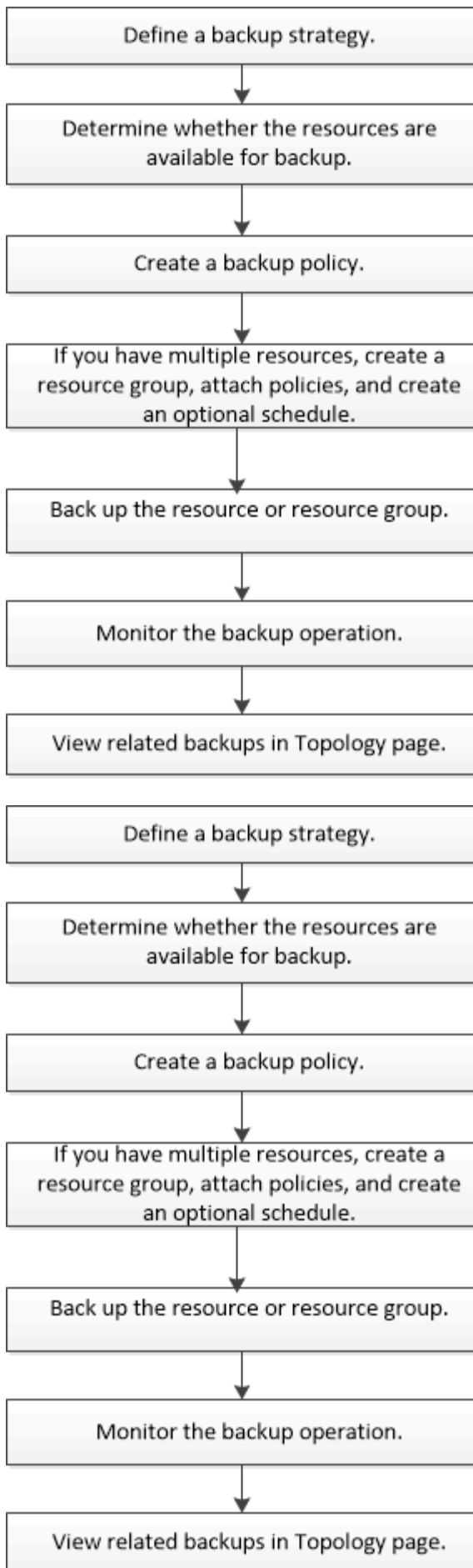
備份 Windows 檔案系統

備份 Windows 檔案系統

在您的環境中安裝適用於 Microsoft Windows 的SnapCenter外掛程式時，您可以使用SnapCenter備份 Windows 檔案系統。您可以備份單一檔案系統或包含多個檔案系統的資源群組。您可以根據需要或根據定義的保護計劃進行備份。

您可以安排多個備份同時在伺服器之間執行。不能對相同資源同時執行備份和復原作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 幫助或 "[SnapCenter 軟體 Cmdlet 參考指南](#)" 包含有關 PowerShell cmdlet 的詳細資訊。

確定 Windows 檔案系統的資源可用性

資源是檔案系統中的 LUN 和類似元件，由您安裝的插件維護。您可以將這些資源新增至資源組中，以便可以在多個資源上執行資料保護作業，但首先您必須確定哪些資源可用。發現可用資源還可以驗證插件安裝是否已成功完成。

開始之前

- 您必須已經完成安裝 SnapCenter Server、新增主機、建立儲存虛擬機器 (SVM) 連線和新增憑證等任務。
- 如果檔案駐留在 VMware RDM LUN 或 VMDK 上，則必須部署 SnapCenter Plug-in for VMware vSphere 並向 SnapCenter 註冊外掛程式。有關更多信息，請參閱 "[SnapCenter Plug-in for VMware vSphere 文檔](#)"。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從清單中選擇*檔案系統*。
3. 選擇主機來過濾資源列表，然後按一下「刷新資源」。

新新增、重新命名或刪除的檔案系統將更新至 SnapCenter 伺服器清單。



如果資料庫在 SnapCenter 之外重新命名，則必須刷新資源。

為 Windows 檔案系統建立備份策略

您可以在使用 SnapCenter 備份 Windows 檔案系統之前為資源建立新的備份策略，也可以在建立資源群組或備份資源時建立新的備份策略。

開始之前

- 您必須已經定義了您的備份策略。"[了解更多](#)"
- 您必須做好資料保護的準備。

為了準備資料保護，您必須完成安裝 SnapCenter、新增主機、發現資源和建立儲存虛擬機器 (SVM) 連線等任務。

- 如果您要將快照複製到映像或保管庫二級存儲，SnapCenter 管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。
- 如果您想要在前腳本和後腳本中執行 PowerShell 腳本，則應在 web.config 檔案中將 usePowershellProcessforScripts 參數的值設為 true。

預設值為 false

- 查看 SnapMirror 主動同步特定的先決條件和限制。欲了解詳細信息，請參閱 "[SnapMirror 主動同步的物件限制](#)"。

關於此任務

- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

• SnapLock

- 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
- 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，選擇「設定」。
2. 在設定頁面中，選擇*策略*。
3. 選擇“新建”。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「備份和複製」頁面中，執行下列任務：
 - a. 選擇備份設定。

選項	描述
檔案系統一致性備份	如果您希望SnapCenter在備份作業開始之前將檔案系統所在的磁碟機置於靜止狀態，然後在備份作業結束後還原磁碟機，請選擇此選項。
檔案系統崩潰一致性備份	如果您不希望SnapCenter使檔案系統所在的磁碟機處於靜止狀態，請選擇此選項。

- b. 選擇計劃頻率（也稱為策略類型）。

此策略僅指定備份頻率。備份的具體保護計劃在資源組中定義。因此，兩個或多個資源組可以共享相同的策略和備份頻率，但具有不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- c. 選擇一個策略標籤。

根據您選擇的快照標籤，ONTAP將套用與該標籤相符的輔助快照保留策略。



如果您選擇了*建立本機 Snapshot 副本後更新SnapMirror*，則可以選擇指定輔助原則標籤。但是，如果您選擇了*建立本機 Snapshot 副本後更新SnapVault*，則應指定輔助原則標籤。

6. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
建立本地 Snapshot 副本後更新SnapMirror	選擇此選項可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror）。 應為 SnapSnapMirror 主動同步啟用此選項。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓撲頁面中查看相關備份和克隆"。
建立 Snapshot 副本後更新SnapVault	選擇此選項可執行磁碟到磁碟的備份複製。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的刷新按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，按一下「拓撲」頁面中的「刷新」按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期限。 有關SnapLock Vault 的更多信息，請參閱 "將 Snapshot 副本提交到保管庫目標上的 WORM"
錯誤重試次數	輸入進程停止之前應發生的複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

7. 在「保留設定」頁面中，指定按需備份和所選每個計畫頻率的保留設定。

選項	描述
要保留的 Snapshot 副本總數	如果您想在自動刪除快照之前指定SnapCenter儲存的快照數量，請選擇此選項。
保留 Snapshot 副本	如果您想要指定SnapCenter在刪除備份副本之前保留該副本的天數，請選擇此選項。

選項	描述
快照副本鎖定期	選擇快照鎖定期限，並指定持續時間（天、月或年）。 SnapLock保留期應少於 100 年。



您應該將保留計數設為 2 或更高。保留計數的最小值為 2。



最大保留值為 1018。如果保留設定的值高於ONTAP版本支援的值，則備份將會失敗。

- 在腳本頁面中，分別輸入您希望SnapCenter伺服器在備份作業之前或之後執行的前腳本或後置腳本的路徑，以及SnapCenter在逾時之前等待腳本執行的時間限制。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報和傳送日誌。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

- 查看摘要，然後按一下「完成」。

為 Windows 檔案系統建立資源組

資源組是可以新增多個想要保護的檔案系統的容器。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型，然後指定備份計畫。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新檔案系統新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下為現有資源組新增檔案系統。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

- 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，從清單中選擇*檔案系統*。



如果您最近為SnapCenter新增了檔案系統，請按一下「刷新資源」以查看新新增的資源。

- 按一下“新建資源組”。
- 在精靈的名稱頁面中，執行下列操作：

對於這個領域...	這樣做...
Name	輸入資源組名稱。  資源組名稱不應超過 250 個字元。
對 Snapshot 副本使用自訂名稱格式	可選：輸入自訂快照名稱和格式。 例如，customtext_resourcegroup_policy_hostname 或 resourcegroup_hostname。預設情況下，時間戳記會附加到快照名稱。
標籤	輸入描述性標籤以協助尋找資源組。

5. 在資源頁面中，執行以下任務：

- a. 選擇主機來過濾資源清單。

如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

- b. 在可用資源部分中，按一下要備份的檔案系統，然後按一下向右箭頭將其移至已新增部分。

如果您選擇「自動選擇相同儲存磁碟區上的所有資源」選項，則會選擇同一磁碟區上的所有資源。當您將它們移至「已新增」部分時，該磁碟區上的所有資源都會一起移動。

若要新增單一檔案系統，請清除*自動選擇相同儲存磁碟區上的所有資源*選項，然後選擇要移至「已新增」部分的檔案系統。

6. 在「策略」頁面中，執行以下任務：

- a. 從下拉清單中選擇一個或多個策略。

您可以選擇任何現有策略並按一下「詳細資料」來確定是否可以使用該策略。

如果現有策略均不符合您的要求，您可以按一下 * 建立新策略  * 啟動策略精靈。

所選策略列在「為所選策略配置計畫」部分的「策略」欄位中。

- b. 在「配置所選策略的計畫」部分中，按一下 *  * 在您想要設定計畫的政策的政策設定計畫列中。

- c. 如果該策略與多種計畫類型（頻率）相關聯，請選擇要設定的頻率。

- d. 在「為政策_policy_name_新增計畫」對話方塊中，透過指定開始日期、到期日和頻率來配置計畫，然後按一下「完成」。

配置的計畫列在「為選定策略配置計畫」部分中的「已套用計畫」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。您不應該修改 Windows 工作排程器和 SQL Server 代理程式中的計畫。

7. 在通知頁面中，提供通知訊息，如下所示：

對於這個領域...	這樣做...
電子郵件偏好	選擇*始終*、失敗時*或*失敗或警告時，在建立備份資源群組、附加原則和設定計劃後向收件者傳送電子郵件。輸入 SMTP 伺服器、預設電子郵件主旨行以及收件者和寄件者電子郵件地址。
從	電子郵件
到	電子郵件地址
主題	預設電子郵件主題行

8. 查看摘要，然後按一下「完成」。

您可以按需執行備份或等待計畫的備份發生。

在ASA r2 系統上建立資源組並為 Windows 檔案系統啟用二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，`customtext_resource group_policy_hostname` 或 `resource group_hostname`。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

- 4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

- 5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。

- 6. 在應用程式設定頁面中，選擇備份選項。

- 7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b.

點選  在要設定計劃的策略的配置計劃列中。

- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

- 8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

- a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。

- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtptServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 執行資料保護作業之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在SnapCenter GUI 中顯示為「不可用於備份」或「不在NetApp儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter不支援不同叢集上具有相同名稱的多個儲存系統。 SnapCenter支援的每個儲存系統都應具有唯一的名稱和唯一的管理 LIF IP 位址。

步驟

1. 使用 Open-SmConnection cmdlet 啟動 PowerShell Core 連線會話。

此範例開啟一個 PowerShell 會話：

```
PS C:\> Open-SmConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

此範例建立一個新的儲存系統連線：

```
PS C:\> Add-SmStorageConnection -Storage test_vsl -Protocol Https  
-Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例使用 Windows 憑證建立一個名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

按需備份 **Windows** 檔案系統的單一資源

如果資源不在資源組中，您可以從資源頁面按需備份該資源。

關於此任務

如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。



備份檔案系統時，SnapCenter 不會備份正在備份的檔案系統中掛載在磁碟區掛載點 (VMP) 上的 LUN。



如果您在 Windows 檔案系統環境中工作，請不要備份資料庫檔案。這樣做會導致備份不一致，並且在復原時可能會遺失資料。若要保護資料庫文件，必須使用適合資料庫的 SnapCenter 外掛程式（例如，適用於 Microsoft SQL Server 的 SnapCenter 外掛程式或適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式）。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，選擇檔案系統資源類型，然後選擇要備份的資源。
3. 如果檔案系統 - 保護精靈沒有自動啟動，請按一下*保護*以啟動精靈。

指定保護設置，如建立資源組任務所述。

4. 可選：在精靈的資源頁面中，輸入快照的自訂名稱格式。

例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳記會附加到快照名稱。

5. 在「策略」頁面中，執行以下任務：

- a. 從下拉清單中選擇一個或多個策略。

您可以選擇任何現有策略，然後按一下「詳細資料」以確定是否可以使用的策略。

如果沒有現有策略滿足您的要求，您可以複製現有策略並進行修改，也可以透過點擊  啟動策略精靈。如果沒有現有策略滿足您的要求，您可以複製現有策略並進行修改，也可以透過點擊  啟動策略精靈。

所選策略列在「為所選策略配置計畫」部分的「策略」欄位中。

- b. 在「配置所選策略的計畫」部分中，按一下  在要設定計畫的策略的配置計畫列中。
- c. 在「為政策_policy_name_新增計畫」對話方塊中，透過指定開始日期、到期日和頻率來配置計畫，然後按一下「完成」。

配置的計畫列在「為選定策略配置計畫」部分中的「已套用計畫」欄位中。

"計劃操作可能會失敗"

6. 在通知頁面中，執行以下操作：

對於這個領域...	這樣做...
電子郵件偏好	選擇“始終”、“失敗時”或“失敗或警告時”，在建立備份資源群組、附加原則和設定計畫後向收件者發送電子郵件。 輸入 SMTP 伺服器資訊、預設電子郵件主旨行以及「收件者」和「寄件者」電子郵件地址。
從	電子郵件

對於這個領域...	這樣做...
到	電子郵件地址
主題	預設電子郵件主題行

- 查看摘要，然後按一下「完成」。

進入資料庫拓撲頁面。

- 點選*立即備份*。

- 在備份頁面中，執行以下步驟：

- 如果您已對資源套用了多個策略，請從策略下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- 按一下“備份”。

- 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

- 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-smconnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

顯示使用者名稱和密碼提示。

- 使用 Add-SmPolicy cmdlet 建立備份策略。

此範例建立一個 SQL 備份類型為 FullBackup 的新備份策略：

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

此範例建立一個新的備份策略，其 Windows 檔案系統備份類型為 CrashConsistent：

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

- 使用 Get-SmResources cmdlet 來發現主機資源。

此範例發現指定主機上的 Microsoft SQL 外掛程式的資源：

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com  
-PluginCode SCSQL
```

此範例發現指定主機上的 Windows 檔案系統的資源：

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com  
-PluginCode SCW
```

4. 使用 Add-SmResourceGroup cmdlet 為 SnapCenter 新增新的資源組。

此範例使用指定的策略和資源建立一個新的 SQL 資料庫備份資源組：

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource  
-Resources @{"Host"="vise-f6.org.com";  
"Type"="SQL Database"; "Names"="vise-f6\PayrollDatabase"}  
-Policies "BackupPolicy"
```

此範例使用指定的策略和資源建立一個新的 Windows 檔案系統備份資源群組：

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource  
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";  
"Type"="Windows Filesystem"; "Names"="E:\"}  
-Policies "EngineeringBackupPolicy"
```

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

```
PS C:\> New-SmBackup -ResourceGroupName PayrollDataset -Policy  
FinancePolicy
```

6. 使用 Get-SmBackupReport cmdlet 查看備份作業的狀態。

此範例顯示在指定日期執行的所有作業的作業摘要報表：

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份 Windows 檔案系統的資源組

資源組是主機或叢集上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要將具有SnapMirror關係的資源備份到二級存儲，則分配給儲存使用者的角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。
- 如果資源組有來自不同主機的多個資料庫，則由於網路問題，某些主機上的備份操作可能會延遲觸發。您應該使用 Set-SmConfigSettings PowerShell cmdlet 在 web.config 中設定 MaxRetryForUninitializedHosts 的值



備份檔案系統時，SnapCenter不會備份正在備份的檔案系統中掛載在磁碟區掛載點 (VMP) 上的 LUN。



如果您在 Windows 檔案系統環境中工作，請不要備份資料庫檔案。這樣做會導致備份不一致，並且在復原時可能會遺失資料。若要保護資料庫文件，必須使用適合資料庫的SnapCenter外掛程式（例如，適用於 Microsoft SQL Server 的SnapCenter外掛程式或適用於 Microsoft Exchange Server 的SnapCenter外掛程式）。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或按一下並選擇標籤。然後您可以點擊關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後按一下「立即備份」。



對於 Oracle 資料庫的SnapCenter插件，如果您有一個包含兩個資料庫的聯合資源群組，並且其中一個資料庫的資料檔案位於非NetApp儲存體上，即使另一個資料庫位於NetApp儲存體上，備份作業也會中止。

4. 在備份頁面中，執行以下步驟：
 - a. 如果您已將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。

5. 透過點選「監視」>「作業」來監視操作進度。

- 在MetroCluster配置中，SnapCenter可能無法在故障轉移後偵測到保護關係。

"MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java 堆大

小不夠大，則備份可能會失敗。若要增加 Java 堆大小，請找到腳本文件 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method``命令啟動 SnapCenter VMware 插件服務。將該命令更新為以下內容：``Java -jar -Xmx8192M -Xms4096M`。

監視備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

監視活動窗格中的操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消備份作業

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	a. 在左側導覽窗格中，按一下「監控」>「作業」。 b. 選擇操作，然後按一下「取消作業」。
活動窗格	a. 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 b. 選擇操作。 c. 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓撲頁面中查看相關備份和克隆

當您準備備份或複製資源時，您可以查看主儲存和輔助儲存上所有備份和複製的圖形表示。在拓撲頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。
 - 顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數量為 6。
-  鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。
-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓撲頁面。

4. 查看摘要卡以了解主儲存和輔助儲存上可用的備份和複製數量的摘要。

摘要卡部分顯示備份和克隆的總數。僅適用於 Oracle 資料庫，「摘要卡」部分也會顯示日誌備份的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 會自動配置為新的主目標。
- 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製、重新命名和刪除操作。

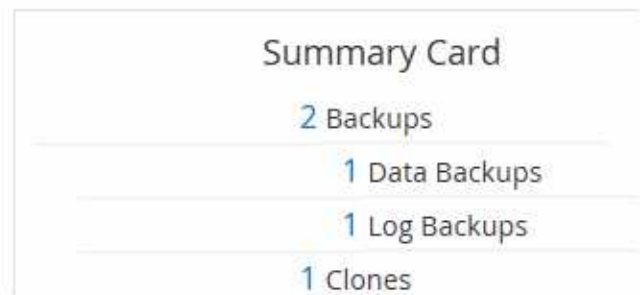
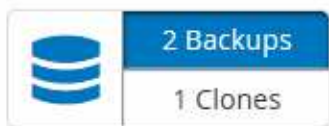


您無法重新命名或刪除輔助儲存系統上的備份。

7. 如果要刪除克隆，請從表中選擇克隆，然後按一下  刪除克隆。

顯示主儲存體上的備份和克隆的範例

Manage Copies



使用 PowerShell cmdlet 清理輔助備援計數

您可以使用 Remove-SmBackup cmdlet 清理沒有快照的輔助備份的備份計數。當管理副本拓撲中顯示的快照總數與輔助儲存快照保留設定不符時，您可能需要使用此 cmdlet。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146/
```

2. 使用 -CleanupSecondaryBackups 參數清理輔助備援計數。

此範例清理沒有快照的輔助備份的備份計數：

```
Remove-SmBackup -CleanupSecondaryBackups
Remove-SmBackup
Are you sure want to remove the backup(s).
[Y] Yes   [A] Yes to All   [N] No   [L] No to All   [S] Suspend   [?] Help
(default is "Y"):
```

還原 Windows 檔案系統

恢復 Windows 檔案系統備份

您可以使用SnapCenter來恢復檔案系統備份。檔案系統復原是一個多階段過程，將所有資料從指定的備份複製到檔案系統的原始位置。

開始之前

- 您必須已經備份檔案系統。
- 如果檔案系統目前正在執行計劃操作（例如備份操作），則必須先取消該操作，然後才能開始復原作業。
- 您只能將檔案系統備份還原到原始位置，而不能還原到備用路徑。

您無法從備份中還原單一文件，因為還原的文件系統會覆蓋文件系統原始位置上的所有資料。要從檔案系統備份還原單一文件，您必須複製備份並存取複製中的檔案。

- 您無法復原系統或啟動磁碟區。
- SnapCenter可以在不使叢集組離線的情況下恢復 Windows 叢集中的檔案系統。

關於此任務

- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：[API /4.7/configsettings](#)

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 若要過濾資源列表，請選擇檔案系統和資源組選項。
3. 從清單中選擇一個資源組，然後按一下「恢復」。
4. 在備份頁面中，選擇是否要從主儲存系統或輔助儲存系統恢復，然後選擇要恢復的備份。
5. 在還原精靈中選擇您的選項。
6. 您可以分別輸入您希望SnapCenter在還原作業之前或之後執行的前置腳本或後置腳本的路徑和參數。

例如，您可以執行腳本來更新 SNMP 陷阱、自動發出警報、傳送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

7. 在通知頁面中，選擇以下選項之一：

對於這個領域...	這樣做...
將SnapCenter伺服器事件記錄到儲存系統 syslog	選擇此選項可將SnapCenter Server 事件記錄到儲存系統的系統日誌中。
向儲存系統發送操作失敗的AutoSupport通知	選擇此選項可使用AutoSupport將任何失敗操作的資訊傳送至NetApp。
電子郵件偏好	選擇「始終」、「失敗時」或「失敗或警告時」在恢復備份後向收件者發送電子郵件訊息。輸入SMTP 伺服器、預設電子郵件主旨行以及收件者和寄件者電子郵件地址。

8. 查看摘要，然後按一下「完成」。
9. 透過點選「監視」>「作業」來監視操作進度。



如果復原的檔案系統包含資料庫，那麼您也必須還原該資料庫。如果不恢復資料庫，那麼您的資料庫可能處於無效狀態。有關恢復資料庫的信息，請參閱該資料庫的資料保護指南。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：


```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDateTime "1/29/2015" -ToDateTime "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1' -BackupId 269  
-Confirm:$false  
output:  
Name                : Restore  
'scc54.sccore.test.com\DummyPlugin\NTP\DB1'  
Id                  : 2368  
StartTime           : 10/4/2016 11:22:02 PM  
EndTime            :  
IsCancellable       : False  
IsRestartable       : False  
IsCompleted         : False  
IsVisible           : True  
IsScheduled         : False  
PercentageCompleted : 0  
Description         :  
Status              : Queued  
Owner                :  
Error                :  
Priority             : None  
Tasks               : {}  
ParentJobID         : 0  
EventId             : 0  
JobTypeId           :  
ApisJobKey          :  
ObjectId            : 0  
PluginCode          : NONE  
PluginName          :
```

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

使用 PowerShell cmdlet 還原資源

恢復資源備份包括啟動與SnapCenter伺服器的連線會話、列出備份並檢索備份資訊以及恢復備份。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 `Get-SmBackup` 和 `Get-SmBackupReport` cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDateTime "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority            : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監視恢復操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成

-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

取消恢復操作

您可以取消排隊的還原作業。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消恢復操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的復原操作。
- 您無法取消正在執行的復原操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的還原作業。
- 對於無法取消的復原操作，「取消作業」按鈕將被停用。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊復原作業。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇作業並點選「取消作業」。

從...	行動
活動窗格	1. 啟動恢復操作後，按一下  在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

克隆 Windows 檔案系統

從 Windows 檔案系統備份克隆

您可以使用 SnapCenter 克隆 Windows 檔案系統備份。如果您想要錯誤刪除或更改的單一檔案的副本，那麼您可以複製備份並在複製中存取該檔案。

開始之前

- 您應該已經透過完成新增主機、識別資源和建立儲存虛擬機器 (SVM) 連線等任務為資料保護做好了準備。
- 您應該有一個檔案系統的備份。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 您不能克隆資源組。您只能克隆單一檔案系統備份。
- 如果備份駐留在具有 VMDK 磁碟的虛擬機器上，則 SnapCenter 無法將備份複製到實體伺服器。
- 如果您複製 Windows 叢集（例如，共用 LUN 或叢集共用磁碟區 (CSV) LUN），則複製將作為專用 LUN 儲存在您指定的主機上。
- 對於克隆操作，卷掛載點的根目錄不能是共享目錄。
- 您不能在非聚合主節點上建立克隆。
- 您無法為 Windows 檔案系統安排重複複製（複製生命週期）操作；您只能按需複製備份。
- 如果將包含複製的 LUN 移至新磁碟區，SnapCenter 將不再支援該複製。例如，您不能使用 SnapCenter 刪除該克隆。
- 您不能跨環境克隆。例如，從實體磁碟複製到虛擬磁碟或反之亦然。

關於此任務

- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從清單中選擇*檔案系統*。
3. 選擇主機。

如果資源受到保護，則會自動顯示拓樸視圖。

4. 從資源清單中，選擇要複製的備份，然後按一下複製圖示。
5. 在「選項」頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	選擇要建立克隆的主機。
“自動分配掛載點”或“自動分配路徑下的磁碟區掛載點”	選擇是否自動指派掛載點或路徑下的磁碟區掛載點。 自動分配路徑下的磁碟區掛載點：路徑下的掛載點可讓您提供將在其中建立掛載點的特定目錄。在選擇此選項之前，您必須驗證目錄是否為空。如果目錄中存在備份，則掛載作業後備份將處於無效狀態。
存檔位置	如果您要複製輔助備份，請選擇存檔位置。

6. 在腳本頁面中，指定您想要執行的任何前腳本或後腳本。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

7. 查看摘要，然後按一下「完成」。
8. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. 列出可以使用 Get-SmBackup 或 Get-SmResourceGroup cmdlet 克隆的備份。

此範例顯示有關所有可用備份的資訊：


```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

此範例顯示有關指定資源組、其資源和相關策略的資訊：

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :
CreationTime : 8/4/2015 3:44:05 PM
ModificationTime : 8/4/2015 3:44:05 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMaping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
```

Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}

```

AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False

```

3. 使用 New-SmClone cmdlet 從現有備援啟動複製作業。

此範例從包含所有日誌的指定備份建立複製：

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

此範例建立指定 Microsoft SQL Server 執行個體的複製：

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. 使用 Get-SmCloneReport cmdlet 查看複製作業的狀態。

此範例顯示指定作業 ID 的複製報表：

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監視克隆操作

您可以使用「作業」頁面監控 SnapCenter 複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。

2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

取消克隆操作

您可以取消排隊的複製操作。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消複製操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的複製操作。
- 您無法取消正在執行的克隆操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的複製作業。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊複製操作。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇操作，然後按一下「取消作業」。
活動窗格	1. 啟動克隆操作後，按一下  在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2 後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“*”。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCore 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定SMCore輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為5分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter克隆或驗證失敗，聚合不存在"](#)

保護 Microsoft Exchange Server 資料庫

適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式概念

適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式概述

適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式是 NetApp SnapCenter 軟體的主機端元件，可實現 Exchange 資料庫的應用程式感知資料保護管理。Exchange 外掛程式可自動備份並還原 SnapCenter 環境中的 Exchange 資料庫。

安裝 Exchange 外掛程式後，您可以使用 SnapCenter 和 NetApp SnapMirror 技術在另一個磁碟區上建立備份集的鏡像副本，並使用 NetApp SnapVault 技術執行磁碟到磁碟備份複製，以滿足標準合規性或存檔目的。

如果您想要復原郵件或郵件信箱而不是完整的 Exchange 資料庫，您可以使用單一郵件匣復原 (SMBR) 軟體。NetApp® 單一信箱復原已於 2023 年 5 月 12 日停止提供 (EOA)。NetApp 將在支援期限內繼續為已透過 2020 年 6 月 24 日推出的行銷零件號碼購買郵箱容量、維護和支援的客戶提供支援。

NetApp Single Mailbox Recovery 是 Ontrack 提供的合作夥伴產品。Ontrack PowerControls 提供的功能與 NetApp Single Mailbox Recovery 類似。客戶可以從 Ontrack (透過 licenceteam@ontrack.com) 購買新的 Ontrack PowerControls 軟體許可證以及 Ontrack PowerControls 維護和支援續訂，以實現細粒度的郵箱恢復。

Exchange 外掛程式支援 SnapMirror 主動同步 (最初是作為 SnapMirror 業務連續性 [SM-BC] 發布)，即使整個網站發生故障，該功能也能使業務服務繼續運行，並支援應用程式使用輔助副本透明地進行故障轉移。無需手動幹預或額外的腳本即可透過 SnapMirror 主動同步觸發故障轉移。

它支援 SnapMirror Active Sync 的非對稱、故障轉移或非雙工模式。這是指最佳化路徑僅來自主側 LUN 擁有節點的解決方案。任何來自輔助集群路徑的 I/O 都透過代理到主集群來提供服務。同步複製是單向的，從主節點到次節點。

- 自動執行 SnapCenter 環境中 Microsoft Exchange Server 資料庫和資料庫可用性群組 (DAG) 的應用程式感知備份和還原作業
- 當您部署 SnapCenter Plug-in for VMware vSphere 並向 SnapCenter 註冊外掛程式時，支援 RDM LUN 上的虛擬化 Exchange 伺服器。

SnapCenter 外掛程式 for Microsoft Exchange Server 的功能

您可以使用 Exchange 外掛程式來備份和還原 Exchange Server 資料庫。

- 檢視和管理 Exchange 資料庫可用性群組 (DAG)、資料庫和副本集的活動清單
- 定義提供備份自動化保護設定的策略
- 為資源組分配策略
- 保護單一 DAG 和資料庫
- 備份主 Exchange 信箱資料庫和輔助 Exchange 信箱資料庫
- 從主備份和輔助備份還原資料庫

SnapCenter外掛程式（適用於 Microsoft Windows 和 Microsoft Exchange Server）支援的儲存類型

SnapCenter支援實體機器和虛擬機器上的多種儲存類型。在為您的主機安裝軟體包之前，您必須驗證您的儲存類型是否受支援。

Windows Server 上提供SnapCenter設定和資料保護支援。有關受支援版本的最新信息，請參閱 <https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT>[NetApp互通性矩陣工具^]。

機器	儲存類型	使用配置	支援說明
實體伺服器	FC 連接的 LUN	SnapCenter圖形使用者介面 (GUI) 或 PowerShell cmdlet	
實體伺服器	iSCSI 連接的 LUN	SnapCenter GUI 或 PowerShell cmdlet	
VMware VM	透過 FC 或 iSCSI HBA 連接的 RDM LUN	PowerShell cmdlet	僅實體相容性  不支援 VMDK。
VMware VM	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	 不支援 VMDK。
Hyper-V 虛擬機	透過虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN	SnapCenter GUI 或 PowerShell cmdlet	您必須使用 Hyper-V 管理員來設定由虛擬光纖通道交換器連接的虛擬 FC (vFC) LUN。  不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。

機器	儲存類型	使用配置	支援說明
Hyper-V 虛擬機	iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統	SnapCenter GUI 或 PowerShell cmdlet	 不支援 Hyper-V 直通磁碟和在 NetApp 儲存裝置上配置的 VHD(x) 上的備份資料庫。

Exchange 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限

- 事件產生自動支援日誌
- 工作歷史顯示
- 工作停止
- 倫
- lun 創建
- lun 創建
- lun 創建
- lun 刪除
- lun igroup 新增
- lun igroup 創建
- lun igroup 刪除
- lun igroup 重新命名
- lun igroup 重新命名
- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun修改
- lun 移入磁碟區
- lun 離線

- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線
- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建

- 卷快照刪除
- 卷快照修改
- 磁碟區快照修改-快照鎖定到期時間
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面
 - 網路介面顯示
 - 虛擬伺服器

為SnapMirror和SnapVault複製準備儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

定義 Exchange Server 資源的備份策略

在建立備份作業之前定義備份策略有助於確保您擁有成功還原資料庫所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是指服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於備份策略。

Exchange 資料庫支援的備份類型

使用SnapCenter備份 Exchange 信箱需要您選擇資源類型，例如資料庫和資料庫可用性群組 (DAG)。利用快照技術來建立資源所在磁碟區的線上、唯讀副本。

備份類型	描述
完整備份和日誌備份	備份資料庫和所有交易日誌，包括截斷的日誌。 完整備份完成後，Exchange Server 會截斷已提交至資料庫的交易日誌。 通常，您應該選擇此選項。但是，如果您的備份時間很短，您可以選擇不執行交易日誌備份，而是進行完整備份。
完整備份	備份資料庫和交易日誌。 截斷的交易日誌不會備份。
日誌備份	備份所有交易日誌。 已提交到資料庫的截斷日誌不會備份。如果您在完整資料庫備份之間安排頻繁的交易日誌備份，則可以選擇粒度復原點。

資料庫插件的備份計劃

備份頻率（計畫類型）在策略中指定；備份計畫在資源組配置中指定。確定備份頻率或計畫的最關鍵因素是資源的變化率和資料的重要性。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA 和 RPO 有助於資料保護策略。

即使是使用頻繁的資源，也不需要每天執行一次或兩次以上的完整備份。例如，定期的交易日誌備份可能足以確保您擁有所需的備份。備份資料庫的頻率越高，SnapCenter在復原時需要使用的交易日誌就越少，因此可以加快復原作業的速度。

備份計畫分為兩部分，如下所示：

- 備份頻率

備份頻率（執行備份的頻率），對於某些外掛程式來說稱為_計畫類型_，是策略配置的一部分。您可以選擇每小時、每天、每週或每月作為策略的備份頻率。如果您未選擇任何頻率，則建立的策略是僅按需策略。您可以透過點選「設定」>「策略」來存取策略。

- 備份計畫

備份計畫（確切地指定執行備份的時間）是資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份。您可以透過點選「資源」>「資源群組」來存取資源組計畫。

資料庫所需的備份作業數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

```
resourcegroupname_hostname_timestamp
```

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，customtext_resourcegroup_policy_hostname 或 resourcegroup_hostname。預設情況下，時間戳後綴會加入到快照名稱中。

備份保留選項

您可以選擇保留備份副本的天數，或指定要保留的備份副本數量，ONTAP最多可保留 255 份。例如，您的組織可能要求您保留 10 天的備份副本或 130 份備份副本。

建立策略時，您可以指定備份類型和計畫類型的保留選項。

如果您設定了SnapMirror複製，則保留政策將在目標磁碟區上鏡像。

SnapCenter會刪除具有與計劃類型相符的保留標籤的保留備份。如果資源或資源群組的計劃類型發生更改，則具有舊計劃類型標籤的備份可能仍保留在系統中。



為了長期保留備份副本，您應該使用SnapVault備份。

在 **Exchange Server** 的來源儲存磁碟區上保留交易日誌備份的時間

適用於 Microsoft Exchange Server 的SnapCenter外掛程式需要交易日誌備份來執行最新的還原作業，該操作將資料庫還原到兩次完整備份之間的時間。

例如，如果 Plug-in for Exchange 在上午 8:00 進行了一次完整備份和交易日誌備份，並在下午 5:00 進行了另一次完整備份和交易日誌備份，則它可以使用最新的交易日誌備份將資料庫還原到上午 8:00 至下午 5:00 之間的任何時間。如果沒有交易日誌，Plug-in for Exchange 只能執行時間點還原作業，即將資料庫還原到 Plug-in for Exchange 完成完整備份的時間。

通常，您只需要一兩天的最新恢復操作。預設情況下，SnapCenter至少保留兩天。

定義 **Exchange** 資料庫的還原策略

定義 Exchange Server 的復原策略可讓您成功復原資料庫。

Exchange Server 中還原作業的來源

您可以從主儲存體上的備份副本還原 Exchange Server 資料庫。

您只能從主儲存復原資料庫。

Exchange Server 支援的還原作業類型

您可以使用SnapCenter對 Exchange 資源執行不同類型的還原作業。

- 恢復最新狀態
- 恢復到之前的時間點

恢復最新狀態

在最新的復原作業中，資料庫將恢復到故障點。SnapCenter透過執行以下序列來實現此目的：

1. 從您選擇的完整資料庫備份還原資料庫。
2. 套用所有已備份的交易日誌以及自最近一次備份以來建立的任何新日誌。

交易日誌被向前移動並應用於任何選定的資料庫。

還原完成後，Exchange 會建立一個新的日誌鏈。

最佳實務：建議您在復原完成後執行新的完整備份和日誌備份。

最新的復原操作需要一組連續的交易日誌。

執行最新還原後，用於還原的備份僅可用於時間點還原作業。

如果您不需要為所有備份保留最新的還原功能，則可以透過備份原則設定系統的交易日誌備份保留。

恢復到之前的時間點

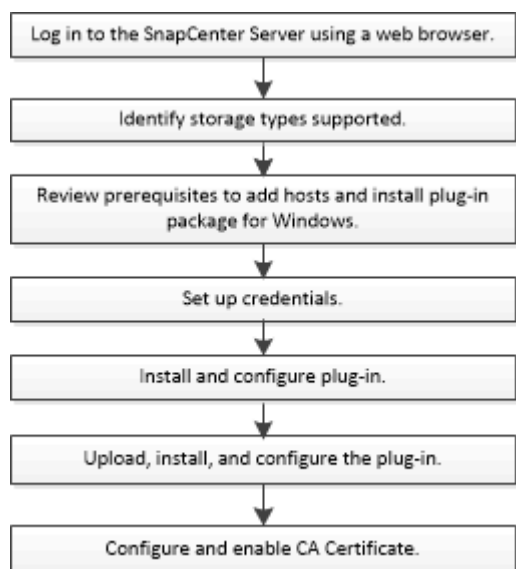
在時間點還原作業中，資料庫僅還原到過去的特定時間。時間點還原操作發生在下列還原情況：

- 資料庫還原到備份交易日誌中的給定時間。
- 資料庫已恢復，並且僅將備份交易日誌的子集套用至該資料庫。

為 Microsoft Exchange Server 安裝SnapCenter插件

適用於 Microsoft Exchange Server 的SnapCenter插件的安裝工作流程

如果您想要保護 Exchange 資料庫，則應該安裝並設定適用於 Microsoft Exchange Server 的SnapCenter外掛程式。



新增主機並安裝適用於 **Microsoft Exchange Server** 的**SnapCenter**外掛程式的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。

- 如果您正在使用 iSCSI，則 iSCSI 服務必須正在執行。
- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 您必須使用 Microsoft Exchange Server 2013、2016 或 2019 進行獨立和資料庫可用性群組配置。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 如果您在SnapCenter中管理叢集節點，則必須擁有對叢集中所有節點具有管理權限的使用者。
- 您必須擁有在 Exchange Server 上具有管理權限的使用者。
- 如果已安裝SnapManager for Microsoft Exchange Server 和SnapDrive for Windows，則必須先取消註冊SnapDrive for Windows 使用的 VSS 硬體提供程序，然後再在同一 Exchange Server 上安裝 Plug-in for Exchange，以確保使用SnapCenter成功保護資料。
- 如果SnapManager for Microsoft Exchange Server 和 Plug-in for Exchange 安裝在同一台伺服器上，則必須從 Windows 排程器中暫停或刪除由SnapManager for Microsoft Exchange Server 建立的所有計畫。
- 主機必須能夠解析為伺服器的完全限定網域名稱 (FQDN)。如果修改了 hosts 檔案以使其可解析，並且在 hosts 檔案中指定了短名稱和 FQDN，則在SnapCenter hosts 檔案中以下列格式建立一個項目：
: <ip_address> <host_fqdn> <host_name>。
- 確保防火牆未封鎖以下端口，否則添加主機操作將失敗。若要解決此問題，您必須配置動態連接埠範圍。有關更多信息，請參閱 ["Microsoft 文件"](#)。
 - Windows 2016 和 Exchange 2016 的連接埠範圍為 50000 - 51000
 - Windows 2012 R2 和 Exchange 2013 的連接埠範圍為 6000 - 6500
 - Windows 2019 的連接埠範圍為 49152 - 65536



若要識別連接埠範圍，請執行下列命令：

- netsh int ipv4 顯示動態連接埠 tcp
- netsh int ipv4 顯示動態連接埠 udp
- netsh int ipv6 顯示動態連接埠 tcp
- netsh int ipv6 顯示動態連接埠 udp

安裝適用於 **Windows** 的**SnapCenter**插件包的主機需求

在安裝適用於 Windows 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具" 。

物品	要求
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統， SnapCenter升級或安裝將會失敗。"

需要 Exchange Server 權限

若要讓SnapCenter能夠新增 Exchange Server 或 DAG，並在主機或 DAG 上安裝適用於 Microsoft Exchange Server 的SnapCenter插件，您必須使用具有最低限度特權和權限的使用者憑證來設定SnapCenter。

您必須擁有具有本機管理員權限的網域用戶，並且具有遠端 Exchange 主機上的本機登入權限以及 DAG 中所有節點上的管理權限。網域使用者需要以下最低權限：

- 新增郵箱資料庫副本
- 解除安裝資料庫
- 取得廣告伺服器設置
- 取得資料庫可用性群組
- 取得 ExchangeServer
- 取得郵箱資料庫
- 取得郵箱資料庫複製狀態
- 取得郵件伺服器

- 獲取郵箱統計信息
- 取得公共資料夾資料庫
- 行動活動信箱資料庫
- 行動資料庫路徑-ConfigurationOnly:\$true
- 掛載資料庫
- 新郵件資料庫
- 新公用資料夾資料庫
- 刪除郵件資料庫
- 刪除-MailboxDatabaseCopy
- 刪除公用資料夾資料庫
- 履歷-郵件資料庫副本
- 設定廣告伺服器設定
- 設定郵件資料庫-allowfilerestore:\$true
- 設定郵箱資料庫副本
- 設定公用資料夾資料庫
- 暫停郵箱資料庫複製
- 更新郵箱資料庫副本

安裝適用於 **Windows** 的SnapCenter插件包的主機需求

在安裝適用於 Windows 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。

物品	要求
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

為 Windows 版SnapCenter插件設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝插件包的憑證以及用於對資料庫執行資料保護操作的附加憑證。

關於此任務

您必須設定在 Windows 主機上安裝插件的憑證。雖然您可以在部署主機和安裝插件後為 Windows 建立憑證，但最佳做法是在新增 SVM 之後、部署主機和安裝插件之前建立憑證。

設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選「新建」。

將顯示“憑證”視窗。

4. 在「憑證」頁面中，執行下列操作：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。

對於這個領域...	這樣做...
使用者名稱	輸入用於身份驗證的使用者名稱。 - 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ NetBIOS\UserName ◦ Domain FQDN\UserName - 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。用戶名字段的有效格式為：UserName
密碼	輸入用於身份驗證的密碼。
驗證	選擇 Windows 作為身份驗證模式。

5. 按一下“確定”。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：

- a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart	Needed	Exit Code	Feature Result
-----	-----	-----	-----	-----
True	No		Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
 - b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA： `Install-AdServiceAccount <gMSA>`
 - c. 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`
5. 將管理權限指派給主機上配置的 gMSA。
 6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

新增主機並安裝 Exchange 插件

您可以使用SnapCenter新增主機頁面來新增 Windows 主機。Exchange 外掛程式會自動安裝在指定的主機上。這是安裝插件的推薦方法。您可以新增主機並為單一主機或叢集安裝插件。

開始之前

- 如果SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 訊息隊列服務必須正在運行。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。有關信息，請參閱["在 Windows Server 2016 或更新版本上為 Microsoft Exchange Server 設定群組託管服務帳戶"](#)。

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。
- 您可以為單一主機或叢集新增主機並安裝插件包。
- 如果交換節點是 DAG 的一部分，則不能僅將一個節點新增至SnapCenter伺服器。
- 如果您在叢集（Exchange DAG）上安裝插件，即使某些節點在NetApp LUN 上沒有資料庫，它們也會安裝在叢集的所有節點上。

從SnapCenter 4.6 開始，SCE 支援多租戶，您可以使用下列方法新增主機：

新增主機操作	4.5 及更早版本	4.6 及更高版本
在跨域或不同域中新增無 IP DAG	不支援	支援
新增多個具有唯一名稱的 IP DAG，位於相同網域或跨網域	支援	支援
在跨網域中新增具有相同主機名稱和/或資料庫名稱的多個 IP 或無 IP DAG	不支援	支援
新增多個具有相同名稱和跨網域的 IP/無 IP DAG	不支援	支援
新增多個同名、跨域的獨立主機	不支援	支援

Exchange 插件依賴 Windows 的SnapCenter插件包，且版本必須相同。在 Exchange 插件安裝期間，預設選擇適用於 Windows 的SnapCenter插件包，並與 VSS 硬體提供者一起安裝。

如果已安裝SnapManager for Microsoft Exchange Server 和SnapDrive for Windows，並且您想要在同一 Exchange Server 上安裝 Plug-in for Exchange，則必須取消註冊SnapDrive for Windows 使用的 VSS 硬體提供程序，因為它與隨 Plug-in for Exchange 和SnapCenter Plug-ins Package for Windows 一起安裝的 VSS 硬體提

供者不相容。有關更多信息，請參閱 ["如何手動註冊Data ONTAP VSS 硬體提供者"](#)。

步驟

- 1. 在左側導覽窗格中，按一下「主機」。
- 2. 驗證頂部是否選擇了「託管主機」。
- 3. 按一下“新增”。
- 4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇 Windows 作為主機類型。 SnapCenter Server 新增主機，然後在主機上安裝適用於 Windows 的插件和適用於 Exchange 的插件（如果尚未安裝）。 適用於 Windows 的插件和適用於 Exchange 的插件必須是同一版本。如果之前安裝了不同版本的 Windows 插件， SnapCenter會在安裝過程中更新版本。

對於這個領域...	這樣做...
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter 依賴 DNS 的正確配置。因此，最佳做法是輸入完全限定網域名稱 (FQDN)。 只有當 IP 位址解析為 FQDN 時，不受信任的網域主機才支援該 IP 位址。 如果您使用 SnapCenter 新增主機且它是子網域的一部分，則必須提供 FQDN。 您可以輸入以下之一的 IP 位址或 FQDN： • 獨立主機 • 交易所 DAG 對於 Exchange DAG，您可以： ◦ 透過提供 DAG 名稱、DAG IP 位址、節點名稱或節點 IP 位址來新增 DAG。 ◦ 透過提供其中一個 DAG 群集節點的 IP 位址或 FQDN 來新增無 IP DAG 群集。 ◦ 新增位於同一網域或不同網域的無 IP DAG。您也可以新增多個具有相同名稱但不同網域的 IP/無 IP DAG。  對於獨立主機或 Exchange DAG（跨網域或相同網域），建議提供主機或 DAG 的 FQDN 或 IP 位址。
證書	選擇您建立的憑證名稱，或建立新的憑證。 該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標置於指定的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

當您選擇「Exchange 外掛程式」時，將自動取消選擇「Microsoft SQL Server 的 SnapCenter 插件」。由於 Exchange 所需的記憶體量和其他資源使用情況，Microsoft 建議不要在同一系統上安裝 SQL Server 和 Exchange 伺服器。

6. (可選) 按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。 預設連接埠號碼為 8145。如果 SnapCenter 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑是 C:\Program Files\NetApp\SnapCenter。 您可以選擇自訂路徑。
添加 DAG 中的所有主機	新增 DAG 時選取此複選框。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	如果要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。 以以下格式提供 gMSA 名稱： : domainName\accountName\$。  gMSA 將僅用作 Windows 服務的 SnapCenter 插件的登入服務帳戶。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\NetApp\SnapCenter\WebApp` 修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 監控安裝進度。

為 **NET TCP** 通訊配置自訂連接埠

預設情況下，從 SnapCenter 6.0 版本開始，適用於 Windows 的 SnapCenter 插件使用連接埠 909 進行 NET TCP

通訊。如果連接埠 909 正在使用，您可以設定另一個連接埠用於 NET TCP 通訊。

步驟

1. 將位於 `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe.config` 的 `NetTCPPort` 鍵的值修改為所需的連接埠號碼。
`<add key="NetTCPPort" value="new_port_number" />`
2. 將位於 `C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\SnapDriveService.dll.config` 的 `NetTCPPort` 鍵的值修改為所需的連接埠號碼。
`<add key="NetTCPPort" value="new_port_number" />`
3. 透過執行以下命令取消註冊 `_Data ONTAP VSS Hardware Provider_` 服務：
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

驗證該服務未顯示在 `_services.msc_` 中的服務清單中。

4. 透過執行以下命令註冊 `_Data ONTAP VSS Hardware Provider_` 服務：
`"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

驗證該服務現在是否顯示在 `_services.msc_` 中的服務清單中。

5. 重新啟動 `_Plug-in for Windows_` 服務。

使用 PowerShell cmdlet 從 SnapCenter 伺服器主機安裝 Exchange 插件

您應該從 SnapCenter GUI 安裝 Exchange 插件。如果您不想使用 GUI，則可以在 SnapCenter Server 主機或遠端主機上使用 PowerShell cmdlet。

開始之前

- 必須已安裝並設定 SnapCenter 伺服器。
- 您必須是主機上的本機管理員或具有管理權限的使用者。
- 您必須是分配有插件、安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員。
- 在安裝 Exchange 外掛程式之前，您必須已經查看了安裝要求和支援的設定類型。
- 您想要安裝 Exchange 外掛程式的主機必須是 Windows 主機。

步驟

1. 在 SnapCenter Server 主機上，使用 `Open-SmConnection` cmdlet 建立會話，然後輸入您的憑證。
2. 使用具有所需參數的 `Add-SmHost` cmdlet 新增要安裝 Exchange 插件的主機。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

主機可以是獨立主機，也可以是 DAG。如果指定 DAG，則需要 `-IsDAG` 參數。

3. 使用帶有所需參數的 `Install-SmHostPackage` cmdlet 安裝 Exchange 插件。

此命令在指定主機上安裝 Exchange 插件，然後向 SnapCenter 註冊該插件。

從命令列靜默安裝適用於 **Exchange** 的**SnapCenter**插件

您應該從SnapCenter使用者介面安裝 Exchange 插件。但是，如果由於某種原因您無法這樣做，您可以從 Windows 命令列以靜默模式無人值守執行 Exchange 外掛程式安裝程式。

開始之前

- 您必須備份您的 Microsoft Exchange Server 資源。
- 您必須已安裝SnapCenter插件包。
- 在安裝之前，您必須刪除適用於 Microsoft SQL Server 的SnapCenter插件的早期版本。

有關更多信息，請參閱 ["如何從插件主機手動直接安裝SnapCenter插件"](#)。

步驟

1. 驗證插件主機上是否存在 `C:\temp` 資料夾以及登入使用者是否對該資料夾具有完全存取權限。
2. 從 `C:\ProgramData\ NetApp\ SnapCenter \Package Repository` 下載適用於 Microsoft Windows 的SnapCenter外掛程式。

可以從安裝SnapCenter伺服器的主機存取此路徑。

3. 將安裝檔案複製到要安裝插件的主機上。
4. 從本機上的 Windows 命令提示符，導覽至儲存插件安裝檔案的目錄。
5. 輸入以下命令安裝插件。

```
snapcenter_windows_host_plugin.exe"/silent
/debuglog"<Debug_Log_Path>"/log"<Log_Path>"BI_SNAPCENTER_PORT=<Num>
SUITE_INSTALLDIR="<Install_Directory_Path>"BI_SERVageACC"。 ISFeatureInstall=HPPW,SCW,SCE
```

例如：

```
C:\ProgramData\ NetApp\ SnapCenter\ NetApp Repository \ snapcenter_windows_host_plugin.exe"/silent
/debuglog"C:\HPPW_SCSQL_Install.log"/log"C:\temp"BI_SNAPCENTER_PORT=8INS145 SU_Y
"BI_SERVICEACCOUNT=domain\administratorBI_SERVICEPWD=passwordISFeatureInstall=HPPW,SCW
,SCE
```



安裝 Exchange 插件期間傳遞的所有參數均區分大小寫。

為變數輸入以下值：

多變的	價值
<code>/debuglog"<偵錯日誌路徑></code>	指定套件安裝程式日誌檔案的名稱和位置，如下例所示： <code>Setup.exe /debuglog "C:\PathToLog\setupexe.log"</code>
<code>BI_SNAPCENTER_連接埠</code>	指定SnapCenter與 SMCore 通訊的連接埠。

多變的	價值
套件安裝目錄	指定主機插件包安裝目錄。
BI_服務帳戶	為 Microsoft Windows Web 服務帳戶指定SnapCenter外掛程式。
BI_SERVICEPWD	指定 Microsoft Windows Web 服務帳戶的SnapCenter外掛程式的密碼。
ISFeature安裝	指定SnapCenter在遠端主機上部署的解決方案。

6. 監視 Windows 工作排程器、主安裝記錄檔 *C:\Installdebug.log* 以及 *C:\Temp* 中的附加安裝檔。
7. 監控 *%temp%* 目錄以檢查 *msiexe.exe* 安裝程式是否正在正確安裝軟體。



安裝 Exchange 插件時，會在主機上註冊該插件，而不是在SnapCenter伺服器上註冊。您可以透過使用SnapCenter GUI 或 PowerShell cmdlet 新增主機在SnapCenter伺服器上註冊插件。新增主機後，會自動發現插件。

監控SnapCenter插件包安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。

- e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入SnapCenter伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。

在此精靈視窗中...	執行以下操作...
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 **CA** 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-Childitem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 **Windows** 主機插件服務設定 **CA** 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

．透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

為插件啟用 **CA** 憑證

您應該設定 CA 憑證並在 SnapCenter 伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。

- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

配置 SnapManager 7.x 以使 Exchange 和 SnapCenter 共存

要使 SnapCenter Plug-in for Microsoft Exchange Server 與 SnapManager for Microsoft Exchange Server 共存，您需要在安裝了 SnapManager for Microsoft Exchange Server 的同一 Exchange Server 上安裝 SnapCenter SnapManager -in for Microsoft Exchange Server，禁用 SnapManager for Exchange 計劃，然後使用 SnapCenter Plug-in for Microsoft Exchange Server 配置新的計劃和備份。

開始之前

- SnapManager for Microsoft Exchange Server 和 SnapDrive for Windows 已安裝，且 SnapManager for Microsoft Exchange Server 備份存在於系統和 SnapInfo 目錄中。
- 您應該已刪除或回收不再需要的 SnapManager for Microsoft Exchange Server 所建立的備份。
- 您應該已從 Windows 排程器中暫停或刪除由 SnapManager for Microsoft Exchange Server 建立的所有計畫。
- 適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式和適用於 Microsoft Exchange Server 的 SnapManager 可以共存於同一 Exchange Server 上，但無法將現有的適用於 Microsoft Exchange Server 的 SnapManager 安裝升級至 SnapCenter。

SnapCenter 不提供升級選項。

- SnapCenter 不支援從 SnapManager for Microsoft Exchange Server 備份還原 Exchange 資料庫。

如果安裝 SnapCenter Plug-in for Microsoft Exchange Server 後未解除安裝 SnapManager for Microsoft Exchange Server，且稍後想要還原 SnapManager for Microsoft Exchange Server 備份，則必須執行其他步驟。

步驟

1. 在所有 DAG 節點上使用 PowerShell，確定 SnapDrive for Windows VSS 硬體提供者是否已註冊：*vssadmin list providers*

```
C:\Program Files\NetApp\SnapDrive>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {ddd3d232-a96f-4ac5-8f7b-250fd91fd102}
Version: 7. 1. 4. 6845
```

2. 從 SnapDrive 目錄中，從 SnapDrive for Windows 取消註冊 VSS 硬體提供者：*navssprv.exe -r service -u*

3. 驗證 VSS 硬體提供者是否已被刪除：*vssadmin list providers*
4. 將 Exchange 主機新增至SnapCenter，然後安裝適用於 Microsoft Windows 的SnapCenter外掛程式和適用於 Microsoft Exchange Server 的SnapCenter外掛程式。
5. 從所有 DAG 節點上的SnapCenter Plug-in for Microsoft Windows 目錄中，驗證 VSS 硬體提供者是否已註冊：*vssadmin list providers*

```
[PS] C:\Windows\system32>vssadmin list providers
vssadmin 1.1 - Volume Shadow Copy Service administrative command-line
tool
(C) Copyright 2001-2013 Microsoft Corp.

Provider name: 'Data ONTAP VSS Hardware Provider'
Provider type: Hardware
Provider Id: {31fca584-72be-45b6-9419-53a3277301d1}
Version: 7. 0. 0. 5561
```

6. 停止SnapManager for Microsoft Exchange Server 備份計畫。
7. 使用SnapCenter GUI，建立按需備份、設定排程備份以及設定保留設定。
8. 解除安裝適用於 Microsoft Exchange Server 的SnapManager。

如果您現在不卸載SnapManager for Microsoft Exchange Server，但稍後想要還原SnapManager for Microsoft Exchange Server 備份：

- a. 從所有 DAG 節點取消註冊適用於 Microsoft Exchange Server 的SnapCenter外掛程式：*navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

- b. 從 *C:\Program Files\NetApp\SnapDrive* 目錄中，在所有 DAG 節點上註冊SnapDrive for Windows：*navssprv.exe -r service -a hostname\username -p password*

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 `/opt/netapp/config/crl`。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

做好資料保護準備

在執行任何資料保護操作（例如備份、複製或復原作業）之前，您必須定義策略並設定環境。您也可以設定SnapCenter伺服器以使用SnapMirror和SnapVault技術。

若要利用SnapVault和SnapMirror技術，您必須在儲存裝置上設定並初始化來源磁碟區和目標磁碟區之間的資料保護關係。您可以使用 NetAppSystem Manager 或儲存控制台命令列來執行這些任務。

查找更多資訊

["開始使用 REST API"](#)

使用適用於 Microsoft Exchange Server 的SnapCenter外掛程式的先決條件

在使用 Exchange 外掛程式之前，SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。
- 登入SnapCenter。
- 透過新增或指派儲存系統連線並建立憑證來配置SnapCenter環境。



SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。SnapCenter支援的每個 SVM 都必須具有唯一的名稱。

- 新增主機，安裝適用於 Microsoft Windows 的SnapCenter插件和適用於 Microsoft Exchange Server 的SnapCenter插件，並發現（重新整理）資源。
- 使用適用於 Microsoft Windows 的SnapCenter外掛程式執行主機端儲存配置。
- 如果您使用SnapCenter Server 保護駐留在 VMware RDM LUN 上的 Exchange 資料庫，則必須部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊外掛程式。SnapCenter Plug-in for VMware vSphere文件包含更多資訊。



不支援 VMDK。

- 使用 Microsoft Exchange 工具將現有的 Microsoft Exchange Server 資料庫從本機磁碟移至支援的儲存體。
- 如果您想要備份複製，請設定SnapMirror和SnapVault關係。

對於SnapCenter 4.1.1 用戶，SnapCenter Plug-in for VMware vSphere包含有關保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.2.x 用戶，NetApp Data Broker 1.0 和 1.0.1 文件包含有關使用基於 Linux 的NetApp Data Broker 虛擬設備（開放虛擬設備格式）提供的適用SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。對於SnapCenter 4.3.x 用戶，SnapCenter Plug-in for VMware vSphere文件包含有關使用基於 Linux 的SnapCenter Plug-in for VMware vSphere保護虛擬化資料庫和檔案系統的資訊。

如何使用資源、資源群組和原則來保護 Exchange Server

在使用SnapCenter之前，了解與要執行的備份、還原和重新播種作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份的郵件資料庫或 Microsoft Exchange 資料庫可用性群組 (DAG)。
- SnapCenter資源組是主機或 Exchange DAG 上的資源集合，資源組可以包含整個 DAG 或單一資料庫。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

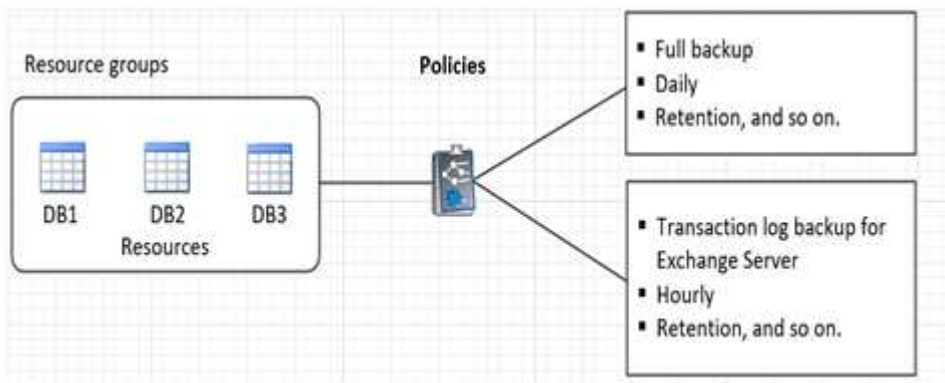
您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

資源組以前稱為資料集。

- 這些策略指定了備份頻率、副本保留、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇一個或多個策略。

可以將資源群組視為定義您想要保護的內容以及您想要在日期和時間方面保護的內容。把政策看作是定義你想如何保護它。例如，如果要備份主機的所有資料庫，則可以建立包含主機中所有資料庫的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加策略時，您可以設定資源組以每天執行一次完整備份，並配置另一個每小時執行一次日誌備份的計畫。下圖說明了資料庫的資源、資源群組和策略之間的關係：



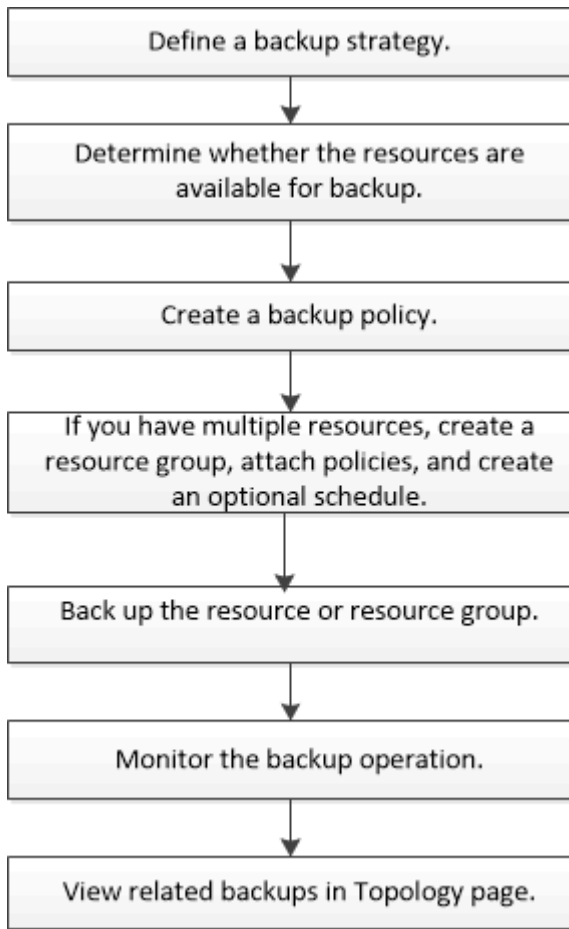
備份 Exchange 資源

備份工作流程

在您的環境中安裝適用於 Microsoft Exchange Server 的SnapCenter外掛程式時，您可以使用SnapCenter備份 Exchange 資源。

您可以安排多個備份同時在伺服器之間執行。不能對相同資源同時執行備份和復原作業。不支援同一卷上的主動和被動備份副本。

以下工作流程顯示了執行備份作業必須遵循的順序：



Exchange 資料庫和備份驗證

適用於 Microsoft Exchange Server 的 SnapCenter 外掛程式不提供備份驗證；但是，您可以使用 Exchange 提供的 Eseutil 工具來驗證 Exchange 資料庫和備份。

Microsoft Exchange Eseutil 工具是 Exchange 伺服器隨附的命令列公用程式。此實用程式可讓您執行一致性檢查以驗證 Exchange 資料庫和備份的完整性。

*最佳實務：*沒有必要對具有至少兩個副本的資料庫可用性群組 (DAG) 配置的一部分的資料庫執行一致性檢查。

有關更多信息，請參閱 ["Microsoft Exchange Server 文件"](#)。

確定 Exchange 資源是否可用於備份

資源是由您安裝的外掛程式維護的資料庫、Exchange 資料庫可用性群組。您可以將這些資源新增至資源組中，以便執行資料保護作業，但首先必須確定您有哪些可用資源。確定可用資源也可以驗證插件安裝是否已成功完成。

開始之前

- 您必須已經完成安裝 SnapCenter Server、新增主機、建立儲存系統連線、新增憑證和安裝 Exchange 插件

等任務。

- 若要利用單一郵件匣復原軟體的功能，您必須將活動資料庫定位在安裝了單一郵件匣復原軟體的 Exchange Server 上。
- 如果資料庫駐留在 VMware RDM LUN 上，則必須部署 SnapCenter Plug-in for VMware vSphere 並向 SnapCenter 註冊外掛程式。這 "[SnapCenter Plug-in for VMware vSphere 文檔](#)" 有更多資訊。

關於此任務

- 當「詳細資料」頁面中的「整體狀態」選項設定為「無法用於備份」時，您無法備份資料庫。當下列任一情況為真時，「總體狀態」選項將設定為「不可用於備份」：
 - 資料庫不在 NetApp LUN 上。
 - 資料庫狀態不正常。

當資料庫處於安裝、解除安裝、重新播種或復原掛起狀態時，它們不處於正常狀態。

- 如果您有資料庫可用性群組 (DAG)，則可以透過從 DAG 執行備份作業來備份群組中的所有資料庫。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從位於“資源”頁面左上角的插件下拉清單中選擇“**Microsoft Exchange Server**”。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*、資料庫可用性群組*或*資源群組*。

所有資料庫和 DAG 都以 FQDN 格式顯示其 DAG 或主機名，因此您可以區分多個資料庫。

點選  並選擇主機名稱和 Exchange Server 來過濾資源。然後您可以點擊  關閉篩選器窗格。

3. 按一下“刷新資源”。

新新增、重新命名或刪除的資源將更新至 SnapCenter 伺服器清單。



如果資料庫在 SnapCenter 之外重新命名，則必須刷新資源。

資源與資源名稱、資料庫可用性群組名稱、資料庫目前處於活動狀態的伺服器、具有副本的伺服器、上次備份的時間以及總體狀態等資訊一起顯示。

- 如果資料庫位於非 NetApp 儲存裝置上，則「整體狀態」欄位中將顯示「不可用於備份」。

在 DAG 中，如果主動資料庫副本位於非 NetApp 儲存體上，且至少有一個被動資料庫副本位於 NetApp 儲存體上，則「整體狀態」欄位中將顯示「未受保護」。

您無法對非 NetApp 儲存類型的資料庫執行資料保護操作。

- 如果資料庫位於 NetApp 儲存空間且未受到保護，則「總體狀態」欄位中將顯示「未受保護」。
- 如果資料庫位於 NetApp 儲存系統上且受到保護，則使用者介面會在 **Overall Status** 欄位中顯示 Backup not run 訊息。
- 如果資料庫位於 NetApp 儲存系統上且受到保護，且如果觸發了資料庫的備份，則使用者介面會在 **Overall Status** 欄位中顯示備份成功訊息。

為 Exchange Server 資料庫建立備份策略

您可以在使用 SnapCenter 備份 Microsoft Exchange Server 資源之前為 Exchange 資源或資源群組建立備份原則，也可以在建立資源群組或備份單一資源時建立備份原則。

開始之前

- 您必須已經定義了您的資料保護策略。

有關詳細信息，請參閱有關定義 Exchange 資料庫的資料保護策略的資訊。

- 您必須透過完成安裝 SnapCenter、新增主機、識別資源和建立儲存系統連線等任務來為資料保護做好準備。
- 您必須刷新（發現）Exchange Server 資源。
- 如果您要將快照複製到映像或保管庫，SnapCenter 管理員必須已為您指派來源磁碟區和目標磁碟區的儲存虛擬機器 (SVM)。
- 如果要在前言和後言中執行 PowerShell 腳本，則應設定 `usePowershellProcessforScripts` 參數為 true `web.config` 文件。

預設值為 false。

- 查看 SnapMirror 主動同步特定的先決條件和限制。欲了解詳細信息，請參閱 ["SnapMirror 主動同步的物件限制"](#)。

關於此任務

- 備份策略是一組規則，用於控制如何管理和保留備份以及資源或資源群組的備份頻率。此外，您也可以指定腳本設定。當您想要將策略重新用於另一個資源群組時，在策略中指定選項可以節省時間。
- 完整備份保留特定於給定的策略。使用策略 A 且完整備份保留期為 4 的資料庫或資源將保留 4 個完整備份，並且對相同資料庫或資源的策略 B 沒有影響，策略 B 可能具有保留期為 3 以保留 3 個完整備份。
- 日誌備份保留跨策略有效，並適用於資料庫或資源的所有日誌備份。因此，當使用策略 B 執行完整備份時，日誌保留設定會影響策略 A 在相同資料庫或資源上建立の日誌備份。同樣，策略 A の日誌保留設定會影響策略 B 在相同資料庫上建立の日誌備份。
- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：API /4.7/configsettings

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

最佳實務：最好根據您想要保留的完整備份和日誌備份的總數來設定輔助保留策略。配置輔助保留策略時，請記住，當資料庫和日誌位於不同的磁碟區時，每個備份可以有三個快照，而當資料庫和日誌位於同一磁碟區時，每個備份可以有兩個快照。

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則 SnapLock 保留期必須小於或等於上述保留天數。

指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數

量。

對於ONTAP 9.12.1 及以下版本、從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選“新建”。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在備份類型和複製頁面中，執行下列步驟：

a. 選擇備份類型：

如果你想...	這樣做...
備份資料庫檔案和所需的交易日誌	選擇*完整備份和日誌備份*。 資料庫採用日誌截斷備份，備份所有日誌，包括被截斷的日誌。  這是建議的備份類型。
備份資料庫檔案和未提交的交易日誌	選擇*完整備份*。 資料庫備份時會進行日誌截斷，截斷的日誌不會備份。
備份所有交易日誌	選擇*日誌備份*。 活動檔案系統上的所有交易日誌都已備份，且沒有日誌截斷。 在與即時日誌相同的磁碟上建立 <i>scebackupinfo</i> 目錄。該目錄包含指向 Exchange 資料庫增量變更的指針，它並不同於完整的日誌檔案。
備份所有資料庫檔案和交易日誌，而不截斷交易日誌文件	選擇*複製備份*。 所有資料庫和所有日誌均已備份，且沒有日誌截斷。您通常使用此備份類型來重新播種副本或測試或診斷問題。



您應該根據完整備份保留而不是最新 (UTM) 保留來定義日誌備份所需的空間。



處理 Exchange 磁碟區 (LUN) 時，為日誌和資料庫建立單獨的保管庫策略，並使用相同的標籤將日誌策略的保留 (keep) 設定為資料庫策略的每個標籤數量的兩倍。欲了解更多信息，請參閱 ["SnapCenter for Exchange 備份僅保留 Vault 目標日誌磁碟區上的一半快照"](#)

- b. 在資料庫可用性群組設定部分中，選擇一個操作：

對於這個領域...	這樣做...
備份活動副本	選擇此選項可僅備份所選資料庫的活動副本。 對於資料庫可用性群組 (DAG)，此選項僅備份 DAG 中所有資料庫的活動副本。 被動副本未備份。
在建立備份作業時選擇的伺服器上備份副本	選擇此選項可備份選定伺服器（主動伺服器和被動伺服器）上資料庫的任何副本。 對於 DAG，此選項將備份選定伺服器上所有資料庫的主動副本和被動副本。



在叢集配置中，備份會根據策略中設定的保留設定保留在叢集的每個節點上。如果叢集的擁有者節點發生變化，則會保留前一個所有者節點的備份。保留僅適用於節點層級。

- c. 在「計畫頻率」部分中，選擇一種或多種頻率類型：按需、每小時、每天、每週*和*每月。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期）。這使您能夠建立共享相同策略和備份頻率的資源群組，但允許您為每個策略指派不同的備份計畫。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計畫。

- a. 選擇策略標籤。



您可以為遠端複製的主快照指派 SnapMirror 標籤，從而允許主快照將快照複製作業從 SnapCenter 卸載到 ONTAP 二級系統。無需在策略頁面中啟用 SnapMirror 或 SnapVault 選項即可完成此操作。

- b. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
建立本地快照後更新SnapMirror	選擇此選項可在另一個磁碟區上保留備份集的鏡像副本（SnapMirror）。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 應為SnapMirror主動同步啟用此選項。  如果為 Exchange ONTAP磁碟區設定了SnapMirror主動同步，則無法使用僅主原則。 SnapCenter不允許這樣做。您應該啟用“鏡像”選項。 點選拓樸頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓樸頁面中查看 Exchange 備份"。
建立本機快照後更新SnapVault	選擇此選項可執行磁碟到磁碟的備份複製。
錯誤重試次數	輸入進程停止之前應發生的複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

6. 在保留頁面中，配置保留設定。

顯示的選項取決於您先前選擇的備份類型和頻率類型。



最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。



如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。

a. 在「日誌備份保留設定」部分中，選擇下列選項之一：

如果你想...	這樣做...
僅保留特定數量的日誌備份	選擇*保留日誌的完整備份數*，並指定您想要最新還原的完整備份數。 最新 (UTM) 保留適用於透過完整或日誌備份建立的日誌備份。例如，如果將 UTM 保留設定配置為保留最近 5 次完整備份的日誌備份，則會保留最近 5 次完整備份的日誌備份。 作為完整和日誌備份的一部分建立的日誌資料夾將作為 UTM 的一部分自動刪除。您不能手動刪除日誌資料夾。例如，如果完整或完整和日誌備份的保留設定設為 1 個月，而 UTM 保留設定為 10 天，則作為這些備份的一部分建立的日誌資料夾將根據 UTM 刪除。因此，只有 10 天的日誌資料夾會存在，並且所有其他備份都標記為時間點復原。 如果您不想執行最新恢復，可以將 UTM 保留值設為 0。這將啟用時間點恢復操作。 *最佳實務：*最好該設定必須等於完整備份保留設定部分中的總快照（完整備份）的設定。這可確保每次完整備份時都保留日誌檔案。
將備份副本保留特定天數	選擇「保留最後的日誌備份」選項，並指定保留日誌備份副本的天數。 日誌備份最多保留完整備份的天數。
快照鎖定期	選擇*Snapshot 副本鎖定期限*，並選擇天、月或年。 SnapLock保留期應少於 100 年。

如果您選擇「日誌備份」作為備份類型，則日誌備份將保留為完整備份的最新保留設定的一部分。

- b. 在完整備份保留設定部分中，為按需備份選擇以下選項之一，然後為完整備份選擇一個：

對於這個領域...	這樣做...
僅保留特定數量的快照	如果要指定要保留的完整備份數量，請選擇*要保留的 Snapshot 副本總數*選項，並指定要保留的快照（完整備份）數量。 如果完整備份的數量超過指定數量，則會刪除超過指定數量的完整備份，並先刪除最舊的副本。
保留完整備份特定天數	選擇「保留快照副本」選項，並指定保留快照（完整備份）的天數。

對於這個領域...	這樣做...
主快照鎖定期	選擇*主快照副本鎖定期限*，並選擇天、月或年。 SnapLock保留期應少於 100 年。
二級快照鎖定期	選擇*次快照副本鎖定期限*，並選擇天、月或年。

如果 DAG 配置中的主機上有一個僅具有日誌備份而沒有完整備份的資料庫，則日誌備份將透過以下方式保留：

- 預設情況下，SnapCenter會在 DAG 中的所有其他主機中尋找此資料庫的最早完整備份，並刪除在完整備份之前在此主機上進行的所有日誌備份。
- 您可以透過在 `C:\Program Files\NetApp\SnapCenter WebApp\web.config` 檔案中新增按鍵 **MaxLogBackupOnlyCountWithoutFullBackup** 來覆寫僅具有日誌備份的 DAG 中主機上的資料庫的上述預設保留行為。

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

在範例中，值 10 表示您在主機上保留最多 10 個日誌備份。

7. 在腳本頁面中，分別輸入應在備份作業之前或之後執行的前置腳本或後置腳本的路徑和參數。

- 預設備份參數包括“\$Database”和“\$ServerInstance”。
- Postscript 備份參數包括「\$Database」、「\$ServerInstance」、「\$BackupName」、「\$LogDirectory」和「\$LogSnapshot」。

您可以執行腳本來更新 SNMP 陷阱、自動發出警報、發送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

8. 查看摘要，然後按一下「完成」。

為 Exchange 伺服器建立資源組並附加策略

任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型和保護計劃。

關於此任務

- SCRIPTS_PATH 是使用插件主機的 `SMCoreServiceHost.exe.Config` 檔案中的 `PredefinedWindowsScriptsDirectory` 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：`API /4.7/configsettings`

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新資料庫新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下將新資料庫新增至現有資源組。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 Microsoft Exchange Server 外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*。



如果您最近為SnapCenter新增了資源，請按一下「刷新資源」以查看新新增的資源。

3. 按一下“新建資源組”。
4. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組名稱。 資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
對 Snapshot 副本使用自訂名稱格式	可選：輸入自訂快照名稱和格式。 例如， <i>customtext_resourcegroup_policy_hostname</i> 或 <i>resourcegroup_hostname</i> 。預設情況下，時間戳記會附加到快照名稱。

5. 在資源頁面中，執行以下步驟：
 - a. 從下拉清單中選擇資源類型和資料庫可用性群組來過濾可用資源清單。



如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

在可用資源和選定資源部分中，資料庫名稱會與主機的 FQDN 一起顯示。此 FQDN 僅表示資料庫在該特定主機上處於活動狀態，且可能不會在該主機上進行備份。您應該從伺服器選擇選項中選擇一個或多個備份伺服器，如果您在政策中選擇了*在建立備份作業時選擇的伺服器上備份副本*選項，則需要在該伺服器中進行備份。

- b. 在搜尋文字方塊中輸入資源名稱，或捲動以找到資源。
- c. 若要將資源從可用資源部分移至選取資源部分，請執行下列步驟之一：
 - 選擇「自動選擇相同儲存磁碟區上的所有資源」以將同一磁碟區上的所有資源移至「選取資源」部

分。

- 從「可用資源」部分選擇資源，然後按一下向右箭頭將其移至「選定資源」部分。

SnapCenter for Microsoft Exchange Server 的資源組每個快照不能有超過 30 個資料庫。如果一個資源組中有超過 30 個資料庫，則會為其他資料庫建立第二個快照。因此，在主備份作業下建立了 2 個子作業。對於具有二級複製的備份、當 SnapMirror 或 SnapVault 更新正在進行中、可能會出現兩個子作業的更新重疊的情況。即使日誌顯示作業已完成，主備份作業仍會繼續執行。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 * 來建立策略  *。



如果政策包含 * 在建立備份作業時選擇的伺服器上備份副本 * 選項，則會顯示伺服器選擇選項以選擇一個或多個伺服器。伺服器選擇選項將僅列出所選資料庫位於 NetApp 儲存裝置上的伺服器。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 在「配置所選策略的計畫」部分中，按一下 *  * 在您想要設定計畫的政策「設定計畫」欄位中。
- c. 在「為政策_policy_name_新增計畫」對話方塊中，透過指定開始日期、到期日和頻率來配置計畫，然後按一下「確定」。

您必須對策略中列出的每個頻率執行此操作。配置的計畫列在「為選定策略配置計畫」部分的「已套用的計畫」列中。

當第三方備份計畫與 SnapCenter 備份計畫重疊時，不支援第三方備份計畫。

7. 在通知頁面中，從 * 電子郵件首選項 * 下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇 * 附加作業報告 *。

對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令指定 SMTP 伺服器詳細資訊 `Set-SmSmtServer`。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

8. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 為 Exchange Server 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 進行備份和還原之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

步驟

1. 使用 `Open-SmConnection` 命令。

此範例開啟一個 PowerShell 會話：

```
PS C:\> Open-SmConnection
```

2. 使用 `Add-SmStorageConnection` 命令。

此範例建立一個新的儲存系統連線：

```
PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
-Timeout 60
```

3. 使用以下方式建立新的運行方式帳戶 `Add-Credential` 命令。

此範例使用 Windows 憑證建立一個名為 ExchangeAdmin 的新運行方式帳戶：

```
PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
-Credential sddev\administrator
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份 Exchange 資料庫

如果資料庫不屬於任何資源群組，您可以從資源頁面備份資料庫或資料庫可用性群組。

開始之前

- 您必須已經建立了備份策略。
- 您必須已將備份作業正在使用的聚合指派給資料庫使用的 SVM。

- 如果要備份與二級儲存具有SnapMirror關係的資源，則指派給儲存使用者的角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。
- 如果您要對在NetApp和非NetApp儲存上具有主動/被動資料庫副本的資料庫或資料庫可用性群組執行備份，並且您在政策中選擇了*備份主動副本*或*備份在備份作業建立時要選擇的伺服器上的副本*選項，則備份作業將進入警告狀態。對於NetApp儲存上的主動/被動資料庫副本，備份將會成功；對於非NetApp儲存體上的主動/被動資料庫副本，備份將會失敗。

*最佳實務：*不要同時執行主動資料庫和被動資料庫的備份。可能會出現競爭情況，並且其中一個備份可能會失敗。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“Microsoft Exchange Server 外掛程式”。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資料庫可用性群組*。

在資源頁面中，圖示表示資料庫位於非NetApp儲存體上。



在 DAG 中，如果主動資料庫副本位於非NetApp儲存體上，且至少一個被動資料庫副本駐留在NetApp儲存上，那麼您可以保護資料庫。

點擊  *，然後選擇主機名稱和資料庫類型來過濾資源。然後您可以點擊  * 關閉篩選窗格。

- 如果要備份資料庫，請按一下資料庫名稱。
 - i. 如果顯示拓撲視圖，請按一下「保護」。
 - ii. 如果顯示資料庫 - 保護資源精靈，請繼續步驟 3。
 - 如果要備份資料庫可用性群組，請按一下資料庫可用性群組名稱。
3. 如果要指定自訂快照名稱，請在資源頁面中選取*使用自訂名稱格式作為快照副本*複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，*customtext_policy_hostname* 或 *resource_hostname*。預設情況下，時間戳記會附加到快照名稱。

4. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 *  *。



如果政策包含*在建立備份作業時選擇的伺服器上備份副本*選項，則會顯示伺服器選擇選項以選擇一個或多個伺服器。伺服器選擇選項將僅列出所選資料庫位於NetApp儲存裝置上的伺服器。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點擊 *  * 在您想要設定計畫的政策的設計計畫列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

5. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源執行的備份作業

的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

6. 查看摘要，然後按一下「完成」。

進入資料庫拓撲頁面。

7. 點選*立即備份*。

8. 在備份頁面中，執行以下步驟：

- a. 如果您已對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。

9. 透過雙擊頁面底部「活動」窗格中的作業來監控備份進度，以顯示「作業詳細資料」頁面。

- 在MetroCluster配置中， SnapCenter可能無法在故障轉移後偵測到保護關係。

有關信息，請參閱：["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java堆大小不夠大，則備份可能會失敗。

若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method` 命令啟動SnapCenter VMware 插件服務。將此指令更新為以下內容：`Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmPolicy cmdlet 建立備份策略。

此範例建立一個具有完整備份和日誌備份 Exchange 備份類型的新備份策略：

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy  
-PolicyType Backup -PluginPolicytype SCE -SceBackupType  
FullBackupAndLogBackup -BackupActiveCopies
```

此範例建立一個新的備份策略，其中包含每小時完整備份和日誌備份 Exchange 備份類型：

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Hourly_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies -ScheduleType Hourly
-RetentionSettings
@{'BackupType'='DATA';'ScheduleType'='Hourly';'RetentionCount'='10'}
```

此範例建立新的備份策略以僅備份 Exchange 日誌：

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. 使用 Get-SmResources cmdlet 來發現主機資源。

此範例發現指定主機上的 Microsoft Exchange Server 外掛程式的資源：

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. 使用 Add-SmResourceGroup cmdlet 為 SnapCenter 新增新的資源組。

此範例使用指定的政策和資源建立一個新的 Exchange Server 資料庫備份資源組：

```
C:\PS> Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG
-Description 'Backup ResourceGroup with Full and Log backup policy'
-PluginCode SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy
-Resources @{'Host'='sce-w2k12-exch';'Type'='Exchange Database';'Names'='sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_1,sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2'}
```

此範例使用指定的政策和資源建立一個新的 Exchange 資料庫可用性群組 (DAG) 備份資源群組：

```
Add-SmResourceGroup -ResourceGroupName SCE_w2k12_bkp_RG -Description
'Backup ResourceGroup with Full and Log backup policy' -PluginCode
SCE -Policies
SCE_w2k12_Full_bkp_Policy,SCE_w2k12_Full_Log_bkp_Policy,SCE_w2k12_Log_bkp_Policy
-Resources @{"Host"="DAGSCE0102";"Type"="Database Availability Group";"Names"="DAGSCE0102"}
```

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy  
SCE_w2k12_Full_Log_bkp_Policy
```

此範例建立了到輔助儲存的新備份：

```
New-SMBackup -DatasetName ResourceGroup1 -Policy  
Secondary_Backup_Policy4
```

6. 使用 Get-SmBackupReport cmdlet 查看備份作業的狀態。

此範例顯示在指定日期執行的所有作業的作業摘要報表：

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

此範例顯示特定作業 ID 的作業摘要報表：

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

可以透過執行 `_Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，參見 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

備份 Exchange 資源組

資源組是主機或 Exchange DAG 上的資源集合，資源組可以包括整個 DAG 或單一資料庫。您可以從資源頁面備份資源組。

開始之前

- 您必須已建立附加有策略的資源群組。
- 您必須已將備份作業正在使用的聚合指派給資料庫使用的儲存虛擬機器 (SVM)。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。
- 如果資源組有來自不同主機的多個資料庫，則由於網路問題，某些主機上的備份作業可能會延遲啟動。您應該配置 `MaxRetryForUninitializedHosts` 在 `web.config` 透過使用 `Set-SmConfigSettings` PowerShell 指令。
- 在資源群組中，如果您包含一個在 NetApp 和非 NetApp 儲存裝置上具有主動/被動資料庫副本的資料庫或資料庫可用性群組，並且您在原則中選擇了 備份主動副本 或 備份在備份作業建立時要選擇的伺服器上的副本 選項，則備份作業將進入警告狀態。

對於 NetApp 儲存上的主動/被動資料庫副本，備份將會成功；對於非 NetApp 儲存體上的主動/被動資料庫副本，備份將會失敗。

關於此任務

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“**Microsoft Exchange Server 外掛程式**”。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或按一下 * 來搜尋資源組  *，然後選擇標籤。然後您可以點擊 *  * 關閉篩選窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後按一下「立即備份」。
4. 在備份頁面中，執行以下步驟：
 - a. 如果您已將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。
5. 透過雙擊頁面底部「活動」窗格中的作業來監控備份進度，以顯示「作業詳細資料」頁面。

監視備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。

- d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

監視活動窗格中的操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消 Exchange 資料庫的備份作業

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	- 在左側導覽窗格中，按一下「監控」>「作業」。 - 選擇操作，然後按一下「取消作業」。
活動窗格	- 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 - 選擇操作。 - 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓樸頁面中查看 **Exchange** 備份

當您準備備份資源時，您可能會發現查看主儲存和輔助儲存上所有備份的圖形表示很有幫助。

關於此任務

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份。您可以查看這些備份的詳細信息，然後選擇它們來執行資料保護作業。

您可以在「管理副本」檢視中查看以下圖標，以確定備份是否在主儲存或輔助儲存上可用（鏡像副本或保管庫副本）。

-  顯示主儲存體上可用的備份數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份數量。

◦ 顯示的備份數量包括從輔助儲存中刪除的備份。

例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。

最佳實務：為確保顯示正確的複製備份數量，我們建議您刷新拓樸。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。

-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資料庫、資源或資源群組。
3. 從資料庫詳細資訊檢視或資源組詳細資料檢視中選擇資源。

如果資源受到保護，則會顯示所選資源的拓樸頁面。

4. 請查看摘要卡部分，以了解主儲存和輔助儲存上可用的備份數量的摘要。

摘要卡部分顯示備份總數和日誌備份總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 在故障轉移後自動配置為新的主目標。
- 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」以查看備份的詳細資訊。

備份的詳細資訊以表格形式顯示。

6. 從表格中選擇備份，然後按一下資料保護圖示執行還原、重新命名和刪除操作。



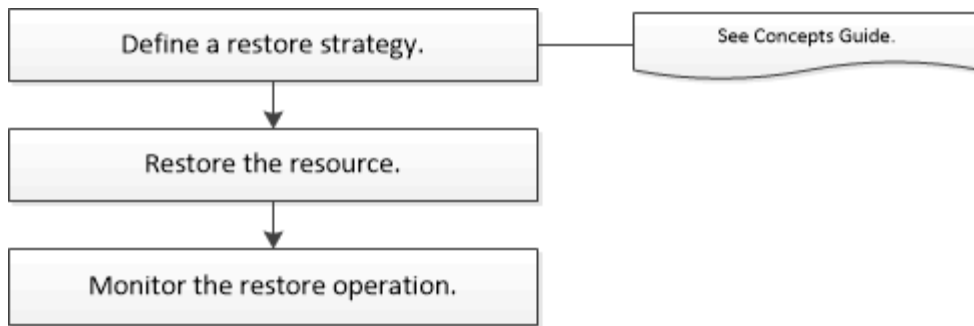
您無法重新命名或刪除輔助儲存體上的備份。刪除快照由ONTAP保留設定處理。

還原 Exchange 資源

復原工作流程

您可以使用SnapCenter透過將一個或多個備份還原到活動檔案系統來還原 Exchange 資料庫。

以下工作流程顯示了執行 Exchange 資料庫還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份和復原作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

還原 Exchange 資料庫的要求

從適用於 Microsoft Exchange Server 備份的 SnapCenter 外掛程式還原 Exchange Server 資料庫之前，必須確保符合幾個要求。



若要完全使用還原功能，必須將 SnapCenter 伺服器 and SnapCenter Plug-in for Exchange 資料庫都升級到 4.6。

- 在復原資料庫之前，Exchange Server 必須處於線上狀態並且正在執行。
- 資料庫必須存在於 Exchange Server 上。



不支援恢復已刪除的資料庫。

- 必須暫停資料庫的 SnapCenter 方案。
- SnapCenter 伺服器 and 適用於 Microsoft Exchange Server 主機的 SnapCenter 插件必須連接到包含要還原的備份的主儲存和輔助儲存。

還原 Exchange 資料庫

您可以使用 SnapCenter 還原備份的 Exchange 資料庫。

開始之前

- 您必須備份資源組、資料庫或資料庫可用性群組 (DAG)。
- 當 Exchange 資料庫遷移到另一個位置時，復原作業對舊備份不起作用。
- 如果您要將快照複製到映像或保管庫，SnapCenter 管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。
- 在 DAG 中，如果主動資料庫副本位於非 NetApp 儲存體上，而您想要從 NetApp 儲存裝置上的被動資料庫副本備份進行還原，則將被動副本 (NetApp 儲存) 設為主動副本，重新整理資源並執行還原作業。

運行 `Move-ActiveMailboxDatabase` 命令將被動資料庫副本設為主動資料庫副本。

這 "[Microsoft 文件](#)" 包含有關此命令的資訊。

關於此任務

- 當對資料庫執行復原作業時，資料庫將重新安裝在同一主機上，並且不會建立新的磁碟區。
- 必須從單一資料庫還原 DAG 等級的備份。
- 當存在 Exchange 資料庫 (.edb) 檔案以外的檔案時，不支援完整磁碟還原。

如果磁碟包含 Exchange 檔案（例如用於複製的檔案），則 Exchange 外掛程式不會對磁碟執行完全還原。當完全還原可能會影響 Exchange 功能時，Exchange 外掛程式會執行單一檔案還原操作。

- Exchange 外掛程式無法還原 BitLocker 加密的磁碟機。
- SCRIPTS_PATH 是使用插件主機的 SMCoreServiceHost.exe.Config 檔案中的 PredefinedWindowsScriptsDirectory 鍵定義的。

如果需要，您可以變更此路徑並重新啟動 SMcore 服務。為了安全起見，建議您使用預設路徑。

可以透過 API 從 Swagger 顯示該鍵的值：[API /4.7/configsettings](#)

您可以使用 GET API 來顯示鍵的值。不支援 SET API。

- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。
- 對於 SnapMirror 活動同步恢復操作，您必須從主位置選擇備份。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下資源頁面左上角的「資源」。
2. 從下拉清單中選擇 Exchange Server 插件。
3. 在資源頁面中，從視圖清單中選擇*資料庫*。
4. 從清單中選擇資料庫。
5. 從“管理副本”視圖中，從“主備份”表中選擇“備份”，然後按一下**。
6. 在「選項」頁面中，選擇下列日誌備份選項之一：

選項	描述
所有日誌備份	選擇*所有日誌備份*執行最新的備份還原作業，以還原完整備份後所有可用的日誌備份。
通過日誌備份直到	選擇「按日誌備份直到」來執行時間點還原作業，該操作會根據日誌備份直到所選日誌來還原資料庫。  下拉清單中顯示的日誌數量是基於 UTM。例如，如果完整備份保留為 5，UTM 保留為 3，則可用的日誌備份數為 5，但在下拉式選單中僅列出 3 個日誌來執行復原作業。
按特定日期直至	選擇「以特定日期直到」來指定將交易日誌套用到復原的資料庫的日期和時間。此時間點還原作業將還原在指定日期和時間的最後一次備份之前記錄的交易日誌條目。
沒有任何	當您只需要還原完整備份而不還原任何日誌備份時，請選擇「無」。

您可以執行下列操作之一：

- 恢復後恢復並掛載資料庫 - 預設選擇此選項。
- 恢復前不要驗證備份中交易日誌的完整性 - 預設情況下，SnapCenter在執行復原作業之前驗證備份中交易日誌的完整性。

*最佳實務：*您不應選擇此選項。

7. 在腳本頁面中，分別輸入應在復原作業之前或之後執行的預腳本或後腳本的路徑和參數。

恢復處方參數包括 \$Database 和 \$ServerInstance。

復原後記參數包括 \$Database、\$ServerInstance、\$BackupName、\$LogDirectory 和 \$TargetServerInstance。

您可以執行腳本來更新 SNMP 陷阱、自動發出警報、發送日誌等。



前言或後記路徑不應包含磁碟機或共用。該路徑應相對於 SCRIPTS_PATH。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

9. 查看摘要，然後按一下「完成」。

10. 您可以透過展開頁面底部的活動面板來查看還原作業的狀態。

您應該使用「監控」>「作業」頁面來監控復原過程。

從備份還原活動資料庫時，如果副本和活動資料庫之間存在滯後，則被動資料庫可能會進入掛起或失敗狀態。

當活動資料庫的日誌鏈分叉並開始中斷複製的新分支時，可能會發生狀態變化。Exchange Server 嘗試修復副本，但如果無法修復，則在還原後，您應該建立新的備份，然後重新播種副本。

PowerShell cmdlet

步驟

1. SnapCenter `Open-SmConnection` 命令。

```
Open-smconnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. 使用 `Get-SmBackup` 命令。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
-----	-----
341	ResourceGroup_36304978_UTM...
12/8/2017 4:13:24 PM	Full Backup
342	ResourceGroup_36304978_UTM...
12/8/2017 4:16:23 PM	Full Backup
355	ResourceGroup_06140588_UTM...
12/8/2017 6:32:36 PM	Log Backup
356	ResourceGroup_06140588_UTM...
12/8/2017 6:36:20 PM	Full Backup

3. 使用 `Restore-SmBackup` 命令。

此範例恢復最新備份：

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true
```

此範例還原時間點備份：

```
C:\ PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341  
-IsRecoverMount:$true -LogRestoreType ByTransactionLogs -LogCount 2
```

此範例將二級儲存上的備份還原到主儲存：

```
C:\ PS> Restore-SmBackup -PluginCode 'SCE' -AppObjectId 'DB2'  
-BackupId 81 -IsRecoverMount:$true -Confirm:$false  
-archive @{Primary="paw_vs:vol1";Secondary="paw_vs:vol1_mirror"}  
-logrestoretype All
```

這 `-archive` 參數可讓您指定要用於還原的主磁碟區和輔助磁碟區。

這 `-IsRecoverMount:\$true` 參數可讓您在還原後掛載資料庫。

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

郵件和郵箱的粒度恢復

單一郵件匣復原 (SMBR) 軟體可讓您還原和復原郵件或郵件信箱，而不是完整的 Exchange 資料庫。

僅僅為了恢復一封郵件而恢復整個資料庫將耗費大量的時間和資源。SMBR 透過建立快照的複製副本，然後使用 Microsoft API 在 SMBR 中安裝郵箱來協助快速復原郵件。有關如何使用 SMBR 的信息，請參閱 "[SMBR 管理指南](#)"。

有關 SMBR 的更多信息，請參閱以下內容：

- "[如何使用 SMBR 手動恢復單一項目（也適用於 Ontrack Power Control 恢復）](#)"
- "[如何使用 SnapCenter 從 SMBR 中的二級儲存進行還原](#)"
- "[使用 SMBR 從 SnapVault 恢復 Microsoft Exchange 郵件](#)"

從輔助儲存還原 Exchange Server 資料庫

您可以從輔助儲存體（映像或保管庫）還原備份的 Exchange Server 資料庫。

您必須已將快照從主儲存複製到輔助儲存。

關於此任務

- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。
- 對於 SnapMirror 活動同步恢復操作，您必須從主位置選擇備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“**Microsoft Exchange Server 外掛程式**”。
2. 在資源頁面中，從*視圖*下拉清單中選擇*資料庫*或*資源組*。
3. 選擇資料庫或資源組。

進入資料庫或資源組拓撲頁面。

4. 在「管理副本」部分，從輔助儲存系統（鏡像或保險庫）中選擇「備份」。
5. 從清單中選擇備份，然後按一下 。
6. 在「位置」頁面中，選擇用於還原所選資源的目標磁碟區。
7. 完成還原精靈，查看摘要，然後按一下「完成」。

重新植入被動 Exchange 節點副本

如果您需要重新播種副本（例如，當副本損壞時），您可以使用 SnapCenter 中的重新播種功能重新播種到最新備份。

開始之前

您必須已經建立了要重新播種的資料庫的備份。

+ 為了避免節點之間滯後，您可以在執行重新播種作業之前建立新的備份，或選擇具有最新備份的主機。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“**Microsoft Exchange Server 外掛程式**”。
2. 在資源頁面中，從視圖清單中選擇適當的選項：

選項	描述
重新植入單一資料庫	從視圖清單中選擇*資料庫*。
在 DAG 中重新植入資料庫	從視圖清單中選擇“資料庫可用性群組”。

3. 選擇您想要重新播種的資源。
4. 在「管理副本」頁面中，按一下「重新播種」。
5. 從重新播種精靈中的不健康資料庫副本清單中，選擇要重新播種的資料庫副本，然後按一下「下一步」。
6. 在「主機」視窗中，選擇要重新播種的備份主機，然後按一下「下一步」。
7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

8. 查看摘要，然後按一下「完成」。
9. 您可以透過展開頁面底部的活動面板來查看作業的狀態。



如果被動資料庫副本駐留在非NetApp儲存裝置上，則不支援重新播種作業。

使用 PowerShell cmdlet 為 Exchange 資料庫重新設定副本

您可以使用 PowerShell cmdlet 透過使用同一主機上的最新副本或備用主機上的最新副本來恢復不健康的副本。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. SnapCenter ``Open-SmConnection`` 命令。

```
Open-smconnection -SMSbaseurl https:\\snapctr.demo.netapp.com:8146/
```

2. 使用 ``reseed-SmDagReplicaCopy`` 命令。

此範例使用主機「mva-rx200.netapp.com」上的最新備份重新播種該主機上名為 `execdb` 的資料庫的失敗副本。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb
```

此範例使用備用主機「mva-rx201.netapp.com」上資料庫的最新備份（生產/副本）重新播種名為 execdb 的資料庫的失敗副本。

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database  
execdb -BackupHost "mva-rx201.netapp.com"
```

監視恢復操作

您可以使用「作業」頁面監控不同SnapCenter還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

取消 Exchange 資料庫的還原操作

您可以取消排隊的還原作業。

您應該以SnapCenter管理員或作業所有者的身分登入才能取消恢復操作。

關於此任務

- 您可以從「監視」頁面或「活動」窗格取消排隊的復原操作。
- 您無法取消正在執行的復原操作。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消排隊的還原作業。
- 對於無法取消的復原操作，「取消作業」按鈕將被停用。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊復原作業。

步

執行下列操作之一：

從...	行動
監控頁面	1. 在左側導覽窗格中，按一下「監控」>「作業」。 2. 選擇作業並點選「取消作業」。
活動窗格	1. 啟動恢復操作後，按一下在活動窗格上查看最近的五項操作。 2. 選擇操作。 3. 在「工作詳情」頁面中，按一下「取消工作」。

保護 IBM Db2

適用於 IBM Db2 的SnapCenter插件

適用於 IBM Db2 的SnapCenter插件概述

IBM Db2 資料庫的SnapCenter外掛程式是NetApp SnapCenter software的主機端元件，可實現 IBM Db2 資料庫的應用程式感知資料保護管理。IBM Db2 資料庫外掛程式可自動執行SnapCenter環境中 IBM Db2 資料庫的備份、復原和複製。

- SnapCenter 6.0 支援 IBM Db2 10.5 及更高版本。
- SnapCenter 6.0.1 支援 IBM Db2 9.7.x 及更高版本。此外，從SnapCenter 6.0.1 開始，支援 AIX 上的 IBM Db2。

SnapCenter支援單一執行個體和多重執行個體 Db2 設定。您可以在 Linux 和 Windows 環境中使用 IBM Db2 資料庫外掛程式。在 Windows 環境中，Db2 將作為手動資源得到支援。



不支援 Db2 pureScale 環境和 Db2 多節點 (DPF) 系統。

安裝 IBM Db2 資料庫外掛程式後，您可以使用具有NetApp SnapMirror技術的SnapCenter在另一個磁碟區上建立備份集的鏡像副本。您也可以使用具有NetApp SnapVault技術的插件來執行磁碟到磁碟的備份複製，以符合標準。

SnapCenter Plug-in for Db2 支援ONTAP和 Azure NetApp檔案儲存佈局上的 NFS 和 SAN。

支援VMDK、vVol、RDM虛擬儲存佈局。

使用適用於 IBM Db2 的SnapCenter插件可以做什麼

在您的環境中安裝 IBM Db2 資料庫外掛程式時，您可以使用SnapCenter備份、還原和複製 IBM Db2 資料庫及其資源。您也可以執行支援這些操作的任務。

- 新增資料庫。
- 建立備份。
- 從備份中復原。
- 克隆備份。
- 安排備份作業。
- 監控備份、復原和克隆作業。
- 查看備份、復原和克隆作業的報告。

適用於 IBM Db2 的SnapCenter插件功能

SnapCenter與插件應用程式以及儲存系統上的NetApp技術整合。若要使用 IBM Db2 資料庫插件，您需要使用SnapCenter圖形使用者介面。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份、復原和複製作業、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以及監控所有外掛程式中的作業。

- 自動化中央管理

您可以安排備份作業、設定基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷**NetApp**快照複製技術

SnapCenter使用NetApp快照技術和 IBM Db2 資料庫外掛程式來備份資源。

使用 IBM Db2 外掛程式還可帶來以下好處：

- 支援備份、復原和複製工作流程
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 使用NetApp FlexClone技術建立節省空間的資源時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 作為建立備份的一部分，支援ONTAP的一致性群組 (CG) 快照功能。
- 能夠跨多個資源主機同時執行多個備份

在單次操作中，當單一主機中的資源共用同一磁碟區時，快照就會合併。

- 能夠使用外部命令建立快照。
- 支援 XFS 檔案系統上的 Linux LVM。

SnapCenter Plug-in for IBM Db2 支援的儲存類型

SnapCenter支援實體機器和虛擬機器 (VM) 上的多種儲存類型。在安裝適用於 IBM Db2 的SnapCenter插件之前，您必須驗證對儲存類型的支援。

機器	儲存類型
實體伺服器	• FC 連接的 LUN • iSCSI 連接的 LUN • NFS 連結卷

機器	儲存類型
VMware ESXi	- 透過 FC 或 iSCSI ESXi HBA 連線的 RDM LUN 主機匯流排適配器 (HBA) 掃描可能需要很長時間才能完成，因為SnapCenter會掃描主機中存在的所有主機匯流排適配器。 您可以編輯位於 <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> 的 LinuxConfig.pm 文件，將 SCSI_HOSTS_OPTIMIZED_RESCAN 參數的值設定為 1，以僅重新掃描 HBA_DRI VBA 中列出的那些參數的值。 - iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統 - NFS 資料儲存上的 VMDK - VMFS 上的 VMDK 已建立 - NFS 磁碟區直接連接到客戶系統 - NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

IBM Db2 外掛程式所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - 倫
 - lun 創建
 - lun 創建
 - lun 創建
 - lun 刪除
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 重新命名

- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun 映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun 修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線

- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照修改-快照鎖定到期時間
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面

- 網路介面顯示
- 虛擬伺服器

為 IBM Db2 的SnapMirror和SnapVault複製準備儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

IBM Db2 的備份策略

定義 IBM Db2 的備份策略

在建立備份作業之前定義備份策略有助於您獲得成功復原或複製資源所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

關於此任務

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

步驟

1. 確定何時應該備份資源。
2. 確定您需要多少個備份作業。
3. 決定如何命名您的備份。
4. 決定是否要建立基於 Snapshot 副本的策略來備份資料庫的應用程式一致的快照。
5. 決定是否要使用NetApp SnapMirror技術進行複製或使用NetApp SnapVault技術進行長期保留。
6. 確定來源儲存系統和SnapMirror目標上的快照的保留期限。

7. 確定是否要在備份作業之前或之後執行任何命令，並提供前言或後記。

Linux主機上的資源自動發現

資源是 Linux 主機上由SnapCenter管理的 IBM Db2 資料庫和執行個體。安裝適用於 IBM Db2 外掛程式的SnapCenter外掛程式後，該 Linux 主機上所有執行個體的 IBM Db2 資料庫都會自動被發現並顯示在「資源」頁面中。

支援的備份類型

備份類型指定您要建立的備份類型。 SnapCenter支援 IBM Db2 資料庫的基於快照複製的備份類型。

基於快照副本的備份

基於快照副本的備份利用NetApp快照技術來建立 IBM Db2 資料庫所在磁碟區的線上只讀副本。

SnapCenter Plug-in for IBM Db2 如何使用一致性群組快照

您可以使用外掛程式為資源組建立一致性組快照。一致性群組是一個可以容納多個磁碟區的容器，以便您可以將它們作為一個實體進行管理。一致性組是多個磁碟區的同時快照，提供一組磁碟區的一致副本。

您也可以指定儲存控制器對快照進行一致分組的等待時間。可用的等待時間選項有*緊急*、中等*和*寬鬆。您也可以在一致的群組快照操作期間啟用或停用任意位置寫入檔案佈局 (WAFL) 同步。 WAFL同步提高了一致性組快照的效能。

SnapCenter如何管理資料備份

SnapCenter管理儲存系統和檔案系統層級的資料備份。

根據保留設定刪除主儲存或輔助儲存上的快照及其在 IBM Db2 目錄中的對應項目。

確定 IBM Db2 備份計畫的注意事項

確定備份計畫的最關鍵因素是資源的變化率。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

備份計畫分為兩部分，如下所示：

- 備份頻率（執行備份的頻率）

備份頻率（對於某些外掛程式也稱為計畫類型）是策略配置的一部分。例如，您可以將備份頻率設定為每小時、每天、每週或每月。

- 備份計畫（確切執行備份的時間）

備份計畫是資源或資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則

可以將計劃配置為每週四晚上 10:00 進行備份

IBM Db2 所需的備份作業數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

IBM Db2 資料庫外掛程式的備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

`resourcegroupname_hostname_timestamp`

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳後綴會加入到快照名稱中。

IBM Db2 的還原與復原策略

定義 IBM Db2 資源的還原與復原策略

您必須在還原和復原資料庫之前定義一個策略，以便能夠成功執行還原和復原作業。



僅支援手動恢復資料庫。

步驟

1. 確定手動新增的 IBM Db2 資源支援的還原策略
2. 確定自動發現的 IBM Db2 資料庫支援的還原策略

手動新增的 IBM Db2 資源支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。手動新增的 IBM Db2 資源有兩種復原策略。



您無法復原手動新增的 IBM Db2 資源。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

自動發現的 **IBM Db2** 支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。

完整資源復原是針對自動發現的 IBM Db2 資料庫支援的復原策略。這將恢復資源的所有磁碟區、qtree 和 LUN。

自動發現的 **IBM Db2** 的還原作業類型

IBM Db2 的 SnapCenter 外掛程式支援單一檔案 SnapRestore 以及自動發現的 IBM Db2 資料庫的連線和複製復原類型。

單檔 SnapRestore 在 **NFS** 環境中針對以下場景執行：

- 如果僅選擇*完整資源*選項
- 當選擇的備份來自 SnapMirror 或 SnapVault 二級位置，並且選擇了「完整資源」選項時

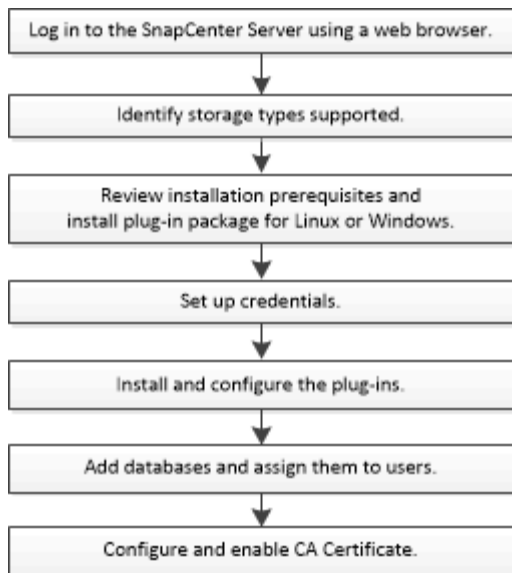
單一檔案 SnapRestore 在 **SAN** 環境中針對下列場景執行：

- 如果僅選擇*完整資源*選項
- 從 SnapMirror 或 SnapVault 二級位置選擇備份，並選擇「完整資源」選項時

準備安裝適用於 **IBM Db2** 的 SnapCenter 插件

SnapCenter Plug-in for IBM Db2 的安裝工作流程

如果您想要保護 IBM Db2 資料庫，則應該安裝並設定適用於 IBM Db2 的 SnapCenter 外掛程式。



新增主機並安裝 **Windows**、**Linux** 或 **AIX** 插件包的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。Windows、Linux 和 AIX 環境支援適用於 IBM Db2 的 SnapCenter 插件。

- 您必須在主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 對於 Windows，外掛程式建立者服務應該使用「LocalSystem」Windows 使用者執行，這是以網域管理員身分安裝 IBM Db2 外掛程式時的預設行為。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。適用於 Microsoft Windows 的 SnapCenter 外掛程式將預設與 Windows 主機上的 IBM Db2 外掛程式一起部署。
- SnapCenter 伺服器應該可以存取 IBM Db2 主機插件的 8145 或自訂連接埠。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 在 Windows 主機上安裝適用於 IBM Db2 的外掛程式時，適用於 Microsoft Windows 的 SnapCenter 外掛程式會自動安裝。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Windows 主機上安裝 Java 11。

["下載適用於 Windows 的 JAVA"](#)

["NetApp 互通性表工具"](#)

Linux 和 AIX 主機

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。

- 您必須在 Linux 主機上安裝 Java 11。

["下載適用於 Linux 的 JAVA"](#)

["下載適用於 AIX 的 JAVA"](#)

["NetApp互通性表工具"](#)

- 對於在 Linux 主機上執行的 IBM Db2 資料庫，在安裝 IBM Db2 插件時，會自動安裝 UNIX 的 SnapCenter 插件。
- 您應該將 **bash** 作為插件安裝的預設 shell。

補充命令

若要在 IBM Db2 的 SnapCenter 插件上執行補充命令，必須將其包含在 `allowed_commands.config` 檔案中。

- Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 主機上的預設位置：`/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`

若要允許插件主機上的補充命令，請在編輯器中開啟 `_allowed_commands.config` 檔案。每個命令在單獨的行上輸入，並且命令不區分大小寫。確保指定完全限定的路徑名，並且如果路徑名包含空格，則將其括在引號 (") 中。

例如：

命令：`mount`

命令：`umount`

指令：`"C:\Program Files\ NetApp\ SnapCreator 指令\ sdcli.exe"`

指令：`myscript.bat`

如果不存在 `allowed_commands.config` 文件，命令或腳本執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行 "[mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」

如果命令或腳本不在 `_allowed_commands.config` 中，則命令或腳本的執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行 "[mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」



您不應使用通配符 (*) 來允許所有命令。

為 Linux 主機的非 root 使用者配置 sudo 權限

SnapCenter 允許非 root 使用者安裝適用於 Linux 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 為 0027，請確保 java 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 Linux 的SnapCenter插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`LINUX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

為 AIX 主機的非 root 使用者配置 `sudo` 權限

SnapCenter 4.4 及更高版本允許非 root 用戶安裝適用於 AIX 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 `sudo` 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 `umask` 為 0027，請確保 `java` 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。

- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 AIX 的 SnapCenter 插件包的 AIX 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`AIX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 Windows 的 SnapCenter 插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp 互通性表工具"。

物品	要求
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統， SnapCenter升級或安裝將會失敗。"

安裝適用於 Linux 的SnapCenter插件包的主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間和大小需求。

物品	要求
作業系統	• 紅帽企業 Linux • SUSE Linux 企業伺服器 (SLES) 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB

物品	要求
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間有所不同，取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 與 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

為 IBM Db2 的SnapCenter插件設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

關於此任務

- Linux 主機

您必須設定在 Linux 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。

2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>使用者名稱 ◦ 域 <i>FQDN</i>用戶名 • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i> 請勿在密碼中使用雙引號 (") 或反引號 (')。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，<i>lessthan<!10</i>、<i>lessthan10<!`</i>、<i>backtick`12</i>。
密碼	輸入用於身份驗證的密碼。
認證模式	選擇您想要使用的身份驗證模式。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。

為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
 - b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA：Install-AdServiceAccount <gMSA>
 - c. 透過執行以下命令驗證你的 gMSA 帳戶：Test-AdServiceAccount <gMSA>
5. 將管理權限指派給主機上配置的 gMSA。
 6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

安裝適用於 IBM Db2 的 SnapCenter 插件

新增主機並在遠端主機上安裝插件包

您必須使用 SnapCenter 新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以為單一主機或叢集新增主機並安裝插件包。

開始之前

- 如果 SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 您應該確保訊息佇列服務正在運行。

- 管理文件包含有關管理主機的資訊。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

"在 Windows Server 2016 或更高版本上為 IBM Db2 設定群組託管服務帳戶"

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux  IBM Db2 外掛程式安裝在 IBM Db2 用戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。
主機名稱	輸入通訊主機名稱。輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標放在您提供的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

使用 REST API 安裝 Db2 插件時，必須傳遞版本為 3.0。例如，Db2:3.0

6. (可選) 按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	IBM Db2 外掛程式安裝在 IBM Db2 用戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。 - 對於適用於 Windows 的SnapCenter插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您也可以選擇自訂路徑。 - 對於適用於 Linux 的SnapCenter插件包，預設路徑為 /opt/ NetApp/snapcenter。您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	對於 Windows 主機，如果您要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。  以以下格式提供 gMSA 名稱： ：domainName\accountName\$。  gMSA 將僅用作 Windows 服務的SnapCenter插件的登入服務帳戶。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）以及 Java 11（適用於 Windows 和 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 檔案以修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 如果主機類型為Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

- 對於 Windows 插件，安裝和升級日誌位於：`C:\Windows\SnapCenter plugin\Install<JOBID>\`
- 對於 Linux 插件，安裝日誌位於：`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log`，升級日誌位於：`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_JfA_Plug.Plug`。

完成後

如果要升級到SnapCenter 6.0 或更高版本，則會從遠端插件伺服器中卸載現有的基於 PERL 的 Db2 插件。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux** 或 **Windows** 的**SnapCenter**插件包

您可以使用 `Install-SmHostPackage PowerShell cmdlet` 同時在多個主機上安裝適用於 Linux 或 Windows 的**SnapCenter**插件套件。

開始之前

您必須以網域使用者身分登入SnapCenter，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，使用 `Open-SmConnection cmdlet` 建立會話，然後輸入您的憑證。
3. 使用 `Install-SmHostPackage cmdlet` 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 `cmdlet` 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝適用於 **IBM Db2** 的**SnapCenter**插件

您應該使用**SnapCenter**使用者介面 (UI) 安裝適用於 IBM Db2 資料庫的**SnapCenter**插件。如果您的環境不允許從**SnapCenter** UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控制台模式或靜默模式安裝 IBM Db2 資料庫插件。

開始之前

- 您應該在 IBM Db2 用戶端所在的每個 Linux 主機上安裝 IBM Db2 資料庫外掛程式。
- 安裝 IBM Db2 資料庫的**SnapCenter**插件的 Linux 主機必須符合相關軟體、資料庫和作業系統需求。

互通性矩陣工具 (IMT) 包含受支援配置的最新資訊。

["NetApp互通性表工具"](#)

- IBM Db2 資料庫的**SnapCenter**插件是 Linux 的**SnapCenter**插件包的一部分。在安裝適用於 Linux 的**SnapCenter**插件包之前，您應該已經在 Windows 主機上安裝了**SnapCenter**。

關於此任務

如果未提及參數，則使用預設值安裝SnapCenter。

步驟

1. 將 Linux 安裝檔案 (snapcenter_linux_host_plugin.bin) 的SnapCenter插件包從 C:\ProgramData\NetApp\SnapCenter\Package Repository 複製到要安裝 IBM Db2 插件的主機。

您可以從安裝了SnapCenter伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。
3. 安裝插件：`path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`
 - -DPORT 指定 SMCORE HTTPS 通訊連接埠。
 - -DSERVER_IP 指定SnapCenter伺服器 IP 位址。
 - -DSERVER_HTTPS_PORT 指定SnapCenter伺服器 HTTPS 連接埠。
 - -DUSER_INSTALL_DIR 指定要安裝 Linux 版SnapCenter插件包的目錄。
 - DINSTALL_LOG_NAME 指定日誌檔案的名稱。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent  
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146  
-DUSER_INSTALL_DIR=/opt  
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log  
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. 編輯 <安裝目錄> NetApp文件，然後新增 PLUGINS_ENABLED = DB2:3.0 參數。
5. 使用 Add-Smhost cmdlet 和所需參數將主機新增至SnapCenter伺服器。

可以透過執行 `_Get-Help command_name_` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

監控 IBM Db2 插件的安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的

-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。

2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在SnapCenter伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

為 Linux 主機上的SnapCenter IBM Db2 插件服務設定 CA 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

插件使用位於 `/opt/NetApp/snapcenter/scc/etc` 的檔案「keystore.jks」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與密鑰“KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks
```

． 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/ NetApp/snapcenter/scc/etc`。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

． 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導航至包含插件金鑰庫 `/opt/ NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

• 如果CA憑證中的別名較長，且包含空格或特殊字元（"*"，"，"），請將別名修改為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

• 在 agent.properties 檔案中配置來自 CA 憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

8. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於此任務

- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter插件的 CRL 檔案的預設目錄是「opt/ NetApp/snapcenter/scc/etc/crl」。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 agent.properties 檔案中的預設目錄。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

為 **Windows** 主機上的**SnapCenter IBM Db2** 插件服務設定 **CA** 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

外掛程式使用位於 C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc 的檔案 keystore.jks 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與金鑰 `KEYSTORE_PASS` 對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore 金鑰庫.jks
```



如果 Windows 命令提示字元無法辨識「keytool」命令，請將 keytool 命令替換為其完整路徑。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe"-storepasswd -keystore keystore.jks
```

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks
```

對 `agent.properties` 檔案中的金鑰 `KEYSTORE_PASS` 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 `C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc`
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 **CA** 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案 *_keystore.jks_*。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 *agent.properties* 檔案中密鑰 *KEYSTORE_PASS* 的值。

```
keytool -keypasswd -alias 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在 *_agent.properties_* 檔案中配置來自CA憑證的別名。

根據鍵 *SCC_CERTIFICATE_ALIAS* 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter\SnapCenter的 CRL 檔案的預設目錄是 '*C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl*'。

步驟

1. 您可以根據鍵 *CRL_PATH* 修改和更新 *agent.properties* 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器和對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

做好資料保護準備

使用適用於 IBM Db2 的 SnapCenter 插件的先決條件

在使用 IBM Db2 的 SnapCenter 插件之前，SnapCenter 管理員必須安裝和設定 SnapCenter 伺服器並執行先決條件任務。

- 安裝並配置 SnapCenter 伺服器。
- 登入 SnapCenter 伺服器。
- 透過新增儲存系統連接和建立憑證（如果適用）來配置 SnapCenter 環境。
- 在您的 Linux 或 Windows 主機上安裝 Java 11。

您必須在主機的環境路徑變數中設定 Java 路徑。

- 如果您想要備份複製，請設定 SnapMirror 和 SnapVault。

如何使用資源、資源群組和政策來保護 IBM Db2

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的 IBM Db2 資料庫。
- SnapCenter資源組是主機上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

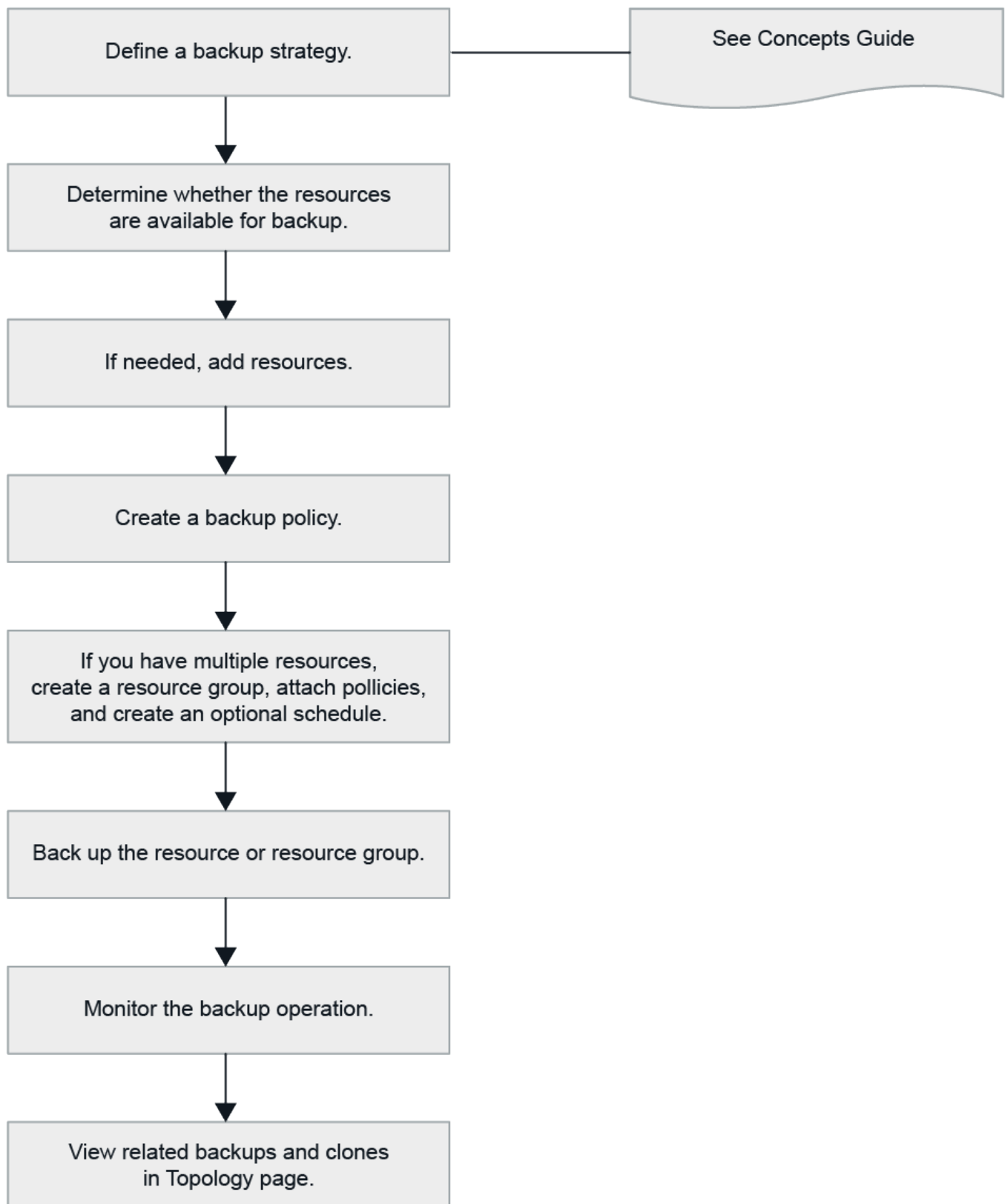
資源群組可以視為定義您想要保護的內容以及何時以日期和時間進行保護。把政策看作是定義你想如何保護它。例如，如果要備份所有資料庫，則可以建立一個包含主機中所有資料庫的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加原則時，您可以配置資源組以每天執行完整備份。

備份 IBM Db2 資源

備份 IBM Db2 資源

您可以建立資源（資料庫）或資源組的備份。備份工作流程包括規劃、識別要備份的資料庫、管理備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。 SnapCenter cmdlet 說明和 cmdlet 參考資訊包含更多有關 PowerShell cmdlet 的資訊。 <https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenter軟體 Cmdlet 參考指南"]。

自動發現資料庫

資源是 Linux 主機上由SnapCenter管理的 IBM Db2 資料庫。發現可用的 IBM Db2 資料庫後，您可以將資源新增至資源組以執行資料保護作業。

開始之前

- 您必須已經完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。
- IBM Db2 的SnapCenter外掛程式不支援自動發現駐留在 RDM/VMDK 虛擬環境中的資源。手動新增資料庫時必須提供虛擬環境的儲存資訊。

關於此任務

- 安裝外掛程式後，該Linux主機上的所有資料庫都會自動發現並顯示在資源頁面上。
- 僅資料庫是自動發現的。

自動發現的資源不能被修改或刪除。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇 IBM Db2 外掛程式。
2. 在資源頁面中，從視圖清單中選擇資源類型。
3. （可選）點擊  *，然後選擇主機名稱。

然後您可以點擊  * 關閉篩選窗格。

4. 按一下「刷新資源」以發現主機上可用的資源。

資源與資源類型、主機名稱、關聯資源群組、備份類型、政策和總體狀態等資訊一起顯示。

- 如果資料庫位於NetApp儲存空間且未受保護，則「整體狀態」欄位中顯示「未受保護」。
- 如果資料庫位於NetApp儲存系統上並受到保護，且沒有執行備份操作，則「整體狀態」欄位中會顯示「備份未執行」。否則，狀態將根據上次備份狀態變更為備份失敗或備份成功。



如果資料庫在SnapCenter之外重新命名，則必須刷新資源。

手動將資源新增至插件主機

Windows 主機不支援自動發現。您必須手動新增 Db2 執行個體和資料庫資源。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。

關於此任務

以下配置不支援手動發現：

- RDM 和 VMDK 佈局

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從下拉清單中選擇適用於 IBM Db2 的 SnapCenter 插件。
2. 在資源頁面中，按一下「新增 IBM DB2 資源」。
3. 在提供資源詳細資訊頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	指定資料庫名稱。
主機名稱	輸入主機名稱。
類型	選擇資料庫或實例。
實例	指定實例的名稱，它是資料庫的父級。
證書	選擇憑證或新增憑證資訊。 這是可選的。

4. 在「提供儲存佔用空間」頁面中，選擇儲存類型並選擇一個或多個磁碟區、LUN 和 qtree，然後按一下「儲存」。

可選：您可以點擊 *  * 圖示用於從其他儲存系統新增更多磁碟區、LUN 和 qtree。

5. 選用：在資源設定頁面中，對於 Windows 主機上的資源，輸入 IBM Db2 外掛程式的自訂鍵值對
6. 查看摘要，然後按一下「完成」。

資料庫與主機名稱、相關資源群組和策略以及整體狀態等資訊一起顯示

如果您想讓使用者存取資源，您必須將資源指派給使用者。這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

"新增使用者或群組並分配角色和資產"

新增資料庫後，您可以修改 IBM Db2 資料庫詳細資訊。

為 IBM Db2 建立備份策略

在使用 SnapCenter 備份 IBM Db2 資源之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。

開始之前

- 您必須已經定義了您的備份策略。

有關詳細信息，請參閱有關為 IBM Db2 資料庫定義資料保護策略的資訊。

- 您必須已完成安裝 SnapCenter、新增主機、設定儲存系統連線和新增資源等任務，為資料保護做好準備。

- 如果您要將快照複製到映像或保管庫， SnapCenter 管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。

此外，您還可以在策略中指定複製、腳本和應用程式設定。當您想要將該策略重新用於另一個資源群組時，這些選項可以節省時間。

關於此任務

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
 - 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能會導致保留的快照數量超過策略中指定的數量。
 - 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選“新建”。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「策略類型」頁面中，執行以下操作：
 - a. 選擇儲存類型。
 - b. 在*自訂備份設定*部分，提供任何必須以鍵值格式傳遞給外掛程式的特定備份設定。

您可以提供多個鍵值傳遞給插件。

6. 在「快照和複製」頁面中，執行下列操作。
 - a. 透過選擇*按需*、每小時、每天、*每週*或*每月*來指定計畫頻率。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，還使您能夠為每個策略分配不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- a. 在快照設定部分中，執行以下操作：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。

如果你想...	然後...
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*並指定天、月或年。 Snaplock 保留期應少於 100 年。



對於基於 Snapshot 副本的備份，如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。

b. 指定策略標籤。

您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

7. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
建立本地 Snapshot 副本後更新SnapMirror	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 應為SnapMirror主動同步啟用此選項。
建立本機 Snapshot 副本後更新SnapVault	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

8. 查看摘要，然後按一下「完成」。

建立資源組並附加策略

資源組是您必須新增要備份和保護的資源的容器。資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。  資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
使用自訂名稱格式進行快照複製	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

4. 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。

這有助於過濾螢幕上的信息。

5. 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
6. 在應用程式設定頁面中，執行以下操作：
 - a. 按一下“備份”箭頭以設定其他備份選項：

啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+

- 點擊“腳本”箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- 按一下「自訂配置」箭頭並輸入使用此資源的所有資料保護操作所需的自訂鍵值對。

範圍	環境	描述
歸檔日誌啟用	(是/否)	啟用存檔日誌管理以刪除存檔日誌。
歸檔日誌保留	天數	指定存檔日誌保留的天數。 此設定必須等於或大於 NTAP_SNAPSHOT_RETENTIONS。
歸檔日誌目錄	更改訊息目錄/日誌	指定包含存檔日誌的目錄的路徑。
ARCHIVE_LOG_EXT	檔案副檔名	指定存檔日誌檔案擴充長度。 例如，如果歸檔日誌為log_backup_0_0_0_0.1615185519429，且file_extension值為5，則日誌的副檔名將保留5位數，即16151。
ARCHIVE_LOG_RECURSIVE_SEARCH	(是/否)	啟用子目錄內的存檔日誌管理。 如果存檔日誌位於子目錄下，則應使用此參數。



自訂鍵值對支援 IBM Db2 Linux 外掛系統，但不支援註冊為集中式 Windows 外掛程式的 IBM Db2 資料庫。

c. 點選*Snapshot Copy Tool*箭頭選擇建立快照的工具：

如果你想...	然後...
SnapCenter使用適用於 Windows 的插件並在建立快照之前將檔案系統置於一致狀態。對於 Linux 資源，此選項不適用。	選擇*具有檔案系統一致性的SnapCenter *
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
輸入要在主機上執行的命令來建立快照副本。	選擇*其他*，然後輸入要在主機上執行的建立快照的命令。

7. 在「策略」頁面中，執行以下步驟：

a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 * 來建立策略  *。

這些策略列在「為選定的策略配置計劃」部分中。

b. 在配置計劃列中，按一下 *  * 您想要配置的策略。

c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。

其中，policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。必須在*設定* > *全域設定*中設定 SMTP 伺服器。

9. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並為 IBM Db2 資源啟用二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。

- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。

- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

- a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。

- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。

- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。

- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。

- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtptServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 為 IBM Db2 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 備份、還原或複製 IBM Db2 資料庫之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

步驟

1. 點選 **SnapCenterPS** 啟動 PowerShell Core。
2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap  
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例顯示如何使用 Windows 憑證建立名為 FinanceAdmin 的新憑證：

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux  
-AuthenticationType PasswordBased -Credential db2hostuser  
-EnableSudoPrivileges:$true
```

4. 將 IBM Db2 通訊主機新增至 SnapCenter Server。

對於 Linux：

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'  
-CredentialName 'defaultcreds'
```

對於 Windows：

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. 在主機上安裝軟體套件和適用於 IBM Db2 的 SnapCenter 插件。

對於 Linux：

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2
```

對於 Windows：

```
PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
DB2, SCW
```

6. 設定 SQLLIB 的路徑。

對於 Windows，Db2 外掛程式將使用 SQLLIB 資料夾的預設路徑：“C:\Program Files\IBM\SQLLIB\BIN”

如果要覆蓋預設路徑，請使用下列命令。

```
PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
-PluginCode DB2 -configSettings
@{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份 Db2 資料庫

備份資料庫包括與 SnapCenter 伺服器建立連線、新增資源、新增原則、建立備份資源群組和備份。

開始之前

- 您必須已經建立了備份策略。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用「vsadmin」角色，則不需要「snapmirror all」權限。
- 對於基於 Snapshot 副本的備份作業，請確保所有租用戶資料庫均有效且處於活動狀態。
- 對於靜默、快照和取消靜默操作的預先命令和後命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：*C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in*

Creator\etc\allowed_commands.config

- Linux 主機上的預設位置：*/opt/NetApp/snapcenter/scc/etc/allowed_commands.config*



如果命令清單中不存在該命令，則操作將失敗。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

選擇，然後選擇主機名稱和資源類型來過濾資源。然後您可以選擇關閉篩選器窗格。

3. 選擇要備份的資源。
4. 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。

例如，*customtext_policy_hostname* 或 *resource_hostname*。預設情況下，時間戳記會附加到快照名稱。

5. 在應用程式設定頁面中，執行以下操作：

- 選擇“備份”箭頭來設定其他備份選項：

如果需要，請啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待「一致性組快照」操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

- 選擇「腳本」箭頭來執行靜默、快照和取消靜默操作的前置和後置命令。

您也可以在退出備份作業之前執行預命令。前言和後記在SnapCenter伺服器中運作。

- 選擇自訂配置箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
- 選擇*Snapshot Copy Tool*箭頭來選擇建立快照的工具：

如果你想...	然後...
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
SnapCenter使用適用於 Windows 的插件將檔案系統置於一致狀態，然後建立快照	選擇*具有檔案系統一致性的SnapCenter *。
輸入建立快照的命令	選擇*其他*，然後輸入建立快照的命令。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 * 來建立策略  *.

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 選擇 *  * 在您想要設定計畫的政策的政策設定計畫列中。
- c. 在為政策_policy_name_新增計劃對話方塊中，配置計畫，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後選擇*完成*。

進入資源拓樸頁面。

9. 選擇*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行

保留。

b. 選擇*備份*。

11. 透過點選「監視」>「作業」來監視操作進度。

◦ 在MetroCluster配置中， SnapCenter可能無法在故障轉移後偵測到保護關係。

有關信息，請參閱：["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-SmConnection
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmResources cmdlet 新增手動資源。

此範例顯示如何新增 IBM Db2 實例：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2  
-ResourceType Instance -ResourceName db2inst1 -StorageFootPrint  
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

對於 Db2 資料庫：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2  
-ResourceType Database -ResourceName SALESDB -StorageFootPrint  
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. 使用 Add-SmPolicy cmdlet 建立備份策略。

4. 使用 Add-SmResourceGroup cmdlet 保護資源或為SnapCenter新增資源組。

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

此範例顯示如何備份資源組：

```
C:\PS> New-SMBackup -ResourceGroupName  
'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
```

此範例備份 Db2 實例：

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
db2_policy
```

此範例備份 Db2 資料庫：

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDDB";"PluginName"="DB2"
} -Policy db2_policy
```

6. 使用 Get-smJobSummaryReport cmdlet 監視作業狀態（正在執行、已完成或失敗）。

```
PS C:\> Get-SmJobSummaryReport -JobId 467

SmJobId           : 467
JobCreatedDateTime : 
JobStartDateTime  : 27-Jun-24 01:40:09
JobEndDateTime    : 27-Jun-24 01:41:15
JobDuration       : 00:01:06.7013330
JobName           : Backup of Resource Group
'SCDB201WIN_RAVIR1_OPENLAB_NETAPP_LOCAL_DB2_DB2_WINCIR' with policy
'snapshot-based-db2'
JobDescription     : 
Status            : Completed
IsScheduled        : False
JobError           : 
JobType           : Backup
PolicyName         : db2_policy
JobResultData      :
```

7. 使用 Get-SmBackupReport cmdlet 監視備份作業詳細資料（如備份 ID、備份名稱）以執行還原或複製作業。

```

PS C:\> Get-SmBackupReport -JobId 467

BackedUpObjects      : {WINCIR}
FailedObjects        : {}
IsScheduled          : False
HasMetadata          : False
SmBackupId           : 84
SmJobId              : 467
StartDateTime        : 27-Jun-24 01:40:09
EndDateTime          : 27-Jun-24 01:41:15
Duration             : 00:01:06.7013330
CreatedDateTime      : 27-Jun-24 18:39:45
Status               : Completed
ProtectionGroupName  : HOSTFQDN_DB2_DB2_WINCIR
SmProtectionGroupId  : 23
PolicyName           : db2_policy
SmPolicyId           : 13
BackupName           : HOSTFQDN _DB2_DB2_WINCIR_HOST_06-27-
2024_01.40.09.7397
VerificationStatus   : NotApplicable
VerificationStatuses :
SmJobError           :
BackupType           : SCC_BACKUP
CatalogingStatus     : NotApplicable
CatalogingStatuses   :
ReportDataCreatedDateTime :
PluginCode           : SCC
PluginName           : DB2
PluginDisplayName     : IBM DB2
JobTypeId            :
JobHost              : HOSTFQDN

```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

備份資源組

資源組是主機上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用「vsadmin」角色，則不需要「snapmirror all」權限。

關於此任務

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或選擇，然後選擇標籤。然後您可以選擇關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：
 - a. 如果您將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 選擇*備份*。
5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

監控 IBM Db2 備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。

- d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監控 **IBM Db2** 資料庫上的資料保護作業

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消 **IBM Db2** 的備份作業

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	- 在左側導覽窗格中，按一下「監控」>「作業」。 - 選擇操作，然後按一下「取消作業」。
活動窗格	- 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 - 選擇操作。 - 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓樸頁面中查看 IBM Db2 備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。



顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

步驟

- 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。

3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓樸頁面。

4. 查看*摘要卡*以了解主儲存和輔助儲存上可用的備份和克隆數量的摘要。

*摘要卡*部分顯示基於 Snapshot 副本的備份和克隆的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

按需備份後，按一下「刷新」按鈕以刷新備份或複製的詳細資訊。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

7. 如果要刪除克隆，請從表中選擇克隆，然後按一下 .

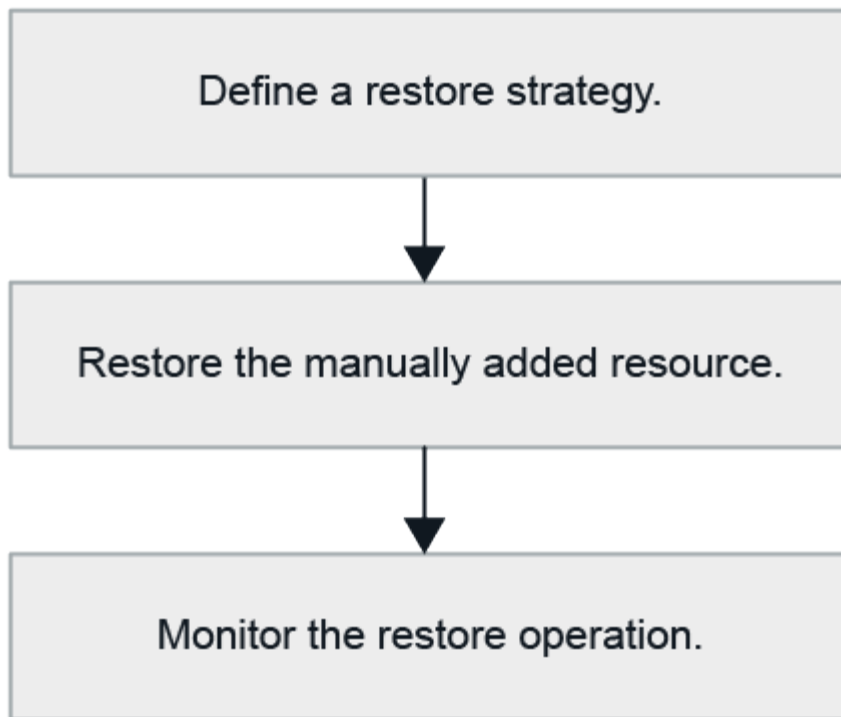
8. 如果要拆分克隆，請從表中選擇克隆，然後按一下 .

還原 IBM Db2

復原工作流程

還原和復原工作流程包括規劃、執行還原操作和監視操作。

以下工作流程顯示了執行還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

["SnapCenter軟體 Cmdlet 參考指南"](#)。

還原手動新增的資源備份

您可以使用SnapCenter從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.

Primary Backup(s)	
search	T
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. 在「復原範圍」頁面中，選擇「完整資源」。
 - a. 如果選擇*完整資源*，則會還原 IBM Db2 資料庫的所有已設定資料磁碟區。

如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果在相同的磁碟區或 qtree 上託管任何其他資源，則該資源也會被刪除。

您可以選擇多個 LUN。



如果選擇“全部”，則會還原磁碟區、qtree 或 LUN 上的所有檔案。

7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。
8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。
9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

10. 查看摘要，然後按一下「完成」。

11. 透過點選「監視」>「作業」來監視操作進度。

完成後

僅當 Rollforward 狀態處於「DB pending」狀態時才可以進行復原。此狀態適用於啟用了存檔日誌記錄的 Db2 資料庫。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-SmConnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 來辨識要還原的備份。

此範例顯示有兩個備份可供還原：

```
PS C:\> Get-SmBackup -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\Library
```

	BackupId	BackupName	BackupTime
BackupType	-----	-----	-----

	1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32
AM Full Backup			
	2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17
AM			

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId           : 113
  SmJobId             : 2032
  StartDateTime       : 2/2/2015 6:57:03 AM
  EndDateTime         : 2/2/2015 6:57:11 AM
  Duration            : 00:00:07.3060000
  CreatedDateTime     : 2/2/2015 6:57:23 AM
  Status              : Completed
  ProtectionGroupName : Clone
  SmProtectionGroupId : 34
  PolicyName          : Vault
  SmPolicyId          : 18
  BackupName          : Clone_SCSPR0019366001_02-02-2015_06.57.08
  VerificationStatus  : NotVerified

  SmBackupId         : 114
  SmJobId             : 2183
  StartDateTime       : 2/2/2015 1:02:41 PM
  EndDateTime         : 2/2/2015 1:02:38 PM
  Duration            : -00:00:03.2300000
  CreatedDateTime     : 2/2/2015 1:02:53 PM
  Status              : Completed
  ProtectionGroupName : Clone
  SmProtectionGroupId : 34
  PolicyName          : Vault
  SmPolicyId          : 18
  BackupName          : Clone_SCSPR0019366001_02-02-2015_13.02.45
  VerificationStatus  : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。



AppObjectId 是“Host\Plugin\UID”，其中 UID = <instance_name> 表示手動發現的 DB2 實例資源，UID = <instance_name>\<database_name> 表示 IBM Db2 資料庫資源。您可以從 Get-smResources cmdlet 取得 ResourceID。

```
Get-smResources -HostName cn24.sscore.test.com -PluginCode DB2
```

此範例顯示如何從主儲存復原資料庫：

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

此範例顯示如何從輔助儲存恢復資料庫：

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId  
cn24.sscore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false  
-Archive @( @{"Primary"="<Primary  
Vserver>:<PrimaryVolume>"; "Secondary"="<Secondary  
Vserver>:<SecondaryVolume>"} )
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

還原和還原自動發現的資料庫備份

您可以使用 SnapCenter 從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 對於自動發現的資源，SFSR 支援恢復。
- 不支援自動恢復。
- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從“檢視”下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.



6. 在「復原範圍」頁面中，選擇「完整資源」以還原 IBM Db2 資料庫的已設定資料磁碟區。
7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

自動發現的資源不需要卸載命令。

8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源不需要掛載指令。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

完成後

僅當 Rollforward 狀態處於「DB pending」狀態時才可以進行復原。此狀態適用於啟用了存檔日誌記錄的 Db2 資料庫。

監控 IBM Db2 恢復操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成

-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

克隆 IBM Db2 資源備份

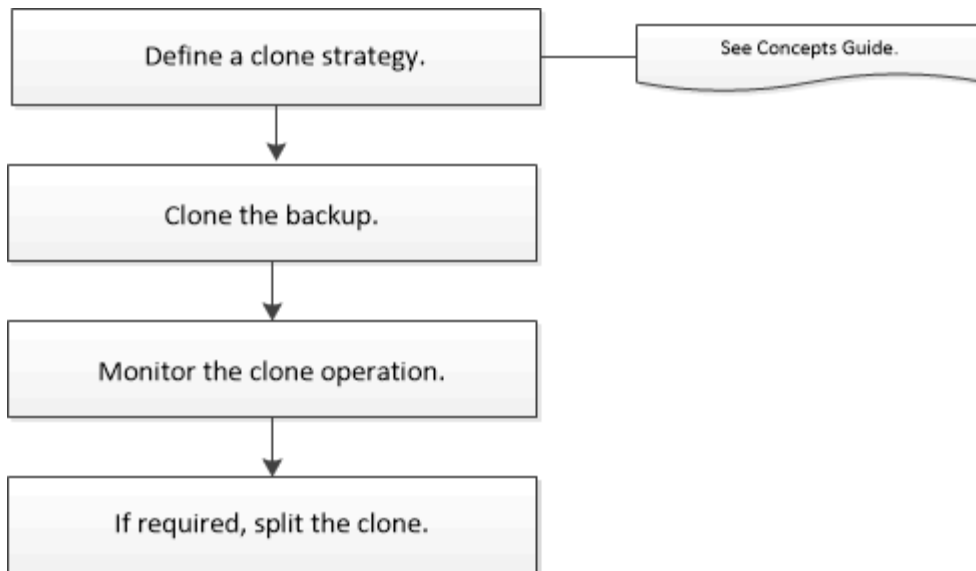
克隆工作流程

克隆工作流程包括執行克隆操作和監視操作。

關於此任務

- 您可以在來源 IBM Db2 伺服器上進行複製。
- 您可能會因為以下原因而複製資源備份：
 - 在應用程式開發週期中測試必須使用目前資源結構和內容實現的功能
 - 用於填充資料倉儲時的資料擷取和操作工具
 - 恢復被錯誤刪除或更改的數據

以下工作流程顯示了執行複製操作必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

完成後

克隆自動發現的 Db2 資源後，克隆的資源被標記為手動資源。按一下*刷新資源*以恢復克隆的 Db2 資源。當您刪除克隆時，儲存和主機也會被清理。

如果克隆操作後不刷新資源並嘗試刪除克隆，則儲存和主機將不會被清理。您必須在 fstab 中手動刪除條目。

克隆 IBM Db2 備份

您可以使用 SnapCenter 克隆備份。您可以從主備份或輔助備份複製。

開始之前

- 您應該已經備份資源或資源組。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 在備用主機上為 Db2 建立複製時，必須為複製掛載路徑建立與另一台主機上的原始掛載路徑相同的 n-1 目錄結構。掛載路徑應具有 `_755_` 執行權限。
- 對於克隆前或克隆後命令，您應該從以下路徑檢查這些命令是否存在於插件主機上可用的命令清單中：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 有關 FlexClone 磁碟區拆分操作的信息，請參閱 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["將 FlexClone 磁碟區從其父卷中拆分出來"]。
- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和策略以及狀態等資訊一起顯示。

3. 選擇資源或資源組。

如果選擇資源組，則必須選擇資源。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	選擇要建立克隆的主機。
目標克隆實例	輸入要從現有備份中複製的目標 Db2 複製實例 ID。 這僅適用於 ANF 儲存類型資源。
目標克隆名稱	輸入克隆的名稱。 這僅適用於 Db2 資料庫資源。
NFS 匯出 IP 位址	輸入將會匯出複製磁碟區的 IP 位址或主機名稱。 這僅適用於 NFS 儲存類型資源。
容量池最大吞吐量 (MiB/s)	輸入容量池的最大吞吐量。

7. 在腳本頁面中，執行以下步驟：



腳本在插件主機上運行。

- a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。
 - 克隆前指令：刪除現有的同名資料庫
 - 克隆後指令：驗證資料庫或啟動資料庫。
- b. 輸入 mount 指令將檔案系統掛載到主機。

Linux 電腦上磁碟區或 qtree 的掛載指令：

NFS 範例：mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

9. 查看摘要，然後按一下「完成」。
10. 透過點選「監視」>「作業」來監視操作進度。

完成後

克隆自動發現的 Db2 資源後，克隆的資源被標記為手動資源。按一下*刷新資源*以恢復克隆的 Db2 資源。當您刪除克隆時，儲存和主機也會被清理。

如果克隆操作後不刷新資源並嘗試刪除克隆，則儲存和主機將不會被清理。您必須在 fstab 中手動刪除條目。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與 SnapCenter 伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl https://snapctr.demo.netapp.com:8146
```

2. 列出可以使用 Get-SmBackup 或 Get-SmResourceGroup cmdlet 克隆的備份。

此範例顯示有關所有可用備份的資訊：

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

此範例顯示有關指定資源組、其資源和相關策略的資訊：

```
PS C:\> Get-SmResourceGroup -ListResources -ListPolicies
```

```
Description :  
CreationTime : 8/4/2015 3:44:05 PM  
ModificationTime : 8/4/2015 3:44:05 PM
```

```
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {FinancePolicy}
HostResourceMapping : {}
Configuration : SMCoreContracts.SmCloneConfiguration
LastBackupStatus :
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo : SMCoreContracts.SmVerificationServerInfo
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassCredential : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Name : Payrolldataset
Type : Group
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
ApplySnapvaultUpdate : False
ApplyRetention : False
RetentionCount : 0
RetentionDays : 0
ApplySnapMirrorUpdate : False
SnapVaultLabel :
MirrorVaultUpdateRetryCount : 7
AppPolicies : {}
Description : FinancePolicy
PreScriptPath :
PreScriptArguments :
PostScriptPath :
```

```
PostScriptArguments :
ScriptTimeout : 60000
DateModified : 8/4/2015 3:43:30 PM
DateCreated : 8/4/2015 3:43:30 PM
Schedule : SMCoreContracts.SmSchedule
PolicyType : Backup
PluginPolicyType : SMSQL
Name : FinancePolicy
Type :
Id : 1
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
clab-a13-13.sddev.lab.netapp.com
DatabaseGUID :
SQLInstance : clab-a13-13
DbStatus : AutoClosed
DbAccess : eUndefined
IsSystemDb : False
IsSimpleRecoveryMode : False
IsSelectable : True
SqlDbFileGroups : {}
SqlDbLogFiles : {}
AppFileStorageGroups : {}
LogDirectory :
AgName :
Version :
VolumeGroupIndex : -1
IsSecondary : False
Name : TEST
Type : SQL Database
Id : clab-a13-13\TEST
Host : clab-a13-13.sddev.mycompany.com
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
```

3. 使用 New-SmClone cmdlet 從現有備援啟動複製作業。

此範例從包含所有日誌的指定備份建立複製：

```

PS C:\> New-SmClone
-BackupName payroll_dataset_vise-f3_08-05-2015_15.28.28.9774
-Resources @{"Host"="vise-f3.sddev.mycompany.com";
"Type"="SQL Database";"Names"="vise-f3\SQLExpress\payroll"}
-CloneToInstance vise-f3\sqlexpress -AutoAssignMountPoint
-Suffix _clonefrombackup
-LogRestoreType All -Policy clonefromprimary_ondemand

PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy

```

此範例建立指定 Microsoft SQL Server 執行個體的複製：

```

PS C:\> New-SmClone
-BackupName "BackupDS1_NY-VM-SC-SQL_12-08-2015_09.00.24.8367"
-Resources @{"host"="ny-vm-sc-sql";"Type"="SQL Database";
"Names"="ny-vm-sc-sql\AdventureWorks2012_data"}
-AppPluginCode SMSQL -CloneToInstance "ny-vm-sc-sql"
-Suffix _CLPOSH -AssignMountPointUnderPath "C:\SCMounts"

```

4. 使用 Get-SmCloneReport cmdlet 查看複製作業的狀態。

此範例顯示指定作業 ID 的複製報表：

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId : 1
SmJobId : 186
StartDateTime : 8/3/2015 2:43:02 PM
EndDateTime : 8/3/2015 2:44:08 PM
Duration : 00:01:06.6760000
Status : Completed
ProtectionGroupName : Draper
SmProtectionGroupId : 4
PolicyName : OnDemand_Clone
SmPolicyId : 4
BackupPolicyName : OnDemand_Full_Log
SmBackupPolicyId : 1
CloneHostName : SCSPR0054212005.mycompany.com
CloneHostId : 4
CloneName : Draper__clone__08-03-2015_14.43.53
SourceResources : {Don, Betty, Bobby, Sally}
ClonedResources : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
                  Sally_DRAPER}
```

可以透過執行 `_Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 IBM Db2 克隆操作

您可以使用「作業」頁面監控 SnapCenter 複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。

2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“*”  *。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。

6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCore 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定 SMCore 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為 5 分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter 克隆或驗證失敗，聚合不存在"](#)

升級 SnapCenter 後刪除或拆分 IBM Db2 資料庫克隆

升級到 SnapCenter 4.3 後，您將不再看到克隆。您可以從建立克隆的資源的拓樸頁面中刪除克隆或分割克隆。

關於此任務

如果您要找到隱藏複製的儲存空間，請執行以下命令：Get-SmClone -ListStorageFootprint

步驟

1. 使用 remove-smbbackup cmdlet 刪除克隆資源的備份。
2. 使用 remove-smresourcegroup cmdlet 刪除克隆資源的資源群組。
3. 使用 remove-smprotectresource cmdlet 刪除克隆資源的保護。
4. 從資源頁面中選擇父資源。

進入資源拓樸頁面。

5. 從「管理副本」檢視中，選擇來自主或輔助（鏡像或複製）儲存系統的複製。
6. 選擇克隆，然後按一下  刪除克隆或點擊  分裂克隆。
7. 按一下“確定”。

保護 PostgreSQL

適用於 PostgreSQL 的SnapCenter插件

SnapCenter PostgreSQL 插件概述

適用於 PostgreSQL 叢集的SnapCenter插件是NetApp SnapCenter software的主機端元件，可實現 PostgreSQL 叢集的應用程式感知資料保護管理。PostgreSQL 叢集外掛程式可自動執行SnapCenter環境中 PostgreSQL 叢集的備份、復原和複製。

SnapCenter支援單一叢集和多叢集 PostgreSQL 設定。您可以在 Linux 和 Windows 環境中使用 PostgreSQL 叢集外掛程式。在 Windows 環境中，PostgreSQL 將作為手動資源得到支援。

安裝 PostgreSQL 叢集外掛程式後，您可以使用具有NetApp SnapMirror技術的SnapCenter在另一個磁碟區上建立備份集的鏡像副本。您也可以使用具有NetApp SnapVault技術的插件來執行磁碟到磁碟的備份複製，以符合標準。

適用於 PostgreSQL 的SnapCenter外掛程式支援ONTAP和 Azure NetApp檔案儲存佈局上的 NFS 和 SAN。

支援VMDK、vVol、RDM虛擬儲存佈局。

使用適用於 PostgreSQL 的SnapCenter插件可以做些什麼

在您的環境中安裝適用於 PostgreSQL 叢集的插件時，您可以使用SnapCenter備份、還原和複製 PostgreSQL 叢集及其資源。您也可以執行支援這些操作的任務。

- 新增集群。
- 建立備份。
- 從備份中復原。
- 克隆備份。
- 安排備份作業。
- 監控備份、復原和克隆作業。
- 查看備份、復原和克隆作業的報告。

適用於 PostgreSQL 的SnapCenter插件功能

SnapCenter與插件應用程式以及儲存系統上的NetApp技術整合。若要使用 PostgreSQL 叢集插件，您需要使用SnapCenter圖形使用者介面。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份、復原和複製作業、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以及監控所有外掛程式中的作業。

- 自動化中央管理

您可以安排備份作業、設定基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷**NetApp**快照複製技術

SnapCenter使用NetApp快照技術和 PostgreSQL 叢集外掛程式來備份資源。

使用 PostgreSQL 外掛程式還可帶來以下好處：

- 支援備份、復原和複製工作流程
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 使用NetApp FlexClone技術建立節省空間的資源時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 作為建立備份的一部分，支援ONTAP的一致性群組 (CG) 快照功能。
- 能夠跨多個資源主機同時執行多個備份

在單次操作中，當單一主機中的資源共用同一磁碟區時，快照就會合併。

- 能夠使用外部命令建立快照。
- 支援 XFS 檔案系統上的 Linux LVM。

SnapCenter Plug-in for PostgreSQL 支援的儲存類型

SnapCenter支援實體機器和虛擬機器 (VM) 上的多種儲存類型。在安裝 PostgreSQL 的SnapCenter插件之前，您必須驗證對儲存類型的支援。

機器	儲存類型
實體伺服器	• FC 連接的 LUN • iSCSI 連接的 LUN • NFS 連結卷

機器	儲存類型
VMware ESXi	- 透過 FC 或 iSCSI ESXi HBA 連線的 RDM LUN 主機匯流排適配器 (HBA) 掃描可能需要很長時間才能完成，因為SnapCenter會掃描主機中存在的所有主機匯流排適配器。 您可以編輯位於 <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> 的 LinuxConfig.pm 文件，將 SCSI_HOSTS_OPTIMIZED_RESCAN 參數的值設定為 1，以僅重新掃描 HBA_DRI VBA 中列出的那些參數的值。 - iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統 - NFS 資料儲存上的 VMDK - VMFS 上的 VMDK - NFS 磁碟區直接連接到客戶系統 - NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

PostgreSQL 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令：ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - 倫
 - lun 創建
 - lun 創建
 - lun 創建
 - lun 刪除
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 重新命名

- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線

- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照修改-快照鎖定到期時間
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面

- 網路介面顯示
- 虛擬伺服器

為 PostgreSQL 的 SnapMirror 和 SnapVault 複製準備儲存系統

您可以使用具有 ONTAP SnapMirror 技術的 SnapCenter 插件在另一個磁碟區上建立備份集的鏡像副本，並使用 ONTAP SnapVault 技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter 完成 Snapshot 作業後對 SnapMirror 和 SnapVault 執行更新。SnapMirror 和 SnapVault 更新作為 SnapCenter 作業的一部分執行；不要建立單獨的 ONTAP 計畫。



如果您從 NetApp SnapManager 產品前往 SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP 會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter 不支援 SnapMirror 和 SnapVault 磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter 支援版本靈活的 SnapMirror 關係的管理。有關版本靈活的 SnapMirror 關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

PostgreSQL 的備份策略

定義 PostgreSQL 的備份策略

在建立備份作業之前定義備份策略有助於您獲得成功復原或複製資源所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

關於此任務

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

步驟

1. 確定何時應該備份資源。
2. 確定您需要多少個備份作業。
3. 決定如何命名您的備份。
4. 決定是否要建立基於 Snapshot 副本的策略來備份叢集的應用程式一致的快照。
5. 決定是否要使用 NetApp SnapMirror 技術進行複製或使用 NetApp SnapVault 技術進行長期保留。
6. 確定來源儲存系統和 SnapMirror 目標上的快照的保留期限。

7. 確定是否要在備份作業之前或之後執行任何命令，並提供前言或後記。

Linux主機上的資源自動發現

資源是 Linux 主機上由SnapCenter管理的 PostgreSQL 叢集和執行個體。安裝SnapCenter Plug-in for PostgreSQL 外掛程式後，該 Linux 主機上所有執行個體的 PostgreSQL 叢集都會自動被發現並顯示在資源頁面中。

支援的備份類型

備份類型指定您要建立的備份類型。 SnapCenter支援 PostgreSQL 叢集的基於快照複製的備份類型。

基於快照副本的備份

基於快照副本的備份利用NetApp快照技術來建立 PostgreSQL 叢集所在磁碟區的線上只讀副本。

SnapCenter Plug-in for PostgreSQL 如何使用一致性群組快照

您可以使用外掛程式為資源組建立一致性組快照。一致性群組是一個可以容納多個磁碟區的容器，以便您可以將它們作為一個實體進行管理。一致性組是多個磁碟區的同時快照，提供一組磁碟區的一致副本。

您也可以指定儲存控制器對快照進行一致分組的等待時間。可用的等待時間選項有*緊急*、中等*和*寬鬆。您也可以在一致的群組快照操作期間啟用或停用任意位置寫入檔案佈局 (WAFL) 同步。 WAFL同步提高了一致性組快照的效能。

SnapCenter如何管理資料備份

SnapCenter管理儲存系統和檔案系統層級的資料備份。

根據保留設定刪除主儲存或輔助儲存上的快照及其在 PostgreSQL 目錄中的對應項目。

確定 PostgreSQL 備份計畫的注意事項

確定備份計畫的最關鍵因素是資源的變化率。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

備份計畫分為兩部分，如下所示：

- 備份頻率（執行備份的頻率）

備份頻率（對於某些外掛程式也稱為計畫類型）是策略配置的一部分。例如，您可以將備份頻率設定為每小時、每天、每週或每月。

- 備份計畫（確切執行備份的時間）

備份計畫是資源或資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則

可以將計劃配置為每週四晚上 10:00 進行備份

PostgreSQL 所需的備份作業數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

PostgreSQL 叢集外掛程式的備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

`resourcegroupname_hostname_timestamp`

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳後綴會加入到快照名稱中。

PostgreSQL 的還原與復原策略

定義 PostgreSQL 資源的還原與復原策略

您必須在還原和復原叢集之前定義一個策略，以便能夠成功執行還原和復原作業。



僅支援手動恢復集群。

步驟

1. 確定手動新增的 PostgreSQL 資源支援的還原策略
2. 確定自動發現的 PostgreSQL 叢集支援的復原策略
3. 確定要執行的復原操作的類型。

手動新增的 **PostgreSQL** 資源支援的復原策略類型

您必須先定義一個策略，然後才能使用SnapCenter成功執行還原作業。



您無法還原手動新增的 PostgreSQL 資源。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

注意：PostgreSQL 外掛程式在 `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` 資料夾中建立 `backup_label` 和 `tablespace_map` 以協助手動復原。

自動發現的 **PostgreSQL** 支援的復原策略類型

您必須先定義一個策略，然後才能使用SnapCenter成功執行還原作業。

完整資源復原是自動發現的 PostgreSQL 叢集支援的復原策略。這將恢復資源的所有磁碟區、qtree 和 LUN。

自動發現的 **PostgreSQL** 的復原操作類型

SnapCenter Plug-in for PostgreSQL 支援單一檔案SnapRestore以及自動發現的 PostgreSQL 叢集的連線和複製復原類型。

單檔SnapRestore在 **NFS** 環境中針對以下場景執行：

- 如果僅選擇*完整資源*選項
- 當選擇的備份來自SnapMirror或SnapVault二級位置，並且選擇了「完整資源」選項時

單一檔案SnapRestore在 **SAN** 環境中針對下列場景執行：

- 如果僅選擇*完整資源*選項
- 從SnapMirror或SnapVault二級位置選擇備份，並選擇「完整資源」選項時

PostgreSQL 叢集支援的復原操作類型

SnapCenter可讓您對 PostgreSQL 叢集執行不同類型的復原操作。

- 將叢集恢復到最新狀態
- 將叢集恢復到特定時間點

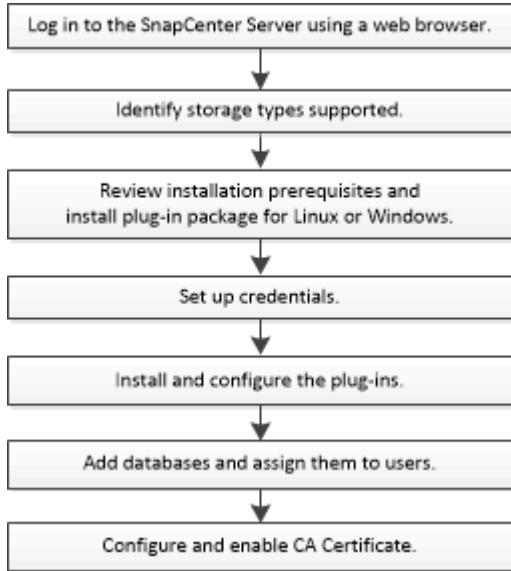
您必須指定恢復的日期和時間。

SnapCenter也為 PostgreSQL 叢集提供了無復原選項。

準備安裝適用於 PostgreSQL 的 SnapCenter 插件

SnapCenter Plug-in for PostgreSQL 的安裝工作流程

如果您想要保護 PostgreSQL 集群，則應該安裝並設定適用於 PostgreSQL 的 SnapCenter 插件。



新增主機並安裝 PostgreSQL 的 SnapCenter 插件的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。 SnapCenter Plug-in for PostgreSQL 可在 Windows 和 Linux 環境中使用。

- 您必須在主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 對於 Windows，插件建立服務應該使用「LocalSystem」Windows 使用者執行，這是以網域管理員身分安裝 PostgreSQL 插件時的預設行為。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用屬於本機工作群組用戶，則必須在主機上停用 UAC。適用於 Microsoft Windows 的 SnapCenter 外掛程式將預設與 Windows 主機上的 PostgreSQL 外掛程式一起部署。
- SnapCenter 伺服器應該可以存取 PostgreSQL 主機插件的 8145 或自訂連接埠。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 在 Windows 主機上安裝適用於 PostgreSQL 的外掛程式時，適用於 Microsoft Windows 的 SnapCenter 外掛程式會自動安裝。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Windows 主機上安裝 Java 11。

"下載適用於所有作業系統的 JAVA"

"NetApp互通性表工具"

Linux 主機

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Linux 主機上安裝 Java 11。

"下載適用於所有作業系統的 JAVA"

"NetApp互通性表工具"

- 對於在 Linux 主機上執行的 PostgreSQL 集群，在安裝 PostgreSQL 插件時，會自動安裝 UNIX 的 SnapCenter 插件。
- 您應該將 **bash** 作為插件安裝的預設 shell。

補充命令

要在 PostgreSQL 的 SnapCenter 插件上執行補充命令，必須將其包含在 *allowed_commands.config* 檔案中。

- Windows 主機上的預設位置：*C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Linux 主機上的預設位置：*/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config*

若要允許插件主機上的補充命令，請在編輯器中開啟 *_allowed_commands.config* 檔案。每個命令在單獨的行上輸入，並且命令不區分大小寫。確保指定完全限定的路徑名，並且如果路徑名包含空格，則將其括在引號 (") 中。

例如：

指令：mount 指令：umount 指令：「C:\Program Files\ NetApp\ SnapCreator commands\ sdcli.exe」 指令：
：myscript.bat

如果不存在 *allowed_commands.config* 文件，命令或腳本執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行 "[mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」

如果命令或腳本不在 *_allowed_commands.config* 中，則命令或腳本的執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行 "[mnt/mount -a]。透過在插件主機上的檔案 %s 中新增命令來授權。」



您不應使用通配符 (*) 來允許所有命令。

為 Linux 主機的非 root 使用者配置 sudo 權限

SnapCenter 允許非 root 使用者安裝適用於 Linux 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 umask 為 0027，請確保 java 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。
- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 Linux 的SnapCenter插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Precchecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```

LINUX_USER 是您建立的非 root 使用者的名稱。

您可以從 **sc_unix_plugins_checksum.txt** 檔案中取得 *checksum_value*，該檔案位於：

- *_C:\ProgramData\NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _* 如果 SnapCenter Server 安裝在 Windows 主機上。
- *_/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _* 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 **Windows** 的**SnapCenter**插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 " NetApp 互通性表工具 "。
主機上 SnapCenter 插件的最小 RAM	1GB

物品	要求
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統， SnapCenter升級或安裝將會失敗。"

安裝適用於 Linux 的SnapCenter插件包的主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間和大小需求。

物品	要求
作業系統	• 紅帽企業 Linux • SUSE Linux 企業伺服器 (SLES) 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間有所不同，取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。

物品	要求
所需軟體包	Java 11 Oracle Java 與 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 /var/opt/snapcenter/spl/etc/spl.properties 的 JAVA_HOME 選項設定為正確的 JAVA 版本和正確的路徑。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

為 PostgreSQL 的 SnapCenter 插件設定憑證

SnapCenter 使用憑證對 SnapCenter 操作的使用者進行身份驗證。您應該建立用於安裝 SnapCenter 插件的憑證以及用於在叢集或 Windows 檔案系統上執行資料保護作業的其他憑證。

關於此任務

- Linux 主機

您必須設定在 Linux 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

- 在左側導覽窗格中，按一下「設定」。
- 在「設定」頁面中，按一下「憑證」。
- 點選「新建」。
- 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。

對於這個領域...	這樣做...
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 - 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 - 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i> 請勿在密碼中使用雙引號（"）或反引號（`）。密碼中不應同時使用小於號（<）和驚嘆號（!）符號。例如，lessthan<!10、lessthan10<!、backtick`12。
密碼	輸入用於身份驗證的密碼。
認證模式	選擇您想要使用的身份驗證模式。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。
- 為此，請從 PowerShell 執行以下命令：

```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- a. 重新啟動主機。
- b. 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA：Install-AdServiceAccount

<gMSA>

c. 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`

5. 將管理權限指派給主機上配置的 gMSA。
6. 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

安裝適用於 PostgreSQL 的 SnapCenter 插件

新增主機並在遠端主機上安裝插件包

您必須使用 SnapCenter 新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以新增主機並為單一主機安裝插件包。

開始之前

- 如果 SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 您應該確保訊息佇列服務正在運行。
- 管理文件包含有關管理主機的資訊。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

["在 Windows Server 2016 或更高版本上為 PostgreSQL 設定群組託管服務帳戶"](#)

關於此任務

- 您不能將 SnapCenter 伺服器作為插件主機新增至另一個 SnapCenter 伺服器。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下「新增」。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux  PostgreSQL 外掛程式安裝在 PostgreSQL 用戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。
主機名稱	輸入通訊主機名稱。輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。SnapCenter 依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標放在您提供的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

使用 REST API 安裝 PostgreSQL 外掛程式時，必須傳遞版本為 3.0。例如，PostgreSQL:3.0

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果 SnapCenter 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。

對於這個領域...	這樣做...
安裝路徑	PostgreSQL 外掛程式安裝在 PostgreSQL 用戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。 - 對於適用於 Windows 的 SnapCenter 插件包，預設路徑為 C:\Program Files\NetApp\SnapCenter。您也可以選擇自訂路徑。 - 對於適用於 Linux 的 SnapCenter 插件包，預設路徑為 /opt/NetApp/snapcenter。您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
新增叢集中的所有主機	選取此複選框可新增所有叢集節點。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	對於 Windows 主機，如果您要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。  以以下格式提供 gMSA 名稱： ：domainName\accountName\$。  gMSA 將僅用作 Windows 服務的 SnapCenter 插件的登入服務帳戶。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）和 Java 版本（適用於 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 C:\Program Files\NetApp\SnapCenter WebApp 的 web.config 檔案以修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 web.config 文件，則必須在兩個節點上更新該文件。

8. 如果主機類型為 Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



即使之前已將同一台主機新增至 SnapCenter 並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

- 對於 Windows 插件，安裝和升級日誌位於：C:\Windows\SnapCenter plugin\Install<JOBID>_

- 對於 Linux 插件，安裝日誌位於：`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log_`，升級日誌位於：`_/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-JOB_grade_f.`

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux** 或 **Windows** 的 **SnapCenter** 插件包

您可以使用 `Install-SmHostPackage PowerShell cmdlet` 同時在多個主機上安裝適用於 **Linux** 或 **Windows** 的 **SnapCenter** 插件套件。

開始之前

您必須以網域使用者身分登入 **SnapCenter**，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 **PowerShell**。
2. 在 **SnapCenter Server** 主機上，使用 `Open-SmConnection cmdlet` 建立會話，然後輸入您的憑證。
3. 使用 `Install-SmHostPackage cmdlet` 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 `cmdlet` 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝適用於 **PostgreSQL** 的 **SnapCenter** 插件

您應該使用 **SnapCenter** 使用者介面 (UI) 安裝適用於 **PostgreSQL** 叢集的 **SnapCenter** 插件。如果您的環境不允許從 **SnapCenter** UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控制台模式或靜默模式安裝適用於 **PostgreSQL** 叢集的插件。

開始之前

- 您應該在 **PostgreSQL** 用戶端所在的每個 **Linux** 主機上安裝 **PostgreSQL** 叢集插件。
- 要安裝 **SnapCenter Plug-in for PostgreSQL** 叢集的 **Linux** 主機必須符合相關軟體、叢集和作業系統要求。

互通性矩陣工具 (IMT) 包含受支援配置的最新資訊。

"[NetApp 互通性表工具](#)"

- 適用於 **PostgreSQL** 叢集的 **SnapCenter** 插件是適用於 **Linux** 的 **SnapCenter** 插件包的一部分。在安裝適用於 **Linux** 的 **SnapCenter** 插件包之前，您應該已經在 **Windows** 主機上安裝了 **SnapCenter**。

步驟

1. 將 **Linux** 安裝檔案 (`snapcenter_linux_host_plugin.bin`) 的 **SnapCenter** 插件包從 `C:\ProgramData\NetApp\SnapCenter\Package Repository` 複製到要安裝 **PostgreSQL** 插件的主機。

您可以從安裝了 **SnapCenter** 伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。

3. 安裝插件： `path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT 指定 SMCORE HTTPS 通訊連接埠。
- -DSERVER_IP 指定 SnapCenter 伺服器 IP 位址。
- -DSERVER_HTTPS_PORT 指定 SnapCenter 伺服器 HTTPS 連接埠。
- -DUSER_INSTALL_DIR 指定要安裝 Linux 版 SnapCenter 插件包的目錄。
- DINSTALL_LOG_NAME 指定日誌檔案的名稱。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. 編輯 `<安裝目錄> NetApp` 文件，然後新增 `PLUGINS_ENABLED = PostgreSQL:3.0` 參數。
5. 使用 `Add-Smhost cmdlet` 和所需參數將主機新增至 SnapCenter 伺服器。

可以透過執行 `_Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

監控 PostgreSQL 插件安裝狀態

您可以使用「作業」頁面監控 SnapCenter 插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。

- b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
 5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入SnapCenter伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 從 PowerShell 執行以下操作：
 - a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0:_{SMCore Port}
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
. 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0:_{SMCore Port}_ certhash=$cert
appid="$guid"
```

為 Linux 主機上的 SnapCenter PostgreSQL 插件服務設定 CA 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

插件使用位於 `/opt/NetApp/snapcenter/scc/etc` 的檔案「keystore.jks」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與密鑰“KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks
. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：
```



```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/ NetApp/snapcenter/scc/etc`。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。
```



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導航至包含插件金鑰庫 `/opt/ NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

• 如果CA憑證中的別名較長，且包含空格或特殊字元（"*"，"，"，"），請將別名修改為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

• 在 agent.properties 檔案中配置來自 CA 憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

8. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於此任務

- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter插件的 CRL 檔案的預設目錄是「opt/ NetApp/snapcenter/scc/etc/crl」。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 agent.properties 檔案中的預設目錄。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

為 **Windows** 主機上的**SnapCenter PostgreSQL** 插件服務設定 **CA** 證書

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

外掛程式使用位於 *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc* 的檔案 *keystore.jks* 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與金鑰_KEYSTORE_PASS_對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore 金鑰庫.jks
```



如果 Windows 命令提示字元無法辨識「keytool」命令，請將 keytool 命令替換為其完整路徑。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe"-storepasswd -keystore keystore.jks
```

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks
```

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案“_keystore.jks”。

3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。

7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在_agent.properties_檔案中配置來自CA憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenterSnapCenter的 CRL 檔案的預設目錄是 'C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl'。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 agent.properties 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器和對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行_Set-SmCertificateSettings_cmdlet 來啟用或停用 CA 憑證。
- 您可以使用_Get-SmCertificateSettings_顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

做好資料保護準備

使用適用於 **PostgreSQL** 的**SnapCenter**插件的先決條件

在使用SnapCenter Plug-in for PostgreSQL 之前， SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。
- 登入SnapCenter伺服器。
- 透過新增儲存系統連接和建立憑證（如果適用）來配置SnapCenter環境。
- 在您的 Linux 或 Windows 主機上安裝 Java 11。

您必須在主機的環境路徑變數中設定 Java 路徑。

- 如果您想要備份複製，請設定SnapMirror和SnapVault。

如何使用資源、資源群組和策略來保護 **PostgreSQL**

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的 PostgreSQL 叢集。

- SnapCenter資源組是主機上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

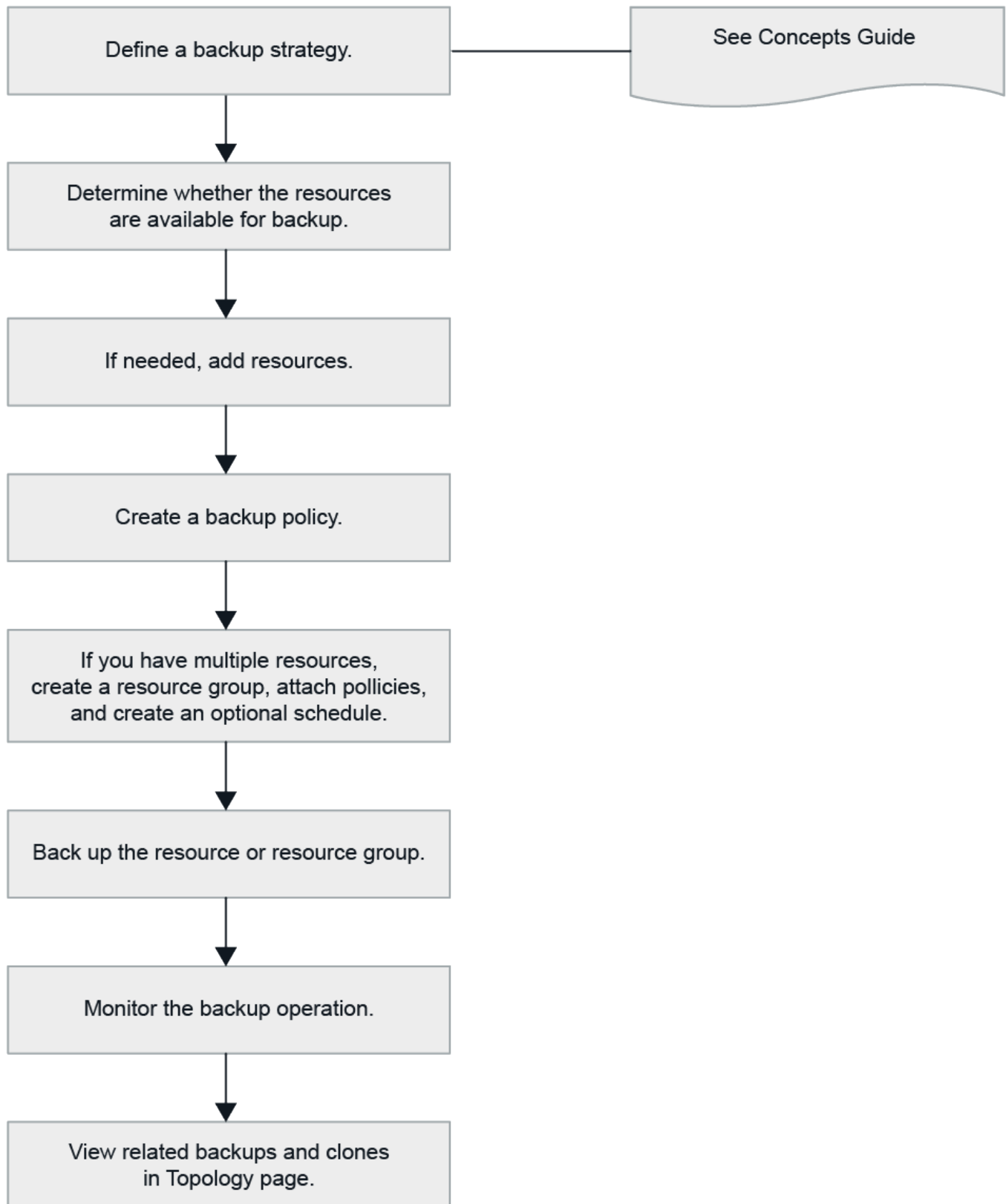
資源群組可以視為定義您想要保護的內容以及何時以日期和時間進行保護。把政策看作是定義你想如何保護它。例如，如果要備份所有集群，則可以建立一個包含主機中所有集群的資源組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加原則時，您可以配置資源組以每天執行完整備份。

備份 PostgreSQL 資源

備份 PostgreSQL 資源

您可以建立資源（叢集）或資源群組的備份。備份工作流包括規劃、識別要備份的叢集、管理備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含更多有關 PowerShell cmdlet 的資訊。<https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenter軟體 Cmdlet 參考指南"]。

自動發現集群

資源是 Linux 主機上由SnapCenter管理的 PostgreSQL 叢集。您可以在發現可用的 PostgreSQL 叢集後，將資源新增至資源群組以執行資料保護作業。

開始之前

- 您必須已經完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。
- SnapCenter Plug-in for PostgreSQL 不支援自動發現駐留在 RDM/VMDK 虛擬環境中的資源。

關於此任務

- 安裝外掛程式後，該Linux主機上的所有叢集都會自動發現並顯示在資源頁面上。
- 僅自動發現集群。

自動發現的資源不能被修改或刪除。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“PostgreSQL 外掛程式”。
2. 在資源頁面中，從視圖清單中選擇資源類型。
3. （可選）點擊  *，然後選擇主機名稱。

然後您可以點擊  * 關閉篩選窗格。

4. 按一下「刷新資源」以發現主機上可用的資源。

資源與資源類型、主機名稱、關聯資源群組、備份類型、政策和總體狀態等資訊一起顯示。

- 如果叢集位於NetApp儲存上且未受保護，則「整體狀態」欄位中顯示「未受保護」。
- 如果叢集位於NetApp儲存系統上並且受到保護，且沒有執行備份操作，則「整體狀態」欄位中會顯示「備份未執行」。否則，狀態將根據上次備份狀態變更為備份失敗或備份成功。



如果叢集在SnapCenter之外重新命名，則必須刷新資源。

手動將資源新增至插件主機

Windows 主機不支援自動發現。您必須手動新增 Postgresql 叢集資源。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。

關於此任務

以下配置不支援自動發現：

- RDM 和 VMDK 佈局

步驟

1. 在左側導覽窗格中，從下拉清單中選擇適用於 Postgresql 的SnapCenter插件，然後按一下「資源」。

2. 在資源頁面中，按一下*新增 Postgresql 資源*。
3. 在提供資源詳細資訊頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	指定叢集名稱。
主機名稱	輸入主機名稱。
類型	選擇集群。
實例	指定實例的名稱，該實例是叢集的父級。
證書	選擇憑證或新增憑證資訊。 這是可選的。

4. 在「提供儲存佔用空間」頁面中，選擇儲存類型並選擇一個或多個磁碟區、LUN 和 qtree，然後按一下「儲存」。

可選：您可以點擊 *  * 圖示用於從其他儲存系統新增更多磁碟區、LUN 和 qtree。

5. 選用：在資源設定頁面中，對於 Windows 主機上的資源，輸入 PostgreSQL 外掛程式的自訂鍵值對
6. 查看摘要，然後按一下「完成」。

叢集與主機名稱、相關資源群組和策略以及整體狀態等資訊一起顯示

如果您想讓使用者存取資源，您必須將資源指派給使用者。這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

"新增使用者或群組並分配角色和資產"

完成後

- 新增叢集後，您可以修改PostgreSQL叢集的詳細資訊。
- 從SnapCenter 5.0 遷移的資源（表空間和叢集）將在SnapCenter 6.0 中標記為 PostgreSQL 叢集類型。
- 修改從SnapCenter 5.0 或更早版本遷移的手動新增的資源時，請在「資源設定」頁面中對自訂鍵值對執行下列操作：
 - 在*名稱*欄位中指定術語「PORT」。
 - 在「值」欄位中指定連接埠號碼。

為 PostgreSQL 建立備份策略

在使用SnapCenter備份 PostgreSQL 資源之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。

開始之前

- 您必須已經定義了您的備份策略。

有關詳細信息，請參閱有關為 PostgreSQL 叢集定義資料保護策略的資訊。

- 您必須已完成安裝SnapCenter、新增主機、設定儲存系統連線和新增資源等任務，為資料保護做好準備。
- 如果您要將快照複製到映像或保管庫， SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。

此外，您還可以在策略中指定複製、腳本和應用程式設定。當您想要將該策略重新用於另一個資源群組時，這些選項可以節省時間。

關於此任務

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
 - 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能會導致保留的快照數量超過策略中指定的數量。
 - 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選「新建」。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「策略類型」頁面中，執行以下操作：
 - a. 選擇儲存類型。
 - b. 在*自訂備份設定*部分，提供任何必須以鍵值格式傳遞給外掛程式的特定備份設定。

您可以提供多個鍵值傳遞給插件。

6. 在「備份和複製」頁面中，執行以下操作：
 - a. 透過選擇*按需*、每小時、每天、*每週*或*每月*來指定計畫頻率。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，還使您能夠為每個策略分配不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- a. 在「快照設定」部分中，指定在「備份類型」頁面中選擇的備份類型和計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。  最大保留值為 1018。如果保留設定的值高於ONTAP版本支援的值，則備份將會失敗。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*，並指定天、月或年。 SnapLock保留期應少於 100 年。

7. 選擇一個策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

8. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
*建立本機 Snapshot 副本後更新SnapMirror *	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 如果ONTAP中的保護關係屬於鏡像和保險庫類型，並且您僅選擇此選項，則在主伺服器上建立的快照將不會傳輸到目標伺服器，但會在目標伺服器中列出。如果從目標中選擇此快照來執行還原操作，則會顯示下列錯誤訊息：對於所選的保管/鏡像備份，輔助位置不可用。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓撲頁面中查看 PostgreSQL 資源相關的備份和克隆"。
*建立本機 Snapshot 副本後更新SnapVault *	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。 有關SnapLock Vault 的更多信息，請參閱將快照提交到保管庫目標上的 WORM 看"在拓撲頁面中查看 PostgreSQL 資源相關的備份和克隆"。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

9. 查看摘要，然後按一下「完成」。

建立資源組並附加策略

資源組是您必須新增要備份和保護的資源的容器。資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資

源組，以定義要執行的資料保護作業的類型。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

- 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，按一下「新資源組」。
- 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。  資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
使用自訂名稱格式進行快照複製	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。

這有助於過濾螢幕上的信息。

- 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
- 在應用程式設定頁面中，執行以下操作：
 - 按一下“備份”箭頭以設定其他備份選項：

啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。

對於這個領域...	這樣做...
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+

- 點擊“腳本”箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- 按一下「自訂配置」箭頭並輸入使用此資源的所有資料保護操作所需的自訂鍵值對。

範圍	環境	描述
歸檔日誌啟用	(是/否)	啟用存檔日誌管理以刪除存檔日誌。
歸檔日誌保留	天數	指定存檔日誌保留的天數。 此設定必須等於或大於 NTAP_SNAPSHOT_RETENTIONS。
歸檔日誌目錄	更改訊息目錄/日誌	指定包含存檔日誌的目錄的路徑。
ARCHIVE_LOG_EXT	檔案副檔名	指定存檔日誌檔案擴充長度。 例如，如果歸檔日誌為log_backup_0_0_0.1615185519429，且file_extension值為5，則日誌的副檔名將保留5位數，即16151。

範圍	環境	描述
ARCHIVE_LOG_RECURSIVE_SEARCH	(是/否)	啟用子目錄內的存檔日誌管理。 如果存檔日誌位於子目錄下，則應使用此參數。



自訂鍵值對支援 PostgreSQL Linux 插件系統，不支援註冊為集中式 Windows 插件的 PostgreSQL 叢集。

- c. 點選*Snapshot Copy Tool*箭頭選擇建立快照的工具：

如果你想...	然後...
SnapCenter使用適用於 Windows 的插件並在建立快照之前將檔案系統置於一致狀態。對於 Linux 資源，此選項不適用。	選擇*具有檔案系統一致性的SnapCenter *
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
輸入要在主機上執行的命令來建立快照副本。	選擇*其他*，然後輸入要在主機上執行的建立快照的命令。

7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 *  *.

這些策略列在「為選定的策略配置計劃」部分中。

- b. 在配置計劃列中，按一下 *  * 您想要配置的策略。
c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。

其中，policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。必須在*設定* > *全域設定*中設定 SMTP 伺服器。

9. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並為 PostgreSQL 資源啟用二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建​​立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

- a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 為 PostgreSQL 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 備份、還原或複製 PostgreSQL 叢集之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且叢集狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

步驟

1. 使用 Open-SmConnection cmdlet 啟動 PowerShell Core 連線會話。

```
PS C:\> Open-SmConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例顯示如何使用 Windows 憑證建立名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. 將 PostgreSQL 通訊主機新增至 SnapCenter Server。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode PostgreSQL
```

5. 在主機上安裝軟體包和適用於 PostgreSQL 的 SnapCenter 插件。

對於 Linux：

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode PostgreSQL
```

對於 Windows：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. 設定 SQLLIB 的路徑。

對於 Windows，PostgreSQL 外掛程式將使用 SQLLIB 資料夾的預設路徑：“C:\Program Files\IBM\SQLLIB\BIN”

如果要覆蓋預設路徑，請使用下列命令。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” = “<custom_path>\IBM\SQLLIB\BIN”}
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份 PostgreSQL

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

開始之前

- 您必須已經建立了備份策略。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用「vsadmin」角色，則不需要「snapmirror all」權限。
- 對於基於 Snapshot 副本的備份作業，請確保所有租用戶叢集均有效且處於活動狀態。
- 對於靜默、快照和取消靜默操作的預先命令和後命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：

- Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 主機上的預設位置：`/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

選擇  *，然後選擇主機名稱和資源類型來過濾資源。然後您可以選擇  關閉篩選器窗格。

3. 選擇要備份的資源。
4. 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。

例如，*customtext_policy_hostname* 或 *resource_hostname*。預設情況下，時間戳記會附加到快照名稱。

5. 在應用程式設定頁面中，執行以下操作：

- 選擇“備份”箭頭來設定其他備份選項：

如果需要，請啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待「一致性組快照」操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

- 選擇「腳本」箭頭來執行靜默、快照和取消靜默操作的前置和後置命令。

您也可以在退出備份作業之前執行預命令。前言和後記在SnapCenter伺服器中運作。

- 選擇自訂配置箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
- 選擇*Snapshot Copy Tool*箭頭來選擇建立快照的工具：

如果你想...	然後...
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
SnapCenter使用適用於 Windows 的插件將檔案系統置於一致狀態，然後建立快照	選擇*具有檔案系統一致性的SnapCenter *。
輸入建立快照的命令	選擇*其他*，然後輸入建立快照的命令。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 * 來建立策略  *.

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 選擇 *  * 在您想要設定計畫的政策的政策設定計畫列中。
- c. 在為政策_policy_name_新增計劃對話方塊中，配置計畫，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後選擇*完成*。

進入資源拓樸頁面。

9. 選擇*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行

保留。

b. 選擇*備份*。

11. 透過點選「監視」>「作業」來監視操作進度。

- 在MetroCluster配置中， SnapCenter可能無法在故障轉移後偵測到保護關係。

有關信息，請參閱：["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java堆大小不夠大，則備份可能會失敗。

若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method` 命令啟動SnapCenter VMware 插件服務。將此指令更新為以下內容：`Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-SmConnection
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmResources cmdlet 新增手動資源。

此範例顯示如何新增 PostgreSQL 實例：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode PostgreSQL  
-ResourceType Instance -ResourceName postgresqlinst1  
-StorageFootPrint  
(@{"VolumeName"="winpostgresql01_data01";"LUNName"="winpostgresql01_  
data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. 使用 Add-SmPolicy cmdlet 建立備份策略。

4. 使用 Add-SmResourceGroup cmdlet 保護資源或為SnapCenter新增資源組。

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

此範例顯示如何備份資源組：

```
C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-  
clusters-using-powershell-cmdlets-postgresql.adocith_Resources'  
-Policy postgresql_policy1
```

此範例備份受保護的資源：

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
-Policy postgresql_policy2
```

6. 使用 `Get-smJobSummaryReport` cmdlet 監視作業狀態（正在執行、已完成或失敗）。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. 使用 `Get-SmBackupReport` cmdlet 監視備份作業詳細資料（如備份 ID、備份名稱）以執行還原或複製作業。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId               : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime              : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份資源組

資源組是主機上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要備份與二級儲存具有SnapMirror關係的資源，則指派給儲存使用者的ONTAP角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。

關於此任務

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或選擇，然後選擇標籤。然後您可以選擇關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：

- a. 如果您將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 選擇*備份*。

5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

監控 PostgreSQL 備份操作

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監控 PostgreSQL 叢集上的資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消 PostgreSQL 的備份操作

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，

則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	- 在左側導覽窗格中，按一下「監控」>「作業」。 - 選擇操作，然後按一下「取消作業」。
活動窗格	- 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 - 選擇操作。 - 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓樸頁面中查看 PostgreSQL 備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。



顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓樸頁面。

4. 查看*摘要卡*以了解主儲存和輔助儲存上可用的備份和克隆數量的摘要。

*摘要卡*部分顯示基於 Snapshot 副本的備份和克隆的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

按需備份後，按一下「刷新」按鈕以刷新備份或複製的詳細資訊。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

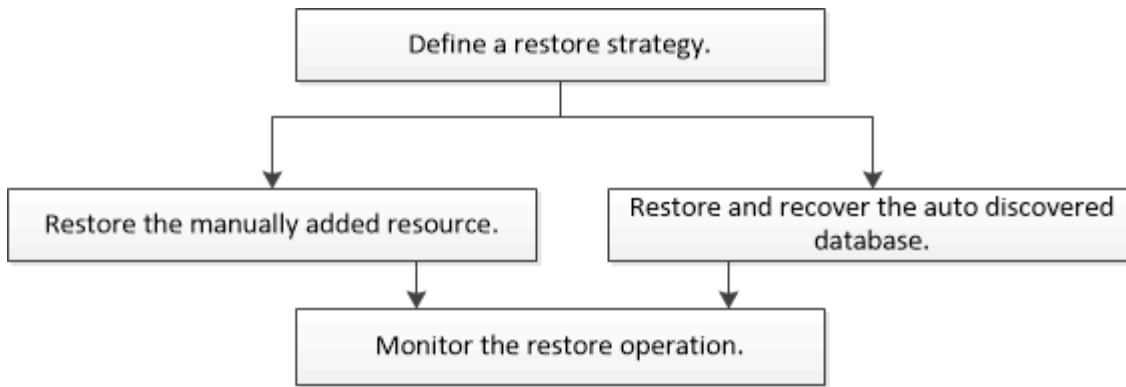
7. 如果要刪除克隆，請從表中選擇克隆，然後按一下 .
8. 如果要拆分克隆，請從表中選擇克隆，然後按一下 .

還原 PostgreSQL

復原工作流程

還原和復原工作流程包括規劃、執行還原操作和監視操作。

以下工作流程顯示了執行還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

["SnapCenter軟體 Cmdlet 參考指南"](#)。

還原並還原手動新增的資源備份

您可以使用SnapCenter從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.



6. 在「復原範圍」頁面中，選擇「完整資源」。
 - a. 如果選擇*完整資源*，則會還原 PostgreSQL 叢集的所有設定資料磁碟區。

如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果在相同的磁碟區或 qtree 上託管任何其他資源，則該資源也會被刪除。

您可以選擇多個 LUN。



如果選擇“全部”，則會還原磁碟區、qtree 或 LUN 上的所有檔案。

7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。


```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

還原和還原自動發現的叢集備份

您可以使用 SnapCenter 從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 無法從SnapCenter還原基於檔案的備份副本。
- 對於自動發現的資源，SFSR 支援恢復。
- 不支援自動恢復。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.

Primary Backup(s)	
search 	  
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 在復原範圍頁面中，選擇*完整資源*，還原PostgreSQL叢集配置的資料卷。
7. 在「恢復範圍」頁面中，選擇以下選項之一：

如果你...	這樣做...
希望恢復到盡可能接近當前時間	選擇*恢復到最近的狀態*。對於單一容器資源，指定一個或多個日誌和目錄備份位置。

想要恢復到指定的時間點	選擇*恢復到時間點*。 a. 輸入日期和時間。輸入日期和時間。例如，PostgreSQL Linux 主機位於加州桑尼維爾，而北卡羅來納州羅利的用戶正在將日誌還原到SnapCenter。 如果使用者想要恢復到凌晨 5 點，則使用者必須將瀏覽器時區設定為 PostgreSQL Linux 主機時區，即 GMT-07:00，並將日期和時間指定為凌晨 5:00
不想恢復	選擇*不恢復*。



您無法還原手動新增的 PostgreSQL 資源。



SnapCenter Plug-in for PostgreSQL 在 `/<OS_temp_folder>/postgresql_sc_recovery<Restore_JobId>/` 資料夾中建立 backup_label 和 tablespace_map 以協助手動復原。

1. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

2. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

3. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

4. 查看摘要，然後按一下「完成」。

5. 透過點選「監視」>「作業」來監視操作進度。

使用 PowerShell cmdlet 還原資源

恢復資源備份包括啟動與SnapCenter伺服器的連線會話、列出備份並檢索備份資訊以及恢復備份。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 `Get-SmBackup` 和 `Get-SmBackupReport` cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08... 8/4/2015	11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08... 8/4/2015	11:23:17 AM

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```

PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"

SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified

SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified

```

3. 使用 `Restore-SmBackup` cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 PostgreSQL 復原操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成

-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

複製 PostgreSQL 資源備份

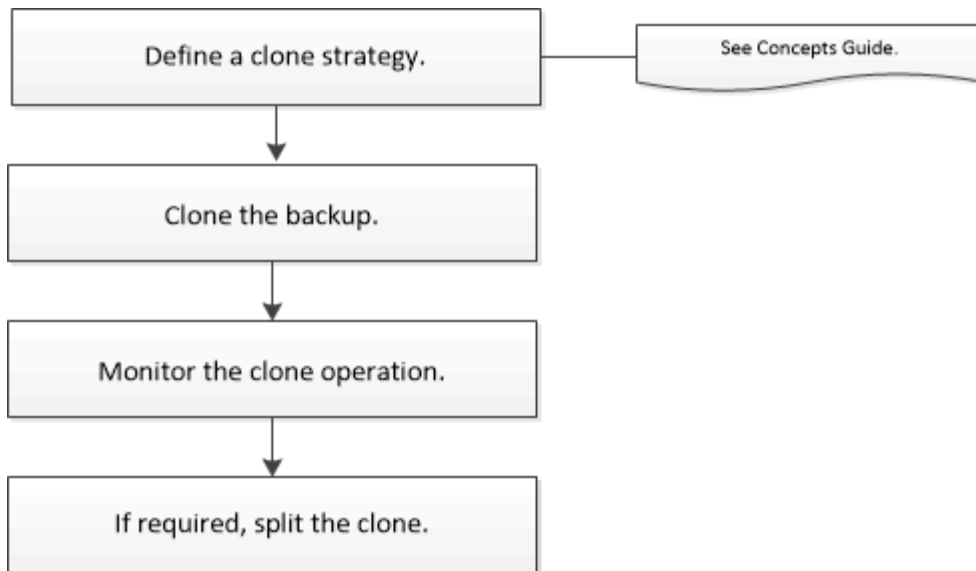
克隆工作流程

克隆工作流程包括執行克隆操作和監視操作。

關於此任務

- 您可以在來源 PostgreSQL 伺服器上複製。
- 您可能會因為以下原因而複製資源備份：
 - 在應用程式開發週期中測試必須使用目前資源結構和內容實現的功能
 - 用於填充資料倉儲時的資料擷取和操作工具
 - 恢復被錯誤刪除或更改的數據

以下工作流程顯示了執行複製操作必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

複製 PostgreSQL 備份

您可以使用 SnapCenter 克隆備份。您可以從主備份或輔助備份複製。

開始之前

- 您應該已經備份資源或資源組。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 對於克隆前或克隆後命令，您應該從以下路徑檢查這些命令是否存在於插件主機上可用的命令清單中：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 有關 FlexClone 磁碟區拆分操作的信息，請參閱 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html>["將 FlexClone 磁碟區從其父卷中拆分出來"]。
- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和策略以及狀態等資訊一起顯示。

3. 選擇資源或資源組。

如果選擇資源組，則必須選擇資源。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	選擇要建立克隆的主機。
目標連接埠	輸入要從現有備份複製的目標 PostgreSQL 目標連接埠。
NFS 匯出 IP 位址	輸入將會匯出複製磁碟區的 IP 位址或主機名稱。 這僅適用於 NFS 儲存類型資源。
容量池最大吞吐量（MiB/s）	輸入容量池的最大吞吐量。 這僅適用於 ANF 儲存類型資源。

7. 在腳本頁面中，執行以下步驟：



腳本在插件主機上運行。

- a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。
 - 克隆前命令：刪除現有的同名集群
 - 克隆後命令：驗證叢集或啟動叢集。
- b. 輸入 mount 指令將檔案系統掛載到主機。

Linux 電腦上磁碟區或 qtree 的掛載指令：

NFS 範例：`mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

- 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

- 查看摘要，然後按一下「完成」。
- 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

- 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-SmConnection
```

- 使用 Get-SmBackup cmdlet 檢索備份以執行複製作業。

此範例顯示有兩個備份可供複製：

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

- 從現有備份啟動複製操作，並指定複製磁碟區匯出到的 NFS 匯出 IP 位址。

此範例顯示要複製的備份具有 NFSExportIPs 位址 10.32.212.14：

對於 PostgreSQL 叢集：

```
PS C:\> New-SmClone -AppPluginCode PostgreSQL -BackupName "
scpostgresql01_ openenglab_netapp_com_PostgreSQL_postgres_5432_06-
26-2024_00_33_41_1570" -Resources @{"Host"="
10.32.212.13";"Uid"="postgres_5432"} -port 2345 -CloneToHost
10.32.212.14
```



如果沒有指定NFSExportIPs，則預設匯出至複製目標主機。

- 使用 Get-SmCloneReport cmdlet 查看複製作業詳細信息，以驗證備份是否已成功複製。

您可以查看複製 ID、開始日期和時間、結束日期和時間等詳細資訊。

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

監控 PostgreSQL 克隆操作

您可以使用「作業」頁面監控SnapCenter複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。

2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“*”  *。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。

6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCore 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定 SMCore 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為 5 分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter 克隆或驗證失敗，聚合不存在"](#)

升級 SnapCenter 後刪除或分割 PostgreSQL 叢集克隆

升級到 SnapCenter 4.3 後，您將不再看到克隆。您可以從建立克隆的資源的拓樸頁面中刪除克隆或分割克隆。

關於此任務

如果您要找到隱藏複製的儲存空間，請執行以下命令：Get-SmClone -ListStorageFootprint

步驟

1. 使用 remove-smbbackup cmdlet 刪除克隆資源的備份。
2. 使用 remove-smresourcegroup cmdlet 刪除克隆資源的資源群組。
3. 使用 remove-smprotectresource cmdlet 刪除克隆資源的保護。
4. 從資源頁面中選擇父資源。

進入資源拓樸頁面。

5. 從「管理副本」檢視中，選擇來自主或輔助（鏡像或複製）儲存系統的複製。
6. 選擇克隆，然後按一下  刪除克隆或點擊  分裂克隆。
7. 按一下“確定”。

保護 MySQL

適用於 MySQL 的SnapCenter插件

適用於 MySQL 的SnapCenter插件概述

適用於 MySQL 資料庫的SnapCenter外掛程式是NetApp SnapCenter software的主機端元件，可實現 MySQL 資料庫的應用程式感知資料保護管理。MySQL 資料庫外掛程式可自動執行SnapCenter環境中 MySQL 資料庫的備份、復原和複製。

SnapCenter支援單一實例 MySQL 設定。您可以在 Linux 和 Windows 環境中使用 MySQL 資料庫外掛程式。在 Windows 環境中，MySQL 將作為手動資源得到支援。

安裝 MySQL 資料庫外掛程式後，您可以使用具有NetApp SnapMirror技術的SnapCenter在另一個磁碟區上建立備份集的鏡像副本。您也可以使用具有NetApp SnapVault技術的插件來執行磁碟到磁碟的備份複製，以符合標準。

適用於 MySQL 的SnapCenter外掛程式支援ONTAP和 Azure NetApp檔案儲存佈局上的 NFS 和 SAN。

支援VMDK、vVol、RDM虛擬儲存佈局。

不支援符號連結。

使用適用於 MySQL 的SnapCenter插件可以做什麼

在您的環境中安裝 MySQL 資料庫外掛程式時，您可以使用SnapCenter備份、還原和複製 MySQL 執行個體。您也可以執行支援這些操作的任務。

- 新增實例。
- 建立備份。
- 從備份中復原。
- 克隆備份。
- 安排備份作業。
- 監控備份、復原和克隆作業。
- 查看備份、復原和克隆作業的報告。

適用於 MySQL 的SnapCenter插件功能

SnapCenter與插件應用程式以及儲存系統上的NetApp技術整合。若要使用 MySQL 資料庫插件，您需要使用SnapCenter圖形使用者介面。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。SnapCenter介面可讓您跨外掛程式完成一致的備份、復原和複製作業、使用集中式報表、使用一目了然的儀表板視圖、設定基於角色的存取控制 (RBAC) 以

及監控所有外掛程式中的作業。

- 自動化中央管理

您可以安排備份作業、設定基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷**NetApp**快照複製技術

SnapCenter使用NetApp快照技術和 MySQL 資料庫外掛程式來備份資源。

使用 MySQL 外掛程式還可帶來以下好處：

- 支援備份、復原和複製工作流程
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 使用NetApp FlexClone技術建立節省空間的資源時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 作為建立備份的一部分，支援ONTAP的一致性群組 (CG) 快照功能。
- 能夠跨多個資源主機同時執行多個備份

在單次操作中，當單一主機中的資源共用同一磁碟區時，快照就會合併。

- 能夠使用外部命令建立快照。
- 支援 XFS 檔案系統上的 Linux LVM。

SnapCenter Plug-in for MySQL 支援的儲存類型

SnapCenter支援實體機器和虛擬機器 (VM) 上的多種儲存類型。在安裝 MySQL 的SnapCenter插件之前，您必須驗證對您的儲存類型的支援。

機器	儲存類型
實體伺服器	• FC 連接的 LUN • iSCSI 連接的 LUN • NFS 連結卷

機器	儲存類型
VMware ESXi	- 透過 FC 或 iSCSI ESXi HBA 連線的 RDM LUN 主機匯流排適配器 (HBA) 掃描可能需要很長時間才能完成，因為SnapCenter會掃描主機中存在的所有主機匯流排適配器。 您可以編輯位於 <code>/opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config</code> 的 LinuxConfig.pm 文件，將 SCSI_HOSTS_OPTIMIZED_RESCAN 參數的值設定為 1，以僅重新掃描 HBA_DRI VBA 中列出的那些參數的值。 - iSCSI LUN 由 iSCSI 啟動器直接連接到客戶系統 - NFS 資料儲存上的 VMDK - VMFS 上的 VMDK 已建立 - NFS 磁碟區直接連接到客戶系統 - NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

MySQL 插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令： ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - 倫
 - lun 創建
 - lun 創建
 - lun 創建
 - lun 刪除
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 重新命名

- lun igroup 秀
- lun 映射新增報告節點
- lun 映射創建
- lun 映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun 修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 持久預留清除
- lun 大小調整
- lun 序號
- 倫秀
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 ls 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線

- 在線量
- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照修改-快照鎖定到期時間
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- 虛擬伺服器 iSCSI
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面

- 網路介面顯示
- 虛擬伺服器

為 MySQL 的 SnapMirror 和 SnapVault 複製準備儲存系統

您可以使用具有 ONTAP SnapMirror 技術的 SnapCenter 插件在另一個磁碟區上建立備份集的鏡像副本，並使用 ONTAP SnapVault 技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間配置資料保護關係並初始化該關係。

SnapCenter 完成 Snapshot 作業後對 SnapMirror 和 SnapVault 執行更新。SnapMirror 和 SnapVault 更新作為 SnapCenter 作業的一部分執行；不要建立單獨的 ONTAP 計畫。



如果您從 NetApp SnapManager 產品前往 SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP 會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter 不支援 SnapMirror 和 SnapVault 磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter 支援版本靈活的 SnapMirror 關係的管理。有關版本靈活的 SnapMirror 關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

MySQL 的備份策略

定義 MySQL 的備份策略

在建立備份作業之前定義備份策略有助於您獲得成功復原或複製資源所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

關於此任務

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

步驟

1. 確定何時應該備份資源。
2. 確定您需要多少個備份作業。
3. 決定如何命名您的備份。
4. 決定是否要建立基於 Snapshot 副本的策略來備份資料庫的應用程式一致的快照。
5. 決定是否要使用 NetApp SnapMirror 技術進行複製或使用 NetApp SnapVault 技術進行長期保留。
6. 確定來源儲存系統和 SnapMirror 目標上的快照的保留期限。

7. 確定是否要在備份作業之前或之後執行任何命令，並提供前言或後記。

Linux主機上的資源自動發現

資源是 Linux 主機上由SnapCenter管理的 MySQL 執行個體。安裝SnapCenter Plug-in for MySQL 外掛程式後，該 Linux 主機上的 MySQL 執行個體將自動被發現並顯示在資源頁面中。

支援的備份類型

備份類型指定您要建立的備份類型。SnapCenter支援基於快照複製的 MySQL 資料庫備份類型。

基於快照副本的備份

基於快照副本的備份利用NetApp快照技術來建立 MySQL 資料庫所在磁碟區的線上只讀副本。

SnapCenter Plug-in for MySQL 如何使用一致性群組快照

您可以使用外掛程式為資源組建立一致性組快照。一致性群組是一個可以容納多個磁碟區的容器，以便您可以將它們作為一個實體進行管理。一致性組是多個磁碟區的同時快照，提供一組磁碟區的一致副本。

您也可以指定儲存控制器對快照進行一致分組的等待時間。可用的等待時間選項有*緊急*、中等*和*寬鬆。您也可以在一致的群組快照操作期間啟用或停用任意位置寫入檔案佈局 (WAFL) 同步。WAFL同步提高了一致性組快照的效能。

SnapCenter如何管理日誌備份

SnapCenter管理儲存系統和檔案系統層級的資料備份。

確定 MySQL 備份計畫的注意事項

確定備份計畫的最關鍵因素是資源的變化率。您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

備份計畫分為兩部分，如下所示：

- 備份頻率（執行備份的頻率）

備份頻率（對於某些外掛程式也稱為計畫類型）是策略配置的一部分。例如，您可以將備份頻率設定為每小時、每天、每週或每月。

- 備份計畫（確切執行備份的時間）

備份計畫是資源或資源組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份

MySQL 所需的備份作業數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

MySQL 資料庫外掛程式的備份命名約定

您可以使用預設快照命名約定，也可以使用自訂命名約定。預設備份命名約定會在快照名稱中新增時間戳，以協助您識別副本的建立時間。

快照使用以下預設命名約定：

```
resourcegroupname_hostname_timestamp
```

您應該對備份資源組進行邏輯命名，如下例所示：

```
dts1_mach1x88_03-12-2015_23.17.26
```

在這個例子中，語法元素具有以下含義：

- *dts1* 是資源組名稱。
- *mach1x88* 是主機名稱。
- *03-12-2015_23.17.26* 是日期和時間戳記。

或者，您可以在保護資源或資源群組時選擇「使用自訂名稱格式進行 Snapshot 複製」來指定 Snapshot 名稱格式。例如，`customtext_resourcegroup_policy_hostname` 或 `resourcegroup_hostname`。預設情況下，時間戳後綴會加入到快照名稱中。

MySQL 的還原與復原策略

定義 MySQL 資源的還原與復原策略

您必須在還原和復原資料庫之前定義一個策略，以便能夠成功執行還原和復原作業。



僅支援手動恢復資料庫。

步驟

1. 確定手動新增的 MySQL 資源支援的還原策略
2. 確定自動發現的 MySQL 資料庫支援的復原策略
3. 確定要執行的復原操作的類型。

手動新增的 MySQL 資源支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。手動新增的 MySQL 資源的復原策略有兩種。



您無法還原手動新增的 MySQL 資源。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

自動發現的 **MySQL** 支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。

完整資源復原是自動發現的 MySQL 資料庫支援的復原策略。這將恢復資源的所有磁碟區、qtree 和 LUN。

自動發現的 **MySQL** 的復原操作類型

適用於 MySQL 的 SnapCenter 外掛程式支援單一檔案 SnapRestore 以及自動發現的 MySQL 資料庫的連接和複製還原類型。

單檔 SnapRestore 在 **NFS** 環境中針對以下場景執行：

- 如果僅選擇*完整資源*選項
- 當選擇的備份來自 SnapMirror 或 SnapVault 二級位置，並且選擇了「完整資源」選項時

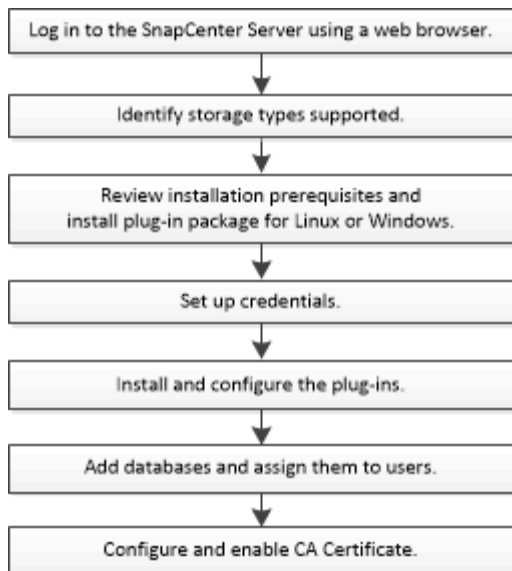
單一檔案 SnapRestore 在 **SAN** 環境中針對下列場景執行：

- 如果僅選擇*完整資源*選項
- 從 SnapMirror 或 SnapVault 二級位置選擇備份，並選擇「完整資源」選項時

準備安裝適用於 **MySQL** 的 SnapCenter 插件

SnapCenter Plug-in for MySQL 的安裝工作流程

如果您想要保護 MySQL 資料庫，則應該安裝並設定適用於 MySQL 的 SnapCenter 插件。



新增主機並安裝 **MySQL** 的**SnapCenter**插件的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。 SnapCenter Plug-in for MySQL 可在 Windows 和 Linux 環境中使用。

- 您必須在主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 對於 Windows，外掛程式建立服務應該使用「LocalSystem」 Windows 使用者執行，這是以網域管理員身分安裝 MySQL 外掛程式時的預設行為。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。適用於 Microsoft Windows 的 SnapCenter 外掛程式將預設與 Windows 主機上的 MySQL 外掛程式一起部署。
- SnapCenter 伺服器應該可以存取 MySQL 主機插件的 8145 或自訂連接埠。
- 對於 MySQL 5.7，應該在 mysql 配置（my.cnf 或 mysql-server.cnf）檔案中指定 binlog。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 在 Windows 主機上安裝適用於 MySQL 的外掛程式時，適用於 Microsoft Windows 的 SnapCenter 外掛程式會自動安裝。
- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Windows 主機上安裝 Java 11。

["下載適用於所有作業系統的 JAVA"](#)

["NetApp 互通性表工具"](#)

Linux 主機

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Linux 主機上安裝 Java 11。

"[下載適用於所有作業系統的 JAVA](#)"

"[NetApp互通性表工具](#)"

- 對於在 Linux 主機上執行的 MySQL 資料庫，安裝 MySQL 插件時，會自動安裝 UNIX 的 SnapCenter 插件。
- 您應該將 **bash** 作為插件安裝的預設 shell。

補充命令

要在 MySQL 的 SnapCenter 插件上執行補充命令，必須將其包含在 `allowed_commands.config` 檔案中。

- Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 主機上的預設位置：`/opt/ NetApp/ snapcenter/ scc/ etc/ allowed_commands.config`

若要允許插件主機上的補充命令，請在編輯器中開啟 `_allowed_commands.config` 檔案。每個命令在單獨的行上輸入，並且命令不區分大小寫。確保指定完全限定的路徑名，並且如果路徑名包含空格，則將其括在引號 (") 中。

例如：

指令：`mount` 指令：`umount` 指令：`「C:\Program Files\ NetApp\ SnapCreator commands\ sdcli.exe」` 指令：`myscript.bat`

如果不存在 `allowed_commands.config` 文件，命令或腳本執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行“`[/mnt/mount -a]`。透過在插件主機上的檔案 `%s` 中新增命令來授權。」

如果命令或腳本不在 `_allowed_commands.config` 中，則命令或腳本的執行將被阻止，並且工作流程將失敗並出現以下錯誤：

不允許執行“`[/mnt/mount -a]`。透過在插件主機上的檔案 `%s` 中新增命令來授權。」



您不應使用通配符 (*) 來允許所有命令。

為 Linux 主機的非 root 使用者配置 **sudo** 權限

SnapCenter 允許非 root 使用者安裝適用於 Linux 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 `sudo` 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 如果 `umask` 為 0027，請確保 `java` 資料夾及其內部的所有檔案的權限為 555。否則插件安裝可能會失敗。

- 對於非root用戶，請確保非root用戶的名稱和用戶所在群組的名稱相同。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 Linux 的SnapCenter插件套件的 Linux 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
LINUX_USER/.sc_netapp/Linux_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
Cmnd_Alias SCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`LINUX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt` _ 如果 SnapCenter Server 安裝在 Windows 主機上。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` _ 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 Windows 的 SnapCenter 插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統， SnapCenter升級或安裝將會失敗。"

安裝適用於 Linux 的SnapCenter插件包的主機需求

在安裝適用於 Linux 的SnapCenter插件包之前，您應該熟悉一些基本的主機系統空間和大小需求。

物品	要求
作業系統	• 紅帽企業 Linux • SUSE Linux 企業伺服器 (SLES) 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。
主機上SnapCenter插件的最小 RAM	1GB

物品	要求
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間有所不同，取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 與 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。

為 MySQL 的 SnapCenter 插件設定憑證

SnapCenter 使用憑證對 SnapCenter 操作的使用者進行身份驗證。您應該建立用於安裝 SnapCenter 插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

關於此任務

- Linux 主機

您必須設定在 Linux 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。

2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>使用者名稱 ◦ 域 <i>FQDN</i>用戶名 • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i> 請勿在密碼中使用雙引號 (") 或反引號 (')。密碼中不應同時使用小於號 (<) 和驚嘆號 (!) 符號。例如，lessthan<!10、lessthan10<!、backtick`12。
密碼	輸入用於身份驗證的密碼。
認證模式	選擇您想要使用的身份驗證模式。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面中將憑證維護指派給使用者或使用者群組。

安裝適用於 MySQL 的SnapCenter插件

新增主機並在遠端主機上安裝插件包

您必須使用SnapCenter新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以新增主機並為單一主機安裝插件包。

開始之前

- 如果SnapCenter Server 主機的作業系統是 Windows 2019，而插件主機的作業系統是 Windows 2022，則應執行下列操作：
 - 升級到 Windows Server 2019（作業系統內部版本 17763.5936）或更高版本
 - 升級到 Windows Server 2022（作業系統內部版本 20348.2402）或更高版本
- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 您應該確保訊息佇列服務正在運行。
- 管理文件包含有關管理主機的資訊。

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux i 必須在 MySQL 資料庫伺服器上安裝 MySQL 插件。
主機名稱	輸入通訊主機名稱。輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。

對於這個領域...	這樣做...
證書	選擇您建立的憑證名稱或建立新的憑證。該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標放在您提供的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的插件部分中，選擇要安裝的插件。

使用 REST API 安裝 MySQL 外掛程式時，必須傳遞版本為 3.0。例如，MySQL:3.0

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。預設連接埠號碼為 8145。如果 SnapCenter 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	MySQL 插件安裝在 MySQL 客戶端主機上，該主機可以是 Windows 系統，也可以是 Linux 系統。 - 對於適用於 Windows 的 SnapCenter 插件包，預設路徑為 C:\Program Files\ NetApp\ SnapCenter。您也可以選擇自訂路徑。 - 對於適用於 Linux 的 SnapCenter 插件包，預設路徑為 /opt/ NetApp/snapcenter。您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。
新增叢集中的所有主機	不適用。
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	不適用。

7. 點選“提交”。

如果您未選取「跳過預先檢查」複選框，則會驗證主機是否符合安裝插件的要求。系統會根據最低要求驗證

磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）和 Java 版本（適用於 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\ NetApp\ SnapCenter WebApp` 的 `web.config` 檔案以修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果您要更新 `web.config` 文件，則必須在兩個節點上更新該文件。

8. 如果主機類型為Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

- 對於 Windows 插件，安裝和升級日誌位於：`C:\Windows\ SnapCenter plugin\Install<JOBID>\_`
- 對於 Linux 插件，安裝日誌位於：`/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plugin_Install<JOBID>.log_`，升級日誌位於：`_var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-JOB_grade_f.`

完成後

如果要升級到SnapCenter 6.0 版本，則會從遠端插件伺服器中解除安裝現有的基於 PERL 的 MySQL 插件。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux** 或 **Windows** 的**SnapCenter**插件包

您可以使用 `Install-SmHostPackage PowerShell cmdlet` 同時在多個主機上安裝適用於 Linux 或 Windows 的**SnapCenter**插件套件。

開始之前

您必須以網域使用者身分登入SnapCenter，並在要安裝插件包的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，使用 `Open-SmConnection cmdlet` 建立會話，然後輸入您的憑證。
3. 使用 `Install-SmHostPackage cmdlet` 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 `cmdlet` 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝適用於 **MySQL** 的**SnapCenter**插件

您應該使用SnapCenter使用者介面 (UI) 安裝適用於 MySQL 資料庫的SnapCenter插件。如果您的環境不允許從SnapCenter UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控

制台模式或靜默模式安裝 MySQL 資料庫插件。

開始之前

- 您應該在每個必須保護 MySQL 執行個體的 Linux 主機上安裝 MySQL 資料庫外掛程式。
- 安裝 MySQL 資料庫的SnapCenter插件的 Linux 主機必須符合相關軟體、資料庫和作業系統要求。

互通性矩陣工具 (IMT) 包含受支援配置的最新資訊。

"NetApp互通性表工具"

- 適用於 MySQL 資料庫的SnapCenter插件是適用於 Linux 的SnapCenter插件包的一部分。在安裝適用於 Linux 的SnapCenter插件包之前，您應該已經在 Windows 主機上安裝了SnapCenter。

步驟

1. 將 Linux 安裝檔案 (snapcenter_linux_host_plugin.bin) 的SnapCenter插件包從 C:\ProgramData\ NetApp\ SnapCenter\Package Repository 複製到要安裝 MySQL 插件的主機。

您可以從安裝了SnapCenter伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。
3. 安裝插件：`path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

- -DPORT 指定 SMCORE HTTPS 通訊連接埠。
- -DSERVER_IP 指定SnapCenter伺服器 IP 位址。
- -DSERVER_HTTPS_PORT 指定SnapCenter伺服器 HTTPS 連接埠。
- -DUSER_INSTALL_DIR 指定要安裝 Linux 版SnapCenter插件包的目錄。
- DINSTALL_LOG_NAME 指定日誌檔案的名稱。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. 編輯 /<安裝目錄> NetApp文件，然後新增 PLUGINS_ENABLED = MySQL:3.0 參數。
5. 使用 Add-Smhost cmdlet 和所需參數將主機新增至SnapCenter伺服器。

可以透過執行 `_Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

監控 MySQL 外掛程式安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以

確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用SnapCenter部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網

域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

- 1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
- 2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
- 3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
- 4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
- 5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
- 6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：.pfx、.p12、*.p7b）。

- 7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

- 1. 在 GUI 上執行以下操作：
 - a. 雙擊該證書。
 - b. 在「證書」對話方塊中，按一下「詳細資料」標籤。
 - c. 捲動瀏覽欄位清單並按一下「指紋」。
 - d. 從框複製十六進位字元。
 - e. 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e6f83886b00d4277a32a7b”。

2. 從 PowerShell 執行以下操作：

- a. 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- b. 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- ． 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

為 Linux 主機上的 SnapCenter MySQL 插件服務設定 CA 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

插件使用位於 `/opt/NetApp/snapcenter/scc/etc` 的檔案「`keystore.jks`」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與密鑰“`KEYSTORE_PASS`”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks  
. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

對 `agent.properties` 檔案中的金鑰 `KEYSTORE_PASS` 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/NetApp/snapcenter/scc/etc`。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks  
. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。
```



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 **CA** 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導航至包含插件金鑰庫 `/opt/ NetApp/snapcenter/scc/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 `agent.properties` 檔案中密鑰 `KEYSTORE_PASS` 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

． 如果CA憑證中的別名較長，且包含空格或特殊字元（“*”，“，”，“”），請將別名修改為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

． 在 `agent.properties` 檔案中配置來自 CA 憑證的別名。

根據鍵 `SCC_CERTIFICATE_ALIAS` 更新此值。

8. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於此任務

- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter插件的 CRL 檔案的預設目錄是「`opt/ NetApp/snapcenter/scc/etc/crl`」。

步驟

1. 您可以根據鍵 `CRL_PATH` 修改和更新 `agent.properties` 檔案中的預設目錄。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

為 Windows 主機上的SnapCenter MySQL 插件服務設定 CA 證書

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

外掛程式使用位於 *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc* 的檔案 *keystore.jks* 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 CA 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與金鑰_KEystore_PASS_對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore 金鑰庫.jks
```



如果 Windows 命令提示字元無法辨識「keytool」命令，請將 keytool 命令替換為其完整路徑。

```
C:\Program Files\Java\<jdk_version>\bin\keytool.exe"-storepasswd -keystore keystore.jks
```

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks
```

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 *C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc*
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. 找到檔案 `_keystore.jks_`。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12  
-destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。

7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 `agent.properties` 檔案中密鑰 `KEYSTORE_PASS` 的值。

```
keytool -keypasswd -alias 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在 `_agent.properties_` 檔案中配置來自CA憑證的別名。

根據鍵 `SCC_CERTIFICATE_ALIAS` 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenterSnapCenter的 CRL 檔案的預設目錄是 `'C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl'`。

步驟

1. 您可以根據鍵 `CRL_PATH` 修改和更新 `agent.properties` 檔案中的預設目錄。

2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 **CA** 憑證

您應該設定 CA 憑證並在 SnapCenter 伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器和插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

做好資料保護準備

使用適用於 **MySQL** 的 SnapCenter 插件的先決條件

在使用 MySQL 的 SnapCenter 插件之前，SnapCenter 管理員必須安裝和設定 SnapCenter 伺服器並執行先決條件任務。

- 安裝並配置 SnapCenter 伺服器。
- 登入 SnapCenter 伺服器。

- 透過新增儲存系統連接和建立憑證（如果適用）來配置SnapCenter環境。
- 在您的 Linux 或 Windows 主機上安裝 Java 11。

您必須在主機的環境路徑變數中設定 Java 路徑。

- 如果您想要備份複製，請設定SnapMirror和SnapVault。

如何使用資源、資源群組和策略來保護 **MySQL**

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的 MySQL 執行個體。
- SnapCenter資源組是主機上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

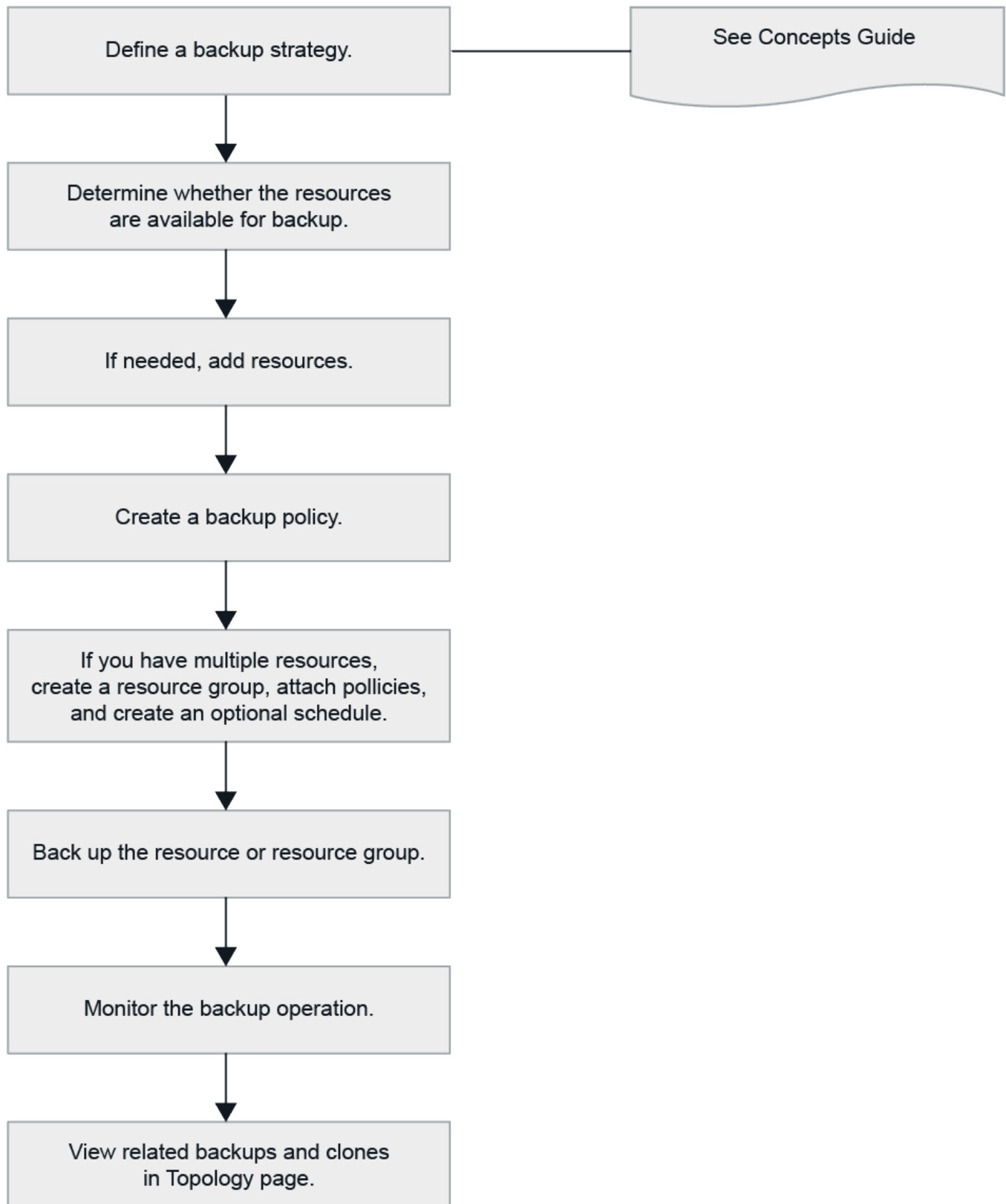
資源群組可以視為定義您想要保護的內容以及何時以日期和時間進行保護。把政策看作是定義你想如何保護它。例如，如果要備份所有資料庫，則可以建立一個包含主機中所有資料庫的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源組並附加原則時，您可以配置資源組以每天執行完整備份。

備份 **MySQL** 資源

備份 **MySQL** 資源

您可以建立資源（資料庫）或資源組的備份。備份工作流程包括規劃、識別要備份的資料庫、管理備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。 SnapCenter cmdlet 說明和 cmdlet 參考資訊包含更多有關 PowerShell cmdlet 的資訊。 <https://docs.netapp.com/us-en/snapcenter-cmdlets/index.html>["SnapCenter軟體 Cmdlet 參考指南"]。

自動發現資料庫

資源是 Linux 主機上由SnapCenter管理的 MySQL 資料庫。發現可用的 MySQL 資料庫後，您可以將資源新增至資源組以執行資料保護作業。

開始之前

- 您必須已經完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。
- SnapCenter Plug-in for MySQL 不支援自動發現駐留在 RDM/VMDK 虛擬環境中的資源。手動新增資料庫時必須提供虛擬環境的儲存資訊。

關於此任務

- 安裝外掛程式後，該Linux主機上的所有資料庫都會自動發現並顯示在資源頁面上。
- 僅資料庫是自動發現的。

自動發現的資源不能被修改或刪除。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇“MySQL 外掛程式”。
2. 在資源頁面中，從視圖清單中選擇資源類型。
3. （可選）點擊**，然後選擇主機名稱。

然後您可以點擊** 關閉篩選窗格。

4. 按一下「刷新資源」以發現主機上可用的資源。

資源與資源類型、主機名稱、關聯資源群組、備份類型、政策和總體狀態等資訊一起顯示。

- 如果資料庫位於NetApp儲存空間且未受保護，則「整體狀態」欄位中顯示「未受保護」。
- 如果資料庫位於NetApp儲存系統上並受到保護，且沒有執行備份操作，則「整體狀態」欄位中會顯示「備份未執行」。否則，狀態將根據上次備份狀態變更為備份失敗或備份成功。



如果執行個體在SnapCenter之外重新命名，則必須刷新資源。

手動將資源新增至插件主機

Windows 主機不支援自動發現。您必須手動新增 MySQL 執行個體和資料庫資源。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機和設定儲存系統連線等任務。

步驟

1. 在左側導覽窗格中，從下拉清單中選擇適用於 MySQL 的SnapCenter插件，然後按一下「資源」。
2. 在資源頁面中，按一下*新增 MySQL 資源*。
3. 在提供資源詳細資訊頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	指定資料庫名稱。
主機名稱	輸入主機名稱。
類型	選擇實例。
實例	不適用。
證書	選擇憑證或新增憑證資訊。 這是可選的。

- 在「提供儲存佔用空間」頁面中，選擇儲存類型並選擇一個或多個磁碟區、LUN 和 qtree，然後按一下「儲存」。

可選：您可以點擊 *  * 圖示用於從其他儲存系統新增更多磁碟區、LUN 和 qtree。

- 選用：在資源設定頁面中，輸入 MySQL 外掛程式的自訂鍵值對。
- 查看摘要，然後按一下「完成」。

資料庫與主機名稱、相關資源群組和策略以及整體狀態等資訊一起顯示

如果您想讓使用者存取資源，您必須將資源指派給使用者。這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

"新增使用者或群組並分配角色和資產"

新增資料庫後，您可以修改 MySQL 資料庫詳細資訊。

為 MySQL 建立備份策略

在使用 SnapCenter 備份 MySQL 資源之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。

開始之前

- 您必須已經定義了您的備份策略。

有關詳細信息，請參閱有關定義 MySQL 資料庫的資料保護策略的資訊。

- 您必須已完成安裝 SnapCenter、新增主機、設定儲存系統連線和新增資源等任務，為資料保護做好準備。
- 如果您要將快照複製到映像或保管庫，SnapCenter 管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。

此外，您還可以在策略中指定複製、腳本和應用程式設定。當您想要將該策略重新用於另一個資源群組時，這些選項可以節省時間。

關於此任務

- SnapLock

- 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
- 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能會導致保留的快照數量超過策略中指定的數量。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選“新建”。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「策略類型」頁面中，執行以下操作：
 - a. 選擇儲存類型。
 - b. 在自訂備份設定部分，提供任何必須以鍵值格式傳遞給外掛程式的特定備份設定。

您可以提供多個鍵值傳遞給插件。

6. 在「快照和複製」頁面中，執行下列步驟：
 - a. 透過選擇*按需*、每小時、每日、*每週*或*每月*來指定方案類型。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，但允許您為每個策略指派不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- a. 在「快照設定」部分中，指定在「備份類型」頁面中選擇的備份類型和計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。  最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*，並指定天、月或年。 SnapLock保留期應少於 100 年。

b. 選擇一個策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

7. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
*建立本機 Snapshot 副本後更新SnapMirror *	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 如果ONTAP中的保護關係屬於鏡像和保險庫類型，並且您僅選擇此選項，則在主伺服器上建立的快照將不會傳輸到目標伺服器，但會在目標伺服器中列出。如果從目標中選擇此快照來執行還原操作，則會顯示下列錯誤訊息：對於所選的保管/鏡像備份，輔助位置不可用。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓撲頁面中查看 MySQL 資源相關的備份和克隆"。
*建立本機 Snapshot 副本後更新SnapVault *	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。 有關SnapLock Vault 的更多信息，請參閱將快照提交到保管庫目標上的 WORM 看"在拓撲頁面中查看 MySQL 資源相關的備份和克隆"。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

8. 查看摘要，然後按一下「完成」。

建立資源組並附加策略

資源組是您必須新增要備份和保護的資源的容器。資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資

源組，以定義要執行的資料保護作業的類型。

關於此任務

- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

- 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，按一下「新資源組」。
- 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。  資源組名稱不應超過 250 個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
使用自訂名稱格式進行快照複製	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。

這有助於過濾螢幕上的信息。

- 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
- 在應用程式設定頁面中，執行以下操作：
 - 按一下“備份”箭頭以設定其他備份選項：

啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。

對於這個領域...	這樣做...
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+

- 點擊“腳本”箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- 按一下「自訂配置」箭頭並輸入使用此資源的所有資料保護操作所需的自訂鍵值對。

範圍	環境	描述
歸檔日誌啟用	(是/否)	啟用存檔日誌管理以刪除存檔日誌。
歸檔日誌保留	天數	指定存檔日誌保留的天數。 此設定必須等於或大於 NTAP_SNAPSHOT_RETENTIONS。
歸檔日誌目錄	更改訊息目錄/日誌	指定包含存檔日誌的目錄的路徑。
ARCHIVE_LOG_EXT	檔案副檔名	指定存檔日誌檔案擴充長度。 例如，如果歸檔日誌為log_backup_0_0_0.1615185519429，且file_extension值為5，則日誌的副檔名將保留5位數，即16151。

範圍	環境	描述
ARCHIVE_LOG_RECURSIVE_SEARCH	(是/否)	啟用子目錄內的存檔日誌管理。 如果存檔日誌位於子目錄下，則應使用此參數。



自訂鍵值對支援 MySQL Linux 外掛系統，不支援註冊為集中式 Windows 外掛程式的 MySQL 資料庫。

- c. 點選*Snapshot Copy Tool*箭頭選擇建立快照的工具：

如果你想...	然後...
SnapCenter使用適用於 Windows 的插件並在建立快照之前將檔案系統置於一致狀態。對於 Linux 資源，此選項不適用。	選擇*具有檔案系統一致性的SnapCenter *
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
輸入要在主機上執行的命令來建立快照副本。	選擇*其他*，然後輸入要在主機上執行的建立快照的命令。

7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊 *  *.

這些策略列在「為選定的策略配置計劃」部分中。

- b. 在配置計劃列中，按一下 *  * 您想要配置的策略。
c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。

其中，policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。必須在*設定* > *全域設定*中設定 SMTP 伺服器。

9. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並啟用 MySQL 資源的二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建建立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

- a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

- a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
- b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。
- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
- e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 為 MySQL 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 備份、還原或複製 MySQL 資料庫之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的資料 LIF IP 位址。

步驟

1. 使用 Open-SmConnection cmdlet 啟動 PowerShell Core 連線會話。

```
PS C:\> Open-SmConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例顯示如何使用 Windows 憑證建立名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

4. 將 MySQL 通訊主機新增至 SnapCenter Server。

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName FinanceAdmin -PluginCode mysql
```

5. 在主機上安裝軟體套件和適用於 MySQL 的 SnapCenter 插件。

對於 Linux：

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
```

對於 Windows：

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql -FilesystemCode scw -RunAsName FinanceAdmin
```

6. 設定 QLLIB 的路徑。

對於 Windows，MySQL 外掛程式將使用 QLLIB 資料夾的預設路徑：“C:\Program Files\IBM\SQLLIB\BIN”

如果要覆蓋預設路徑，請使用下列命令。

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode MySQL -configSettings @{“MySQL_SQLLIB_CMD” = “<custom_path>\IBM\SQLLIB\BIN”}
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份 MySQL

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

開始之前

- 您必須已經建立了備份策略。
- 如果要備份與二級儲存具有 SnapMirror 關係的資源，則指派給儲存使用者的 ONTAP 角色應包括「snapmirror all」權限。但是，如果您使用「vsadmin」角色，則不需要「snapmirror all」權限。
- 對於基於 Snapshot 副本的備份作業，請確保所有租用戶資料庫均有效且處於活動狀態。
- 對於靜默、快照和取消靜默操作的預先命令和後命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：

- Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
- Linux 主機上的預設位置：`/opt/ NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

選擇  *，然後選擇主機名稱和資源類型來過濾資源。然後您可以選擇  關閉篩選器窗格。

3. 選擇要備份的資源。
4. 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。

例如，*customtext_policy_hostname* 或 *resource_hostname*。預設情況下，時間戳記會附加到快照名稱。

5. 在應用程式設定頁面中，執行以下操作：

- 選擇“備份”箭頭來設定其他備份選項：

如果需要，請啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待「一致性組快照」操作完成	選擇「緊急」、「中」或「寬鬆」來指定等待快照操作完成的時間。緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

- 選擇「腳本」箭頭來執行靜默、快照和取消靜默操作的前置和後置命令。

您也可以在退出備份作業之前執行預命令。前言和後記在SnapCenter伺服器中運作。

- 選擇自訂配置箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
- 選擇*Snapshot Copy Tool*箭頭來選擇建立快照的工具：

如果你想...	然後...
SnapCenter建立儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
SnapCenter使用適用於 Windows 的插件將檔案系統置於一致狀態，然後建立快照	選擇*具有檔案系統一致性的SnapCenter *。
輸入建立快照的命令	選擇*其他*，然後輸入建立快照的命令。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊  來建立策略 .

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 選擇  在您想要設定計畫的政策的政策設定計畫列中。
- c. 在為政策_policy_name_新增計劃對話方塊中，配置計畫，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後選擇*完成*。

進入資源拓樸頁面。

9. 選擇*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行

保留。

b. 選擇*備份*。

11. 透過點選「監視」>「作業」來監視操作進度。

- 在MetroCluster配置中， SnapCenter可能無法在故障轉移後偵測到保護關係。

有關信息，請參閱：["MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"](#)

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java堆大小不夠大，則備份可能會失敗。

若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method` 命令啟動SnapCenter VMware 插件服務。將此指令更新為以下內容：`Java -jar -Xmx8192M -Xms4096M`

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmResources cmdlet 新增手動資源。

此範例顯示如何新增 MySQL 實例：

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL  
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint  
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"StorageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. 使用 Add-SmPolicy cmdlet 建立備份策略。

4. 使用 Add-SmResourceGroup cmdlet 保護資源或為SnapCenter新增資源組。

5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

此範例顯示如何備份資源組：

```
C:\PS> New-SmBackup -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"PluginName"="MySQL"} -Policy "MySQL_snapshotbased"
```

此範例備份受保護的資源：

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy mysql_policy2
```

6. 使用 `Get-smJobSummaryReport` cmdlet 監視作業狀態（正在執行、已完成或失敗）。

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. 使用 `Get-SmBackupReport` cmdlet 監視備份作業詳細資料（如備份 ID、備份名稱）以執行還原或複製作業。

```
PS C:\> Get-SmBackupReport -JobId 351
Output:
BackedUpObjects           : {DB1}
FailedObjects             : {}
IsScheduled               : False
HasMetadata               : False
SmBackupId               : 269
SmJobId                   : 2361
StartDateTime             : 10/4/2016 11:20:45 PM
EndDateTime              : 10/4/2016 11:21:32 PM
Duration                  : 00:00:46.2536470
CreatedDateTime           : 10/4/2016 11:21:09 PM
Status                    : Completed
ProtectionGroupName       : Verify_ASUP_Message_windows
SmProtectionGroupId       : 211
PolicyName                : test2
SmPolicyId                : 20
BackupName                : Verify_ASUP_Message_windows_scc54_10-04-
2016_23.20.46.2758
VerificationStatus        : NotVerified
VerificationStatuses      :
SmJobError                :
BackupType                : SCC_BACKUP
CatalogingStatus          : NotApplicable
CatalogingStatuses        :
ReportDataCreatedDateTime :
```

可以透過執行 `Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份資源組

資源組是主機上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要備份與二級儲存具有SnapMirror關係的資源，則指派給儲存使用者的ONTAP角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。

關於此任務

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或選擇，然後選擇標籤。然後您可以選擇關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：

- a. 如果您將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 選擇*備份*。

5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

監控 MySQL 備份作業

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監控 **MySQL** 實例上的資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

取消 **MySQL** 的備份操作

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，

則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	- 在左側導覽窗格中，按一下「監控」>「作業」。 - 選擇操作，然後按一下「取消作業」。
活動窗格	- 啟動備份作業後，按一下** 在活動窗格上查看最近的五項操作。 - 選擇操作。 - 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓樸頁面中查看 **MySQL** 備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。



顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓樸頁面。

4. 查看*摘要卡*以了解主儲存和輔助儲存上可用的備份和克隆數量的摘要。

*摘要卡*部分顯示基於 Snapshot 副本的備份和克隆的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

按需備份後，按一下「刷新」按鈕以刷新備份或複製的詳細資訊。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

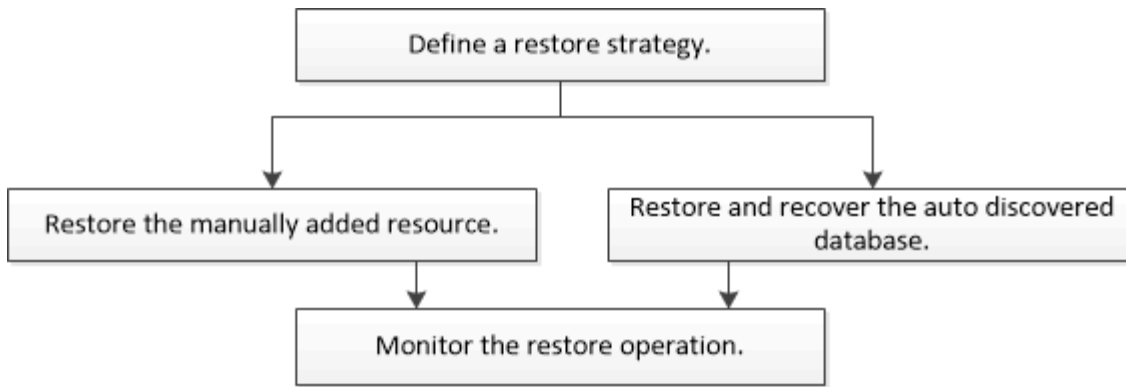
7. 如果要刪除克隆，請從表中選擇克隆，然後按一下 .
8. 如果要拆分克隆，請從表中選擇克隆，然後按一下 .

復原 MySQL

復原工作流程

還原和復原工作流程包括規劃、執行還原操作和監視操作。

以下工作流程顯示了執行還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

["SnapCenter軟體 Cmdlet 參考指南"](#)。

還原並還原手動新增的資源備份

您可以使用SnapCenter從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 對於ONTAP 9.12.1 及更早版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.

Primary Backup(s)	
search	T
Backup Name	End Date
rg1_scspr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM

6. 在「復原範圍」頁面中，選擇「完整資源」。
 - a. 如果選擇*完整資源*，則會還原 MySQL 資料庫的所有設定資料磁碟區。

如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果在相同的磁碟區或 qtree 上託管任何其他資源，則該資源也會被刪除。

您可以選擇多個 LUN。



如果選擇“全部”，則會還原磁碟區、qtree 或 LUN 上的所有檔案。

7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM	

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

還原和還原自動發現的資料庫備份

您可以使用 SnapCenter 從一個或多個備份還原和還原資料。

開始之前

- 您必須已備份資源或資源群組。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。
- 對於還原前、還原後、安裝和卸載命令，您應該檢查這些命令是否存在於插件主機上可用的命令清單中，路徑如下：
 - Windows 主機上的預設位置：`C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc\allowed_commands.config`

◦ Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。

關於此任務

- 對於自動發現的資源，SFSR 支援恢復。
- 不支援時間點和最新自動恢復。
- 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從“檢視”下拉清單中過濾資源。

資源與類型、主機、相關資源群組和政策以及狀態一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中顯示「未受保護」。這可能意味著該資源未受到保護，或該資源已被其他使用者備份。

3. 選擇資源，或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *.

Primary Backup(s)	
search	
Backup Name	End Date
rg1_scscr0191685001_01-05-2017_01.35.06.6463	1/5/2017 1:35:27 AM 

6. 在復原範圍頁面中，選擇“完整資源”，還原MySQL資料庫配置的資料卷。
7. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。

卸載命令不適用於自動發現的資源。

8. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。

自動發現的資源無法使用掛載指令。

9. 在通知頁面中，從“電子郵件首選項”下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在“設定” > “全域設定”頁面上設

定 SMTP。

10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

使用 PowerShell cmdlet 還原資源

恢復資源備份包括啟動與SnapCenter伺服器的連線會話、列出備份並檢索備份資訊以及恢復備份。

您必須準備好 PowerShell 環境才能執行 PowerShell cmdlet。

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime
BackupType		
-----	-----	-----

1	Payroll Dataset_vise-f6_08...	8/4/2015 11:02:32 AM
Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015 11:23:17 AM

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：

```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status           : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。


```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 MySQL 復原操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成

-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

克隆 MySQL 資源備份

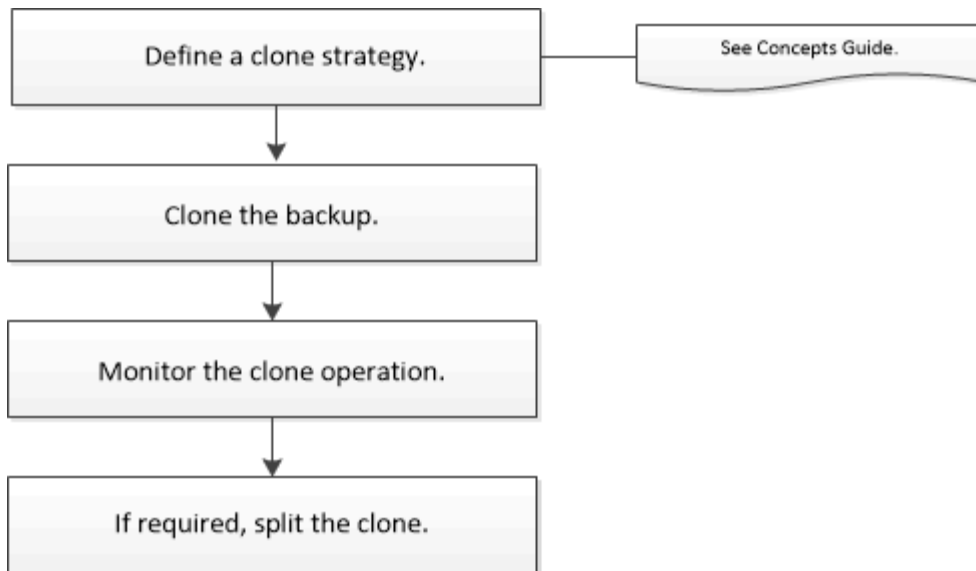
克隆工作流程

克隆工作流程包括執行克隆操作和監視操作。

關於此任務

- 您可以在來源 MySQL 伺服器上克隆。
- 您可能會因為以下原因而複製資源備份：
 - 在應用程式開發週期中測試必須使用目前資源結構和內容實現的功能
 - 用於填充資料倉儲時的資料擷取和操作工具
 - 恢復被錯誤刪除或更改的數據

以下工作流程顯示了執行複製操作必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。SnapCenter cmdlet 說明和 cmdlet 參考資訊包含有關 PowerShell cmdlet 的詳細資訊。

克隆 MySQL 備份

您可以使用 SnapCenter 克隆備份。您可以從主備份或輔助備份複製。

開始之前

- 您應該已經備份資源或資源組。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。
- 對於克隆前或克隆後命令，您應該從以下路徑檢查這些命令是否存在於插件主機上可用的命令清單中：
 - Windows 主機上的預設位置：`C:\Program Files\NetApp\SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config`
 - Linux 主機上的預設位置：`/opt/NetApp/snapcenter/scc/etc/allowed_commands.config`



如果命令清單中不存在該命令，則操作將失敗。* 對於 MySQL 5.7 版本，您應該在 MySQL.properties 檔案中設定 IGNORE_MYSQLX_PORT = true (預設為 false)。

關於此任務

- 您無法保護複製的 MySQL 實例。
- 有關 FlexClone 磁碟區拆分操作的信息，請參閱 <https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html> ["將 FlexClone 磁碟區從其父卷中拆分出來"]。
- 對於 ONTAP 9.12.1 及更早版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機、相關資源群組和策略以及狀態等資訊一起顯示。

3. 選擇資源或資源組。

如果選擇資源組，則必須選擇資源。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	選擇要建立克隆的主機。
港口	提供要啟動複製的 MySQL 實例的連接埠。
NFS 匯出 IP 位址	輸入將會匯出複製磁碟區的 IP 位址或主機名稱。

7. 在腳本頁面中，執行以下步驟：



腳本在插件主機上運行。

- a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。

- 克隆前指令：刪除現有的同名資料庫
- 克隆後指令：驗證資料庫或啟動資料庫。

- b. 輸入 mount 指令將檔案系統掛載到主機。

Linux 電腦上磁碟區或 qtree 的掛載指令：

NFS 範例：`mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

9. 查看摘要，然後按一下「完成」。
10. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-SmConnection -SMSbaseurl  
https://snapctr.demo.netapp.com:8146/
```

2. 使用 Get-SmBackup cmdlet 檢索備份以執行複製作業。

此範例顯示有兩個備份可供複製：

```
C:\PS> Get-SmBackup
```

BackupId	BackupName
BackupTime	BackupType
-----	-----
1	Payroll Dataset_vise-f6_08...
8/4/2015 11:02:32 AM	Full Backup
2	Payroll Dataset_vise-f6_08...
8/4/2015 11:23:17 AM	

3. 從現有備份啟動複製操作，並指定複製磁碟區匯出到的 NFS 匯出 IP 位址。

此範例顯示要複製的備份具有 NFSExportIPs 位址 10.32.212.14：

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName  
"scs000211748_gdl_englab_netapp_com_MySQL_mysql_d_3306_scs000211748_0  
6-26-2024_06.08.35.4307" -Resources  
@{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306"}  
-Port 3320 -CloneToHost shivarhel30.rtp.openenglab.netapp.com
```



如果沒有指定NFSExportIPs，則預設匯出至複製目標主機。

4. 使用 Get-SmCloneReport cmdlet 查看複製作業詳細信息，以驗證備份是否已成功複製。

您可以查看複製 ID、開始日期和時間、結束日期和時間等詳細資訊。

```
PS C:\> Get-SmCloneReport -JobId 186
```

```
SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName           : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName     : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

監控 MySQL 複製操作

您可以使用「作業」頁面監控SnapCenter複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。

3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“*”  *。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCORE 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 _SMCoreServiceHost.exe.config_ 檔案中的 _CloneSplitStatusCheckPollTime_ 參數的值來設定 SMCORE 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為 5 分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter 克隆或驗證失敗，聚合不存在"](#)

升級 SnapCenter 後刪除或分割 MySQL 資料庫克隆

升級到 SnapCenter 4.3 後，您將不再看到克隆。您可以從建立克隆的資源的拓樸頁面中刪除克隆或分割克隆。

關於此任務

如果您要找到隱藏複製的儲存空間，請執行以下命令：`Get-SmClone -ListStorageFootprint`

步驟

1. 使用 `remove-smbbackup cmdlet` 刪除克隆資源的備份。
2. 使用 `remove-smresourcegroup cmdlet` 刪除克隆資源的資源群組。
3. 使用 `remove-smprotectresource cmdlet` 刪除克隆資源的保護。
4. 從資源頁面中選擇父資源。

進入資源拓樸頁面。

5. 從「管理副本」檢視中，選擇來自主或輔助（鏡像或複製）儲存系統的複製。
6. 選擇克隆，然後按一下  刪除克隆或點擊  分裂克隆。
7. 按一下「確定」。

使用NetApp支援的插件保護應用程式

NetApp支援的插件

NetApp支援的插件概述

您可以將NetApp支援的插件（如 MongoDB、ORASCPM（Oracle 應用程式）、SAP ASE、SAP MaxDB 和儲存插件）用於您使用的應用程式，然後使用SnapCenter備份、還原或克隆這些應用程式。NetApp支援的插件可作為NetApp SnapCenter軟體的主機端元件，實現應用程式感知的資料保護和資源管理。

安裝NetApp支援的外掛程式後，您可以使用具有NetApp SnapMirror技術的SnapCenter在另一個磁碟區上建立備份集的鏡像副本，並使用NetApp SnapVault技術執行磁碟到磁碟的備份複製。NetApp支援的插件可以在Windows 和 Linux 環境中使用。



SnapCenterCLI 不支援NetApp支援的插件命令。

NetApp提供儲存插件，使用SnapCenter內建的插件框架對ONTAP儲存上的資料磁碟區執行資料保護作業。

您可以從新增主機頁面安裝NetApp支援的外掛程式。

["新增主機並在遠端主機上安裝插件包。"](#)



SnapCenter支援策略將涵蓋對外掛程式框架、核心引擎和相關 API 的支援。支援不包括插件原始程式碼和在插件框架上建置的相關腳本。

NetApp支援的插件可以做什麼

您可以使用NetApp支援的插件（如 MongoDB、ORASCPM、Oracle 應用程式、SAP ASE、SAP MaxDB 和儲存插件）進行資料保護作業。

- 新增資料庫、執行個體、文件或表空間等資源。
- 建立備份。
- 從備份中復原。
- 克隆備份。
- 安排備份作業。
- 監控備份、復原和克隆作業。
- 查看備份、復原和克隆作業的報告。

您可以使用NetApp支援的插件進行資料保護操作。

- 對ONTAP叢集中的儲存磁碟區進行一致性群組快照。
- 使用內建的預先腳本和後腳本框架備份自訂應用程式

您可以備份ONTAP磁碟區、LUN 或 Qtree。

- 利用現有的複製關係（ SnapVault/ SnapMirror/統一複製）並使用SnapCenter策略將主伺服器上拍攝的快照更新到ONTAP輔助伺服器上

ONTAP主伺服器和輔助伺服器可以是ONTAP FAS、 AFF、 ASA、 ONTAP Select或Cloud Volumes ONTAP。

- 還原完整的ONTAP磁碟區、LUN 或檔案。

您應該手動提供相應的文件路徑，因為瀏覽或索引功能並未內建於產品中。

不支援 Qtree 或目錄還原，但如果備份範圍是在 Qtree 層級定義的，則您只能複製和匯出 Qtree。

NetApp支援的插件功能

SnapCenter與插件應用程式以及儲存系統上的NetApp技術整合。若要使用NetApp支援的插件（如 MongoDB、ORASCPM（Oracle 應用程式）、SAP ASE、SAP MaxDB 和儲存插件），您可以使用SnapCenter圖形使用者介面。

- 統一的圖形使用者介面

SnapCenter介面提供跨插件和環境的標準化和一致性。 SnapCenter介面可讓您跨插件完成一致的備份、還原、還原和複製操作，使用集中式報告，使用一目了然的儀表板視圖，設定基於角色的存取控制 (RBAC)，並監控所有插件中的作業。

- 自動化中央管理

您可以安排備份作業、設定基於政策的備份保留以及執行復原作業。您也可以透過設定SnapCenter發送電子郵件警報來主動監控您的環境。

- 無中斷**NetApp Snapshot** 技術

SnapCenter使用NetApp Snapshot 技術和NetApp支援的插件來備份資源。快照佔用的儲存空間極小。

NetApp支援的插件還具有以下優勢：

- 支援備份、復原和複製工作流程
- RBAC 支援的安全性和集中角色委派

您也可以設定憑證，以便授權的SnapCenter使用者擁有應用程式等級的權限。

- 使用NetApp FlexClone技術建立節省空間的資源時間點副本，用於測試或資料擷取

您要建立克隆的儲存系統上需要有FlexClone許可證。

- 支援ONTAP的一致性群組 (CG) 快照功能作為建立備份的一部分。
- 能夠跨多個資源主機同時執行多個備份

在單一操作中，當單一主機中的資源共用同一磁碟區時，快照就會合併。

- 能夠使用外部命令建立快照。
- 能夠在 Windows 環境中建立檔案系統一致的快照。

NetApp支援的插件支援的儲存類型

SnapCenter支援實體機器和虛擬機器上的多種儲存類型。在安裝NetApp支援的插件之前，您必須驗證您的儲存類型的支援。

機器	儲存類型
VM 主機上的實體和 NFS 直接掛載（不支援 VMDK 和 RDM LUN。）	FC 連接的 LUN
VM 主機上的實體和 NFS 直接掛載（不支援 VMDK 和 RDM LUN。）	iSCSI 連接的 LUN
VM 主機上的實體和 NFS 直接掛載（不支援 VMDK 和 RDM LUN。）	NFS 連結卷
VMware ESXi	NFS 和 SAN 上的 vVol 資料存儲 vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。

NetApp支援的插件所需的最低ONTAP權限

所需的最低ONTAP權限會根據您用於資料保護的SnapCenter插件而有所不同。

- 全存取指令： ONTAP 9.12.1 及更高版本所需的最低權限
 - 事件產生自動支援日誌
 - 工作歷史顯示
 - 工作停止
 - lun 屬性顯示
 - lun 創建
 - lun 刪除
 - 倫幾何
 - lun igroup 新增
 - lun igroup 創建
 - lun igroup 刪除
 - lun igroup 重新命名
 - lun igroup 秀

- lun 映射新增報告節點
- lun 映射創建
- lun 映射刪除
- lun 映射刪除報告節點
- 倫圖秀
- lun 修改
- lun 移入磁碟區
- lun 離線
- 倫在線
- lun 大小調整
- lun 序號
- 倫秀
- 網路介面
- SnapMirror 策略新增規則
- snapmirror 策略修改規則
- snapmirror 策略刪除規則
- SnapMirror 策略顯示
- SnapMirror 恢復
- SnapMirror 顯示
- snapmirror 顯示歷史記錄
- SnapMirror 更新
- snapmirror 更新 Is 設定
- snapmirror 清單目標
- 版本
- 卷克隆創建
- 卷克隆顯示
- 卷克隆拆分開始
- 卷克隆拆分停止
- 卷創建
- 捲銷毀
- 卷文件克隆創建
- 磁碟區文件顯示磁碟使用情況
- 卷離線
- 在線量

- 音量修改
- 卷 qtree 創建
- 卷 qtree 刪除
- 卷 qtree 修改
- 卷 qtree 顯示
- 音量限制
- 音量顯示
- 卷快照創建
- 卷快照刪除
- 卷快照修改
- 磁碟區快照重命名
- 卷快照還原
- 卷快照恢復文件
- 卷快照顯示
- 解除安裝卷
- 虛擬伺服器 CIFS
- 虛擬伺服器 CIFS 共享創建
- 虛擬伺服器 CIFS 共享刪除
- vservers cifs 影子複製顯示
- vservers cifs 共享顯示
- 虛擬伺服器 CIFS 顯示
- 虛擬伺服器匯出策略創建
- 虛擬伺服器匯出策略刪除
- 虛擬伺服器匯出策略規則創建
- 虛擬伺服器匯出策略規則顯示
- 虛擬伺服器匯出策略顯示
- vservers iscsi 連線顯示
- 虛擬伺服器顯示
- 唯讀指令：ONTAP 8.3.0 及更高版本所需的最低權限
 - 網路介面

為NetApp支援的插件準備SnapMirror和SnapVault複製的儲存系統

您可以使用具有ONTAP SnapMirror技術的SnapCenter插件在另一個磁碟區上建立備份集的鏡像副本，並使用ONTAP SnapVault技術執行磁碟到磁碟備份複製，以滿足標準合規性和其他與治理相關的目的。在執行這些任務之前，您必須在來源磁碟區和目標磁碟區之間

配置資料保護關係並初始化該關係。

SnapCenter完成 Snapshot 作業後對SnapMirror和SnapVault執行更新。SnapMirror和SnapVault更新作為SnapCenter作業的一部分執行；不要建立單獨的ONTAP計畫。



如果您從NetApp SnapManager產品前往SnapCenter，並且對所配置的資料保護關係感到滿意，則可以跳過此部分。

資料保護關係將主儲存（來源磁碟區）上的資料複製到輔助儲存（目標磁碟區）。初始化關係時，ONTAP會將來源磁碟區上所引用的資料區塊傳送到目標磁碟區。



SnapCenter不支援SnapMirror和SnapVault磁碟區之間的連鎖關係（**Primary > Mirror > Vault**）。您應該使用扇出關係。

SnapCenter支援版本靈活的SnapMirror關係的管理。有關版本靈活的SnapMirror關係及其設定方法的詳細信息，請參閱 ["ONTAP 文件"](#)。

定義備份策略

在建立備份作業之前定義備份策略可確保您擁有成功復原或複製資源所需的備份。您的服務等級協定 (SLA)、復原時間目標 (RTO) 和復原點目標 (RPO) 在很大程度上決定了您的備份策略。

關於此任務

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RTO 是服務中斷後必須恢復業務流程的時間。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA、RTO 和 RPO 有助於資料保護策略。

步驟

1. 確定何時應該備份資源。
2. 確定您需要多少個備份作業。
3. 決定如何命名您的備份。
4. 決定是否需要一致性群組快照，並決定刪除一致性群組快照的適當選項。
5. 決定是否要使用NetApp SnapMirror技術進行複製或使用NetApp SnapVault技術進行長期保留。
6. 確定來源儲存系統和SnapMirror目標上的快照的保留期限。
7. 確定是否要在備份作業之前或之後執行任何命令，並提供前言或後記。

NetApp支援的插件的備份策略

NetApp支援的插件資源的備份計劃

確定備份計畫的最關鍵因素是資源的變化率。備份資源的頻率越高，SnapCenter用於復原的存檔日誌就越少，因此可以加快復原作業的速度。

您可能每小時備份一次使用頻繁的資源，而可能每天備份一次很少使用的資源。其他因素包括資源對您的組織的重要性、您的服務等級協定 (SLA) 和您的復原點目標 (RPO)。

SLA 定義了預期的服務等級並解決了許多與服務相關的問題，包括服務的可用性和效能。RPO 定義了必須從備份儲存中復原的檔案的年齡策略，以便在故障後復原常規作業。SLA 和 RPO 有助於資料保護策略。

備份計畫分為兩部分，如下所示：

- 備份頻率

備份頻率（執行備份的頻率），對於某些外掛程式也稱為計畫類型，是策略配置的一部分。例如，您可以將備份頻率設定為每小時、每天、每週或每月。您可以透過點擊 **設定 > 政策** 來存取 SnapCenter GUI 中的政策。

- 備份計畫

備份計畫（確切地指定執行備份的時間）是資源或資源群組配置的一部分。例如，如果您有一個資源組，該資源組的策略配置為每週備份，則可以將計畫配置為每週四晚上 10:00 進行備份。您可以透過點擊 **資源**，然後選擇對應的插件，再點擊 **查看 > 資源群組**，在 SnapCenter GUI 中存取資源群組計畫。

所需備份作業的數量

決定所需備份作業數量的因素包括資源的大小、使用的磁碟區數、資源的變化率以及服務等級協定 (SLA)。

您選擇的備份作業的數量通常取決於您放置資源的磁碟區的數量。例如，如果您將一組小資源放在一個磁碟區上，並將一組大資源放在另一個磁碟區上，則可以為小資源建立一個備份作業，為大資源建立一個備份作業。

手動新增的 NetApp 支援的插件資源支援的復原策略類型

您必須先定義一個策略，然後才能使用 SnapCenter 成功執行還原作業。對於手動新增的 NetApp 支援的插件資源，有兩種類型的復原策略。



您無法恢復手動新增的 NetApp 支援的插件資源。

完成資源恢復

- 恢復資源的所有磁碟區、qtree 和 LUN



如果資源包含磁碟區或 qtree，則在這些磁碟區或 qtree 上選擇還原的快照之後拍攝的快照將被刪除，且無法復原。此外，如果任何其他資源託管在相同的磁碟區或 qtree 上，則該資源也會被刪除。

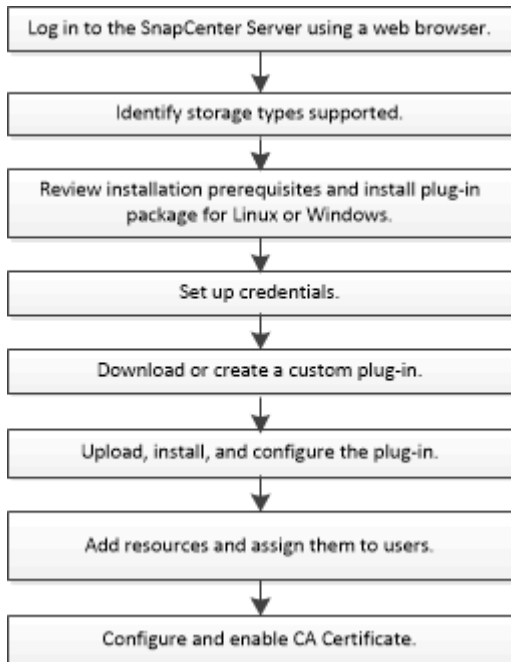
檔案級恢復

- 從磁碟區、qtree 或目錄還原文件
- 僅恢復選定的 LUN

準備安裝 NetApp 支援的插件

SnapCenter NetApp支援的插件的安裝工作流程

如果您想要保護NetApp支援的插件資源，則應該安裝並設定SnapCenter NetApp支援的插件。



新增主機並安裝 **Windows**、**Linux** 或 **AIX** 插件包的先決條件

在新增主機和安裝插件包之前，您必須完成所有要求。NetApp支援的插件在 Windows、Linux 和 AIX 環境中均受支援。



AIX 支援儲存和 Oracle 應用程式。

- 您必須在 Linux、Windows 或 AIX 主機上安裝 Java 11。



IBM Java 在 Windows 和 Linux 主機上不受支援。

- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 執行新增主機操作的客戶端主機上必須提供NetApp支援的插件，如 MongoDB、ORASCPM、Oracle 應用程式、SAP ASE、SAP MaxDB 和儲存插件。

一般的

如果您正在使用 iSCSI，則 iSCSI 服務應該正在執行。

Windows 主機

- 您必須擁有具有本機管理員權限的網域用戶，並在遠端主機上擁有本機登入權限。
- 如果您在SnapCenter中管理叢集節點，則必須擁有對叢集中所有節點具有管理權限的使用者。

- 您必須手動選擇適用於 Microsoft Windows 的 SnapCenter 外掛程式。

["下載適用於 Windows 的 JAVA"](#)

Linux 和 AIX 主機



AIX 支援儲存和 Oracle 應用程式。

- 您必須為 root 使用者或非 root 使用者啟用基於密碼的 SSH 連線。
- 您必須在 Linux 主機上安裝 Java 11。

如果您使用 Windows Server 2019 或 Windows Server 2016 作為 SnapCenter Server 主機，則必須安裝 Java 11。互通性矩陣工具 (IMT) 包含有關要求的最新資訊。

["下載適用於 Linux 的 JAVA"](#)

["下載適用於 AIX 的 JAVA"](#)

["NetApp 互通性表工具"](#)

- 您必須為非 root 使用者設定 sudo 權限以提供對多個路徑的存取權限。使用 visudo Linux 實用程式將以下行新增至 /etc/sudoers 檔案。



確保您使用的是 Sudo 版本 1.8.7 或更高版本。

```
Cmnd_Alias HPPLCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/snapcenter_linux_host_plugin.bin,  
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,  
/opt/NetApp/snapcenter/spl/bin/spl, /opt/NetApp/snapcenter/scc/bin/scc  
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/  
LINUX_USER/.sc_netapp/Linux_Prechecks.sh  
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config  
_Check.sh  
Cmnd_Alias SCCMD = sha224:checksum_value==  
/opt/NetApp/snapcenter/spl/bin/sc_command_executor  
Cmnd_Alias SCCMDEXECUTOR =checksum_value==  
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor  
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,  
CONFIGCHECKCMD, SCCMDEXECUTOR, SCCMD  
Defaults: LINUX_USER env_keep += "IATEMPDIR"  
Defaults: LINUX_USER env_keep += "JAVA_HOME"  
Defaults: LINUX_USER !visiblepw  
Defaults: LINUX_USER !requiretty
```

LINUX_USER 是您建立的非 root 使用者的名稱。

您可以從 **sc_unix_plugins_checksum.txt** 檔案中取得 *checksum_value*，該檔案位於：

- *C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt*（如果 SnapCenter Server 安裝在 Windows 主機上）。
- */opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

AIX 主機需求

在安裝適用於 AIX 的 SnapCenter 插件包之前，您應該確保主機符合要求。



AIX 支援儲存和 Oracle 應用程式。



SnapCenter Plug-in for UNIX 是 SnapCenter Plug-ins Package for AIX 的一部分，不支援並發磁碟區組。

物品	要求
作業系統	AIX 7.1 或更高版本
主機上 SnapCenter 插件的最小 RAM	4GB
主機上 SnapCenter 插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 IBM Java 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。

有關受支援版本的最新信息，請參閱 ["NetApp 互通性表工具"](#)。

為 AIX 主機的非 **root** 使用者配置 **sudo** 權限

SnapCenter 4.4 及更高版本允許非 root 用戶安裝適用於 AIX 的 SnapCenter 插件包並啟動插件進程。插件進程將以有效的非 root 使用者身分運行。您應該為非 root 使用者配置 sudo 權限以提供對多個路徑的存取。

您需要什麼

- Sudo 版本 1.8.7 或更高版本。
- 編輯 `/etc/ssh/sshd_config` 文件，設定訊息認證碼演算法：MACs hmac-sha2-256、MACs hmac-sha2-512。

更新設定檔後重新啟動sshd服務。

範例：

```
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
#Legacy changes
#KexAlgorithms diffie-hellman-group1-sha1
#Ciphers aes128-cbc
#The default requires explicit activation of protocol
Protocol 2
HostKey/etc/ssh/ssh_host_rsa_key
MACs hmac-sha2-256
```

關於此任務

您應該為非 root 使用者配置 sudo 權限以提供對以下路徑的存取權限：

- `/home/AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx`
- `/custom_location/ NetApp/snapcenter/spl/安裝/插件/卸載`
- `/custom_location/ NetApp/snapcenter/spl/bin/spl`

步驟

1. 登入要安裝適用於 AIX 的SnapCenter插件包的 AIX 主機。
2. 使用 visudo Linux 實用程式將以下行新增至 `/etc/sudoers` 檔案。

```

Cmnd_Alias HPPACMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/snapcenter_aix_host_plugin.bsx,
/opt/NetApp/snapcenter/spl/installation/plugins/uninstall,
/opt/NetApp/snapcenter/spl/bin/spl
Cmnd_Alias PRECHECKCMD = sha224:checksum_value== /home/
AIX_USER/.sc_netapp/AIX_Prechecks.sh
Cmnd_Alias CONFIGCHECKCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/plugins/scu/scucore/configurationcheck/Config
_Check.sh
Cmnd_Alias SCCMD = sha224:checksum_value==
/opt/NetApp/snapcenter/spl/bin/sc_command_executor
AIX_USER ALL=(ALL) NOPASSWD:SETENV: HPPACMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: AIX_USER !visiblepw
Defaults: AIX_USER !requiretty

```



如果您有 RAC 設置，以及其他允許的命令，您應該將以下內容添加到 `/etc/sudoers` 檔案：
`"/<crs_home>/bin/olsnodes"`

您可以從 `/etc/oracle/olr.loc` 檔中取得 `_crs_home` 的值。

`AIX_USER` 是您建立的非 root 使用者的名稱。

您可以從 `sc_unix_plugins_checksum.txt` 檔案中取得 `checksum_value`，該檔案位於：

- `C:\ProgramData\NetApp\SnapCenter\Package Repository\sc_unix_plugins_checksum.txt`（如果 SnapCenter Server 安裝在 Windows 主機上）。
- `/opt/NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt` 如果 SnapCenter Server 安裝在 Linux 主機上。



此範例僅應作為建立您自己的資料的參考。

安裝適用於 Windows 的 SnapCenter 插件包的主機需求

在安裝適用於 Windows 的 SnapCenter 插件包之前，您應該熟悉一些基本的主機系統空間需求和大小需求。

物品	要求
作業系統	微軟 Windows 有關受支援版本的最新信息，請參閱 "NetApp 互通性表工具"。

物品	要求
主機上SnapCenter插件的最小 RAM	1GB
主機上SnapCenter插件的最小安裝和日誌空間	5GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	• ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包 • PowerShell 核心 7.4.2 • Java 11 Oracle Java 與 OpenJDK Java 11 Oracle Java 和 OpenJDK 僅適用於 SAP HANA、IBM Db2、PostgreSQL、MySQL、NetApp支援的插件以及可安裝在 Windows 主機上的其他自訂應用程式。 有關受支援版本的最新信息，請參閱 "NetApp互通性表工具"。 有關 .NET 特定的故障排除信息，請參閱 "對於沒有網路連線的傳統系統，SnapCenter升級或安裝將會失敗。"

安裝適用於 **Linux** 和 **AIX** 的**SnapCenter**插件包的主機需求

在安裝適用於 Linux 或 AIX 的SnapCenter插件包之前，您應該確保主機符合要求。



AIX 支援儲存和 Oracle 應用程式。

物品	要求
作業系統	• 紅帽企業 Linux • Oracle Linux • SUSE Linux 企業伺服器 (SLES)
主機上SnapCenter插件的最小 RAM	1GB

物品	要求
主機上SnapCenter插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 或 OpenJDK 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。

有關受支援版本的最新信息，請參閱 ["NetApp互通性表工具"](#)

為NetApp支援的插件設定憑證

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。您應該建立用於安裝SnapCenter插件的憑證以及用於在資料庫或 Windows 檔案系統上執行資料保護作業的附加憑證。

開始之前

- Linux 或 AIX 主機

您必須設定在 Linux 或 AIX 主機上安裝插件的憑證。

您必須為 root 使用者或具有 sudo 權限的非 root 使用者設定憑證才能安裝和啟動插件進程。

最佳實務：雖然您可以在部署主機和安裝外掛程式後為 Linux 建立憑證，但最佳實務是在新增 SVM 之後、部署主機和安裝外掛程式之前建立憑證。

- Windows 主機

在安裝插件之前，您必須設定 Windows 憑證。

您必須設定具有管理員權限的憑證，包括遠端主機上的管理員權限。

- NetApp支援的插件應用程式

該插件使用在新增資源時選擇或建立的憑證。如果資源在資料保護作業期間不需要憑證，則可以將憑證設定為*無*。

關於此任務

如果您為單一資源群組設定憑證，且使用者名稱沒有完全管理權限，則必須至少為該使用者名稱指派資源群組和備份權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定配置憑證所需的資訊：

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
使用者名稱	輸入用於身份驗證的使用者名稱和密碼。 • 網域管理員或管理員群組的任何成員 指定要安裝SnapCenter插件的系統上的網域管理員或管理員群組的任何成員。用戶名字段的有效格式為： ◦ <i>NetBIOS</i>\使用者名稱 ◦ 域 <i>FQDN</i>\用戶名 • 本機管理員（僅適用於工作群組） 對於屬於工作群組的系統，請在要安裝SnapCenter插件的系統上指定內建的本機管理員。如果使用者帳戶具有提升的權限或主機系統上停用了使用者存取控制功能，則可以指定屬於本機管理員群組的本機使用者帳戶。使用者名字段的有效格式為：<i>UserName</i>
密碼	輸入用於身份驗證的密碼。
身份驗證類型	選擇您想要使用的身份驗證類型。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請勾選「使用 sudo 權限」複選框。  僅適用於 Linux 和 AIX 使用者。

5. 按一下“確定”。

完成憑證設定後，您可能想要在「使用者和造訪」頁面上將憑證維護指派給使用者或使用者群組。

在 Windows Server 2016 或更高版本上設定 gMSA

Windows Server 2016 或更高版本可讓您建立群組託管服務帳戶 (gMSA)，該帳戶會從託

管網域帳戶提供自動服務帳戶密碼管理。

開始之前

- 您應該擁有 Windows Server 2016 或更高版本的網域控制站。
- 您應該擁有一個 Windows Server 2016 或更高版本的主機，它是網域的成員。

步驟

1. 建立 KDS 根金鑰來為 gMSA 中的每個物件產生唯一的密碼。
2. 對於每個網域，從 Windows 網域控制站執行以下命令：Add-KDSRootKey -EffectiveImmediately
3. 建立並配置 gMSA：
 - a. 建立用戶群組帳號，格式如下：

```
domainName\accountName$  
.. 將電腦物件新增至群組。  
.. 使用您剛剛建立的使用者群組來建立 gMSA。
```

例如，

```
New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>  
-PrincipalsAllowedToRetrieveManagedPassword <group>  
-ServicePrincipalNames <SPN1,SPN2,...>  
.. 跑步 `Get-ADServiceAccount` 命令來驗證服務帳戶。
```

4. 在您的主機上設定 gMSA：
 - a. 在要使用 gMSA 帳號的主機上啟用 Windows PowerShell 的 Active Directory 模組。
- 為此，請從 PowerShell 執行以下命令：


```
PS C:\> Get-WindowsFeature AD-Domain-Services
```

Display Name	Name	Install State
-----	----	-----
[] Active Directory Domain Services	AD-Domain-Services	Available

```
PS C:\> Install-WindowsFeature AD-DOMAIN-SERVICES
```

Success	Restart Needed	Exit Code	Feature Result
-----	-----	-----	-----
True	No	Success	{Active Directory Domain Services, Active ...

WARNING: Windows automatic updating is not enabled. To ensure that your newly-installed role or feature is automatically updated, turn on Windows Update.

- 重新啟動主機。
 - 透過從 PowerShell 命令提示字元執行以下命令在主機上安裝 gMSA： `Install-AdServiceAccount <gMSA>`
 - 透過執行以下命令驗證你的 gMSA 帳戶： `Test-AdServiceAccount <gMSA>`
- 將管理權限指派給主機上配置的 gMSA。
 - 透過在 SnapCenter 伺服器中指定配置的 gMSA 帳戶來新增 Windows 主機。

SnapCenter Server 將在主機上安裝選定的插件，並且指定的 gMSA 將在插件安裝期間用作服務登入帳戶。

安裝 NetApp 支援的插件

新增主機並在遠端主機上安裝插件包

您必須使用 SnapCenter 新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。您可以新增主機並為單一主機或叢集安裝插件包。

開始之前

- 您應該是被指派具有插件安裝和卸載權限的角色的用戶，例如 SnapCenter 管理員角色。
- 您應該確保訊息佇列服務正在運行。
- 如果您使用群組託管服務帳戶 (gMSA)，則應使用管理權限設定 gMSA。

["在 Windows Server 2016 或更高版本上為自訂應用程式設定群組託管服務帳戶"](#)

- 對於 Windows 主機，您必須確保選擇適用於 Windows 的 SnapCenter 插件。

關於此任務

- 您不能將SnapCenter伺服器作為插件主機新增至另一個SnapCenter伺服器。
- 如果在叢集（WSFC）上安裝插件，則插件將安裝在叢集的所有節點上。

步驟

1. 在左側導覽窗格中，選擇*主機*。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 選擇“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇主機類型： • 視窗 • Linux • AIX  NetApp支援的插件可以在 Windows、Linux 和 AIX 環境中使用。  AIX 支援儲存和 Oracle 應用程式。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 對於 Windows 環境，只有當 IP 位址解析為 FQDN 時，不受信任的網域主機才支援該 IP 位址。 您可以輸入獨立主機的 IP 位址或 FQDN。 如果您使用SnapCenter新增主機且該主機是子網域的一部分，則必須提供 FQDN。
證書	選擇您建立的憑證名稱，或建立新的憑證。 憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標置於指定的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在*選擇要安裝的插件*部分中，選擇要安裝的插件。

您可以從清單中安裝以下插件：

- MongoDB
- ORASCPM（顯示為 Oracle 應用程式）
- SAP ASE
- SAP MaxDB
- 儲存

6. （可選）選擇“更多選項”來安裝其他外掛程式。

對於這個領域...	這樣做...
港口	保留預設連接埠號，或指定連接埠號。 預設連接埠號碼為 8145。如果 SnapCenter 伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	NetApp 支援的插件可以安裝在 Windows 系統或 Linux 系統上。 • 對於適用於 Windows 的 SnapCenter 插件包，預設路徑為 C:\Program Files\NetApp\SnapCenter。 您也可以選擇自訂路徑。 • 對於 Linux 的 SnapCenter 插件包和 AIX 的 SnapCenter 插件包，預設路徑為 /opt/NetApp/snapcenter。 您也可以選擇自訂路徑。
跳過預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。

對於這個領域...	這樣做...
使用群組託管服務帳戶 (gMSA) 執行外掛程式服務	對於 Windows 主機，如果您要使用群組託管服務帳戶 (gMSA) 來執行外掛程式服務，請選取此核取方塊。  以以下格式提供 gMSA 名稱： ：domainName\accountName\$。  gMSA 將僅用作 Windows 服務的 SnapCenter 插件的登入服務帳戶。

7. 選擇*提交*。

如果您未選取「跳過預檢」複選框，則會驗證主機是否符合安裝外掛程式的要求。系統會根據最低要求驗證磁碟空間、RAM、PowerShell 版本、.NET 版本、位置（適用於 Windows 外掛程式）和 Java 版本（適用於 Linux 外掛程式）。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。

如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\NetApp\SnapCenter WebApp` 修改預設值。如果錯誤與其他參數有關，則必須修復該問題。



在 HA 設定中，如果要更新 SnapManager.Web.UI.dll.config，則必須在兩個節點上更新該檔案並重新啟動 SnapCenter 應用程式集區。

Windows 預設路徑是 C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config

Linux 預設路徑是

/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config

8. 如果主機類型是 Linux，驗證指紋，然後選擇*確認並提交*。



即使之前已將同一台主機新增至 SnapCenter 並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

安裝特定的日誌檔案位於 `/custom\_location/snapcenter/` 紀錄。

使用 **cmdlet** 在多個遠端主機上安裝適用於 **Linux**、**Windows** 或 **AIX** 的 SnapCenter 插件包

您可以使用 Install-SmHostPackage PowerShell cmdlet 同時在多個主機上安裝適用於 Linux、Windows 或 AIX 的 SnapCenter 插件套件。

開始之前

新增主機的使用者應該具有該主機的管理權限。



AIX 支援儲存和 Oracle 應用程式。

步驟

1. 啟動 PowerShell。
2. 在 SnapCenter Server 主機上，使用 Open-SmConnection cmdlet 建立會話，然後輸入您的憑證。
3. 使用 Install-SmHostPackage cmdlet 和所需參數在多個主機上安裝插件。

可以透過執行 `_Get-Help command_name` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

當您手動安裝了插件並且不想驗證主機是否符合安裝插件的要求時，可以使用 `-skipprecheck` 選項。

4. 輸入您的遠端安裝憑證。

使用命令列介面在 **Linux** 主機上安裝 NetApp 支援的插件

您應該使用 SnapCenter 使用者介面 (UI) 安裝 NetApp 支援的插件。如果您的環境不允許從 SnapCenter UI 遠端安裝插件，您可以使用命令列介面 (CLI) 以控制台模式或靜默模式安裝 NetApp 支援的插件。

步驟

1. 將 Linux 安裝檔 (snapcenter_linux_host_plugin.bin) 的 SnapCenter 插件包從 `C:\ProgramData\NetApp\SnapCenter\Package Repository` 複製到要安裝 NetApp 支援的插件的主機。

您可以從安裝了 SnapCenter 伺服器的主機存取此路徑。

2. 從命令提示字元處，導覽至複製安裝檔案的目錄。
3. 安裝插件：`path_to_installation_bin_file/snapcenter_linux_host_plugin.bin -i silent -DPORT=port_number_for_host -DSERVER_IP=server_name_or_ip_address -DSERVER_HTTPS_PORT=port_number_for_server`

- `-DPORT` 指定 SMCORE HTTPS 通訊連接埠。
- `-DSERVER_IP` 指定 SnapCenter 伺服器 IP 位址。
- `-DSERVER_HTTPS_PORT` 指定 SnapCenter 伺服器 HTTPS 連接埠。
- `-DUSER_INSTALL_DIR` 指定要安裝 Linux 版 SnapCenter 插件包的目錄。
- `_DINSTALL_LOG_NAME` 指定日誌檔案的名稱。

```
/tmp/sc-plugin-installer/snapcenter_linux_host_plugin.bin -i silent
-DPORT=8145 -DSERVER_IP=scserver.domain.com -DSERVER_HTTPS_PORT=8146
-DUSER_INSTALL_DIR=/opt
-DINSTALL_LOG_NAME=SnapCenter_Linux_Host_Plugin_Install_2.log
-DCHOSEN_FEATURE_LIST=CUSTOM
```

4. 使用 Add-Smhost cmdlet 和所需參數將主機新增至 SnapCenter 伺服器。

可以透過執行 `_Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

5. 登入SnapCenter並從 UI 或使用 PowerShell cmdlet 上傳NetApp支援的插件。

您可以從 UI 上傳NetApp支援的插件，參考["新增主機並在遠端主機上安裝插件包"](#)部分。

SnapCenter cmdlet 說明和 cmdlet 參考資訊包含更多有關 PowerShell cmdlet 的資訊。

["SnapCenter軟體 Cmdlet 參考指南"](#)。

監控NetApp支援的插件的安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。
 - b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

設定 CA 憑證

產生CA憑證CSR文件

您可以產生憑證簽署要求 (CSR) 並匯入可使用產生的 CSR 從憑證授權單位 (CA) 取得的憑證。該憑證將有一個與之關聯的私鑰。

CSR 是一段編碼文本，提供給授權憑證供應商以取得簽署的 CA 憑證。



CA 憑證 RSA 金鑰長度必須至少為 3072 位元。

有關生成 CSR 的信息，請參閱 ["如何產生CA憑證CSR文件"](#)。



如果您擁有您的網域 (*.domain.company.com) 或您的系統 (machine1.domain.company.com) 的 CA 證書，您可以跳過生成 CA 證書 CSR 檔案。您可以使用 SnapCenter 部署現有的 CA 憑證。

對於叢集配置，CA 憑證中應提及叢集名稱（虛擬叢集 FQDN）和對應的主機名稱。在取得憑證之前，可以透過填寫主題備用名稱 (SAN) 欄位來更新憑證。對於通配符憑證 (*.domain.company.com)，該憑證將隱式包含網域的所有主機名稱。

匯入 CA 憑證

您必須使用 Microsoft 管理主控台 (MMC) 將 CA 憑證匯入 SnapCenter 伺服器 and Windows 主機外掛程式。

步驟

1. 前往 Microsoft 管理主控台 (MMC)，然後按一下 檔案 > 新增/移除管理單元。
2. 在“新增或刪除管理單元”視窗中，選擇“證書”，然後按一下“新增”。
3. 在憑證管理單元視窗中，選擇「電腦帳戶」選項，然後按一下「完成」。
4. 按一下 控制台根 > 憑證 - 本機電腦 > 受信任的根憑證授權單位 > 憑證。
5. 右鍵單擊資料夾“受信任的根憑證授權單位”，然後選擇*所有任務*>*匯入*以啟動匯入精靈。
6. 完成嚮導，如下圖所示：

在此精靈視窗中...	執行以下操作...
導入私鑰	選擇選項*是*，匯入私鑰，然後按一下*下一步*。
導入文件格式	不做任何更改；按一下“下一步”。
安全	指定匯出憑證要使用的新密碼，然後按一下「下一步」。
完成憑證匯入精靈	查看摘要，然後按一下「完成」開始匯入。



匯入憑證時需攜帶私鑰（支援格式為：**.pfx**、**.p12**、***.p7b**）。

7. 對「個人」資料夾重複步驟 5。

取得 CA 憑證指紋

憑證指紋是用於識別憑證的十六進位字串。指紋是使用指紋演算法根據憑證內容計算出來的。

步驟

1. 在 GUI 上執行以下操作：

- 雙擊該證書。
- 在「證書」對話方塊中，按一下「詳細資料」標籤。
- 捲動瀏覽欄位清單並按一下「指紋」。
- 從框複製十六進位字元。
- 刪除十六進制數之間的空格。

例如，如果指紋為：“a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b”，刪除空格後，將為：“a909502dd82ae41433e68383883”。

2. 從 PowerShell 執行以下操作：

- 執行以下命令列出已安裝憑證的指紋並透過主題名稱識別最近安裝的憑證。

```
Get-ChildItem -Path 憑證:\LocalMachine\My
```

- 複製指紋。

使用 Windows 主機插件服務設定 CA 憑證

您應該使用 Windows 主機外掛程式服務來設定 CA 憑證以啟動已安裝的數位憑證。

在 SnapCenter 伺服器 and 所有已部署 CA 憑證的插件主機上執行下列步驟。

步驟

1. 透過執行以下命令刪除與 SMCore 預設連接埠 8145 的現有憑證綁定：

```
> netsh http delete sslcert ipport=0.0.0.0: _<SMCore Port>
```

例如：

```
> netsh http delete sslcert ipport=0.0.0.0:8145
```

- 透過執行下列命令將新安裝的憑證與 Windows 主機插件服務綁定：

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

例如：


```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"  
> $guid = [guid]::NewGuid().ToString("B")  
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert  
appid="$guid"
```

為 **Linux** 主機上**NetApp**支援的插件服務配置 **CA** 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用SnapCenter插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

插件使用位於 `/opt/ NetApp/snapcenter/scc/etc` 的檔案「keystore.jks」作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與密鑰“KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks  
. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

對 `agent.properties` 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導航至包含插件金鑰庫的資料夾：`/opt/ NetApp/snapcenter/scc/etc`。
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file  
/root/USERTrustRSA_Root.cer -keystore keystore.jks
```

． 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 **CA** 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導航至包含插件金鑰庫 /opt/ NetApp/snapcenter/scc/etc 的資料夾。
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore  
keystore.jks
```

． 如果CA憑證中的別名較長，且包含空格或特殊字元（“*” ， “ ” ， “ ” ） ，請將別名修改為簡單名稱：

```
keytool -changealias -alias "long_alias_name" -destalias "simple_alias"  
-keystore keystore.jks
```

． 在 agent.properties 檔案中配置來自 CA 憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

8. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為插件配置憑證撤銷清單 (CRL)

關於此任務

- SnapCenter 插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenter 插件的 CRL 檔案的預設目錄是「opt/ NetApp/snapcenter/scc/etc/crl」。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 agent.properties 檔案中的預設目錄。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

在 **Windows** 主機上為 **NetApp** 支援的插件服務配置 **CA** 憑證

您應該管理插件金鑰庫及其證書的密碼，配置 CA 證書，將根證書或中間證書配置到插件信任庫，並使用 SnapCenter 插件服務將 CA 簽名金鑰對配置到插件信任庫以啟動已安裝的數位證書。

外掛程式使用位於 *C:\Program Files\ NetApp\ SnapCenter\ Snapcenter Plug-in Creator\etc* 的檔案 *keystore.jks* 作為其信任庫和金鑰庫。

管理插件金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從外掛程式代理屬性檔案中檢索外掛程式密鑰庫預設密碼。

它是與金鑰_KEystore_PASS_對應的值。

2. 更改密鑰庫密碼：

`keytool -storepasswd -keystore 金鑰庫.jks`



如果 Windows 命令提示字元無法辨識「keytool」命令，請將 keytool 命令替換為其完整路徑。

`C:\Program Files\Java\<jdk_version>\bin\keytool.exe -storepasswd -keystore keystore.jks`

3. 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

`keytool -keypasswd -alias 「別名在憑證中」 -keystore keystore.jks`

對 *agent.properties* 檔案中的金鑰 KEYSTORE_PASS 進行相同的更新。

4. 修改密碼後重啟服務。



插件金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

設定根憑證或中間憑證以插入信任庫

您應該配置沒有私鑰的根憑證或中間憑證來插入信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks
```

5. 設定根憑證或中間憑證以插入信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

配置 CA 簽署金鑰對以插入信任庫

您應該將 CA 簽署的金鑰對配置到插件信任庫。

步驟

1. 導覽至包含外掛程式金鑰庫的資料夾 `C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc`
2. 找到檔案“_keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

4. 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

6. 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。
7. 將新增的CA憑證私鑰密碼變更為keystore密碼。

預設插件密鑰庫密碼是 agent.properties 檔案中密鑰 KEYSTORE_PASS 的值。

```
keytool -keypasswd -alias 「別名在CA憑證中的名稱」 -keystore keystore.jks
```

8. 在_agent.properties_ 檔案中配置來自CA憑證的別名。

根據鍵 SCC_CERTIFICATE_ALIAS 更新此值。

9. 配置 CA 簽署金鑰對以插入信任庫後重新啟動服務。

為SnapCenter插件配置憑證撤銷清單 (CRL)

關於此任務

- 若要下載相關 CA 憑證的最新 CRL 文件，請參閱 ["如何更新SnapCenter CA 憑證中的憑證撤銷清單文件"](#)。
- SnapCenter插件將在預先配置的目錄中搜尋 CRL 檔案。
- SnapCenterSnapCenter的 CRL 檔案的預設目錄是 'C:\Program Files\ NetApp \ SnapCenter \Snapcenter Plug-in Creator\ etc\crl'。

步驟

1. 您可以根據鍵 CRL_PATH 修改和更新 *agent.properties* 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在SnapCenter伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示SnapCenter伺服器和插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

做好資料保護準備

使用NetApp支援的插件的先決條件

在使用SnapCenter NetApp支援的插件之前，SnapCenter管理員必須安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。
- 登入SnapCenter伺服器。
- 透過新增儲存系統連接和建立憑證（如果適用）來配置SnapCenter環境。
- 新增主機，並安裝和上傳插件。
- 如果適用，請在外掛程式主機上安裝 Java 11。
- 如果您有多個資料路徑 (LIF) 或 dNFS 配置，則可以使用資料庫主機上的SnapCenter CLI 執行下列操作：
 - 預設情況下，資料庫主機的所有 IP 位址都會新增至複製磁碟區的儲存虛擬機器 (SVM) 中的 NFS 儲存匯出原則。如果您想要特定的 IP 位址或限制為 IP 位址的子集，請執行 `Set-PreferredHostIPsInStorageExportPolicy` CLI。
 - 如果 SVM 中有多個資料路徑 (LIF)，SnapCenter會選擇適當的資料路徑 (LIF) 來掛載 NFS 複製磁碟區。但是，如果要指定特定的資料路徑 (LIF)，則必須執行 `Set-SvmPreferredDataPath` CLI。可以透過執行 `_Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體命令參考指南](#)"。
- 如果您想要備份複製，請設定SnapMirror和SnapVault。
- 確保連接埠 9090 未被主機上的任何其他應用程式使用。

除了SnapCenter所需的其他連接埠外，還必須保留連接埠 9090 以供NetApp支援的插件使用。

如何使用資源、資源群組和策略來保護NetApp支援的插件資源

在使用SnapCenter之前，了解與要執行的備份、複製和還原作業相關的基本概念會很有幫助。您與資源、資源群組和策略進行互動以執行不同的操作。

- 資源通常是使用SnapCenter備份或複製的資料庫、Windows 檔案系統或虛擬機器。
- SnapCenter資源群組是主機或叢集上的資源集合。

當您對資源組執行操作時，您將根據為資源組指定的計劃對資源組中定義的資源執行該操作。

您可以按需備份單一資源或資源群組。您也可以對單一資源和資源群組執行排程備份。

- 這些策略指定了備份頻率、副本保留、複製、腳本以及資料保護作業的其他特徵。

建立資源組時，您可以為該組選擇一個或多個策略。您也可以對單一資源執行按需備份時選擇策略。

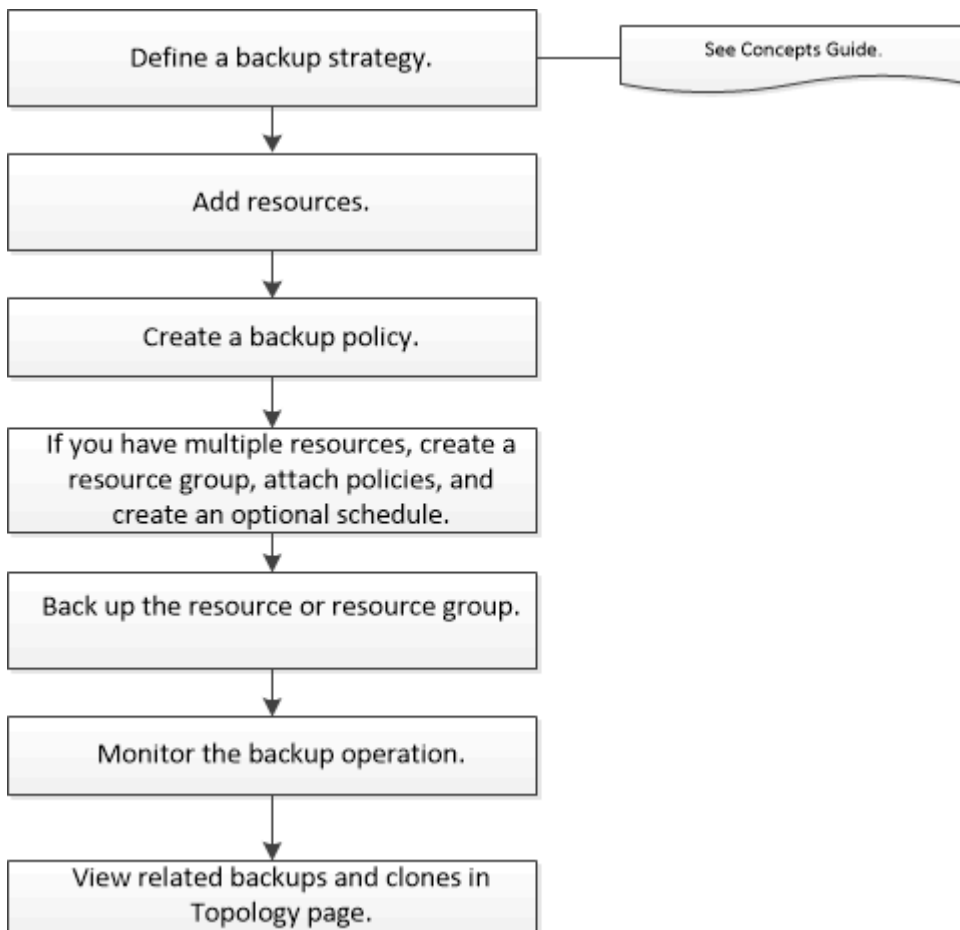
可以將資源群組視為定義您想要保護的內容以及您想要在日期和時間方面保護的內容。把政策看作是定義你想如何保護它。例如，如果要備份主機的所有資料庫或所有檔案系統，則可以建立包含主機中的所有資料庫或所有檔案系統的資源群組。然後，您可以將兩個策略附加到資源群組：每日策略和每小時策略。建立資源群組並附加策略時，您可以設定資源群組以每天執行基於檔案的備份，並配置另一個每小時執行基於快照的備份的計畫。

備份NetApp支援的插件資源

備份NetApp支援的插件資源

備份工作流程包括規劃、確定備份資源、管理備份策略、建立資源群組和附加策略、建立備份以及監控作業。

以下工作流程顯示了執行備份作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 ["SnapCenter 軟體 Cmdlet 參考指南"](#)

為NetApp支援的插件新增資源

您必須新增想要備份或複製的資源。根據您的環境，資源可能是您想要備份或複製的資料庫執行個體或集合。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機、建立儲存系統連線和新增憑證等任務。
- 您必須已將插件上傳到SnapCenter伺服器。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，選擇*新增資源*。
3. 在提供資源詳細資訊頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源的名稱。
主機名稱	選擇主機。
類型	選擇類型。類型是用戶根據插件描述文件定義的。例如資料庫和實例。 如果所選類型有父級，請輸入父級的詳細資料。例如，如果類型是資料庫且父級是實例，請輸入實例的詳細資訊。
憑證名稱	選擇憑證或建立新憑證。
安裝路徑	輸入資源掛載的掛載路徑。這僅適用於 Windows 主機。

4. 在「提供儲存佔用空間」頁面中，選擇儲存系統並選擇一個或多個磁碟區、LUN 和 qtree，然後選擇*儲存*。

可選：選擇  圖示從其他儲存系統新增更多磁碟區、LUN 和 qtree。



NetApp支援的外掛程式不支援資源的自動發現。實體和虛擬環境的儲存細節也無法自動發現。建立資源時必須提供實體和虛擬環境的儲存資訊。

5. 在資源設定頁面中，為資源提供自訂鍵值對。



確保自訂鍵名稱是大寫的。

Resource settings

Name	Value
HOST	localhost
PORT	3306
MASTER_SLAVE	NO

有關個別插件參數，請參閱["配置資源的參數"](#)

6. 查看摘要，然後選擇*完成*。

結果

資源與類型、主機或叢集名稱、相關資源群組和策略以及總體狀態等資訊一起顯示。



如果資料庫在SnapCenter之外重新命名，則必須刷新資源。

完成後

如果您想向其他使用者提供對資產的存取權限， SnapCenter管理員必須將資產指派給這些使用者。這使用戶能夠對分配給他們的資產執行他們有權限執行的操作。

新增資源後，您可以修改資源詳情。如果NetApp支援的外掛程式資源具有與其關聯的備份，則無法修改下列欄位：資源名稱、資源類型和主機名稱。

配置資源的參數

如果您手動新增插件，則可以使用下列參數在資源設定頁面中配置資源。

MongoDB 插件

資源設定：

- MONGODB_APP_SERVER=（對於資源類型為分片群集）或 MONGODB_REPLICASET_SERVER=（對於資源類型為副本集）
- OPLOG_PATH=（如果從 MongoDB.properties 檔案提供，則為可選參數）
- MONGODB_AUTHENTICATION_TYPE=（LDAP 驗證為 PLAIN，其他驗證為 None）

您必須提供 MongoDB.properties 檔案中需要提供的以下參數：

- 禁用啟動停止服務=
 - 如果啟動/停止服務由插件執行，則為 N。
 - 如果啟動/停止服務由使用者執行，則為 Y。
 - 可選參數的預設值設定為 N。
- OPLOG_PATH_=（如果它已經在 SnapCenter 中作為自訂鍵值對提供，則為可選參數）。

MaxDB 插件

資源設定：

- XUSER_ENABLE (Y|N) 啟用或停用 MaxDB 的 xuser 使用，這樣資料庫使用者就不需要密碼了。
- HANDLE_LOGWRITER (Y|N) 執行暫停日誌寫入器 (N) 或復原日誌寫入器 (Y) 操作。
- DBMCLICMD (path_to_dbmcli_cmd) 指定 MaxDB dbmcli 指令的路徑。如果未設置，則使用搜尋路徑上的 dbmcli。



對於 Windows 環境，路徑必須在雙引號內 (“...”)。

- SQLCLICMD (path_to_sqlcli_cmd) 指定 MaxDB sqlcli 指令的路徑。如果未設定路徑，則在搜尋路徑上使用 sqlcli。
- MAXDB_UPDATE_HIST_LOG (Y|N) 指示 MaxDB 備份程式是否應更新 MaxDB 歷史日誌。
- MAXDB_CHECK_SNAPSHOT_DIR：例如，SID1：directory[,directory...]; [SID2：directoary[,directory...]] 檢查 Snap Creator Snapshot 複製操作是否成功並確保建立了快照。

這僅適用於 NFS。該目錄必須指向包含 .snapshot 目錄的位置。多個目錄可以包含在以逗號分隔的清單中。

在 MaxDB 7.8 及更高版本中，資料庫備份請求在備份歷史記錄中標記為「失敗」。

- MAXDB_BACKUP_TEMPLATES：為每個資料庫指定一個備份範本。

該模板必須存在，並且是外部類型的備份模板。若要為 MaxDB 7.8 及更高版本啟用快照集成，您必須具有 MaxDB 後台伺服器功能並且已配置 EXTERNAL 類型的 MaxDB 備份模板。

- MAXDB_BG_SERVER_PREFIX：指定後台伺服器名稱的前綴。

如果設定了 MAXDB_BACKUP_TEMPLATES 參數，則也必須設定 MAXDB_BG_SERVER_PREFIX 參數。如果不設定前綴，則使用預設值 na_bg_。

SAP ASE 插件

資源設定：

- SYBASE_SERVER (data_server_name) 指定 Sybase 資料庫伺服器名稱 (isql 指令上的 -S 選項)。例如，p_test。
- 如果使用「ALL」構造，SYBASE_DATABASES_EXCLUDE (db_name) 允許排除資料庫。

您可以使用分號分隔的清單指定多個資料庫。例如：pubs2;test_db1。

- SYBASE_USER：user_name 指定可以執行 isql 指令的作業系統使用者。

UNIX 必需。如果執行 Snap Creator Agent 啟動和停止命令的使用者（通常是 root 使用者）與執行 isql 命令的使用者不同，則需要此參數。

- SYBASE_TRAN_DUMP db_name:directory_path 讓您能夠在建立快照後執行 Sybase 交易轉儲。例如，pubs2:/sybasedumps/pubs2

您必須指定每個需要事務轉儲的資料庫。

- SYBASE_TRAN_DUMP_COMPRESS (Y|N) 啟用或停用本機 Sybase 交易轉儲壓縮。
- SYBASE_ISQL_CMD (例如，/opt/sybase/OCS-15_0/bin/isql) 定義 isql 指令的路徑。
- SYBASE_EXCLUDE_TEMPDB (Y|N) 可讓您自動排除使用者建立的臨時資料庫。

Oracle 應用程式外掛程式 (ORASCPM)

資源設定：

- SQLPLUS_CMD 指定 SQLplus 的路徑。
- ORACLE_DATABASES 列出了要備份的 Oracle 資料庫和對應的使用者（資料庫：使用者）。
- CNTL_FILE_BACKUP_DIR 指定控制檔備份的目錄。
- ORA_TEMP 指定暫存檔案的目錄。
- ORACLE_HOME 指定 Oracle 軟體的安裝目錄。
- ARCHIVE_LOG_ONLY 指定是否備份存檔日誌。
- ORACLE_BACKUPMODE 指定是否執行線上或離線備份。
- ORACLE_EXPORT_PARAMETERS 指定在執行 `/bin/su <user running sqlplus> -c sqlplus /nolog <cmd>` 時是否應重新匯出上面定義的環境變數。通常情況下，當執行 sqlplus 的使用者尚未設定使用 `connect / as sysdba` 連接到資料庫所需的所有環境變數時，就會發生這種情況。

為NetApp支援的插件資源建立策略

在使用SnapCenter備份NetApp支援的特定外掛程式資源之前，您必須為要備份的資源或資源群組建立備份原則。

開始之前

- 您應該已經定義了您的備份策略。

有關詳細信息，請參閱有關為NetApp支援的插件定義資料保護策略的資訊。

- 您應該已經做好資料保護的準備。

資料保護的準備工作包括安裝SnapCenter、新增主機、建立儲存系統連線和新增資源等任務。

- 應為您指派儲存虛擬機器 (SVM) 以執行鏡像或保管庫操作。

如果您要將快照複製到映像或保管庫，SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的SVM。

- 您應該手動新增想要保護的資源。

關於此任務

- 備份策略是一組規則，用於控制如何管理、排程和保留備份。此外，您還可以指定複製、腳本和應用程式設定。
- 當您想要將策略重新用於另一個資源群組時，在策略中指定選項可以節省時間。
- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。
 - 指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。
 - 對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。



主SnapLock設定在SnapCenter備份策略中管理，輔助SnapLock設定由ONTAP管理。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選「新建」。
4. 在名稱頁面中，輸入策略名稱和詳細資訊。
5. 在「策略類型」頁面中，執行以下操作：
 - a. 選擇儲存類型。
 - b. 在自訂備份設定部分，提供任何必須以鍵值格式傳遞給外掛程式的特定備份設定。

您可以提供多個鍵值傳遞給插件。

6. 在「快照和複製」頁面中，執行下列步驟：
 - a. 透過選擇*按需*、每小時、每日、*每週*或*每月*來指定方案類型。



您可以在建立資源組時指定備份作業的計畫（開始日期、結束日期和頻率）。這使您能夠建立共享相同策略和備份頻率的資源群組，但允許您為每個策略指派不同的備份計劃。



如果您已安排在凌晨 2:00，則夏令時 (DST) 期間不會觸發該計劃。

- a. 在「快照設定」部分中，指定在「備份類型」頁面中選擇的備份類型和計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。  最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*，並指定天、月或年。 SnapLock保留期應少於 100 年。

- b. 選擇一個策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

7. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
*建立本機 Snapshot 副本後更新SnapMirror *	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 如果ONTAP中的保護關係屬於鏡像和保險庫類型，並且您僅選擇此選項，則在主伺服器上建立的快照將不會傳輸到目標伺服器，但會在目標伺服器中列出。如果從目標中選擇此快照來執行還原操作，則會顯示下列錯誤訊息：對於所選的保管/鏡像備份，輔助位置不可用。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。 點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 看"在拓撲頁面中查看NetApp支援的插件資源相關的備份和克隆"。
*建立本機 Snapshot 副本後更新SnapVault *	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。 在二次複製期間， SnapLock到期時間會載入主SnapLock到期時間。點選拓撲頁面中的「刷新」按鈕可重新整理從ONTAP擷取的輔助和主SnapLock到期時間。 當僅在ONTAP的輔助節點（稱為SnapLock Vault）上配置SnapLock時，點擊拓撲頁面中的 刷新 按鈕將刷新從ONTAP檢索到的輔助節點上的鎖定期。 有關SnapLock Vault 的更多信息，請參閱將快照提交到保險庫目標上的 WORM。 看"在拓撲頁面中查看NetApp支援的插件資源相關的備份和克隆"。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。



您應該在ONTAP中為二級儲存配置SnapMirror保留策略，以避免達到二級儲存上快照的最大限制。

8. 查看摘要，然後按一下「完成」。

建立資源組並附加策略

資源組是您必須新增要備份和保護的資源的容器。它使您能夠同時備份與給定應用程式相關的所有資料。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業

的類型。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，選擇新資源組。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。 注意：資源組名稱不得超過250個字元。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。 例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。 例如， <i>customtext_resource</i> <i>group_policy_hostname</i> 或 <i>resource</i> <i>group_hostname</i> 。預設情況下，時間戳記會附加到快照名稱。

4. 選用：在資源頁面中，從 主機 下拉清單中選擇主機名，從 資源類型 下拉清單中選擇資源類型。

這有助於過濾螢幕上的信息。

5. 從「可用資源」部分中選擇資源，然後選擇右箭頭將其移至「選定資源」部分。
6. 可選：在「應用程式設定」頁面中，執行以下操作：

- a. 選擇備份箭頭來設定其他備份選項：

啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中等」或「輕鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+

- a. 選擇腳本箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- b. 選擇自訂配置箭頭並輸入使用此資源的所有資料保護操作所需的自訂鍵值對。

範圍	環境	描述
歸檔日誌啟用	(是/否)	啟用存檔日誌管理以刪除存檔日誌。
歸檔日誌保留	天數	指定存檔日誌保留的天數。 此設定必須等於或大於 NTAP_SNAPSHOT_RETENTIONS。
歸檔日誌目錄	更改訊息目錄/日誌	指定包含存檔日誌的目錄的路徑。
ARCHIVE_LOG_EXT	檔案副檔名	指定存檔日誌檔案擴充長度。 例如，如果歸檔日誌為log_backup_0_0_0_0.1615185519429，且file_extension值為5，則日誌的副檔名將保留5位數，即16151。
ARCHIVE_LOG_RECURSIVE_SEARCH	(是/否)	啟用子目錄內的存檔日誌管理。 如果存檔日誌位於子目錄下，則應使用此參數。

c. 選擇*Snapshot Copy Tool*箭頭來選擇建立快照的工具：

如果你想...	然後...
SnapCenter使用適用於 Windows 的插件並在建立快照之前將檔案系統置於一致狀態。對於 Linux 資源，此選項不適用。	選擇*具有檔案系統一致性的SnapCenter *。 此選項不適用於 SAP HANA 資料庫的SnapCenter 插件。
SnapCenter建立儲存等級 Snapshot	選擇“* 不具有檔案系統一致性的SnapCenter *”。
輸入要在主機上執行的命令來建立快照。	選擇*其他*，然後輸入要在主機上執行的指令來建立Snapshot。

7. 在「策略」頁面中，執行以下步驟：

a. 從下拉清單中選擇一個或多個策略。



您也可以透過選擇 * 來建立策略  *.

這些策略列在「為選定的策略配置計劃」部分中。

b. 在“配置計劃”欄中，選擇“*”  * 您想要配置的策略。

c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃並選擇確定。

其中 policy_name 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 從「通知」頁面上的「電子郵件首選項」下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。必須在*設定* > *全域設定*中設定SMTP 伺服器。

9. 查看摘要，然後選擇*完成*。

建立資源組並為ASA r2 系統上的資源啟用二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。

- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：

a. 選擇複製策略的類型。



不支援同步複製策略。

b. 指定要使用的一致性組後綴。

c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：

a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。

b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。

c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。

e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

使用 PowerShell cmdlet 建立儲存系統連線和憑證

在使用 PowerShell cmdlet 執行資料保護作業之前，必須建立儲存虛擬機器 (SVM) 連線和憑證。

開始之前

- 您應該已經準備好 PowerShell 環境來執行 PowerShell cmdlet。
- 您應該擁有基礎設施管理員角色所需的權限來建立儲存連線。
- 您應該確保插件安裝沒有正在進行中。

新增儲存系統連線時，不得進行主機外掛程式安裝，因為主機快取可能不會更新，且資料庫狀態可能會在 SnapCenter GUI 中顯示為「不可用於備份」或「不在 NetApp 儲存上」。

- 儲存系統名稱應該是唯一的。

SnapCenter 不支援不同叢集上具有相同名稱的多個儲存系統。SnapCenter 支援的每個儲存系統都應具有唯一的名稱和唯一的管理 LIF IP 位址。

步驟

1. 使用 Open-SmConnection cmdlet 啟動 PowerShell Core 連線會話。

此範例開啟一個 PowerShell 會話：

```
PS C:\> Open-SmConnection
```

2. 使用 Add-SmStorageConnection cmdlet 建立與儲存系統的新連線。

此範例建立一個新的儲存系統連線：

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https  
-Timeout 60
```

3. 使用 Add-SmCredential cmdlet 建立新憑證。

此範例使用 Windows 憑證建立一個名為 FinanceAdmin 的新憑證：

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows  
-Credential sddev\administrator
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

備份單一NetApp支援的插件資源

如果單一NetApp支援的外掛資源不屬於任何資源組，您可以從「資源」頁面備份該資源。您可以按需備份資源，或者，如果資源附加了策略並配置了計劃，則備份將根據計劃自動進行。

開始之前

- 您必須已經建立了備份策略。
- 如果要備份與二級儲存具有SnapMirror關係的資源，則指派給儲存使用者的ONTAP角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

點選，然後選擇主機名稱和資源類型來過濾資源。然後您可以點選關閉篩選器窗格。

3. 按一下要備份的資源。
4. 在資源頁面中，如果要使用自訂名稱，請選取*使用自訂名稱格式作為 Snapshot 副本*複選框，然後輸入自訂名稱格式作為 Snapshot 名稱。

例如，`customtext_policy_hostname` 或 `resource_hostname`。預設情況下，時間戳記會附加到快照名稱。

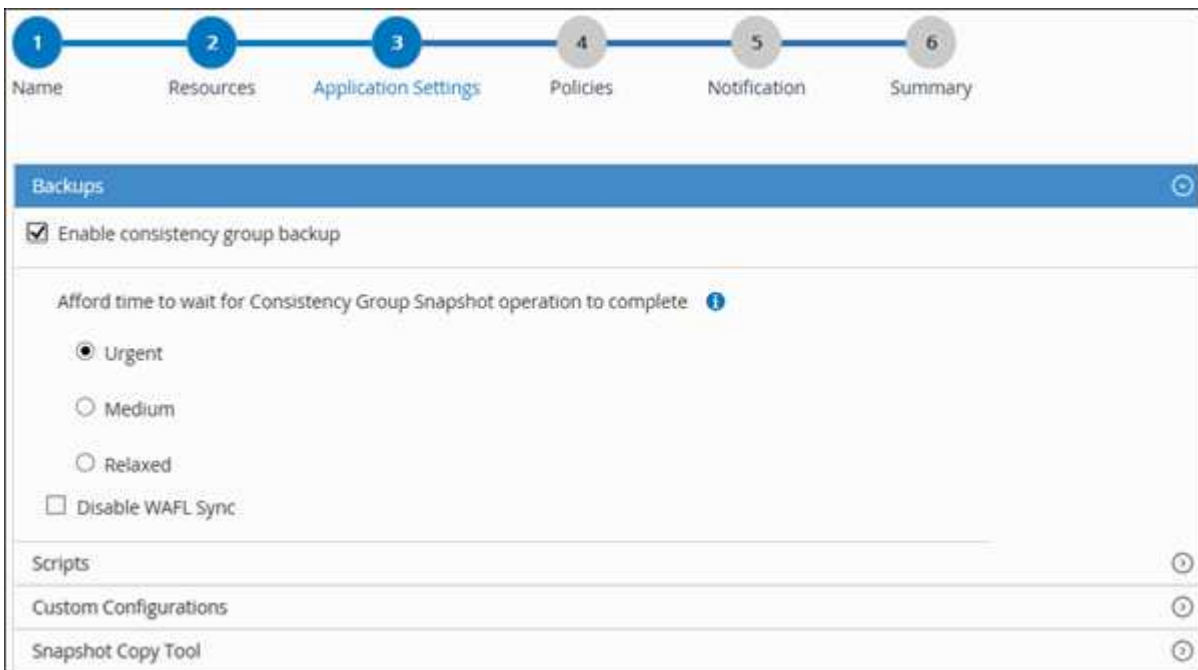
5. 在應用程式設定頁面中，執行以下操作：

- a. 按一下“備份”箭頭以設定其他備份選項：

如果需要，請啟用一致性群組備份並執行下列任務：

對於這個領域...	這樣做...
留出時間等待一致性群組快照操作完成	選擇「緊急」、「中等」或「輕鬆」來指定等待快照操作完成的時間。 緊急 = 5 秒，中等 = 7 秒，輕鬆 = 20 秒。
禁用WAFL同步	選擇此項以避免強制使用WAFL一致點。

+



1 Name 2 Resources 3 Application Settings 4 Policies 5 Notification 6 Summary

Backups

☒ Enable consistency group backup

Afford time to wait for Consistency Group Snapshot operation to complete ⓘ

☒ Urgent

☐ Medium

☐ Relaxed

☐ Disable WAFL Sync

Scripts ⓘ

Custom Configurations ⓘ

Snapshot Copy Tool ⓘ

- a. 按一下「腳本」箭頭可執行靜止、快照和取消靜止操作的前置和後置命令。您也可以在退出備份作業之前執行預命令。

前言和後記在SnapCenter伺服器中運作。

- b. 按一下「自訂設定」箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
- c. 點選*Snapshot Copy Tool*箭頭選擇建立快照的工具：

如果你想...	然後...
SnapCenter用於拍攝儲存層級快照	選擇“* 不具有檔案系統一致性的SnapCenter *”。
SnapCenter使用 Windows 外掛程式將檔案系統置於一致狀態，然後拍攝快照	選擇*具有檔案系統一致性的SnapCenter *。
輸入建立快照的命令	選擇*其他*，然後輸入建立快照的命令。

6. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後按一下「完成」。

進入資源拓樸頁面。

9. 點選*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果您已對資源套用了多個策略，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行

保留。

b. 按一下“備份”。

11. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-smconnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146\\
```

顯示使用者名稱和密碼提示。

2. 使用 Add-SmResources cmdlet 新增資源。

此範例新增資源：

```
Add-SmResource -HostName 'scc55.sscore.test.com' -PluginCode  
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database  
-StorageFootPrint (  
@{"VolumeName"="qtree_vol1_scc55_sscore_test_com";"QTREENAME"="qtree  
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. 使用 Add-SmPolicy cmdlet 建立備份策略。

此範例建立一個新的備份策略：

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'  
-PluginPolicyType DummyPlugin -description 'testPolicy'
```

4. 使用 Add-SmResourceGroup cmdlet 為SnapCenter新增新的資源組。

此範例使用指定的策略和資源建立一個新的資源組：

```
Add-SmResourceGroup -ResourceGroupName  
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'  
-Resources  
@(@{"Host"="scc55.sscore.test.com";"Uid"="QTREE2";"PluginName"="Dumm  
yPlugin"},@{"Host"="scc55.sscore.test.com";"Uid"="QTREE";"PluginName  
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'  
-usesnapcenterwithoutfilesystemconsistency
```


5. 使用 New-SmBackup cmdlet 啟動新的備份作業。

```
New-SMBackup -DatasetName  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy  
test2
```

6. 使用 Get-SmBackupReport cmdlet 查看備份作業的狀態。

此範例顯示在指定日期執行的所有作業的作業摘要報表：

```
Get-SmBackupReport -JobId 149  
  
BackedUpObjects           : {QTREE2, QTREE}  
FailedObjects             : {}  
IsScheduled               : False  
HasMetadata               : False  
SmBackupId                : 1  
SmJobId                   : 149  
StartDateTime             : 1/15/2024 1:35:17 AM  
EndDateTime               : 1/15/2024 1:36:19 AM  
Duration                  : 00:01:02.4265750  
CreatedDateTime           : 1/15/2024 1:35:51 AM  
Status                    : Completed  
ProtectionGroupName       :  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows  
SmProtectionGroupId       : 1  
PolicyName                 : test2  
SmPolicyId                : 4  
BackupName                :  
Verify_Backup_on_Multiple_Qtree_different_vserver_windows_scc55_01-  
15-2024_01.35.17.4467  
VerificationStatus        : NotApplicable  
VerificationStatuses      :  
SmJobError                 :  
BackupType                : SCC_BACKUP  
CatalogingStatus          : NotApplicable  
CatalogingStatuses       :  
ReportDataCreatedDateTime :  
PluginCode                : SCC  
PluginName                 : DummyPlugin  
PluginDisplayName         : DummyPlugin  
JobTypeId                 :  
JobHost                    : scc55.sscore.test.com
```

備份NetApp支援的插件資源的資源組

您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計劃，則備份將根據計劃自動進行。

開始之前

- 您必須已建立附加有策略的資源群組。
- 如果要將具有SnapMirror關係的資源備份到二級存儲，則分配給儲存使用者的ONTAP角色應包括「snapmirror all」權限。但是，如果您使用“vsadmin”角色，則不需要“snapmirror all”權限。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

您可以透過在搜尋框中輸入資源組名稱或按一下並選擇標籤。然後您可以點擊關閉篩選器窗格。

3. 在資源組頁面中，選擇要備份的資源組，然後按一下「立即備份」。
4. 在備份頁面中，執行以下步驟：
 - a. 如果您已將多個策略與資源群組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。
5. 透過點選「監視」>「作業」來監視操作進度。
 - 在MetroCluster配置中，SnapCenter可能無法在故障轉移後偵測到保護關係。

"MetroCluster故障轉移後無法偵測SnapMirror或SnapVault關係"

- 如果您正在備份 VMDK 上的應用程式數據，並且SnapCenter Plug-in for VMware vSphere的Java 堆大小不夠大，則備份可能會失敗。若要增加 Java 堆大小，請找到腳本檔案 `/opt/netapp/init_scripts/scvservice`。在該腳本中，`do_start method``命令啟動SnapCenter VMware 插件服務。將該命令更新為以下內容：``Java -jar -Xmx8192M -Xms4096M``。

監控NetApp支援的插件資源備份操作

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的

-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。
4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

取消NetApp支援的外掛程式的備份操作

您可以取消排隊的備份作業。

您需要什麼

- 您必須以SnapCenter管理員或作業所有者的身分登入才能取消操作。
- 您可以從「監視」頁面或「活動」窗格取消備份作業。
- 您無法取消正在執行的備份作業。
- 您可以使用SnapCenter GUI、PowerShell cmdlet 或 CLI 指令取消備份作業。
- 對於無法取消的操作，「取消作業」按鈕處於停用狀態。
- 如果您在建立角色時在“使用者\群組”頁面中選擇了“此角色的所有成員都可以檢視和操作其他成員的物件”，則可以在使用該角色時取消其他成員的排隊備份作業。

步驟

1. 執行下列操作之一：

從...	行動
監控頁面	a. 在左側導覽窗格中，按一下「監控」>「作業」。 b. 選擇操作，然後按一下「取消作業」。
活動窗格	a. 啟動備份作業後，按一下*  * 在活動窗格上查看最近的五項操作。 b. 選擇操作。 c. 在「工作詳情」頁面中，按一下「取消工作」。

操作被取消，資源恢復到之前的狀態。

在拓撲頁面中查看NetApp支援的插件資源相關的備份和克隆

當您準備備份或複製資源時，您可能會發現查看主儲存和輔助儲存上所有備份和複製的圖形表示很有幫助。在拓撲頁面中，您可以看到所選資源或資源組可用的所有備份和複製。您可以查看這些備份和克隆的詳細信息，然後選擇它們來執行資料保護操作。

關於此任務

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。

顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數量為 6。

-  鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。

2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受保護，則顯示所選資源的拓樸頁面。

4. 查看摘要卡以了解主儲存和輔助儲存上可用的備份和複製數量的摘要。

摘要卡部分顯示備份和克隆的總數。

點擊刷新按鈕將開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當應用程式資源分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

按需備份後，按一下「刷新」按鈕以刷新備份或複製的詳細資訊。

5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製、重新命名和刪除操作。



您無法重新命名或刪除輔助儲存系統上的備份。



您不能重新命名主儲存系統上的備份。

7. 如果要刪除克隆，請從表中選擇克隆，然後按一下  刪除克隆。

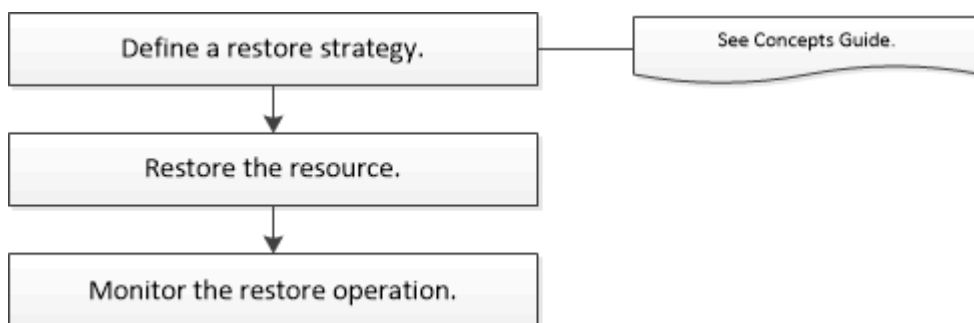
恢復NetApp支援的插件資源

恢復NetApp支援的插件資源

還原和復原工作流程包括規劃、執行還原操作和監視操作。

關於此任務

以下工作流程顯示了執行還原作業必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。有關 PowerShell cmdlet 的信息，請使用 SnapCenter cmdlet 協助或參閱 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

恢復資源備份

您可以使用 SnapCenter 來恢復資源。恢復操作的功能取決於您使用的插件。

開始之前

- 您必須已備份資源或資源群組。
- 如果您要將快照複製到映像或保管庫， SnapCenter 管理員必須已為來源磁碟區和目標磁碟區指派儲存虛擬機器 (SVM)。
- 您必須取消目前正在進行的要還原的資源或資源群組的任何備份作業。

關於此任務

- 預設恢復操作僅恢復儲存物件。只有當 NetApp 支援的插件提供該功能時，才能執行應用程式層級的復原操作。
- 對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。

資源與類型、主機或叢集名稱、相關資源群組和策略以及狀態等資訊一起顯示。



儘管備份可能針對資源群組，但在復原時，您必須選擇要還原的單一資源。

如果資源未受保護，則「總體狀態」欄位中將顯示「未受保護」。

*總體狀態*列中的狀態_不受保護_可能表示資源不受保護，或資源已由其他使用者備份。

3. 選擇資源或選擇資源組，然後選擇該組中的資源。

進入資源拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 。



6. 在「復原範圍」頁面中，選擇「完整資源」或「檔案層級」。
 - a. 如果您選擇了*完整資源*，則資源備份將會還原。

如果資源包含磁碟區或 qtree 作為儲存佔用空間，則此類磁碟區或 qtree 上的較新快照將被刪除且無法復原。此外，如果在相同的磁碟區或 qtree 上託管任何其他資源，則該資源也會被刪除。

- b. 如果您選擇了“檔案等級”，那麼您可以選擇“全部”，或選擇磁碟區或 qtree，然後輸入與所選磁碟區或 qtree 相關的路徑（以逗號分隔）。
 - 您可以選擇多個磁碟區和 qtree。
 - 如果資源類型是 LUN，則還原整個 LUN。您可以選擇多個 LUN。+ 注意：如果選擇“全部”，則會恢復磁碟區、qtree 或 LUN 上的所有檔案。

7. 在 **Pre ops** 頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。
8. 在 **Post ops** 頁面中，輸入執行復原作業後要執行的 mount 和 post restore 指令。
9. 在*通知*頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面中設定 SMTP。

10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

1. 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
PS C:\> Open-Smconnection
```

2. 使用 Get-SmBackup 和 Get-SmBackupReport cmdlet 檢索有關要還原的一個或多個備份的資訊。

此範例顯示有關所有可用備份的資訊：

```
PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

此範例顯示有關 2015 年 1 月 29 日至 2015 年 2 月 3 日備份的詳細資訊：


```
PS C:\> Get-SmBackupReport -FromDate "1/29/2015" -ToDate "2/3/2015"
```

```
SmBackupId      : 113
SmJobId          : 2032
StartDateTime    : 2/2/2015 6:57:03 AM
EndDateTime      : 2/2/2015 6:57:11 AM
Duration         : 00:00:07.3060000
CreatedDateTime  : 2/2/2015 6:57:23 AM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_06.57.08
VerificationStatus : NotVerified
```

```
SmBackupId      : 114
SmJobId          : 2183
StartDateTime    : 2/2/2015 1:02:41 PM
EndDateTime      : 2/2/2015 1:02:38 PM
Duration         : -00:00:03.2300000
CreatedDateTime  : 2/2/2015 1:02:53 PM
Status          : Completed
ProtectionGroupName : Clone
SmProtectionGroupId : 34
PolicyName       : Vault
SmPolicyId       : 18
BackupName       : Clone_SCSPR0019366001_02-02-2015_13.02.45
VerificationStatus : NotVerified
```

3. 使用 Restore-SmBackup cmdlet 從備份還原資料。

```
Restore-SmBackup -PluginCode 'DummyPlugin' -AppObjectId
'scc54.sscore.test.com\DummyPlugin\NTP\DB1' -BackupId 269
-Confirm:$false
output:
Name                : Restore
'scc54.sscore.test.com\DummyPlugin\NTP\DB1'
Id                  : 2368
StartTime           : 10/4/2016 11:22:02 PM
EndTime             :
IsCancellable       : False
IsRestartable       : False
IsCompleted         : False
IsVisible           : True
IsScheduled         : False
PercentageCompleted : 0
Description         :
Status              : Queued
Owner               :
Error               :
Priority             : None
Tasks               : {}
ParentJobID         : 0
EventId             : 0
JobTypeId           :
ApisJobKey          :
ObjectId            : 0
PluginCode          : NONE
PluginName          :
```

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

監控 NetApp 支援的插件資源復原操作

您可以使用「作業」頁面監控不同 SnapCenter 還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中

-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

克隆NetApp支援的外掛資源備份

克隆NetApp支援的外掛資源備份

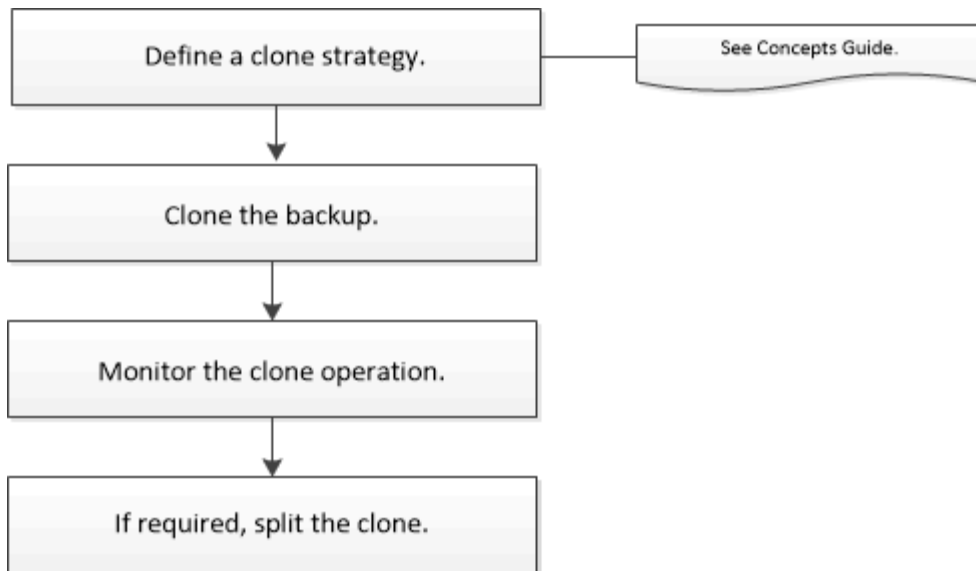
克隆工作流程包括執行克隆操作和監視操作。

關於此任務

您可能會因為以下原因而複製資源備份：

- 在應用程式開發週期中測試必須使用目前資源結構和內容實現的功能
- 用於填充資料倉儲時的資料擷取和操作工具
- 恢復被錯誤刪除或更改的數據

以下工作流程顯示了執行複製操作必須遵循的順序：



您也可以手動或在腳本中使用 PowerShell cmdlet 來執行備份、還原和複製作業。有關 PowerShell cmdlet 的詳細信息，請使用 SnapCenter cmdlet 協助或參閱 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

從備份克隆

您可以使用 SnapCenter 克隆備份。您可以從主備份或輔助備份複製。克隆操作的功能取決於您使用的插件。

開始之前

- 您必須已備份資源或資源群組。
- 預設克隆操作僅克隆儲存物件。只有當 NetApp 支援的插件提供該功能時，才可以執行應用程式層級的複製操作。
- 您應確保託管磁碟區的聚合位於儲存虛擬機器 (SVM) 的已指派聚合清單中。

關於此任務

對於 ONTAP 9.12.1 及以下版本、作為復原的一部分從 SnapLock Vault 快照建立的克隆將繼承 SnapLock Vault 到期時間。儲存管理員應在 SnapLock 到期後手動清理克隆。

SnapCenter使用者介面

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，根據資源類型從「檢視」下拉清單中過濾資源。

資源與類型、主機或叢集名稱、相關資源群組和策略以及狀態等資訊一起顯示。

3. 選擇資源或資源組。

如果選擇資源組，則必須選擇資源。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。
6. 在位置頁面中執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	預設情況下，來源主機已填入。 如果要指定不同的主機，請選擇要安裝複製並安裝插件的主機。
克隆後綴	當克隆目標與來源相同時，這是強制性的。 輸入將附加到新克隆的資源名稱的後綴。此後綴確保克隆的資源在主機上是唯一的。 例如，rs1_clone。如果要複製到與原始資源相同的主機，則必須提供後綴以區分複製的資源和原始資源；否則操作將失敗。

如果選擇的資源是 LUN，且您正在從輔助備份進行克隆，則會列出目標磁碟區。單一來源可以有多個目標磁碟區。

7. 在「設定」頁面中，執行以下操作：

對於這個領域...	這樣做...
發起者名稱	輸入主機啟動器名稱，可以是 IQDN 或 WWPN。
Igroup協議	選擇 Igroup 協定。



僅當儲存類型為 LUN 時才會顯示設定頁面。

- 在腳本頁面中，輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。輸入 mount 指令將檔案系統掛載到主機。

例如：

- 克隆前指令：刪除現有的同名資料庫
- 克隆後指令：驗證資料庫或啟動資料庫。

Linux 電腦上磁碟區或 qtree 的掛載指令：mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

- 在*通知*頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。

- 查看摘要並點擊“完成”。
- 透過點選「監視」>「作業」來監視操作進度。

PowerShell cmdlet

步驟

- 使用 Open-SmConnection cmdlet 為指定使用者啟動與SnapCenter伺服器的連線會話。

```
Open-SmConnection -SMSbaseurl  
https:\\snapctr.demo.netapp.com:8146/
```

- 列出可以使用 Get-SmBackup 或 Get-SmResourceGroup cmdlet 克隆的備份。

此範例顯示有關所有可用備份的資訊：

```
C:\PS>PS C:\> Get-SmBackup
```

BackupId	BackupName	BackupTime	BackupType
-----	-----	-----	-----
1	Payroll Dataset_vise-f6_08...	8/4/2015	11:02:32
AM	Full Backup		
2	Payroll Dataset_vise-f6_08...	8/4/2015	11:23:17
AM			

此範例顯示有關指定資源組的資訊：

```
PS C:\> Get-SmResourceGroup
```

Description	:

```

CreationTime           : 10/10/2016 4:45:53 PM
ModificationTime       : 10/10/2016 4:45:53 PM
EnableEmail            : False
EmailSMTPServer        :
EmailFrom              :
EmailTo                :
EmailSubject           :
EnableSysLog           : False
ProtectionGroupType    : Backup
EnableAsupOnFailure    : False
Policies               : {}
HostResourceMapping    : {}
Configuration          :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus       : Completed
VerificationServer     :
EmailBody              :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance   :
CustomText             :
CustomSnapshotFormat   :
SearchResources        : False
ByPassCredential       : False
IsCustomSnapshot       :
MaintenanceStatus      : Production
PluginProtectionGroupTypes : {SMSQL}
Tag                    :
IsInternal             : False
EnableEmailAttachment  : False
VerificationSettings   : {}
Name                   : NFS_DB
Type                   : Group
Id                     : 2
Host                   :
UserName               :
Passphrase             :
Deleted                : False
Auth                   : SMCoreContracts.SmAuth
IsClone                : False
CloneLevel             : 0
Hosts                  :
StorageName            :
ResourceGroupNames     :
PolicyNames            :

```

```

Description :
CreationTime : 10/10/2016 4:51:36 PM
ModificationTime : 10/10/2016 5:27:57 PM
EnableEmail : False
EmailSMTPServer :
EmailFrom :
EmailTo :
EmailSubject :
EnableSysLog : False
ProtectionGroupType : Backup
EnableAsupOnFailure : False
Policies : {}
HostResourceMapping : {}
Configuration :
SMCoreContracts.SmCloneConfiguration
LastBackupStatus : Failed
VerificationServer :
EmailBody :
EmailNotificationPreference : Never
VerificationServerInfo :
SchedulerSQLInstance :
CustomText :
CustomSnapshotFormat :
SearchResources : False
ByPassRunAs : False
IsCustomSnapshot :
MaintenanceStatus : Production
PluginProtectionGroupTypes : {SMSQL}
Tag :
IsInternal : False
EnableEmailAttachment : False
VerificationSettings : {}
Name : Test
Type : Group
Id : 3
Host :
UserName :
Passphrase :
Deleted : False
Auth : SMCoreContracts.SmAuth
IsClone : False
CloneLevel : 0
Hosts :
StorageName :
ResourceGroupNames :
PolicyNames :

```


3. 使用 `New-SmClone cmdlet` 從複製資源組或現有備援啟動複製作業。

此範例從包含所有日誌的指定備份建立複製：

```
New-SmClone -BackupName
Verify_delete_clone_on_qtree_windows_scc54_10-04-2016_19.05.48.0886
-Resources @{"Host"="scc54.sccore.test.com";"Uid"="QTREE1"} -
CloneToInstance scc54.sccore.test.com -Suffix '_QtreeCloneWin9'
-AutoAssignMountPoint -AppPluginCode 'DummyPlugin' -initiatorname
'iqn.1991-
05.com.microsoft:scc54.sccore.test.com' -igroupprotocol 'mixed'
```

4. 使用 `Get-SmCloneReport cmdlet` 查看複製作業的狀態。

此範例顯示指定作業 ID 的複製報表：

```
PS C:\> Get-SmCloneReport -JobId 186

SmCloneId           : 1
SmJobId              : 186
StartDateTime        : 8/3/2015 2:43:02 PM
EndDateTime          : 8/3/2015 2:44:08 PM
Duration             : 00:01:06.6760000
Status               : Completed
ProtectionGroupName  : Draper
SmProtectionGroupId  : 4
PolicyName            : OnDemand_Clone
SmPolicyId           : 4
BackupPolicyName      : OnDemand_Full_Log
SmBackupPolicyId     : 1
CloneHostName        : SCSPR0054212005.mycompany.com
CloneHostId          : 4
CloneName            : Draper__clone__08-03-2015_14.43.53
SourceResources       : {Don, Betty, Bobby, Sally}
ClonedResources       : {Don_DRAPER, Betty_DRAPER, Bobby_DRAPER,
Sally_DRAPER}
SmJobError            :
```

監控NetApp支援的插件資源克隆操作

您可以使用「作業」頁面監控SnapCenter複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

保護 Unix 檔案系統

您可以使用適用於 Unix 檔案系統的SnapCenter插件做什麼

當您的環境中安裝了適用於 Unix 檔案系統的插件時，您可以使用SnapCenter備份、還原和複製 Unix 檔案系統。您也可以執行支援這些操作的任務。

- 發現資源
- 備份 Unix 檔案系統
- 安排備份作業
- 恢復檔案系統備份
- 克隆檔案系統備份
- 監控備份、復原和複製操作

支援的配置

物品	支援的配置
環境	• 實體伺服器 • 虛擬伺服器 NFS 和 SAN 上的 vVol 資料儲存。vVol 資料儲存只能使用適用於 VMware vSphere 的ONTAP Tools 進行設定。
作業系統	• 紅帽企業 Linux • Oracle Linux • SUSE Linux 企業伺服器 (SLES)
檔案系統	• SAN： ◦ 基於 LVM 和非 LVM 的檔案系統 ◦ VMDK ext3、ext4 與 xfs 上的 LVM • NFS：NFS v3、NFS v4.x
協定	• FC • 光纖通道 • iSCSI • NFS
多路徑	是的

限制

- 不支援在磁碟區組中混合使用 RDM 和虛擬磁碟。
- 不支援檔案級恢復。

但是，您可以透過複製備份然後手動複製檔案來手動執行檔案級復原。

- 不支援混合來自 NFS 和 VMFS 資料儲存的 VMDK 上的檔案系統。
- 不支援 NVMe。
- 不支援配置。

特徵

- 透過處理 Linux 或 AIX 系統上的底層主機儲存堆疊，使 Oracle 資料庫外掛程式能夠對 Oracle 資料庫執行資料保護操作
- 在運作ONTAP的儲存系統上支援網路檔案系統 (NFS) 和儲存區域網路 (SAN) 協定。
- 對於 Linux 系統，當您部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊該插件時，VMDK 和 RDM LUN 上的 Oracle 資料庫受支援。
- 支援 SAN 檔案系統和 LVM 佈局上的 AIX Mount Guard。
- 僅支援增強型日誌檔案系統 (JFS2) 在 SAN 檔案系統上進行內嵌日誌記錄以及針對 AIX 系統的 LVM 佈局。

支援 SAN 本機設備、檔案系統以及在 SAN 設備上建置的 LVM 佈局。

- 自動執行SnapCenter環境中 UNIX 檔案系統的應用程式感知備份、還原和克隆作業

為 Unix 檔案系統安裝SnapCenter插件

新增主機並安裝 Linux 插件包的先決條件

在新增主機並安裝 Linux 的插件包之前，您必須完成所有要求。

- 如果您正在使用 iSCSI，則 iSCSI 服務必須正在執行。
- 您可以對 root 使用者或非 root 使用者使用基於密碼的身份驗證，也可以使用基於 SSH 金鑰的身份驗證。

非 root 使用者可以安裝適用於 Unix 檔案系統的SnapCenter插件。但是，您應該為非 root 使用者配置 sudo 權限來安裝和啟動插件進程。安裝插件後，進程將作為有效的非 root 用戶運行。

- 為安裝使用者建立以 Linux 為身份驗證模式的憑證。
- 您必須在 Linux 主機上安裝 Java 11。



確保您在 Linux 主機上僅安裝了 JAVA 11 的認證版本。

有關下載 JAVA 的信息，請參閱：["適用於所有作業系統的 Java 下載"](#)

- 您應該將 **bash** 作為插件安裝的預設 shell。

Linux 主機需求

在安裝適用於 Linux 的 SnapCenter 插件包之前，您應該確保主機符合要求。

物品	要求
作業系統	• 紅帽企業 Linux • Oracle Linux • SUSE Linux 企業伺服器 (SLES)
主機上 SnapCenter 插件的最小 RAM	2GB
主機上 SnapCenter 插件的最小安裝和日誌空間	2GB  您應該分配足夠的磁碟空間並監控日誌資料夾的儲存消耗。所需的日誌空間取決於要保護的實體的數量和資料保護操作的頻率。如果沒有足夠的磁碟空間，則不會為最近執行的操作建立日誌。
所需軟體包	Java 11 Oracle Java 與 OpenJDK  確保您在 Linux 主機上僅安裝了 JAVA 11 的認證版本。 如果您已將 JAVA 升級至最新版本，則必須確保位於 <code>/var/opt/snapcenter/spl/etc/spl.properties</code> 的 <code>JAVA_HOME</code> 選項設定為正確的 JAVA 版本和正確的路徑。

有關受支援版本的最新信息，請參閱 ["NetApp 互通性表工具"](#)。

使用 GUI 新增主機並安裝 Linux 插件包

您可以使用「新增主機」頁面新增主機，然後安裝適用於 Linux 的 SnapCenter 插件套件。插件會自動安裝在遠端主機上。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：

對於這個領域...	這樣做...
主機類型	選擇 Linux 作為主機類型。
主機名稱	輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。 SnapCenter依賴 DNS 的正確配置。因此，最佳做法是輸入 FQDN。 如果您使用SnapCenter新增主機且該主機是子網域的一部分，則必須提供 FQDN。
證書	選擇您建立的憑證名稱或建立新的憑證。 該憑證必須具有遠端主機的管理權限。有關詳細信息，請參閱有關建立憑證的資訊。 您可以將遊標置於指定的憑證名稱上來查看有關憑證的詳細資訊。  憑證驗證模式由您在新增主機精靈中指定的主機類型決定。

5. 在選擇要安裝的外掛程式部分中，選擇*Unix 檔案系統*。

6. （可選）按一下“更多選項”。

對於這個領域...	這樣做...
港口	保留預設連接埠號碼或指定連接埠號碼。 預設連接埠號碼為 8145。如果SnapCenter伺服器安裝在自訂連接埠上，則該連接埠號碼將顯示為預設連接埠。  如果您手動安裝了插件並指定了自訂端口，則必須指定相同的端口。否則，操作失敗。
安裝路徑	預設路徑為 <code>/opt/ NetApp/snapcenter</code>。 您可以選擇自訂路徑。如果您使用自訂路徑，請確保 <code>sudoers</code> 的預設內容使用自訂路徑進行更新。
跳過可選的預安裝檢查	如果您已經手動安裝了插件並且不想驗證主機是否符合安裝插件的要求，請選取此核取方塊。

7. 點選“提交”。

如果您沒有選取「跳過預檢查」複選框，則會對主機進行驗證，以驗證主機是否符合安裝外掛程式的要求。



如果防火牆拒絕規則中指定了插件連接埠防火牆狀態，則預先檢查腳本不會驗證該狀態。

如果未滿足最低要求，則會顯示適當的錯誤或警告訊息。如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 `C:\Program Files\NetApp\SnapCenter WebApp` 的 `web.config` 檔案以修改預設值。如果錯誤與其他參數有關，則應修復該問題。



在 HA 設定中，如果您要更新 `web.config` 文件，則必須在兩個節點上更新該文件。

8. 驗證指紋，然後按一下*確認並提交*。



SnapCenter不支援 ECDSA 演算法。



即使之前已將同一台主機新增至SnapCenter並且已確認指紋，也必須進行指紋驗證。

9. 監控安裝進度。

特定於安裝的日誌檔案位於 `/custom_location/snapcenter/logs`。

結果

主機上掛載的所有檔案系統都會自動發現並顯示在資源頁面下。如果沒有顯示任何內容，請按一下「刷新資源」。

監控安裝狀態

您可以使用「作業」頁面監控SnapCenter插件包的安裝進度。您可能需要檢查安裝進度以確定安裝何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，若要篩選清單以便僅列出外掛程式安裝操作，請執行下列操作：
 - a. 按一下“過濾器”。

- b. 可選：指定開始日期和結束日期。
 - c. 從類型下拉式選單中，選擇*插件安裝*。
 - d. 從狀態下拉式選單中，選擇安裝狀態。
 - e. 按一下“應用”。
4. 選擇安裝作業並點擊*詳細資料*以查看作業詳細資料。
 5. 在「作業詳情」頁面中，按一下「檢視日誌」。

配置SnapCenter插件Loader服務

SnapCenter插件載入Loader服務會載入 Linux 的插件包以便與SnapCenter伺服器互動。安裝適用於 Linux 的SnapCenter插件包時，也會安裝SnapCenter插件載入Loader服務。

關於此任務

安裝適用於 Linux 的SnapCenter插件包後， SnapCenter插件Loader服務將自動啟動。如果SnapCenter插件Loader服務無法自動啟動，您應該：

- 確保插件運行的目錄沒有被刪除
- 增加分配給 Java 虛擬機器的記憶體空間

spl.properties 檔案位於 `/custom_location/ NetApp/snapcenter/spl/etc/`，包含下列參數。這些參數被分配了預設值。

參數名稱	描述
日誌等級	顯示支援的日誌等級。 可能的值是 TRACE、DEBUG、INFO、WARN、ERROR 和 FATAL。
SPL_協定	顯示SnapCenter插件Loader程式支援的協定。 僅支援HTTPS協定。如果缺少預設值，您可以新增該值。
SNAPCENTER_SERVER_協議	顯示SnapCenter Server 支援的協定。 僅支援HTTPS協定。如果缺少預設值，您可以新增該值。
跳過JAVAHOME更新	預設情況下，SPL 服務會偵測 java 路徑並更新 JAVA_HOME 參數。 因此預設值設定為 FALSE。如果您想要停用預設行為並手動修復 java 路徑，可以將其設定為 TRUE。

參數名稱	描述
SPL_KEYSTORE_PASS	顯示密鑰庫檔案的密碼。 僅當您變更密碼或建立新的金鑰庫檔案時才可以變更此值。
SPL_埠	顯示SnapCenter插件Loader服務正在執行的連接埠號碼。 如果缺少預設值，您可以新增該值。  安裝插件後您不應更改該值。
SNAPCENTER_SERVER_HOST	顯示SnapCenter伺服器的 IP 位址或主機名稱。
SPL_KEYSTORE_PATH	顯示密鑰庫檔案的絕對路徑。
SNAPCENTER_SERVER_PORT	顯示SnapCenter伺服器正在執行的連接埠號碼。
日誌最大數量	顯示保留在 <code>/custom_location/snapcenter/spl/logs</code> 資料夾中的SnapCenter插件Loader日誌檔案的數量。 預設值設定為 5000。如果計數超過指定值，則保留最後 5000 個修改的檔案。從SnapCenter插件Loader服務啟動時起，每 24 小時自動檢查一次檔案數量。  如果手動刪除 <code>spl.properties</code> 文件，則要保留的文件數將設定為 9999。
JAVA_HOME	顯示用於啟動 SPL 服務的 JAVA_HOME 的絕對目錄路徑。 此路徑是在安裝期間和啟動 SPL 的過程中確定的。
日誌最大大小	顯示作業日誌檔案的最大大小。 一旦達到最大大小，日誌檔案就會被壓縮，並且日誌會被寫入該作業的新檔案中。
保留最近幾天的日誌	顯示日誌最多保留的天數。
啟用憑證驗證	當主機啟用 CA 憑證驗證時顯示 true。 您可以透過編輯 <code>spl.properties</code> 或使用SnapCenter GUI 或 <code>cmdlet</code> 來啟用或停用此參數。

如果這些參數中的任何一個沒有分配預設值或您想要分配或更改值，那麼您可以修改 `spl.properties` 檔案。您也可以驗證 `spl.properties` 檔案並編輯該檔案以解決與指派給參數的值相關的任何問題。修改 `spl.properties` 檔案後，您應該重新啟動SnapCenter插件Loader服務。

步驟

1. 根據需要執行以下操作之一：

◦ 啟動SnapCenter插件Loader服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl start`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`

◦ 停止SnapCenter插件Loader服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl stop`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`



您可以將 `-force` 選項與 `stop` 命令結合使用來強制停止SnapCenter插件Loader服務。但是，在執行此操作之前應謹慎，因為它也會終止現有操作。

◦ 重新啟動SnapCenter插件Loader服務：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl restart`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`

◦ 尋找SnapCenter插件Loader服務的狀態：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl status`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ 尋找SnapCenter插件Loader服務中的變更：

- 以 root 使用者身分執行：`/custom_location/NetApp/snapcenter/spl/bin/spl change`
- 以非 root 使用者身分執行：`sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

在 Linux 主機上使用SnapCenter插件Loader(SPL) 服務設定 CA 證書

您應該管理 SPL 金鑰庫及其憑證的密碼，配置 CA 證書，將根憑證或中間憑證配置到 SPL 信任庫，並使用SnapCenter插件Loader服務將 CA 簽章金鑰對配置到 SPL 信任庫以啟動已安裝的數位憑證。



SPL 使用位於「`/var/opt/snapcenter/spl/etc`」的檔案「`keystore.jks`」作為其信任庫和金鑰庫。

管理 **SPL** 金鑰庫的密碼以及正在使用的 **CA** 簽章金鑰對的別名

步驟

1. 您可以從 SPL 屬性檔案中檢索 SPL 金鑰庫預設密碼。

它是與鍵“SPL_KEYSTORE_PASS”對應的值。

2. 更改密鑰庫密碼：

```
keytool -storepasswd -keystore keystore.jks
```

- ． 將金鑰庫中所有私鑰條目別名的密碼變更為與金鑰庫相同的密碼：

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

對 spl.properties 檔案中的金鑰 SPL_KEYSTORE_PASS 進行相同的更新。

3. 修改密碼後重啟服務。



SPL 金鑰庫的密碼和私鑰的所有相關別名的密碼應該相同。

將根憑證或中繼憑證設定到 **SPL** 信任庫

您應該將沒有私鑰的根憑證或中間憑證設定到 SPL 信任庫。

步驟

1. 導覽至包含 SPL 金鑰庫的資料夾：`/var/opt/snapcenter/spl/etc`。
2. 找到檔案“keystore.jks”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

- ． 新增根證書或中間證書：

```
keytool -import -trustcacerts -alias  
<AliasNameForCertificateToBeImported> -file /<CertificatePath> -keystore  
keystore.jks
```

- ． 將根憑證或中間憑證配置到 SPL 信任庫後重新啟動服務。



您應該新增根 CA 證書，然後新增中間 CA 證書。

將 CA 簽章金鑰對配置到 SPL 信任庫

您應該將 CA 簽署的金鑰對配置到 SPL 信任庫。

步驟

1. 導航至包含 SPL 金鑰庫 `/var/opt/snapcenter/spl/etc` 的資料夾。
2. 找到檔案“`keystore.jks`”。
3. 列出密鑰庫中新增的憑證：

```
keytool -list -v -keystore keystore.jks
```

． 新增具有私鑰和公鑰的 CA 憑證。

```
keytool -importkeystore -srckeystore <CertificatePathToImport>  
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

． 列出密鑰庫中新增的憑證。

```
keytool -list -v -keystore keystore.jks
```

． 驗證金鑰庫是否包含與新增至金鑰庫的新 CA 憑證相對應的別名。

． 將新增的CA憑證私鑰密碼變更為`keystore`密碼。

預設 SPL 金鑰庫密碼是 `spl.properties` 檔案中金鑰 `SPL_KEYSTORE_PASS` 的值。

```
keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore  
keystore.jks
```

． 如果CA憑證中的別名較長，且包含空格或特殊字元（“*”、“ ”、“ ”），請將別名修改為簡單名稱：

```
keytool -changealias -alias "<OriginalAliasName>" -destalias  
"<NewAliasName>" -keystore keystore.jks
```

． 從位於 `spl.properties` 檔案中的金鑰庫配置別名。

根據鍵 `SPL_CERTIFICATE_ALIAS` 更新此值。

4. 將 CA 簽署金鑰對配置到 SPL 信任庫後重新啟動服務。

為 SPL 設定憑證撤銷清單 (CRL)

您應該為 SPL 配置 CRL

關於此任務

- SPL 將在預先配置的目錄中尋找 CRL 檔案。
- SPL 的 CRL 檔案的預設目錄是 `/var/opt/snapcenter/spl/etc/crl`。

步驟

1. 您可以根據鍵 `SPL_CRL_PATH` 修改和更新 `spl.properties` 檔案中的預設目錄。
2. 您可以在此目錄中放置多個 CRL 檔案。

將根據每個 CRL 驗證傳入的憑證。

為插件啟用 CA 憑證

您應該設定 CA 憑證並在 SnapCenter 伺服器 and 對應的插件主機中部署 CA 憑證。您應該為插件啟用 CA 憑證驗證。

開始之前

- 您可以使用執行 `_Set-SmCertificateSettings_ cmdlet` 來啟用或停用 CA 憑證。
- 您可以使用 `_Get-SmCertificateSettings_` 顯示插件的憑證狀態。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇單一或多個插件主機。
4. 按一下“更多選項”。
5. 選擇*啟用憑證驗證*。

完成後

託管主機選項卡主機顯示一個掛鎖，掛鎖的顏色表示 SnapCenter 伺服器 and 插件主機之間的連線狀態。

- *  * 表示 CA 憑證未啟用或未指派給插件主機。
- *  * 表示 CA 憑證驗證成功。
- *  * 表示無法驗證 CA 憑證。
- *  * 表示無法檢索連線資訊。



當狀態為黃色或綠色時，表示資料保護操作已成功完成。

SnapCenter Plug-in for VMware vSphere

如果您的資料庫或檔案系統儲存在虛擬機器 (VM) 上，或者您想要保護 VM 和資料儲存區，則必須部署 SnapCenter Plug-in for VMware vSphere。

有關部署的信息，請參閱 ["部署概述"](#)。

部署 CA 憑證

若要使用適用SnapCenter Plug-in for VMware vSphere設定 CA 證書，請參閱 ["建立或匯入 SSL 憑證"](#)。

配置 CRL 文件

SnapCenter Plug-in for VMware vSphere在預先設定的目錄中尋找 CRL 檔案。SnapCenter Plug-in for VMware vSphere的 CRL 檔案的預設目錄是 `/opt/netapp/config/crl`。

您可以在此目錄中放置多個 CRL 檔案。將根據每個 CRL 驗證傳入的憑證。

準備保護 Unix 檔案系統

在執行任何資料保護操作（例如備份、複製或復原作業）之前，您應該設定您的環境。您也可以設定SnapCenter伺服器以使用SnapMirror和SnapVault技術。

若要利用SnapVault和SnapMirror技術，您必須在儲存裝置上設定並初始化來源磁碟區和目標磁碟區之間的資料保護關係。您可以使用 NetAppSystem Manager 或儲存控制台命令列來執行這些任務。

在使用適用於 Unix 檔案系統的插件之前，SnapCenter管理員應安裝和設定SnapCenter伺服器並執行先決條件任務。

- 安裝並配置SnapCenter伺服器。["了解更多"](#)
- 透過新增儲存系統連接來配置SnapCenter環境。["了解更多"](#)



SnapCenter不支援不同叢集上具有相同名稱的多個 SVM。使用 SVM 註冊或叢集註冊向SnapCenter註冊的每個 SVM 都必須是唯一的。

- 新增主機、安裝插件、發現資源。
- 如果您使用SnapCenter Server 保護駐留在 VMware RDM LUN 或 VMDK 上的 Unix 檔案系統，則必須部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊外掛程式。
- 在您的 Linux 主機上安裝 Java。
- 如果您需要備份複製，請在ONTAP上設定SnapMirror和SnapVault。

備份 Unix 檔案系統

發現可用於備份的 UNIX 檔案系統

安裝外掛程式後，該主機上的所有檔案系統都會自動發現並顯示在資源頁面中。您可以將這些檔案系統新增至資源組以執行資料保護操作。

開始之前

- 您必須完成安裝SnapCenter伺服器、新增主機和建立儲存系統連線等任務。

- 如果檔案系統駐留在虛擬機器磁碟 (VMDK) 或原始裝置對映 (RDM) 上，則必須部署SnapCenter Plug-in for VMware vSphere並向SnapCenter註冊外掛程式。

有關更多信息，請參閱 ["SnapCenter Plug-in for VMware vSphere"](#)。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從檢視清單中選擇*路徑*。
3. 按一下“刷新資源”。

檔案系統與類型、主機名稱、相關資源群組和政策以及狀態等資訊一起顯示。

為 Unix 檔案系統建立備份策略

在使用SnapCenter備份 Unix 檔案系統之前，您必須為要備份的資源或資源群組建立備份原則。備份策略是一組規則，用於控制如何管理、排程和保留備份。您也可以指定複製、腳本和備份類型設定。當您想要在另一個資源或資源群組上重複使用策略時，建立策略可以節省時間。

開始之前

- 您必須已完成安裝SnapCenter、新增主機、發現檔案系統和建立儲存系統連線等任務，為資料保護做好準備。
- 如果您要將快照複製到映像或保管庫二級存儲，SnapCenter管理員必須已為您指派來源磁碟區和目標磁碟區的 SVM。
- 查看SnapMirror主動同步特定的先決條件和限制。欲了解詳細信息，請參閱 ["SnapMirror主動同步的物件限制"](#)。

關於此任務

- SnapLock
 - 如果選擇了「保留備份副本特定天數」選項，則SnapLock保留期必須小於或等於上述保留天數。

指定快照鎖定期可防止在保留期到期之前刪除快照。這可能導致保留的快照數量超過策略中指定的數量。

對於ONTAP 9.12.1 及以下版本、作為復原的一部分從SnapLock Vault 快照建立的克隆將繼承SnapLock Vault 到期時間。儲存管理員應在SnapLock到期後手動清理克隆。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 從下拉清單中選擇“**Unix 檔案系統**”。
4. 點選“新建”。
5. 在名稱頁面中，輸入策略名稱和詳細資訊。

6. 在「備份和複製」頁面中，執行以下操作：

- a. 指定備份設定。
- b. 透過選擇*按需*、每小時、每天、*每週*或*每月*來指定計畫頻率。
- c. 在「選擇輔助複製選項」部分中，選擇以下一個或兩個輔助複製選項：

對於這個領域...	這樣做...
建立本地 Snapshot 副本後更新SnapMirror	選擇此欄位可在另一個磁碟區上建立備份集的鏡像副本（SnapMirror複製）。 應為SnapMirror主動同步啟用此選項。
建立本機 Snapshot 副本後更新SnapVault	選擇此選項可執行磁碟到磁碟備份複製（SnapVault備份）。
錯誤重試次數	輸入操作停止之前允許的最大複製嘗試次數。

7. 在「保留」頁面中，指定「備份和複製」頁面中所選的備份類型和計畫類型的保留設定：

如果你想...	然後...
保留一定數量的快照	選擇*要保留的副本*，然後指定要保留的快照數量。 如果快照數量超過指定數量，則會刪除快照，並先刪除最舊的副本。  最大保留值為 1018。如果保留設定的值高於底層ONTAP版本支援的值，則備份將會失敗。  如果您打算啟用SnapVault複製，則必須將保留計數設為 2 或更高。如果將保留計數設為 1，則保留操作可能會失敗，因為第一個快照是SnapVault關係的參考快照，直到較新的快照複製到目標。
將快照保留一定天數	選擇*保留副本*，然後指定在刪除快照之前要保留快照的天數。
快照副本鎖定期	選擇*Snapshot 副本鎖定期限*並指定天、月或年的持續時間。 Snaplock 保留期應少於 100 年。

8. 選擇策略標籤。



您可以為遠端複製的主快照指派SnapMirror標籤，從而允許主快照將快照複製作業從SnapCenter卸載到ONTAP二級系統。無需在策略頁面中啟用SnapMirror或SnapVault選項即可完成此操作。

9. 在腳本頁面中，分別輸入要在備份作業之前或之後執行的前置腳本或後置腳本的路徑和參數。



您應該檢查這些命令是否存在於插件主機上可用的命令清單中，該清單位於 _NetApp 路徑下。

您也可以指定腳本超時值。預設值為 60 秒。

10. 查看摘要，然後按一下「完成」。

為 Unix 檔案系統建立資源組並附加策略

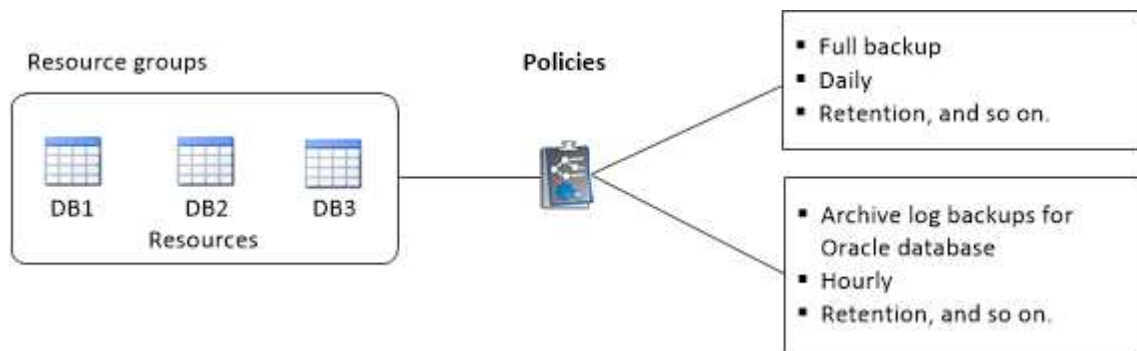
資源組是一個容器，您可以在其中新增要備份和保護的資源。資源組可讓您備份與檔案系統相關的所有資料。

關於此任務

- 具有 ASM 磁碟組中檔案的資料庫必須處於「MOUNT」或「OPEN」狀態才能使用 Oracle DBVERIFY 公用程式驗證其備份。

將一個或多個策略附加到資源組以定義要執行的資料保護作業的類型。

下圖說明了資料庫的資源、資源群組和策略之間的關係：



- 對於啟用SnapLock的策略、對於ONTAP 9.12.1 及以下版本、如果指定 Snapshot 鎖定期限、則作為恢復的一部分從防篡改快照創建的克隆將繼承SnapLock到期時間。儲存管理員應在SnapLock到期後手動清理克隆。
- 不支援將沒有SnapMirror主動同步的新檔案系統新增至包含具有SnapMirror主動同步的資源的現有資源組。
- 不支援在SnapMirror主動同步的故障轉移模式下為現有資源組新增檔案系統。您只能在常規或故障回復狀態下將資源新增至資源組。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

- a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，`customtext_resource group_policy_hostname` 或 `resource group_hostname`。預設情況下，時間戳記會附加到快照名稱。

4. 在資源頁面中，從 主機 下拉清單中選擇一個 Unix 檔案系統主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從“可用資源”部分中選擇資源並將其移至“選定資源”部分。

6. 在應用程式設定頁面中，執行以下操作：

- 選擇腳本箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
- 選擇備份一致性選項之一：
 - 如果您想確保在建立備份之前刷新檔案系統快取數據，並且在建立備份時不允許對檔案系統進行任何輸入或輸出操作，請選擇「檔案系統一致」。



對於檔案系統一致性，將對磁碟區組中涉及的 LUN 進行一致性群組快照。

- 如果您想確保在建立備份之前刷新檔案系統快取數據，請選擇*崩潰一致*。



如果您在資源組中新增了不同的檔案系統，資源組中不同檔案系統的所有磁碟區都會被放入一致性群組中。

7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtServer 指定 SMTP 伺服器詳細資訊。

9. 查看摘要，然後按一下「完成」。

在ASA r2 系統上建立資源組並為 Unix 檔案系統啟用二級保護

您應該建立資源組來新增ASA r2 系統上的資源。您也可以在建​​立資源組時配置輔助保護。

開始之前

- 您應該確保沒有將ONTAP 9.x 資源和ASA r2 資源新增至同一個資源群組。
- 您應該確保您沒有同時具有ONTAP 9.x 資源和ASA r2 資源的資料庫。

關於此任務

- 只有當登入使用者被指派到啟用了 **SecondaryProtection** 功能的角色時，才可以使用二級保護。
- 如果啟用了輔助保護，則在建立主一致性群組和輔助一致性群組時，資源群組將進入維護模式。建立主一致性群組和輔助一致性群組後，資源組將退出維護模式。
- SnapCenter不支援對克隆資源進行二次保護。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：
 - a. 在名稱欄位中輸入資源組的名稱。



資源組名稱不應超過 250 個字元。

- b. 在標籤欄位中輸入一個或多個標籤，以協助您稍後搜尋資源組。

例如，如果您將 HR 作為標籤新增至多個資源群組，稍後您可以找到與 HR 標籤關聯的所有資源群組。

- c. 選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如，customtext_resource group_policy_hostname 或 resource group_hostname。預設情況下，時間戳記會附加到快照名稱。

- d. 指定您不想備份的存檔日誌檔案的目標。



如果需要，您應該使用與應用程式中設定的完全相同的目的地，包括前綴。

4. 在資源頁面中，從*主機*下拉清單中選擇資料庫主機名稱。



只有當成功發現資源時，該資源才會列在「可用資源」部分。如果您最近新增了資源，則只有在刷新資源清單後，它們才會出現在可用資源清單中。

5. 從可用資源部分選擇ASA r2 資源並將其移至選定資源部分。
6. 在應用程式設定頁面中，選擇備份選項。
7. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。



您也可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在要設定計劃的策略的配置計劃列中。
- c. 在為政策_policy_name_新增計劃視窗中，配置計劃，然後按一下*確定*。

其中，*policy_name* 是您選擇的政策的名稱。

配置的計劃列在「已套用的計劃」欄位中。

當第三方備份計畫與SnapCenter備份計畫重疊時，不支援第三方備份計畫。

8. 如果您選擇的策略啟用了二級保護，則會顯示二級保護頁面，您需要執行下列步驟：
 - a. 選擇複製策略的類型。



不支援同步複製策略。

- b. 指定要使用的一致性組後綴。
- c. 從目標叢集和目標 SVM 下拉選單中選擇要使用的對等叢集和 SVM。



SnapCenter不支援叢集和 SVM 對等連線。您應該使用 System Manager 或ONTAP CLI 來執行叢集和 SVM 對等連線。



如果資源已在SnapCenter之外受到保護，則這些資源將顯示在「輔助受保護資源」部分。

1. 在驗證頁面上，執行以下步驟：
 - a. 按一下「載入定位器」以載入SnapMirror或SnapVault卷，對二級儲存執行驗證。
 - b. 點選  在設定計劃列中設定策略所有計劃類型的驗證計劃。

- c. 在新增驗證計畫 policy_name 對話方塊中，執行下列操作：

如果你想...	這樣做...
備份後運行驗證	選擇*備份後執行驗證*。
安排驗證	選擇*執行計劃驗證*，然後從下拉清單中選擇計劃類型。

- d. 選擇*在輔助位置驗證*以在輔助儲存系統上驗證您的備份。
e. 按一下“確定”。

配置的驗證計劃列在「已套用的計劃」欄位中。

2. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源組執行的操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 Set-SmSmtPServer 指定 SMTP 伺服器詳細資訊。

3. 查看摘要，然後按一下「完成」。

備份 Unix 檔案系統

如果資源不屬於任何資源群組，您可以從資源頁面備份該資源。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，從檢視清單中選擇*路徑*。
3. 點選，然後選擇主機名稱和Unix檔案系統來過濾資源。
4. 選擇要備份的檔案系統。
5. 在資源頁面中，您可以執行以下步驟：
 - a. 選取複選框，然後輸入要用於快照名稱的自訂名稱格式。

例如， customtext_policy_hostname`或者 `resource_hostname。預設情況下，時間戳記會附加到快照名稱。

6. 在應用程式設定頁面中，執行以下操作：
 - 選擇腳本箭頭並輸入靜止、快照和取消靜止操作的前置和後置命令。您也可以輸入在發生故障時退出之前要執行的預命令。
 - 選擇備份一致性選項之一：
 - 如果您想確保在建立備份之前刷新檔案系統快取數據，並且在建立備份時不對檔案系統執行任何操作，請選擇「檔案系統一致」。

- 如果您想確保在建立備份之前刷新檔案系統快取數據，請選擇*崩潰一致*。

7. 在「策略」頁面中，執行以下步驟：

- a. 從下拉清單中選擇一個或多個策略。



您可以透過點擊來建立策略 。

在「為選定策略配置計畫」部分中，列出了選定的策略。

- b. 點選  在配置時間表列中為您想要的策略配置時間表。

- c. 在「為政策_policy_name_新增計畫」視窗中，配置計畫，然後選擇 OK。

policy_name 是您選擇的政策的名稱。

配置的計畫列在「已套用的計畫」欄位中。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中選擇您想要傳送電子郵件的場景。

您必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果要附加對資源執行的備份作業的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令指定 SMTP 伺服器詳細資訊 `Set-SmSmtServer`。

9. 查看摘要，然後按一下「完成」。

進入拓樸頁面。

10. 點選*立即備份*。

11. 在備份頁面中，執行以下步驟：

- a. 如果您已對資源套用了多個策略，請從策略下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 按一下“備份”。

12. 透過點選「監視」>「作業」來監視操作進度。

備份 Unix 檔案系統資源組

您可以備份資源組中定義的 Unix 檔案系統。您可以從資源頁面按需備份資源群組。如果資源組附加了策略並配置了計畫，則會根據計畫建立備份。

步驟

1. 在左側導覽窗格中，選擇“資源”，然後從清單中選擇適當的插件。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

3. 在搜尋框中輸入資源組名稱，或按一下 ，然後選擇標籤。

點選  關閉篩選器窗格。

4. 在資源組頁面中，選擇要備份的資源組。

5. 在備份頁面中，執行以下步驟：

a. 如果您有多個與資源群組關聯的策略，請從「策略」下拉清單中選擇要使用的備份策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

b. 選擇*備份*。

6. 透過選擇「監控」>「作業」來監控進度。

監控 Unix 檔案系統備份

了解如何監控備份作業和資料保護作業的進度。

監控 Unix 檔案系統備份操作

您可以使用 SnapCenterJobs 頁面監控不同備份作業的進度。您可能需要檢查進度以確定何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上並指示對應的操作狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在「作業」頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出備份操作。
 - b. 指定開始和結束日期。
 - c. 從「類型」下拉清單中，選擇「備份」。
 - d. 從*狀態*下拉式選單中，選擇備份狀態。
 - e. 點擊“應用”即可查看操作是否已成功完成。

4. 選擇一個備份作業，然後按一下「詳細資料」以查看作業詳細資料。



儘管備份作業狀態顯示 ，當您按一下作業詳細資料時，您可能會看到備份作業的一些子任務仍在進行中或標有警告標誌。

5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

在活動窗格中監視資料保護操作

活動窗格顯示最近執行的五個操作。活動窗格也會顯示操作的啟動時間和操作的狀態。

活動窗格顯示有關備份、復原、複製和排程備份作業的資訊。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 點選  在活動窗格上查看最近的五項操作。

當您按一下其中一個操作時，操作詳細資料將列在「作業詳細資料」頁面中。

在拓樸頁面中查看受保護的 **Unix** 檔案系統

當您準備備份、還原或複製資源時，您可能會發現查看主儲存和輔助儲存上的所有備份、還原的檔案系統和複製的圖形表示很有幫助。

關於此任務

在拓樸頁面中，您可以看到所選資源或資源組可用的所有備份、還原的檔案系統和複製。您可以查看這些備份、還原的檔案系統和克隆的詳細信息，然後選擇它們來執行資料保護操作。

您可以查看「管理副本」檢視中的以下圖標，以確定備份和複製是否在主儲存或輔助儲存（鏡像副本或保管庫副本）上可用。

-  顯示主儲存體上可用的備份和克隆的數量。
-  顯示使用SnapMirror技術在二級儲存上鏡像的備份和克隆的數量。
-  顯示使用SnapVault技術在二級儲存上複製的備份和克隆的數量。

顯示的備份數量包括從輔助儲存中刪除的備份。例如，如果您使用僅保留 4 個備份的策略建立了 6 個備份，則顯示的備份數為 6。



鏡像保管庫類型磁碟區上的版本靈活鏡像的備份的複製顯示在拓撲視圖中，但拓撲視圖中的鏡像備份計數不包括版本靈活備份。

如果您具有作為SnapMirror主動同步的輔助關係（最初是作為SnapMirror業務連續性 [SM-BC] 發布），您可以看到以下附加圖示：

-  副本網站已啟動。
-  副本網站已關閉。
-  輔助鏡像或保險庫關係尚未重新建立。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從資源詳細資料檢視或資源群組詳細資料檢視中選擇資源。

如果資源受到保護，則會顯示所選資源的拓撲頁面。

4. 查看摘要卡以了解主儲存和輔助儲存上可用的備份和複製數量的摘要。

摘要卡部分顯示備份和克隆的總數。

點擊“刷新”按鈕開始查詢儲存以顯示準確的計數。

如果進行了啟用SnapLock的備份，則按一下「刷新」按鈕將刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。每週計劃還會刷新從ONTAP檢索到的主 SnapLock 和輔助SnapLock到期時間。

當檔案系統分佈在多個磁碟區上時，備份的SnapLock到期時間將是磁碟區中快照設定的最長SnapLock到期時間。從ONTAP中檢索最長的SnapLock到期時間。

對於SnapMirror活動同步，按一下「刷新」按鈕可透過查詢主網站和副本網站的ONTAP來刷新SnapCenter備份清單。每週計劃也會針對包含SnapMirror活動同步關係的所有資料庫執行此活動。

- 對於SnapMirror主動同步且僅適用於ONTAP 9.14.1，應在故障轉移後手動配置與新主目標的非同步鏡像或非同步 MirrorVault 關係。從ONTAP 9.15.1 開始，非同步鏡像或非同步 MirrorVault 會自動配置為新的主目標。
 - 故障轉移後，應為SnapCenter建立備份以了解故障轉移。只有在建立備份後，您才可以點選「刷新」。
5. 在「管理副本」檢視中，按一下主儲存或輔助儲存中的「備份」或「複製」以查看備份或複製的詳細資訊。

備份和克隆的詳細資訊以表格形式顯示。

6. 從表中選擇備份，然後按一下資料保護圖示執行復原、複製和刪除操作。



您無法重新命名或刪除輔助儲存體上的備份。

7. 如果要刪除克隆，請從表中選擇克隆，然後按一下  。

顯示主儲存體上的備份和克隆的範例



還原和恢復 Unix 檔案系統

恢復 Unix 檔案系統

如果發生資料遺失，您可以使用SnapCenter恢復 Unix 檔案系統。

關於此任務

- 您應該執行以下命令來與SnapCenter伺服器建立連接，列出備份並檢索其訊息，以及恢復備份。

可以透過執行 `Get-Help command_name` 來取得有關可與命令一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體命令參考指南"](#)。

- 對於SnapMirror活動同步恢復操作，您必須從主位置選擇備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*路徑*或*資源組*。
3. 從詳細資料檢視或資源群組詳細資料檢視中選擇檔案系統。

進入拓樸頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助（鏡像或複製）儲存系統中選擇「備份」。
5. 從表格中選擇備份，然後按一下**。
6. 在「還原範圍」頁面中：

- 對於 NFS 檔案系統，預設選擇“連接和複製”恢復。您也可以選擇*卷恢復*或*快速恢復*。
- 對於非 NFS 檔案系統，復原範圍是根據佈局選擇的。

根據檔案系統類型和佈局，備份後建立的新檔案在復原後可能無法使用。

7. 在 PreOps 頁面中，輸入執行復原作業之前要執行的預復原指令。
8. 在 PostOps 頁面中，輸入執行還原作業後要執行的還原後指令。



您應該檢查這些命令是否存在於插件主機上位於 `_/opt/NetApp/snapcenter/scc/etc/allowed_commands.config_path` 位置的命令清單中。

9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件通知的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的復原作業的報告，您必須選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtptServer` 指定 SMTP 伺服器詳細資訊。

10. 查看摘要，然後按一下「完成」。



如果恢復操作失敗，則不支援回滾。



如果還原位於磁碟區組上的檔案系統，則不會刪除檔案系統上的舊內容。只有克隆檔案系統的內容才會被複製到來源檔案系統。當卷冊組上有多個檔案系統並且預設 NFS 檔案系統恢復時，這適用。

11. 透過點選「監視」>「作業」來監視操作進度。

監控 Unix 檔案系統恢復操作

您可以使用「作業」頁面監控不同SnapCenter還原作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

還原後狀態描述了還原作業之後資源的狀況以及您可以採取的任何進一步還原作業。

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中

-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾清單以便僅列出恢復操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“恢復”。
 - d. 從“狀態”下拉清單中，選擇恢復狀態。
 - e. 按一下「應用」以查看已成功完成的操作。
4. 選擇恢復作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳情」頁面中，按一下「檢視日誌」。

*查看日誌*按鈕顯示所選操作的詳細日誌。

克隆 Unix 檔案系統

克隆 Unix 檔案系統備份

您可以使用SnapCenter透過檔案系統的備份來複製 Unix 檔案系統。

開始之前

- 您可以將位於 `/opt/NetApp/snapcenter/scc/etc` 的 `agent.properties` 檔案中的 `SKIP_FSTAB_UPDATE` 值設為 **true** 來跳過 `fstab` 檔案更新。
- 您可以將位於 `/opt/NetApp/snapcenter/scc/etc` 的 `agent.properties` 檔案中的 `USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT` 的值設為 **true** 來獲得靜態複製磁碟區名稱和連接路徑。更新檔案後，您應該透過執行以下命令重新啟動SnapCenter插件創建者服務：
`/opt/NetApp/snapcenter/scc/bin/scc restart`。

範例：如果沒有此屬性，複製磁碟區名稱和連線路徑將類似於
`<Source_volume_name>_Clone_<Timestamp>`，但現在它將是
`<Source_volume_name>_Clone_<Clone_Name>`

這樣可以保持名稱不變，以便如果您不想透過SnapCenter更新 `fstab`，您可以手動更新 `fstab` 檔案。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*路徑*或*資源組*。
3. 從詳細資料檢視或資源群組詳細資料檢視中選擇檔案系統。

進入拓樸頁面。

4. 從管理副本檢視中，從本機副本（主副本）、鏡像副本（次副本）或保管庫副本（次副本）中選擇備份。
5. 從表格中選擇備份，然後按一下**。
6. 在位置頁面中，執行以下操作：

對於這個領域...	這樣做...
克隆伺服器	預設情況下，來源主機已填入。
克隆掛載點	指定檔案系統的掛載路徑。

7. 在腳本頁面中，執行以下步驟：
 - a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。



您應該檢查這些命令是否存在於插件主機上可用的命令清單中，該清單位於 `/opt/NetApp/snapcenter/scc/etc/allowed_commands.config` 路徑下。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。如果您想要附加執行的複製操作的報告，請選擇*附加作業報告*。



對於電子郵件通知，您必須使用 GUI 或 PowerShell 命令 `Set-SmSmtServer` 指定 SMTP 伺服器詳細資訊。

9. 查看摘要，然後按一下「完成」。
10. 透過點選「監視」>「作業」來監視操作進度。

分裂克隆

您可以使用SnapCenter將克隆資源從父資源中拆分出來。被分割的克隆變得獨立於父資源。

關於此任務

- 您無法對中間克隆執行克隆分割操作。

例如，從資料庫備份建立 clone1 後，您可以建立 clone1 的備份，然後複製此備份（clone2）。創建clone2 後，clone1為中間克隆，無法對clone1進行克隆分裂操作。但是可以對clone2進行克隆分裂操作。

在對 clone2 進行分裂之後，就可以對 clone1 進行克隆分裂操作了，因為 clone1 已經不再是中間克隆了。

- 當您拆分克隆時，克隆的備份副本和克隆作業將被刪除。
- 有關FlexClone磁碟區拆分操作的信息，請參閱 ["將FlexClone磁碟區從其父卷中拆分出來"](#)。
- 確保儲存系統上的磁碟區或聚合處於線上狀態。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在「資源」頁面中，從「檢視」清單中選擇適當的選項：

選項	描述
對於資料庫應用程式	從視圖清單中選擇*資料庫*。
對於檔案系統	從檢視清單中選擇*路徑*。

3. 從清單中選擇適當的資源。

進入資源拓樸頁面。

4. 從“管理副本”視圖中，選擇複製的資源（例如，資料庫或 LUN），然後按一下“*”。
5. 查看要拆分的克隆的估計大小以及聚合上可用的所需空間，然後按一下「開始」。
6. 透過點選「監視」>「作業」來監視操作進度。

如果 SMCORE 服務重新啟動，克隆拆分操作將停止回應。您應該執行 Stop-SmJob cmdlet 來停止複製分割操作，然後重試複製分割作業。

如果您想要更長的輪詢時間或更短的輪詢時間來檢查克隆是否拆分，您可以變更 `_SMCoreServiceHost.exe.config` 檔案中的 `_CloneSplitStatusCheckPollTime_` 參數的值來設定 SMCORE 輪詢克隆拆分操作狀態的時間間隔。該值的單位是毫秒，預設值為 5 分鐘。

例如：

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

如果正在進行備份、復原或另一個克隆拆分，則克隆拆分啟動作業將失敗。僅當正在運行的操作完成後，才應重新啟動克隆拆分操作。

相關資訊

["SnapCenter 克隆或驗證失敗，聚合不存在"](#)

監控 Unix 檔案系統克隆操作

您可以使用「作業」頁面監控 SnapCenter 複製作業的進度。您可能想要檢查操作的進度以確定操作何時完成或是否有問題。

關於此任務

以下圖示出現在「作業」頁面上，指示操作的狀態：

-  進行中
-  成功完成
-  失敗的
-  已完成但有警告，或因警告而無法啟動
-  排隊
-  取消

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「作業」。
3. 在 **Jobs** 頁面中，執行下列步驟：
 - a. 點選  過濾列表以便僅列出克隆操作。
 - b. 指定開始和結束日期。
 - c. 從“類型”下拉清單中，選擇“克隆”。
 - d. 從“狀態”下拉清單中，選擇克隆狀態。
 - e. 點擊“應用”即可查看已成功完成的操作。
4. 選擇複製作業，然後按一下「詳細資料」以查看作業詳細資料。
5. 在「作業詳細資料」頁面中，按一下「查看日誌」。

保護在Azure NetApp Files上運行的應用程式

保護在Azure NetApp Files上運行的應用程式

SnapCenter支援保護駐留在Azure NetApp Files上的應用程式，例如 Oracle、SQL 和 SAP HANA。從 6.0.1 版本開始，SnapCenter支援Azure NetApp Files備份功能，該功能透過為長期復原、存檔和合規性提供完全託管的備份解決方案來擴展Azure NetApp Files的資料保護功能。

Azure NetApp Files是一種進階儲存解決方案，長期備份保留的成本可能較高。為了優化成本，您可以將備份從Azure NetApp Files儲存移至 Azure 物件儲存體。從SnapCenter 6.0.1 開始，您可以將駐留在Azure NetApp Files上的應用程式備份並複製到 Azure Blob 儲存體（物件儲存）。您可以保留資料的兩個副本， Azure NetApp Files儲存上的磁碟區快照副本用於短期恢復， Azure Blob 儲存體上的另一個副本用於長期復原。

當啟用具有Azure NetApp Files備份的政策並將其與資源關聯時， SnapCenter會處理磁碟區快照的建立並將其備份到 Azure Blob 儲存體。 SnapCenter建立備份庫並為磁碟區啟用備份。如果您已啟用磁碟區的備份， SnapCenter將利用現有的保管庫。

限制

- 不支援FAS、ASA或AFF ONTAP以及Amazon FSx for NetApp ONTAP儲存系統的物件儲存功能。
- Oracle 和 SAP HANA 掛載和目錄工作流程不支援物件儲存備份，但支援快照。
- Oracle PDB 克隆不支援物件儲存備份，但支援快照。
- 不支援來自物件儲存的備份驗證、REST API 支援、來自物件儲存的複製生命週期管理以及物件儲存備份的報告功能。
- 不支援從 Azure Blob 儲存體上的備份還原到Azure NetApp Files。您也可以使用克隆選項。
- 不支援克隆拆分。

安裝SnapCenter並建立憑證

在 Azure 虛擬機器上安裝SnapCenter

您可以從NetApp支援網站下載SnapCenter software並在 Azure 虛擬機器上安裝軟體。

開始之前

- 確保 Azure Windows 虛擬機器符合SnapCenter Server 安裝的需求。有關信息，請參閱["安裝SnapCenter伺服器的要求"](#)。
- 如果您是Azure NetApp Files 的新使用者且沒有現有的NetApp帳戶，請確保您已註冊，以便可以存取SnapCenter軟體。更多信息，請參閱["註冊以存取SnapCenter software"](#)。

步驟

1. 從下列位置下載SnapCenter Server 安裝包 ["NetApp支援站點"](#)。
2. 雙擊下載的 .exe 檔案啟動SnapCenter Server 安裝。

啟動安裝後，將執行所有預檢查，如果不符合最低要求，則會顯示相應的錯誤或警告訊息。您可以忽略警告訊息並繼續安裝；但是，錯誤應該得到修復。

3. 查看SnapCenter伺服器安裝所需的預先填入值並根據需要進行修改。

您不必指定 MySQL 伺服器儲存庫資料庫的密碼。在SnapCenter Server 安裝期間，密碼會自動產生。



儲存庫資料庫的自訂路徑不支援特殊字元“%”。如果路徑中包含“%”，安裝將會失敗。

4. 按一下“立即安裝”。

如果您指定的任何值無效，則會顯示相應的錯誤訊息。您應該重新輸入這些值，然後開始安裝。



如果點選*取消*按鈕，正在執行的步驟將會完成，然後開始回溯操作。 SnapCenter伺服器將從主機中完全刪除。

但是，如果在執行“SnapCenter Server 網站重新啟動”或“等待SnapCenter Server 啟動”操作時按一下“取消”，則安裝將繼續進行而不會取消操作。

註冊產品以獲得支持

如果您是NetApp新用戶且沒有現有的NetApp帳戶，則應該註冊該產品以獲得支援。

步驟

1. 安裝SnapCenter後，導覽至 幫助 > 關於。
2. 在「關於 SnapCenter」對話方塊中，記下SnapCenter實例，這是一個以 971 開頭的 20 位數。
3. 點選 <https://register.netapp.com>。
4. 點擊“我不是註冊的NetApp客戶”。
5. 指定您的詳細資料以進行註冊。
6. 將NetApp參考 SN 欄位留空。
7. 從產品線下拉式選單中選擇* SnapCenter*。
8. 選擇計費提供者。
9. 輸入 20 位元SnapCenter執行個體 ID。
10. 點選“提交”。

在SnapCenter中建立 Azure 憑證

您應該在SnapCenter中建立 Azure 憑證來存取 Azure NetApp帳戶。

開始之前

- 確保您已在 Azure 中建立服務主體。
- 確保您擁有與服務主體關聯的租用戶 ID、客戶端 ID 和金鑰。
 - 可以在 Azure 入口網站的 Entra ID 概述頁面上找到租用戶 ID。

- 客戶端 ID 也稱為企業應用程式/服務主體的應用程式 ID。您可以在 Azure 入口網站的概述頁面上找到您建立的作為 SnapCenter 服務主體的企業應用程式。
- 客戶端密鑰也稱為秘密值。您可以透過導覽至 Entra ID 下的 **App registrations** 在 Azure 入口網站中建立此用戶端機密。選擇您建立的企業應用程式後，導覽至*憑證和機密*，然後導覽至*新用戶端機密*。



秘密值只有在創建時才可以存取。您以後將無法訪問它。

- 服務主體需要被授予權限。貢獻者的角色將允許服務主體在 Azure 中執行所需的操作。這可以從訂閱頁面內的存取控制 (IAM) 頁面授予。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定建立憑證所需的下列資訊。

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
認證模式	從下拉清單中選擇“Azure 憑證”。
租戶 ID	輸入租戶 ID。
客戶端 ID	輸入客戶端 ID。
客戶端密鑰	輸入客戶端密鑰。

5. 按一下“確定”。

配置 Azure 儲存體帳戶

您應該在 SnapCenter 中設定 Azure 儲存體帳戶。

Azure 儲存帳戶包含訂閱 ID、Azure 憑證和 Azure NetApp 帳戶的詳細資訊。



Azure NetApp Files 不需要標準授權和基於容量的授權。

步驟

1. 在左側導覽窗格中，按一下「儲存系統」。
2. 在“儲存系統”頁面中，選擇“Azure NetApp Files”，然後按一下“新建”。
3. 從對應的下拉清單中選擇憑證、訂閱 ID 和 NetApp 帳戶。
4. 點選“提交”。

建立憑證以新增插件主機

SnapCenter使用憑證對SnapCenter操作的使用者進行身份驗證。

您應該建立用於安裝SnapCenter插件的憑證以及用於執行資料保護操作的附加憑證。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「憑證」。
3. 點選“新建”。
4. 在「憑證」頁面中，指定建立憑證所需的下列資訊。

對於這個領域...	這樣做...
憑證名稱	輸入憑證的名稱。
認證模式	從下拉清單中選擇身份驗證模式。
身份驗證類型	選擇 基於密碼 或 基於 SSH 金鑰（僅適用於 Linux 主機）。
使用者名稱	指定使用者名稱。
密碼	如果您選擇了基於密碼的身份驗證，請指定密碼。
SSH 私鑰	如果您選擇了基於 SSH 金鑰的身份驗證，請指定私鑰。
使用 sudo 權限	如果您要為非 root 使用者建立憑證，請選取使用 sudo 權限複選框。  這僅適用於 Linux 用戶。

5. 按一下“確定”。

保護 SAP HANA 資料庫

為 **SAP HANA** 資料庫新增主機並安裝SnapCenter插件

您必須使用SnapCenter新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。

開始之前

- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員角色。

- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。
- 如果您在集中式主機上安裝，請確保該主機上安裝了 SAP HANA 用戶端軟體，並在 SAP HANA 資料庫主機上開啟所需的連接埠以遠端執行 HDB SQL 查詢。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證是否選擇了「託管主機」標籤。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：
 - a. 在主機類型欄位中，選擇主機類型。
 - b. 在主機名字段中，輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。
 - c. 在憑證欄位中，輸入您建立的憑證。
5. 在選擇要安裝的插件部分中，選擇要安裝的插件。
6. （可選）點擊“更多選項”並指定詳細資訊。
7. 點選“提交”。
8. 如果主機類型為Linux，請驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。

9. 監控安裝進度。

新增 SAP HANA 資料庫

您應該手動新增 SAP HANA 資料庫。

關於此任務

如果插件安裝在集中式伺服器上，則需要手動新增資源。如果 HANA 資料庫主機上安裝了 SAP HANA 插件，則會自動發現 HANA 系統。



HANA 多主機配置不支援自動發現，必須僅透過集中插件新增。

步驟

1. 在左側導覽窗格中，從下拉清單中選擇適用於 SAP HANA 資料庫的SnapCenter插件，然後按一下「資源」。
2. 在資源頁面中，按一下*新增 SAP HANA 資料庫*。
3. 在提供資源詳細資訊頁面中，執行以下操作：
 - a. 輸入資源類型為單一容器、多租用戶資料庫容器或非資料磁碟區。
 - b. 輸入 SAP HANA 系統名稱。
 - c. 輸入系統 ID (SID)。
 - d. 選擇插件主機。

- e. 輸入密鑰以連接到 SAP HANA 系統。
 - f. 輸入配置了 HDB 安全用戶儲存金鑰的使用者名稱。
4. 在「提供儲存佔用空間」頁面中，選擇「Azure NetApp Files」作為儲存類型。
 - a. 選擇 Azure NetApp帳戶。
 - b. 選擇容量池和關聯的磁碟區。
 - c. 點選“儲存”。
 5. 查看摘要，然後按一下「完成」。

為 SAP HANA 資料庫建立備份策略

在使用SnapCenter備份 SAP HANA 資料庫資源之前，您必須為要備份的資源或資源群組建立備份原則。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選“新建”。
4. 在名稱頁面中，輸入策略名稱和描述。
5. 在「策略類型」頁面中，執行下列步驟：
 - a. 選擇“Azure NetApp Files”作為儲存類型。
 - b. 如果要執行資料庫的完整性檢查，請選擇「基於檔案」。
 - c. 如果您想使用快照技術建立備份，請選擇*基於快照*。
6. 在快照和備份頁面中，執行下列步驟：
 - a. 選擇計劃備份的頻率。
 - b. 指定保留設定。
 - c. 如果要啟用Azure NetApp Files備份，請選擇「啟用備份」並指定保留設定。
7. 查看摘要並點擊“完成”。

建立資源組並附加 SAP HANA 備份策略

資源組是您必須新增要備份和保護的資源的容器。

資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

- 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。
- 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
- 在「策略」頁面中，執行以下步驟：
 - 從下拉清單中選擇一個或多個策略。
 - 在配置計劃列中，按一下 *  * 您想要配置的策略。
 - 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。
- 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
- 查看摘要，然後按一下「完成」。

備份在Azure NetApp Files上執行的 SAP HANA 資料庫

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

步驟

- 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。
- 選擇要備份的資源。
- 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。
- 在應用程式設定頁面中，執行以下操作：
 - 選擇*備份*箭頭來設定其他備份選項。
 - 選擇「腳本」箭頭來執行靜默、快照和取消靜默操作的前置和後置命令。
 - 選擇*自訂配置*箭頭，然後輸入使用此資源的所有作業所需的自訂值對。
 - 選擇*Snapshot Copy Tool > SnapCenter without File System Consistency*來建立快照。

*檔案系統一致性*選項僅適用於 Windows 主機上執行的應用程式。
- 在「策略」頁面中，執行以下步驟：
 - 從下拉清單中選擇一個或多個策略。
 - 選擇 *  * 在您想要設定計畫的政策的政策設定計畫列中。

- c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。

7. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*中配置 SMTP。

8. 查看摘要，然後選擇*完成*。

9. 選擇*立即備份*。

10. 在備份頁面中，執行以下步驟：

- a. 如果多個策略與資源關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

11. 選擇*備份*。

12. 透過點選「監視」>「作業」來監視操作進度。

備份 SAP HANA 資源組

資源組是主機上的資源的集合。資源組上的備份作業會針對資源組中定義的所有資源執行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。

2. 在資源頁面中，從*視圖*清單中選擇*資源組*。

3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。

4. 在備份頁面中，執行以下步驟：

- a. 如果多個策略與資源組關聯，請從「策略」下拉清單中選擇要用於備份的策略。

如果為按需備份選擇的策略與備份計畫相關聯，則按需備份將根據為計畫類型指定的保留設定進行保留。

- b. 選擇*備份*。

5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

還原和還原 SAP HANA 資料庫

您可以從備份中還原資料。

關於此任務

對於自動發現的 HANA 系統，如果選擇了「完整資源」選項，則使用單一檔案快照復原技術執行復原。如果選取「快速復原」複選框，則使用磁碟區復原技術。

對於手動新增的資源，請始終使用 Volume Revert 技術。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。
3. 選擇資源或選擇資源組，然後選擇該組中的資源。
4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或保管）中選擇「備份」。
5. 在主備份表中，選擇要從中還原的備份，然後按一下 *  *。
6. 在「復原範圍」頁面中，選擇「完整資源」。

SAP HANA 資料庫的所有設定資料磁碟區均已復原。

7. 對於自動發現的 HANA 系統，在「復原範圍」頁面中執行下列操作：
 - a. 如果您想要盡可能接近當前時間恢復，請選擇*恢復到最近狀態*。
 - b. 如果要恢復到指定的時間點，請選擇*恢復到時間點*。
 - c. 如果要還原到特定的資料備份，請選擇*還原到指定的資料備份*。
 - d. 如果您現在不想恢復，請選擇「不恢復」。
 - e. 指定日誌備份位置。
 - f. 指定備份目錄位置。
8. 在「Pre ops」頁面中，輸入執行復原作業之前要執行的預先復原和卸載命令。
9. 在 Post ops 頁面中，輸入執行還原作業後要執行的 mount 和 post restore 指令。
10. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

您也必須指定寄件者和收件者的電子郵件地址以及電子郵件的主題。也必須在*設定* > *全域設定*頁面上設定 SMTP。

11. 查看摘要，然後按一下「完成」。
12. 透過點選「監視」>「作業」來監視操作進度。

克隆 SAP HANA 資料庫備份

您可以使用 SnapCenter 透過資料庫備份克隆 SAP HANA 資料庫。創建的克隆是厚克隆，是在父容量池上創建的。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，根據資源類型從*檢視*下拉清單中過濾資源。
3. 選擇資源或資源組。
4. 從「管理副本」檢視中，從主儲存系統中選擇「備份」。
5. 從表中選擇資料備份，然後按一下 。

6. 在位置頁面中，執行以下操作：

- a. 選擇安裝了 SAP HANA 插件的主機，用於管理複製的 HANA 系統。

它可以是集中式插件主機，也可以是HANA系統主機。



如果 HANA 外掛程式安裝在管理其他主機上的 HANA 資料庫的集中式主機上，則在建立或刪除複製時，SnapCenter會故意跳過主機端操作（掛載或卸載檔案系統），因為目標伺服器是集中式主機。您應該使用自訂的克隆前或克隆後腳本來執行掛載和卸載操作。

- a. 輸入要從現有備份複製的 SAP HANA SID。
- b. 輸入將會匯出複製磁碟區的 IP 位址或主機名稱。
- c. 如果 SAP HANA 資料庫 ANF 磁碟區是在手動 QOS 容量池中設定的，請指定複製磁碟區的 QOS。

如果未指定複製磁碟區的 QOS，則會使用來源磁碟區的 QOS。如果使用自動QOS容量池，則指定的QOS值將被忽略。

7. 在腳本頁面中，執行以下步驟：

- a. 輸入分別應在克隆操作之前或之後運行的預克隆或後克隆命令。
- b. 輸入 mount 指令將檔案系統掛載到主機。

如果來源 HANA 系統自動發現，且複製目標主機外掛程式安裝在 SAP HANA 主機上，則SnapCenter會自動卸載複製目標主機上的現有 HANA 資料卷，並安裝新複製的 HANA 資料磁碟區。

8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
9. 查看摘要，然後按一下「完成」。
10. 透過點選「監視」>「作業」來監視操作進度。



克隆分割對於 ANF 克隆是停用的，因為 ANF 克隆已經是從所選快照建立的獨立磁碟區。

保護 Microsoft SQL Server 資料庫

新增主機並為 **SQL Server** 資料庫安裝**SnapCenter**插件

SnapCenter支援Azure NetApp Files上 SMB 共用上的 SQL 執行個體的資料保護。支援獨立和可用性群組 (AG) 配置。

您必須使用SnapCenter新增主機頁面來新增主機，然後安裝插件包。插件會自動安裝在遠端主機上。

開始之前

- 您必須是分配有插件安裝和卸載權限的角色的用戶，例如SnapCenter管理員角色。
- 在 Windows 主機上安裝插件時，如果指定非內建的憑證，或使用者屬於本機工作群組用戶，則必須在主機上停用 UAC。

步驟

1. 在左側導覽窗格中，選擇*主機*。
2. 驗證頂部的「託管主機」標籤是否已選取。
3. 選擇“新增”。
4. 在「主機」頁面中執行以下操作：
 - a. 在主機類型欄位中，選擇主機類型。
 - b. 在主機名字段中，輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。
 - c. 在憑證欄位中，輸入您建立的憑證。
5. 在*選擇要安裝的插件*部分中，選擇要安裝的插件。
6. (可選) 點擊“更多選項”並指定詳細資訊。
7. 選擇*提交*。
8. 選擇*設定日誌目錄*，在設定主機日誌目錄頁面中輸入主機日誌目錄的SMB路徑，點選*儲存*。
9. 點擊*提交*並監控安裝進度。

為 SQL Server 資料庫建立備份策略

您可以在使用SnapCenter備份 SQL Server 資源之前為資源或資源群組建立備份策略，也可以在建立資源群組或備份單一資源時建立備份原則。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 點選“新建”。
4. 在名稱頁面中，輸入策略名稱和描述。
5. 在「策略類型」頁面中，執行下列步驟：
 - a. 選擇“Azure NetApp Files”作為儲存類型。
 - b. 選擇備份類型。
 - i. 如果要備份資料庫檔案和交易日誌，請選擇「完整備份和日誌備份」。
 - ii. 如果您只想備份資料庫文件，請選擇“完整備份”。
 - iii. 如果您只想備份交易日誌，請選擇「日誌備份」。
 - iv. 如果您想使用其他應用程式備份您的資源，請選擇*僅複製備份*。
 - c. 在可用性群組設定部分中，執行以下操作：
 - i. 如果您只想在副本上備份，請選擇在首選備份副本上備份。
 - ii. 選擇主 AG 副本或輔助 AG 副本進行備份。
 - iii. 選擇備份優先權。
6. 在快照和備份頁面中，執行下列步驟：
 - a. 選擇計劃備份的頻率。

- b. 根據所選的備份類型指定保留設定。
- c. 如果要啟用 Azure NetApp Files 備份，請選擇「啟用備份」並指定保留設定。

7. 在驗證頁面中，執行以下步驟：

- a. 在「執行以下備份計畫的驗證」部分中，選擇計畫頻率。
- b. 在資料庫一致性檢查選項部分中，執行下列操作：
 - i. 選擇*將完整性結構限制為資料庫的實體結構（PHYSICAL_ONLY）*以將完整性檢查限制為資料庫的實體結構，並偵測影響資料庫的頁面撕裂、校驗和失敗以及常見硬體故障。
 - ii. 選擇*抑制所有訊息（NO_INFOMSGS）*以抑制所有訊息。

預設選擇。

- iii. 選擇*顯示每個物件報告的所有錯誤訊息（ALL_ERRORMSG）*以顯示每個物件報告的所有錯誤。
- iv. 如果不想檢查非聚集索引，請選擇「不檢查非聚集索引（NOINDEX）」。

SQL Server 資料庫使用 Microsoft SQL Server 資料庫一致性檢查器 (DBCC) 來檢查資料庫中物件的邏輯和實體完整性。

- v. 選擇*限制檢查並取得鎖定而不是使用內部資料庫快照副本（TABLOCK）*來限制檢查並取得鎖定而不是使用內部資料庫快照。
- c. 在*日誌備份*部分中，選擇*完成後驗證日誌備份*以在完成後驗證日誌備份。
- d. 在*驗證腳本設定*部分中，分別輸入在驗證操作之前或之後應執行的腳本或後腳本的路徑和參數。

8. 查看摘要並點擊“完成”。

建立資源組並附加 SQL 備份策略

資源組是您必須新增要備份和保護的資源的容器。

資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。

4. 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。
5. 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
6. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。
 - b. 在配置計劃列中，按一下 *  * 您想要配置的策略。
 - c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。
 - d. 選擇 Microsoft SQL Server 排程器。
7. 在驗證頁面中，執行以下步驟：
 - a. 選擇驗證伺服器。
 - b. 選擇您要設定驗證計劃的策略，然後按一下*  *.
 - c. 選擇*備份後執行驗證*或*執行計劃驗證*。
 - d. 按一下“確定”。
8. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
9. 查看摘要，然後按一下「完成」。

備份在Azure NetApp Files上執行的 SQL Server 資料庫

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

開始之前

如果 Azure Windows 故障轉移叢集沒有指派叢集 IP 或無法從SnapCenter存取，則應該建立負載平衡器。應配置負載平衡器的 IP 並使其可從SnapCenter伺服器存取。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖下拉清單中選擇*資料庫*、*實例*或*可用性群組*。
3. 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。
4. 在「策略」頁面中，執行以下步驟：
 - a. 從下拉清單中選擇一個或多個策略。
 - b. 選擇 *  * 在您要設定計畫的政策的政策設定計畫列中。
 - c. 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後選擇*確定*。

policy_name 是您選擇的政策的名稱。
 - d. 選擇“使用 Microsoft SQL Server 排程器”，然後從與排程原則關聯的“排程器實例”下拉清單中選擇排程器實例。
5. 在驗證頁面中，執行以下步驟：

- a. 選擇驗證伺服器。
 - b. 選擇您要設定驗證計劃的策略，然後按一下*  *.
 - c. 選擇*備份後執行驗證*或*執行計劃驗證*。
 - d. 按一下“確定”。
6. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
 7. 查看摘要，然後按一下「完成」。
 8. 選擇*立即備份*。
 9. 在備份頁面中，執行以下步驟：
 - a. 如果多個策略與資源關聯，請從「策略」下拉清單中選擇要用於備份的策略。
 - b. 選擇*備份後驗證*。
 - c. 選擇*備份*。
 10. 透過點選「監視」>「作業」來監視操作進度。

備份 SQL Server 資源組

您可以備份由多個資源組成的資源組。資源組上的備份作業會針對資源組中定義的所有資源執行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：
 - a. 如果多個策略與資源組關聯，請從「策略」下拉清單中選擇要用於備份的策略。
 - b. 備份後，選擇*驗證*來驗證按需備份。
 - c. 選擇*備份*。
5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

還原和還原 SQL Server 資料庫

您可以使用SnapCenter來還原備份的 SQL Server 資料庫。資料庫復原是一個多階段過程，將所有資料和日誌頁從指定的 SQL Server 備份複製到指定的資料庫。

關於此任務

您應該確保要恢復的目標實例配置了屬於 SMB ADactive 目錄域的活動目錄用戶，並且該用戶具有適當設定文件權限的權限。您應該在執行個體層級配置SnapCenter中的憑證。

SMB 設定不支援目標執行個體的 SQL 驗證。應在SnapCenter中配置目標實例，並讓活動目錄使用者俱有所需的權限。

如果SnapCenter插件服務服務帳戶不是活動目錄用戶，則在執行還原到備用主機時，需要對來源磁碟區具有完全控制權的用戶，以便可以模擬並執行所需的操作。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 從清單中選擇資料庫或資源組。
4. 從「管理副本」檢視中，從儲存系統中選擇「備份」。
5. 從表中選擇備份，然後按一下  圖示。
6. 在「還原範圍」頁面中，選擇下列選項之一：
 - a. 如果要將資料庫還原到已建立備份的相同 SQL 伺服器，請選擇「將資料庫還原到建立備份的相同主機」。
 - b. 如果您希望將資料庫還原到與備份相同的或不同的主機中的不同 SQL 伺服器，請選擇「將資料庫還原到備用主機」。
7. 在「恢復範圍」頁面中，選擇以下選項之一：
 - a. 當您只需要還原完整備份而不還原任何日誌時，請選擇「無」。
 - b. 選擇*所有日誌備份*最新備份還原作業，在完整備份後還原所有可用的日誌備份。
 - c. 選擇「按日誌備份」執行時間點還原作業，該操作會根據備份日誌還原資料庫，直到選定日期的備份日誌。
 - d. 選擇「以特定日期直到」來指定交易日誌不應用於復原資料庫的日期和時間。
 - e. 如果您選擇了“所有日誌備份”、“按日誌備份”或“按特定日期直到”並且日誌位於自訂位置，請選擇“使用自訂日誌目錄”，然後指定日誌位置。
8. 在「操作前」和「操作後」頁面中，指定所需的詳細資訊。
9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
10. 查看摘要，然後按一下「完成」。
11. 使用「監控」>「作業」頁面監控復原過程。

克隆 SQL Server 資料庫備份

您可以使用SnapCenter使用資料庫備份來克隆 SQL 資料庫。創建的克隆是厚克隆，是在父容量池上創建的。

關於此任務

您應該確保複製的目標實例配置了屬於 SMB ADactive 目錄域的活動目錄用戶，並且該用戶有權適當地設定檔案權限。您應該在執行個體層級配置SnapCenter中的憑證。

SMB 設定不支援目標執行個體的 SQL 驗證。應在SnapCenter中配置目標實例，並讓活動目錄使用者俱有所需的權限。

如果SnapCenter插件服務服務帳戶不是活動目錄用戶，則在執行複製時，需要對來源磁碟區具有完全控制權的用戶，以便可以模擬並執行所需的操作。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 選擇資料庫或資源組。
4. 從*管理副本*視圖頁面中，選擇來自主儲存系統的備份。
5. 選擇備份，然後選擇**。
6. 在*克隆選項*頁面中，提供所有必需的詳細資訊。
7. 在位置頁面中，選擇用於建立複製的儲存位置。

如果在手動 QOS 容量池中設定了 SQL Server 資料庫 ANF 卷，請指定複製卷的 QOS。

如果未指定複製磁碟區的 QOS，則會使用來源磁碟區的 QOS。如果使用自動QOS容量池，則指定的QOS值將被忽略。

8. 在日誌頁面中，選擇以下選項之一：
 - a. 如果您只想克隆完整備份而不克隆任何日誌，請選擇「無」。
 - b. 如果要複製完整備份之後的所有可用日誌備份，請選擇「所有日誌備份」。
 - c. 如果要根據截至選定日期的備份日誌所建立的備份日誌來複製資料庫，請選擇「按日誌備份直至」。
 - d. 如果您不想在指定日期和時間之後套用交易日誌，請選擇*按特定日期直到*。
9. 在*腳本*頁面中，分別輸入腳本逾時、路徑以及複製操作之前或之後應執行的預腳本或後腳本的參數。
10. 在*通知*頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
11. 查看摘要，然後選擇*完成*。
12. 透過選擇 **Monitor > Jobs** 來監控操作進度。

執行複製生命週期

使用SnapCenter，您可以從資源組或資料庫建立克隆。您可以執行按需克隆，也可以安排資源群組或資料庫的重複克隆操作。如果您定期複製備份，則可以使用該複製來開發應用程式、填充資料或還原資料。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資料庫*或*資源組*。
3. 選擇資料庫或資源組。
4. 從*管理副本*視圖頁面中，選擇來自主儲存系統的備份。
5. 選擇備份，然後選擇**。
6. 在*克隆選項*頁面中，提供所有必需的詳細資訊。
7. 在位置頁面中，選擇用於建立複製的儲存位置。

如果在手動 QOS 容量池中設定了 SQL Server 資料庫 ANF 卷，請指定複製卷的 QOS。

如果未指定複製磁碟區的 QOS，則會使用來源磁碟區的 QOS。如果使用自動QOS容量池，則指定的 QOS值將被忽略。

8. 在*腳本*頁面中，分別輸入腳本逾時、路徑以及複製操作之前或之後應執行的預腳本或後腳本的參數。
9. 在「計劃」頁面中，執行下列其中一項操作：
 - 如果您想立即執行複製作業，請選擇*立即執行*。
 - 當您想要確定克隆操作發生的頻率、克隆計劃的開始時間、克隆操作發生的日期、計劃的到期時間以及計劃到期後是否必須刪除克隆時，請選擇*配置計劃*。
10. 在*通知*頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
11. 查看摘要，然後選擇*完成*。
12. 透過選擇 **Monitor > Jobs** 來監控操作進度。

保護 Oracle 資料庫

新增主機並為 Oracle 資料庫安裝SnapCenter插件

您可以使用「新增主機」頁面新增主機，然後安裝適用於 Linux 的SnapCenter插件套件或適用於 AIX 的SnapCenter插件套件。插件會自動安裝在遠端主機上。

您可以為單一主機或叢集新增主機並安裝插件包。如果在叢集（Oracle RAC）上安裝該插件，則該插件將安裝在叢集的所有節點上。對於 Oracle RAC One Node，您應該在主動節點和被動節點上安裝該插件。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證是否選擇了「託管主機」標籤。
3. 按一下“新增”。
4. 在「主機」頁面中，執行下列操作：
 - a. 在主機類型欄位中，選擇主機類型。
 - b. 在主機名字段中，輸入主機的完全限定網域名稱 (FQDN) 或 IP 位址。
 - c. 在憑證欄位中，輸入您建立的憑證。
5. 在選擇要安裝的插件部分中，選擇要安裝的插件。
6. （可選）點擊“更多選項”並指定詳細資訊。
7. 點選“提交”。
8. 驗證指紋，然後按一下*確認並提交*。

在叢集設定中，您應該驗證叢集中每個節點的指紋。

9. 監控安裝進度。

為 Oracle 資料庫建立備份策略

在使用SnapCenter備份 Oracle 資料庫資源之前，您必須為要備份的資源或資源群組建立

備份原則。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 從下拉清單中選擇 Oracle 資料庫。
4. 點選“新建”。
5. 在名稱頁面中，輸入策略名稱和描述。
6. 在「策略類型」頁面中，執行下列步驟：
 - a. 選擇“Azure NetApp Files”作為儲存類型。
 - b. 選擇備份類型為線上備份或離線備份。
 - c. 如果要使用 Oracle Recovery Manager (RMAN) 進行目錄備份，請選擇*使用 Oracle Recovery Manager (RMAN) 進行目錄備份*。
 - d. 如果要在備份後修剪存檔日誌，請選擇*備份後修剪存檔日誌*。
 - e. 指定刪除存檔日誌設定。
7. 在快照和備份頁面中，執行下列步驟：
 - a. 選擇計劃備份的頻率。
 - b. 指定保留設定。
 - c. 如果要啟用 Azure NetApp Files 備份，請選擇「啟用備份」並指定保留設定。
8. 在腳本頁面中，分別輸入要在備份作業之前或之後執行的前置腳本或後置腳本的路徑和參數。
9. 在「驗證」頁面中，選擇要執行驗證作業的備份計劃，並分別輸入要在驗證作業之前或之後執行的前置腳本或後置腳本的路徑和參數。
10. 查看摘要並點擊“完成”。

建立資源組並附加 **Oracle** 備份策略

資源組是您必須新增要備份和保護的資源的容器。

資源組可讓您同時備份與給定應用程式相關的所有資料。任何資料保護作業都需要資源組。您還必須將一個或多個策略附加到資源組，以定義要執行的資料保護作業的類型。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，按一下「新資源組」。
3. 在名稱頁面中，執行以下操作：

對於這個領域...	這樣做...
Name	輸入資源組的名稱。

對於這個領域...	這樣做...
標籤	輸入一個或多個標籤，以協助您稍後搜尋資源組。
對 Snapshot 副本使用自訂名稱格式	選取此複選框，然後輸入要用於快照名稱的自訂名稱格式。
存檔日誌檔目標	指定存檔日誌檔案的目標。

- 在資源頁面中，從*主機*下拉清單中選擇主機名，從*資源類型*下拉清單中選擇資源類型。
- 從「可用資源」部分中選擇資源，然後按一下右箭頭將其移至「選定資源*」部分。
- 在「策略」頁面中，執行以下步驟：
 - 從下拉清單中選擇一個或多個策略。
 - 在配置計劃列中，按一下 *  * 您想要配置的策略。
 - 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後按一下*確定*。
- 在驗證頁面中，執行以下步驟：
 - 選擇驗證伺服器。
 - 選擇您要設定驗證計劃的策略，然後按一下*  。
 - 選擇*備份後執行驗證*或*執行計劃驗證*。
 - 按一下“確定”。
- 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
- 查看摘要，然後按一下「完成」。

備份在Azure NetApp Files上執行的 Oracle 資料庫

如果資源尚未屬於任何資源群組，您可以從資源頁面備份該資源。

步驟

- 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
- 在資源頁面中，從視圖下拉清單中選擇*資料庫*。
- 在資源頁面中，選擇*使用自訂名稱格式作為 Snapshot 副本*，然後輸入要用於 Snapshot 名稱的自訂名稱格式。
- 在「策略」頁面中，執行以下步驟：
 - 從下拉清單中選擇一個或多個策略。
 - 選擇 *  * 在您想要設定計畫的政策的政策設定計畫列中。
 - 在為政策_policy_name_新增計劃對話方塊中，配置計劃，然後選擇*確定*。
- 在驗證頁面中，執行以下步驟：

- a. 選擇驗證伺服器。
 - b. 選擇您要設定驗證計劃的策略，然後按一下*  *.
 - c. 選擇*備份後執行驗證*或*執行計劃驗證*。
 - d. 按一下“確定”。
6. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
 7. 查看摘要，然後按一下「完成」。
 8. 選擇*立即備份*。
 9. 在備份頁面中，執行以下步驟：
 - a. 如果多個策略與資源關聯，請從「策略」下拉清單中選擇要用於備份的策略。
 - b. 按一下“備份”。
 10. 透過點選「監視」>「作業」來監視操作進度。

備份 Oracle 資源組

您可以備份由多個資源組成的資源組。資源組上的備份作業會針對資源組中定義的所有資源執行。

步驟

1. 在左側導覽窗格中，選擇*資源*，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 在資源組頁面中，選擇要備份的資源組，然後選擇*立即備份*。
4. 在備份頁面中，執行以下步驟：
 - a. 如果多個策略與資源組關聯，請從「策略」下拉清單中選擇要用於備份的策略。
 - b. 選擇*備份*。
5. 透過選擇 **Monitor > Jobs** 來監控操作進度。

還原和還原 Oracle 資料庫

如果發生資料遺失，您可以使用SnapCenter將資料從一個或多個備份還原到活動檔案系統，然後還原資料庫。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 從清單中選擇資料庫或資源組。
4. 從「管理副本」檢視中，從主儲存系統中選擇「備份」。
5. 從表格中選擇備份，然後按一下*  *.

6. 在「還原範圍」頁面中，執行下列任務：
 - a. 如果您已選擇 RAC 環境中資料庫的備份，請選擇 RAC。
 - b. 執行以下操作：
 - i. 如果您只想恢復資料庫文件，請選擇“所有資料文件”。
 - ii. 如果您只想恢復表空間，請選擇「表空間」。
 - iii. 如果要還原 Data Guard 備用資料庫或 Active Data Guard 備用資料庫的重做日誌文件，請選擇「重做日誌檔案」。
 - iv. 選擇*可插拔資料庫*並指定要復原的 PDB。
 - v. 選擇*可插入資料庫 (PDB) 表空間*，然後指定要復原的 PDB 和該 PDB 的表空間。
 - vi. 如果要將資料庫還原到已建立備份的相同 SQL 伺服器，請選擇「將資料庫還原到建立備份的相同主機」。
 - vii. 如果您希望將資料庫還原到與備份相同的或不同的主機中的不同 SQL 伺服器，請選擇「將資料庫還原到備用主機」。
 - viii. 選擇*如果需要還原和復原則變更資料庫狀態*將資料庫的狀態變更為執行還原和復原作業所需的狀態。
 - ix. 如果要在備份後新增資料檔案或在 LVM 磁碟組中新增、刪除或重新建立 LUN 的情況下執行就地還原，請選擇「強制就地還原」。
7. 在「恢復範圍」頁面中，選擇以下選項之一：
 - a. 如果您想恢復到最後一個事務，請選擇「所有日誌」。
 - b. 如果要恢復到特定的 SCN，請選擇*直到 SCN（系統變更號碼）*。
 - c. 如果要恢復到特定的日期和時間，請選擇*日期和時間*。
 - d. 如果您不想恢復，請選擇*不恢復*。
 - e. 如果要指定外部存檔日誌檔案的位置，請選擇*指定外部存檔日誌位置*。
8. 在「操作前」和「操作後」頁面中，指定所需的詳細資訊。
9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
10. 查看摘要，然後按一下「完成」。
11. 透過點選「監視」>「作業」來監視操作進度。

使用時間點復原來還原和還原表空間

您可以還原已損壞或刪除的表空間的子集，而不會影響資料庫中的其他表空間。SnapCenter使用 RMAN 執行表空間的時間點復原 (PITR)。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 選擇單一實例（多租用戶）類型的資料庫。
4. 從管理副本檢視中，從儲存系統中選擇*備份*。

如果備份未編入目錄，您應該選擇該備份並點擊*目錄*。

5. 選擇已編目的備份，然後按一下 *  *。
6. 在「還原範圍」頁面中，執行下列任務：
 - a. 如果您已選擇 RAC 環境中資料庫的備份，請選擇 **RAC**。
 - b. 如果您只想恢復表空間，請選擇「表空間」。
 - c. 選擇*如果需要還原和復原則變更資料庫狀態*將資料庫的狀態變更為執行還原和復原作業所需的狀態。
7. 在「恢復範圍」頁面中，選擇以下選項之一：
 - a. 如果要恢復到特定的 SCN，請選擇*直到 SCN（系統變更號碼）*。
 - b. 如果要恢復到特定的日期和時間，請選擇*日期和時間*。
8. 在「操作前」和「操作後」頁面中，指定所需的詳細資訊。
9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
10. 查看摘要，然後按一下「完成」。
11. 使用「監控」>「作業」頁面監控復原過程。

使用時間點復原來恢復可插拔資料庫

您可以還原和還原已損壞或刪除的可插拔資料庫 (PDB)，而不會影響容器資料庫 (CDB) 中的其他 PDB。SnapCenter 使用 RMAN 執行 PDB 的時間點復原 (PITR)。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 選擇單一實例（多租用戶）類型的資料庫。
4. 從管理副本檢視中，從儲存系統中選擇*備份*。

如果備份未編入目錄，您應該選擇該備份並點擊*目錄*。

5. 選擇已編目的備份，然後按一下 *  *。
6. 在「還原範圍」頁面中，執行下列任務：
 - a. 如果您已選擇 RAC 環境中資料庫的備份，請選擇 **RAC**。
 - b. 根據您是否要還原 PDB 或 PDB 中的表空間，執行下列其中一項操作：
 - 如果要還原 PDB，請選擇*可插拔資料庫 (PDB)*。
 - 如果要在 PDB 中還原表空間，請選擇*可插入資料庫 (PDB) 表空間*。
7. 在「恢復範圍」頁面中，選擇以下選項之一：
 - a. 如果要恢復到特定的 SCN，請選擇*直到 SCN（系統變更號碼）*。
 - b. 如果要恢復到特定的日期和時間，請選擇*日期和時間*。
8. 在「操作前」和「操作後」頁面中，指定所需的詳細資訊。
9. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。

10. 查看摘要，然後按一下「完成」。
11. 使用「監控」>「作業」頁面監控復原過程。

克隆 Oracle 資料庫備份

您可以使用 SnapCenter 透過資料庫備份來克隆 Oracle 資料庫。創建的克隆是厚克隆，是在父容量池上創建的。

步驟

1. 在左側導覽窗格中，按一下「資源」，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 選擇資料庫。
4. 從「管理副本」檢視頁面中，選擇來自主儲存系統的備份。
5. 選擇資料備份，然後點擊**。
6. 在名稱頁面中，選擇是否要複製資料庫（CDB 或非 CDB）或複製可插拔資料庫（PDB）。
7. 在位置頁面中，指定所需的詳細資訊。

如果在手動 QOS 容量池中配置了 Oracle 資料庫 ANF 卷，請指定複製卷的 QOS。

如果未指定複製磁碟區的 QOS，則會使用來源磁碟區的 QOS。如果使用自動 QOS 容量池，則指定的 QOS 值將被忽略。

8. 在「憑證」頁面中，執行下列操作之一：
 - a. 對於 sys 使用者的憑證名稱，選擇用於定義複製資料庫的 sys 使用者密碼的憑證。
 - b. 對於 ASM 實例憑證名稱，如果啟用了 OS 驗證以連接到複製主機上的 ASM 實例，請選擇 無。

否則，請選擇使用「sys」使用者或具有適用於複製主機的「sysasm」權限的使用者配置的 Oracle ASM 憑證。

9. 在「Pre-Ops」頁面中指定處方的路徑和參數，並在「資料庫參數設定」部分中修改用於初始化資料庫的預先填入資料庫參數的值。
10. 在 Post-Ops 頁面中，預設選擇 **Recover database** 和 **Until Cancel** 來執行克隆資料庫的復原。
 - a. 如果您選擇“直到取消”， SnapCenter 將透過安裝最新的日誌備份來執行恢復，該日誌備份具有在選擇進行複製的資料備份之後的不間斷存檔日誌序列。
 - b. 如果選擇“日期和時間”， SnapCenter 將恢復到指定日期和時間的資料庫。
 - c. 如果選擇“直到 **SCN**”， SnapCenter 會將資料庫還原到指定的 SCN。
 - d. 如果您選擇“指定外部存檔日誌位置”， SnapCenter 將根據指定的 SCN 或選定的日期和時間識別並安裝最佳數量的日誌備份。
 - e. 預設情況下，選取「建立新 **DBID**」複選框，為複製的資料庫產生一個唯一的編號（DBID），以區別於來源資料庫。

如果要將來源資料庫的 DBID 指派給複製的資料庫，請清除該核取方塊。在這種情況下，如果您想將複製的資料庫註冊到來源資料庫已註冊的外部 RMAN 目錄，則操作會失敗。

- f. 如果要為克隆資料庫的預設臨時表空間建立臨時文件，請勾選「為臨時表空間建立臨時文件」複選框。
- g. 在*輸入建立複製時要套用的 SQL 項目*中，新增要在建立複製時套用的 SQL 項目。
- h. 在*輸入複製操作後執行的腳本*中，指定複製操作後要執行的後記的路徑和參數。
11. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
12. 查看摘要，然後選擇*完成*。
13. 透過選擇 **Monitor > Jobs** 來監控操作進度。

克隆可插入資料庫

您可以將可插拔資料庫 (PDB) 複製到同一主機或備用主機上不同或相同的目標 CDB。您也可以將克隆的 PDB 還原到所需的 SCN 或日期和時間。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從視圖清單中選擇*資料庫*或*資源組*。
3. 選擇單一實例（多租用戶）類型的資料庫。
4. 從「管理副本」檢視頁面中，選擇來自主儲存系統的備份。
5. 選擇備份，然後按一下**。
6. 在名稱頁面中，選擇*PDB Clone*並指定其他詳細資訊。
7. 在位置頁面中，指定所需的詳細資訊。
8. 在「Pre-Ops」頁面中指定處方的路徑和參數，並在「資料庫參數設定」部分中修改用於初始化資料庫的預先填入資料庫參數的值。
9. 在 Post-Ops 頁面中，預設選擇 **Until Cancel** 來執行複製資料庫的復原。
 - a. 如果您選擇“直到取消”，SnapCenter將透過安裝最新的日誌備份來執行恢復，該日誌備份具有在選擇進行複製的資料備份之後的不間斷存檔日誌序列。
 - b. 如果選擇“日期和時間”，SnapCenter將恢復到指定日期和時間的資料庫。
 - c. 如果您選擇“指定外部存檔日誌位置”，SnapCenter將根據指定的 SCN 或選定的日期和時間識別並安裝最佳數量的日誌備份。
 - d. 預設情況下，選取「建立新 **DBID**」複選框，為複製的資料庫產生一個唯一的編號（DBID），以區別於來源資料庫。

如果要將來源資料庫的 DBID 指派給複製的資料庫，請清除該核取方塊。在這種情況下，如果您想將複製的資料庫註冊到來源資料庫已註冊的外部 RMAN 目錄，則操作會失敗。

- e. 如果要為克隆資料庫的預設臨時表空間建立臨時文件，請勾選「為臨時表空間建立臨時文件」複選框。
- f. 在*輸入建立複製時要套用的 SQL 項目*中，新增要在建立複製時套用的 SQL 項目。
- g. 在*輸入複製操作後執行的腳本*中，指定複製操作後要執行的後記的路徑和參數。
10. 在通知頁面中，從*電子郵件首選項*下拉清單中，選擇您想要傳送電子郵件的場景。
11. 查看摘要，然後選擇*完成*。
12. 透過選擇 **Monitor > Jobs** 來監控操作進度。

管理SnapCenter伺服器 and 插件

查看儀表板

儀表板概覽

從SnapCenter左側導覽窗格中，儀表板可讓您初步了解系統的運作狀況，包括最近的作業活動、警報、保護摘要、儲存效率和使用情況、SnapCenter作業的狀態（備份、複製、還原）、獨立和 Windows 叢集主機的設定狀態、SnapCenter管理的儲存空間 (SVM) 虛擬數量以及授權容量。

儀表板視圖中顯示的資訊取決於指派給目前登入SnapCenter的使用者的角色。如果使用者沒有權限查看某些訊息，則可能不會顯示該內容。

在許多情況下，您可以將滑鼠懸停在 **i** 上來查看有關顯示器的更多資訊。在某些情況下，儀表板顯示中的信息會連結到SnapCenter GUI 頁面中的詳細來源信息，例如資源、監視器和報告。

最近的工作活動

「最近的作業活動」圖塊顯示您有權存取的任何備份、還原和複製作業的最新作業活動。此顯示中的作業具有以下狀態之一：已完成、警告、失敗、正在執行、排隊和已取消。

將滑鼠懸停在某個工作上可以提供更多資訊。您可以透過點擊特定的作業編號來查看其他作業訊息，該編號會將您重新導向到「監視」頁面。從那裡，您可以獲得作業詳細資訊或日誌信息，並產生特定於該作業的報告。

按一下「查看全部」以查看所有SnapCenter作業的歷史記錄。

警報

警報磁貼顯示主機和SnapCenter伺服器的最新未解決的嚴重和警告警報。

嚴重和警告類別警報的總數顯示在顯示器頂部。點擊「嚴重」或「警告」總數會將您重新導向到「警報」頁面，並在「警報」頁面中套用特定的過濾器。

點擊特定警報會將您重定向到「警報」頁面，以查看有關該警報的詳細資訊。點擊顯示器底部的「查看全部」會將您重新導向到「警報」頁面，以查看所有警報的清單。

最新保護摘要

最新保護摘要圖塊為您提供您有權存取的所有實體的保護狀態。預設情況下，顯示設定為提供所有插件的狀態。提供以快照形式備份到主儲存的資源以及使用SnapMirror和SnapVault技術備份到二級儲存的資源的狀態資訊。二級儲存的保護狀態資訊的可用性取決於所選的插件類型。



如果您使用鏡像保管庫保護策略，則保護摘要的計數器將顯示在SnapVault摘要圖表中，而不是SnapMirror圖表中。

透過從下拉式選單中選擇插件，可以查看單一插件的保護狀態。環形圖顯示所選插件的受保護資源百分比。點擊環形圖切片會將您重新導向到「報表」>「外掛」頁面，該頁面提供指定外掛程式所有主儲存和二級儲存活動的詳細報告。



有關二級儲存的報告僅適用於SnapVault；不支援SnapMirror報告。



SAP HANA 為快照的主儲存和輔助儲存提供保護狀態資訊。對於基於檔案的備份，僅主儲存保護狀態可用。

保護狀態	主儲存	二級儲存
失敗的	屬於資源組的實體的數量，其中資源組已執行備份，但備份失敗。	備份未能傳輸至輔助目標的實體數量。
成功的	資源組中已成功備份的實體的數量。	已成功傳輸到輔助目標的具有備份的實體的數量。
未配置	不屬於任何資源組且尚未備份的實體的數量。	屬於一個或多個資源組且未配置為將備份傳送到輔助目標的實體的數量。
未發起	屬於資源組但尚未執行備份的實體的數量。	不適用。



如果您使用SnapCenter Server 4.2 和早期版本的插件（早於 4.2）來建立備份，則 最新保護摘要圖塊不會顯示這些備份的SnapMirror保護狀態。

工作

作業磁貼為您提供了您有權存取的備份、還原和複製作業的摘要。您可以使用下拉式選單自訂任何報告的時間範圍。時間範圍選項固定為過去 24 小時、過去 7 天和過去 30 天。預設報告顯示過去 7 天內執行的資料保護作業。

備份、復原和複製作業資訊顯示在環形圖中。點擊甜甜圈切片會將您重新導向到「監視」頁面，其中作業過濾器已預先套用到選擇。

作業狀態	描述
失敗的	失敗的作業數量。
警告	遇到錯誤的作業數量。
成功的	已成功完成的作業數量。
跑步	目前正在運行的作業數量。

儲存

存儲磁貼顯示 90 天內保護作業所消耗的主儲存和輔助存儲，以圖形方式描繪消耗趨勢，併計算主存儲節省量。儲存資訊每24小時凌晨12點更新一次

當天的消耗總量（包括SnapCenter中可用的備份總數以及這些備份佔用的大小）將顯示在顯示器頂部。一個備份可以有許多與之關聯的快照，並且計數將反映相同的情況。這適用於主快照和次快照。例如，您建立了 10 個備份，其中 2 個由於基於策略的備份保留而被刪除，1 個備份被您明確刪除。因此，將顯示 7 個備份的數量以及這 7 個備份所佔用的大小。

主儲存的儲存節省係數是邏輯容量（複製和快照節省加上消耗的儲存）與主儲存的實體容量的比率。長條圖顯示了儲存節省情況。

此折線圖分別繪製了連續 90 天期間每天的主儲存和二級儲存消耗。將滑鼠懸停在圖表上即可查看每日的詳細結果。



如果您使用SnapCenter Server 4.2 和早期版本的插件（早於 4.2）來建立備份，則 儲存 圖塊不會顯示備份數量、這些備份消耗的儲存空間、快照節省、複製節省和快照大小。

配置

設定磁貼提供SnapCenter正在管理且您有權存取的所有活動獨立主機和 Windows 叢集主機的綜合狀態資訊。這包括與這些主機相關的插件狀態資訊。

點擊「主機」旁邊的數字會將您重新導向到「主機」頁面中的「託管主機」部分。從那裡，您可以獲得所選主機的詳細資訊。

此外，此顯示還顯示了SnapCenter正在管理且您有權存取的獨立ONTAP SVM 和叢集ONTAP SVM 的總和。點擊 SVM 旁邊的數字會將您重新導向到「儲存系統」頁面。從那裡，您可以獲得所選 SVM 的詳細資訊。

主機配置狀態顯示為紅色（嚴重）、黃色（警告）和綠色（活動），以及每種狀態的主機數量。為每個狀態提供狀態訊息。

配置狀態	描述
強制升級	運行不支援的插件且需要升級的主機數量。不受支援的插件與此版本的SnapCenter不相容。
強制遷移	運行不支援的插件且需要遷移的主機數量。不受支援的插件與此版本的SnapCenter不相容。
未安裝任何插件	新增成功但需要安裝插件或插件安裝失敗的主機數量。
暫停	計劃暫停和正在維護的主機數量。
已停止	已啟動但插件服務未運行的主機數量。
主機宕機	已關閉或無法存取的主機數量。
可升級（可選）	可升級新版本插件包的主機數量。
可遷移（可選）	可供遷移較新版本插件的主機數量。

配置狀態	描述
配置日誌目錄	必須配置日誌目錄以便 SCSQL 進行交易日誌備份的主機數量。
配置 VMware 插件	需要新增適用SnapCenter Plug-in for VMware vSphere的主機數量。
未知	已註冊但尚未觸發安裝的主機數量。
跑步	已啟動且正在執行插件的主機數量。對於 SCSQL 插件，需要設定日誌目錄和虛擬機器管理程式。
安裝\解除安裝插件	正在進行插件安裝或卸載的主機數量。

如何查看儀表板上的信息

從SnapCenter左側導覽窗格中，您可以查看各種儀表板磁貼或顯示以及相關的系統詳細資訊。儀表板中可用的顯示數量是固定的，無法變更。每個顯示中提供的內容取決於基於角色的存取控制 (RBAC)。

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 點擊每個顯示器上的活動區域以獲取更多資訊。

例如，按一下「**Jobs**」中的環形圖，會將您重新導向至「監控」頁面以取得有關您的選擇的更多資訊。點擊「保護摘要」中的環形圖，將重定向到「報告」頁面，該頁面可以提供有關您的選擇的更多資訊。

從儀表板請求作業的狀態報告

您可以從儀表板頁面要求有關備份、還原和複製作業的報告。如果您想確定SnapCenter環境中成功或失敗的作業總數，這將非常有用。

步驟

1. 在左側導覽窗格中，按一下“儀表板”
2. 在儀表板中找到「作業」圖塊，然後選擇「備份」、「復原」或「複製」。
3. 使用下拉式選單，選擇您想要取得工作資訊的時間範圍：24 小時、7 天或 30 天。

系統顯示一個涵蓋資料的環形圖。

4. 按一下代表您想要報告的作業資訊的環形切片。

當您按一下環形圖時，您將從儀表板頁面重新導向至監視器頁面。監控頁面顯示您從環形圖中選擇的狀態的作業。

5. 從「監視」頁面清單中，按一下特定作業以選擇它。
6. 在監控頁面頂部，按一下「報告」。

結果

此報告僅顯示您選擇的作業的資訊。您可以查看該報告或將其下載到本機系統。

從儀表板請求保護狀態報告

您可以使用儀表板請求由特定外掛程式管理的資源的保護詳細資訊。資料保護摘要僅考慮資料備份。

步驟

1. 在左側導覽窗格中，按一下「儀表板」。
2. 在儀表板中找到「最新保護摘要」圖塊，然後使用下拉式選單選擇一個插件。

儀表板顯示備份到主儲存的資源的環形圖，如果適用於插件，則顯示備份到輔助儲存的資源的環形圖。



資料保護報告僅適用於特定插件類型。不支援指定*所有插件*。

3. 點選代表您想要報告的狀態的環形切片。

當您按一下環形圖時，您將從儀表板頁面重新導向至報告，然後重新導向至外掛程式頁面。報告僅顯示您選擇的插件的狀態。您可以查看該報告或將其下載到本機系統。



不支援重定向到SnapMirror環形圖和基於檔案的 SAP HANA 備份的報表頁面。

管理 RBAC

SnapCenter可讓您修改角色、使用者和群組。

修改角色

您可以修改SnapCenter角色以刪除使用者或群組並變更與該角色關聯的權限。當您想要變更或消除整個角色使用的權限時，修改角色特別有用。

開始之前

您必須以「SnapCenterAdmin」角色登入。



您無法修改或刪除 SnapCenterAdmin 角色的權限。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「角色」。

3. 在角色名稱欄位中，按一下要修改的角色。
4. 選擇“此角色的所有成員都可以看到其他成員的物件”，使該角色的其他成員在刷新資源清單後可以看到磁碟區和主機等資源。

如果您不希望該角色的成員看到指派給其他成員的對象，請取消選取此選項。



啟用此選項後，如果使用者與建立物件或資源的使用者屬於相同角色，則無需為使用者指派對物件或資源的存取權限。

5. 在角色詳細資料頁面中根據需要變更權限或取消指派成員。
6. 點選“提交”。

修改使用者和群組

您可以修改SnapCenter使用者或群組以變更其角色和資產。

開始之前

您必須以SnapCenter管理員身分登入。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「使用者和造訪」。
3. 從使用者或群組名稱清單中，按一下要修改的使用者或群組。
4. 在使用者或群組詳細資料頁面中，變更角色和資產。
5. 點選“提交”。

管理主機

您可以新增主機並安裝SnapCenter插件包、新增驗證伺服器、刪除主機、遷移備份作業以及更新主機以升級插件包或新增新的插件包。根據您使用的插件，您還可以設定磁碟、管理 SMB 共用、管理啟動器群組 (igroup)、管理 iSCSI 會話以及遷移資料。

您可以執行這些任務...	對於 Microsoft Exchange Server	對於 Microsoft SQL Server	對於 Microsoft Windows	對於 Oracle 資料庫	對於 SAP HANA 資料庫	對於 NetApp 支援的插件	對於 Db2	對於 PostgreSQL	對於 MySQL
新增主機並安裝插件包	是的	是的	是的	是的	是的	是的	是的	是的	是的

您可以執行這些任務...	對於 Microsoft Exchange Server	對於 Microsoft SQL Server	對於 Microsoft Windows	對於 Oracle 資料庫	對於 SAP HANA 資料庫	對於 NetApp 支援的插件	對於 Db2	對於 PostgreSQL	對於 MySQL
更新主機的 ESXi 訊息	不	是的	不	不	不	不	不	不	不
暫停計劃並將主機置於維護模式	是的	是的	是的	是的	是的	是的	是的	是的	是的
透過新增、升級或刪除插件來修改主機	是的	是的	是的	是的	是的	是的	是的	是的	是的
從 SnapCenter 中刪除主機	是的	是的	是的	是的	是的	是的	是的	是的	是的
啟動插件服務（僅適用於 Windows 主機上執行的插件）	是的	是的	是的	不	是的	是的	是的	是的	是的
配置磁碟	不	不	是的	不	不	不	不	不	不
管理 SMB 共享	不	不	是的	不	不	不	不	不	不
管理 iGroups	不	不	是的	不	不	不	不	不	不
管理 iSCSI 會話	不	不	是的	不	不	不	不	不	不

刷新虛擬機器資訊

當 VMware vCenter 憑證發生變更或資料庫或檔案系統主機重新啟動時，您應該刷新虛擬機器資訊。重新整理 SnapCenter 中的虛擬機器資訊將啟動與 VMware vSphere vCenter 的通訊並取得 vCenter 憑證。



基於 RDM 的磁碟由安裝在資料庫主機上的適用於 Microsoft Windows 的 SnapCenter 插件管理。為了管理 RDM，適用於 Microsoft Windows 的 SnapCenter 外掛程式與管理資料庫主機的 vCenter 伺服器進行通訊。

步驟

1. 在 SnapCenter 左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 在「託管主機」頁面中，選擇要更新的主機。
4. 按一下「刷新虛擬機器」。

修改插件主機

安裝插件後，您可以根據需要修改插件主機詳細資料。您可以修改憑證、安裝路徑、外掛程式、適用於 Microsoft SQL Server 的 SnapCenter 程式的日誌目錄詳細資料、群組寄存服務帳戶 (gMSA) 和外掛程式連接埠。



確保插件版本與 SnapCenter 伺服器版本相同。

關於此任務

- 只有在安裝插件後，您才可以修改插件連接埠。
- 升級操作正在進行時，您無法修改插件連接埠。
- 修改插件連接埠時，您應該注意以下連接埠回滾場景：
 - 在獨立設定中，如果 SnapCenter 無法更改其中一個元件的端口，則操作失敗，並且所有元件都將保留舊端口。

如果所有組件的連接埠都已更改，但其中一個元件無法使用新連接埠啟動，則所有元件仍將保留舊連接埠。例如，如果您想更改獨立主機上兩個插件的端口，而 SnapCenter 無法將新端口應用於其中一個插件，則操作將失敗（並顯示相應的錯誤訊息），並且兩個插件都將保留舊端口。
 - 在叢集設定中，如果 SnapCenter 無法變更安裝在其中一個節點上的插件的端口，則操作失敗，並且所有節點都將保留舊端口。

例如，如果插件安裝在叢集設定中的四個節點上，並且其中一個節點的連接埠未更改，則所有節點都會保留舊連接埠。

當插件與 gMSA 一起安裝時，您可以在 更多選項 視窗中進行修改。當沒有 gMSA 安裝外掛程式時，您可以指定 gMSA 帳戶以將其用作插件服務帳戶。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 驗證頂部是否選擇了「託管主機」。
3. 選擇要修改的主機並修改任一個欄位。

一次只能修改一個字段。

4. 點選“提交”。

結果

主機已驗證並新增至SnapCenter伺服器。

啟動或重新啟動插件服務

啟動SnapCenter插件服務可讓您啟動未執行的服務，或重新啟動正在執行的服務。您可能需要在維護完成後重新啟動服務。

您應該確保重新啟動服務時沒有正在執行的作業。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 在「受管主機」頁面中，選擇要啟動的主機。
4. 點選圖示並點選*啟動服務*或*重新啟動服務*。

您可以同時啟動或重新啟動多個主機的服務。

暫停主機維護計劃

當您想要阻止主機執行任何SnapCenter排程作業時，您可以將主機置於維護模式。您應該在升級外掛程式之前或在主機上執行維護任務時執行此操作。



您無法暫停已關閉的主機上的計劃，因為SnapCenter無法與該主機通訊。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 在「託管主機」頁面中，選擇要暫停的主機。
4. 點選圖標，然後按一下「暫停計劃」以將此插件的主機置於維護模式。

您可以同時暫停多個主機的方案。



您不必先停止插件服務。插件服務可以處於運作或停止狀態。

結果

暫停主機上的計劃後，託管主機頁面將在主機的整體狀態欄位中顯示 已暫停。

完成主機維護後，您可以點選「啟動計畫」使主機退出維護模式。您可以同時啟動多個主機的計劃。

資源頁面支援的操作

您可以從資源頁面發現資源並執行資料保護操作。根據您用來管理資源的插件，您可以執行的操作會有所不同。

在資源頁面中，您可以執行下列任務：

您可以執行這些任務...	對於 Microsoft Exchange Server	對於 Microsoft SQL Server	對於 Microsoft Windows	對於 Oracle 資料庫	對於 SAP HANA 資料庫
確定資源是否可用於備份	是的	是的	是的	是的	是的
執行資源的按需備份	是的	是的	是的	是的	是的
從備份還原	是的	是的	是的	是的	是的
克隆備份	不	是的	是的	是的	是的
管理備份	是的	是的	是的	是的	是的
管理複製	不	是的	是的	是的	是的
管理政策	是的	是的	是的	是的	是的
管理儲存連接	是的	是的	是的	是的	是的
掛載備份	不	不	不	是的	不
卸載備份	不	不	不	是的	不
查看詳細信息	是的	是的	是的	是的	是的

管理政策

您可以從資源或資源群組中分離策略，並進行修改、刪除、檢視和複製。

修改策略

當策略附加到資源或資源組時，您可以修改複製選項、快照保留設定、錯誤重試計數或腳本資訊。只有在分離策略後，您才可以修改計劃類型（頻率）。

關於此任務

修改政策中的計劃類型需要額外的步驟，因為SnapCenter伺服器僅在將政策附加到資源或資源群組時註冊計劃類型。

如果你想...	然後...
新增額外的計劃類型	建立新策略並將其附加到必要的資源或資源群組。 例如，如果資源組策略僅指定每小時備份，而您也想新增每日備份，則可以建立具有每日排程類型的策略並將其新增至資源組。資源組將有兩個策略：每小時和每天。
刪除或變更計劃類型	執行以下操作： 1. 將該策略與使用該策略的每個資源和資源群組分開。 2. 修改排程類型。 3. 將該策略重新附加到所有資源和資源群組。 例如，如果某個策略指定每小時備份，而您想要將其變更為每日備份，則必須先分開該策略。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 選擇策略，然後按一下「修改」。
4. 修改訊息，然後按一下「完成」。

分離策略

如果您不再希望策略來管理資源的資料保護，則可以隨時從資源或資源群組中分離這些策略。您必須先分離策略，然後才能刪除它或修改計劃類型。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 選擇資源組，然後按一下「修改資源組」。
4. 在修改資源組精靈的政策頁面中，從下拉清單中清除要分離的策略旁的複選標記。

5. 在精靈的其餘部分對資源組進行任何其他修改，然後按一下「完成」。

刪除策略

如果您不再需要策略，您可能需要刪除它們。

開始之前

如果策略與任何資源或資源組關聯，則應將策略與資源或資源組分開。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「策略」。
3. 選擇該策略，然後按一下“刪除”。
4. 按一下“是”。

管理資源組

您可以對資源組執行各種操作。

您可以執行與資源組相關的下列任務：

- 透過選擇資源組並按一下「修改資源組」來修改資源組，以編輯您在建立資源組時提供的資訊。



您可以在修改資源組的同時變更計劃。但是，要變更計劃類型，您必須修改策略。



如果從資源群組中刪除資源，則目前附加到資源群組的政策中定義的備份保留設定將繼續套用於已刪除的資源。

- 建立資源組的備份。
- 建立備份的克隆。

您可以從 SQL、Oracle、Windows 檔案系統、自訂應用程式和 SAP HANA 資料庫資源或資源群組的現有備份中進行複製。

- 建立資源組的克隆。

此操作僅支援 SQL 資源組（僅包含資料庫）。您可以設定複製資源群組的計畫（複製生命週期）。

- 阻止資源組上的預定操作啟動。
- 刪除資源組。

停止和恢復資源組的操作

您可以暫時禁止在資源組上啟動計劃操作。稍後當您需要時，您可以啟用這些操作。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 選擇資源組並點選*維護*。
4. 按一下“確定”。

如果要還原已置於維護模式的資源組的操作，請選擇該資源組並按一下「生產」。

刪除資源組

如果不再需要保護資源組中的資源，則可以刪除該資源組。您必須確保在從SnapCenter中刪除插件之前刪除資源組。

關於此任務

您應該手動刪除為資源組中的任何資源建立的所有克隆。您可以選擇強制刪除與資源組相關的所有備份、元資料、政策和快照。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*視圖*清單中選擇*資源組*。
3. 選擇資源組，然後按一下“刪除”。
4. 選用：勾選「刪除備份並分離與此資源組關聯的策略」複選框以刪除與該資源組關聯的所有備份、元資料、政策和快照。
5. 按一下“確定”。

管理備份

您可以重新命名和刪除備份。您也可以同時刪除多個備份。

重新命名備份

如果您想提供更好的名稱以提高可搜尋性，您可以重新命名備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從清單中選擇資源或資源組。

進入資源或資源群組拓撲頁面。如果資源或資源組未配置資料保護，則會顯示保護精靈而不是拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統中選擇「備份」。

您不能重新命名輔助儲存系統上的備份。

如果您已使用 Oracle Recovery Manager (RMAN) 對 Oracle 資料庫的備份進行了分類，則無法重新命名這些已分類的備份。

5. 選擇備份，然後按一下 。
6. 在*將備份重新命名為*欄位中，輸入新名稱，然後按一下*確定*。

刪除備份

如果您不再需要備份來進行其他資料保護操作，則可以刪除備份。

開始之前

刪除備份之前，您必須先刪除相關的克隆。



如果備份與複製資源相關聯，則無法刪除該備份。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。
3. 從清單中選擇資源或資源組。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統中選擇「備份」。

您無法刪除輔助儲存系統上的備份。

5. 選擇備份，然後按一下 。

如果您刪除 SAP HANA 資料庫備份，則該備份的關聯 SAP HANA 目錄也會被刪除。



如果刪除了最後剩餘的備份，則無法刪除相關的 HANA 目錄條目。

6. 按一下“確定”。



如果SnapCenter中有一些過時的資料庫備份，但在儲存系統上沒有相應的備份，則必須使用 `remove-smbbackup` 指令清理這些過時的備份項目。如果過時的備份已被編目，它們將從還原目錄資料庫中取消編目。

移除保護

刪除保護將刪除所有備份並分離所有策略。在刪除保護之前，您應該確保備份未被掛載並且沒有複製與備份關聯。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。

2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。

3. 從清單中選擇資源或資源組。

進入資源或資源群組拓撲頁面。

4. 選擇備份並點擊*刪除保護*。

刪除克隆

如果您發現克隆不再需要，您可以刪除它們。

關於此任務

您無法刪除充當其他克隆來源的克隆。

例如，如果生產資料庫是 db1，則資料庫 clone1 是從 db1 的備份克隆的，並且隨後 clone1 受到保護。資料庫 clone2 是從 clone1 的備份克隆而來的。如果您決定刪除 clone1，則必須先刪除 clone2，然後再刪除 clone1。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。

2. 在資源頁面中，從*檢視*下拉清單中選擇資源或資源群組。

3. 從清單中選擇資源或資源組。

進入資源或資源群組拓撲頁面。

4. 從「管理副本」檢視中，從主儲存系統或輔助儲存系統（鏡像或複製）中選擇「複製」。

5. 選擇克隆，然後按一下 。

如果要刪除 SAP HANA 資料庫克隆，請在「刪除克隆」頁面中執行下列操作：

a. 在*Pre clone delete*欄位中，輸入在刪除克隆之前應執行的命令。

b. 在 **Unmount** 欄位中，輸入刪除克隆之前卸載克隆的命令。

6. 按一下“確定”。

完成後

有時檔案系統不會被刪除。您必須透過執行以下命令來增加 CLONE_DELETE_DELAY 參數的值：`./sccli Set-SmConfigSettings`



CLONE_DELETE_DELAY 參數指定完成應用程式複製刪除後，開始刪除檔案系統之前等待的秒數。

修改參數值後，重新啟動SnapCenter插件Loader(SPL) 服務。

監控作業、計畫、事件和日誌

您可以從「監視」頁面監視作業的進度、取得有關排程作業的資訊以及查看事件和日誌。

監控作業

您可以查看有關SnapCenter備份、複製、還原和驗證作業的資訊。您可以根據開始和結束日期、作業類型、資源群組、政策或SnapCenter插件來篩選此視圖。您還可以獲得指定作業的其他詳細資訊和日誌檔案。

您也可以監控與SnapMirror和SnapVault作業相關的作業。



除非您被指派了SnapCenter管理員或其他超級使用者角色，否則您只能監控您建立的與您相關的作業。

您可以執行以下與監控作業相關的任務：

- 監控備份、複製、復原和驗證作業。
- 查看作業詳細資訊和報告。
- 停止預定的作業。

管理計畫的備份作業

從SnapCenter 6.0.1 版本開始，引入了一個新參數 **JobConcurrencyThreshold**，它為可在任何給定時間運行的計劃作業數量設定閾值。這可讓您根據系統硬體配置控制要執行的備份次數。

指派給 **JobConcurrencyThreshold** 的預設值為 0，即停用。如果您在計劃的備份視窗期間觀察到效能下降，則可以透過指派值來啟用。



如果您啟用 **JobConcurrencyThreshold** 來管理並發作業，SnapCenter將不允許您控制備份的順序，且備份可能不會在計畫中指定的時間同時觸發。

步驟

1. 設定位於 *C:\Program Files\NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config* 的 *JobConcurrencyThreshold* 參數的值。
2. 透過點選 IIS > 應用程式集區 > SnapCenter > 重新啟動來回收SnapCenter應用程式集區。
3. 點選 IIS > 網站 > SnapCenter > 重新啟動，重新啟動SnapCenter Web 服務。

管理過時的作業

陳舊的作業是由於SnapCenter中斷或不正確的作業更新而創建的。從SnapCenter 6.0.1 版本開始，引入了預先定義的計劃來清理這些停滯超過 72 小時的陳舊作業。您可以透過編輯可設定參數 **CleanUpStaleJobsIntervalHours** 來變更計劃頻率。

您可以從 **Monitor > Schedules > SnapCenter_StaleJobCleanUp** 執行計畫來按需觸發清理。

步驟

1. 設定位於 *C:\Program Files\NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config* 的 *CleanUpStaleJobsIntervalHours* 參數的值。

2. 透過點選 IIS > 應用程式集區 > SnapCenter > 重新啟動來回收SnapCenter應用程式集區。
3. 點選 IIS > 網站 > SnapCenter > 重新啟動，重新啟動SnapCenter Web 服務。

監控時間表

您可能想要查看當前計劃以確定操作何時開始、上次運行的時間以及下次運行的時間。您也可以確定執行該操作的主機，以及該操作的資源群組和政策資訊。

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在監控頁面中，按一下*計劃*。
3. 選擇資源組和計劃類型。
4. 查看已排程的操作清單。

監視事件

您可以查看系統中的SnapCenter事件列表，例如使用者建立資源群組時或系統啟動活動時（例如建立排程備份）。您可能想要查看事件以確定備份或還原作業等作業目前是否正在進行中。

關於此任務

所有工作資訊都會顯示在「事件」頁面中。例如，當備份作業開始時，就會出現「備份開始」事件。當備份完成時，會出現「備份完成」事件。

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「監控」頁面中，按一下「事件」。
3. （可選）在過濾器框中，輸入開始或結束日期、事件類別（例如備份、資源組或策略）和嚴重性級別，然後按一下*套用*。或者，在搜尋框中輸入字元。
4. 查看事件清單。

監控日誌

您可以檢視和下載SnapCenter伺服器日誌、SnapCenter主機代理程式日誌和插件日誌。您可能希望查看日誌以協助進行故障排除。

關於此任務

您可以過濾日誌以僅顯示特定的日誌嚴重性等級：

- 偵錯
- 資訊
- 警告
- 錯誤

- 致命的

您也可以取得作業等級日誌，例如協助您排除備份作業失敗原因的日誌。對於作業等級日誌，請使用 **Monitor > Jobs** 選項。

步驟

1. 在左側導覽窗格中，按一下「監控」。
2. 在「作業」頁面中，選擇一個作業並按一下「下載日誌」。

下載的壓縮資料夾包含作業日誌和公用日誌。壓縮資料夾名稱包含所選的作業 ID 和作業類型。

3. 在「監控」頁面中，按一下「日誌」。
4. 選擇日誌類型、主機和實例。

如果將日誌類型選擇為“插件”，則可以選擇主機或SnapCenter插件。如果日誌類型為“伺服器*”，則無法執行此操作。

5. 若要以特定來源、訊息或日誌等級過濾日誌，請按一下列標題頂部的篩選器圖示。

若要顯示所有日誌，請選擇*大於或等於*作為`Debug`等級。

6. 按一下“刷新”。
7. 查看日誌列表。
8. 按一下“下載”下載日誌。

下載的壓縮資料夾包含作業日誌和公用日誌。壓縮資料夾名稱包含所選的作業 ID 和作業類型。

在大型配置中，為了獲得最佳效能，您應該使用 PowerShell cmdlet 將SnapCenter的日誌設定設為最低等級。

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10  
-JobLogsMaxFileSize 10MB -Server
```



若要在故障轉移作業完成後存取運作狀況或設定信息，請執行 cmdlet `Get-SmRepositoryConfig`。

從SnapCenter中刪除作業和日誌

您可以從SnapCenter中刪除備份、還原、複製和驗證作業和日誌。SnapCenter會無限期中地儲存成功和失敗的作業日誌，除非您將其刪除。您可能想要移除它們以補充儲存空間。

關於此任務

目前一定沒有正在運行的作業。您可以透過提供作業 ID 來刪除特定作業，也可以在指定時間內刪除作業。

您不需要將主機置於維護模式來刪除作業。

步驟

1. 啟動 PowerShell。
2. 在命令提示字元下輸入： `Open-SMConnection`
3. 在命令提示字元下輸入： `Remove-SmJobs`
4. 在左側導覽窗格中，按一下「監控」。
5. 在「監控」頁面中，按一下「作業」。
6. 在「作業」頁面中，檢視作業的狀態。

相關資訊

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

SnapCenter報告功能概述

SnapCenter提供多種報告選項，使您能夠監控和管理系統健康和操作成功。

報告類型	描述
備份報告	備份報告提供有關SnapCenter環境的備份趨勢的整體資料、備份成功率以及有關在指定時間內執行的每個備份的一些資訊。如果刪除了備份，則報告不會顯示已刪除備份的任何狀態資訊。備份詳細報告提供有關指定備份作業的詳細信息，並列出成功備份的資源和失敗的資源。
克隆報告	克隆報告提供有關SnapCenter環境的克隆趨勢的總體數據、克隆成功率以及有關在指定時間內執行的每個克隆作業的一些資訊。如果刪除了克隆，則報告不會顯示已刪除克隆的任何狀態資訊。複製詳細報告提供指定複製、複製主機和複製作業任務狀態的詳細資訊。如果任務失敗，複製詳細報告將顯示有關失敗的資訊。
恢復報告	恢復報告提供有關恢復作業的總體資訊。恢復詳細資訊報告提供有關指定恢復作業的詳細信息，包括主機名稱、備份名稱、作業開始和持續時間以及各個作業任務的狀態。如果任務失敗，恢復詳細報告將顯示有關失敗的資訊。
保護報告	這些報告提供所有SnapCenter插件執行個體管理的資源的保護詳細資訊。此報告提供所有插件實例管理的資源的保護詳細資訊。您可以查看概覽、未受保護資源的詳細資訊、產生報告時尚未備份的資源、備份作業失敗的資源組的資源以及SnapVault狀態。

報告類型	描述
定期報告	這些報告計劃定期運行，例如每天、每週或每月。報告會在指定的日期和時間自動生成，並透過電子郵件發送給相關人員。您可以啟用、停用、修改或刪除計畫。透過點選「立即執行」按鈕，可以按需執行已啟用的計畫。管理員可以執行任何計畫，但產生的報告將包含基於建立該計畫的使用者提供的權限的資料。 除管理員之外的任何其他使用者都可以根據其權限查看或修改計畫。如果在新增角色頁面中選擇了該角色的所有成員都可以看到其他成員的物件選項，則該角色的其他成員將能夠檢視和修改。

訪問報告

您可以使用SnapCenter儀表板快速了解系統健康狀況。您可以從儀表板深入了解更多詳細資訊。或者，您可以直接存取詳細報告。

您可以透過以下方法之一存取報告：

- 在左側導覽窗格中，按一下“儀表板”，然後按一下“上次保護摘要”圓餅圖以在“報表”頁面中查看更多詳細資訊。
- 在左側導覽窗格中，按一下「報告」。

過濾報告

您可能希望根據所需資訊的詳細程度和時間跨度，按照一系列參數來篩選報告資料。

步驟

1. 在左側導覽窗格中，按一下「報告」。
2. 如果未顯示參數視圖，請按一下報表工具列中的「切換參數區域」圖示。
3. 指定您想要執行報表的時間範圍。+ 如果省略結束日期，您將檢索所有可用資訊。
4. 根據以下任一條件過濾報告資訊：
 - 資源組
 - 主持人
 - 政策
 - 資源
 - 地位
 - 插件名稱
5. 按一下“應用”。

匯出或列印報告

匯出SnapCenter報告可讓您以多種其他格式查看報告。您也可以列印報告。

步驟

1. 在左側導覽窗格中，按一下「報告」。
2. 從報告工具列中執行以下操作之一：
 - 按一下「切換列印預覽」圖示即可預覽可列印的報告。
 - 從*匯出*圖示下拉清單中選擇一種格式，將報告匯出為其他格式。
3. 若要列印報告，請按一下「列印」圖示。
4. 若要查看特定的報告摘要，請捲動至報告的相應部分。

設定電子郵件通知的 **SMTP** 伺服器

您可以指定用於向自己或其他人傳送資料保護作業報告的 SMTP 伺服器。您也可以傳送測試電子郵件來驗證配置。這些設定將全域套用至您設定電子郵件通知的任何SnapCenter作業。

此選項配置 SMTP 伺服器以傳送所有資料保護作業報告。但是，如果您希望定期將特定資源的SnapCenter資料保護作業更新傳送給您自己或其他人，以便您可以監控這些更新的狀態，則可以在建立資源群組時配置透過電子郵件傳送SnapCenter報表的選項。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在設定頁面中，按一下*全域設定*。
3. 輸入 SMTP 伺服器並點擊 儲存。
4. 若要傳送測試電子郵件，請輸入您要傳送電子郵件的電子郵件地址，輸入主題，然後按一下「傳送」。

配置透過電子郵件傳送報告的選項

如果您希望定期將SnapCenter資料保護作業更新傳送給自己或其他人，以便您可以監視這些更新的狀態，您可以在建立資源群組時配置透過電子郵件傳送SnapCenter報表的選項。

開始之前

您必須在「設定」下的「全域設定」頁面中設定您的 SMTP 伺服器。

步驟

1. 在左側導覽窗格中，按一下“資源”，然後從清單中選擇適當的外掛程式。
2. 選擇您要檢視的資源類型並點選*新資源群組*，或選擇現有的資源群組並點選*修改*為現有資源群組設定電子郵件報表。
3. 在新資源組精靈的通知面板中，從下拉式選單中選擇是否始終接收報告、在失敗時接收報告、在失敗或警告時接收報告。
4. 輸入電子郵件的寄件地址、收件者地址以及電子郵件的主題。

管理SnapCenter伺服器儲存庫

與從SnapCenter執行的各種操作相關的資訊儲存在SnapCenter Server 資料庫儲存庫中。您必須建立儲存庫的備份以保護SnapCenter伺服器免於資料遺失。

SnapCenter Server 儲存庫有時被稱為 NSM 資料庫。

保護SnapCenter儲存庫的先決條件

您的環境應滿足某些先決條件才能保護SnapCenter儲存庫。

- 管理儲存虛擬機器 (SVM) 連接

您應該配置儲存憑證。

- 預配主機

SnapCenter儲存庫主機上應至少存在一個NetApp儲存磁碟。如果SnapCenter儲存庫主機上沒有NetApp磁碟，則必須建立一個。

有關新增主機、設定 SVM 連接和配置主機的詳細信息，請參閱安裝說明。

- 配置 iSCSI LUN 或 VMDK

對於高可用性 (HA) 配置，您可以在其中一個SnapCenter伺服器中設定 iSCSI LUN 或 VMDK。

備份SnapCenter儲存庫

備份SnapCenter Server 儲存庫有助於防止資料遺失。您可以透過執行 `_Protect-SmRepository_ cmdlet` 來備份儲存庫。

關於此任務

Protect-SmRepository cmdlet 完成下列任務：

- 建立資源群組和策略
- 為SnapCenter儲存庫建立備份計劃

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，使用 *Open-SmConnection* cmdlet 建立會話，然後輸入您的憑證。
3. 使用 *Protect-SmRepository* cmdlet 和所需參數備份儲存庫。

查看SnapCenter儲存庫的備份

您可以透過執行 *Get-SmRepositoryBackups* cmdlet 顯示SnapCenter Server 資料庫儲存庫備份的清單。

儲存庫備份是根據 *Protect-SmRepository* cmdlet 中指定的計畫建立的。

步驟

1. 啟動 PowerShell。
2. 在命令提示字元下，輸入下列 cmdlet，然後提供憑證以連接到 SnapCenter 伺服器：*Open-SMConnection*
3. 使用 *Get-SmRepositoryBackups* cmdlet 列出所有可用的 SnapCenter 資料庫備份。

還原 SnapCenter 資料庫儲存庫

您可以透過執行 *Restore-SmRepositoryBackup* cmdlet 來還原 SnapCenter 儲存庫。

還原 SnapCenter 儲存庫時，正在執行的其他 SnapCenter 作業將受到影響，因為在還原作業期間儲存庫資料庫無法存取。

步驟

1. 啟動 PowerShell。
2. 在命令提示字元下，輸入下列 cmdlet，然後提供憑證以連接到 SnapCenter 伺服器：*Open-SMConnection*
3. 使用 *Restore-SmRepositoryBackup* cmdlet 還原儲存庫備份。

以下 cmdlet 從 iSCSI LUN 或 VMDK 上現有的備份還原 SnapCenter MySQL 資料庫儲存庫：

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
```

當 iSCSI LUN 中的備份檔案意外刪除時，下列 cmdlet 會還原 SnapCenter MySQL 資料庫。對於 VMDK，請從 ONTAP 快照手動還原備份。

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```



執行復原作業後擷取儲存庫備份時，將不會列出用於執行儲存庫復原作業的備份。

遷移 SnapCenter 儲存庫

您可以將 SnapCenter Server 資料庫儲存庫從預設位置遷移到另一個磁碟。當您想要將儲存庫重新定位到具有更多空間的磁碟時，您可能會遷移儲存庫。

步驟

1. 在 Windows 中停止 MySQL57 服務。
2. 找到 MySQL 資料目錄。

通常可以在 C:\ProgramData\MySQL\MySQL Server 5.7\Data 找到資料目錄。

3. 將 MySQL 資料目錄複製到新位置，例如 E:\Data\nsm。
4. 右鍵點選新目錄，然後選擇*屬性*>*安全性*將網路服務本機伺服器帳戶新增至新目錄，然後為該帳戶指派完全控制權。
5. 重新命名原始資料庫目錄，例如 nsm_copy。
6. 在 Windows 命令提示字元下，使用 *mklink* 命令建立符號目錄連結。

```
"mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
```

7. 在Windows中啟動MySQL57服務。
8. 透過登入SnapCenter並檢查儲存庫條目，或登入 MySQL 實用程式並連接到新儲存庫來驗證資料庫位置變更是否成功。
9. 刪除原始的、重新命名的資料庫儲存庫目錄（nsm_copy）。

重置SnapCenter儲存庫密碼

MySQL Server 儲存庫資料庫密碼是在SnapCenter 4.2 安裝SnapCenter Server 期間自動產生的。SnapCenter 用戶在任何時候都不知道這個自動產生的密碼。如果您想存取儲存庫資料庫，您應該重設密碼。

開始之前

您應該具有SnapCenter管理員權限才能重設密碼。

步驟

1. 啟動 PowerShell。
2. 在命令提示字元下，輸入下列命令，然後提供連接到SnapCenter伺服器的憑證：*Open-SMConnection*
3. 重置儲存庫密碼：*Set-SmRepositoryPassword*

以下命令重設儲存庫密碼：

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: *****
ConfirmPassword: *****
Successfully updated the MySQL server password.
```

相關資訊

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

管理不受信任域的資源

除了管理 Active Directory (AD) 受信任網域中的主機之外， SnapCenter還管理多個 AD 不受信任網域中的主機。不受信任的 AD 網域必須在SnapCenter伺服器上註冊。SnapCenter支援多個不受信任的 AD 網域的使用者和群組。

您可以在網域或工作群組中的電腦上安裝SnapCenter伺服器。若要安裝SnapCenter伺服器，如果電腦在網域中，則應指定網域憑證；如果電腦在工作群組中，則應指定本機管理員憑證。

不支援屬於未在SnapCenter Server 註冊的網域的 Active Directory (AD) 群組。雖然您可以使用這些 AD 群組建立SnapCenter角色，但登入SnapCenter伺服器會失敗並顯示下列錯誤訊息：您嘗試登入的使用者不屬於任何角色。請聯絡您的管理員。

修改不受信任的網域

當您想要更新網域控制器 IP 位址或完全限定網域名稱 (FQDN) 時，可以修改不受信任的網域。

關於此任務

修改 FQDN 後，相關資產（主機、使用者和群組）可能無法如預期運作。

若要修改不受信任的網域，您可以使用SnapCenter使用者介面或 PowerShell cmdlet。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在設定頁面中，按一下*全域設定*。
3. 在全域設定頁面中，按一下「網域設定」。

4. ，然後提供以下詳細資訊：

對於這個領域...	這樣做...
域 FQDN	指定 FQDN，然後按一下“解析”。
網域控制器 IP 位址	如果網域 FQDN 不可解析，請指定一個或多個網域控制器 IP 位址。

5. 按一下“確定”。

取消註冊不受信任的 **Active Directory** 網域

如果您不想使用與該網域關聯的資產，您可以取消註冊不受信任的 Active Directory 網域。

開始之前

您應該刪除與不受信任的網域相關聯的主機、使用者、群組和憑證。

關於此任務

- 從SnapCenter Server 取消註冊網域後，該網域的使用者將無法存取SnapCenter Server。
- 如果有關聯資產（主機、使用者和群組），則在取消註冊網域後，這些資產將無法運作。
- 若要取消註冊不受信任的網域，您可以使用SnapCenter使用者介面或 PowerShell cmdlet。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在設定頁面中，按一下*全域設定*。
3. 在全域設定頁面中，按一下「網域設定」。
4. 從網域清單中，選擇要取消註冊的網域。
5. 點選 ，然後按一下「確定」。

管理儲存系統

新增儲存系統後，您可以修改儲存系統配置和連接，或刪除儲存系統。

修改儲存系統配置

如果您想要變更使用者名稱、密碼、平台、連接埠、協定、逾時期限、首選 IP 位址或訊息選項，則可以使用 SnapCenter 修改儲存系統配置。

關於此任務

您可以修改單一使用者或群組的儲存連線。如果您屬於一個或多個具有相同儲存系統權限的群組，則儲存連線名稱會在儲存連線清單中顯示多次，每個具有該儲存系統權限的群組顯示一次。

步驟

1. 在左側導覽窗格中，按一下「儲存系統」。
2. 在儲存系統頁面中，從*類型*下拉式選單中執行下列其中一項：

選擇...	步驟...
ONTAP SVM	查看所有已新增的儲存虛擬機器 (SVM)，並修改所需的 SVM 配置。 - 在「儲存連線」頁面中，按一下對應的 SVM 名稱。 - 執行下列操作之一： - 如果 SVM 不屬於任何集群，請在修改儲存系統頁面中修改配置，例如使用者名稱、密碼、EMS 和 AutoSupport 設定、平台、協定、連接埠、逾時和首選 IP。 - 如果 SVM 是叢集的一部分，則在「修改儲存系統」頁面中，選擇*獨立管理 SVM*，並修改配置，例如使用者名稱、密碼、EMS 和 AutoSupport 設定、平台、協定、連接埠、逾時和首選 IP。 將 SVM 修改為獨立管理後，如果決定透過叢集進行管理，則應刪除該 SVM，然後按一下 重新發現。SVM 將會加入到 ONTAP 叢集。  當在 SnapCenter GUI 上更新儲存系統密碼時，您應該重新啟動對應插件或伺服器主機的 SMCORE 服務，因為更新後的密碼不會反映在 SMCORE 中，並且備份作業將因憑證錯誤而失敗。
ONTAP 叢集	查看所有已新增的叢集並修改所需的叢集配置。 - 在儲存連線頁面中，按一下叢集名稱。 - 在修改儲存系統頁面，點選使用者名稱旁邊的編輯圖標，修改使用者名稱和密碼。 - 選擇或清除 EMS 和 AutoSupport 設定。 - 點擊*更多選項*並修改其他配置，例如平台、協定、連接埠、逾時和首選 IP。

3. 點選“提交”。

刪除儲存系統

您可以使用 SnapCenter 刪除任何未使用的儲存系統。

關於此任務

您可以刪除單一使用者或群組的儲存連線。如果您屬於一個或多個具有相同儲存系統權限的群組，則儲存系統名稱會在儲存連線清單中顯示多次，每個具有該儲存系統權限的群組顯示一次。



刪除儲存系統時，在該儲存系統上執行的所有操作都會失敗。

步驟

1. 在左側導覽窗格中，按一下「儲存系統」。
2. 在儲存系統頁面中，從 類型 下拉式選單中選擇 * ONTAP SVM* 或 * ONTAP叢集*。
3. 在「儲存連線」頁面中，選取要刪除的 SVM 或叢集旁的核取方塊。



您不能選擇屬於叢集的 SVM。

4. 按一下“刪除”。
5. 在「刪除儲存系統連線設定」頁面中，按一下「確定」。



如果使用ONTAP GUI 從ONTAP叢集中刪除 SVM，請在SnapCenter GUI 中按 重新發現 以更新 SVM 清單。

REST API 支援

預設情況下，所有ASA、AFF或FAS系統與ONTAP的連線都將透過 ZAPI。可以為特定ONTAP版本啟用 REST API。

SnapCenter利用 REST API 在ASA r2 系統上執行所有操作，而 ASA r2 系統不支援 ZAPI。

您可以修改以下設定檔中的設定鍵：

- IsRestEnabledForStorageConnection

預設值為 false。

- MinOntapVersionToUseREST

預設值為 9.13.1。

透過 REST API 啟用連接

1. 將 IsRestEnabledForStorageConnection 設為 true。
2. 在伺服器和 Windows 插件主機上的 SMCoreServiceHost.dll.config 和 SnapDriveService.dll.config 中新增金鑰。

<新增鍵="IsRestEnabledForStorageConnection" 值="true" />

將透過 REST API 的連線限制為特定版本的ONTAP

1. 將組態參數 MinOntapVersionToUseREST 設為 true。
2. 在伺服器和 Windows 插件主機上的 SMCoreServiceHost.dll.config 和 SnapDriveService.dll.config 中新增金鑰。

<新增鍵="MinOntapVersionToUseREST" 值="9.13.1" />

3. 重新啟動伺服器上的 SmCore 服務以及插件上的插件和SnapDrive服務。

管理 EMS 資料收集

您可以使用 PowerShell cmdlet 安排和管理事件管理系統 (EMS) 資料收集。EMS 資料收集涉及收集有關SnapCenter伺服器、已安裝的SnapCenter插件包、主機和類似資訊的詳細信息，然後將其發送到指定的ONTAP儲存虛擬機器 (SVM)。



資料收集任務進行時系統 CPU 使用率很高。只要操作進行，無論資料大小如何，CPU 使用率都會保持在較高水準。

停止 EMS 資料收集

EMS 資料收集預設為啟用，並在安裝日期後每七天運行一次。您可以隨時使用 PowerShell cmdlet *Disable-SmDataCollectionEMS* 停用資料收集。

步驟

1. 從 PowerShell 命令列輸入 *Open-SmConnection* 與SnapCenter建立會話。
2. 透過輸入 *_Disable-SmDataCollectionEms_* 來停用 EMS 資料收集。

開始 EMS 資料收集

EMS 資料收集預設為啟用，並計劃從安裝日期起每七天運行一次。如果您已停用它，則可以使用 *Enable-SmDataCollectionEMS* cmdlet 再次啟動 EMS 資料收集。

NetApp ONTAP事件 generate-autosupport-log 權限已授予儲存虛擬機器 (SVM) 使用者。

步驟

1. 從 PowerShell 命令列輸入 *Open-SmConnection* 與SnapCenter建立會話。
2. 透過輸入 *_Enable-SmDataCollectionEMS_* 來啟用 EMS 資料收集。

更改 EMS 資料收集計劃和目標 SVM

您可以使用 PowerShell cmdlet 來變更 EMS 資料收集計畫或目標儲存虛擬機器 (SVM)。

步驟

1. 從 PowerShell 命令列，若要與SnapCenter建立會話，請輸入 *Open-SmConnection* cmdlet。
2. 若要變更 EMS 資料收集目標，請輸入 *Set-SmDataCollectionEmsTarget* cmdlet。
3. 若要變更 EMS 資料收集計劃，請輸入 *Set-SmDataCollectionEmsSchedule* cmdlet。

監控EMS資料收集狀態

您可以使用多個 PowerShell cmdlet 監控 EMS 資料收集的狀態。您可以取得有關計劃、儲存虛擬機器 (SVM) 目標和狀態的資訊。

步驟

1. 從 PowerShell 命令列輸入 *Open-SmConnection* 與 SnapCenter 建立會話。
2. 透過輸入 *Get-SmDataCollectionEmsSchedule* 檢索有關 EMS 資料收集計劃的資訊。
3. 透過輸入 *Get-SmDataCollectionEmsStatus* 檢索有關 EMS 資料收集狀態的資訊。
4. 透過輸入 *Get-SmDataCollectionEmsTarget* 檢索有關 EMS 資料收集目標的資訊。

相關資訊

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter 軟體 Cmdlet 參考指南](#)"。

升級SnapCenter伺服器 and 插件

配置SnapCenter以檢查可用更新

SnapCenter定期與NetApp支援站點通信，以通知您可用的軟體更新。您也可以建立一個時間表來指定接收有關可用更新的資訊的時間間隔。

步驟

1. 在左側導覽窗格中，按一下「設定」。
2. 在「設定」頁面中，按一下「軟體」。

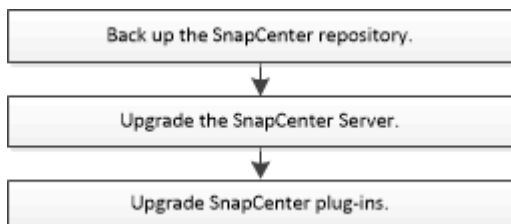
可用軟體頁面顯示可用的插件包、可用的版本及其安裝狀態。

3. 點擊“檢查更新”以查看是否有任何較新版本的插件包可用。
4. 按一下「計劃更新」以建立計劃，以指定您想要接收可用更新的資訊的時間間隔：
 - a. 在*檢查更新*中選擇間隔。
 - b. 選擇SnapCenter Server Admin Windows 憑證並按一下「確定」。

升級工作流程

SnapCenter的每個版本都包含更新的SnapCenter伺服器和插件包。插件包更新隨SnapCenter安裝程式一起分發。您可以設定SnapCenter來檢查可用的更新。

工作流程顯示了升級SnapCenter伺服器和插件包所需的任務。



支援的升級路徑

升級路徑可協助您了解可以從哪些早期版本的SnapCenter升級至最新版本的SnapCenter以及支援哪些版本的外掛程式。

如果您使用的是 SnapCenter Server 版本...	您可以直接將 SnapCenter Server 升級到...	支援的插件版本
5.0	6.0	• 5.0 • 6.0
	6.0.1	• 6.0.1
	6.1	• 6.1
6.0	6.0.1	• 6.0 • 6.0.1
	6.1	• 6.1
6.0.1	6.1	• 6.0.1 • 6.1

有關升級適用SnapCenter Plug-in for VMware vSphere的信息，請參閱 ["升級SnapCenter Plug-in for VMware vSphere"](#)。

升級 Windows 主機上的SnapCenter伺服器

您應該升級SnapCenter伺服器以存取最新版本中提供的最新功能和增強功能。

開始之前

- 使用最新的 Windows 更新來更新SnapCenter Server 主機，並確保沒有待處理的系統重新啟動。
- 確保在開始升級之前沒有其他操作正在運行。
- 安裝 ASP.NET Core Runtime 8.0.12（以及所有後續 8.0.x 修補程式）託管包和 PowerShell 7.4.2 或更高版本。
- 確保沒有正在執行的作業後，備份SnapCenter儲存庫（MySQL）資料庫。在升級SnapCenter Server 和 Exchange 插件之前建議這樣做。

有關信息，請參閱["備份SnapCenter儲存庫"](#)。

- 備份SnapCenter伺服器主機或插件主機上修改的所有已修改的SnapCenter設定檔。

SnapCenter設定檔範例：SnapDriveService.exe.config、SMCoreServiceHost.exe.config 等等。

- 如果您在SnapCenter 5.0 中安裝了多個版本的自訂插件，則在升級到 6.0 或更高版本之前，您應該執行 powershell cmdlet 從SnapCenter儲存庫（NSM 資料庫）中刪除所有早期版本的自訂插件（最新版本除外）。
 - 跑步 `Open-SmConnection` 並使用 SnapCenterAdmin 角色憑證登入
 - 跑步 Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>

有關更多信息，請參閱 ["升級到SnapCenter 6.0 或更高版本失敗"](#)。

關於此任務

- 在升級期間，SnapCenter執行 SQL 腳本來更新 NSM 資料庫中的 Exchange 數據，將 DAG 和主機短名稱轉換為 FQDN。這僅適用於將SnapCenter Server 與 Exchange 外掛程式一起使用的情況。
- 如果您已手動將伺服器主機置於維護模式，則升級後選擇*主機*>*啟動計劃*以使伺服器主機退出維護模式。
- 對於策略中啟用了前置腳本和後置腳本的現有備份和驗證計劃，升級後備份作業將繼續進行。

在*作業詳情*頁面中，一條警告訊息建議客戶將腳本複製到 SCRIPTS_PATH 並編輯策略以提供相對於 SCRIPTS_PATH 的路徑。對於複製生命週期作業，警告訊息出現在子作業層級。

步驟

1. 從NetApp支援網站下載SnapCenter Server 安裝套件。

<https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab>

2. 建立位於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config 的副本。
3. 如果升級失敗，請從 Windows 工作排程器匯出SnapCenter插件主機方案以還原它們。

```
md d:\\SCBackup\\schtasks /query /xml /TN taskname >>
"D:\\SCBackup\\taskname.xml"
```

4. 如果未配置儲存庫備份，則建立SnapCenter MySQL 資料庫轉儲。

```
md d:\\SCBackup\\mysqldump --all-databases --single-transaction --add-drop
-database --triggers --routines --events -u root -p >
D:\\SCBackup\\SCRepoBackup.dmp
```

出現提示時，輸入密碼。

5. 雙擊下載的 .exe 檔案以啟動SnapCenter伺服器升級。

開始升級後，SnapCenter會執行預檢查。如果系統不符合最低要求，SnapCenter會顯示錯誤或警告訊息。您可以忽略警告並繼續安裝，但必須修復所有錯誤。



SnapCenter繼續使用安裝早期版本的SnapCenter Server 期間提供的現有 MySQL Server 儲存庫資料庫密碼。

6. 選擇*升級*。

如果您在任何階段選擇“取消”，SnapCenter將停止升級。它不會將SnapCenter伺服器回滾到先前的狀態。

*最佳實務：*登出並重新登錄，或開啟新的瀏覽器來存取SnapCenter使用者介面。

完成後

- 如果使用 sudo 使用者安裝插件，則應複製 C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt 中的 sha224 金鑰來更新 /etc/sudoers 檔案。
- 您應該在伺服器主機上執行新的資源發現。

如果SnapCenter顯示伺服器主機狀態為已停止，請等待一段時間並執行新的發現。您也可以將 **HostRefreshInterval** 參數的值（預設值為 3600 秒）變更為任何大於 10 分鐘的值。

- 如果升級失敗，請清理失敗的安裝，重新安裝早期版本的SnapCenter，並將 NSM 資料庫還原到先前的狀態。
- 升級伺服器主機後，還必須升級插件才能新增任何儲存系統。

升級 Linux 主機上的SnapCenter伺服器

您可以使用SnapCenter Server 安裝程式檔案來升級SnapCenter Server。

步驟

1. 執行其中一項操作來升級SnapCenter伺服器。

如果你想表演...	這樣做...
非互動式升級	<pre>sudo ./snapcenter-linux-server- (e18/e19/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename></pre> 範例：sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log 日誌將儲存在 <i>/var/opt/snapcenter/logs</i>。 升級需要傳遞的參數： • DINSTALL_LOG_NAME：儲存安裝日誌的日誌檔案名稱。 • DUPGRADE：預設值為 0。指定此參數及其值為 0 以外的任何整數來升級SnapCenter伺服器。
互動式安裝	<pre>./snapcenter-linux-server- (e18/e19/sles15).bin</pre> 系統將提示您確認升級。輸入 0 以外的任何值以確認SnapCenter伺服器升級。



您應該登出然後登入SnapCenter，或關閉然後開啟新的瀏覽器來存取SnapCenter GUI。

升級你的插件包

插件包作為SnapCenter升級的一部分進行分發。

您不必手動將每個要升級的插件主機置於維護模式，因為升級過程會將您的 Windows、Linux 或 AIX 插件主機置於維護模式。維護模式可防止在升級期間在插件主機上執行任何計劃的作業。

開始之前

- 如果您是可以存取 Linux 機器的非 root 用戶，則應在執行升級作業之前使用最新的校驗和值更新 `/etc/sudoers` 檔案。
- 預設情況下，SnapCenter 從環境中偵測 `JAVA_HOME`。如果您想要使用固定的 `JAVA_HOME`，並且要在 Linux 主機上升級插件，則應在位於 `/var/opt/snapcenter/spl/etc/` 的 `spl.properties` 檔案中手動新增 `SKIP_JAVAHOME_UPDATE` 參數，並將值設為 `TRUE`。

當外掛程式升級或 SnapCenter 插件載入器 (SPL) 服務重新啟動時，`JAVA_HOME` 的值會更新。在升級或重新啟動 SPL 之前，如果新增 `SKIP_JAVAHOME_UPDATE` 參數並將其值設為 `TRUE`，則 `JAVA_HOME` 的值不會更新。

- 您應該已經備份了在 SnapCenter 伺服器主機或插件主機上修改的所有 SnapCenter 設定檔。

SnapCenter 設定檔範例：`SnapDriveService.exe.config`、`SMCoreServiceHost.exe.config` 等等。

關於此任務

- 對於適用於 Microsoft SQL Server 的 SnapCenter 插件、適用於 Microsoft Exchange Server 的 SnapCenter 插件和適用於 Microsoft Windows 的 SnapCenter 插件，建議將伺服器和插件主機都升級到最新版本，以便 `SCRIPTS_PATH` 運作。

對於策略中啟用了前置腳本和後置腳本的現有備份和驗證計劃，升級後備份作業將繼續進行。

在*作業詳情*頁面中，一條警告訊息建議客戶將腳本複製到 `SCRIPTS_PATH` 並編輯策略以提供相對於 `SCRIPTS_PATH` 的路徑。對於複製生命週期作業，警告訊息出現在子作業層級。

步驟

1. 在左側導覽窗格中，按一下「主機」>「託管主機」。
2. 透過執行下列任務之一來升級主機：
 - 如果“整體狀態”列顯示其中一個外掛程式主機的“可升級”，請按一下該外掛程式主機名稱並執行下列操作：
 - i. 按一下“更多選項”。
 - ii. 如果您不想驗證插件主機是否符合升級插件的要求，請選擇「跳過預檢」。
 - iii. 點選*升級*。
 - 如果要升級多台主機，請選擇所有主機，點選，然後按一下*升級*>*確定*。

在插件升級過程中，所有相關服務都會重新啟動。



套件中的所有插件都會被選中，但只有隨早期版本的 SnapCenter 安裝的插件才會升級，其餘插件不會安裝。您必須使用*新增插件*選項來安裝任何新插件。

如果您未選取「跳過預先檢查」複選框，則會驗證插件主機是否符合安裝插件的要求。如果不符合最低要求，則會顯示相應的錯誤或警告訊息。解決問題後，按一下*升級*。



如果錯誤與磁碟空間或 RAM 有關，您可以更新位於 C:\Program Files\ NetApp\ SnapCenter WebApp 的 web.config，或位於 C:\Windows\System32\WindowsPowerShell\v1.0\Modules\SnapCenter\ 的 PowerShell 設定檔以修改預設值。如果錯誤與剩餘參數有關，那麼您必須解決問題，然後再次驗證要求。

技術更新

SnapCenter Server 主機的技術更新

當SnapCenter Server 主機需要刷新時，您可以在新主機上安裝相同版本的SnapCenter Server，然後執行API 從舊伺服器備份SnapCenter並在新伺服器上還原它。

步驟

1. 部署新主機並執行下列任務：
 - a. 安裝相同版本的SnapCenter伺服器。
 - b. （可選）配置 CA 憑證並啟用雙向 SSL。更多信息，請參閱 ["設定 CA 憑證"](#)和 ["配置並啟用雙向 SSL"](#)。
 - c. （可選）配置多重身份驗證。有關更多信息，請參閱 ["啟用多重身份驗證"](#)。
2. 以SnapCenter管理員用戶身分登入。
3. 使用下列 API 在舊主機上建立SnapCenter伺服器的備份：`/<snapcenter\_version>/server/backup` 或 cmdlet：*New-SmServerBackup*。



在進行備份之前，暫停所有排程的作業並確保沒有作業正在執行。



如果要在新的網域上執行的SnapCenter伺服器上還原備份，則在進行備份之前，您應該在舊的SnapCenter主機中新增新的網域使用者並指派SnapCenter管理員角色。

4. 將備份從舊主機複製到新主機。
5. 使用下列 API 在新主機上還原SnapCenter伺服器的備份：`/<snapcenter\_version>/server/restore` 或 cmdlet：*Restore-SmServerBackup*。

預設情況下，復原將更新所有主機中的新SnapCenter伺服器 URL。如果您想跳過更新，請使用 *-SkipSMSURLInHosts* 屬性，並透過執行下列 API 單獨更新伺服器 URL：

`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。



如果插件主機無法解析伺服器主機名，請登入每個插件主機，並以 *<New IP> SC_Server_Name* 格式新增 IP 的 *etc/host* 項目。



伺服器 *etc/host* 項目將不會被恢復。您可以從舊伺服器手動恢復它。

如果新的網域上執行的 SnpCenter 伺服器上還原了備份，並且想要繼續使用舊網域用戶，則應在新的SnapCenter伺服器上註冊舊網域。



如果您已手動更新舊SnapCenter主機中的 *web.config* 文件，則更新將不會複製到新主機。您應該在新主機的 *web.config* 檔案中手動進行相同的變更。

6. 如果您跳過了更新SnapCenter伺服器 URL 或在還原過程中任何主機關閉，請使用下列 API 更新SnapCenter管理的所有主機或指定主機中的新伺服器名稱：`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。
7. 從新的SnapCenter伺服器啟動所有主機上的排程作業。

F5 叢集中節點的技術更新

您可以透過刪除節點並新增節點來對 F5 叢集中的任何節點進行技術更新。如果需要刷新的節點處於活動狀態，則將叢集的另一個節點設為活動狀態，然後刪除該節點。

有關如何向 F5 叢集新增節點的信息，請參閱 ["使用 F5 設定 SnapCenter 伺服器以實現高可用性"](#)。



如果 F5 叢集的 url 發生變化，則可以使用下列 API 在所有主機中更新 url：
`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。

停用舊的 SnapCenter Server 主機

在驗證新的 SnapCenter Server 已啟動並正在運作且所有插件主機都能夠與新的 SnapCenter SnapCenter 主機。

回滾到舊的 SnapCenter Server 主機

如果發生任何問題，您可以使用下列 API 更新所有主機中的 SnapCenter Server URL，從而還原舊的 SnapCenter Server 主機：`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。

災難復原

獨立 SnapCenter 主機的災難復原

您可以透過將伺服器備份還原到新主機來執行災難復原。

開始之前

確保您有舊 SnapCenter 伺服器的備份。

步驟

1. 部署新主機並執行下列任務：
 - a. 安裝相同版本的 SnapCenter 伺服器。
 - b. 設定 CA 憑證並啟用雙向 SSL。更多信息，請參閱 ["設定 CA 憑證"](#) 和 ["配置並啟用雙向 SSL"](#)。
2. 將舊的 SnapCenter Server 備份複製到新主機。
3. 以 SnapCenter 管理員用戶身分登入。
4. 使用下列 API 在新主機上還原 SnapCenter 伺服器的備份：`/<snapcenter\_version>/server/restore` 或 cmdlet：*Restore-SmServerBackup*。

預設情況下，復原將更新所有主機中的新 SnapCenter 伺服器 URL。如果要跳過更新，請使用 *-SkipSMSURLInHosts* 屬性，並使用下列 API 單獨更新伺服器 URL：
`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。



如果插件主機無法解析伺服器主機名，請登入每個插件主機，並以 *<New IP> SC_Server_Name* 格式新增 IP 的 *etc/host* 項目。



伺服器 *etc/host* 項目將不會被恢復。您可以從舊伺服器手動恢復它。

5. 如果您跳過了更新 URL 或任何主機在還原過程中關閉，請使用下列 API 更新SnapCenter管理的所有主機或指定主機中的新伺服器名稱：`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。

SnapCenter F5 叢集的災難復原

您可以透過將伺服器備份還原到新主機，然後將獨立主機轉換為叢集來執行災難復原。

開始之前

確保您有舊SnapCenter伺服器的備份。

步驟

1. 部署新主機並執行下列任務：
 - a. 安裝相同版本的SnapCenter伺服器。
 - b. 設定CA憑證並啟用雙向SSL。更多信息，請參閱 ["設定 CA 憑證"](#)和 ["配置並啟用雙向 SSL"](#)。
2. 將舊的SnapCenter Server 備份複製到新主機。
3. 以SnapCenter管理員用戶身分登入。
4. 使用下列 API 在新主機上還原SnapCenter伺服器的備份：`/<snapcenter\_version>/server/restore` 或 cmdlet：*Restore-SmServerBackup*。

預設情況下，復原將更新所有主機中的新SnapCenter伺服器 URL。如果要跳過更新，請使用 *-SkipSMSURLInHosts* 屬性，並使用下列 API 單獨更新伺服器 URL：
`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。



如果插件主機無法解析伺服器主機名，請登入每個插件主機，並以 <New IP> SC_Server_Name 格式新增 IP 的 *etc/host* 項目。



伺服器 *etc/host* 項目將不會被恢復。您可以從舊伺服器手動恢復它。

5. 如果您跳過了更新 URL 或任何主機在還原過程中關閉，請使用下列 API 更新SnapCenter管理的所有主機或指定主機中的新伺服器名稱：`/<snapcenter\_version>/server/configureurl` 或 cmdlet：*Set-SmServerConfig*。
6. 將獨立主機轉換為 F5 叢集。

有關如何配置 F5 的信息，請參閱 ["使用 F5 設定SnapCenter伺服器以實現高可用性"](#)。

相關資訊

有關 API 的信息，您需要訪問 Swagger 頁面。請參閱["如何使用 Swagger API 網頁存取 REST API"](#)。

可以透過執行 *_Get-Help command_name* 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter軟體 Cmdlet 參考指南"](#)。

SnapCenter插件主機的技術更新

當SnapCenter插件主機需要刷新時，您應該將資源從舊主機移至新主機。當新主機新增至SnapCenter時，它將發現所有資源，但將被視為新資源。

關於此任務

您應該執行 API 或 cmdlet，它將以舊主機名稱和新主機名稱作為輸入，按名稱比較資源，並將符合資源的物件從舊主機重新連結到新主機。匹配的資源將被標記為受保護。

- *IsDryRun* 參數預設為 True，用於識別新舊主機的匹配資源。

驗證符合資源後，應將 *_IsDryRun_* 參數設為 False，以將符合資源的物件從舊主機重新連結到新主機。

- *AutoMigrateManuallyAddedResources* 參數預設為 True，這會自動將手動新增的資源從舊主機複製到新主機。

AutoMigrateManuallyAddedResources 參數僅適用於 Oracle 和 SAP HANA 資源。

- 如果舊主機和新主機之間的實例名稱不同，則應使用 *SQLInstanceMapping* 參數。如果它是預設實例，則使用 *default_instance* 作為實例名稱。

以下 SnapCenter 插件支援技術更新：

- 適用於 Microsoft SQL Server 的 SnapCenter 插件
 - 如果 SQL 資料庫在執行個體層級受到保護，並且作為主機技術更新的一部分，只有部分資源被移至新主機，那麼現有的執行個體層級保護將轉換為資源群組保護，並且來自兩個主機的執行個體都會新增至資源群組。
 - 如果 SQL 主機（例如 host1）用作另一台主機（例如 host2）的資源的調度程序或驗證伺服器，則在 host1 上執行技術更新時，計劃或驗證詳細資訊將不會遷移並將繼續在 host1 上執行。如果必須修改，那麼您應該在相應的主機中手動更改它。
 - 如果您正在使用 SQL 故障轉移叢集執行個體 (FCI) 設定，則可以透過將新節點新增至 FCI 叢集並重新整理 SnapCenter 中的外掛程式主機來執行技術重新整理。
 - 如果您使用 SQL 可用性群組 (AG) 設置，則不需要技術更新。您可以將新節點新增至 AG 並在 SnapCenter 中刷新主機。
- 適用於 Windows 的 SnapCenter 插件
- 適用於 Oracle 資料庫的 SnapCenter 插件

如果您使用的是 Oracle Real Application Cluster (RAC) 設置，則可以透過將新節點新增至 RAC 叢集並刷新 SnapCenter 中的插件主機來執行技術刷新。

- 適用於 SAP HANA 資料庫的 SnapCenter 插件

支援的用例包括：

- 將資源從一個主機遷移到另一個主機。
- 將資源從多個主機遷移到一個或更少的主機。
- 將資源從一個主機遷移到多個主機。

支援的場景有：

- 新主機與舊主機的名稱不同
- 現有主機已重新命名

開始之前

由於此工作流程修改了 SnapCenter 儲存庫中的數據，因此建議備份 SnapCenter 儲存庫。如果發生任何資料問題，可以使用備份將 SnapCenter 儲存庫還原為舊狀態。

有關更多信息，請參閱 ["備份 SnapCenter 儲存庫"](#)。

步驟

1. 部署新主機並安裝應用程式。
2. 暫停舊主持人的日程安排。
3. 將所需資源從舊主機移至新主機。
 - a. 從同一儲存在新主機中啟動所需的資料庫。
 - 確保儲存體對應到與舊主機相同的磁碟機或相同的掛載路徑。如果儲存空間未正確映射，則舊主機中建立的備份無法用於復原。



預設情況下，Windows 會自動指派下一個可用的磁碟機。

- 如果啟用了儲存 DR，則應在新主機中安裝相應的儲存。
- b. 如果應用程式版本發生變化，請檢查相容性。
 - c. 僅適用於 Oracle 插件主機，確保 Oracle 及其群組使用者的 UID 和 GID 與舊主機相同。

有關信息，請參閱：

- ["如何將 SQL 資料庫從舊主機遷移到新主機"](#)
- ["如何將 Oracle 資料庫從舊主機遷移到新主機"](#)
- ["如何將 SAP HANA 資料庫移轉到新主機"](#)

4. 將新主機新增至 SnapCenter。
5. 驗證是否發現了所有資源。
6. 執行主機刷新 API：``/<snapcenter_version>/techrefresh/host`` 或 cmdlet：`Invoke-SmTechRefreshHost`。



預設啟用試運行並識別要重新連結的匹配資源。您可以透過執行 API：`「/jobs/{jobid}」` 或 cmdlet `Get-SmJobSummaryReport` 來驗證資源。

如果您已從多個主機遷移資源，則應該為所有主機執行 API 或 cmdlet。如果新主機中的磁碟機或安裝路徑與舊主機不同，則下列復原操作將會失敗：

- SQL 就地還原將會失敗。但是，可以利用 RTAL 功能。
- Oracle 和 SAP HANA 資料庫的還原將會失敗。

如果要遷移到多個主機，則應該對所有主機執行從步驟 1 開始的所有步驟。



您可以在同一台主機上執行多次 API 或 cmdlet，只有在識別出新資源時它才會重新連結。

7. (可選) 從 SnapCenter 中刪除一個或多個舊主機。

相關資訊

有關 API 的信息，您需要訪問 Swagger 頁面。請參閱["如何使用 Swagger API 網頁存取 REST API"](#)。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 ["SnapCenter 軟體 Cmdlet 參考指南"](#)。

儲存系統技術更新

當儲存進行技術更新時，資料將遷移到新的儲存，並且應用程式主機將安裝新的儲存。如果新儲存空間在 SnapCenter 中註冊，SnapCenter 備份工作流將識別新儲存空間並建立快照。

您可以對儲存刷新後建立的新備份執行還原、掛載和複製。但是，當對儲存刷新之前建立的備份執行這些操作時，這些操作將會失敗，因為備份具有舊的儲存詳細資訊。您應該執行儲存技術刷新 API 或 cmdlet 來使用新的儲存詳細資料更新 SnapCenter 中的舊備份。

以下 SnapCenter 插件支援技術更新：

- 適用於 Microsoft SQL Server 的 SnapCenter 插件
- 適用於 Windows 的 SnapCenter 插件
- 適用於 Oracle 資料庫的 SnapCenter 插件
- 適用於 SAP HANA 資料庫的 SnapCenter 插件
- 適用於 Microsoft Exchange Server 的 SnapCenter 插件

支援的用例包括：

- 主儲存刷新
支援儲存技術更新，以新儲取代主儲存。您無法將現有的輔助儲存轉換為主儲存。
- 二級儲存刷新

更新主儲存的備份

當儲存裝置進行技術刷新時，您應該執行儲存技術刷新 API 或 cmdlet 以使用新的儲存詳細資料更新 SnapCenter 中的舊備份。

開始之前

由於此工作流修改了 SnapCenter 儲存庫中的數據，因此建議備份 SnapCenter 儲存庫。如果發生任何資料問題，可以使用備份將 SnapCenter 儲存庫還原為舊狀態。

有關更多信息，請參閱 ["備份 SnapCenter 儲存庫"](#)。

步驟

1. 將資料從舊儲存遷移到新儲存。

有關如何遷移的信息，請參閱：

- "如何將資料遷移到新存儲"
- "如何複製磁碟區並保留所有 Snapshot 副本?"

2. 將主機置於維護模式。
3. 在對應的主機上安裝新的儲存空間並啟動資料庫。

新的儲存應以與先前相同的方式連接到主機。例如，如果它是作為 SAN 連接的，則需要將其作為 SAN 連接。

新的儲存需要安裝在與舊儲存相同的磁碟機或路徑上。

4. 驗證所有資源是否已啟動並正在運作。
5. 在SnapCenter中新增儲存。

確保SnapCenter中各個叢集的 SVM 名稱都是唯一的。如果您在新儲存中使用相同的 SVM 名稱、並且在執行儲存刷新之前可以遷移 SVM 的所有磁碟區、則建議刪除舊叢集中的 SVM 並在SnapCenter中重新發現舊叢集、這將從快取中刪除 SVM。

6. 將主機置於生產模式。
7. 在SnapCenter中，建立已遷移儲存的資源的備份。 SnapCenter需要新的備份來識別最新的儲存佔用空間，並且它將用於更新現有舊備份的元資料。



每當一個新的 LUN 連接到主機時，它都會有一個新的序號。在發現 Windows 檔案系統期間， SnapCenter會將每個唯一序號視為新資源。在儲存技術刷新期間，當新儲存中的 LUN 以相同的磁碟機號碼或路徑連接到主機時， SnapCenter中 Windows 檔案系統的發現會將現有資源標記為已刪除，即使它以相同的磁碟機號碼或路徑安裝，並將新 LUN 顯示為新資源。由於資源被標記為已刪除，因此SnapCenter中不會考慮對其進行儲存技術更新，並且舊資源的所有備份都會遺失。每當發生儲存刷新時，對於 Windows 檔案系統資源，在執行儲存刷新 API 或 cmdlet 之前不應執行資源發現。

8. 運行儲存刷新 API： ``/<snapcenter_version>/techrefresh/primarystorage`` 或 cmdlet： `Invoke-SmTechRefreshPrimaryStorage`。



如果資源配置了啟用複製的策略，則儲存刷新後的最新備份應該具有輔助儲存的詳細資訊。

- a. 如果您使用 SQL 故障轉移群集實例 (FCI) 設置，則備份將在群集層級維護。您應該提供叢集名稱作為儲存技術更新的輸入。
- b. 如果您使用 SQL 可用性群組 (AG) 設置，則備份將在節點層級維護。您應該提供節點名稱作為儲存技術更新的輸入。
- c. 如果您使用 Oracle Real Application Clusters (RAC) 來設置，則可以在任何節點上執行儲存技術刷新。

`IsDryRun` 屬性預設為 `True`。它將識別刷新儲存的資源。您可以透過執行 API：`「<snapcenter_version>/jobs/{jobid}」` 或 cmdlet `Get-SmJobSummaryReport` 來查看資源和變更的儲存詳細資訊。

9. 驗證儲存詳細資訊後，將 `IsDryRun` 屬性設為 `False` 並執行儲存刷新 API：``/<snapcenter_version>/techrefresh/primarystorage`` 或 cmdlet： `Invoke-SmTechRefreshPrimaryStorage`。

這將更新舊備份中的儲存詳細資訊。

您可以在同一台主機上執行多次 API 或 cmdlet，只有在刷新儲存時它才會更新舊備份中的儲存詳細資料。



克隆層次結構無法在ONTAP中遷移。如果正在遷移的儲存在SnapCenter中具有任何克隆元數據，則克隆的資源將被標記為獨立資源。克隆元資料的克隆將被遞歸刪除。

10. (可選) 如果所有快照都未從舊主儲存移動到新主儲存，請執行下列 API：
``/<snapcenter_version>/hosts/primarybackupsexistencecheck`` 或 cmdlet `Invoke-SmPrimaryBackupsExistenceCheck`。

這將對新的主儲存執行快照存在性檢查，並將對應的備份標記為不可用於SnapCenter中的任何操作。

更新輔助儲存的備份

當儲存裝置進行技術刷新時，您應該執行儲存技術刷新 API 或 cmdlet 以使用新的儲存詳細資料更新SnapCenter中的舊備份。

開始之前

由於此工作流程修改了SnapCenter儲存庫中的數據，因此建議備份SnapCenter儲存庫。如果發生任何資料問題，可以使用備份將SnapCenter儲存庫還原為舊狀態。

有關更多信息，請參閱 ["備份SnapCenter儲存庫"](#)。

步驟

1. 將資料從舊儲存遷移到新儲存。

有關如何遷移的信息，請參閱：

- ["如何將資料遷移到新存儲"](#)
- ["如何複製磁碟區並保留所有 Snapshot 副本？"](#)

2. 在主儲存和新的二級儲存之間建立SnapMirror關係，並確保關係狀況良好。
3. 在SnapCenter中，建立已遷移儲存的資源的備份。

SnapCenter需要新的備份來識別最新的儲存佔用空間，並且它將用於更新現有舊備份的元資料。



您應該等到此操作完成。如果在完成之前繼續下一步，SnapCenter將完全遺失舊的輔助快照元資料。

4. 成功建立主機中所有資源的備份後，執行輔助儲存刷新 API：
``/<snapcenter_version>/techrefresh/secondarystorage`` 或 cmdlet：`Invoke-SmTechRefreshSecondaryStorage`。

這將更新給定主機中舊備份的輔助儲存詳細資訊。

如果您想在資源層級執行此功能，請按一下每個資源的*刷新*以更新輔助儲存元資料。

5. 成功更新舊備份後，您可以中斷舊的輔助儲存與主儲存的關係。

解除安裝SnapCenter伺服器 and 插件

卸載SnapCenter插件包

刪除主機的先決條件

您可以使用SnapCenter GUI 刪除主機並卸載單一插件或插件包。您也可以使用SnapCenter Server 主機上的命令列介面 (CLI) 或在任何主機上本機使用 Windows 解除安裝程式 選項卸載遠端主機上的個別外掛程式或外掛程式套件。

從SnapCenter Server 中刪除主機之前，您應該完成先決條件。

- 您應該以管理員身分登入。
- 您應該確保發現作業未在主機上執行。
- 您應該被指派一個具有所需權限的角色來刪除與主機相關的所有物件。否則，刪除操作失敗。
- 如果將主機新增至SnapCenter後修改了 SSH 金鑰，則應確認指紋。
- 如果SnapCenter主機升級到更高版本的SnapCenter，但插件主機仍在運行早期版本的插件，則應確認指紋。

使用基於角色的存取控制刪除主機的先決條件

- 您應該使用具有讀取、刪除主機、安裝、卸載插件和刪除物件權限的 RBAC 角色登入。

物件可以是克隆、備份、資源群組、儲存系統等等。

- 您應該已將 RBAC 使用者新增至 RBAC 角色。
- 您應該將 RBAC 使用者指派給要刪除的主機、插件、憑證、資源群組和儲存系統（用於複製）。
- 您應該以 RBAC 使用者身分登入SnapCenter。

刪除具有透過複製生命週期操作建立的複製的主機的先決條件

- 您應該已經使用 SQL 資料庫的克隆生命週期管理建立了克隆作業。
- 您應該已經建立了一個具有克隆讀取和刪除、資源讀取和刪除、資源組讀取和刪除、儲存讀取和刪除、配置讀取和刪除、掛載、卸載、插件安裝和卸載、主機讀取和刪除權限的 RBAC 角色。
- 您應該已將 RBAC 使用者指派給 RBAC 角色。
- 您應該已將 RBAC 使用者指派給主機、適用於 Microsoft SQL Server 的SnapCenter插件、憑證、複製生命週期資源群組和儲存系統。
- 您應該以 RBAC 使用者身分登入SnapCenter。

有關卸載適用SnapCenter Plug-in for VMware vSphere的信息，請參閱 "[刪除SnapCenter Plug-in for VMware vSphere](#)"。

刪除主機

當SnapCenter伺服器刪除主機時，它會先刪除SnapCenter資源頁面上為該主機列出的備份、複製、複製作業、資源群組和資源，然後卸載主機上的插件包。

關於此任務

- 如果刪除主機，則與該主機關聯的備份、複製和資源群組也將被刪除。
- 當您刪除資源組時，所有相關的計劃也會被刪除。
- 如果主機具有與另一個主機共用的資源群組並且您刪除該主機，則資源群組也會被刪除。
- 您應該使用 *Remove-SmHost* cmdlet 來刪除已退役或無法存取的插件主機。

可以透過執行 `_Get-Help command_name_` 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"

- 刪除主機所需的時間取決於備份的數量和保留設定。這是因為快照已從每個控制器中刪除，且元資料已清除。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 選擇要刪除的主機，然後按一下“刪除”。
4. 對於 Oracle RAC 集群，要從集群中的所有主機中刪除SnapCenter software，請選擇「包含集群的所有主機」。

您也可以刪除叢集的一個節點，然後逐一刪除所有節點。

5. 按一下“確定”。



當您在叢集上卸載並重新安裝主機插件時，叢集資源不會被自動發現。選擇叢集主機名，然後按一下「刷新資源」以自動發現叢集資源。

使用SnapCenter GUI 卸載插件

當您決定不再需要單一插件或插件包時，您可以使用SnapCenter介面將其卸載。

開始之前

- 您應該已經刪除了正在卸載的插件包的資源組。
- 您應該已經分離了與要卸載的插件包的資源組關聯的策略。

關於此任務

您可以卸載單一插件。例如，您可能需要卸載適用於 Microsoft SQL Server 的SnapCenter插件，因為主機資源不足，而您想將該插件移至功能更強大的主機。您也可以卸載整個插件包。例如，您可能需要卸載適用於 Linux 的SnapCenter插件包，其中包括適用於 Oracle 資料庫的SnapCenter插件和適用於 UNIX 的SnapCenter插件。

- 刪除主機包括卸載所有插件。

從SnapCenter中刪除主機時， SnapCenter會在刪除主機之前卸載主機上的所有插件包。

- SnapCenter GUI 一次從一個主機中刪除插件。

使用SnapCenter GUI 時，您一次只能卸載一台主機上的插件。但是，您可以同時執行多個卸載操作。

您也可以使用 *Uninstall-SmHostPackage* cmdlet 和所需參數從多個主機卸載插件。可以透過執行 *_Get-Help command_name_* 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。



從安裝了SnapCenter伺服器的主機上解除安裝適用於 Windows 的SnapCenter插件包將損壞SnapCenter伺服器安裝。除非您確定不再需要SnapCenter伺服器，否則請勿解除安裝適用於 Windows 的SnapCenter插件套件。

步驟

1. 在左側導覽窗格中，按一下「主機」。
2. 在「主機」頁面中，按一下「託管主機」。
3. 在「受管主機」頁面中，選擇要從中解除安裝外掛程式或外掛程式套件的主機。
4. 在您想要刪除的插件旁邊，點擊*刪除*>*提交*。

完成後

您應該等待 5 分鐘，然後再在該主機上重新安裝插件。此時段足以讓SnapCenter GUI 刷新託管主機的狀態。如果立即重新安裝該插件，安裝將會失敗。

如果您要卸載適用於 Linux 的SnapCenter插件包，則可以在下列位置找到卸載特定的日誌檔案：
: */custom_location/snapcenter/log*。

使用 PowerShell cmdlet 解除安裝 Windows 插件

您可以使用SnapCenter Server 主機命令列介面上的 *Uninstall-SmHostPackage* cmdlet 從一個或多個主機卸載單一插件或卸載插件包。

您應該以網域使用者身分登入SnapCenter，並在要卸載插件的每個主機上擁有本機管理員權限。

步驟

1. 啟動 PowerShell。
2. 在SnapCenter Server 主機上，輸入：*Open-SMConnection -SMSbaseUri https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME* 指令，然後輸入您的憑證。
3. 使用 *Uninstall-SmHostPackage* cmdlet 和所需參數卸載 Windows 外掛程式。

可以透過執行 *_Get-Help command_name_* 來取得有關可與 cmdlet 一起使用的參數及其描述的資訊。或者，您也可以參考 "[SnapCenter軟體 Cmdlet 參考指南](#)"。

在主機本地卸載插件

如果您無法從SnapCenter伺服器存取主機，則可以在主機上本機卸載SnapCenter插件。

關於此任務

卸載單一插件或插件包的最佳做法是使用SnapCenter GUI 或使用SnapCenter Server 主機命令列介面上的 Uninstall-SmHostPackage cmdlet。這些程式可協助SnapCenter伺服器隨時了解任何變更。

但是，您可能很少需要在本地卸載插件。例如，您可能已從SnapCenter伺服器執行卸載作業但該作業失敗，或者您卸載了SnapCenter伺服器並且孤立插件仍保留在主機上。



在主機本機卸載外掛程式包不會刪除與主機相關的資料；例如排程作業和備份元資料。



請勿嘗試從控制臺本機卸載適用於 Windows 的SnapCenter插件包。您必須使用SnapCenter GUI 來確保正確解除安裝適用於 Microsoft Windows 的SnapCenter外掛程式。

步驟

1. 在主機系統上，導航至控制台並點擊*卸載程式*。
2. 在程式清單中，選擇要卸載的SnapCenter插件或插件包，然後按一下「卸載」。

Windows 解除安裝所選套件中的所有插件。

使用 CLI 卸載 Linux 或 AIX 的插件包

您可以使用命令列介面卸載適用於 Linux 的SnapCenter插件包或適用於 AIX 的SnapCenter插件包。

開始之前

- 確保已刪除計劃作業
- 確保所有正在執行的作業都已完成。

步

執行 `/custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall` 進行卸載。

在 Windows 主機上解除安裝SnapCenter伺服器

如果您不再希望使用SnapCenter Server 來管理資料保護作業，則可以使用SnapCenter Server 主機上的程式和功能控制面板來解除安裝SnapCenter Server。卸載SnapCenter伺服器將刪除其所有元件。

開始之前

- 確保安裝SnapCenter伺服器的磁碟機上至少有 2 GB 的可用空間。
- 確保安裝SnapCenter伺服器的網域未被刪除。

如果刪除安裝了SnapCenter伺服器的網域，然後嘗試卸載，則操作將會失敗。

- 您應該備份儲存庫資料庫，因為儲存庫資料庫將被清理和卸載。

步驟

1. 在SnapCenter伺服器主機上，導覽至控制台。
2. 確保您處於*類別*視圖。
3. 在“程式”下，按一下“卸載程式”。

程式和功能視窗開啟。

4. 選擇NetApp SnapCenter Server，然後按一下「解除安裝」。

從SnapCenter 4.2 開始，當您解除安裝SnapCenter伺服器時，其所有元件（包括 MySQL 伺服器儲存庫資料庫）都會被解除安裝。

- 從 NLB 叢集中刪除 NLB 節點需要重新啟動SnapCenter Server 主機。如果不重新啟動主機，則嘗試重新安裝SnapCenter伺服器時可能會遇到失敗。
- 您應該手動卸載卸載過程中未刪除的 .NET Framework。

在 Linux 主機上解除安裝SnapCenter伺服器

如果您不再希望使用SnapCenter Server 來管理資料保護作業，則可以解除安裝SnapCenter Server。卸載SnapCenter伺服器將刪除其所有元件。

步驟

1. 執行其中一項操作來解除安裝SnapCenter Server。

如果你想表演...	這樣做...
非互動式卸載	<pre>\$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1</pre> 範例：sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall
互動式卸載	<pre>\$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall</pre> 在確認輸入中輸入 0 以外的任何值以確認卸載。

使用 REST API 實現自動化

使用 REST API 實現SnapCenter自動化

您可以使用 REST API 執行多項SnapCenter管理作業。REST API 透過 Swagger 網頁公開。您可以造訪

`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/` 上的 Swagger 網頁來顯示 REST API 文檔，以及手動發出 API 呼叫。

支援 REST API 的插件有：

- Microsoft SQL Server 外掛
- SAP HANA 資料庫插件
- Oracle 資料庫插件

有關適用於SnapCenter Plug-in for VMware vSphere的信息，請參閱 "[SnapCenter Plug-in for VMware vSphere](#)"

如何在本機存取SnapCenter REST API

您可以使用任何支援 REST 用戶端的程式語言直接存取SnapCenter REST API。流行的語言選擇包括 Python、PowerShell 和 Java。

REST Web 服務基礎

表述性狀態傳輸 (REST) 是一種用於建立分散式 Web 應用程式的樣式。當應用於 Web 服務 API 的設計時，它可以建立一套用於公開基於伺服器的資源並管理其狀態的技術和最佳實踐。它採用主流協議和標準，為管理SnapCenter提供靈活的基礎。

資源和國家代表

資源是基於 Web 系統的基本元件。在建立 REST Web 服務應用程式時，早期設計任務包括：

識別系統或基於伺服器的資源

每個系統都會使用和維護資源。資源可以是文件、業務事務、流程或管理實體。基於 REST Web 服務設計應用程式的首要任務之一就是識別資源。

資源狀態和相關狀態操作的定義

資源總是處於有限數量的狀態之一。應該明確定義狀態以及用於影響狀態變化的相關操作。

URI 端點

每個 REST 資源都必須使用定義明確的尋址方案進行定義和提供。資源所在和識別的端點使用統一資源標識符

(URI)。URI

提供了一個通用框架，用於為網路中的每個資源建立唯一名稱。統一資源定位符 (URL) 是一種用於 Web 服務識別和存取資源的 URI。資源通常以類似文件目錄的層級結構公開。

HTTP 郵件

超文本傳輸協定 (HTTP) 是 Web 服務用戶端和伺服器用來交換資源請求和回應訊息的協定。

作為設計 Web 服務應用程式的一部分，HTTP 方法被對應到資源和對應的狀態管理作業。HTTP 是無狀態的。因此，要將一組相關的請求和回應關聯為一個交易的一部分，必須在請求和回應資料流攜帶的 HTTP 標頭中包含附加資訊。

JSON 格式

雖然可以透過多種方式在 Web 服務用戶端和伺服器之間建置和傳輸訊息，但最受歡迎的選項是 JavaScript 物件表示法 (JSON)。

是一種行業標準，用於以純文字表示簡單資料結構，並用於傳輸描述資源的狀態資訊。SnapCenter REST API 使用 JSON 來格式化每個 HTTP 請求和回應主體中攜帶的資料。

基本運作特性

雖然 REST 確立了一套通用的技術和最佳實踐，但每個 API 的細節可能會因設計選擇而異。

請求和回應 API 事務

每個 REST API 呼叫都以對 SnapCenter 伺服器系統的 HTTP 請求執行，該系統會產生與客戶端相關的回應。該請求和回應對被視為 API 事務。

在使用 API 之前，您應該熟悉可用於控制請求的輸入變數和回應輸出的內容。

支援 CRUD 操作

透過 SnapCenter REST API 可用的每個資源都是基於 CRUD 模型存取的：

- 創造
- 讀
- 更新
- 刪除

對於某些資源，僅支援部分操作。

物件標識符

每個資源實例或物件在建立時都會指派一個唯一識別碼。大多數情況下，該識別碼是 128 位元 UUID。這些識別碼在特定的 SnapCenter 伺服器內是全域唯一的。

發出建立新物件實例的 API 呼叫後，帶有關聯 ID 的 URL 將在 HTTP 回應的位置標頭中傳回給呼叫者。您可以提取標識符，並在後續呼叫中引用資源實例時使用它。



物件標識符的內容和內部結構可能隨時變更。在引用關聯物件時，應僅在適用的 API 呼叫中根據需要使用這些標識符。

物件實例和集合

根據資源路徑和 HTTP 方法，API 呼叫可以應用於特定的物件實例或物件集合。

同步和非同步操作

SnapCenter 以同步或非同步方式執行從客戶端接收的 HTTP 請求。

同步處理

SnapCenter 立即執行請求，如果成功則以 HTTP 狀態碼 200 或 201 回應。

每個使用 GET 方法的請求始終同步執行。此外，如果預計使用 POST 的請求將在兩秒鐘內完成，則這些請求將設計為同步運行。

非同步處理

如果非同步請求有效，SnapCenter 會建立一個背景任務來處理該請求，並建立作業物件來錨定該任務。HTTP 狀態碼 202 與作業物件一起傳回給呼叫者。您應該檢索作業的狀態以確定成功或失敗。

如果預計使用 POST 和 DELETE 方法的請求需要兩秒以上的時間才能完成，則這些請求將設計為非同步運作。

安全

REST API 提供的安全性主要基於 SnapCenter 提供的現有安全功能。API 使用以下安全性：

傳輸層安全性

根據 SnapCenter 配置設置，SnapCenter 伺服器 and 客戶端之間透過網路傳送的所有流量通常使用 TLS 加密。

HTTP 驗證

在 HTTP 級別，基本驗證用於 API 事務。每個請求都會新增一個 HTTP 標頭，其中包含 base64 字串中的使用者名稱和密碼。

控制 API 請求的輸入變數

您可以透過 HTTP 請求中設定的參數和變數來控制如何處理 API 呼叫。

HTTP 方法

SnapCenter REST API 支援的 HTTP 方法如下表所示。



並非所有 HTTP 方法在每個 REST 端點上都可用。

HTTP 方法	描述
得到	檢索資源實例或集合上的物件屬性。
郵政	根據提供的輸入建立一個新的資源實例。
刪除	刪除現有的資源實例。
放	修改現有的資源實例。

請求標頭

您應該在 HTTP 請求中包含幾個標頭。

內容類型

如果請求主體包含 JSON，則此標頭應設定為 *application/json*。

接受

此標頭應設定為 *application/json*。

授權

應設定基本身份驗證，將使用者名稱和密碼編碼為 base64 字串。

請求正文

請求主體的內容根據具體呼叫而有所不同。HTTP 請求主體由以下之一組成：

- 帶有輸入變數的 JSON 對象
- 空的

篩選對象

發出使用 GET 的 API 呼叫時，您可以根據任意屬性限制或過濾傳回的物件。例如，您可以指定要符合的精確值：

<field>=<query value>

除了精確匹配之外，還可以使用其他運算子來傳回一系列值上的物件。SnapCenter REST API 支援下表所示的篩選運算子。

操作員	描述
=	等於
<	少於
>	大於

操作員	描述
<=	小於或等於
>=	大於或等於
更新	或者
!	不等於
*	貪婪通配符

您也可以透過使用 **null** 關鍵字或其否定 **!null** 作為查詢的一部分，根據特定欄位是否設定來傳回物件集合。



任何未設定的欄位通常都會被排除在符合查詢之外。

請求特定物件字段

預設情況下，使用 GET 發出 API 呼叫僅傳回唯一標識一個或多個物件的屬性。這組最小欄位將充當每個物件的鍵，並根據物件類型而有所不同。您可以使用 `fields` 查詢參數有以下幾種方式：

通用或標準字段

指定 **fields=*** 來檢索最常用的物件欄位。這些欄位通常保存在本機伺服器記憶體中或幾乎不需要處理即可存取。這些是使用帶有 URL 路徑鍵（UUID）的 GET 後為物件返回的相同屬性。

所有字段

指定 **fields=**** 來檢索所有物件字段，包括那些需要額外的伺服器處理才能存取的字段。

自訂欄位選擇

使用 **fields=<field_name>** 指定您想要的確切欄位。請求多個欄位時，必須使用逗號分隔值，且不能使用空格。



作為最佳實踐，您應該始終識別所需的特定欄位。您應該只在需要時檢索公共欄位集或所有欄位。哪些欄位被歸類為常見欄位並使用 *fields=** 返回，由 NetApp 根據內部效能分析決定。字段的分類在未來的版本中可能會發生變化。

對輸出集中的物件進行排序

資源集中的記錄將按照物件定義的預設順序傳回。您可以使用 `order\_by` 查詢參數的欄位名稱和排序方向如下：

```
order_by=<field name> asc|desc
```

例如，您可以按降序對類型欄位進行排序，然後按升序對 id 進行排序：

```
order_by=type desc, id asc
```

- 如果指定了排序欄位但未提供方向，則值將按升序排序。
- 當包含多個參數時，必須用逗號分隔欄位。

檢索集合中的物件時進行分頁

當使用 GET 發出 API 呼叫來存取相同類型的物件集合時，SnapCenter 會嘗試根據兩個約束傳回盡可能多的物件。您可以使用請求中的附加查詢參數來控制每個約束。對於特定的 GET 請求，達到的第一個約束將終止該請求，從而限制傳回的記錄數。



如果請求在遍歷所有物件之前結束，則回應包含檢索下一批記錄所需的連結。

限制對象的數量

預設情況下，SnapCenter 對於 GET 請求最多傳回 10,000 個物件。您可以使用 *max_records* 查詢參數來變更此限制。例如：

```
max_records=20
```

根據相關時間限制以及系統中的物件總數，實際傳回的物件數量可能小於有效的最大值。

限制檢索物件所花費的時間

預設情況下，SnapCenter 會在 GET 請求允許的時間內傳回盡可能多的物件。預設超時時間為 15 秒。您可以使用 *return_timeout* 查詢參數來變更此限制。例如：

```
return_timeout=5
```

根據物件數量的相關限制以及系統中物件總數，實際傳回的物件數量可能小於有效的最大值。

縮小結果集

如果需要，您可以將這兩個參數與其他查詢參數組合以縮小結果集。例如，以下內容傳回指定時間之後產生的最多 10 個 EMS 事件：

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

您可以發出多個請求來翻閱物件。每個後續 API 呼叫都應根據最後一個結果集中的最新事件使用新的時間值。

尺寸屬性

一些 API 呼叫以及某些查詢參數使用的輸入值是數字。您可以選擇使用後綴，而不是提供以位元組為單位的整數，如下表所示。

後綴	描述
知識庫	KB 千字節 (1024 位元組) 或千比字節
MB	MB 兆位元組 (KB x 1024 位元組) 或兆比位元組
英國	GB 千兆位元組 (MB x 1024 位元組) 或吉比位元組
結核病	TB 太字節 (GB x 1024 位元組) 或太比位元組
鉛	PB 拍字節 (TB x 1024 位元組) 或 pebibytes

API 回應的解釋

每個 API 請求都會產生一個回應傳回給客戶端。您應該檢查回應以確定它是否成功並根據需要檢索其他資料。

HTTP 狀態碼

SnapCenter REST API 使用的 HTTP 狀態碼如下所述。

程式碼	描述
200	OK 表示呼叫成功，但未建立新物件。
201	建立 物件已成功建立。回應中的位置標頭包含物件的唯一識別碼。
202	已接受 後台作業已啟動以執行請求，但尚未完成。
400	錯誤請求 請求輸入無法辨識或不合適。
401	未經授權的使用者身份驗證失敗。
403	由於授權（RBAC）錯誤，禁止存取被拒絕。
404	未找到請求中引用的資源不存在。
405	方法不允許 此資源不支援請求中的 HTTP 方法。
409	衝突 嘗試建立物件失敗，因為必須先建立不同的物件或要求的物件已存在。
500	內部錯誤 伺服器發生一般內部錯誤。

響應標頭

SnapCenter產生的 HTTP 回應中包含幾個標頭。

地點

當建立一個物件時，位置標頭包含新物件的完整 URL，其中包括指派給該物件的唯一識別碼。

內容類型

這通常是 `application/json`。

回應正文

API 請求產生的回應主體的內容會因物件、處理類型以及請求的成功或失敗而有所不同。回應始終以 JSON 形式呈現。

單一對象

根據請求，可以傳回帶有一組欄位的單一物件。例如，您可以使用 GET 操作，透過唯一識別碼檢索叢集的選定屬性。

多個物件

可以傳回資源集中的多個物件。在所有情況下，都使用一致的格式，`num\_records` 指示記錄數以及包含物件實例陣列的記錄。例如，您可以檢索特定叢集中定義的節點。

作業對象

如果非同步處理 API 調用，則會傳回一個 Job 物件來錨定後台任務。例如，用於更新叢集配置的 PATCH 請求是非同步處理的，並傳回一個 Job 物件。

錯誤對象

如果發生錯誤，則始終傳回 Error 物件。例如，當您嘗試變更未為叢集定義的欄位時，您將收到錯誤。

空的

在某些情況下，不會傳回任何數據，且回應主體包含一個空的 JSON 物件。

錯誤

如果發生錯誤，則會在回應主體中傳回錯誤物件。

格式

錯誤物件具有以下格式：

```
"error": {  
  "message": "<string>",  
  "code": <integer>[,  
  "target": "<string>"]  
}
```

您可以使用代碼值來確定一般錯誤類型或類別，並使用訊息來確定特定錯誤。當可用時，目標欄位包括與錯誤相關的特定使用者輸入。

常見錯誤代碼

常見錯誤代碼如下表所示。特定的 API 呼叫可能包含額外的錯誤代碼。

程式碼	描述
409	具有相同標識符的物件已存在。
400	欄位的值無效或缺失，或提供了額外的欄位。
400	不支援該操作。
405	找不到具有指定標識符的物件。
403	執行請求的權限被拒絕。
409	資源正在使用中。

SnapCenter伺服器 and 插件支援的 REST API

透過SnapCenter REST API 可用的資源按類別組織，如SnapCenter API 文件頁面所示。以下簡要介紹了每個資源及其基本資源路徑，並在適當的情況下提供了額外的使用注意事項。

授權

您可以使用此 API 登入SnapCenter伺服器。此 API 傳回使用者授權令牌，用於驗證後續請求。

域

您可以使用 API 來執行不同的操作。

- 檢索SnapCenter中的所有網域
- 檢索特定域的詳細信息
- 註冊或取消註冊域名
- 修改域名

工作

您可以使用 API 來執行不同的操作。

- 檢索SnapCenter中的所有作業
- 檢索作業狀態
- 取消或停止作業

設定

您可以使用 API 來執行不同的操作。

- 註冊、修改或刪除憑證
- 顯示在SnapCenter伺服器中註冊的憑證信息
- 配置通知設定
- 檢索目前配置為發送電子郵件通知的 SMTP 伺服器的訊息，並顯示 SMTP 伺服器的名稱、收件者的名稱以及寄件者的姓名
- 顯示SnapCenter伺服器登入的多重驗證 (MFA) 配置
- 為SnapCenter伺服器登入啟用或停用並配置 MFA
- 建立設定 MFA 所需的設定文件

主機

您可以使用 API 來執行不同的操作。

- 查詢所有SnapCenter主機
- 從SnapCenter中刪除一個或多個主機
- 透過名稱檢索主機
- 檢索主機上的所有資源
- 使用資源 ID 檢索資源
- 檢索插件配置詳細信息
- 配置插件主機
- 檢索 Microsoft SQL Server 主機外掛程式的所有資源
- 檢索 Oracle 資料庫主機插件的所有資源
- 檢索自訂應用程式主機插件的所有資源
- 檢索 SAP HANA 主機插件的所有資源
- 檢索已安裝的插件
- 在現有主機上安裝插件
- 升級主機包
- 從現有主機中刪除插件
- 在主機上新增插件
- 新增或修改主機
- 取得Linux主機的簽名
- 註冊Linux主機的簽名
- 將主機置於維護或生產模式
- 啟動或重新啟動主機上的插件服務
- 重新命名主機

資源

您可以使用 API 來執行不同的操作。

- 檢索所有資源
- 使用資源 ID 檢索資源
- 檢索 Microsoft SQL Server 主機外掛程式的所有資源
- 檢索 Oracle 資料庫主機插件的所有資源
- 檢索自訂應用程式主機插件的所有資源
- 檢索 SAP HANA 主機插件的所有資源
- 使用金鑰檢索 Microsoft SQL Server 資源
- 使用密鑰檢索自訂資源
- 修改自訂應用程式主機插件的資源

- 使用金鑰刪除自訂應用程式主機插件的資源
- 使用密鑰檢索 SAP HANA 資源
- 修改 SAP HANA 主機插件的資源
- 使用金鑰刪除 SAP HANA 主機插件的資源
- 使用金鑰檢索 Oracle 資源
- 建立 Oracle 應用程式捲資源
- 修改 Oracle 應用程式捲資源
- 使用金鑰刪除 Oracle 應用程式捲資源
- 檢索 Oracle 資源的輔助詳細信息
- 使用 Microsoft SQL Server 外掛程式備份 Microsoft SQL Server 資源
- 使用 Oracle 資料庫插件備份 Oracle 資源
- 使用自訂應用程式外掛程式備份自訂資源
- 配置 SAP HANA 資料庫
- 配置 Oracle 資料庫
- 恢復 SQL 資料庫備份
- 還原 Oracle 資料庫備份
- 恢復自訂應用程式備份
- 建立 SAP HANA 資源
- 使用自訂應用程式外掛程式保護自訂資源
- 使用 Microsoft SQL Server 外掛程式保護 Microsoft SQL Server 資源
- 修改受保護的 Microsoft SQL Server 資源
- 刪除對 Microsoft SQL Server 資源的保護
- 使用 Oracle 資料庫插件保護 Oracle 資源
- 修改受保護的 Oracle 資源
- 刪除 Oracle 資源的保護
- 使用自訂應用程式外掛程式從備份中克隆資源
- 使用 Oracle 資料庫外掛程式從備份克隆 Oracle 應用程式捲
- 使用 Microsoft SQL Server 外掛程式從備份複製 Microsoft SQL Server 資源
- 建立 Microsoft SQL Server 資源的複製生命週期
- 修改 Microsoft SQL Server 資源的複製生命週期
- 刪除 Microsoft SQL Server 資源的複製生命週期
- 將現有的 Microsoft SQL Server 資料庫從本機磁碟移至 NetApp LUN
- 為 Oracle 資料庫建立克隆規範文件
- 啟動 Oracle 資源的按需克隆刷新作業

- 使用克隆規範檔案從備份建立 Oracle 資源
- 將資料庫還原到輔助副本並將資料庫重新加入可用性群組
- 建立 Oracle 應用程式捲資源

備份

您可以使用 API 來執行不同的操作。

- 按備份名稱、類型、插件、資源或日期檢索備份詳細信息
- 檢索所有備份
- 檢索備份詳細信息
- 重新命名或刪除備份
- 掛載 Oracle 備份
- 解除安裝 Oracle 備份
- 編目 Oracle 備份
- 取消編目 Oracle 備份
- 取得執行時間點復原所需的所有備份

複製

您可以使用 API 來執行不同的操作。

- 建立、顯示、修改和刪除 Oracle 資料庫克隆規範文件
- 顯示 Oracle 資料庫克隆層次結構
- 檢索克隆詳細信息
- 檢索所有克隆
- 刪除克隆
- 透過 ID 檢索克隆詳細信息
- 啟動 Oracle 資源的按需克隆刷新作業
- 使用克隆規範檔案從備份克隆 Oracle 資源

克隆分裂

您可以使用 API 來執行不同的操作。

- 估計克隆資源的克隆分裂操作
- 檢索克隆分裂操作的狀態
- 啟動或停止克隆分裂操作

資源組

您可以使用 API 來執行不同的操作。

- 檢索所有資源組的詳細信息
- 按名稱檢索資源組
- 為自訂應用程式的插件建立資源組
- 為 Microsoft SQL Server 外掛程式建立資源組
- 為 Oracle 資料庫外掛程式建立資源組
- 修改自訂應用程式插件的資源群組
- 修改 Microsoft SQL Server 外掛程式的資源群組
- 修改 Oracle 資料庫插件的資源組
- 建立、修改或刪除 Microsoft SQL Server 外掛程式資源群組的複製生命週期
- 備份資源組
- 將資源組置於維修或生產模式
- 刪除資源組

政策

您可以使用 API 來執行不同的操作。

- 檢索策略詳細信息
- 按名稱檢索策略詳細信息
- 刪除策略
- 建立現有策略的副本
- 建立或修改自訂應用程式插件的策略
- 建立或修改 Microsoft SQL Server 外掛程式的策略
- 建立或修改 Oracle 資料庫插件的策略
- 建立或修改 SAP HANA 資料庫插件的策略

儲存

您可以使用 API 來執行不同的操作。

- 檢索所有股份
- 按名稱檢索共享
- 建立或刪除共享
- 檢索儲存詳細信息
- 按名稱檢索儲存詳細信息

- 建立、修改或刪除存儲
- 發現儲存叢集上的資源
- 檢索儲存叢集上的資源

分享

您可以使用 API 來執行不同的操作。

- 檢索共享的詳細信息
- 檢索所有股票的詳細信息
- 在儲存空間上建立或刪除共享
- 按名稱檢索共享

外掛

您可以使用 API 來執行不同的操作。

- 列出主機的所有插件
- 使用金鑰檢索 Microsoft SQL Server 資源
- 使用金鑰修改自訂資源
- 使用金鑰刪除自訂資源
- 使用密鑰檢索 SAP HANA 資源
- 使用金鑰修改 SAP HANA 資源
- 使用密鑰刪除 SAP HANA 資源
- 使用金鑰檢索 Oracle 資源
- 使用金鑰修改 Oracle 應用程式捲資源
- 使用金鑰刪除 Oracle 應用程式捲資源
- 使用 Microsoft SQL Server 外掛程式和金鑰備份 Microsoft SQL Server 資源
- 使用 Oracle 資料庫外掛程式和金鑰備份 Oracle 資源
- 使用自訂應用程式外掛程式和金鑰備份自訂應用程式資源
- 使用金鑰配置 SAP HANA 資料庫
- 使用金鑰配置 Oracle 資料庫
- 使用密鑰恢復自訂應用程式備份
- 建立 SAP HANA 資源
- 建立 Oracle 應用程式捲資源
- 使用自訂應用程式外掛程式保護自訂資源
- 使用 Microsoft SQL Server 外掛程式保護 Microsoft SQL Server 資源
- 修改受保護的 Microsoft SQL Server 資源

- 刪除對 Microsoft SQL Server 資源的保護
- 使用 Oracle 資料庫插件保護 Oracle 資源
- 修改受保護的 Oracle 資源
- 刪除 Oracle 資源的保護
- 使用自訂應用程式外掛程式從備份中克隆資源
- 使用 Oracle 資料庫外掛程式從備份克隆 Oracle 應用程式捲
- 使用 Microsoft SQL Server 外掛程式從備份複製 Microsoft SQL Server 資源
- 建立 Microsoft SQL Server 資源的複製生命週期
- 修改 Microsoft SQL Server 資源的複製生命週期
- 刪除 Microsoft SQL Server 資源的複製生命週期
- 為 Oracle 資料庫建立克隆規範文件
- 啟動 Oracle 資源的按需複製生命週期
- 使用克隆規範檔案從備份克隆 Oracle 資源

報告

您可以使用 API 來執行不同的操作。

- 檢索各個外掛程式的備份、還原和克隆作業的報告
- 新增、運行、刪除或修改計劃
- 檢索計劃報告的數據

警報

您可以使用 API 來執行不同的操作。

- 檢索所有警報
- 透過 ID 檢索警報
- 刪除多個警報或按 ID 刪除警報

RBAC

您可以使用 API 來執行不同的操作。

- 檢索使用者、群組和角色的詳細信息
- 新增或刪除用戶
- 將使用者指派給角色
- 取消指派使用者的角色
- 建立、修改或刪除角色
- 將群組分配給角色

- 取消分配組的角色
- 新增或刪除群組
- 建立現有角色的副本
- 為使用者或群組分配或取消分配資源

配置

您可以使用 API 來執行不同的操作。

- 查看配置設定
- 修改配置設定

證書設定

您可以使用 API 來執行不同的操作。

- 查看SnapCenter伺服器或插件主機的憑證狀態
- 修改SnapCenter伺服器或插件主機的憑證設置

儲存庫

您可以使用 API 來執行不同的操作。

- 檢索儲存庫備份
- 查看儲存庫的設定資訊
- 保護並恢復SnapCenter儲存庫
- 取消保護SnapCenter儲存庫
- 重建和故障轉移儲存庫

版本

您可以使用此 API 查看SnapCenter版本。

如何使用 **Swagger API** 網頁存取 **REST API**

REST API 透過 Swagger 網頁公開。您可以造訪 Swagger 網頁來顯示SnapCenter Server REST API，以及手動發出 API 呼叫。您可以使用 REST API 來協助管理您的SnapCenter 伺服器或執行資料保護作業。

您應該知道要執行 REST API 的SnapCenter伺服器的管理 IP 位址或網域名稱。

您不需要特殊權限來執行 REST API 用戶端。任何使用者都可以造訪 Swagger 網頁。透過 REST API 存取的物件上的相應權限取決於產生用於登入 REST API 的令牌的使用者。

步驟

1. 在瀏覽器中，輸入 URL 以存取 Swagger 網頁，格式為
`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/`。



確保 REST API URL 不包含以下字元：+、\、\、% 和 &。

2. 在 **Swagger Explore** 欄位中，如果 Swagger API 文件未自動顯示，請鍵入
：`https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/ SnapCenter.yaml`
3. 按一下“探索”。

顯示 API 資源類型或類別的清單。

4. 按一下 API 資源類型可顯示該資源類型中的 API。

如果在執行 SnapCenter REST API 時遇到意外行為，您可以使用日誌檔案找出原因並解決問題。您可以透過點擊「監控」>「日誌」>「下載」從 SnapCenter 使用者介面下載日誌檔案。

開始使用 REST API

您可以使用 SnapCenter REST API 快速開始。在開始在即時設定中使用更複雜的工作流程之前，存取 API 可以提供一些視角。

你好世界

您可以在系統上執行一個簡單的命令來開始使用 SnapCenter REST API 並確認其可用性。

開始之前

- 確保您的系統上有 Curl 實用程式。
- SnapCenter 伺服器的 IP 位址或主機名
- 有權存取 SnapCenter REST API 的帳戶的使用者名稱和密碼。



如果您的憑證包含特殊字符，則需要根據您使用的 shell 以 Curl 可接受的方式對其進行格式化。例如，您可以在每個特殊字元前插入反斜杠，或者將整個 `username:password` 單引號中的字串。

步

在命令列介面，執行以下命令來檢索插件資訊：

```
curl -X GET -u username:password -k  
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

範例：

```
curl -X GET -u admin:password -k  
"https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

法律聲明

法律聲明提供對版權聲明、商標、專利等的存取。

版權

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

商標

NETAPP、NETAPP 標誌和NetApp商標頁面上列出的標誌是NetApp, Inc. 的商標。其他公司和產品名稱可能是其各自所有者的商標。

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

專利

NetApp擁有的專利的最新清單可在以下位置找到：

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

隱私權政策

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

開源

通知文件提供有關NetApp軟體中使用的第三方版權和許可的資訊。

["SnapCenter 6.1 通知"](#)

版權資訊

Copyright © 2025 NetApp, Inc. 版權所有。台灣印製。非經版權所有人事先書面同意，不得將本受版權保護文件的任何部分以任何形式或任何方法（圖形、電子或機械）重製，包括影印、錄影、錄音或儲存至電子檢索系統中。

由 NetApp 版權資料衍伸之軟體必須遵守下列授權和免責聲明：

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

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

本手冊所述之產品受到一項（含）以上的美國專利、國外專利或申請中專利所保障。

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

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

商標資訊

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