# Documentazione SnapCenter software

## SnapCenter software

NetApp
November 06, 2025

This PDF was generated from https://docs.netapp.com/it-it/snapcenter-61/index.html on November 06, 2025. Always check docs.netapp.com for the latest.

# Sommario


Documentazione SnapCenter software . . . 1
Note di rilascio . . . 2
- Note di rilascio . . . 2
- Percorsi di aggiornamento supportati per SnapCenter . . . 2

Iniziare . . . 3
- Scopri di più sul SnapCenter software . . . 3
  - Panoramica SnapCenter . . . 3
  - Funzionalità di sicurezza in SnapCenter . . . 7
  - Controllo degli accessi basato sui ruoli in SnapCenter . . . 9
  - Ripristino di emergenza in SnapCenter . . . 14
  - Licenze richieste da SnapCenter . . . 15
  - Sincronizzazione attiva SnapMirror in SnapCenter . . . 17
  - Concetti chiave della protezione dei dati . . . 18
  - Sistemi di archiviazione e applicazioni supportati da SnapCenter . . . 20
  - Metodi di autenticazione per le credenziali SnapCenter . . . 20
- Operazioni SnapCenter supportate per sistemi ASA r2 . . . 22
- Avvio rapido del SnapCenter software . . . 23

Installa e configura SnapCenter Server . . . 24
- Prepararsi all'installazione di SnapCenter Server . . . 24
  - Requisiti per installare SnapCenter Server . . . 24
  - Registrati per accedere al SnapCenter software . . . 31
  - Autenticazione a più fattori (MFA) . . . 31
- Installare il server SnapCenter . . . 41
  - Installa SnapCenter Server sull'host Windows . . . 41
  - Installa SnapCenter Server sull'host Linux . . . 46
  - Registra SnapCenter . . . 50
  - Accedi a SnapCenter utilizzando l'autorizzazione RBAC . . . 50
- Configurare il server SnapCenter . . . 54
  - Aggiungere e predisporre il sistema di archiviazione . . . 54
  - Aggiungi licenze basate sul controller SnapCenter Standard . . . 75
  - Configurare l'alta disponibilità . . . 80
  - Configurare il controllo degli accessi basato sui ruoli (RBAC) . . . 84
  - Configurare le impostazioni del registro di controllo . . . 113
  - Configurare connessioni MySQL protette con SnapCenter Server . . . 114
- Configurare l'autenticazione basata su certificato . . . 120
  - Abilita l'autenticazione basata sul certificato . . . 120
  - Esportare i certificati dell'autorità di certificazione (CA) da SnapCenter Server . . . 120
  - Importa il certificato CA negli host dei plug-in di Windows . . . 121
  - Importa il certificato CA negli host del plug-in UNIX . . . 122
  - Esportare i certificati SnapCenter . . . 123
- Configurare il certificato CA per l'host Windows . . . 124
  - Genera file CSR del certificato CA . . . 124
  - Importa certificati CA . . . 124

Ottieni l'impronta digitale del certificato CA . . . 125
Configurare il certificato CA con i servizi plug-in host di Windows . . . 126
Configurare il certificato CA con il sito SnapCenter . . . 126
Abilita i certificati CA per SnapCenter . . . 127
Configurare il certificato CA per l'host Linux . . . 128
Configurare il certificato nginx . . . 128
Configurare il certificato del registro di controllo . . . 128
Configurare il certificato dei servizi SnapCenter . . . 128
Configurare e abilitare la comunicazione SSL bidirezionale sull'host Windows . . . 129
Configurare la comunicazione SSL bidirezionale sull'host Windows . . . 129
Abilita la comunicazione SSL bidirezionale sull'host Windows . . . 132
Configurare e abilitare la comunicazione SSL bidirezionale sull'host Linux . . . 133
Configurare la comunicazione SSL bidirezionale sull'host Linux . . . 133
Abilita la comunicazione SSL sull'host Linux . . . 134
Configurare Active Directory, LDAP e LDAPS . . . 135
Registra domini Active Directory non attendibili . . . 135
Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory . . . 137
Configurare il certificato client CA per LDAPS . . . 137
Proteggere i database di Microsoft SQL Server . . . 138
Plug-in SnapCenter per Microsoft SQL Server . . . 138
Panoramica del plug-in SnapCenter per Microsoft SQL Server . . . 138
Cosa puoi fare con il plug-in SnapCenter per Microsoft SQL Server . . . 138
Funzionalità del plug-in SnapCenter per Microsoft SQL Server . . . 139
Supporto per il mapping LUN asimmetrico nei cluster Windows . . . 140
Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft SQL Server . . . 141
Raccomandazioni sul layout di archiviazione per il plug-in SnapCenter per Microsoft SQL Server . . . 143
Privilegi ONTAP minimi richiesti per il plug-in SQL . . . 145
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per il plug-in per SQL Server . . . 148
Strategia di backup per le risorse di SQL Server . . . 148
Strategia di ripristino per SQL Server . . . 153
Definire una strategia di clonazione per SQL Server . . . 156
Prepararsi all'installazione del plug-in SnapCenter per Microsoft SQL Server . . . 157
Flusso di lavoro di installazione per il plug-in SnapCenter per Microsoft SQL Server . . . 157
Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft SQL Server . . . 157
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 158
Imposta le credenziali per il pacchetto plug-in SnapCenter per Windows . . . 159
Configurare le credenziali per una singola risorsa di SQL Server . . . 161
Configurare gMSA su Windows Server 2016 o versioni successive . . . 163
Installa il plug-in SnapCenter per Microsoft SQL Server . . . 164
Configurare il certificato CA . . . 170
Configurare il ripristino di emergenza . . . 173
Installa il SnapCenter Plug-in for VMware vSphere . . . 175
Distribuisci il certificato CA . . . 176
Configurare il file CRL . . . 176

Prepararsi alla protezione dei dati . . . 176
Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft SQL Server . . . 176
Come vengono utilizzate risorse, gruppi di risorse e criteri per proteggere SQL Server . . . 177
Eseguire il backup del database, dell'istanza o del gruppo di disponibilità di SQL Server . . . 178
Flusso di lavoro di backup . . . 178
Determinare se le risorse sono disponibili per il backup . . . 179
Migrare le risorse al sistema di archiviazione NetApp . . . 181
Creare criteri di backup per i database di SQL Server . . . 182
Creare gruppi di risorse e associare criteri per SQL Server . . . 188
Crea gruppi di risorse e abilita la protezione secondaria per le risorse di Microsoft SQL Server sui sistemi ASA r2 . . . 191
Requisiti per il backup delle risorse SQL . . . 194
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell . . . 194
Eseguire il backup delle risorse SQL . . . 195
Eseguire il backup dei gruppi di risorse di SQL Server . . . 201
Monitorare le operazioni di backup delle risorse SQL nella pagina SnapCenter Jobs . . . 202
Annullare il plug-in SnapCenter per le operazioni di backup di Microsoft SQL Server . . . 203
Visualizza i backup e i cloni di SQL Server nella pagina Topologia . . . 204
Pulisci il conteggio dei backup secondari utilizzando i cmdlet di PowerShell . . . 206
Ripristinare le risorse di SQL Server . . . 206
Ripristina flusso di lavoro . . . 206
Requisiti per il ripristino di un database . . . 207
Ripristinare i backup del database di SQL Server . . . 208
Ripristinare un database SQL Server da un archivio secondario . . . 215
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 216
Reseed dei database del gruppo di disponibilità . . . 218
Monitorare le operazioni di ripristino delle risorse SQL . . . 219
Annulla le operazioni di ripristino delle risorse SQL . . . 220
Clona le risorse del database SQL Server . . . 220
Flusso di lavoro di clonazione . . . 220
Clonazione da un backup del database SQL Server . . . 221
Eseguire il ciclo di vita della clonazione . . . 229
Monitorare le operazioni di clonazione del database SQL . . . 232
Annulla le operazioni di clonazione delle risorse SQL . . . 232
Dividi un clone . . . 233
Proteggere i database SAP HANA . . . 235
Plug-in SnapCenter per database SAP HANA . . . 235
Panoramica del plug-in SnapCenter per il database SAP HANA . . . 235
Cosa puoi fare utilizzando il plug-in SnapCenter per il database SAP HANA . . . 235
Funzionalità del plug-in SnapCenter per il database SAP HANA . . . 235
Tipi di archiviazione supportati dal plug-in SnapCenter per il database SAP HANA . . . 236
Privilegi ONTAP minimi richiesti per il plug-in SAP HANA . . . 237
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per i database SAP HANA . . . 240
Strategia di backup per database SAP HANA . . . 240

Strategia di ripristino e recupero per database SAP HANA . . . 244
Prepararsi all'installazione del plug-in SnapCenter per il database SAP HANA . . . 246
Flusso di lavoro di installazione del plug-in SnapCenter per il database SAP HANA . . . 246
Prerequisiti per l'aggiunta di host e l'installazione del plug-in SnapCenter per il database SAP HANA . . . 246
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 250
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux . . . 251
Imposta le credenziali per il plug-in SnapCenter per il database SAP HANA . . . 252
Configurare gMSA su Windows Server 2016 o versioni successive . . . 255
Installa il plug-in SnapCenter per i database SAP HANA . . . 256
Configurare il certificato CA . . . 262
Installa il SnapCenter Plug-in for VMware vSphere . . . 269
Distribuisci il certificato CA . . . 270
Configurare il file CRL . . . 270
Prepararsi alla protezione dei dati . . . 270
Prerequisiti per l'utilizzo del plug-in SnapCenter per il database SAP HANA . . . 270
Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere i database SAP HANA . . . 270
Eseguire il backup delle risorse SAP HANA . . . 271
Eseguire il backup delle risorse SAP HANA . . . 271
Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA . . . 272
Scopri le risorse e prepara i contenitori di database multitenant per la protezione dei dati . . . 273
Aggiungere manualmente le risorse all'host del plug-in . . . 275
Creare policy di backup per i database SAP HANA . . . 277
Crea gruppi di risorse e allega criteri . . . 283
Crea gruppi di risorse e abilita la protezione secondaria per le risorse SAP HANA sui sistemi ASA r2 . . . 287
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per il database SAP HANA . . . 290
Eseguire il backup dei database SAP HANA . . . 291
Eseguire il backup dei gruppi di risorse . . . 299
Monitorare le operazioni di backup dei database SAP HANA . . . 299
Annulla le operazioni di backup per SAP HANA . . . 300
Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia . . . 301
Ripristinare i database SAP HANA . . . 303
Ripristina flusso di lavoro . . . 303
Ripristina e recupera un backup di risorse aggiunto manualmente . . . 304
Ripristina e recupera un backup del database rilevato automaticamente . . . 308
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 312
Monitorare le operazioni di ripristino dei database SAP HANA . . . 314
Clona i backup delle risorse SAP HANA . . . 315
Flusso di lavoro di clonazione . . . 315
Clonare un backup del database SAP HANA . . . 316
Monitorare le operazioni di clonazione del database SAP HANA . . . 320
Dividi un clone . . . 320
Eliminare o dividere i cloni del database SAP HANA dopo l'aggiornamento SnapCenter . . . 322
Proteggere i database Oracle . . . 323

Panoramica del plug-in SnapCenter per Oracle Database . . . 323
Cosa puoi fare con il plug-in per Oracle Database . . . 323
Caratteristiche del plug-in per Oracle Database . . . 323
Tipi di archiviazione supportati dal plug-in per Oracle Database . . . 325
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per Plug-in per Oracle . . . 327
Privilegi ONTAP minimi richiesti per il plug-in per Oracle . . . 327
Installa il plug-in SnapCenter per Oracle Database . . . 329
Flusso di lavoro di installazione del plug-in SnapCenter per Oracle Database . . . 330
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto plug-in per Linux o AIX . . . 330
Aggiungi host e installa il pacchetto plug-in per Linux o AIX utilizzando l'interfaccia grafica . . . 339
Metodi alternativi per installare il pacchetto Plug-in per Linux o AIX . . . 343
Configurare il servizio SnapCenter Plug-in Loader . . . 346
Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux . . . 349
Abilita i certificati CA per i plug-in . . . 351
Importa dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter . . . 352
Installa il SnapCenter Plug-in for VMware vSphere . . . 358
Distribuisci il certificato CA . . . 358
Configurare il file CRL . . . 358
Prepararsi alla protezione dei database Oracle . . . 358
Eseguire il backup dei database Oracle . . . 359
Panoramica della procedura di backup . . . 359
Informazioni sulla configurazione del backup . . . 360
Requisiti per il backup di un database Oracle . . . 373
Scopri i database Oracle disponibili per il backup . . . 373
Creare policy di backup per i database Oracle . . . 375
Crea gruppi di risorse e allega policy per i database Oracle . . . 381
Crea gruppi di risorse e abilita la protezione secondaria per le risorse Oracle sui sistemi ASA r2 . . . 384
Eseguire il backup delle risorse Oracle . . . 386
Eseguire il backup dei gruppi di risorse del database Oracle . . . 389
Monitorare il backup del database Oracle . . . 390
Altre operazioni di backup . . . 391
Montare e smontare i backup del database . . . 395
Montare un backup del database . . . 396
Smontare un backup del database . . . 397
Ripristinare e recuperare i database Oracle . . . 397
Ripristina flusso di lavoro . . . 398
Definire una strategia di ripristino e recupero per i database Oracle . . . 398
Variabili di ambiente predefinite per ripristinare specifici prescript e postscript . . . 403
Requisiti per il ripristino di un database Oracle . . . 404
Ripristinare e recuperare il database Oracle . . . 405
Ripristina e recupera gli spazi tabella utilizzando il ripristino point-in-time . . . 410
Ripristina e recupera il database collegabile utilizzando il ripristino point-in-time . . . 411
Ripristinare e recuperare i database Oracle utilizzando i comandi UNIX . . . 414
Monitorare le operazioni di ripristino del database Oracle . . . 414
Annulla le operazioni di ripristino del database Oracle . . . 415

Clona il database Oracle . . . 416
Flusso di lavoro di clonazione . . . 416
Definire una strategia di clonazione per i database Oracle . . . 417
Variabili di ambiente predefinite per prescript e postscript specifici del clone . . . 418
Requisiti per la clonazione di un database Oracle . . . 419
Clonare un backup del database Oracle . . . 421
Clonare un database collegabile . . . 431
Clonare i backup del database Oracle utilizzando i comandi UNIX . . . 436
Dividi un clone di database Oracle . . . 436
Clone diviso di un database collegabile . . . 437
Monitorare le operazioni di clonazione del database Oracle . . . 438
Aggiorna un clone . . . 439
Elimina il clone di un database collegabile . . . 440
Gestire i volumi delle applicazioni . . . 440
Cosa sono i volumi di applicazione . . . 440
Aggiungere volumi di applicazione . . . 441
Volumi di applicazione di backup . . . 442
Backup del volume dell'applicazione clonata . . . 444
Proteggere i file system di Windows . . . 447
Plug-in SnapCenter per concetti di Microsoft Windows . . . 447
Panoramica del plug-in SnapCenter per Microsoft Windows . . . 447
Cosa puoi fare con il plug-in SnapCenter per Microsoft Windows . . . 447
Funzionalità del plug-in SnapCenter per Windows . . . 448
Come SnapCenter esegue il backup dei file system di Windows . . . 449
Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft Windows . . . 449
Privilegi ONTAP minimi richiesti per il plug-in di Windows . . . 451
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault . . . 453
Definire una strategia di backup per i file system di Windows . . . 454
Origini e destinazioni dei cloni per i file system di Windows . . . 456
Installa il plug-in SnapCenter per Microsoft Windows . . . 456
Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Windows . . . 456
Requisiti di installazione per il plug-in SnapCenter per Microsoft Windows . . . 457
Aggiungi host e installa il plug-in SnapCenter per Microsoft Windows . . . 461
Installa il plug-in SnapCenter per Microsoft Windows su più host remoti utilizzando i cmdlet di PowerShell . . . 465
Installare il plug-in SnapCenter per Microsoft Windows in modo silenzioso dalla riga di comando . . . 465
Monitorare lo stato di installazione del pacchetto plug-in SnapCenter . . . 467
Configurare il certificato CA . . . 468
Installa il SnapCenter Plug-in for VMware vSphere . . . 471
Distribuisci il certificato CA . . . 471
Configurare il file CRL . . . 471
Eseguire il backup dei file system di Windows . . . 471
Eseguire il backup dei file system di Windows . . . 471
Determinare la disponibilità delle risorse per i file system di Windows . . . 473
Creare criteri di backup per i file system di Windows . . . 473

Creare gruppi di risorse per i file system di Windows . . . 477
Crea gruppi di risorse e abilita la protezione secondaria per i file system Windows sui sistemi ASA r2 . . . 479
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell . . . 482
Eseguire il backup di una singola risorsa su richiesta per i file system di Windows . . . 483
Eseguire il backup dei gruppi di risorse per i file system di Windows . . . 487
Monitorare le operazioni di backup . . . 488
Annulla le operazioni di backup . . . 489
Visualizza i backup e i cloni correlati nella pagina Topologia . . . 490
Pulisci il conteggio dei backup secondari utilizzando i cmdlet di PowerShell . . . 492
Ripristinare i file system di Windows . . . 493
Ripristinare i backup del file system di Windows . . . 493
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 498
Monitorare le operazioni di ripristino . . . 501
Annulla le operazioni di ripristino . . . 502
Clonare i file system di Windows . . . 503
Clona da un backup del file system di Windows . . . 503
Monitorare le operazioni di clonazione . . . 509
Annulla le operazioni di clonazione . . . 510
Dividi un clone . . . 511
Proteggere i database di Microsoft Exchange Server . . . 513
Concetti del plug-in SnapCenter per Microsoft Exchange Server . . . 513
Panoramica del plug-in SnapCenter per Microsoft Exchange Server . . . 513
Cosa puoi fare con il plug-in SnapCenter per Microsoft Exchange Server . . . 513
Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft Windows e per Microsoft Exchange Server . . . 514
Privilegi ONTAP minimi richiesti per il plug-in di Exchange . . . 515
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault . . . 518
Definire una strategia di backup per le risorse di Exchange Server . . . 518
Definire una strategia di ripristino per i database di Exchange . . . 521
Installa il plug-in SnapCenter per Microsoft Exchange Server . . . 522
Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Exchange Server . . . 522
Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft Exchange Server . . . 523
Imposta le credenziali per il plug-in SnapCenter per Windows . . . 526
Configurare gMSA su Windows Server 2016 o versioni successive . . . 528
Aggiungi host e installa il plug-in per Exchange . . . 529
Installa il plug-in per Exchange dall’host del server SnapCenter utilizzando i cmdlet di PowerShell . . . 535
Installare il plug-in SnapCenter per Exchange in modo silenzioso dalla riga di comando . . . 535
Monitorare lo stato di installazione del pacchetto plug-in SnapCenter . . . 537
Configurare il certificato CA . . . 538
Configurare SnapManager 7.x affinché Exchange e SnapCenter coesistano . . . 541
Installa il SnapCenter Plug-in for VMware vSphere . . . 543
Distribuisci il certificato CA . . . 543
Configurare il file CRL . . . 543
Prepararsi alla protezione dei dati . . . 543

Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft Exchange Server . . . 544
Come vengono utilizzate risorse, gruppi di risorse e criteri per proteggere Exchange Server . . . 544
Eseguire il backup delle risorse di Exchange . . . 545
Flusso di lavoro di backup . . . 545
Verifica del database di Exchange e del backup . . . 546
Determina se le risorse di Exchange sono disponibili per il backup . . . 546
Creare criteri di backup per i database di Exchange Server . . . 548
Creare gruppi di risorse e allegare criteri per i server Exchange . . . 555
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per Exchange Server . . . 558
Eseguire il backup dei database di Exchange . . . 559
Eseguire il backup dei gruppi di risorse di Exchange . . . 564
Monitorare le operazioni di backup . . . 565
Annulla le operazioni di backup per il database di Exchange . . . 566
Visualizza i backup di Exchange nella pagina Topologia . . . 567
Ripristinare le risorse di Exchange . . . 568
Ripristina flusso di lavoro . . . 568
Requisiti per il ripristino di un database di Exchange . . . 569
Ripristinare i database di Exchange . . . 569
Recupero granulare di e-mail e caselle di posta . . . 574
Ripristinare un database di Exchange Server da un archivio secondario . . . 574
Reinizializzare una replica di un nodo Exchange passivo . . . 575
Ripristinare il seeding di una replica utilizzando i cmdlet di PowerShell per il database di Exchange . . . 576
Monitorare le operazioni di ripristino . . . 576
Annulla le operazioni di ripristino per il database di Exchange . . . 577
Proteggi IBM Db2 . . . 579
Plug-in SnapCenter per IBM Db2 . . . 579
Panoramica del plug-in SnapCenter per IBM Db2 . . . 579
Cosa puoi fare utilizzando il plug-in SnapCenter per IBM Db2 . . . 579
Funzionalità del plug-in SnapCenter per IBM Db2 . . . 579
Tipi di archiviazione supportati dal plug-in SnapCenter per IBM Db2 . . . 580
Privilegi ONTAP minimi richiesti per il plug-in IBM Db2 . . . 581
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per IBM Db2 . . . 584
Strategia di backup per IBM Db2 . . . 584
Strategia di ripristino e recupero per IBM Db2 . . . 587
Prepararsi all'installazione del plug-in SnapCenter per IBM Db2 . . . 588
Flusso di lavoro di installazione del plug-in SnapCenter per IBM Db2 . . . 588
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Windows, Linux o AIX . . . 588
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 593
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux . . . 594
Imposta le credenziali per il plug-in SnapCenter per IBM Db2 . . . 595
Configurare gMSA su Windows Server 2016 o versioni successive . . . 597
Installa il plug-in SnapCenter per IBM Db2 . . . 598
Configurare il certificato CA . . . 604
Prepararsi alla protezione dei dati . . . 612

Prerequisiti per l'utilizzo del plug-in SnapCenter per IBM Db2 . . . 612
Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere IBM Db2 . . . 612
Eseguire il backup delle risorse IBM Db2 . . . 613
Eseguire il backup delle risorse IBM Db2 . . . 613
Scopri automaticamente i database . . . 615
Aggiungere manualmente le risorse all'host del plug-in . . . 615
Creare policy di backup per IBM Db2 . . . 617
Crea gruppi di risorse e allega criteri . . . 619
Crea gruppi di risorse e abilita la protezione secondaria per le risorse IBM Db2 sui sistemi ASA r2 . . . 623
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per IBM Db2 . . . 625
Eseguire il backup dei database Db2 . . . 627
Eseguire il backup dei gruppi di risorse . . . 634
Monitorare le operazioni di backup di IBM Db2 . . . 635
Annulla le operazioni di backup per IBM Db2 . . . 636
Visualizza i backup e i cloni di IBM Db2 nella pagina Topologia . . . 637
Ripristina IBM Db2 . . . 639
Ripristina flusso di lavoro . . . 639
Ripristina un backup di risorse aggiunto manualmente . . . 639
Ripristina e recupera un backup del database rilevato automaticamente . . . 644
Monitorare le operazioni di ripristino di IBM Db2 . . . 645
Clona i backup delle risorse IBM Db2 . . . 646
Flusso di lavoro di clonazione . . . 646
Clonare un backup IBM Db2 . . . 647
Monitorare le operazioni di clonazione IBM Db2 . . . 654
Dividi un clone . . . 655
Eliminare o dividere i cloni del database IBM Db2 dopo l'aggiornamento SnapCenter . . . 656
Proteggere PostgreSQL . . . 658
Plug-in SnapCenter per PostgreSQL . . . 658
Panoramica del plug-in SnapCenter per PostgreSQL . . . 658
Cosa puoi fare utilizzando il plug-in SnapCenter per PostgreSQL . . . 658
Funzionalità del plug-in SnapCenter per PostgreSQL . . . 658
Tipi di archiviazione supportati dal plug-in SnapCenter per PostgreSQL . . . 659
Privilegi ONTAP minimi richiesti per il plug-in PostgreSQL . . . 660
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per PostgreSQL . . . 663
Strategia di backup per PostgreSQL . . . 663
Strategia di ripristino e recupero per PostgreSQL . . . 666
Prepararsi all'installazione del plug-in SnapCenter per PostgreSQL . . . 667
Flusso di lavoro di installazione del plug-in SnapCenter per PostgreSQL . . . 667
Prerequisiti per aggiungere host e installare il plug-in SnapCenter per PostgreSQL . . . 667
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 671
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux . . . 672
Imposta le credenziali per il plug-in SnapCenter per PostgreSQL . . . 673
Configurare gMSA su Windows Server 2016 o versioni successive . . . 675
Installa il plug-in SnapCenter per PostgreSQL . . . 676

Configurare il certificato CA . . . 682
Prepararsi alla protezione dei dati . . . 689
Prerequisiti per l'utilizzo del plug-in SnapCenter per PostgreSQL . . . 690
Come vengono utilizzate le risorse, i gruppi di risorse e le policy per proteggere PostgreSQL . . . 690
Eseguire il backup delle risorse PostgreSQL . . . 690
Eseguire il backup delle risorse PostgreSQL . . . 690
Scopri automaticamente i cluster . . . 692
Aggiungere manualmente le risorse all'host del plug-in . . . 692
Creare policy di backup per PostgreSQL . . . 694
Crea gruppi di risorse e allega criteri . . . 697
Crea gruppi di risorse e abilita la protezione secondaria per le risorse PostgreSQL sui sistemi ASA r2 . . . 701
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per PostgreSQL . . . 703
Eseguire il backup di PostgreSQL . . . 705
Eseguire il backup dei gruppi di risorse . . . 710
Monitorare le operazioni di backup di PostgreSQL . . . 711
Annulla le operazioni di backup per PostgreSQL . . . 712
Visualizza i backup e i cloni di PostgreSQL nella pagina Topologia . . . 713
Ripristina PostgreSQL . . . 714
Ripristina flusso di lavoro . . . 714
Ripristina e recupera un backup di risorse aggiunto manualmente . . . 715
Ripristina e recupera un backup del cluster rilevato automaticamente . . . 719
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 721
Monitorare le operazioni di ripristino di PostgreSQL . . . 724
Clona i backup delle risorse PostgreSQL . . . 725
Flusso di lavoro di clonazione . . . 725
Clonare un backup PostgreSQL . . . 726
Monitorare le operazioni di clonazione di PostgreSQL . . . 729
Dividi un clone . . . 730
Elimina o dividi i cloni del cluster PostgreSQL dopo l'aggiornamento SnapCenter . . . 731
Proteggi MySQL . . . 733
Plug-in SnapCenter per MySQL . . . 733
Panoramica del plug-in SnapCenter per MySQL . . . 733
Cosa puoi fare utilizzando il plug-in SnapCenter per MySQL . . . 733
Funzionalità del plug-in SnapCenter per MySQL . . . 733
Tipi di archiviazione supportati dal plug-in SnapCenter per MySQL . . . 734
Privilegi ONTAP minimi richiesti per il plug-in MySQL . . . 735
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per MySQL . . . 738
Strategia di backup per MySQL . . . 738
Strategia di ripristino e recupero per MySQL . . . 740
Preparati a installare il plug-in SnapCenter per MySQL . . . 742
Flusso di lavoro di installazione del plug-in SnapCenter per MySQL . . . 742
Prerequisiti per aggiungere host e installare il plug-in SnapCenter per MySQL . . . 742
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 745
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux . . . 746

Imposta le credenziali per il plug-in SnapCenter per MySQL . . . 747
Installa il plug-in SnapCenter per MySQL . . . 750
Configurare il certificato CA . . . 755
Prepararsi alla protezione dei dati . . . 762
Prerequisiti per l'utilizzo del plug-in SnapCenter per MySQL . . . 762
Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere MySQL . . . 763
Eseguire il backup delle risorse MySQL . . . 763
Eseguire il backup delle risorse MySQL . . . 763
Scopri automaticamente i database . . . 765
Aggiungere manualmente le risorse all'host del plug-in . . . 765
Creare policy di backup per MySQL . . . 766
Crea gruppi di risorse e allega criteri . . . 770
Crea gruppi di risorse e abilita la protezione secondaria per le risorse MySQL sui sistemi ASA r2 . . . 774
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per MySQL . . . 776
Eseguire il backup di MySQL . . . 778
Eseguire il backup dei gruppi di risorse . . . 783
Monitorare le operazioni di backup di MySQL . . . 784
Annulla le operazioni di backup per MySQL . . . 785
Visualizza i backup e i cloni di MySQL nella pagina Topologia . . . 786
Ripristina MySQL . . . 787
Ripristina flusso di lavoro . . . 787
Ripristina e recupera un backup di risorse aggiunto manualmente . . . 788
Ripristina e recupera un backup del database rilevato automaticamente . . . 792
Ripristinare le risorse utilizzando i cmdlet di PowerShell . . . 794
Monitorare le operazioni di ripristino di MySQL . . . 796
Clona i backup delle risorse MySQL . . . 797
Flusso di lavoro di clonazione . . . 797
Clonare un backup MySQL . . . 798
Monitorare le operazioni di clonazione di MySQL . . . 801
Dividi un clone . . . 802
Elimina o dividi i cloni del database MySQL dopo l'aggiornamento SnapCenter . . . 803
Proteggi le applicazioni utilizzando i plug-in supportati NetApp . . . 804
Plug-in supportati da NetApp . . . 804
Panoramica dei plug-in supportati da NetApp . . . 804
Cosa puoi fare con i plug-in supportati da NetApp . . . 804
Funzionalità dei plug-in supportati da NetApp . . . 805
Tipi di storage supportati dai plug-in supportati da NetApp . . . 806
Privilegi ONTAP minimi richiesti per il plug-in supportato NetApp . . . 806
Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per i plug-in supportati da NetApp . . . 809
Definire una strategia di backup . . . 809
Strategia di backup per i plug-in supportati da NetApp . . . 810
Tipi di strategie di ripristino supportate per le risorse plug-in supportate NetApp aggiunte manualmente . . . 811

Preparati a installare i plug-in supportati da NetApp . . . 811
Flusso di lavoro di installazione dei plug-in supportati da SnapCenter NetApp . . . 811
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Windows, Linux o AIX . . . 812
Requisiti host per installare il pacchetto plug-in SnapCenter per Windows . . . 816
Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux e AIX . . . 817
Imposta le credenziali per i plug-in supportati da NetApp . . . 818
Configurare gMSA su Windows Server 2016 o versioni successive . . . 820
Installa i plug-in supportati da NetApp . . . 821
Configurare il certificato CA . . . 828
Prepararsi alla protezione dei dati . . . 835
Prerequisiti per l'utilizzo dei plug-in supportati NetApp . . . 835
Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere le risorse dei plug-in supportati da NetApp . . . 836
Eseguire il backup delle risorse dei plug-in supportati NetApp . . . 837
Eseguire il backup delle risorse dei plug-in supportati NetApp . . . 837
Aggiungi risorse ai plug-in supportati da NetApp . . . 837
Creare policy per le risorse plug-in supportate NetApp . . . 842
Crea gruppi di risorse e allega criteri . . . 846
Crea gruppi di risorse e abilita la protezione secondaria per le risorse sui sistemi ASA r2 . . . 849
Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell . . . 852
Eseguire il backup delle singole risorse dei plug-in supportati NetApp . . . 853
Eseguire il backup dei gruppi di risorse delle risorse plug-in supportate NetApp . . . 858
Monitora le operazioni di backup delle risorse plug-in supportate NetApp . . . 859
Annulla le operazioni di backup per i plug-in supportati da NetApp . . . 860
Visualizza i backup e i cloni correlati alle risorse dei plug-in supportati da NetApp nella pagina Topologia . . . 861
Ripristina le risorse dei plug-in supportati da NetApp . . . 862
Ripristina le risorse dei plug-in supportati da NetApp . . . 863
Ripristinare un backup delle risorse . . . 863
Monitora le operazioni di ripristino delle risorse dei plug-in supportati NetApp . . . 867
Clona i backup delle risorse dei plug-in supportati NetApp . . . 868
Clona i backup delle risorse dei plug-in supportati NetApp . . . 868
Clona da un backup . . . 869
Monitora le operazioni di clonazione delle risorse plug-in supportate NetApp . . . 875
Proteggere i file system Unix . . . 877
Cosa puoi fare con il plug-in SnapCenter per i file system Unix . . . 877
Configurazioni supportate . . . 877
Limitazioni . . . 878
Caratteristiche . . . 878
Installa il plug-in SnapCenter per i file system Unix . . . 878
Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Linux . . . 878
Aggiungi host e installa il pacchetto Plug-in per Linux utilizzando l'interfaccia grafica . . . 880
Configurare il servizio SnapCenter Plug-in Loader . . . 882
Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux . . . 885

Abilita i certificati CA per i plug-in . . . 888
Installa il SnapCenter Plug-in for VMware vSphere . . . 889
Distribuisci il certificato CA . . . 889
Configurare il file CRL . . . 889
Prepararsi alla protezione dei file system Unix . . . 889
Eseguire il backup dei file system Unix . . . 890
Scopri i file system UNIX disponibili per il backup . . . 890
Creare policy di backup per i file system Unix . . . 890
Crea gruppi di risorse e allega policy per i file system Unix . . . 893
Crea gruppi di risorse e abilita la protezione secondaria per i file system Unix sui sistemi ASA r2 . . . 895
Eseguire il backup dei file system Unix . . . 897
Eseguire il backup dei gruppi di risorse dei file system Unix . . . 899
Monitorare il backup dei file system Unix . . . 899
Visualizza i file system Unix protetti nella pagina Topologia . . . 901
Ripristinare e recuperare i file system Unix . . . 903
Ripristinare i file system Unix . . . 903
Monitorare le operazioni di ripristino dei file system Unix . . . 904
Clonare i file system Unix . . . 905
Clona il backup del file system Unix . . . 905
Dividi un clone . . . 907
Monitorare le operazioni di clonazione dei file system Unix . . . 908
Proteggere le applicazioni in esecuzione su Azure NetApp Files . . . 909
Proteggere le applicazioni in esecuzione su Azure NetApp Files . . . 909
Limitazioni . . . 909
Installa SnapCenter e crea le credenziali . . . 909
Installa SnapCenter sulla macchina virtuale di Azure . . . 909
Creare le credenziali di Azure in SnapCenter . . . 911
Configurare l’account di archiviazione di Azure . . . 912
Crea le credenziali per aggiungere l’host del plug-in . . . 912
Proteggere i database SAP HANA . . . 913
Aggiungi host e installa il plug-in SnapCenter per il database SAP HANA . . . 913
Aggiungi il database SAP HANA . . . 914
Creare policy di backup per i database SAP HANA . . . 914
Crea gruppi di risorse e collega policy di backup SAP HANA . . . 915
Eseguire il backup dei database SAP HANA in esecuzione su Azure NetApp Files . . . 916
Eseguire il backup dei gruppi di risorse SAP HANA . . . 917
Ripristinare e recuperare i database SAP HANA . . . 917
Clona il backup del database SAP HANA . . . 918
Proteggere i database di Microsoft SQL Server . . . 919
Aggiungi host e installa il plug-in SnapCenter per il database SQL Server . . . 919
Creare criteri di backup per i database di SQL Server . . . 920
Crea gruppi di risorse e collega criteri di backup SQL . . . 921
Eseguire il backup dei database di SQL Server in esecuzione su Azure NetApp Files . . . 923
Eseguire il backup dei gruppi di risorse di SQL Server . . . 924
Ripristinare e recuperare i database di SQL Server . . . 924

Clona il backup del database SQL Server . . . 925
Proteggere i database Oracle . . . 927
Aggiungi host e installa il plug-in SnapCenter per il database Oracle . . . 927
Creare policy di backup per i database Oracle . . . 928
Crea gruppi di risorse e collega policy di backup Oracle . . . 928
Eseguire il backup dei database Oracle in esecuzione su Azure NetApp Files . . . 930
Eseguire il backup dei gruppi di risorse Oracle . . . 930
Ripristinare e recuperare i database Oracle . . . 931
Clona il backup del database Oracle . . . 933
Gestisci SnapCenter Server e i plug-in . . . 936
Visualizza dashboard . . . 936
Panoramica della dashboard . . . 936
Come visualizzare le informazioni sulla dashboard . . . 940
Richiedi report sullo stato dei lavori dalla dashboard . . . 940
Richiedi report sullo stato della protezione dalla dashboard . . . 940
Gestisci RBAC . . . 941
Modificare un ruolo . . . 941
Modifica utenti e gruppi . . . 942
Gestisci gli host . . . 942
Aggiorna le informazioni della macchina virtuale . . . 944
Modifica gli host dei plug-in . . . 944
Avvia o riavvia i servizi plug-in . . . 945
Sospendere le pianificazioni per la manutenzione dell'host . . . 946
Operazioni supportate dalla pagina Risorse . . . 946
Gestire le politiche . . . 947
Modificare le politiche . . . 947
Distacca le politiche . . . 948
Elimina le policy . . . 949
Gestire gruppi di risorse . . . 949
Interrompere e riprendere le operazioni sui gruppi di risorse . . . 949
Elimina gruppi di risorse . . . 950
Gestire i backup . . . 950
Rinomina i backup . . . 950
Elimina i backup . . . 951
Rimuovi protezione . . . 952
Elimina i cloni . . . 952
Monitora lavori, pianificazioni, eventi e registri . . . 953
Monitorare i lavori . . . 953
Monitorare gli orari . . . 954
Monitorare gli eventi . . . 954
Monitorare i registri . . . 955
Rimuovere lavori e registri da SnapCenter . . . 956
Panoramica delle funzionalità di reporting SnapCenter . . . 956
Rapporti di accesso . . . 958
Filtra il tuo report . . . 958

Esportare o stampare report . . . 959
Imposta il server SMTP per le notifiche e-mail . . . 959
Configurare l'opzione per inviare i report via e-mail . . . 959
Gestire il repository di SnapCenter Server . . . 960
Prerequisiti per la protezione del repository SnapCenter . . . 960
Eseguire il backup del repository SnapCenter . . . 960
Visualizza i backup del repository SnapCenter . . . 961
Ripristinare il repository del database SnapCenter . . . 961
Migrare il repository SnapCenter . . . 962
Reimposta la password del repository SnapCenter . . . 962
Gestire le risorse dei domini non attendibili . . . 963
Modificare i domini non attendibili . . . 963
Annullare la registrazione dei domini Active Directory non attendibili . . . 964
Gestire il sistema di archiviazione . . . 964
Modificare la configurazione del sistema di archiviazione . . . 964
Elimina il sistema di archiviazione . . . 967
Supporto API REST . . . 968
Gestire la raccolta dati EMS . . . 968
Interrompere la raccolta dati EMS . . . 968
Avvia la raccolta dati EMS . . . 969
Modificare il programma di raccolta dati EMS e l'SVM di destinazione . . . 969
Monitorare lo stato della raccolta dati EMS . . . 969
Aggiorna SnapCenter Server e i plug-in . . . 971
Configura SnapCenter per verificare la disponibilità di aggiornamenti . . . 971
Flusso di lavoro di aggiornamento . . . 971
Percorsi di aggiornamento supportati . . . 971
Aggiornare il server SnapCenter sull'host Windows . . . 972
Aggiornare il server SnapCenter sull'host Linux . . . 974
Aggiorna i tuoi pacchetti plug-in . . . 975
Aggiornamento tecnologico . . . 978
Aggiornamento tecnologico dell'host del server SnapCenter . . . 978
Aggiornamento tecnico di un nodo nel cluster F5 . . . 979
Dismissione del vecchio host del server SnapCenter . . . 979
Ripristina il vecchio host del server SnapCenter . . . 979
Ripristino dopo un disastro . . . 979
Aggiornamento tecnologico degli host dei plug-in SnapCenter . . . 981
Aggiornamento tecnologico del sistema di archiviazione . . . 983
Aggiorna i backup dello storage primario . . . 984
Aggiorna i backup dello storage secondario . . . 986
Disinstallare SnapCenter Server e i plug-in . . . 988
Disinstallare i pacchetti plug-in SnapCenter . . . 988
Prerequisiti per la rimozione di un host . . . 988
Rimuovere un host . . . 989
Disinstallare i plug-in utilizzando l'interfaccia grafica utente SnapCenter . . . 989
Disinstallare i plug-in di Windows utilizzando il cmdlet PowerShell . . . 990

Disinstallare i plug-in localmente su un host . . . 991
Disinstallare il pacchetto plug-in per Linux o AIX tramite CLI . . . 991
Disinstallare SnapCenter Server sull'host Windows . . . 992
Disinstallare SnapCenter Server sull'host Linux . . . 992
Automatizzare utilizzando le API REST . . . 994
Automazione SnapCenter tramite API REST . . . 994
Come accedere in modo nativo all'API REST di SnapCenter . . . 994
Fondazione dei servizi web REST . . . 994
Risorse e rappresentanza statale . . . 994
Endpoint URI . . . 995
Messaggi HTTP . . . 995
Formattazione JSON . . . 995
Caratteristiche operative di base . . . 995
Transazione API di richiesta e risposta . . . 995
Supporto per le operazioni CRUD . . . 995
Identificatori di oggetti . . . 996
Istanze e raccolte di oggetti . . . 996
Operazioni sincrone e asincrone . . . 996
Sicurezza . . . 996
Variabili di input che controllano una richiesta API . . . 997
Metodi HTTP . . . 997
Intestazioni di richiesta . . . 997
Corpo della richiesta . . . 997
Filtraggio degli oggetti . . . 998
Richiesta di campi di oggetti specifici . . . 998
Ordinamento degli oggetti nel set di output . . . 999
Paginazione durante il recupero di oggetti in una raccolta . . . 999
Proprietà dimensionali . . . 1000
Interpretazione di una risposta API . . . 1000
Codice di stato HTTP . . . 1000
Intestazioni di risposta . . . 1001
Corpo della risposta . . . 1001
Errori . . . 1002
API REST supportate per SnapCenter Server e plug-in . . . 1003
Autenticazione . . . 1003
Domini . . . 1003
Lavori . . . 1003
Impostazioni . . . 1003
Ospiti . . . 1003
Risorse . . . 1004
Backup . . . 1005
Cloni . . . 1006
Clone diviso . . . 1006
Gruppi di risorse . . . 1006
Politiche . . . 1007

Magazzinaggio . . . 1007
Condividere . . . 1007
Plugin . . . 1007
Rapporti . . . 1009
Avvisi . . . 1009
Rbac . . . 1009
Configurazione . . . 1009
Impostazioni del certificato . . . 1009
Deposito . . . 1010
Versione . . . 1010
Come accedere alle API REST utilizzando la pagina web dell'API Swagger . . . 1010
Inizia con l'API REST . . . 1011
Ciao mondo . . . 1011
Note legali . . . 1012
Copyright . . . 1012
Marchi . . . 1012
Brevetti . . . 1012
Politica sulla riservatezza . . . 1012
Open source . . . 1012

# Documentazione SnapCenter software

# Note di rilascio

## Note di rilascio

Scopri le nuove e migliorate funzionalità disponibili in SnapCenter 6.1.

Per un elenco completo delle nuove funzionalità e dei miglioramenti, consultare "Novità di SnapCenter 6.1" .

Per i dettagli sui problemi noti, le limitazioni, i problemi risolti e i comandi nuovi e modificati, vedere "Note sulla versione 6.1 del software SnapCenter" . Per accedere alle Note sulla versione è necessario effettuare l'accesso con il proprio account NetApp o creare un account.

## Percorsi di aggiornamento supportati per SnapCenter

Il percorso di aggiornamento ti aiuta a capire da quali versioni precedenti di SnapCenter puoi effettuare l'aggiornamento alle versioni più recenti di SnapCenter e quali versioni dei plug-in sono supportate.

| Se utilizzi la versione SnapCenter Server… | È possibile aggiornare direttamente SnapCenter Server a… | Versioni di plug-in supportate |
|---|---|---|
| 5,0 | 6,0 | • 5,0<br>• 6,0 |
| | 6.0.1 | • 6.0.1 |
| | 6,1 | • 6,1 |
| 6,0 | 6.0.1 | • 6,0<br>• 6.0.1 |
| | 6,1 | • 6,1 |
| 6.0.1 | 6,1 | • 6.0.1<br>• 6,1 |

Per informazioni sull'aggiornamento del SnapCenter Plug-in for VMware vSphere, vedere "Aggiorna il SnapCenter Plug-in for VMware vSphere" .

# Iniziare

## Scopri di più sul SnapCenter software

### Panoramica SnapCenter

Il SnapCenter software è una piattaforma semplice, centralizzata e scalabile per la protezione dei dati coerente con le applicazioni. Protegge applicazioni, database, file system host e VM sui sistemi ONTAP nel cloud ibrido.

SnapCenter utilizza le tecnologie NetApp Snapshot, SnapRestore, FlexClone, SnapMirror e SnapVault per fornire:

- Backup basati su disco rapidi, efficienti in termini di spazio e coerenti con le applicazioni
- Ripristino rapido e dettagliato e recupero coerente con l'applicazione
- Clonazione rapida e salvaspazio

SnapCenter include SnapCenter Server e plug-in leggeri. È possibile automatizzare la distribuzione dei plug-in su host di applicazioni remote, pianificare operazioni di backup, verifica e clonazione e monitorare le operazioni di protezione dei dati.

Per proteggere i dati, puoi installare SnapCenter in locale o su un cloud pubblico.

- In sede per proteggere quanto segue:
  - Dati presenti sui sistemi primari ONTAP FAS, AFF o ASA e replicati sui sistemi secondari ONTAP FAS, AFF o ASA
  - Dati presenti sui sistemi primari ONTAP Select
  - Dati presenti sui sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti nell'archiviazione di oggetti StorageGRID locale
  - Dati presenti sui sistemi primari e secondari ONTAP ASA r2
- In locale in un cloud ibrido per proteggere quanto segue:
  - Dati presenti sui sistemi primari ONTAP FAS, AFF o ASA e replicati su Cloud Volumes ONTAP
  - Dati presenti sui sistemi primari e secondari ONTAP FAS, AFF o ASA e protetti su storage di oggetti e archivi nel cloud tramite l'integrazione di backup e ripristino NetApp
- In un cloud pubblico per proteggere quanto segue:
  - Dati presenti sui sistemi primari Cloud Volumes ONTAP (in precedenza ONTAP Cloud)
  - Dati presenti su Amazon FSX per ONTAP
  - Dati presenti nei Azure NetApp Files primari (Oracle, Microsoft SQL e SAP HANA)

#### Caratteristiche principali

SnapCenter offre le seguenti funzionalità principali:

- Protezione dei dati centralizzata e coerente con le applicazioni di diverse applicazioni

  La protezione dei dati è supportata per Microsoft Exchange Server, Microsoft SQL Server, Oracle

Database su Linux o AIX, database SAP HANA, IBM Db2, PostgreSQL, MySQL e file system host Windows in esecuzione su sistemi ONTAP . SnapCenter supporta anche la protezione di applicazioni quali MongoDB, Storage, MaxDB, Sybase ASE, ORASCPM.

- Backup basati su policy

  I backup basati su policy sfruttano la tecnologia NetApp Snapshot per creare backup basati su disco rapidi, efficienti in termini di spazio e coerenti con le applicazioni. È anche possibile impostare la protezione automatica di questi backup su un archivio secondario aggiornando le relazioni di protezione esistenti.

- Backup per più risorse

  È possibile eseguire il backup di più risorse (applicazioni, database o file system host) dello stesso tipo contemporaneamente utilizzando i gruppi di risorse SnapCenter .

- Ripristino e recupero

  SnapCenter fornisce ripristini rapidi e granulari dei backup e ripristini basati sul tempo e coerenti con l'applicazione. È possibile effettuare il ripristino da qualsiasi destinazione nel cloud ibrido.

- Clonazione

  SnapCenter consente una clonazione rapida, efficiente in termini di spazio e coerente con l'applicazione. È possibile clonare su qualsiasi destinazione nel cloud ibrido.

- Interfaccia utente grafica per la gestione di un singolo utente

  SnapCenter fornisce un'unica interfaccia per gestire backup e cloni in qualsiasi destinazione Hybrid Cloud.

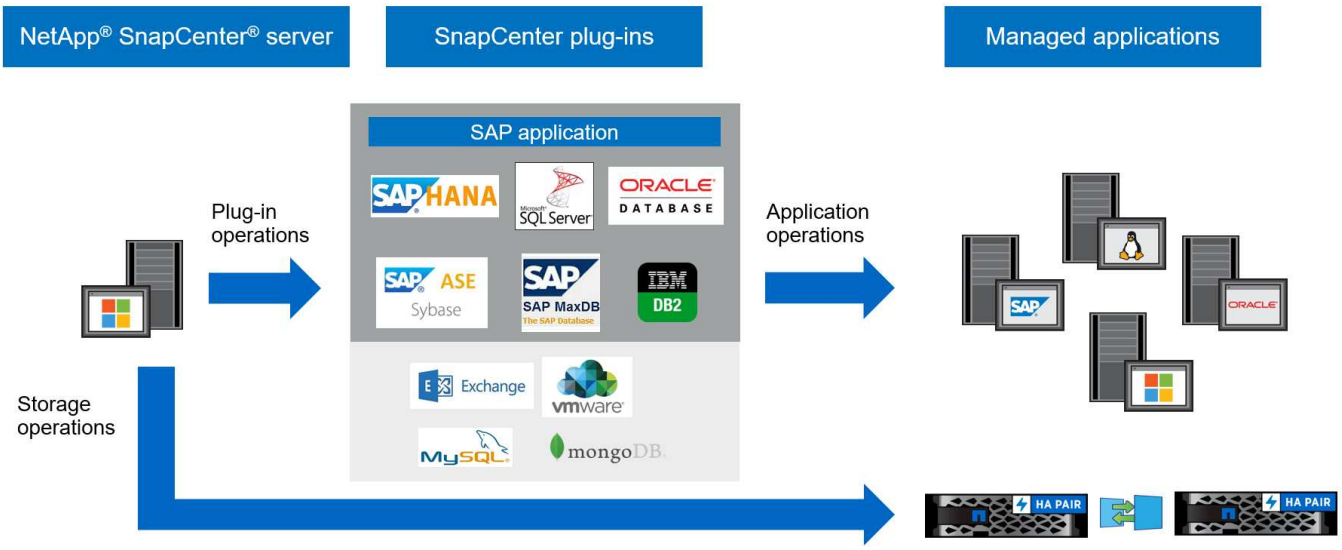
- API REST, cmdlet di Windows, comandi UNIX

  SnapCenter fornisce API REST per la maggior parte delle funzionalità per l'integrazione con qualsiasi software di orchestrazione e l'uso di cmdlet di Windows PowerShell e interfaccia della riga di comando.

- Dashboard e reporting centralizzati sulla protezione dei dati
- Controllo degli accessi basato sui ruoli (RBAC) per la sicurezza e la delega
- Un database di repository integrato con elevata disponibilità per archiviare tutti i metadati di backup
- Installazione push automatizzata dei plug-in
- Alta disponibilità
- Ripristino di emergenza (DR)
- SnapLock "Saperne di più"
- Sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC])
- Mirroring sincrono "Saperne di più"

### Architettura e componenti SnapCenter

SnapCenter utilizza un design a strati con un server di gestione centrale e host plug-in. Il server e gli host dei plug-in possono trovarsi in posizioni diverse.




SnapCenter include SnapCenter Server, il pacchetto SnapCenter Plug-in per Windows e il pacchetto SnapCenter Plug-in per Linux. Ogni pacchetto contiene plug-in per varie applicazioni e componenti infrastrutturali.

#### Server SnapCenter

SnapCenter Server supporta i sistemi operativi Microsoft Windows e Linux (RHEL 8.x, RHEL 9.x, SLES 15 SP5). Il server SnapCenter include un server Web, un'interfaccia utente centralizzata basata su HTML5, cmdlet PowerShell, API REST e il repository SnapCenter .

SnapCenter memorizza le informazioni sulle sue operazioni nel repository SnapCenter .

#### Plug-in SnapCenter

Ogni plug-in SnapCenter supporta ambienti, database e applicazioni specifici.

| Nome del plug-in | Incluso nel pacchetto di installazione | Richiede altri plug-in | Installato sull'host | Piattaforma supportata |
|---|---|---|---|---|
| Plug-in SnapCenter per Microsoft SQL Server | Pacchetto di plug-in per Windows | Plug-in per Windows | Host di SQL Server | Finestre |
| Plug-in SnapCenter per Windows | Pacchetto di plug-in per Windows | | Host Windows | Finestre |
| Plug-in SnapCenter per Microsoft Exchange Server | Pacchetto di plug-in per Windows | Plug-in per Windows | Host del server Exchange | Finestre |
| Plug-in SnapCentre per Oracle Database | Pacchetto di plug-in per Linux e pacchetto di plug-in per AIX | Plug-in per UNIX | Host Oracle | Linux o AIX |

| Nome del plug-in | Incluso nel pacchetto di installazione | Richiede altri plug-in | Installato sull'host | Piattaforma supportata |
|---|---|---|---|---|
| Plug-in SnapCenter per il database SAP HANA | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host client HDBSQL | Linux o Windows |
| Plug-in SnapCenter per IBM Db2 | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host DB2 | Linux, AIX o Windows |
| Plug-in SnapCenter per PostgreSQL | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host PostgreSQL | Linux o Windows |
| Plug-in SnaoCenter per MySQL | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o Plug-in per Windows | Host MySQL | Linux o Windows |
| Plug-in SnapCenter per MongoDB | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host MongoDB | Linux o Windows |
| Plug-in SnapCenter per ORASCPM (Oracle Applications) | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host Oracle | Linux o Windows |
| Plug-in SnapCenter per SAP ASE | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host SAP | Linux o Windows |
| Plug-in SnapCenter per SAP MaxDB | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host SAP MaxDB | Linux o Windows |
| Plug-in SnapCenter per il plug-in di archiviazione | Pacchetto di plug-in per Linux e pacchetto di plug-in per Windows | Plug-in per UNIX o plug-in per Windows | Host di archiviazione | Linux o Windows |

Il SnapCenter Plug-in for VMware vSphere supporta operazioni di backup e ripristino coerenti con gli arresti

anomali e con le VM per macchine virtuali (VM), datastore e dischi di macchine virtuali (VMDK). Supporta inoltre operazioni di backup e ripristino coerenti con l'applicazione per database e file system virtualizzati.

Per proteggere database, file system, VM o datastore su VM, distribuire il SnapCenter Plug-in for VMware vSphere . Per informazioni, fare riferimento "Documentazione SnapCenter Plug-in for VMware vSphere" .

#### Repository SnapCenter

Il repository SnapCenter , a volte denominato database NSM, memorizza informazioni e metadati per ogni operazione SnapCenter .

L'installazione SnapCenter Server installa per impostazione predefinita il database del repository MySQL Server. Se hai già installato MySQL Server e vuoi eseguire una nuova installazione di SnapCenter Server, devi disinstallare MySQL Server.

SnapCenter supporta MySQL Server 8.0.37 o versioni successive come database del repository SnapCenter . Se si utilizza una versione precedente di MySQL Server con una release precedente di SnapCenter, il processo di aggiornamento di SnapCenter aggiorna MySQL Server alla versione 8.0.37 o successiva.

Il repository SnapCenter memorizza le seguenti informazioni e metadati:

- Metadati di backup, clonazione, ripristino e verifica
- Informazioni su report, lavori ed eventi
- Informazioni sull'host e sul plug-in
- Dettagli su ruolo, utente e autorizzazione
- Informazioni sulla connessione del sistema di archiviazione

## Funzionalità di sicurezza in SnapCenter

### SnapCenter utilizza rigorose funzionalità di sicurezza e autenticazione per consentirti di proteggere i tuoi dati.

SnapCenter include le seguenti funzionalità di sicurezza:

- Tutte le comunicazioni con SnapCenter utilizzano HTTP su SSL (HTTPS).
- Tutte le credenziali in SnapCenter sono protette tramite crittografia Advanced Encryption Standard (AES).
- Supporta algoritmi di sicurezza conformi allo standard Federal Information Processing Standard (FIPS).
- Supporta l'utilizzo dei certificati CA autorizzati forniti dal cliente.
- Supporta Transport Layer Security (TLS) 1.3 per la comunicazione con ONTAP. È possibile utilizzare anche TLS 1.2 per la comunicazione tra client e server.
- Supporta un determinato set di suite di crittografia SSL per garantire la sicurezza nelle comunicazioni di rete. "Saperne di più" .
- SnapCenter viene installato all'interno del firewall aziendale per consentire l'accesso a SnapCenter Server e la comunicazione tra SnapCenter Server e i plug-in.
- L'accesso alle API e alle operazioni SnapCenter utilizza token crittografati con crittografia AES, che scadono dopo 24 ore.
- SnapCenter si integra con Windows Active Directory per l'accesso e il controllo degli accessi basato sui ruoli (RBAC) che regolano le autorizzazioni di accesso.

- IPsec è supportato con SnapCenter su ONTAP per macchine host Windows e Linux. "Saperne di più" .
- I cmdlet SnapCenter PowerShell sono protetti dalla sessione.
- Dopo un periodo predefinito di 15 minuti di inattività, SnapCenter ti avvisa che verrai disconnesso entro 5 minuti.

  Dopo 20 minuti di inattività, SnapCenter effettua la disconnessione e sarà necessario effettuare nuovamente l'accesso. È possibile modificare il periodo di disconnessione.

- L'accesso viene temporaneamente disabilitato dopo 5 tentativi di accesso errati.
- Supporta l'autenticazione del certificato CA tra SnapCenter Server e ONTAP. "Saperne di più" .
- Integrity Verifier viene aggiunto a SnapCenter Server e ai plug-in e convalida tutti i file binari forniti durante le operazioni di nuova installazione e aggiornamento.

### Panoramica del certificato CA

Il programma di installazione di SnapCenter Server abilita il supporto centralizzato dei certificati SSL durante l'installazione. Per migliorare la comunicazione protetta tra il server e il plug-in, SnapCenter supporta l'utilizzo dei certificati CA autorizzati forniti dal cliente.

È necessario distribuire i certificati CA dopo aver installato SnapCenter Server e i rispettivi plug-in. Per ulteriori informazioni, consultare "Genera file CSR del certificato CA" .

È anche possibile distribuire il certificato CA per il plug-in SnapCenter per VMware vSphere. Per ulteriori informazioni, vedere "Creare e importare certificati" .

### Comunicazione SSL bidirezionale

La comunicazione SSL bidirezionale protegge la comunicazione reciproca tra SnapCenter Server e i plug-in.

### Panoramica sull'autenticazione basata su certificato

L'autenticazione basata su certificato verifica l'autenticità dei rispettivi utenti che tentano di accedere all'host del plug-in SnapCenter . L'utente deve esportare il certificato del server SnapCenter senza chiave privata e importarlo nell'archivio attendibile dell'host del plug-in. L'autenticazione basata su certificato funziona solo se è abilitata la funzionalità SSL bidirezionale.

### Autenticazione a più fattori (MFA)

MFA utilizza un Identity Provider (IdP) di terze parti tramite Security Assertion Markup Language (SAML) per gestire le sessioni utente. Questa funzionalità migliora la sicurezza dell'autenticazione offrendo la possibilità di utilizzare più fattori, come TOTP, dati biometrici, notifiche push ecc., insieme al nome utente e alla password esistenti. Inoltre, consente al cliente di utilizzare i propri provider di identità utente per ottenere un accesso utente unificato (SSO) per tutto il proprio portafoglio.

L'MFA è applicabile solo per l'accesso all'interfaccia utente di SnapCenter Server. Gli accessi vengono autenticati tramite l'IdP Active Directory Federation Services (AD FS). È possibile configurare vari fattori di autenticazione in AD FS. SnapCenter è il fornitore del servizio e dovresti SnapCenter come relying party in AD FS. Per abilitare MFA in SnapCenter, saranno necessari i metadati AD FS.

Per informazioni su come abilitare MFA, vedere"Abilita l'autenticazione a più fattori" .

## Controllo degli accessi basato sui ruoli in SnapCenter

Il controllo degli accessi basato sui ruoli (RBAC) SnapCenter e le autorizzazioni ONTAP consentono agli amministratori SnapCenter di delegare il controllo delle risorse SnapCenter a diversi utenti o gruppi di utenti. Questo accesso gestito centralmente consente agli amministratori delle applicazioni di lavorare in modo sicuro all'interno di ambienti delegati.

È possibile creare e modificare i ruoli e aggiungere l'accesso alle risorse agli utenti in qualsiasi momento. Tuttavia, quando si configura SnapCenter per la prima volta, è necessario almeno aggiungere utenti o gruppi di Active Directory ai ruoli e quindi aggiungere l'accesso alle risorse a tali utenti o gruppi.

Non è possibile utilizzare SnapCenter per creare account utente o di gruppo. Dovresti creare account utente o di gruppo in Active Directory del sistema operativo o del database.

### Tipi di RBAC in SnapCenter

SnapCenter utilizza i seguenti tipi di controllo degli accessi basato sui ruoli:

- SnapCenter RBAC
- RBAC a livello di applicazione
- Plug-in SnapCenter per VMware vSphere RBAC
- Autorizzazioni ONTAP

#### SnapCenter RBAC

SnapCenter ha ruoli predefiniti ed è possibile assegnare utenti o gruppi di utenti a tali ruoli. I ruoli predefiniti sono:

- Ruolo di amministratore SnapCenter
- Ruolo di amministratore di backup e clonazione delle app
- Ruolo di visualizzatore di backup e clonazione
- Ruolo di amministratore dell'infrastruttura

Quando assegni un ruolo a un utente, nella pagina Lavori saranno visibili solo i lavori pertinenti a quell'utente, a meno che non gli sia stato assegnato il ruolo SnapCenterAdmin.

Puoi anche creare nuovi ruoli e gestire autorizzazioni e utenti. È possibile assegnare autorizzazioni a utenti o gruppi per accedere agli oggetti SnapCenter , quali host, connessioni di archiviazione e gruppi di risorse.

È possibile assegnare autorizzazioni RBAC a utenti e gruppi all'interno della stessa foresta e a utenti appartenenti a foreste diverse. Non è possibile assegnare autorizzazioni RBAC agli utenti appartenenti a gruppi nidificati in più foreste.

Se si crea un ruolo personalizzato, questo deve contenere tutte le autorizzazioni del ruolo SnapCenterAdmin. Se si copiano solo alcune autorizzazioni, ad esempio Aggiunta host o Rimozione host, non sarà possibile eseguire tali operazioni.

Gli utenti sono tenuti a fornire l'autenticazione durante l'accesso, tramite l'interfaccia utente grafica (GUI) o utilizzando i cmdlet di PowerShell. Se gli utenti sono membri di più di un ruolo, dopo aver immesso le

credenziali di accesso, verrà chiesto loro di specificare il ruolo che desiderano utilizzare. Gli utenti devono inoltre fornire l'autenticazione per eseguire le API.

#### RBAC a livello di applicazione

SnapCenter utilizza le credenziali per verificare che gli utenti SnapCenter autorizzati dispongano anche delle autorizzazioni a livello di applicazione.

Ad esempio, se si desidera eseguire operazioni di protezione dei dati in un ambiente SQL Server, è necessario impostare le credenziali con le credenziali Windows o SQL appropriate. Il server SnapCenter autentica le credenziali impostate utilizzando entrambi i metodi. Se si desidera eseguire operazioni di protezione dei dati in un ambiente file system Windows su un archivio ONTAP , il ruolo di amministratore SnapCenter deve disporre di privilegi di amministratore sull'host Windows.

Allo stesso modo, se si desidera eseguire operazioni di protezione dei dati su un database Oracle e se l'autenticazione del sistema operativo (SO) è disabilitata nell'host del database, è necessario impostare le credenziali con il database Oracle o con le credenziali Oracle ASM. Il server SnapCenter autentica le credenziali impostate utilizzando uno di questi metodi, a seconda dell'operazione.

#### SnapCenter Plug-in for VMware vSphere RBAC

Se si utilizza il plug-in SnapCenter VMware per la protezione dei dati coerente con la VM, vCenter Server fornisce un livello aggiuntivo di RBAC. Il plug-in SnapCenter VMware supporta sia vCenter Server RBAC sia ONTAP RBAC. "Saperne di più"

| **Procedura consigliata:** NetApp consiglia di creare un ruolo ONTAP per il SnapCenter Plug-in for VMware vSphere e di assegnargli tutti i privilegi richiesti. |
|---|

#### Autorizzazioni ONTAP

È necessario creare un account vsadmin con le autorizzazioni necessarie per accedere al sistema di archiviazione."Saperne di più"

### Autorizzazioni assegnate ai ruoli predefiniti SnapCenter

Quando si aggiunge un utente a un ruolo, è necessario assegnare l'autorizzazione StorageConnection per abilitare la comunicazione con la macchina virtuale di archiviazione (SVM) oppure assegnare una SVM all'utente per abilitare l'autorizzazione a utilizzare la SVM. L'autorizzazione Connessione di archiviazione consente agli utenti di creare connessioni SVM.

Ad esempio, un utente con il ruolo di amministratore SnapCenter può creare connessioni SVM e assegnarle a un utente con il ruolo di amministratore di backup e clonazione delle app, che per impostazione predefinita non ha l'autorizzazione per creare o modificare connessioni SVM. Senza una connessione SVM, gli utenti non possono completare alcuna operazione di backup, clonazione o ripristino.

#### Ruolo di amministratore SnapCenter

Il ruolo di amministratore SnapCenter ha tutte le autorizzazioni abilitate. Non è possibile modificare le autorizzazioni per questo ruolo. È possibile aggiungere utenti e gruppi al ruolo oppure rimuoverli.

#### Ruolo di amministratore di backup e clonazione delle app

Il ruolo di amministratore di backup e clonazione delle app dispone delle autorizzazioni necessarie per eseguire azioni amministrative per i backup delle applicazioni e le attività correlate alla clonazione. Questo ruolo non dispone delle autorizzazioni per la gestione dell'host, il provisioning, la gestione della connessione di

archiviazione o l'installazione remota.

| Permessi | Abilitato | Creare | Leggere | Aggiornamento | Eliminare |
|---|---|---|---|---|---|
| Gruppo di risorse | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Politica | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Backup | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Ospite | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Connessione di archiviazione | Non applicabile | NO | SÌ | NO | NO |
| Clone | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Disposizione | Non applicabile | NO | SÌ | NO | NO |
| Pannello di controllo | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Rapporti | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Ripristinare | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Risorsa | SÌ | SÌ | SÌ | SÌ | SÌ |
| Installazione/disinstallazione del plug-in | NO | Non applicabile | | Non applicabile | Non applicabile |
| Migrazione | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Montare | SÌ | SÌ | Non applicabile | Non applicabile | Non applicabile |
| Smonta | SÌ | SÌ | Non applicabile | Non applicabile | Non applicabile |
| Ripristino del volume completo | NO | NO | Non applicabile | Non applicabile | Non applicabile |
| Protezione secondaria | NO | NO | Non applicabile | Non applicabile | Non applicabile |
| Monitoraggio del lavoro | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |

#### Ruolo di visualizzatore di backup e clonazione

Il ruolo di Visualizzatore backup e clonazione ha una visualizzazione di sola lettura di tutte le autorizzazioni. Questo ruolo dispone anche di autorizzazioni abilitate per la scoperta, la creazione di report e l'accesso alla Dashboard.

| Permessi | Abilitato | Creare | Leggere | Aggiornamento | Eliminare |
|---|---|---|---|---|---|
| Gruppo di risorse | Non applicabile | NO | SÌ | NO | NO |
| Politica | Non applicabile | NO | SÌ | NO | NO |
| Backup | Non applicabile | NO | SÌ | NO | NO |
| Ospite | Non applicabile | NO | SÌ | NO | NO |
| Connessione di archiviazione | Non applicabile | NO | SÌ | NO | NO |
| Clone | Non applicabile | NO | SÌ | NO | NO |
| Disposizione | Non applicabile | NO | SÌ | NO | NO |
| Pannello di controllo | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Rapporti | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Ripristinare | NO | NO | Non applicabile | Non applicabile | Non applicabile |
| Risorsa | NO | NO | SÌ | SÌ | NO |
| Installazione/disinstallazione del plug-in | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Migrazione | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Montare | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Smonta | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Ripristino del volume completo | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Protezione secondaria | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |

| Permessi | Abilitato | Creare | Leggere | Aggiornamento | Eliminare |
|---|---|---|---|---|---|
| Monitoraggio del lavoro | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |

#### Ruolo di amministratore dell'infrastruttura

Il ruolo di amministratore dell'infrastruttura dispone di autorizzazioni abilitate per la gestione dell'host, la gestione dell'archiviazione, il provisioning, i gruppi di risorse, i report di installazione remota e l'accesso alla dashboard.

| Permessi | Abilitato | Creare | Leggere | Aggiornamento | Eliminare |
|---|---|---|---|---|---|
| Gruppo di risorse | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Politica | Non applicabile | NO | SÌ | SÌ | SÌ |
| Backup | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Ospite | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Connessione di archiviazione | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Clone | Non applicabile | NO | SÌ | NO | NO |
| Disposizione | Non applicabile | SÌ | SÌ | SÌ | SÌ |
| Pannello di controllo | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Rapporti | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Ripristinare | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Risorsa | SÌ | SÌ | SÌ | SÌ | SÌ |
| Installazione/disinstallazione del plug-in | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Migrazione | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Montare | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |
| Smonta | NO | Non applicabile | Non applicabile | Non applicabile | Non applicabile |

| Permessi | Abilitato | Creare | Leggere | Aggiornamento | Eliminare |
|---|---|---|---|---|---|
| Ripristino del volume completo | NO | NO | Non applicabile | Non applicabile | Non applicabile |
| Protezione secondaria | NO | NO | Non applicabile | Non applicabile | Non applicabile |
| Monitoraggio del lavoro | SÌ | Non applicabile | Non applicabile | Non applicabile | Non applicabile |

## Ripristino di emergenza in SnapCenter

La funzionalità di ripristino di emergenza (DR) SnapCenter consente di ripristinare i dati in caso di disastri quali danneggiamento delle risorse o arresti anomali del server. Aiuta a ripristinare il repository SnapCenter , le pianificazioni del server, i componenti di configurazione e il plug-in SnapCenter per SQL Server e il relativo archivio.

Questa sezione spiega i due tipi di DR in SnapCenter:

### SnapCenter Server DR

- I dati di SnapCenter Server vengono sottoposti a backup e possono essere recuperati senza che sia necessario aggiungere o gestire alcun plug-in da SnapCenter Server.
- Il server SnapCenter secondario deve essere installato nella stessa directory di installazione e sulla stessa porta del server SnapCenter primario.
- Per l'autenticazione a più fattori (MFA), durante il ripristino di emergenza di SnapCenter Server, chiudere tutte le schede del browser e riaprire un browser per effettuare nuovamente l'accesso. In questo modo verranno cancellati i cookie di sessione esistenti o attivi e verranno aggiornati i dati di configurazione corretti.
- La funzionalità di ripristino di emergenza SnapCenter utilizza le API REST per eseguire il backup del server SnapCenter . Vedere "Flussi di lavoro API REST per il ripristino di emergenza di SnapCenter Server" .
- Il file di configurazione correlato alle impostazioni di controllo non viene sottoposto a backup nel backup DR né sul server DR dopo l'operazione di ripristino. Dovresti ripetere manualmente le impostazioni del registro di controllo.

### Plug-in SnapCenter e Storage DR

DR è disponibile solo per il plug-in SnapCenter per SQL Server. Se il plug-in non funziona, passare a un altro host SQL e recuperare i dati seguendo alcuni passaggi. Vedere "Ripristino di emergenza del plug-in SnapCenter per SQL Server" .

SnapCenter utilizza ONTAP SnapMirror per replicare i dati, che possono essere utilizzati per il DR mantenendo i dati sincronizzati su un sito secondario. Per avviare il failover, interrompere la replica SnapMirror . Durante il fallback, inverti la sincronizzazione per replicare i dati dal sito DR alla posizione primaria.

## Licenze richieste da SnapCenter

SnapCenter richiede diverse licenze per abilitare la protezione dei dati di applicazioni, database, file system e macchine virtuali. Il tipo di licenze SnapCenter da installare dipende dall'ambiente di archiviazione e dalle funzionalità che si desidera utilizzare.

| Licenza | Dove richiesto |
| --- | --- |
| Basato su controller SnapCenter Standard | Richiesto per FAS, AFF, ASA<br><br>La licenza SnapCenter Standard è una licenza basata su controller ed è inclusa come parte di NetApp ONTAP One. Se si dispone della licenza SnapManager Suite, si ottiene anche il diritto alla licenza SnapCenter Standard. Se si desidera installare SnapCenter in prova con storage FAS, AFF o ASA , è possibile ottenere una licenza di valutazione NetApp ONTAP One contattando il rappresentante commerciale.<br><br>Per informazioni sulle licenze incluse con NetApp ONTAP One, fare riferimento a "Licenze incluse con NetApp ONTAP One" .<br><br>SnapCenter è offerto anche come parte del pacchetto di protezione dei dati. Se hai acquistato A400 o una versione successiva, dovresti acquistare il pacchetto di protezione dei dati. |
| SnapMirror o SnapVault | ONTAP<br><br>Se la replica è abilitata in SnapCenter , è necessaria una licenza SnapMirror o SnapVault . |
| SnapRestore | Necessario per ripristinare e verificare i backup.<br><br>Sui sistemi di archiviazione primari<br><br>• Richiesto sui sistemi di destinazione SnapVault per eseguire la verifica remota e il ripristino da un backup.<br>• Richiesto sui sistemi di destinazione SnapMirror per eseguire la verifica remota. |

| Licenza | Dove richiesto |
| --- | --- |
| FlexClone | Necessario per clonare database e operazioni di verifica.<br><br>Sui sistemi di storage primari e secondari<br><br>• Richiesto sui sistemi di destinazione SnapVault per creare cloni dal backup del vault secondario.<br>• Richiesto sui sistemi di destinazione SnapMirror per creare cloni dal backup SnapMirror secondario. |
| Licenze di protocollo | • Licenza iSCSI o FC per LUN<br>• Licenza CIFS per azioni SMB<br>• Licenza NFS per VMDK di tipo NFS<br>• Licenza iSCSI o FC per VMDK di tipo VMFS<br><br>Richiesto sui sistemi di destinazione SnapMirror per fornire dati se un volume di origine non è disponibile. |
| Licenze SnapCenter Standard (facoltative) | Destinazioni secondarie<br><br>Si consiglia, ma non è obbligatorio, di aggiungere licenze SnapCenter Standard alle destinazioni secondarie. Se le licenze SnapCenter Standard non sono abilitate sulle destinazioni secondarie, non è possibile utilizzare SnapCenter per eseguire il backup delle risorse sulla destinazione secondaria dopo aver eseguito un'operazione di failover. Tuttavia, per eseguire operazioni di clonazione e verifica sulle destinazioni secondarie è necessaria una licenza FlexClone . |

| Licenza | Dove richiesto |
| --- | --- |
| Licenze Single Mailbox Recovery (SMBR) | Se si utilizza il plug-in SnapCenter per Exchange per gestire i database di Microsoft Exchange Server e Single Mailbox Recovery (SMBR), sarà necessaria una licenza aggiuntiva per SMBR, che deve essere acquistata separatamente in base alla casella di posta dell'utente.<br><br>NetApp® Single Mailbox Recovery ha raggiunto la fine della disponibilità (EOA) il 12 maggio 2023. Per maggiori informazioni, fare riferimento"CPC-00507" . NetApp continuerà a supportare i clienti che hanno acquistato capacità di casella di posta, manutenzione e supporto tramite i codici prodotto di marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.<br><br>NetApp Single Mailbox Recovery è un prodotto partner fornito da Ontrack. Ontrack PowerControls offre funzionalità simili a quelle di NetApp Single Mailbox Recovery. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di manutenzione e supporto Ontrack PowerControls da Ontrack (tramite licensingteam@ontrack.com) per il ripristino granulare delle caselle di posta dopo la data di scadenza del 12 maggio 2023. |

Le licenze SnapCenter Advanced e SnapCenter NAS File Services sono obsolete e non sono più disponibili. La licenza standard e la licenza basata sulla capacità non sono più necessarie per Amazon FSx for NetApp ONTAP, ONTAP Select, Cloud Volumes ONTAP e Azure NetApp Files.

Dovresti installare una o più licenze SnapCenter . Per informazioni su come aggiungere licenze, vedere"Aggiungi licenze basate sul controller SnapCenter Standard" .

## Sincronizzazione attiva SnapMirror in SnapCenter

La sincronizzazione attiva SnapMirror consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

Per ulteriori informazioni sulla sincronizzazione attiva SnapMirror , fare riferimento "Panoramica della sincronizzazione attiva SnapMirror" .

Per la sincronizzazione attiva SnapMirror , assicurati di aver soddisfatto i vari requisiti hardware, software e di configurazione del sistema. Per informazioni fare riferimento "Prerequisiti"

I plug-in supportati per questa funzionalità sono SnapCenter Plug-in per SQL Server, SnapCenter Plug-in per Windows, SnapCenter Plug-in per database Oracle, SnapCenter Plug-in per database SAP HANA,

SnapCenter Plug-in per Microsoft Exchange Server e SnapCenter Plug-in per Unix.

> Per supportare la prossimità dell'iniziatore host in SnapCenter, il suo valore, origine o destinazione, deve essere impostato in ONTAP.

Casi d'uso non supportati in SnapCenter:

- Se si convertono i carichi di lavoro attivi SnapMirror asimmetrici esistenti in simmetrici modificando la policy sulle relazioni di sincronizzazione attiva SnapMirror da *automatedfailover* a *automatedfailoverduplex* in ONTAP, la stessa operazione non è supportata in SnapCenter.
- Se sono presenti backup di un gruppo di risorse (già protetti in SnapCenter) e quindi la policy di archiviazione viene modificata nelle relazioni di sincronizzazione attiva SnapMirror da *automatedfailover* a *automatedfailoverduplex* in ONTAP, la stessa cosa non è supportata in SnapCenter.

## Concetti chiave della protezione dei dati

Prima di utilizzare SnapCenter, è necessario comprendere i concetti chiave relativi a backup, clonazione e ripristino.

### Risorse

Le risorse includono database, file system Windows o condivisioni di file sottoposti a backup o clonati con SnapCenter. A seconda dell'ambiente, le risorse potrebbero essere anche istanze di database, gruppi di disponibilità di SQL Server, database Oracle, database RAC o gruppi di applicazioni personalizzati.

### Gruppo di risorse

Un gruppo di risorse è una raccolta di risorse su un host o cluster, potenzialmente provenienti da più host e cluster. Le operazioni eseguite su un gruppo di risorse si applicano a tutte le sue risorse in base alla pianificazione specificata. È possibile eseguire backup su richiesta o pianificati per singole risorse o gruppi.

> Se un host in un gruppo di risorse condivise entra in modalità di manutenzione, tutte le operazioni pianificate per quel gruppo verranno sospese su tutti gli host.

Utilizzare i plug-in appropriati per eseguire il backup di risorse specifiche: plug-in di database per i database, plug-in di file system per i file system e SnapCenter Plug-in for VMware vSphere per VM e datastore.

### Politiche

Le policy specificano la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

È possibile selezionare una o più policy durante la creazione di un gruppo di risorse o durante l'esecuzione di un backup su richiesta.

Un gruppo di risorse definisce cosa deve essere protetto e quando deve essere protetto in termini di giorno e ora. Una politica descrive come verrà attuata la protezione. Ad esempio, se è necessario eseguire il backup di tutti i database o file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o file system nell'host. Al gruppo di risorse potrebbero quindi essere associate due policy: una policy giornaliera e una policy oraria.

Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurarlo per eseguire un backup completo ogni giorno e un'altra pianificazione per i backup del registro ogni ora.

Nelle operazioni di protezione dei dati è possibile utilizzare prescrizioni e post-scrizioni personalizzate. Questi script consentono l'automazione prima o dopo il processo di protezione dei dati. Ad esempio, uno script potrebbe notificare automaticamente errori o avvisi relativi ai processi di protezione dei dati. Prima di impostare prescript e postscript è fondamentale comprendere i requisiti per la creazione di questi script.

## Utilizzo di prescrizioni e poscrizioni

Prescrizioni e post-script personalizzati possono automatizzare le attività di protezione dei dati prima o dopo il lavoro. Ad esempio, puoi aggiungere uno script per ricevere notifiche di errori o avvisi nei processi. Prima di configurarli, assicurati di aver compreso i requisiti per questi script.

### Tipi di script supportati

Per Windows sono supportati i seguenti tipi di script:

- File batch
- Script di PowerShell
- script Perl

Per UNIX sono supportati i seguenti tipi di script:

- script Perl
- script Python
- Script di shell

> Oltre alla shell bash predefinita, sono supportate anche altre shell come sh-shell, k-shell e c-shell.

### Percorso dello script

Tutti i prescript e i postscript eseguiti come parte delle operazioni SnapCenter su sistemi di archiviazione virtualizzati e non virtualizzati vengono eseguiti sull'host plug-in.

- Gli script di Windows dovrebbero trovarsi sull'host del plug-in.

> Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

- Gli script UNIX dovrebbero trovarsi sull'host del plug-in.

> Il percorso dello script viene convalidato al momento dell'esecuzione.

### Dove specificare gli script

Gli script sono specificati nei criteri di backup. Quando viene avviato un processo di backup, il criterio associa automaticamente lo script alle risorse sottoposte a backup. Quando si crea un criterio di backup, è possibile specificare gli argomenti prescript e postscript.

> Non è possibile specificare più script.

#### Timeout degli script

Per impostazione predefinita, il timeout è impostato su 60 secondi. È possibile modificare il valore del timeout.

#### Output dello script

La directory predefinita per i file di output prescript e postscript di Windows è Windows\System32.

Non esiste una posizione predefinita per i prescript e i postscript UNIX. È possibile reindirizzare il file di output in qualsiasi posizione preferita.

## Sistemi di archiviazione e applicazioni supportati da SnapCenter

Dovresti conoscere i sistemi di archiviazione, le applicazioni e i database supportati da SnapCenter.

#### Sistemi di archiviazione supportati

- NetApp ONTAP 9.12.1 e versioni successive
- Azure NetApp Files
- Amazon FSx for NetApp ONTAP

  Supporta la memoria non volatile express (NVMe) tramite Transport Control Protocol (TCP).

  Per informazioni su Amazon FSx for NetApp ONTAP, vedere "Documentazione Amazon FSx for NetApp ONTAP" .

- Sistemi NetApp ASA r2 che eseguono NetApp ONTAP 9.16.1.

#### Applicazioni e database supportati

SnapCenter supporta la protezione di diverse applicazioni e database. Per informazioni dettagliate sulle applicazioni e sui database supportati, vedere "Strumento matrice di interoperabilità NetApp" .

SnapCenter supporta la protezione dei carichi di lavoro Oracle e Microsoft SQL negli ambienti VMware Cloud su Amazon Web Services (AWS) Software-Defined Data Center (SDDC). "Saperne di più" .

## Metodi di autenticazione per le credenziali SnapCenter

Le credenziali utilizzano metodi di autenticazione diversi a seconda dell'applicazione o dell'ambiente. Le credenziali autenticano gli utenti in modo che possano eseguire le operazioni SnapCenter . Dovresti creare un set di credenziali per l'installazione dei plug-in e un altro per le operazioni di protezione dei dati.

#### Autenticazione di Windows

Il metodo di autenticazione di Windows esegue l'autenticazione tramite Active Directory. Per l'autenticazione di Windows, Active Directory è configurato all'esterno di SnapCenter. SnapCenter esegue l'autenticazione senza alcuna configurazione aggiuntiva. Per aggiungere host, installare pacchetti plug-in e pianificare attività, è necessario disporre delle credenziali Windows.

### Autenticazione di dominio non attendibile

SnapCenter consente agli utenti e ai gruppi appartenenti a domini non attendibili di creare credenziali Windows. Per far sì che l'autenticazione vada a buon fine, è necessario registrare i domini non attendibili con SnapCenter.

### Autenticazione del gruppo di lavoro locale

SnapCenter consente la creazione di credenziali Windows con utenti e gruppi di lavoro locali. L'autenticazione di Windows per gli utenti e i gruppi di lavoro locali non avviene durante la creazione delle credenziali di Windows, ma viene posticipata finché non vengono eseguite la registrazione dell'host e altre operazioni sull'host.

### Autenticazione di SQL Server

Il metodo di autenticazione SQL esegue l'autenticazione su un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere individuata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. Per eseguire operazioni quali la pianificazione su SQL Server o l'individuazione di risorse è necessaria l'autenticazione di SQL Server.

### Autenticazione Linux

Il metodo di autenticazione Linux esegue l'autenticazione su un host Linux. È necessaria l'autenticazione Linux durante la fase iniziale di aggiunta dell'host Linux e di installazione remota del pacchetto plug-in SnapCenter per Linux dalla GUI SnapCenter .

### Autenticazione AIX

Il metodo di autenticazione AIX esegue l'autenticazione su un host AIX. È necessaria l'autenticazione AIX durante la fase iniziale di aggiunta dell'host AIX e di installazione remota del pacchetto plug-in SnapCenter per AIX dalla GUI SnapCenter .

### Autenticazione del database Oracle

Il metodo di autenticazione del database Oracle esegue l'autenticazione su un database Oracle. Per eseguire operazioni sul database Oracle è necessaria l'autenticazione del database Oracle se l'autenticazione del sistema operativo (SO) è disabilitata sull'host del database. Pertanto, prima di aggiungere una credenziale del database Oracle, è necessario creare un utente Oracle nel database Oracle con privilegi sysdba.

### Autenticazione Oracle ASM

Il metodo di autenticazione Oracle ASM esegue l'autenticazione su un'istanza di Oracle Automatic Storage Management (ASM). L'autenticazione Oracle ASM è obbligatoria se è necessario accedere a un'istanza Oracle ASM e l'autenticazione del sistema operativo è disabilitata sull'host del database. Prima di aggiungere una credenziale Oracle ASM, creare un utente Oracle con privilegi di sistema nell'istanza ASM.

### Autenticazione del catalogo RMAN

Il metodo di autenticazione del catalogo RMAN esegue l'autenticazione in base al database del catalogo Oracle Recovery Manager (RMAN). Se hai configurato un meccanismo di catalogo esterno e registrato il tuo database nel database di catalogo, devi aggiungere l'autenticazione del catalogo RMAN.

# Operazioni SnapCenter supportate per sistemi ASA r2

I sistemi di archiviazione ASA r2 sono supportati a partire da SnapCenter 6.1. "Scopri di più sui sistemi ASA r2"

SnapCenter sfrutta le API REST per eseguire tutte le operazioni sui sistemi ASA r2, che non supportano le ZAPI.

**Operazioni supportate da SnapCenter per sistemi ASA r2**

- Creazione di backup primari delle applicazioni su VMDK
- Trasferimento degli snapshot del gruppo di coerenza al sistema di archiviazione secondario
- Ripristino dei backup dai sistemi di archiviazione primari e secondari all'host originale o all'host alternativo
  - Ripristino sul posto da sistemi di archiviazione primari e secondari utilizzando VMware vMotion
  - Connetti e copia il ripristino dai sistemi di archiviazione primari e secondari
- Clonazione dei backup sull'host originale o sull'host alternativo

SnapCenter può scoprire o creare gruppi di coerenza ONTAP . Può anche predisporre e inizializzare le relazioni SnapMirror sul cluster di destinazione per una protezione secondaria.

Per informazioni sull'abilitazione della protezione secondaria sui sistemi ASA r2 per la tua applicazione, fai riferimento a:

- "Abilita la protezione secondaria per le risorse di Microsoft SQL Server"
- "Abilita la protezione secondaria per le risorse SAP HANA"
- "Abilita la protezione secondaria per le risorse Oracle"
- "Abilita la protezione secondaria per i file system di Windows"
- "Abilita la protezione secondaria per le risorse IBM Db2"
- "Abilita la protezione secondaria per le risorse PostgreSQL"
- "Abilita la protezione secondaria per le risorse MySQL"
- "Abilita la protezione secondaria per i file system Unix"

**Operazioni non supportate da SnapCenter per i sistemi ASA r2**

- Mappatura dei dispositivi grezzi (RDM)
- Volumi applicativi per Oracle
- SAP HANA NDV
- LockVault
- Istantanee a prova di manomissione
- Volumi FlexGroup
- Gruppo di coerenza gerarchica
- Migrazione dai sistemi di archiviazione ASA, AFF o FAS ai sistemi di archiviazione ASA r2
- Protezione dei database che hanno un mix di risorse ASA, AFF o FAS e risorse ASA r2
- Ridenominazione degli snapshot

- Provisioning secondario della directory di registro dell'host del plug-in SQL

# Avvio rapido del SnapCenter software

La guida rapida descrive i passaggi di base per installare e configurare il SnapCenter software.

### 1 Prepararsi all'installazione di SnapCenter Server

È necessario assicurarsi che siano soddisfatti tutti i requisiti per l'installazione di SnapCenter Server.

- "Requisiti"
- "Registrati per accedere SnapCenter software"
- "Abilita l'autenticazione a più fattori"

### 2 Installa SnapCenter Server

SnapCenter Server può essere installato su host Windows o Linux. Scaricare il pacchetto di installazione di SnapCenter Server da "Sito di supporto NetApp" ed eseguire il programma di installazione.

- "Installa il server SnapCenter su Windows"
- "Installa SnapCenter Server su Linux"

### 3 Configurare SnapCenter Server

Dopo aver installato SnapCenter Server, è necessario configurarlo in base al proprio ambiente.

### 4 Installa il plug-in per la tua applicazione

Assicurarsi che tutti i requisiti per l'installazione del plug-in specifico dell'applicazione siano soddisfatti in base all'applicazione in uso, quindi procedere con l'installazione del rispettivo plug-in.

### 5 Proteggi la tua applicazione

Dopo aver installato correttamente SnapCenter Server e i plug-in necessari, è possibile avviare la creazione dei backup dell'applicazione. Questi backup possono essere successivamente utilizzati per scopi di ripristino e clonazione, quando necessario.

# Installa e configura SnapCenter Server

## Prepararsi all'installazione di SnapCenter Server

### Requisiti per installare SnapCenter Server

Prima di installare SnapCenter Server su un host Windows o Linux, è necessario verificare e assicurarsi che tutti i requisiti per l'ambiente siano soddisfatti.

#### Requisiti di dominio e gruppo di lavoro per l'host Windows

SnapCenter Server può essere installato su un host Windows appartenente a un dominio o a un gruppo di lavoro.

L'utente con privilegi di amministratore è autorizzato a installare il server SnapCenter .

- Dominio Active Directory: è necessario utilizzare un utente di dominio con diritti di amministratore locale. L'utente del dominio deve essere membro del gruppo Administrator locale sull'host Windows.
- Gruppi di lavoro: è necessario utilizzare un account locale con diritti di amministratore locale.

Sebbene siano supportati trust di dominio, foreste multidominio e trust tra domini, i domini tra foreste non sono supportati. Per ulteriori informazioni, consultare la documentazione Microsoft sui domini e i trust di Active Directory.

Dopo aver installato SnapCenter Server, non modificare il dominio in cui si trova l'host SnapCenter . Se si rimuove l'host di SnapCenter Server dal dominio in cui si trovava al momento dell'installazione di SnapCenter Server e poi si tenta di disinstallare SnapCenter Server, l'operazione di disinstallazione non riesce.

#### Requisiti di spazio e dimensioni

Dovresti conoscere i requisiti di spazio e dimensioni.

| Articolo | Requisiti host Windows | Requisiti host Linux |
|---|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Sono supportate solo le versioni in inglese, tedesco, giapponese e cinese semplificato dei sistemi operativi.<br><br>Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121033;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] . | • Red Hat Enterprise Linux (RHEL) 8 e 9<br>• SUSE Linux Enterprise Server (SLES) 15<br><br>Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121032;&solution=1258&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] . |

| Articolo | Requisiti host Windows | Requisiti host Linux |
| --- | --- | --- |
| Numero minimo di CPU | 4 core | 4 core |
| RAM minima | 8 GB<br>Il buffer pool di MySQL Server utilizza il 20 percento della RAM totale. | 8 GB |
| Spazio minimo sul disco rigido per il software e i registri di SnapCenter Server | 7 GB<br>Se il repository SnapCenter si trova nella stessa unità in cui è installato SnapCenter Server, si consiglia di disporre di 15 GB. | 15 GB |
| Spazio minimo su disco rigido per il repository SnapCenter | 8 GB<br>NOTA: se SnapCenter Server si trova nella stessa unità in cui è installato il repository SnapCenter , si consiglia di disporre di 15 GB. | Non applicabile |

| Articolo | Requisiti host Windows | Requisiti host Linux |
| --- | --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell 7.4.2 o versione successiva<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet" . | • .NET Framework 8.0.12 (e tutte le successive patch 8.0.x)<br>• PowerShell 7.4.2 o versione successiva<br>• Nginx è un server web che può essere utilizzato come proxy inverso<br>• Pam-devel<br><br>PAM (Pluggable Authentication Modules) è uno strumento di sicurezza del sistema che consente agli amministratori di sistema di impostare criteri di autenticazione senza dover ricompilare i programmi che eseguono l'autenticazione. |

ASP.NET Core necessita di IIS_IUSRS per accedere al file system temporaneo in SnapCenter Server su Windows.

### Requisiti dell'host SAN

SnapCenter non include utilità host o un DSM. Se l'host SnapCenter fa parte di un ambiente SAN (FC/iSCSI), potrebbe essere necessario installare e configurare software aggiuntivo sull'host SnapCenter Server.

- Utilità host: le utilità host supportano FC e iSCSI e consentono di utilizzare MPIO sui server Windows. "Saperne di più" .
- Microsoft DSM per Windows MPIO: questo software funziona con i driver Windows MPIO per gestire più percorsi tra NetApp e computer host Windows. Per le configurazioni ad alta disponibilità è necessario un DSM.

Se utilizzavi ONTAP DSM, dovresti migrare a Microsoft DSM. Per ulteriori informazioni, vedere "Come migrare da ONTAP DSM a Microsoft DSM" .

### Requisiti del browser

Il SnapCenter software supporta Chrome 125 e versioni successive e Microsoft Edge 110.0.1587.17 e versioni successive.

### Requisiti portuali

Il SnapCenter software richiede porte diverse per la comunicazione tra i diversi componenti.

- Le applicazioni non possono condividere una porta.
- Per le porte personalizzabili, è possibile selezionare una porta personalizzata durante l'installazione se non si desidera utilizzare la porta predefinita.

- Per le porte fisse, dovresti accettare il numero di porta predefinito.
- Firewall
  - Firewall, proxy o altri dispositivi di rete non devono interferire con le connessioni.
  - Se si specifica una porta personalizzata durante l'installazione SnapCenter, è necessario aggiungere una regola firewall sull'host del plug-in per quella porta per SnapCenter Plug-in Loader.

Nella tabella seguente sono elencate le diverse porte e i relativi valori predefiniti.

| Nome della porta | Numeri di porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|---|
| Porta web SnapCenter | 8146 | HTTPS | Bidirezionale | Questa porta viene utilizzata per la comunicazione tra il client SnapCenter (l'utente SnapCenter ) e il server SnapCenter e viene utilizzata anche per la comunicazione dagli host del plug-in al server SnapCenter .<br><br>È possibile personalizzare il numero di porta. |
| Porta di comunicazione SnapCenter SMCore | 8145 | HTTPS | Bidirezionale | Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e gli host in cui sono installati i plug-in SnapCenter .<br><br>È possibile personalizzare il numero di porta. |

| Nome della porta | Numeri di porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|---|
| Porta del servizio di pianificazione | 8154 | HTTPS | | Questa porta viene utilizzata per orchestrare in modo centralizzato i flussi di lavoro dello scheduler di SnapCenter per tutti i plug-in gestiti all'interno dell'host del server SnapCenter .<br><br>È possibile personalizzare il numero di porta. |
| Porta RabbitMQ | 5672 | TCP | | Questa è la porta predefinita su cui RabbitMQ è in ascolto e viene utilizzata per la comunicazione del modello publisher-subscriber tra il servizio Scheduler e SnapCenter. |
| Porta MySQL | 3306 | HTTPS | | La porta viene utilizzata per comunicare con il database del repository SnapCenter . È possibile creare connessioni protette dal server SnapCenter al server MySQL."Saperne di più" |

| Nome della porta | Numeri di porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|---|
| Host plug-in di Windows | 135, 445 | TCP | | Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host su cui viene installato il plug-in. Dovrebbe essere aperto anche un intervallo di porte dinamiche aggiuntivo specificato da Microsoft. |
| Host plug-in Linux o AIX | 22 | SSH | Unidirezionale | Questa porta viene utilizzata per la comunicazione tra SnapCenter Server e l'host, avviata dal server all'host client. |
| Pacchetto di plug-in SnapCenter per Windows, Linux o AIX | 8145 | HTTPS | Bidirezionale | Questa porta viene utilizzata per la comunicazione tra SMCore e gli host in cui è installato il pacchetto plug-in. Personalizzabile.<br><br>È possibile personalizzare il numero di porta. |
| Plug-in SnapCenter per Oracle Database | 27216 | | | La porta JDBC predefinita viene utilizzata dal plug-in per Oracle per la connessione al database Oracle. |
| Plug-in SnapCenter per database Exchange | 909 | | | La porta NET.TCP predefinita viene utilizzata dal plug-in per Windows per la connessione ai callback di Exchange VSS. |

| Nome della porta | Numeri di porta | Protocollo | Direzione | Descrizione |
| --- | --- | --- | --- | --- |
| Plug-in supportati da NetApp per SnapCenter | 9090 | HTTPS | | Si tratta di una porta interna utilizzata solo sull'host del plug-in; non è richiesta alcuna eccezione del firewall.<br><br>La comunicazione tra SnapCenter Server e i plug-in avviene tramite la porta 8145. |
| Cluster ONTAP o porta di comunicazione SVM | • 443 (HTTPS)<br>• 80 (HTTP) | • HTTPS<br>• HTTP | Bidirezionale | La porta viene utilizzata dal SAL (Storage Abstraction Layer) per la comunicazione tra l'host che esegue SnapCenter Server e SVM. Attualmente la porta è utilizzata anche dal SAL sugli host del plug-in SnapCenter per Windows per la comunicazione tra l'host del plug-in SnapCenter e SVM. |
| Plug-in SnapCenter per database SAP HANA | • 3instance_number13<br>• 3instance_number15 | • HTTPS<br>• HTTP | Bidirezionale | Per un contenitore di database multi-tenant (MDC) con un solo tenant, il numero di porta termina con 13; per un contenitore non MDC, il numero di porta termina con 15.<br><br>È possibile personalizzare il numero di porta. |

| Nome della porta | Numeri di porta | Protocollo | Direzione | Descrizione |
|---|---|---|---|---|
| Plug-in SnapCenter per PostgreSQL | 5432 | | | Questa porta è la porta PostgreSQL predefinita utilizzata per la comunicazione tra il plug-in per PostgreSQL e il cluster PostgreSQL.<br><br>È possibile personalizzare il numero di porta. |

## Registrati per accedere al SnapCenter software

Se non hai familiarità con Amazon FSx for NetApp ONTAP o Azure NetApp Files e non hai un account NetApp esistente, devi registrarti per accedere al SnapCenter software.

**Prima di iniziare**

- Dovresti avere accesso all'ID e-mail aziendale.
- Se si utilizza Azure NetApp Files, è necessario disporre dell'ID di sottoscrizione di Azure.
- Se si utilizza Amazon FSx for NetApp ONTAP, è necessario disporre dell'ID del file system FSx per ONTAP .

**Informazioni su questo compito**

La registrazione è soggetta a convalida delle informazioni e potrebbe volerci fino a un giorno per confermare e aggiornare il nuovo account NetApp Support Site (NSS) dall'accesso **ospite** all'accesso **completo**.

**Passi**

1. Clic https://mysupport.netapp.com/site/user/registration per la registrazione.
2. Inserisci il tuo ID e-mail aziendale, completa il captcha, accetta l'informativa sulla privacy di NetApp e fai clic su **Invia**.
3. Autentica la registrazione inserendo l'OTP inviato al tuo indirizzo e-mail e clicca su **Continua**.
4. Nella pagina di completamento della registrazione, inserisci i seguenti dati per completare la registrazione.
   a. Seleziona **Cliente NetApp /Utente finale**.
   b. Nel campo NUMERO DI SERIE, immettere l'ID della sottoscrizione di Azure se si utilizza Azure NetApp Files oppure l'ID del file system se si utilizza Amazon FSx for NetApp ONTAP.

Puoi sollevare un biglietto a https://mysupport.netapp.com/site/help se riscontri problemi durante la registrazione o per conoscerne lo stato.

## Autenticazione a più fattori (MFA)

**Gestire l'autenticazione a più fattori (MFA)**

È possibile gestire la funzionalità di autenticazione a più fattori (MFA) nel server Active

Directory Federation Service (AD FS) e nel server SnapCenter .

#### Abilita l'autenticazione a più fattori (MFA)

È possibile abilitare la funzionalità MFA per SnapCenter Server utilizzando i comandi di PowerShell.

**Informazioni su questo compito**

- SnapCenter supporta gli accessi basati su SSO quando altre applicazioni sono configurate nello stesso AD FS. In alcune configurazioni di AD FS, SnapCenter potrebbe richiedere l'autenticazione dell'utente per motivi di sicurezza, a seconda della persistenza della sessione AD FS.
- Le informazioni riguardanti i parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo `Get-Help command_name` . In alternativa, puoi anche vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

**Prima di iniziare**

- Windows Active Directory Federation Service (AD FS) deve essere attivo e funzionante nel rispettivo dominio.
- Dovresti disporre di un servizio di autenticazione a più fattori supportato da AD FS, come Azure MFA, Cisco Duo e così via.
- Il timestamp SnapCenter e del server AD FS deve essere lo stesso, indipendentemente dal fuso orario.
- Ottenere e configurare il certificato CA autorizzato per SnapCenter Server.

  Il certificato CA è obbligatorio per i seguenti motivi:

  - Garantisce che le comunicazioni ADFS-F5 non vengano interrotte perché i certificati autofirmati sono univoci a livello di nodo.
  - Garantisce che durante l'aggiornamento, la riparazione o il ripristino di emergenza (DR) in una configurazione autonoma o ad alta disponibilità, il certificato autofirmato non venga ricreato, evitando così la riconfigurazione MFA.
  - Garantisce le risoluzioni IP-FQDN.

    Per informazioni sul certificato CA, vedere"Genera file CSR del certificato CA" .

**Passi**

1. Connettersi all'host Active Directory Federation Services (AD FS).
2. Scarica il file dei metadati della federazione AD FS da"https://<host FQDN>/FederationMetadata/2007-06/FederationMetadata.xml".
3. Copiare il file scaricato su SnapCenter Server per abilitare la funzionalità MFA.
4. Accedere a SnapCenter Server come utente amministratore SnapCenter tramite PowerShell.
5. Utilizzando la sessione di PowerShell, generare il file di metadati SnapCenter MFA utilizzando il cmdlet *New-SmMultifactorAuthenticationMetadata -path*.

   Il parametro path specifica il percorso in cui salvare il file di metadati MFA nell'host del server SnapCenter .
6. Copiare il file generato nell'host AD FS per configurare SnapCenter come entità client.
7. Abilita MFA per SnapCenter Server utilizzando `Set-SmMultiFactorAuthentication` cmdlet.
8. (Facoltativo) Controllare lo stato e le impostazioni della configurazione MFA utilizzando `Get-SmMultiFactorAuthentication` cmdlet.

9. Accedere alla console di gestione Microsoft (MMC) ed eseguire i seguenti passaggi:
    a. Fare clic su **File** > **Aggiungi/Rimuovi snap-in**.
    b. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
    c. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
    d. Fare clic su **Console Root** > **Certificati – Computer locale** > **Personale** > **Certificati**.
    e. Fare clic con il pulsante destro del mouse sul certificato CA associato a SnapCenter , quindi selezionare **Tutte le attività** > **Gestisci chiavi private**.
    f. Nella procedura guidata per le autorizzazioni, eseguire i seguenti passaggi:
        i. Fare clic su **Aggiungi**.
        ii. Fare clic su **Posizioni** e selezionare l'host interessato (in cima alla gerarchia).
        iii. Fare clic su **OK** nella finestra pop-up **Posizioni**.
        iv. Nel campo del nome dell'oggetto, immettere 'IIS_IUSRS' e fare clic su **Controlla nomi**, quindi fare clic su **OK**.

            Se il controllo ha esito positivo, fare clic su **OK**.

10. Nell'host AD FS, aprire la procedura guidata di gestione AD FS ed eseguire i seguenti passaggi:
    a. Fare clic con il pulsante destro del mouse su **Trust della parte affidabile** > **Aggiungi trust della parte affidabile** > **Avvia**.
    b. Selezionare la seconda opzione, sfogliare il file dei metadati SnapCenter MFA e fare clic su **Avanti**.
    c. Specificare un nome visualizzato e fare clic su **Avanti**.
    d. Selezionare una policy di controllo degli accessi in base alle proprie esigenze e fare clic su **Avanti**.
    e. Selezionare le impostazioni predefinite nella scheda successiva.
    f. Fare clic su **Fine**.

        SnapCenter viene ora visualizzato come relying party con il nome visualizzato fornito.

11. Selezionare il nome ed eseguire i seguenti passaggi:
    a. Fare clic su **Modifica politica di emissione reclami**.
    b. Fare clic su **Aggiungi regola** e quindi su **Avanti**.
    c. Specificare un nome per la regola di rivendicazione.
    d. Selezionare **Active Directory** come archivio attributi.
    e. Selezionare l'attributo come **User-Principal-Name** e il tipo di claim in uscita come **Name-ID**.
    f. Fare clic su **Fine**.
12. Eseguire i seguenti comandi PowerShell sul server ADFS.

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

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

13. Per confermare che i metadati siano stati importati correttamente, procedere come segue.

a. Fare clic con il pulsante destro del mouse sul trust della parte affidabile e selezionare **Proprietà**.

b. Assicurarsi che i campi Endpoint, Identificatori e Firma siano compilati.

14. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

La funzionalità SnapCenter MFA può essere abilitata anche tramite API REST.

Per informazioni sulla risoluzione dei problemi, vedere "I tentativi di accesso simultanei in più schede mostrano un errore MFA" .

#### Aggiorna i metadati AD FS MFA

È necessario aggiornare i metadati AD FS MFA in SnapCenter ogni volta che si verifica una modifica nel server AD FS, ad esempio un aggiornamento, un rinnovo del certificato CA, un ripristino di emergenza e così via.

**Passi**

1. Scarica il file dei metadati della federazione AD FS da"https://<host Nome di dominio completo>/FederationMetadata/2007-06/FederationMetadata.xml"
2. Copiare il file scaricato su SnapCenter Server per aggiornare la configurazione MFA.
3. Aggiornare i metadati AD FS in SnapCenter eseguendo il seguente cmdlet:

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

4. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

#### Aggiorna i metadati SnapCenter MFA

È necessario aggiornare i metadati SnapCenter MFA in AD FS ogni volta che si verifica una modifica nel server ADFS, ad esempio riparazione, rinnovo del certificato CA, DR e così via.

**Passi**

1. Nell'host AD FS, aprire la procedura guidata di gestione AD FS ed eseguire i seguenti passaggi:
   a. Selezionare **Trust della parte affidante**.
   b. Fare clic con il pulsante destro del mouse sul trust della relying party creato per SnapCenter e selezionare **Elimina**.

      Verrà visualizzato il nome definito dall'utente del trust della parte affidabile.

   c. Abilita l'autenticazione a più fattori (MFA).

      Vedere "Abilita l'autenticazione a più fattori" .

2. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

#### Disabilitare l'autenticazione a più fattori (MFA)

**Passi**

1. Disabilitare MFA e pulire i file di configurazione creati quando MFA è stato abilitato utilizzando `Set-`

`SmMultiFactorAuthentication` cmdlet.

2. Chiudere tutte le schede del browser e riaprire il browser per cancellare i cookie di sessione esistenti o attivi, quindi effettuare nuovamente l'accesso.

#### Gestire l'autenticazione a più fattori (MFA) utilizzando REST API, PowerShell e SCCLI

L'accesso MFA è supportato da browser, REST API, PowerShell e SCCLI. L'MFA è supportato tramite un gestore di identità AD FS. È possibile abilitare MFA, disabilitare MFA e configurare MFA da GUI, REST API, PowerShell e SCCLI.

##### Imposta AD FS come OAuth/OIDC

#### Configurare AD FS utilizzando la procedura guidata GUI di Windows

1. Passare a **Dashboard di Server Manager** > **Strumenti** > **Gestione ADFS**.
2. Passare a **ADFS** > **Gruppi di applicazioni**.
   a. Fare clic con il tasto destro del mouse su **Gruppi di applicazioni**.
   b. Selezionare **Aggiungi gruppo di applicazioni** e immettere **Nome applicazione**.
   c. Selezionare **Applicazione server**.
   d. Fare clic su **Avanti**.
3. Copia **Identificatore cliente**.

   Questo è l'ID cliente. .. Aggiungere l'URL di callback (URL del server SnapCenter ) nell'URL di reindirizzamento. .. Fare clic su **Avanti**.

4. Seleziona **Genera segreto condiviso**.

   Copia il valore segreto. Questo è il segreto del cliente. .. Fare clic su **Avanti**.

5. Nella pagina **Riepilogo**, fare clic su **Avanti**.
   a. Nella pagina **Completa**, fare clic su **Chiudi**.
6. Fare clic con il pulsante destro del mouse sul **Gruppo applicazioni** appena aggiunto e selezionare **Proprietà**.
7. Selezionare **Aggiungi applicazione** da Proprietà app.
8. Fare clic su **Aggiungi applicazione**.

   Selezionare Web API e fare clic su **Avanti**.

9. Nella pagina Configura API Web, immettere l'URL del server SnapCenter e l'identificatore client creati nel passaggio precedente nella sezione Identificatore.
   a. Fare clic su **Aggiungi**.
   b. Fare clic su **Avanti**.
10. Nella pagina **Scegli criterio di controllo degli accessi**, seleziona il criterio di controllo in base alle tue esigenze (ad esempio, Consenti a tutti e richiedi MFA) e fai clic su **Avanti**.
11. Nella pagina **Configura autorizzazione applicazione**, per impostazione predefinita openid è selezionato come ambito, fare clic su **Avanti**.
12. Nella pagina **Riepilogo**, fare clic su **Avanti**.

Nella pagina **Completa**, fare clic su **Chiudi**.

13. Nella pagina **Proprietà applicazione di esempio**, fare clic su **OK**.
14. Token JWT emesso da un server di autorizzazione (AD FS) e destinato a essere utilizzato dalla risorsa.

    La rivendicazione "aud" o audience di questo token deve corrispondere all'identificatore della risorsa o dell'API Web.

15. Modifica la WebAPI selezionata e verifica che l'URL di callback (URL del server SnapCenter ) e l'identificatore client siano stati aggiunti correttamente.

    Configurare OpenID Connect per fornire un nome utente come claim.

16. Aprire lo strumento **Gestione AD FS** che si trova nel menu **Strumenti** in alto a destra di Server Manager.
    a. Selezionare la cartella **Gruppi di applicazioni** dalla barra laterale sinistra.
    b. Selezionare l'API Web e fare clic su **MODIFICA**.
    c. Vai alla scheda Regole di trasformazione dell'emissione
17. Fare clic su **Aggiungi regola**.
    a. Selezionare **Invia attributi LDAP come claim** nel menu a discesa Modello regola claim.
    b. Fare clic su **Avanti**.
18. Inserisci il nome della **Regola di rivendicazione**.
    a. Selezionare **Active Directory** nel menu a discesa Archivio attributi.
    b. Selezionare **User-Principal-Name** nel menu a discesa **LDAP Attribute** e **UPN** nel menu a discesa O*outgoing Claim Type*.
    c. Fare clic su **Fine**.

#### Creare un gruppo di applicazioni utilizzando i comandi di PowerShell

È possibile creare il gruppo di applicazioni, l'API Web e aggiungere l'ambito e le attestazioni utilizzando i comandi di PowerShell. Questi comandi sono disponibili in formato script automatizzato. Per maggiori informazioni vedere <link all'articolo della Knowledge Base>.

1. Creare il nuovo gruppo di applicazioni in AD FS utilizzando il seguente comando.

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

   `ClientRoleIdentifier`nome del tuo gruppo di applicazioni

   `redirectURL`URL valido per il reindirizzamento dopo l'autorizzazione

2. Creare l'applicazione server AD FS e generare il segreto client.

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

3. Creare l'applicazione ADFS Web API e configurare il nome del criterio che deve utilizzare.

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

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

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

4. Ottieni l'ID client e il segreto client dall'output dei seguenti comandi perché vengono mostrati solo una volta.

```
"client_id = $identifier"

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

5. Concedere all'applicazione AD FS le autorizzazioni allatclaims e openid.

```
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. Scrivere il file delle regole di trasformazione.

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

7. Assegna un nome all'applicazione Web API e definisci le sue regole di trasformazione del rilascio utilizzando un file esterno.

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

$identifier -Identifier $identifier,$redirectURL -IssuanceTransformRulesFile

$relativePath
```

#### Aggiorna il tempo di scadenza del token di accesso

È possibile aggiornare la scadenza del token di accesso utilizzando il comando PowerShell.

### Informazioni su questo compito

- Un token di accesso può essere utilizzato solo per una combinazione specifica di utente, client e risorsa. I token di accesso non possono essere revocati e sono validi fino alla loro scadenza.
- Per impostazione predefinita, il tempo di scadenza di un token di accesso è di 60 minuti. Questo tempo di scadenza minimo è sufficiente e proporzionato. È necessario fornire un valore sufficiente per evitare lavori critici per l'azienda in corso.

### Fare un passo

Per aggiornare la scadenza del token di accesso per un gruppo di applicazioni WebApi, utilizzare il seguente comando nel server AD FS.

+

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

#### Ottieni il token portatore da AD FS

Dovresti compilare i parametri menzionati di seguito in qualsiasi client REST (come Postman) e ti verrà chiesto di inserire le credenziali utente. Inoltre, dovresti inserire l'autenticazione a due fattori (qualcosa che hai e qualcosa che sei) per ottenere il token portatore.

+ La validità del token portatore è configurabile dal server AD FS per applicazione e il periodo di validità predefinito è di 60 minuti.

| Campo | Valore |
|---|---|
| Tipo di sovvenzione | Codice di autorizzazione |
| URL di richiamata | Se non si dispone di un URL di callback, immettere l'URL di base dell'applicazione. |
| URL di autorizzazione | [nome-dominio-adfs]/adfs/oauth2/authorize |
| URL del token di accesso | [nome-dominio-adfs]/adfs/oauth2/token |
| ID cliente | Inserisci l'ID client AD FS |
| Segreto del cliente | Inserisci il segreto del client AD FS |
| Ambito | OpenID |
| Autenticazione del client | Invia come intestazione AUTH di base |
| Risorsa | Nella scheda **Opzioni avanzate**, aggiungi il campo Risorsa con lo stesso valore dell'URL di callback, che viene fornito come valore "aud" nel token JWT. |

### Configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API

## È possibile configurare MFA in SnapCenter Server utilizzando PowerShell, SCCLI e REST API.

#### Autenticazione SnapCenter MFA CLI

In PowerShell e SCCLI, il cmdlet esistente (Open-SmConnection) è esteso con un ulteriore campo denominato "AccessToken" per utilizzare il token di connessione per autenticare l'utente.

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

Dopo l'esecuzione del cmdlet sopra indicato, viene creata una sessione per consentire all'utente interessato di eseguire ulteriori cmdlet SnapCenter .

#### Autenticazione API REST MFA SnapCenter

Utilizzare il token del portatore nel formato *Authorization=Bearer <token di accesso>* nel client REST API (come Postman o Swagger) e menzionare l'utente RoleName nell'intestazione per ottenere una risposta positiva da SnapCenter.

#### Flusso di lavoro dell'API REST MFA

Quando MFA è configurato con AD FS, è necessario autenticarsi utilizzando un token di accesso (bearer) per accedere all'applicazione SnapCenter tramite qualsiasi API REST.

### Informazioni su questo compito

- Puoi utilizzare qualsiasi client REST come Postman, Swagger UI o FireCamp.
- Ottieni un token di accesso e utilizzalo per autenticare le richieste successive (SnapCenter Rest API) per eseguire qualsiasi operazione.

### Passi

### Per autenticarsi tramite AD FS MFA

1. Configurare il client REST per chiamare l'endpoint AD FS per ottenere il token di accesso.

   Quando fai clic sul pulsante per ottenere un token di accesso per un'applicazione, verrai reindirizzato alla pagina AD FS SSO, dove dovrai fornire le tue credenziali AD ed eseguire l'autenticazione con MFA. 1. Nella pagina AD FS SSO, digita il tuo nome utente o indirizzo email nella casella di testo Nome utente.

   + I nomi utente devono essere formattati come utente@dominio o dominio\utente.

2. Nella casella di testo Password, digita la tua password.
3. Fare clic su **Accedi**.
4. Dalla sezione **Opzioni di accesso**, seleziona un'opzione di autenticazione ed esegui l'autenticazione (a seconda della configurazione).
   - Push: approva la notifica push inviata al tuo telefono.
   - Codice QR: usa l'app mobile AUTH Point per scansionare il codice QR, quindi digita il codice di verifica mostrato nell'app

◦ Password monouso: digita la password monouso per il tuo token.

5. Dopo l'autenticazione avvenuta con successo, si aprirà una finestra popup contenente il token di accesso, l'ID e il token di aggiornamento.

   Copia il token di accesso e utilizzalo nell'API Rest SnapCenter per eseguire l'operazione.

6. Nell'API REST, dovresti passare il token di accesso e il nome del ruolo nella sezione dell'intestazione.
7. SnapCenter convalida questo token di accesso da AD FS.

   Se si tratta di un token valido, SnapCenter lo decodifica e ottiene il nome utente.

8. Utilizzando il nome utente e il nome del ruolo, SnapCenter autentica l'utente per l'esecuzione dell'API.

   Se l'autenticazione riesce, SnapCenter restituisce il risultato, altrimenti viene visualizzato un messaggio di errore.

#### Abilita o disabilita la funzionalità SnapCenter MFA per REST API, CLI e GUI

**Interfaccia grafica**

**Passi**

1. Accedi al server SnapCenter come amministratore SnapCenter .
2. Fare clic su **Impostazioni** > **Impostazioni globali** > **Impostazioni di autenticazione a più fattori (MFA)**
3. Selezionare l'interfaccia (GUI/RST API/CLI) per abilitare o disabilitare l'accesso MFA.

**Interfaccia PowerShell**

**Passi**

1. Eseguire i comandi PowerShell o CLI per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

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

   Il parametro path specifica la posizione del file XML dei metadati AD FS MFA.

   Abilita MFA per SnapCenter GUI, REST API, PowerShell e SCCLI configurati con il percorso del file di metadati AD FS specificato.

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando `Get-SmMultiFactorAuthentication` cmdlet.

**Interfaccia SCCLI**

**Passi**

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

**API REST**

1. Eseguire la seguente API post per abilitare MFA per GUI, REST API, PowerShell e SCCLI.

| Parametro | Valore |
|---|---|
| URL richiesto | /api/4.9/settings/autenticazione multifattoriale |
| Metodo HTTP | Inviare |
| Corpo della richiesta | { "IsGuiMFAEnabled": false, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml" } |
| Corpo di risposta | { "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } } |

2. Controllare lo stato e le impostazioni della configurazione MFA utilizzando la seguente API.

| Parametro | Valore |
|---|---|
| URL richiesto | /api/4.9/settings/autenticazione multifattoriale |
| Metodo HTTP | Ottenere |
| Corpo di risposta | { "MFAConfiguration": { "IsGuiMFAEnabled": false, "ADFSConfigFilePath": "C:\\ADFS_metadata\\abc.xml", "SCConfigFilePath": null, "IsRestApiMFAEnabled": true, "IsCliMFAEnabled": false, "ADFSHostName": "win-adfs-sc49.winscedom2.com" } } |

# Installare il server SnapCenter

## Installa SnapCenter Server sull'host Windows

È possibile eseguire il file eseguibile di installazione di SnapCenter Server per installare SnapCenter Server.

Facoltativamente, è possibile eseguire diverse procedure di installazione e configurazione utilizzando i cmdlet di PowerShell. Dovresti utilizzare PowerShell 7.4.2 o versione successiva.

L'installazione silenziosa di SnapCenter Server dalla riga di comando non è supportata.

**Prima di iniziare**

- L'host del server SnapCenter deve essere aggiornato con gli aggiornamenti di Windows e non deve esserci alcun riavvio del sistema in sospeso.
- Dovresti assicurarti che MySQL Server non sia installato sull'host in cui intendi installare SnapCenter Server.
- Avresti dovuto abilitare il debug di Windows Installer.

  Per informazioni sull'abilitazione, consultare il sito Web Microsoft "Registrazione del programma di installazione di Windows" .

  Non installare SnapCenter Server su un host che dispone di Microsoft Exchange Server, Active Directory o Domain Name Server.

**Passi**

1. Scarica il pacchetto di installazione di SnapCenter Server da "Sito di supporto NetApp" .
2. Avviare l'installazione di SnapCenter Server facendo doppio clic sul file .exe scaricato.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati.

   È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

3. Rivedere i valori precompilati richiesti per l'installazione di SnapCenter Server e modificarli se necessario.

   Non è necessario specificare la password per il database del repository di MySQL Server. Durante l'installazione SnapCenter Server la password viene generata automaticamente.

   Il carattere speciale "%" is not supported in the custom path for the repository database. If you include "` %`" nel percorso, l'installazione fallisce.

4. Fare clic su **Installa ora**.

   Se sono stati specificati valori non validi, verranno visualizzati i messaggi di errore appropriati. Dovresti reinserire i valori e poi avviare l'installazione.

   Facendo clic sul pulsante **Annulla**, il passaggio in esecuzione verrà completato e verrà avviata l'operazione di rollback. Il server SnapCenter verrà completamente rimosso dall'host.

   Tuttavia, se si fa clic su **Annulla** quando sono in corso le operazioni "Riavvio del sito di SnapCenter Server" o "In attesa dell'avvio di SnapCenter Server", l'installazione procederà senza annullare l'operazione.

   I file di registro vengono sempre elencati (dal più vecchio) nella cartella %temp% dell'utente amministratore. Se si desidera reindirizzare le posizioni dei registri, avviare l'installazione di SnapCenter Server dal prompt dei comandi eseguendo:`C:\installer_location\installer_name.exe /log"C:\"`

### Funzionalità abilitate sull'host Windows durante l'installazione

Il programma di installazione di SnapCenter Server abilita le funzionalità e i ruoli di Windows sull'host Windows durante l'installazione. Potrebbero essere utili per la risoluzione dei problemi e la manutenzione del sistema host.

| Categoria | Caratteristica |
| --- | --- |
| Server Web | • Servizi di informazione Internet<br>• Servizi del World Wide Web<br>• Funzionalità HTTP comuni<br>◦ Documento predefinito<br>◦ Esplorazione delle directory<br>◦ Errori HTTP<br>◦ Reindirizzamento HTTP<br>◦ Contenuto statico<br>◦ Pubblicazione WebDAV<br>• Salute e diagnostica<br>◦ Registrazione personalizzata<br>◦ Registrazione HTTP<br>◦ Strumenti di registrazione<br>◦ Monitor delle richieste<br>◦ Tracciamento<br>• Caratteristiche delle prestazioni<br>◦ Compressione dei contenuti statici<br>• Sicurezza<br>◦ Sicurezza IP<br>◦ Autenticazione di base<br>◦ Supporto centralizzato per certificati SSL<br>◦ Autenticazione del mapping del certificato client<br>◦ Autenticazione del mapping dei certificati client IIS<br>◦ Restrizioni IP e dominio<br>◦ Filtraggio delle richieste<br>◦ Autorizzazione URL<br>◦ Autenticazione di Windows<br>• Funzionalità di sviluppo delle applicazioni<br>◦ Estensibilità .NET 4.5<br>◦ Inizializzazione dell’applicazione<br>◦ Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>◦ Inclusioni lato server<br>◦ Protocollo WebSocket<br>• Strumenti di gestione<br>Console di gestione IIS |
| | |

| Categoria | Caratteristica |
| --- | --- |
| Script e strumenti di gestione IIS | • Servizio di gestione IIS<br>• Strumenti di gestione web |
| .NET Framework 8.0.12 Funzionalità | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• Attivazione HTTP di Windows Communication Foundation (WCF)45<br>◦ Attivazione TCP<br>◦ Attivazione HTTP<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce per i sistemi legacy che non dispongono di connettività Internet" . |
| Servizio di attivazione dei processi di Windows | Modello di processo |
| API di configurazione | Tutto |

## Installa SnapCenter Server sull'host Linux

È possibile eseguire il file eseguibile di installazione di SnapCenter Server per installare SnapCenter Server.

**Prima di iniziare**

- Se si desidera installare SnapCenter Server utilizzando un utente non root che non dispone di privilegi sufficienti per installare SnapCenter, ottenere il file di checksum sudoers dal sito di supporto NetApp . Dovresti usare un file di checksum appropriato in base alla versione di Linux.
- Se il pacchetto sudo non è disponibile in SUSE Linux, installarlo per evitare errori di autenticazione.
- Per SUSE Linux, configurare il nome host per evitare errori di installazione.
- Controlla lo stato sicuro di Linux eseguendo il comando `sestatus` . Se lo stato *SELinux* è "abilitato" e la *modalità corrente* è "enforcing", procedere come segue:
  - Eseguire il comando: `sudo semanage port -a -t http_port_t -p tcp <WEBAPP_EXTERNAL_PORT_>`

    Il valore predefinito di *WEBAPP_EXTERNAL_PORT* è 8146
  - Se il firewall blocca la porta, eseguire `sudo firewall-cmd --add-port <WEBAPP_EXTERNAL_PORT_>/tcp`

    Il valore predefinito di *WEBAPP_EXTERNAL_PORT* è 8146
  - Esegui i seguenti comandi dalla directory in cui hai i permessi di lettura e scrittura:
    - `sudo ausearch -c 'nginx' --raw | audit2allow -M my-nginx`

Se il comando restituisce "niente da fare", eseguire nuovamente il comando dopo aver installato SnapCenter Server.

- Se il comando crea *my-nginx.pp*, eseguire il comando per rendere attivo il pacchetto di policy: `sudo semodule -i my-nginx.pp`

◦ Il percorso utilizzato per la directory PID di MySQL è */var/opt/mysqld*. Eseguire i seguenti comandi per impostare le autorizzazioni per l'installazione di MySQL.

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

◦ Il percorso utilizzato per la directory dei dati MySQL è */INSTALL_DIR/NetApp/snapcenter/SnapManagerWeb/Repository/MySQL/*. Eseguire i seguenti comandi per impostare le autorizzazioni per la directory dei dati MySQL.

- `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`

**Informazioni su questo compito**

- Quando SnapCenter Server viene installato sull'host Linux, vengono installati servizi di terze parti come MySQL, RabbitMq, Errlang. Non dovresti disinstallarli.
- Il server SnapCenter installato sull'host Linux non supporta:
  - Alta disponibilità
  - Plug-in di Windows
  - Active Directory (supporta solo gli utenti locali, sia root che non root con credenziali)
  - Autenticazione basata su chiave per accedere a SnapCenter
- Durante l'installazione del runtime .NET, se l'installazione non riesce a risolvere le dipendenze della libreria *libicu*, installare *libicu* eseguendo il comando: `yum install -y libicu`
- Se l'installazione di SnapCenter Server non riesce a causa della non disponibilità di *Perl*, installare *Perl* eseguendo il comando: `yum install -y perl`

**Passi**

1. Scarica quanto segue da "Sito di supporto NetApp" nella directory */home*.
   - Pacchetto di installazione di SnapCenter Server - **snapcenter-linux-server-(el8/el9/sles15).bin**
   - File della chiave pubblica - **snapcenter_public_key.pub**
   - File di firma rispettivo - **snapcenter-linux-server-(el8/el9/sles15).bin.sig**
2. Convalidare il file della firma.
   `$openssl dgst -sha256 -verify snapcenter_public_key.pub -signature <path to signature file> <path to bin file>`
3. Per l'installazione da parte di utenti non root, aggiungere il contenuto visudo specificato in **snapcenter_server_checksum_(el8/el9/sles15).txt** disponibile insieme al programma di installazione .bin.

4. Assegnare l'autorizzazione di esecuzione per il programma di installazione .bin.
   `chmod +x snapcenter-linux-server-(el8/el9/sles15).bin`
5. Eseguire una delle azioni per installare SnapCenter Server.

| Se vuoi esibirti… | Fai questo… |
| --- | --- |
| Installazione interattiva | `./snapcenter-linux-server-(el8/el9/sles15).bin`<br><br>Ti verrà chiesto di inserire i seguenti dettagli:<br><br>• Porta esterna dell'applicazione web utilizzata per accedere a SnapCenter Server al di fuori dell'host Linux. Il valore predefinito è 8146.<br>• L'utente di SnapCenter Server che installerà SnapCenter Server.<br>• La directory di installazione in cui verranno installati i pacchetti. |

| Se vuoi esibirti… | Fai questo… |
| --- | --- |
| Installazione non interattiva | `sudo ./snapcenter-linux-server-(el8/el9/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>`<br><br>Esempio: sudo ./snapcenter_linux_server.bin -i silent -DWEBAPP_EXTERNAL_PORT=8146 -DSNAPCENTER_SERVER_USER=root -DUSER_INSTALL_DIR=/opt -DINSTALL_LOG_NAME=InstallerLog.log<br><br>I registri verranno archiviati in */var/opt/snapcenter/logs*.<br><br>Parametri da passare per l'installazione di SnapCenter Server:<br><br>• DWEBAPP_EXTERNAL_PORT: porta esterna dell'applicazione Web utilizzata per accedere a SnapCenter Server al di fuori dell'host Linux. Il valore predefinito è 8146.<br>• DWEBAPP_INTERNAL_PORT: porta interna della Webapp utilizzata per accedere a SnapCenter Server nell'host Linux. Il valore predefinito è 8147.<br>• DSMCORE_PORT: porta SMCore su cui sono in esecuzione i servizi smcore. Il valore predefinito è 8145.<br>• DSCHEDULER_PORT: Porta dello scheduler su cui sono in esecuzione i servizi dello scheduler. Il valore predefinito è 8154.<br>• DSNAPCENTER_SERVER_USER: utente di SnapCenter Server che installerà SnapCenter Server. Per *DSNAPCENTER_SERVER_USER*, l'impostazione predefinita è l'utente che esegue il programma di installazione.<br>• DUSER_INSTALL_DIR: Directory di installazione in cui verranno installati i pacchetti. Per *DUSER_INSTALL_DIR*, la directory di installazione predefinita è */opt*.<br>• DINSTALL_LOG_NAME: Nome del file di registro in cui verranno archiviati i registri di installazione. Questo è un parametro facoltativo e se specificato non verrà visualizzato alcun registro sulla console. Se non si specifica questo parametro, i registri verranno visualizzati sulla console e archiviati anche nel file di registro predefinito. |

**Cosa succederà ora?**

- Se lo stato *SELinux* è "abilitato" e la *modalità corrente* è "enforcing", il servizio **nginx** non riesce ad avviarsi. Dovresti eseguire i seguenti comandi:
  a. Vai alla directory home.
  b. Eseguire il comando: `journalctl -x|grep nginx`.
  c. Se la porta interna della Webapp (8147) non è autorizzata all'accesso, eseguire i seguenti comandi:
     - `ausearch -c 'nginx' --raw | audit2allow -M my-nginx`
     - `semodule -i my-nginx.pp`
  d. Correre `setsebool -P httpd_can_network_connect on`
- DSELINUX: se lo *stato SELinux* è "abilitato", la *modalità corrente* è "enforcing" e sono stati eseguiti i comandi menzionati nella sezione Prima di iniziare, è necessario specificare questo parametro e assegnare il valore 1. Il valore predefinito è 0.
- DUPGRADE: Il valore predefinito è 0. Specificare questo parametro e il suo valore come un numero intero diverso da 0 per aggiornare SnapCenter Server.

**Funzionalità abilitate sull'host Linux durante l'installazione**

SnapCenter Server installa i seguenti pacchetti software che possono aiutare nella risoluzione dei problemi e nella manutenzione del sistema host.

- Rabbitmq
- Erlang

## Registra SnapCenter

Se non hai familiarità con i prodotti NetApp e non hai un account NetApp esistente, dovresti registrare SnapCenter per abilitare il supporto.

**Passi**

1. Dopo aver installato SnapCenter, vai su **Aiuto > Informazioni**.
2. Nella finestra di dialogo *Informazioni su SnapCenter*, prendere nota dell'istanza SnapCenter , un numero di 20 cifre che inizia con 971.
3. Clic https://register.netapp.com .
4. Fare clic su **Non sono un cliente NetApp registrato**.
5. Specifica i tuoi dati per registrarti.
6. Lasciare vuoto il campo NetApp Reference SN.
7. Selezionare * SnapCenter* dal menu a discesa Linea di prodotti.
8. Selezionare il fornitore di fatturazione.
9. Immettere l'ID istanza SnapCenter di 20 cifre.
10. Fare clic su **Invia**.

## Accedi a SnapCenter utilizzando l'autorizzazione RBAC

SnapCenter supporta il controllo degli accessi basato sui ruoli (RBAC). L'amministratore SnapCenter assegna ruoli e risorse tramite SnapCenter RBAC a un utente nel gruppo di lavoro o in Active Directory oppure a gruppi in Active Directory. L'utente RBAC può ora accedere a SnapCenter con i ruoli assegnati.

**Prima di iniziare**

- Dovresti abilitare il servizio Attivazione processo Windows (WAS) in Windows Server Manager.
- Se si desidera utilizzare Internet Explorer come browser per accedere a SnapCenter Server, è necessario assicurarsi che la modalità protetta in Internet Explorer sia disattivata.
- Se SnapCenter Server è installato su un host Linux, è necessario effettuare l'accesso utilizzando l'account utente utilizzato per installare SnapCenter Server.

**Informazioni su questo compito**

Durante l'installazione, la procedura guidata di installazione di SnapCenter Server crea un collegamento e lo posiziona sul desktop e nel menu Start dell'host in cui è installato SnapCenter . Inoltre, al termine dell'installazione, la procedura guidata di installazione visualizza l'URL SnapCenter in base alle informazioni fornite durante l'installazione, che è possibile copiare se si desidera accedere da un sistema remoto.

Se hai più schede aperte nel tuo browser web, chiudendo solo la scheda del browser SnapCenter non verrai disconnesso da SnapCenter. Per terminare la connessione con SnapCenter, è necessario uscire da SnapCenter cliccando sul pulsante **Esci** oppure chiudendo l'intero browser web.

**Migliore pratica:** per motivi di sicurezza, si consiglia di non abilitare il browser per salvare la password SnapCenter .

L'URL GUI predefinito è una connessione sicura alla porta predefinita 8146 sul server su cui è installato SnapCenter Server (*https://server:8146*). Se durante l'installazione SnapCenter è stata specificata una porta server diversa, verrà utilizzata quella porta.

Per la distribuzione ad alta disponibilità (HA), è necessario accedere a SnapCenter utilizzando l'IP del cluster virtuale *https://Virtual_Cluster_IP_or_FQDN:8146*. Se non vedi l'interfaccia utente SnapCenter quando accedi a *https://Virtual_Cluster_IP_or_FQDN:8146* in Internet Explorer (IE), devi aggiungere l'indirizzo IP o FQDN del Virtual Cluster come sito attendibile in IE su ciascun host del plug-in oppure devi disattivare IE Enhanced Security su ciascun host del plug-in. Per ulteriori informazioni, vedere "Impossibile accedere all'indirizzo IP del cluster dalla rete esterna" .

Oltre a utilizzare l'interfaccia utente grafica SnapCenter , è possibile utilizzare i cmdlet di PowerShell per creare script per eseguire operazioni di configurazione, backup e ripristino. Alcuni cmdlet potrebbero essere cambiati con ogni versione SnapCenter . IL "Guida di riferimento ai cmdlet del software SnapCenter" ha i dettagli.

Se accedi a SnapCenter per la prima volta, devi effettuare l'accesso utilizzando le credenziali fornite durante il processo di installazione.

**Passi**

1. Avvia SnapCenter dal collegamento presente sul desktop dell'host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore SnapCenter .
2. Inserisci le credenziali utente.

| Per specificare quanto segue… | Utilizza uno di questi formati… |
| --- | --- |
| Amministratore di dominio | • NetBIOS\Nome utente<br>• Suffisso UserName@UPN<br>Ad esempio, username@netapp.com<br>• Nome FQDN del dominio\Nome utente |
| amministratore locale | Nome utente |

3. Se ti è stato assegnato più di un ruolo, dalla casella Ruolo seleziona il ruolo che desideri utilizzare per questa sessione di accesso.

   Dopo aver effettuato l'accesso, l'utente corrente e il ruolo associato vengono visualizzati in alto a destra in SnapCenter .

**Risultato**

Viene visualizzata la pagina Dashboard.

Se la registrazione fallisce e viene visualizzato l'errore che il sito non è raggiungibile, è necessario mappare il certificato SSL su SnapCenter. "Saperne di più"

**Dopo aver finito**

Dopo aver effettuato l'accesso a SnapCenter Server come utente RBAC per la prima volta, aggiornare l'elenco delle risorse.

Se si dispone di domini Active Directory non attendibili che si desidera vengano supportati SnapCenter , è necessario registrare tali domini con SnapCenter prima di configurare i ruoli per gli utenti sui domini non attendibili. "Saperne di più" .

Se si desidera aggiungere l'host del plug-in in SnapCenter in esecuzione su un host Linux, è necessario ottenere il file di checksum dal percorso: */opt/ NetApp/snapcenter/SnapManagerWeb/Repository*.

A partire dalla versione 6.0, sul desktop viene creato un collegamento per SnapCenter PowerShell. È possibile accedere direttamente ai cmdlet di SnapCenter PowerShell utilizzando il collegamento.

**Accedi a SnapCenter utilizzando l'autenticazione a più fattori (MFA)**

SnapCenter Server supporta l'autenticazione MFA per gli account di dominio, che fanno parte di Active Directory.

**Prima di iniziare**

Avresti dovuto abilitare MFA. Per informazioni su come abilitare MFA, vedere"Abilita l'autenticazione a più fattori"

**Informazioni su questo compito**

- È supportato solo FQDN
- Gli utenti di gruppi di lavoro e di domini multipli non possono accedere tramite MFA

**Passi**

1. Avvia SnapCenter dal collegamento presente sul desktop dell'host locale, dall'URL fornito al termine dell'installazione o dall'URL fornito dall'amministratore SnapCenter .
2. Nella pagina di accesso di AD FS, immettere nome utente e password.

   Quando nella pagina AD FS viene visualizzato il messaggio di errore "nome utente o password non validi", è necessario verificare quanto segue:

   - Se il nome utente o la password sono validi

     L'account utente deve esistere in Active Directory (AD)

   - Se hai superato il numero massimo di tentativi consentiti impostato in AD
   - Se AD e AD FS sono attivi e funzionanti

**Modifica il timeout della sessione GUI predefinita di SnapCenter**

È possibile modificare il periodo di timeout della sessione dell'interfaccia utente grafica SnapCenter per renderlo inferiore o superiore al periodo di timeout predefinito di 20 minuti.

Come misura di sicurezza, dopo un periodo predefinito di 15 minuti di inattività, SnapCenter avvisa che la sessione GUI verrà disconnessa entro 5 minuti. Per impostazione predefinita, SnapCenter disconnette l'utente dalla sessione GUI dopo 20 minuti di inattività, dopodiché sarà necessario effettuare nuovamente l'accesso.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni** > **Impostazioni globali**.
2. Nella pagina Impostazioni globali, fare clic su **Impostazioni di configurazione**.
3. Nel campo Timeout sessione, immettere il nuovo timeout della sessione in minuti, quindi fare clic su **Salva**.

**Proteggi il server web SnapCenter disabilitando SSL 3.0**

Per motivi di sicurezza, dovresti disattivare il protocollo Secure Socket Layer (SSL) 3.0 in Microsoft IIS se è abilitato sul tuo server web SnapCenter .

Il protocollo SSL 3.0 presenta delle falle che un aggressore può sfruttare per causare errori di connessione o per eseguire attacchi man-in-the-middle e osservare il traffico di crittografia tra il tuo sito web e i suoi visitatori.

**Passi**

1. Per avviare l'Editor del Registro di sistema sull'host del server web SnapCenter , fare clic su **Start** > **Esegui**, quindi immettere regedit.
2. Nell'editor del Registro di sistema, vai a HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\.
   - Se la chiave del server esiste già:
     i. Selezionare il valore DWORD abilitato, quindi fare clic su **Modifica** > **Modifica**.
     ii. Modificare il valore su 0, quindi fare clic su **OK**.
   - Se la chiave del server non esiste:

i. Fare clic su **Modifica** > **Nuovo** > **Chiave**, quindi assegnare alla chiave il nome Server.

ii. Dopo aver selezionato la nuova chiave del server, fare clic su **Modifica** > **Nuovo** > **DWORD**.

iii. Assegnare al nuovo DWORD il nome Enabled, quindi immettere 0 come valore.

3. Chiudere l'editor del Registro di sistema.

# Configurare il server SnapCenter

## Aggiungere e predisporre il sistema di archiviazione

### Aggiungere sistemi di archiviazione

È necessario configurare il sistema di archiviazione che consente a SnapCenter di accedere all'archiviazione ONTAP , ai sistemi ASA r2 o Amazon FSx for NetApp ONTAP per eseguire operazioni di protezione dei dati e provisioning.

È possibile aggiungere una SVM autonoma oppure un cluster composto da più SVM. Se si utilizza Amazon FSx for NetApp ONTAP, è possibile aggiungere un LIF di amministrazione FSx composto da più SVM utilizzando l'account fsxadmin oppure aggiungere un SVM FSx in SnapCenter.

**Prima di iniziare**

- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Informazioni su questo compito**

- Quando si configurano i sistemi di archiviazione, è anche possibile abilitare le funzionalità Event Management System (EMS) e AutoSupport . Lo strumento AutoSupport raccoglie dati sullo stato del sistema e li invia automaticamente al supporto tecnico NetApp , consentendogli di risolvere i problemi del sistema.

  Se si abilitano queste funzionalità, SnapCenter invia informazioni AutoSupport al sistema di archiviazione e messaggi EMS al syslog del sistema di archiviazione quando una risorsa è protetta, un'operazione di ripristino o clonazione viene completata correttamente o un'operazione non riesce.

- Se si prevede di replicare gli snapshot su una destinazione SnapMirror o SnapVault , è necessario configurare le connessioni del sistema di archiviazione per l'SVM o il cluster di destinazione, nonché per l'SVM o il cluster di origine.

Se si modifica la password del sistema di archiviazione, i processi pianificati, i backup su richiesta e le operazioni di ripristino potrebbero non riuscire. Dopo aver modificato la password del sistema di archiviazione, è possibile aggiornarla facendo clic su **Modifica** nella scheda Archiviazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, fare clic su **Nuovo**.
3. Nella pagina Aggiungi sistema di archiviazione, fornire le seguenti informazioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Sistema di archiviazione | Immettere il nome del sistema di archiviazione o l'indirizzo IP.<br>I nomi dei sistemi di archiviazione, escluso il nome di dominio, devono contenere al massimo 15 caratteri e devono essere risolvibili. Per creare connessioni al sistema di archiviazione con nomi composti da più di 15 caratteri, è possibile utilizzare il cmdlet Add-SmStorageConnectionPowerShell.<br>Per i sistemi di storage con configurazione MetroCluster (MCC), si consiglia di registrare sia i cluster locali che quelli peer per operazioni non disruptive.<br>SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportato da SnapCenter deve avere un nome univoco.<br>Dopo aver aggiunto la connessione di archiviazione a SnapCenter, non dovresti rinominare l'SVM o il Cluster utilizzando ONTAP.<br>Se SVM viene aggiunto con un nome breve o FQDN, deve essere risolvibile sia da SnapCenter che dall'host del plug-in. |
| Nome utente/Password | Immettere le credenziali dell'utente di archiviazione che dispone dei privilegi richiesti per accedere al sistema di archiviazione. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Impostazioni del sistema di gestione degli eventi (EMS) e AutoSupport | Se si desidera inviare messaggi EMS al syslog del sistema di archiviazione o se si desidera che i messaggi AutoSupport vengano inviati al sistema di archiviazione per la protezione applicata, le operazioni di ripristino completate o le operazioni non riuscite, selezionare la casella di controllo appropriata.<br><br>Quando si seleziona la casella di controllo **Invia notifica AutoSupport per operazioni non riuscite al sistema di archiviazione**, viene selezionata anche la casella di controllo **Registra eventi del server SnapCenter su syslog** perché è necessaria la messaggistica EMS per abilitare le notifiche AutoSupport . |

4. Fare clic su **Altre opzioni** se si desidera modificare i valori predefiniti assegnati a piattaforma, protocollo, porta e timeout.

   a. In Piattaforma, seleziona una delle opzioni dall'elenco a discesa.

      Se l'SVM è il sistema di archiviazione secondario in una relazione di backup, selezionare la casella di controllo **Secondario**. Quando si seleziona l'opzione **Secondaria**, SnapCenter non esegue immediatamente un controllo della licenza.

   Se hai aggiunto SVM in SnapCenter , l'utente dovrà selezionare manualmente il tipo di piattaforma dal menu a discesa.

   a. In Protocollo, seleziona il protocollo configurato durante la configurazione di SVM o Cluster, in genere HTTPS.
   b. Immettere la porta accettata dal sistema di archiviazione.

      In genere funziona la porta predefinita 443.

   c. Inserire il tempo in secondi che deve trascorrere prima che i tentativi di comunicazione vengano interrotti.

      Il valore predefinito è 60 secondi.

   d. Se l'SVM dispone di più interfacce di gestione, selezionare la casella di controllo **IP preferito**, quindi immettere l'indirizzo IP preferito per le connessioni SVM.
   e. Fare clic su **Salva**.
5. Fare clic su **Invia**.

**Risultato**

Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, eseguire una delle seguenti azioni:

- Selezionare * ONTAP SVM* se si desidera visualizzare tutti gli SVM aggiunti.

  Se hai aggiunto SVM FSx, questi vengono elencati qui.

- Selezionare *Cluster ONTAP * se si desidera visualizzare tutti i cluster aggiunti.

  Se hai aggiunto cluster FSx utilizzando fsxadmin, i cluster FSx sono elencati qui.

  Facendo clic sul nome del cluster, tutte le SVM che ne fanno parte vengono visualizzate nella sezione Macchine virtuali di archiviazione.

  Se si aggiunge un nuovo SVM al cluster ONTAP tramite l'interfaccia utente grafica ONTAP , fare clic su **Riscopri** per visualizzare il nuovo SVM aggiunto.

**Dopo aver finito**

Un amministratore del cluster deve abilitare AutoSupport su ciascun nodo del sistema di archiviazione per inviare notifiche e-mail da tutti i sistemi di archiviazione a cui SnapCenter ha accesso, eseguendo il seguente comando dalla riga di comando del sistema di archiviazione:

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

L'amministratore della macchina virtuale di archiviazione (SVM) non ha accesso ad AutoSupport.

**Connessioni di archiviazione e credenziali**

Prima di eseguire operazioni di protezione dei dati, è necessario configurare le connessioni di archiviazione e aggiungere le credenziali che verranno utilizzate da SnapCenter Server e dai plug-in SnapCenter .

**Connessioni di archiviazione**

Le connessioni di archiviazione consentono al server SnapCenter e ai plug-in SnapCenter di accedere all'archiviazione ONTAP . L'impostazione di queste connessioni comporta anche la configurazione delle funzionalità AutoSupport ed Event Management System (EMS).

**Credenziali**

- Amministratore di dominio o qualsiasi membro del gruppo di amministratori

  Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:

  - *NetBIOS\NomeUtente*
  - *FQDN dominio\Nome utente*
  - *NomeUtente@upn*
- Amministratore locale (solo per gruppi di lavoro)

  Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host.

  Il formato valido per il campo Nome utente è: *UserName*

- Credenziali per singoli gruppi di risorse

  Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

## Fornire spazio di archiviazione su host Windows

### Creare e gestire igroup

È possibile creare gruppi di iniziatori (igroup) per specificare quali host possono accedere a una determinata LUN sul sistema di archiviazione. È possibile utilizzare SnapCenter per creare, rinominare, modificare o eliminare un igroup su un host Windows.

#### Crea un igroup

È possibile utilizzare SnapCenter per creare un igroup su un host Windows. L'igroup sarà disponibile nella procedura guidata Crea disco o Connetti disco quando si esegue il mapping dell'igroup a un LUN.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic su **Nuovo**.
4. Nella finestra di dialogo Crea igroup, definire l'igroup:

| In questo campo… | Fai questo… |
|---|---|
| Sistema di archiviazione | Selezionare l'SVM per la LUN che si desidera mappare all'igroup. |
| Ospite | Selezionare l'host su cui si desidera creare l'igroup. |
| Nome del gruppo | Inserisci il nome dell'igroup. |
| Iniziatori | Selezionare l'iniziatore. |
| Tipo | Selezionare il tipo di iniziatore: iSCSI, FCP o misto (FCP e iSCSI). |

5. Quando sei soddisfatto dei tuoi dati, clicca su **OK**.

   SnapCenter crea l'igroup sul sistema di archiviazione.

#### Rinominare un igroup

È possibile utilizzare SnapCenter per rinominare un igroup esistente.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera rinominare.
4. Nell'elenco degli igroup per l'SVM, seleziona l'igroup che vuoi rinominare e fai clic su **Rinomina**.
5. Nella finestra di dialogo Rinomina igroup, immettere il nuovo nome per l'igroup e fare clic su **Rinomina**.

#### Modificare un igroup

È possibile utilizzare SnapCenter per aggiungere iniziatori igroup a un igroup esistente. Durante la creazione di un igroup è possibile aggiungere un solo host. Se si desidera creare un igroup per un cluster, è possibile modificarlo per aggiungere altri nodi a tale igroup.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera modificare.
4. Nell'elenco degli igroup, seleziona un igroup e fai clic su **Aggiungi iniziatore all'igroup**.
5. Seleziona un host.
6. Selezionare gli iniziatori e fare clic su **OK**.

#### Elimina un igroup

È possibile utilizzare SnapCenter per eliminare un igroup quando non ne hai più bisogno.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Igroup**.
3. Nella pagina Gruppi iniziatori, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un elenco a discesa delle SVM disponibili, quindi selezionare la SVM per l'igroup che si desidera eliminare.
4. Nell'elenco degli igroup per l'SVM, seleziona l'igroup che desideri eliminare e fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina igroup, fare clic su **OK**.

   SnapCenter elimina l'igroup.

##### Creare e gestire dischi

L'host Windows vede i LUN sul sistema di archiviazione come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare una LUN connessa tramite FC o tramite iSCSI.

- SnapCenter supporta solo dischi di base. I dischi dinamici non sono supportati.
- Per GPT è consentita solo una partizione dati e per MBR è consentita solo una partizione primaria con un volume formattato con NTFS o CSVFS e un percorso di montaggio.

- Stili di partizione supportati: GPT, MBR; in una VM VMware UEFI, sono supportati solo i dischi iSCSI

SnapCenter non supporta la ridenominazione di un disco. Se un disco gestito da SnapCenter viene rinominato, le operazioni SnapCenter non riusciranno.

### Visualizza i dischi su un host

Puoi visualizzare i dischi su ogni host Windows che gestisci con SnapCenter.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.

   I dischi sono elencati.

### Visualizza i dischi in cluster

È possibile visualizzare i dischi in cluster sul cluster gestito con SnapCenter. I dischi in cluster vengono visualizzati solo quando si seleziona il cluster dal menu a discesa Host.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare il cluster dall'elenco a discesa **Host**.

   I dischi sono elencati.

### Stabilire una sessione iSCSI

Se si utilizza iSCSI per connettersi a un LUN, è necessario stabilire una sessione iSCSI prima di creare il LUN per abilitare la comunicazione.

**Prima di iniziare**

- È necessario aver definito il nodo del sistema di archiviazione come destinazione iSCSI.
- È necessario aver avviato il servizio iSCSI sul sistema di archiviazione. "Saperne di più"

**Informazioni su questo compito**

È possibile stabilire una sessione iSCSI solo tra le stesse versioni IP, da IPv6 a IPv6 o da IPv4 a IPv4.

È possibile utilizzare un indirizzo IPv6 link-local per la gestione delle sessioni iSCSI e per la comunicazione tra un host e una destinazione solo quando entrambi si trovano nella stessa subnet.

Se si modifica il nome di un iniziatore iSCSI, l'accesso alle destinazioni iSCSI ne risente. Dopo aver modificato il nome, potrebbe essere necessario riconfigurare i target a cui accede l'iniziatore in modo che possano riconoscere il nuovo nome. Dopo aver modificato il nome di un iniziatore iSCSI, è necessario assicurarsi di riavviare l'host.

Se l'host dispone di più di un'interfaccia iSCSI, una volta stabilita una sessione iSCSI su SnapCenter utilizzando un indirizzo IP sulla prima interfaccia, non è possibile stabilire una sessione iSCSI da un'altra interfaccia con un indirizzo IP diverso.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Sessione iSCSI**.
3. Dall'elenco a discesa **Macchina virtuale di archiviazione**, selezionare la macchina virtuale di archiviazione (SVM) per la destinazione iSCSI.
4. Dall'elenco a discesa **Host**, seleziona l'host per la sessione.
5. Fare clic su **Stabilisci sessione**.

   Viene visualizzata la procedura guidata Crea sessione.

6. Nella procedura guidata Stabilisci sessione, identifica la destinazione:

| In questo campo… | Entra… |
|---|---|
| Nome del nodo di destinazione | Il nome del nodo della destinazione iSCSI<br><br>Se esiste già un nome di nodo di destinazione, il nome viene visualizzato in formato di sola lettura. |
| Indirizzo del portale di destinazione | L'indirizzo IP del portale di rete di destinazione |
| Portale di destinazione | La porta TCP del portale di rete di destinazione |
| Indirizzo del portale dell'iniziatore | L'indirizzo IP del portale di rete dell'iniziatore |

7. Quando sei soddisfatto dei tuoi dati, clicca su **Connetti**.

   SnapCenter stabilisce la sessione iSCSI.

8. Ripetere questa procedura per stabilire una sessione per ciascun target.

### Creare LUN o dischi connessi tramite FC o tramite iSCSI

L'host Windows vede i LUN sul sistema di archiviazione come dischi virtuali. È possibile utilizzare SnapCenter per creare e configurare una LUN connessa tramite FC o tramite iSCSI.

Se si desidera creare e formattare dischi al di fuori di SnapCenter, sono supportati solo i file system NTFS e CSVFS.

**Prima di iniziare**

- È necessario aver creato un volume per la LUN sul sistema di archiviazione.

  Il volume deve contenere solo LUN e solo LUN creati con SnapCenter.

Non è possibile creare un LUN su un volume clone creato da SnapCenter, a meno che il clone non sia già stato suddiviso.

- È necessario aver avviato il servizio FC o iSCSI sul sistema di archiviazione.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di archiviazione.
- Il pacchetto di plug-in SnapCenter per Windows deve essere installato solo sull'host su cui si sta creando il disco.

**Informazioni su questo compito**

- Non è possibile connettere una LUN a più di un host, a meno che la LUN non sia condivisa dagli host in un cluster di failover di Windows Server.
- Se un LUN è condiviso da host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario creare il disco sull'host proprietario del gruppo di cluster.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.
4. Fare clic su **Nuovo**.

   Si apre la procedura guidata Crea disco.

5. Nella pagina Nome LUN, identificare la LUN:

| In questo campo… | Fai questo… |
|---|---|
| Sistema di archiviazione | Selezionare l'SVM per la LUN. |
| Percorso LUN | Fare clic su **Sfoglia** per selezionare il percorso completo della cartella contenente il LUN. |
| Nome LUN | Immettere il nome del LUN. |
| Dimensione del cluster | Selezionare la dimensione di allocazione del blocco LUN per il cluster.<br><br>La dimensione del cluster dipende dal sistema operativo e dalle applicazioni. |
| Etichetta LUN | Facoltativamente, immettere un testo descrittivo per il LUN. |

6. Nella pagina Tipo di disco, seleziona il tipo di disco:

| Selezionare… | Se… |
| --- | --- |
| Disco dedicato | L'accesso alla LUN è consentito solo a un host.<br><br>Ignora il campo **Gruppo di risorse**. |
| Disco condiviso | Il LUN è condiviso dagli host in un cluster di failover di Windows Server.<br><br>Immettere il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. È necessario creare il disco su un solo host nel cluster di failover. |
| Volume condiviso del cluster (CSV) | Il LUN è condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV.<br><br>Immettere il nome del gruppo di risorse del cluster nel campo **Gruppo di risorse**. Assicurarsi che l'host su cui si sta creando il disco sia il proprietario del gruppo cluster. |

7. Nella pagina Proprietà unità, specificare le proprietà dell'unità:

| Proprietà | Descrizione |
| --- | --- |
| Assegnazione automatica del punto di montaggio | SnapCenter assegna automaticamente un punto di montaggio del volume in base all'unità di sistema.<br><br>Ad esempio, se l'unità di sistema è C:, l'assegnazione automatica crea un punto di montaggio del volume nell'unità C: (C:\scmnpt\). L'assegnazione automatica non è supportata per i dischi condivisi. |
| Assegna lettera di unità | Montare il disco sull'unità selezionata nell'elenco a discesa adiacente. |
| Utilizza il punto di montaggio del volume | Montare il disco sul percorso dell'unità specificato nel campo adiacente.<br><br>La radice del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco. |
| Non assegnare la lettera dell'unità o il punto di montaggio del volume | Selezionare questa opzione se si preferisce montare manualmente il disco in Windows. |
| dimensione LUN | Specificare la dimensione LUN; minimo 150 MB.<br><br>Selezionare MB, GB o TB nell'elenco a discesa adiacente. |

| Proprietà | Descrizione |
| --- | --- |
| Utilizzare il thin provisioning per il volume che ospita questa LUN | Fornire una disposizione sottile della LUN.<br><br>Il thin provisioning alloca solo lo spazio di archiviazione necessario in un dato momento, consentendo alla LUN di crescere in modo efficiente fino alla massima capacità disponibile.<br><br>Assicurati che ci sia abbastanza spazio disponibile sul volume per contenere tutto lo spazio di archiviazione LUN che ritieni necessario. |
| Scegli il tipo di partizione | Selezionare la partizione GPT per una tabella delle partizioni GUID o la partizione MBR per un Master Boot Record.<br><br>Le partizioni MBR potrebbero causare problemi di disallineamento nei cluster di failover di Windows Server.<br><br>I dischi di partizione UEFI (Unified Extensible Firmware Interface) non sono supportati. |

8. Nella pagina Mappa LUN, selezionare l'iniziatore iSCSI o FC sull'host:

| In questo campo… | Fai questo… |
| --- | --- |
| Ospite | Fare doppio clic sul nome del gruppo cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore.<br><br>Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server. |
| Scegli l'iniziatore host | Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host.<br><br>È possibile selezionare più iniziatori FC se si utilizza FC con I/O multipath (MPIO). |

9. Nella pagina Tipo di gruppo, specificare se si desidera mappare un igroup esistente al LUN o crearne uno nuovo:

| Selezionare… | Se… |
| --- | --- |
| Crea un nuovo igroup per gli iniziatori selezionati | Si desidera creare un nuovo igroup per gli iniziatori selezionati. |

| Selezionare… | Se… |
| --- | --- |
| Scegli un igroup esistente o specifica un nuovo igroup per gli iniziatori selezionati | Si desidera specificare un igroup esistente per gli iniziatori selezionati oppure creare un nuovo igroup con il nome specificato.<br><br>Digitare il nome dell'igroup nel campo **nome igroup**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo. |

10. Nella pagina Riepilogo, rivedi le tue selezioni e poi fai clic su **Fine**.

    SnapCenter crea il LUN e lo collega all'unità o al percorso dell'unità specificato sull'host.

### Ridimensionare un disco

È possibile aumentare o diminuire le dimensioni di un disco in base alle esigenze del sistema di archiviazione.

#### Informazioni su questo compito

- Per le LUN con provisioning sottile, la dimensione della geometria LUN ONTAP è indicata come dimensione massima.
- Per le LUN con provisioning spesso, la dimensione espandibile (dimensione disponibile nel volume) viene visualizzata come dimensione massima.
- Le LUN con partizioni di tipo MBR hanno un limite di dimensione di 2 TB.
- Le LUN con partizioni di tipo GPT hanno un limite di dimensione del sistema di archiviazione di 16 TB.
- È consigliabile creare uno snapshot prima di ridimensionare una LUN.
- Se è necessario ripristinare una LUN da uno Snapshot creato prima del ridimensionamento della LUN, SnapCenter ridimensiona automaticamente la LUN in base alle dimensioni dello Snapshot.

  Dopo l'operazione di ripristino, i dati aggiunti al LUN dopo il ridimensionamento devono essere ripristinati da uno snapshot creato dopo il ridimensionamento.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa Host.

   I dischi sono elencati.

4. Seleziona il disco che vuoi ridimensionare e poi clicca su **Ridimensiona**.
5. Nella finestra di dialogo Ridimensiona disco, utilizzare lo strumento cursore per specificare la nuova dimensione del disco oppure immettere la nuova dimensione nel campo Dimensione.

   Se si immette la dimensione manualmente, è necessario fare clic all'esterno del campo Dimensione prima che il pulsante Riduci o Espandi venga abilitato correttamente. Inoltre, è necessario fare clic su MB, GB o TB per specificare l'unità di misura.

6. Quando sei soddisfatto dei dati inseriti, clicca su **Riduci** o **Espandi**, a seconda dei casi.

   SnapCenter ridimensiona il disco.

### Collegare un disco

È possibile utilizzare la procedura guidata Connetti disco per connettere un LUN esistente a un host o per riconnettere un LUN che è stato disconnesso.

**Prima di iniziare**

- È necessario aver avviato il servizio FC o iSCSI sul sistema di archiviazione.
- Se si utilizza iSCSI, è necessario aver stabilito una sessione iSCSI con il sistema di archiviazione.
- Non è possibile connettere una LUN a più di un host, a meno che la LUN non sia condivisa dagli host in un cluster di failover di Windows Server.
- Se il LUN è condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV (Cluster Shared Volumes), è necessario connettere il disco all'host proprietario del gruppo di cluster.
- Il plug-in per Windows deve essere installato solo sull'host a cui si collega il disco.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.
4. Fare clic su **Connetti**.

   Si apre la procedura guidata Connetti disco.

5. Nella pagina Nome LUN, identifica la LUN a cui connettersi:

| In questo campo… | Fai questo… |
|---|---|
| Sistema di archiviazione | Selezionare l'SVM per la LUN. |
| Percorso LUN | Fare clic su **Sfoglia** per selezionare il percorso completo del volume contenente il LUN. |
| Nome LUN | Immettere il nome del LUN. |
| Dimensione del cluster | Selezionare la dimensione di allocazione del blocco LUN per il cluster.<br><br>La dimensione del cluster dipende dal sistema operativo e dalle applicazioni. |
| Etichetta LUN | Facoltativamente, immettere un testo descrittivo per il LUN. |

6. Nella pagina Tipo di disco, seleziona il tipo di disco:

| Selezionare… | Se… |
| --- | --- |
| Disco dedicato | L'accesso alla LUN è consentito solo a un host. |
| Disco condiviso | Il LUN è condiviso dagli host in un cluster di failover di Windows Server.<br><br>È sufficiente collegare il disco a un solo host nel cluster di failover. |
| Volume condiviso del cluster (CSV) | Il LUN è condiviso dagli host in un cluster di failover di Windows Server che utilizza CSV.<br><br>Assicurarsi che l'host su cui ci si connette al disco sia il proprietario del gruppo cluster. |

7. Nella pagina Proprietà unità, specificare le proprietà dell'unità:

| Proprietà | Descrizione |
| --- | --- |
| Assegnazione automatica | Consenti a SnapCenter di assegnare automaticamente un punto di montaggio del volume in base all'unità di sistema.<br><br>Ad esempio, se l'unità di sistema è C:, la proprietà di assegnazione automatica crea un punto di montaggio del volume nell'unità C: (C:\scmnpt\). La proprietà di assegnazione automatica non è supportata per i dischi condivisi. |
| Assegna lettera di unità | Montare il disco sull'unità selezionata nell'elenco a discesa adiacente. |
| Utilizza il punto di montaggio del volume | Montare il disco sul percorso dell'unità specificato nel campo adiacente.<br><br>La radice del punto di montaggio del volume deve essere di proprietà dell'host su cui si sta creando il disco. |
| Non assegnare la lettera dell'unità o il punto di montaggio del volume | Selezionare questa opzione se si preferisce montare manualmente il disco in Windows. |

8. Nella pagina Mappa LUN, selezionare l'iniziatore iSCSI o FC sull'host:

| In questo campo… | Fai questo… |
| --- | --- |
| Ospite | Fare doppio clic sul nome del gruppo cluster per visualizzare un elenco a discesa che mostra gli host che appartengono al cluster, quindi selezionare l'host per l'iniziatore.<br><br>Questo campo viene visualizzato solo se il LUN è condiviso dagli host in un cluster di failover di Windows Server. |
| Scegli l'iniziatore host | Selezionare **Fibre Channel** o **iSCSI**, quindi selezionare l'iniziatore sull'host.<br><br>Se si utilizza FC con MPIO, è possibile selezionare più iniziatori FC. |

9. Nella pagina Tipo di gruppo, specificare se si desidera mappare un igroup esistente al LUN o creare un nuovo igroup:

| Selezionare… | Se… |
| --- | --- |
| Crea un nuovo igroup per gli iniziatori selezionati | Si desidera creare un nuovo igroup per gli iniziatori selezionati. |
| Scegli un igroup esistente o specifica un nuovo igroup per gli iniziatori selezionati | Si desidera specificare un igroup esistente per gli iniziatori selezionati oppure creare un nuovo igroup con il nome specificato.<br><br>Digitare il nome dell'igroup nel campo **nome igroup**. Digitare le prime lettere del nome igroup esistente per completare automaticamente il campo. |

10. Nella pagina Riepilogo, rivedi le tue selezioni e fai clic su **Fine**.

    SnapCenter collega la LUN all'unità o al percorso dell'unità specificato sull'host.

### Disconnettere un disco

È possibile disconnettere una LUN da un host senza alterarne il contenuto, con un'eccezione: se si disconnette un clone prima che sia stato suddiviso, si perde il contenuto del clone.

#### Prima di iniziare

- Assicurarsi che la LUN non sia utilizzata da alcuna applicazione.
- Assicurarsi che la LUN non sia monitorata tramite software di monitoraggio.
- Se la LUN è condivisa, assicurarsi di rimuovere le dipendenze delle risorse del cluster dalla LUN e verificare che tutti i nodi del cluster siano accesi, funzionino correttamente e siano disponibili per SnapCenter.

#### Informazioni su questo compito

Se si disconnette un LUN in un volume FlexClone creato SnapCenter e non sono connessi altri LUN sul volume, SnapCenter elimina il volume. Prima di disconnettere il LUN, SnapCenter visualizza un messaggio che avvisa che il volume FlexClone potrebbe essere eliminato.

Per evitare l'eliminazione automatica del volume FlexClone , è necessario rinominare il volume prima di disconnettere l'ultimo LUN. Quando si rinomina il volume, assicurarsi di modificare più caratteri oltre all'ultimo carattere del nome.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.

   I dischi sono elencati.

4. Selezionare il disco che si desidera disconnettere, quindi fare clic su **Disconnetti**.
5. Nella finestra di dialogo Disconnetti disco, fare clic su **OK**.

   SnapCenter disconnette il disco.

### Elimina un disco

È possibile eliminare un disco quando non ne hai più bisogno. Dopo aver eliminato un disco, non è più possibile ripristinarlo.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Dischi**.
3. Selezionare l'host dall'elenco a discesa **Host**.

   I dischi sono elencati.

4. Seleziona il disco che vuoi eliminare, quindi fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina disco, fare clic su **OK**.

   SnapCenter elimina il disco.

#### Creare e gestire condivisioni SMB

Per configurare una condivisione SMB3 su una macchina virtuale di archiviazione (SVM), è possibile utilizzare l'interfaccia utente di SnapCenter o i cmdlet di PowerShell.

**Procedura consigliata:** si consiglia di utilizzare i cmdlet perché consentono di sfruttare i modelli forniti con SnapCenter per automatizzare la configurazione delle condivisioni.

I modelli racchiudono le best practice per la configurazione del volume e della condivisione. È possibile trovare i modelli nella cartella Modelli nella cartella di installazione del pacchetto plug-in SnapCenter per Windows.

Se ti senti a tuo agio, puoi creare i tuoi modelli seguendo quelli forniti. Prima di creare un modello personalizzato, è opportuno rivedere i parametri nella documentazione del cmdlet.

### Crea una condivisione SMB

È possibile utilizzare la pagina Condivisioni di SnapCenter per creare una condivisione SMB3 su una macchina virtuale di archiviazione (SVM).

Non è possibile utilizzare SnapCenter per eseguire il backup dei database sulle condivisioni SMB. Il supporto SMB è limitato al solo provisioning.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Condivisioni**.
3. Selezionare la SVM dall'elenco a discesa **Macchina virtuale di archiviazione**.
4. Fare clic su **Nuovo**.

   Si apre la finestra di dialogo Nuova condivisione.

5. Nella finestra di dialogo Nuova condivisione, definire la condivisione:

| In questo campo… | Fai questo… |
|---|---|
| Descrizione | Inserisci un testo descrittivo per la condivisione. |
| Condividi il nome | Immettere il nome della condivisione, ad esempio test_share.<br><br>Il nome immesso per la condivisione verrà utilizzato anche come nome del volume.<br><br>Il nome della condivisione:<br><br>• Deve essere una stringa UTF-8.<br>• Non deve includere i seguenti caratteri: caratteri di controllo da 0x00 a 0x1F (entrambi inclusi), 0x22 (virgolette doppie) e caratteri speciali `\ / [ ] : (vertical bar) < > + = ; , ?` |
| Condividi percorso | • Fare clic nel campo per immettere un nuovo percorso del file system, ad esempio /.<br>• Fare doppio clic nel campo per selezionare da un elenco di percorsi di file system esistenti. |

6. Quando sei soddisfatto dei tuoi dati, clicca su **OK**.

   SnapCenter crea la condivisione SMB sulla SVM.

### Elimina una condivisione SMB

È possibile eliminare una condivisione SMB quando non è più necessaria.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Condivisioni**.
3. Nella pagina Condivisioni, fare clic sul campo **Macchina virtuale di archiviazione** per visualizzare un menu a discesa con un elenco delle macchine virtuali di archiviazione (SVM) disponibili, quindi selezionare la SVM per la condivisione che si desidera eliminare.
4. Dall'elenco delle condivisioni sull'SVM, seleziona la condivisione che desideri eliminare e fai clic su **Elimina**.
5. Nella finestra di dialogo Elimina condivisione, fare clic su **OK**.

   SnapCenter elimina la condivisione SMB dall'SVM.

#### Recuperare spazio sul sistema di archiviazione

Sebbene NTFS tenga traccia dello spazio disponibile su una LUN quando i file vengono eliminati o modificati, non segnala le nuove informazioni al sistema di archiviazione. È possibile eseguire il cmdlet PowerShell per il recupero dello spazio sull'host Plug-in per Windows per garantire che i blocchi appena liberati vengano contrassegnati come disponibili nell'archiviazione.

Se si esegue il cmdlet su un host plug-in remoto, è necessario aver eseguito il cmdlet SnapCenterOpen-SMConnection per aprire una connessione al server SnapCenter .

#### Prima di iniziare

- Prima di eseguire un'operazione di ripristino, è necessario assicurarsi che il processo di recupero dello spazio sia stato completato.
- Se il LUN è condiviso dagli host in un cluster di failover di Windows Server, è necessario eseguire il recupero dello spazio sull'host proprietario del gruppo di cluster.
- Per prestazioni di archiviazione ottimali, è opportuno effettuare il recupero dello spazio il più spesso possibile.

  È necessario assicurarsi che l'intero file system NTFS sia stato scansionato.

#### Informazioni su questo compito

- Il recupero dello spazio è un'operazione che richiede molto tempo e impegna molta CPU, quindi in genere è meglio eseguirla quando l'utilizzo del sistema di archiviazione e dell'host Windows è basso.
- Il recupero dello spazio recupera quasi tutto lo spazio disponibile, ma non il 100%.
- Non eseguire la deframmentazione del disco contemporaneamente al recupero dello spazio.

  Ciò potrebbe rallentare il processo di bonifica.

#### Fare un passo

Dal prompt dei comandi di PowerShell del server applicativo, immettere il seguente comando:

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

drive_path è il percorso dell'unità mappato al LUN.

#### Fornire l'archiviazione utilizzando i cmdlet di PowerShell

Se non si desidera utilizzare l'interfaccia utente grafica SnapCenter per eseguire attività di provisioning host e recupero spazio, è possibile utilizzare i cmdlet di PowerShell. È possibile utilizzare i cmdlet direttamente oppure aggiungerli agli script.

Se si eseguono i cmdlet su un host plug-in remoto, è necessario eseguire il cmdlet SnapCenter Open-SMConnection per aprire una connessione al server SnapCenter .

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

Se i cmdlet di SnapCenter PowerShell non funzionano correttamente a causa della rimozione di SnapDrive per Windows dal server, fare riferimento a "I cmdlet SnapCenter non funzionano quando SnapDrive per Windows viene disinstallato" .

### Fornire storage in ambienti VMware

È possibile utilizzare il plug-in SnapCenter per Microsoft Windows negli ambienti VMware per creare e gestire LUN e snapshot.

#### Piattaforme di sistemi operativi guest VMware supportate

- Versioni supportate di Windows Server
- Configurazioni del cluster Microsoft

  Supporto per un massimo di 16 nodi supportati su VMware quando si utilizza Microsoft iSCSI Software Initiator o fino a due nodi utilizzando FC

- LUN RDM

  Supporto per un massimo di 56 RDM LUN con quattro controller LSI Logic SCSI per RDMS normale o 42 RDM LUN con tre controller LSI Logic SCSI su un plug-in box-to-box VMware VM MSCS per la configurazione Windows

  Supporta il controller VMware ParaVirtual SCSI. Sui dischi RDM possono essere supportati 256 dischi.

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

#### Limitazioni relative al server VMware ESXi

- L'installazione del plug-in per Windows su un cluster Microsoft su macchine virtuali utilizzando le credenziali ESXi non è supportata.

  Quando si installa il plug-in per Windows su macchine virtuali in cluster, è necessario utilizzare le credenziali vCenter.

- Tutti i nodi del cluster devono utilizzare lo stesso ID di destinazione (sulla scheda SCSI virtuale) per lo stesso disco del cluster.
- Quando si crea un LUN RDM al di fuori del plug-in per Windows, è necessario riavviare il servizio plug-in per consentirgli di riconoscere il disco appena creato.
- Non è possibile utilizzare contemporaneamente gli iniziatori iSCSI e FC su un sistema operativo guest VMware.

### Privilegi minimi vCenter richiesti per le operazioni SnapCenter RDM

Per eseguire operazioni RDM in un sistema operativo guest, è necessario disporre dei seguenti privilegi vCenter sull'host:

- Datastore: Rimuovi file
- Host: Configurazione > Configurazione partizione di archiviazione
- Macchina virtuale: configurazione

È necessario assegnare questi privilegi a un ruolo a livello di Virtual Center Server. Il ruolo a cui assegni questi privilegi non può essere assegnato a nessun utente senza privilegi di root.

Dopo aver assegnato questi privilegi, è possibile installare il plug-in per Windows sul sistema operativo guest.

#### Gestire le LUN FC RDM in un cluster Microsoft

È possibile utilizzare il plug-in per Windows per gestire un cluster Microsoft mediante LUN FC RDM, ma è necessario prima creare il quorum RDM condiviso e l'archiviazione condivisa all'esterno del plug-in, quindi aggiungere i dischi alle macchine virtuali nel cluster.

A partire da ESXi 5.5, è possibile utilizzare anche hardware ESX iSCSI e FCoE per gestire un cluster Microsoft. Il plug-in per Windows include il supporto immediato per i cluster Microsoft.

### Requisiti

Il plug-in per Windows fornisce supporto per cluster Microsoft che utilizzano LUN FC RDM su due diverse macchine virtuali appartenenti a due diversi server ESX o ESXi, noti anche come cluster across box, quando si soddisfano requisiti di configurazione specifici.

- Le macchine virtuali (VM) devono eseguire la stessa versione di Windows Server.
- Le versioni del server ESX o ESXi devono essere le stesse per ogni host padre VMware.
- Ogni host padre deve disporre di almeno due schede di rete.
- Deve essere presente almeno un datastore VMware Virtual Machine File System (VMFS) condiviso tra i due server ESX o ESXi.
- VMware consiglia di creare il datastore condiviso su una SAN FC.

  Se necessario, il datastore condiviso può essere creato anche tramite iSCSI.

- La LUN RDM condivisa deve essere in modalità di compatibilità fisica.
- Il LUN RDM condiviso deve essere creato manualmente all'esterno del plug-in per Windows.

  Non è possibile utilizzare dischi virtuali per l'archiviazione condivisa.

- Su ogni macchina virtuale del cluster deve essere configurato un controller SCSI in modalità di

compatibilità fisica:

Windows Server 2008 R2 richiede di configurare il controller SCSI LSI Logic SAS su ogni macchina virtuale. Le LUN condivise non possono utilizzare il controller LSI Logic SAS esistente se ne esiste solo uno del suo tipo ed è già collegato all'unità C:.

I controller SCSI di tipo paravirtuale non sono supportati sui cluster VMware Microsoft.

> Quando si aggiunge un controller SCSI a una LUN condivisa su una macchina virtuale in modalità di compatibilità fisica, è necessario selezionare l'opzione **Raw Device Mappings** (RDM) e non l'opzione **Crea un nuovo disco** in VMware Infrastructure Client.

- I cluster di macchine virtuali Microsoft non possono far parte di un cluster VMware.
- Quando si installa il plug-in per Windows su macchine virtuali appartenenti a un cluster Microsoft, è necessario utilizzare le credenziali vCenter e non quelle ESX o ESXi.
- Il plug-in per Windows non può creare un singolo igroup con iniziatori provenienti da più host.

  L'igroup contenente gli iniziatori di tutti gli host ESXi deve essere creato sul controller di archiviazione prima di creare i LUN RDM che verranno utilizzati come dischi del cluster condivisi.

- Assicurarsi di creare un LUN RDM su ESXi 5.0 utilizzando un iniziatore FC.

  Quando si crea un LUN RDM, viene creato un gruppo di iniziatori con ALUA.

### Limitazioni

Il plug-in per Windows supporta i cluster Microsoft che utilizzano LUN RDM FC/iSCSI su diverse macchine virtuali appartenenti a diversi server ESX o ESXi.

> Questa funzionalità non è supportata nelle versioni precedenti a ESX 5.5i.

- Il plug-in per Windows non supporta cluster su datastore ESX iSCSI e NFS.
- Il plug-in per Windows non supporta iniziatori misti in un ambiente cluster.

  Gli iniziatori devono essere FC o Microsoft iSCSI, ma non entrambi.

- Gli iniziatori iSCSI e gli HBA ESX non sono supportati sui dischi condivisi in un cluster Microsoft.
- Il plug-in per Windows non supporta la migrazione di macchine virtuali con vMotion se la macchina virtuale fa parte di un cluster Microsoft.
- Il plug-in per Windows non supporta MPIO su macchine virtuali in un cluster Microsoft.

### Creare un LUN FC RDM condiviso

Prima di poter utilizzare le LUN FC RDM per condividere lo storage tra i nodi in un cluster Microsoft, è necessario creare il disco quorum condiviso e il disco di storage condiviso, quindi aggiungerli a entrambe le macchine virtuali nel cluster.

Il disco condiviso non viene creato utilizzando il plug-in per Windows. Dovresti creare e poi aggiungere la LUN condivisa a ciascuna macchina virtuale nel cluster. Per informazioni, vedere "Cluster di macchine virtuali su host fisici" .

## Aggiungi licenze basate sul controller SnapCenter Standard

Se si utilizzano controller di archiviazione FAS, AFF o ASA , è necessaria una licenza basata sul controller SnapCenter Standard.

La licenza basata sul controller presenta le seguenti caratteristiche:

- Diritto a SnapCenter Standard incluso con l'acquisto di Premium o Flash Bundle (non con il pacchetto base)
- Utilizzo illimitato dello spazio di archiviazione
- Aggiunto direttamente al controller di archiviazione FAS, AFF o ASA tramite ONTAP System Manager o ONTAP CLI.

> Per le licenze basate sul controller SnapCenter non è necessario immettere alcuna informazione sulla licenza nell'interfaccia utente SnapCenter .

- Bloccato sul numero di serie del controller

Per informazioni sulle licenze richieste, vedere"Licenze SnapCenter" .

### Passaggio 1: verificare se la licenza di SnapManager Suite è installata

È possibile utilizzare l'interfaccia utente SnapCenter per verificare se una licenza SnapManager Suite è installata sui sistemi di archiviazione primari FAS, AFF o ASA e identificare quali sistemi necessitano di licenze. Le licenze di SnapManager Suite si applicano solo a SVM o cluster FAS, AFF e ASA su sistemi di storage primari.

> Se sul controller è già presente una licenza SnapManager Suite, SnapCenter fornisce automaticamente il diritto alla licenza Standard basata sul controller. I nomi licenza SnapManagerSuite e licenza basata su controller SnapCenter Standard vengono utilizzati in modo intercambiabile, ma si riferiscono alla stessa licenza.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, seleziona se visualizzare tutti gli SVM o i cluster aggiunti:
   - Per visualizzare tutti gli SVM aggiunti, selezionare * ONTAP SVM*.
   - Per visualizzare tutti i cluster aggiunti, selezionare *Cluster ONTAP *.

     Quando si seleziona il nome del cluster, tutte le SVM che ne fanno parte vengono visualizzate nella sezione Macchine virtuali di archiviazione.
3. Nell'elenco Connessioni di archiviazione, individuare la colonna Licenza controller.

   La colonna Licenza controller visualizza il seguente stato:

   - ✔ indica che una licenza SnapManager Suite è installata su un sistema di archiviazione primario FAS, AFF o ASA .
   -

indica che una licenza SnapManager Suite non è installata su un sistema di archiviazione primario FAS, AFF o ASA .

- Non applicabile indica che una licenza SnapManager Suite non è applicabile perché il controller di storage si trova su Amazon FSx for NetApp ONTAP, Cloud Volumes ONTAP, ONTAP Select o piattaforme di storage secondarie.

### Passaggio 2: identificare le licenze installate sul controller

È possibile utilizzare la riga di comando ONTAP per visualizzare tutte le licenze installate sul controller. Dovresti essere un amministratore del cluster sul sistema FAS, AFF o ASA .

Il controller visualizza la licenza basata sul controller SnapCenter Standard come licenza SnapManagerSuite.

**Passi**

1. Accedere al controller NetApp tramite la riga di comando ONTAP .
2. Immettere il comando license show, quindi visualizzare l'output per verificare se la licenza SnapManagerSuite è installata.

**Esempio di output**

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

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

Serial Number: 1-81-0000000000000000000000000xx
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 -
```

Nell'esempio, è installata la licenza SnapManagerSuite, pertanto non è richiesta alcuna ulteriore azione di

licenza SnapCenter .

### Passaggio 3: recuperare il numero di serie del controller

Ottenere il numero di serie del controller utilizzando la riga di comando ONTAP . Per ottenere il numero di serie della licenza basata sul controller, è necessario essere un amministratore del cluster sul sistema FAS, AFF o ASA .

**Passi**

1. Accedere al controller tramite la riga di comando ONTAP .
2. Immettere il comando system show -instance, quindi rivedere l'output per individuare il numero di serie del controller.

**Esempio di output**

```
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: xxxxxxxxx
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: xxxxxxxxx
System ID: xxxxxxxxxx
Vendor: NetApp
Health: true
Eligibility: true
Differentiated Services: false
All-Flash Optimized: false
2 entries were displayed.
```

3. Annotare i numeri di serie.

### Passaggio 4: recuperare il numero di serie della licenza basata sul controller

Se si utilizza un archivio FAS, ASA o AFF , è possibile recuperare la licenza basata sul controller SnapCenter dal sito di supporto NetApp prima di installarla utilizzando la riga di comando ONTAP .

**Prima di iniziare**

- È necessario disporre di credenziali di accesso valide al sito di supporto NetApp .

  Se non inserisci credenziali valide, il sistema non restituirà alcuna informazione per la tua ricerca.

- Dovresti avere il numero di serie del controller.

**Passi**

1. Accedi al "Sito di supporto NetApp" .
2. Vai a **Sistemi** > **Licenze software**.
3. Nell'area Criteri di selezione, assicurati che sia selezionato Numero di serie (situato sul retro dell'unità), inserisci il numero di serie del controller e seleziona **Vai!**.

   Viene visualizzato un elenco delle licenze per il controller specificato.

4. Individuare e registrare la licenza SnapCenter Standard o SnapManagerSuite.

### Passaggio 5: aggiungere la licenza basata sul controller

È possibile utilizzare la riga di comando ONTAP per aggiungere una licenza basata sul controller SnapCenter quando si utilizzano sistemi FAS, AFF o ASA e si dispone di una licenza SnapCenter Standard o SnapManagerSuite.

**Prima di iniziare**

- Dovresti essere un amministratore del cluster sul sistema FAS, AFF o ASA .
- Dovresti avere la licenza SnapCenter Standard o SnapManagerSuite.

**Informazioni su questo compito**

Se desideri installare SnapCenter in prova con storage FAS, AFF o ASA , puoi ottenere una licenza di valutazione Premium Bundle da installare sul tuo controller.

Se desideri installare SnapCenter in prova, contatta il tuo rappresentante commerciale per ottenere una licenza di valutazione Premium Bundle da installare sul tuo controller.

**Passi**

1. Accedere al cluster NetApp utilizzando la riga di comando ONTAP .
2. Aggiungere la chiave di licenza SnapManagerSuite:

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

   Questo comando è disponibile a livello di privilegio amministratore.

3. Verificare che la licenza SnapManagerSuite sia installata:

   ```
   license show
   ```

#### Passaggio 6: rimuovere la licenza di prova

Se si utilizza una licenza SnapCenter Standard basata su controller e si ha bisogno di rimuovere la licenza di prova basata sulla capacità (numero di serie che termina con “50”), è necessario utilizzare i comandi MySQL per rimuovere manualmente la licenza di prova. La licenza di prova non può essere eliminata tramite l’interfaccia utente SnapCenter .

> La rimozione manuale di una licenza di prova è necessaria solo se si utilizza una licenza basata su controller SnapCenter Standard.

**Passi**

1. Sul server SnapCenter , aprire una finestra di PowerShell per reimpostare la password MySQL.
   a. Eseguire il cmdlet Open-SmConnection per stabilire una connessione con SnapCenter Server per un account SnapCenterAdmin.
   b. Eseguire Set-SmRepositoryPassword per reimpostare la password MySQL.

      Per informazioni sui cmdlet, vedere "Guida di riferimento ai cmdlet del software SnapCenter" .
2. Aprire il prompt dei comandi ed eseguire mysql -u root -p per accedere a MySQL.

   MySQL ti chiederà la password. Inserisci le credenziali fornite durante la reimpostazione della password.
3. Rimuovere la licenza di prova dal database:

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

## Configurare l’alta disponibilità

#### Configurare i server SnapCenter per l’alta disponibilità

Per supportare l’alta disponibilità (HA) in SnapCenter in esecuzione su Windows o Linux, è possibile installare il bilanciatore del carico F5. F5 consente a SnapCenter Server di supportare configurazioni attive-passive in un massimo di due host che si trovano nella stessa posizione. Per utilizzare F5 Load Balancer in SnapCenter, è necessario configurare i server SnapCenter e configurare F5 Load Balancer.

È anche possibile configurare il bilanciamento del carico di rete (NLB) per impostare l’alta disponibilità SnapCenter . Per un’elevata disponibilità, è necessario configurare NLB manualmente al di fuori dell’installazione SnapCenter .

Per l’ambiente cloud, è possibile configurare l’elevata disponibilità utilizzando Amazon Web Services (AWS) Elastic Load Balancing (ELB) e Azure Load Balancer.

**Configurare l'alta disponibilità utilizzando F5**

Per istruzioni su come configurare i server SnapCenter per l'elevata disponibilità utilizzando il bilanciatore del carico F5, fare riferimento a "Come configurare i server SnapCenter per l'elevata disponibilità utilizzando F5 Load Balancer" .

È necessario essere membri del gruppo Amministratori locali sui server SnapCenter (oltre ad avere il ruolo SnapCenterAdmin) per utilizzare i seguenti cmdlet per aggiungere e rimuovere cluster F5:

- Aggiungi-SmServerCluster
- Aggiungi-SmServer
- Rimuovi-SmServerCluster

  Per ulteriori informazioni, consulta "Guida di riferimento ai cmdlet del software SnapCenter" .

Informazioni aggiuntive

- Dopo aver installato e configurato SnapCenter per l'elevata disponibilità, modificare il collegamento sul desktop SnapCenter in modo che punti all'IP del cluster F5.
- Se si verifica un failover tra i server SnapCenter e se è già presente una sessione SnapCenter , è necessario chiudere il browser e accedere nuovamente a SnapCenter .
- Nella configurazione del bilanciatore del carico (NLB o F5), se si aggiunge un host parzialmente risolto dall'host NLB o F5 e se l'host SnapCenter non è in grado di raggiungere questo host, la pagina dell'host SnapCenter passa frequentemente dallo stato di inattività a quello di esecuzione degli host. Per risolvere questo problema, è necessario assicurarsi che entrambi gli host SnapCenter siano in grado di risolvere l'host in NLB o nell'host F5.
- I comandi SnapCenter per le impostazioni MFA devono essere eseguiti su tutti gli host. La configurazione della relying party deve essere eseguita nel server Active Directory Federation Services (AD FS) utilizzando i dettagli del cluster F5. L'accesso all'interfaccia utente SnapCenter a livello host verrà bloccato dopo l'abilitazione dell'MFA.
- Durante il failover, le impostazioni del registro di controllo non verranno riflesse sul secondo host. Pertanto, è necessario ripetere manualmente le impostazioni del registro di controllo sull'host passivo F5 quando diventa attivo.

**Configurare l'alta disponibilità utilizzando il bilanciamento del carico di rete (NLB)**

È possibile configurare il bilanciamento del carico di rete (NLB) per impostare l'alta disponibilità SnapCenter . Per un'elevata disponibilità, è necessario configurare NLB manualmente al di fuori dell'installazione SnapCenter .

Per informazioni su come configurare il bilanciamento del carico di rete (NLB) con SnapCenter , fare riferimento a "Come configurare NLB con SnapCenter" .

**Configurare l'elevata disponibilità utilizzando AWS Elastic Load Balancing (ELB)**

È possibile configurare un ambiente SnapCenter ad alta disponibilità in Amazon Web Services (AWS) impostando due server SnapCenter in zone di disponibilità (AZ) separate e configurandoli per il failover automatico. L'architettura include indirizzi IP privati virtuali, tabelle di routing e sincronizzazione tra database MySQL attivi e in standby.

**Passi**

1. Configurare l'IP overlay privato virtuale in AWS. Per informazioni, fare riferimento a "Configurare l'IP virtuale privato overlay" .

2. Prepara il tuo host Windows
    a. Forzare la priorità di IPv4 rispetto a IPv6:
        - Posizione: HKLM\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters
        - Chiave: DisabledComponents
        - Tipo: REG_DWORD
        - Valore: 0x20
    b. Assicurarsi che i nomi di dominio completi possano essere risolti tramite DNS o tramite la configurazione dell'host locale negli indirizzi IPv4.
    c. Assicurarsi di non aver configurato un proxy di sistema.
    d. Assicurarsi che la password dell'amministratore sia la stessa su entrambi i server Windows quando si utilizza una configurazione senza Active Directory e i server non si trovano nello stesso dominio.
    e. Aggiungere IP virtuale su entrambi i server Windows.
3. Creare il cluster SnapCenter .
    a. Avvia Powershell e connettiti a SnapCenter.
    ```
    Open-SmConnection
    ```
    b. Creare il cluster.
    ```
    Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <cluster_ip>
    -PrimarySCServerIP <primary_ip> -Verbose -Credential administrator
    ```
    c. Aggiungere il server secondario.
    ```
    Add-SmServer -ServerName <server_name> -ServerIP <server_ip>
    -CleanUpSecondaryServer -Verbose -Credential administrator
    ```
    d. Ottieni i dettagli sull'alta disponibilità.
    ```
    Get-SmServerConfig
    ```
4. Creare la funzione Lamda per adattare la tabella di routing nel caso in cui l'endpoint IP privato virtuale non sia più disponibile, monitorato da AWS CloudWatch. Per informazioni, fare riferimento a "Creare una funzione Lambda" .
5. Crea un monitor in CloudWatch per monitorare la disponibilità dell'endpoint SnapCenter . Un allarme è configurato per attivare una funzione Lambda se l'endpoint non è raggiungibile. La funzione Lambda regola la tabella di routing per reindirizzare il traffico al server SnapCenter attivo. Per informazioni, fare riferimento a "Crea canarini sintetici" .
6. Implementare il flusso di lavoro utilizzando una funzione step come alternativa al monitoraggio CloudWatch, garantendo tempi di failover più brevi. Il flusso di lavoro include una funzione di sonda Lambda per testare l'URL SnapCenter , una tabella DynamoDB per memorizzare i conteggi degli errori e la funzione Step stessa.
    a. Utilizzare una funzione lambda per sondare l'URL SnapCenter . Per informazioni, fare riferimento a "Crea funzione Lambda" .
    b. Crea una tabella DynamoDB per memorizzare il conteggio degli errori tra due iterazioni di Step Function. Per informazioni, fare riferimento a "Inizia con la tabella DynamoDB" .
    c. Creare la funzione Step. Per informazioni, fare riferimento a "Documentazione della funzione Step" .
    d. Prova un singolo passaggio.
    e. Testare la funzione completa.

f. Crea un ruolo IAM e modifica le autorizzazioni per poter eseguire la funzione Lambda.

g. Crea una pianificazione per attivare la funzione Step. Per informazioni, fare riferimento a "Utilizzo di Amazon EventBridge Scheduler per avviare Step Functions" .

**Configurare l'alta disponibilità utilizzando il bilanciatore del carico di Azure**

È possibile configurare un ambiente SnapCenter ad alta disponibilità utilizzando il bilanciamento del carico di Azure.

**Passi**

1. Crea macchine virtuali in un set di scalabilità tramite il portale di Azure. Il set di scalabilità delle macchine virtuali di Azure consente di creare e gestire un gruppo di macchine virtuali con bilanciamento del carico. Il numero di istanze di macchine virtuali può aumentare o diminuire automaticamente in base alla domanda o a una pianificazione definita. Per informazioni, fare riferimento a "Crea macchine virtuali in un set di scalabilità utilizzando il portale di Azure" .
2. Dopo aver configurato le macchine virtuali, accedi a ciascuna macchina virtuale nel set di VM e installa SnapCenter Server in entrambi i nodi.
3. Creare il cluster nell'host 1.
   ```
   Add-SmServerCluster -ClusterName <cluster_name> -ClusterIP <specify the load balancer front end virtual ip> -PrimarySCServerIP <ip address> -Verbose -Credential <credentials>
   ```
4. Aggiungere il server secondario.
   ```
   Add-SmServer -ServerName <name of node2> -ServerIP <ip address of node2> -Verbose -Credential <credentials>
   ```
5. Ottieni i dettagli sull'alta disponibilità.
   ```
   Get-SmServerConfig
   ```
6. Se necessario, ricostruire l'host secondario.
   ```
   Set-SmRepositoryConfig -RebuildSlave -Verbose
   ```
7. Failover sul secondo host.
   ```
   Set-SmRepositoryConfig ActiveMaster <name of node2> -Verbose
   ```

== Passa da NLB a F5 per un'elevata disponibilità

È possibile modificare la configurazione SnapCenter HA da Network Load Balancing (NLB) per utilizzare F5 Load Balancer.

**Passi**

1. Configurare i server SnapCenter per un'elevata disponibilità utilizzando F5. "Saperne di più" .
2. Sull'host del server SnapCenter , avviare PowerShell.
3. Avviare una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
4. Aggiornare SnapCenter Server in modo che punti all'indirizzo IP del cluster F5 utilizzando il cmdlet Update-SmServerCluster.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

#### Elevata disponibilità per il repository MySQL SnapCenter

La replicazione MySQL è una funzionalità di MySQL Server che consente di replicare i dati da un server di database MySQL (master) a un altro server di database MySQL (slave). SnapCenter supporta la replica MySQL per un'elevata disponibilità solo su due nodi abilitati per il bilanciamento del carico di rete (NLB).

SnapCenter esegue operazioni di lettura o scrittura sul repository master e indirizza la sua connessione al repository slave quando si verifica un errore sul repository master. Il repository slave diventa quindi il repository master. SnapCenter supporta anche la replica inversa, che è abilitata solo durante il failover.

Se si desidera utilizzare la funzionalità di alta disponibilità (HA) di MySQL, è necessario configurare Network Load Balancer (NLB) sul primo nodo. Il repository MySQL viene installato su questo nodo come parte dell'installazione. Durante l'installazione di SnapCenter sul secondo nodo, è necessario unirsi a F5 del primo nodo e creare una copia del repository MySQL sul secondo nodo.

SnapCenter fornisce i cmdlet PowerShell *Get-SmRepositoryConfig* e *Set-SmRepositoryConfig* per gestire la replica di MySQL.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

È necessario essere consapevoli delle limitazioni relative alla funzionalità MySQL HA:

- NLB e MySQL HA non sono supportati oltre i due nodi.
- Il passaggio da un'installazione autonoma SnapCenter a un'installazione NLB o viceversa e il passaggio da una configurazione autonoma di MySQL a MySQL HA non sono supportati.
- Il failover automatico non è supportato se i dati del repository slave non sono sincronizzati con i dati del repository master.

  È possibile avviare un failover forzato utilizzando il cmdlet *Set-SmRepositoryConfig*.

- Quando viene avviato il failover, i processi in esecuzione potrebbero non riuscire.

  Se il failover avviene perché MySQL Server o SnapCenter Server non è attivo, tutti i processi in esecuzione potrebbero non riuscire. Dopo il failover sul secondo nodo, tutti i processi successivi vengono eseguiti correttamente.

Per informazioni sulla configurazione dell'alta disponibilità, vedere "Come configurare NLB e ARR con SnapCenter" .

## Configurare il controllo degli accessi basato sui ruoli (RBAC)

#### Crea un ruolo

Oltre a utilizzare i ruoli SnapCenter esistenti, puoi creare ruoli personalizzati e personalizzare le autorizzazioni.

Per creare i propri ruoli, è necessario accedere con il ruolo "SnapCenterAdmin".

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Ruoli**.
3. Clic + .
4. Specificare un nome e una descrizione per il nuovo ruolo.

   Nei nomi utente e nei nomi di gruppo è possibile utilizzare solo i seguenti caratteri speciali: spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:).

5. Selezionare **Tutti i membri di questo ruolo possono vedere gli oggetti degli altri membri** per consentire agli altri membri del ruolo di vedere risorse quali volumi e host dopo aver aggiornato l'elenco delle risorse.

   Se non si desidera che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri, è necessario deselezionare questa opzione.

   Quando questa opzione è abilitata, non è necessario assegnare agli utenti l'accesso agli oggetti o alle risorse se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

6. Nella pagina Autorizzazioni, seleziona le autorizzazioni che desideri assegnare al ruolo oppure fai clic su **Seleziona tutto** per concedere tutte le autorizzazioni al ruolo.
7. Fare clic su **Invia**.

#### Aggiungere un ruolo NetApp ONTAP RBAC utilizzando i comandi di accesso di sicurezza

## È possibile utilizzare i comandi di accesso di sicurezza per aggiungere un ruolo NetApp ONTAP RBAC quando i sistemi di storage eseguono ONTAP in cluster.

#### Prima di iniziare

- Identifica l'attività (o le attività) che desideri eseguire e i privilegi richiesti per eseguirle.
- Concedi privilegi ai comandi e/o alle directory dei comandi.

  Per ogni comando/directory di comandi sono previsti due livelli di accesso: accesso completo e sola lettura.

  È sempre necessario assegnare prima i privilegi di accesso completo.

- Assegnare ruoli agli utenti.
- Identifica la tua configurazione a seconda che i tuoi plug-in SnapCenter siano connessi all'IP dell'amministratore del cluster per l'intero cluster o direttamente a una SVM all'interno del cluster.

#### Informazioni su questo compito

Per semplificare la configurazione di questi ruoli sui sistemi di storage, è possibile utilizzare lo strumento RBAC User Creator per NetApp ONTAP , pubblicato sul NetApp Communities Forum.

Questo strumento gestisce automaticamente la corretta impostazione dei privilegi ONTAP . Ad esempio, lo strumento RBAC User Creator per NetApp ONTAP aggiunge automaticamente i privilegi nell'ordine corretto, in modo che i privilegi di accesso completo vengano visualizzati per primi. Se si aggiungono prima i privilegi di sola lettura e poi i privilegi di accesso completo, ONTAP contrassegna i privilegi di accesso completo come duplicati e li ignora.

Se in seguito si aggiorna SnapCenter o ONTAP, è necessario eseguire nuovamente lo strumento RBAC User Creator per NetApp ONTAP per aggiornare i ruoli utente creati in precedenza. I ruoli utente creati per una versione precedente di SnapCenter o ONTAP non funzionano correttamente con le versioni aggiornate. Quando si esegue nuovamente lo strumento, l'aggiornamento viene gestito automaticamente. Non è necessario ricreare i ruoli.

Per ulteriori informazioni sulla configurazione dei ruoli ONTAP RBAC, vedere "Guida all'autenticazione dell'amministratore ONTAP 9 e all'alimentazione RBAC" .

**Passi**

1. Nel sistema di archiviazione, creare un nuovo ruolo immettendo il seguente comando:

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

   - svm_name è il nome dell'SVM. Se si lascia vuoto questo campo, il valore predefinito è amministratore del cluster.
   - role_name è il nome specificato per il ruolo.
   - il comando è la capacità ONTAP .

     È necessario ripetere questo comando per ogni autorizzazione. Ricorda che i comandi di accesso completo devono essere elencati prima dei comandi di sola lettura.

   Per informazioni sull'elenco delle autorizzazioni, vedere"Comandi CLI ONTAP per la creazione di ruoli e l'assegnazione di autorizzazioni" .

2. Crea un nome utente immettendo il seguente comando:

   ```
   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 è il nome dell'utente che stai creando.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà una.
   - svm_name è il nome dell'SVM.

3. Assegnare il ruolo all'utente immettendo il seguente comando:

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

   - <user_name> è il nome dell'utente creato nel passaggio 2. Questo comando consente di modificare l'utente per associarlo al ruolo.
   - <svm_name> è il nome dell'SVM.
   - <role_name> è il nome del ruolo creato nel passaggio 1.
   - <password> è la tua password. Se non specifichi una password, il sistema te ne chiederà una.

4. Verificare che l'utente sia stato creato correttamente immettendo il seguente comando:

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

user_name è il nome dell'utente creato nel passaggio 3.

#### Creare ruoli SVM con privilegi minimi

Quando si crea un ruolo per un nuovo utente SVM in ONTAP , è necessario eseguire diversi comandi ONTAP CLI. Questo ruolo è obbligatorio se si configurano le SVM in ONTAP per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

**Passi**

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

##### Comandi CLI ONTAP per la creazione di ruoli SVM e l'assegnazione di autorizzazioni

Esistono diversi comandi ONTAP CLI che dovresti eseguire per creare ruoli SVM e assegnare autorizzazioni.

- `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`

#### Creare ruoli SVM per i sistemi ASA r2

Per creare un ruolo per un nuovo utente SVM nei sistemi ASA r2, è necessario eseguire

diversi comandi ONTAP CLI. Questo ruolo è obbligatorio se si configurano le SVM nei sistemi ASA r2 per l'utilizzo con SnapCenter e non si desidera utilizzare il ruolo vsadmin.

**Passi**

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

#### Comandi CLI ONTAP per la creazione di ruoli SVM e l'assegnazione di autorizzazioni

Esistono diversi comandi ONTAP CLI che dovresti eseguire per creare ruoli SVM e assegnare autorizzazioni.

- `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

#### Creare ruoli cluster ONTAP con privilegi minimi

È necessario creare un ruolo cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi ONTAP CLI per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

**Passi**

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

##### Comandi CLI ONTAP per la creazione di ruoli del cluster e l'assegnazione di autorizzazioni

Per creare ruoli del cluster e assegnare autorizzazioni, è necessario eseguire diversi comandi ONTAP CLI.

- 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`

#### Creare ruoli cluster ONTAP per sistemi ASA r2

È necessario creare un ruolo cluster ONTAP con privilegi minimi in modo da non dover utilizzare il ruolo di amministratore ONTAP per eseguire operazioni in SnapCenter. È possibile eseguire diversi comandi ONTAP CLI per creare il ruolo del cluster ONTAP e assegnare privilegi minimi.

**Passi**

1. Nel sistema di archiviazione, creare un ruolo e assegnargli tutte le autorizzazioni.

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

   Dovresti ripetere questo comando per ogni autorizzazione.

2. Crea un utente e assegnagli il ruolo.

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

3. Sblocca l'utente.

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

#### Comandi CLI ONTAP per la creazione di ruoli del cluster e l'assegnazione di autorizzazioni

Per creare ruoli del cluster e assegnare autorizzazioni, è necessario eseguire diversi comandi ONTAP CLI.

- `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`

#### Aggiungi un utente o un gruppo e assegna ruoli e risorse

Per configurare il controllo degli accessi basato sui ruoli per gli utenti SnapCenter , è possibile aggiungere utenti o gruppi e assegnare ruoli. Il ruolo determina le opzioni a cui possono accedere gli utenti SnapCenter .

**Prima di iniziare**

- Devi aver effettuato l'accesso con il ruolo "SnapCenterAdmin".
- È necessario aver creato gli account utente o di gruppo in Active Directory nel sistema operativo o nel database. Non è possibile utilizzare SnapCenter per creare questi account.

  Nei nomi utente e nei nomi di gruppo è possibile includere solo i seguenti caratteri speciali: spazio ( ), trattino (-), carattere di sottolineatura (_) e due punti (:).

- SnapCenter include diversi ruoli predefiniti.

  È possibile assegnare questi ruoli all'utente oppure crearne di nuovi.

- Gli utenti AD e i gruppi AD aggiunti a SnapCenter RBAC devono disporre dell'autorizzazione READ sul contenitore Users e sul contenitore Computer in Active Directory.
- Dopo aver assegnato un ruolo a un utente o a un gruppo che contiene le autorizzazioni appropriate, è necessario assegnare all'utente l'accesso alle risorse SnapCenter , come host e connessioni di archiviazione.

  Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

- A un certo punto dovresti assegnare un ruolo all'utente o al gruppo per sfruttare i permessi e l'efficienza di RBAC.
- Durante la creazione dell'utente o del gruppo, è possibile assegnare risorse quali host, gruppi di risorse, policy, connessione di archiviazione, plug-in e credenziali all'utente.
- Le risorse minime che dovresti assegnare a un utente per eseguire determinate operazioni sono le seguenti:

| Operazione | Assegnazione dei beni |
|---|---|
| Proteggere le risorse | ospite, politica |
| Backup | host, gruppo di risorse, policy |

| Operazione | Assegnazione dei beni |
| --- | --- |
| Ripristinare | host, gruppo di risorse |
| Clone | host, gruppo di risorse, policy |
| Ciclo di vita del clone | ospite |
| Crea un gruppo di risorse | ospite |

- Quando un nuovo nodo viene aggiunto a un cluster Windows o a una risorsa DAG (Exchange Server Database Availability Group) e se questo nuovo nodo viene assegnato a un utente, è necessario riassegnare la risorsa all'utente o al gruppo per includere il nuovo nodo nell'utente o nel gruppo.

  È necessario riassegnare l'utente o il gruppo RBAC al cluster o al DAG per includere il nuovo nodo nell'utente o nel gruppo RBAC. Ad esempio, si dispone di un cluster a due nodi e al cluster è stato assegnato un utente o un gruppo RBAC. Quando si aggiunge un altro nodo al cluster, è necessario riassegnare l'utente o il gruppo RBAC al cluster per includere il nuovo nodo per l'utente o il gruppo RBAC.

- Se si prevede di replicare gli snapshot, è necessario assegnare la connessione di archiviazione per il volume di origine e di destinazione all'utente che esegue l'operazione.

  È necessario aggiungere risorse prima di assegnare l'accesso agli utenti.

Se si utilizzano le funzioni SnapCenter Plug-in for VMware vSphere per proteggere VM, VMDK o datastore, è necessario utilizzare l'interfaccia utente grafica di VMware vSphere per aggiungere un utente vCenter a un ruolo SnapCenter Plug-in for VMware vSphere . Per informazioni sui ruoli VMware vSphere, vedere "Ruoli predefiniti forniti con il SnapCenter Plug-in for VMware vSphere" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Utenti e accesso** > * *.
3. Nella pagina Aggiungi utenti/gruppi da Active Directory o gruppo di lavoro:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di accesso | Seleziona Dominio o gruppo di lavoro<br><br>Per il tipo di autenticazione Dominio, è necessario specificare il nome di dominio dell'utente o del gruppo a cui si desidera aggiungere l'utente a un ruolo.<br><br>Per impostazione predefinita, è precompilato con il nome di dominio dell'utente registrato.<br><br>È necessario registrare il dominio non attendibile nella pagina **Impostazioni** > **Impostazioni globali** > **Impostazioni dominio**. |
| Tipo | Seleziona Utente o Gruppo<br><br>SnapCenter supporta solo il gruppo di sicurezza e non il gruppo di distribuzione. |
| Nome utente | a. Digitare il nome utente parziale, quindi fare clic su **Aggiungi**.<br><br>Il nome utente è sensibile alle maiuscole e alle minuscole.<br><br>b. Selezionare il nome utente dall'elenco di ricerca.<br><br>Quando aggiungi utenti da un dominio diverso o da un dominio non attendibile, dovresti digitare il nome utente per intero perché non esiste un elenco di ricerca per gli utenti di domini diversi.<br><br>Ripetere questo passaggio per aggiungere altri utenti o gruppi al ruolo selezionato. |
| Ruoli | Seleziona il ruolo a cui vuoi aggiungere l'utente. |

4. Fare clic su **Assegna**, quindi nella pagina Assegna risorse:
   a. Selezionare il tipo di risorsa dall'elenco a discesa **Risorsa**.
   b. Nella tabella Asset, seleziona l'asset.

      Le risorse vengono elencate solo se l'utente le ha aggiunte a SnapCenter.

c. Ripetere questa procedura per tutte le risorse richieste.

d. Fare clic su **Salva**.

5. Fare clic su **Invia**.

Dopo aver aggiunto utenti o gruppi e assegnato i ruoli, aggiorna l'elenco delle risorse.

## Configurare le impostazioni del registro di controllo

I registri di controllo vengono generati per ogni singola attività del server SnapCenter . Per impostazione predefinita, i registri di controllo sono protetti nel percorso di installazione predefinito *C:\Programmi\ NetApp\ SnapCenter WebApp\audit*.

I registri di controllo sono protetti mediante la generazione di un digest firmato digitalmente per ogni singolo evento di controllo, per proteggerlo da modifiche non autorizzate. I digest generati vengono conservati in un file di checksum di controllo separato e sottoposti a controlli di integrità periodici per garantire l'integrità del contenuto.

Dovresti aver effettuato l'accesso con il ruolo "SnapCenterAdmin".

**Informazioni su questo compito**

- Gli avvisi vengono inviati nei seguenti scenari:
  - La pianificazione del controllo dell'integrità del registro di controllo o il server Syslog è abilitato o disabilitato
  - Controllo dell'integrità del registro di controllo, registro di controllo o errore del registro del server Syslog
  - Poco spazio su disco
- L'e-mail viene inviata solo quando il controllo di integrità fallisce.
- È necessario modificare contemporaneamente i percorsi della directory del registro di controllo e della directory del registro di checksum di controllo. Non è possibile modificarne solo uno.
- Quando vengono modificati i percorsi della directory del registro di controllo e della directory del registro di checksum di controllo, il controllo di integrità non può essere eseguito sui registri di controllo presenti nella posizione precedente.
- I percorsi della directory del registro di controllo e della directory del registro di checksum di controllo devono trovarsi sull'unità locale di SnapCenter Server.

  Le unità condivise o montate in rete non sono supportate.

- Se nelle impostazioni del server Syslog viene utilizzato il protocollo UDP, gli errori dovuti a porta inattiva o non disponibile non possono essere acquisiti come errore o avviso in SnapCenter.
- È possibile utilizzare i comandi Set-SmAuditSettings e Get-SmAuditSettings per configurare i log di controllo.

  Le informazioni sui parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help nome_comando. In alternativa, puoi anche fare riferimento al "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nella pagina **Impostazioni**, vai a **Impostazioni** > **Impostazioni globali** > **Impostazioni registro di**

**controllo**.

2. Nella sezione Registro di controllo, immettere i dettagli.
3. Immettere la **directory del registro di controllo** e la **directory del registro di checksum di controllo**
   a. Inserisci la dimensione massima del file
   b. Inserisci il numero massimo di file di registro
   c. Inserisci la percentuale di utilizzo dello spazio su disco per inviare un avviso
4. (Facoltativo) Abilita **Registra ora UTC**.
5. (Facoltativo) Abilita **Pianificazione controllo integrità registro di controllo** e fai clic su **Avvia controllo integrità** per il controllo di integrità su richiesta.

   È anche possibile eseguire il comando **Start-SmAuditIntegrityCheck** per avviare il controllo di integrità su richiesta.

6. (Facoltativo) Abilitare i log di controllo inoltrati al server syslog remoto e immettere i dettagli del server Syslog.

   È necessario importare il certificato dal server Syslog nella "radice attendibile" per il protocollo TLS 1.2.

   a. Inserisci l'host del server Syslog
   b. Inserisci la porta del server Syslog
   c. Inserisci il protocollo del server Syslog
   d. Inserisci il formato RFC
7. Fare clic su **Salva**.
8. È possibile visualizzare i controlli di integrità e di spazio su disco facendo clic su **Monitor** > **Jobs**.

## Configurare connessioni MySQL protette con SnapCenter Server

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave se si desidera proteggere la comunicazione tra SnapCenter Server e MySQL Server in configurazioni autonome o configurazioni NLB (Network Load Balancing).

### Configurare connessioni MySQL protette per configurazioni di SnapCenter Server autonome

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave se si desidera proteggere la comunicazione tra SnapCenter Server e MySQL Server. È necessario configurare i certificati e i file chiave in MySQL Server e SnapCenter Server.

Vengono generati i seguenti certificati:

- Certificato CA
- File del certificato pubblico e della chiave privata del server
- Certificato pubblico del client e file della chiave privata

**Passi**

1. Imposta i certificati SSL e i file chiave per i server e i client MySQL su Windows utilizzando il comando openssl.

Per informazioni, vedere "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

> Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file chiave deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file del certificato e della chiave non funzionano per i server compilati tramite OpenSSL.

**Migliore pratica:** dovresti usare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file chiave nella cartella MySQL Data.

   Il percorso predefinito della cartella dati MySQL è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\Data\`.

3. Aggiornare i percorsi del certificato CA, del certificato pubblico del server, del certificato pubblico del client, della chiave privata del server e della chiave privata del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è `C:\ProgramData\NetApp\SnapCenter\MySQL Data\my.ini`.

   > È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file chiave copiati nella sezione [mysqld] del file my.ini nella cartella predefinita `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"
   ```

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

   ```
   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. Arrestare l'applicazione Web SnapCenter Server in Internet Information Server (IIS).
5. Riavviare il servizio MySQL.
6. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config.

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato nel file SnapManager.Web.UI.dll.config.

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

7. Aggiornare il file SnapManager.Web.UI.dll.config con i percorsi forniti nella sezione [client] del file my.ini.

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
<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. Avviare l'applicazione Web SnapCenter Server in IIS.

**Configurare connessioni MySQL protette per configurazioni HA**

È possibile generare certificati Secure Sockets Layer (SSL) e file chiave per entrambi i nodi High Availability (HA) se si desidera proteggere la comunicazione tra SnapCenter Server e i server MySQL. È necessario configurare i certificati e i file chiave nei server MySQL e nei nodi HA.

Vengono generati i seguenti certificati:

- Certificato CA

  Un certificato CA viene generato su uno dei nodi HA e questo certificato CA viene copiato sull'altro nodo HA.

- File del certificato pubblico del server e della chiave privata del server per entrambi i nodi HA
- File del certificato pubblico del client e della chiave privata del client per entrambi i nodi HA

**Passi**

1. Per il primo nodo HA, impostare i certificati SSL e i file chiave per i server e i client MySQL su Windows utilizzando il comando openssl.

   Per informazioni, vedere "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

   > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file chiave deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file del certificato e della chiave non funzionano per i server compilati tramite OpenSSL.

   **Migliore pratica:** dovresti usare il nome di dominio completo (FQDN) del server come nome comune per il certificato del server.

2. Copiare i certificati SSL e i file chiave nella cartella MySQL Data.

   Il percorso predefinito della cartella MySQL Data è C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

3. Aggiornare i percorsi del certificato CA, del certificato pubblico del server, del certificato pubblico del client, della chiave privata del server e della chiave privata del client nel file di configurazione del server MySQL (my.ini).

   Il percorso predefinito del file di configurazione del server MySQL (my.ini) è C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\my.ini.

   > È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

   È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

   L'esempio seguente mostra i certificati e i file chiave copiati nella sezione [mysqld] del file my.ini nella cartella predefinita 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"
   ```

L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
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. Per il secondo nodo HA, copiare il certificato CA e generare il certificato pubblico del server, i file della chiave privata del server, il certificato pubblico del client e i file della chiave privata del client. Eseguire i seguenti passaggi:

   a. Copiare il certificato CA generato sul primo nodo HA nella cartella MySQL Data del secondo nodo NLB.

      Il percorso predefinito della cartella MySQL Data è C:\ProgramData\ NetApp\ SnapCenter\MySQL Data\Data\.

      > Non è necessario creare nuovamente un certificato CA. È necessario creare solo il certificato pubblico del server, il certificato pubblico del client, il file della chiave privata del server e il file della chiave privata del client.

   b. Per il primo nodo HA, impostare i certificati SSL e i file chiave per i server e i client MySQL su Windows utilizzando il comando openssl.

      "MySQL versione 5.7: creazione di certificati e chiavi SSL tramite openssl"

      > Il valore del nome comune utilizzato per il certificato del server, il certificato del client e i file chiave deve essere diverso dal valore del nome comune utilizzato per il certificato CA. Se i valori dei nomi comuni sono gli stessi, i file del certificato e della chiave non funzionano per i server compilati tramite OpenSSL.

      Si consiglia di utilizzare il nome di dominio completo del server come nome comune per il certificato del server.

   c. Copiare i certificati SSL e i file chiave nella cartella MySQL Data.

   d. Aggiornare i percorsi del certificato CA, del certificato pubblico del server, del certificato pubblico del client, della chiave privata del server e della chiave privata del client nel file di configurazione del server MySQL (my.ini).

      > È necessario specificare i percorsi del certificato CA, del certificato pubblico del server e della chiave privata del server nella sezione [mysqld] del file di configurazione del server MySQL (my.ini).

      È necessario specificare i percorsi del certificato CA, del certificato pubblico del client e della chiave

privata del client nella sezione [client] del file di configurazione del server MySQL (my.ini).

L'esempio seguente mostra i certificati e i file chiave copiati nella sezione [mysqld] del file my.ini nella cartella predefinita 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"
```

L'esempio seguente mostra i percorsi aggiornati nella sezione [client] del file my.ini.

```
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. Arrestare l'applicazione Web SnapCenter Server in Internet Information Server (IIS) su entrambi i nodi HA.
6. Riavviare il servizio MySQL su entrambi i nodi HA.
7. Aggiornare il valore della chiave MySQLProtocol nel file SnapManager.Web.UI.dll.config per entrambi i nodi HA.

   L'esempio seguente mostra il valore della chiave MySQLProtocol aggiornato nel file SnapManager.Web.UI.dll.config.

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

8. Aggiornare il file SnapManager.Web.UI.dll.config con i percorsi specificati nella sezione [client] del file my.ini per entrambi i nodi HA.

   L'esempio seguente mostra i percorsi aggiornati nella sezione [client] dei file my.ini.

```
<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. Avviare l'applicazione Web SnapCenter Server in IIS su entrambi i nodi HA.
10. Utilizzare il cmdlet PowerShell Set-SmRepositoryConfig -RebuildSlave -Force con l'opzione -Force su uno dei nodi HA per stabilire una replica MySQL protetta su entrambi i nodi HA.

    Anche se lo stato di replica è integro, l'opzione -Force consente di ricostruire il repository slave.

# Configurare l'autenticazione basata su certificato

L'autenticazione basata su certificato aumenta la sicurezza verificando l'identità sia del server SnapCenter che degli host dei plug-in, garantendo comunicazioni sicure e crittografate.

## Abilita l'autenticazione basata sul certificato

Per abilitare l'autenticazione basata su certificato per SnapCenter Server e gli host plug-in di Windows, eseguire il seguente cmdlet di PowerShell. Per gli host plug-in Linux, l'autenticazione basata su certificato verrà abilitata quando si abilita l'SSL bidirezionale.

- Per abilitare l'autenticazione basata sul certificato client:

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

- Per disabilitare l'autenticazione basata sul certificato client:

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

## Esportare i certificati dell'autorità di certificazione (CA) da SnapCenter Server

È necessario esportare i certificati CA dal server SnapCenter agli host plug-in utilizzando la console di gestione Microsoft (MMC).

**Prima di iniziare**

Dovresti aver configurato l'SSL bidirezionale.

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra Snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati - Computer locale** > **Personale** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato CA ottenuto, utilizzato per SnapCenter Server, quindi selezionare **Tutte le attività** > **Esporta** per avviare la procedura guidata di esportazione.
6. Eseguire le seguenti azioni nella procedura guidata.

| Per questa opzione… | Procedi come segue… |
|---|---|
| Esporta chiave privata | Selezionare **No, non esportare la chiave privata**, quindi fare clic su **Avanti**. |
| Formato file di esportazione | Fare clic su **Avanti**. |
| Nome del file | Fare clic su **Sfoglia** e specificare il percorso del file in cui salvare il certificato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di esportazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'esportazione. |

L'autenticazione basata su certificato non è supportata per le configurazioni SnapCenter HA e per il SnapCenter Plug-in for VMware vSphere.

## Importa il certificato CA negli host dei plug-in di Windows

Per utilizzare il certificato CA di SnapCenter Server esportato, è necessario importare il certificato correlato negli host del plug-in Windows SnapCenter tramite la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra Snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati - Computer locale** > **Personale** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Personale", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Eseguire le seguenti azioni nella procedura guidata.

| Per questa opzione… | Procedi come segue… |
|---|---|
| Posizione del negozio | Fare clic su **Avanti**. |

| Per questa opzione… | Procedi come segue… |
| --- | --- |
| File da importare | Selezionare il certificato SnapCenter Server che termina con l'estensione .cer. |
| Archivio certificati | Fare clic su **Avanti**. |
| Completamento della procedura guidata di esportazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

## Importa il certificato CA negli host del plug-in UNIX

Dovresti importare il certificato CA negli host del plug-in UNIX.

### Informazioni su questo compito

- È possibile gestire la password per l'archivio chiavi SPL e l'alias della coppia di chiavi firmata dalla CA in uso.
- La password per il keystore SPL e per tutte le password alias associate alla chiave privata devono essere le stesse.

### Passi

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL. È il valore corrispondente alla chiave `SPL_KEYSTORE_PASS` .
2. Cambia la password del keystore:
   `$ keytool -storepasswd -keystore keystore.jks`
3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:
   `$ keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
4. Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS in `spl.properties` file.
5. Riavviare il servizio dopo aver modificato la password.

### Configurare i certificati radice o intermedi per l'archivio attendibile SPL

È necessario configurare i certificati radice o intermedi su SPL trust-store. Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

### Passi

1. Passare alla cartella contenente il keystore SPL: `/var/opt/snapcenter/spl/etc` .
2. Individuare il file `keystore.jks` .
3. Elenca i certificati aggiunti nel keystore:
   `$ keytool -list -v -keystore keystore.jks`
4. Aggiungi un certificato radice o intermedio:
   `$ keytool -import -trustcacerts -alias <AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore keystore.jks`

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi su SPL trust-store.

#### Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL

È necessario configurare la coppia di chiavi firmata dalla CA su SPL trust-store.

#### Passi

1. Passare alla cartella contenente il keystore dell'SPL `/var/opt/snapcenter/spl/etc` .
2. Individuare il file `keystore.jks` .
3. Elenca i certificati aggiunti nel keystore:
   `$ keytool -list -v -keystore keystore.jks`
4. Aggiungere il certificato CA con chiave sia privata che pubblica.
   `$ keytool -importkeystore -srckeystore <CertificatePathToImport> -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS`
5. Elenca i certificati aggiunti nel keystore.
   `$ keytool -list -v -keystore keystore.jks`
6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS in `spl.properties` file.

   `$ keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore keystore.jks`
8. Se il nome alias nel certificato CA è lungo e contiene spazi o caratteri speciali ("*",","), modificare il nome alias in un nome semplice:
   `$ keytool -changealias -alias "<OrignalAliasName>" -destalias "<NewAliasName>" -keystore keystore.jks`
9. Configurare il nome alias dal keystore situato in `spl.properties` file. Aggiornare questo valore in base alla chiave SPL_CERTIFICATE_ALIAS.
10. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL.

## Esportare i certificati SnapCenter

Dovresti esportare i certificati SnapCenter in formato .pfx.

#### Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, seleziona l'opzione **Il mio account utente**, quindi fai clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati - Utente corrente** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sul certificato con il nome descrittivo SnapCenter , quindi selezionare **Tutte le attività** > **Esporta** per avviare la procedura guidata di esportazione.

6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Esporta chiave privata | Selezionare l'opzione **Sì, esporta la chiave privata**, quindi fare clic su **Avanti**. |
| Formato file di esportazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| File da esportare | Specificare un nome file per il certificato esportato (è necessario utilizzare .pfx), quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di esportazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'esportazione. |

# Configurare il certificato CA per l'host Windows

## Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

## Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

> Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

## Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:

a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

*Get-ChildItem -Percorso Cert:\LocalMachine\My*

b. Copia l'impronta digitale.

## Configurare il certificato CA con i servizi plug-in host di Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Per esempio:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in host di
Windows eseguendo i seguenti comandi:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Per esempio:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

## Configurare il certificato CA con il sito SnapCenter

È necessario configurare il certificato CA con il sito SnapCenter sull'host Windows.

**Passi**

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter .

2. Nel riquadro di navigazione a sinistra, fare clic su **Connessioni**.
3. Espandi il nome del server e **Siti**.
4. Seleziona il sito web SnapCenter su cui desideri installare il certificato SSL.
5. Vai su **Azioni** > **Modifica sito**, fai clic su **Associazioni**.
6. Nella pagina Binding, seleziona **binding per https**.
7. Fare clic su **Modifica**.
8. Dall'elenco a discesa Certificato SSL, seleziona il Certificato SSL importato di recente.
9. Fare clic su **OK**.

Il sito SnapCenter Scheduler (porta predefinita: 8154, HTTPS) è configurato con certificato autofirmato. Questa porta comunica all'interno dell'host del server SnapCenter e non è obbligatorio configurarla con un certificato CA. Tuttavia, se l'ambiente richiede l'utilizzo di un certificato CA, ripetere i passaggi da 5 a 9 utilizzando il sito SnapCenter Scheduler.

Se il certificato CA distribuito di recente non è elencato nel menu a discesa, verificare se il certificato CA è associato alla chiave privata.

Assicurarsi che il certificato venga aggiunto utilizzando il seguente percorso: **Console Root > Certificati – Computer locale > Autorità di certificazione radice attendibili > Certificati**.

## Abilita i certificati CA per SnapCenter

È necessario configurare i certificati CA e abilitare la convalida dei certificati CA per SnapCenter Server.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet Set-SmCertificateSettings.
- È possibile visualizzare lo stato del certificato per SnapCenter Server utilizzando il cmdlet Get-SmCertificateSettings.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, è possibile fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nella pagina Impostazioni, vai su **Impostazioni** > **Impostazioni globali** > **Impostazioni certificato CA**.
2. Selezionare **Abilita convalida certificato**.
3. Fare clic su **Applica**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * 🔒 * indica che non è abilitato o assegnato alcun certificato CA all'host del plug-in.

- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Configurare il certificato CA per l'host Linux

Dopo aver installato SnapCenter Server su Linux, il programma di installazione crea il certificato autofirmato. Se si desidera utilizzare il certificato CA, è necessario configurare i certificati per il proxy inverso nginx, la registrazione degli audit e i servizi SnapCenter .

## Configurare il certificato nginx

**Passi**

1. Vai a */etc/nginx/conf.d*: `cd /etc/nginx/conf.d`
2. Aprire **snapcenter.conf** utilizzando vi o un qualsiasi editor di testo.
3. Passare alla sezione server nel file di configurazione.
4. Modificare i percorsi di *ssl_certificate* e *ssl_certificate_key* in modo che puntino al certificato CA.
5. Salvare e chiudere il file.
6. Ricarica nginx: `$nginx -s reload`

## Configurare il certificato del registro di controllo

**Passi**

1. Aprire *INSTALL_DIR/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config* utilizzando vi o un qualsiasi editor di testo.

   Il valore predefinito di *INSTALL_DIR* è */opt*.

2. Modificare le chiavi **AUDILOG_CERTIFICATE_PATH** e **AUDILOG_CERTIFICATE_PASSWORD** per includere rispettivamente il percorso del certificato CA e la password.

   Per il certificato del registro di controllo è supportato solo il formato *.pfx*.

3. Salvare e chiudere il file.
4. Riavviare il servizio **snapmanagerweb**: `$ systemctl restart snapmanagerweb`

## Configurare il certificato dei servizi SnapCenter

**Passi**

1. Aprire i seguenti file di configurazione utilizzando vi o un qualsiasi editor di testo.
   - *DIR_INSTALL/ NetApp/snapcenter/SnapManagerWeb/ SnapManager.Web.UI.dll.config*
   - *INSTALL_DIR/ NetApp/snapcenter/SMCore/SMCoreServiceHost.dll.config*

- *INSTALL_DIR/ NetApp/snapcenter/Scheduler/Scheduler.Api.dll.config*

  Il valore predefinito di *INSTALL_DIR* è */opt*.

2. Modificare le chiavi **SERVICE_CERTIFICATE_PATH** e **SERVICE_CERTIFICATE_PASSWORD** per includere rispettivamente il percorso del certificato CA e la password.

   Per il certificato dei servizi SnapCenter è supportato solo il formato *.pfx*.

3. Salvare e chiudere i file.
4. Riavviare tutti i servizi.
   - `$ systemctl restart snapmanagerweb`
   - `$ systemctl restart smcore`
   - `$ systemctl restart scheduler`

# Configurare e abilitare la comunicazione SSL bidirezionale sull'host Windows

## Configurare la comunicazione SSL bidirezionale sull'host Windows

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Windows e i plug-in.

**Prima di iniziare**

- Dovresti aver generato il file CSR del certificato CA con la lunghezza minima supportata della chiave pari a 3072.
- Il certificato CA deve supportare l'autenticazione del server e l'autenticazione del client.
- Dovresti avere un certificato CA con chiave privata e dettagli dell'impronta digitale.
- Avresti dovuto abilitare la configurazione SSL unidirezionale.

  Per maggiori dettagli, vedere "Configurare la sezione del certificato CA."

- È necessario abilitare la comunicazione SSL bidirezionale su tutti gli host del plug-in e sul server SnapCenter .

  Non è supportato un ambiente con alcuni host o server non abilitati per la comunicazione SSL bidirezionale.

**Passi**

1. Per associare la porta, eseguire i seguenti passaggi sull'host del server SnapCenter per la porta 8146 (predefinita) del server Web SnapCenter IIS e ancora una volta per la porta 8145 (predefinita) di SMCore utilizzando i comandi di PowerShell.

   a. Rimuovere l'associazione della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

   ```
   > netsh http delete sslcert ipport=0.0.0.0:<SMCore port/IIS port>
   ```

Per esempio,

```
> netsh http delete sslcert ipport=0.0.0.0:8145

> netsh http delete sslcert ipport=0.0.0.0:8146
```

b. Associare il certificato CA appena ottenuto al server SnapCenter e alla porta SMCore.

```
> $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>
```

Per esempio,

```
> $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. Per accedere all'autorizzazione al certificato CA, aggiungere l'utente predefinito del server Web IIS di SnapCenter "**IIS AppPool\ SnapCenter**" nell'elenco delle autorizzazioni del certificato eseguendo i passaggi seguenti per accedere al certificato CA appena ottenuto.
   a. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
   b. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
   c. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
   d. Fare clic su **Console Root** > **Certificati – Computer locale** > **Personale** > **Certificati**.
   e. Selezionare il certificato SnapCenter .
   f. Per avviare la procedura guidata Aggiungi utente/autorizzazione, fare clic con il pulsante destro del mouse sul certificato CA e selezionare **Tutte le attività** > **Gestisci chiavi private**.
   g. Fare clic su **Aggiungi**, nella procedura guidata Seleziona utenti e gruppi modificare la posizione in nome del computer locale (il più in alto nella gerarchia)
   h. Aggiungere l'utente IIS AppPool\ SnapCenter e concedere autorizzazioni di controllo complete.

3. Per **l'autorizzazione IIS del certificato CA**, aggiungere la nuova voce delle chiavi di registro DWORD in SnapCenter Server dal seguente percorso:

   Nell'editor del registro di Windows, passare al percorso indicato di seguito,

   ```
   HKey_Local_Machine\SYSTEM\CurrentControlSet\Control\SecurityProv
   ders\SCHANNEL
   ```

4. Crea una nuova voce di chiave di registro DWORD nel contesto della configurazione del registro SCHANNEL.

   ```
   SendTrustedIssuerList = 0

   ClientAuthTrustMode = 2
   ```

### Configurare il plug-in SnapCenter Windows per la comunicazione SSL bidirezionale

È necessario configurare il plug-in SnapCenter per Windows per la comunicazione SSL bidirezionale utilizzando i comandi di PowerShell.

#### Prima di iniziare

Assicurarsi che l'impronta digitale del certificato CA sia disponibile.

#### Passi

1. Per associare la porta, eseguire le seguenti azioni sull'host plug-in Windows per la porta SMCore 8145 (predefinita).

   a. Rimuovere l'associazione della porta del certificato autofirmato SnapCenter esistente utilizzando il seguente comando PowerShell.

      ```
      > netsh http delete sslcert ipport=0.0.0.0:<SMCore port>
      ```

      Per esempio,

      ```
      > netsh http delete sslcert ipport=0.0.0.0:8145
      ```

   b. Associare il certificato CA appena ottenuto alla porta SMCore.

      ```
      > $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>
      ```

      Per esempio,

      ```
      > $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
```

## Abilita la comunicazione SSL bidirezionale sull'host Windows

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Windows e i plug-in utilizzando i comandi di PowerShell.

**Prima di iniziare**

Eseguire prima i comandi per tutti i plug-in e per l'agente SMCore e poi per il server.

**Passi**

1. Per abilitare la comunicazione SSL bidirezionale, eseguire i seguenti comandi sul server SnapCenter per i plug-in, il server e per ciascuno degli agenti per i quali è richiesta la comunicazione SSL bidirezionale.

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName <Plugin_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="true"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="true"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

```
> Restart-Service -Name SnapManagerCoreService
```

**Disabilita la comunicazione SSL bidirezionale**

È possibile disattivare la comunicazione SSL bidirezionale utilizzando i comandi di PowerShell.

**Informazioni su questo compito**

- Eseguire prima i comandi per tutti i plug-in e per l'agente SMCore e poi per il server.
- Quando si disabilita la comunicazione SSL bidirezionale, il certificato CA e la sua configurazione non vengono rimossi.
- Per aggiungere un nuovo host a SnapCenter Server, è necessario disattivare l'SSL bidirezionale per tutti gli host del plug-in.
- NLB e F5 non sono supportati.

**Passi**

1. Per disattivare la comunicazione SSL bidirezionale, eseguire i seguenti comandi su SnapCenter Server per

tutti gli host del plug-in e per l'host SnapCenter .

```
> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName <Agent_HostName>

> Set-SmConfigSettings -Agent -configSettings @{"EnableTwoWaySSL"="false"}
-HostName localhost

> Set-SmConfigSettings -Server -configSettings @{"EnableTwoWaySSL"="false"}
```

2. Eseguire l'operazione di riciclo del pool di applicazioni IIS SnapCenter utilizzando il seguente comando.
   `> Restart-WebAppPool -Name "SnapCenter"`
3. Per i plug-in di Windows, riavviare il servizio SMCore eseguendo il seguente comando PowerShell:

   ```
   > Restart-Service -Name SnapManagerCoreService
   ```

# Configurare e abilitare la comunicazione SSL bidirezionale sull'host Linux

## Configurare la comunicazione SSL bidirezionale sull'host Linux

È necessario configurare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Linux e i plug-in.

**Prima di iniziare**

- Dovresti aver configurato il certificato CA per l'host Linux.
- È necessario abilitare la comunicazione SSL bidirezionale su tutti gli host del plug-in e sul server SnapCenter .

**Passi**

1. Copia **certificate.pem** in */etc/pki/ca-trust/source/anchors/*.
2. Aggiungi i certificati all'elenco di attendibilità del tuo host Linux.
   - `cp root-ca.pem /etc/pki/ca-trust/source/anchors/`
   - `cp certificate.pem /etc/pki/ca-trust/source/anchors/`
   - `update-ca-trust extract`
3. Verificare se i certificati sono stati aggiunti all'elenco di attendibilità.
   `trust list | grep "<CN of your certificate>"`
4. Aggiornare **ssl_certificate** e **ssl_certificate_key** nel file **nginx** SnapCenter e riavviare.
   - `vim /etc/nginx/conf.d/snapcenter.conf`
   - `systemctl restart nginx`
5. Aggiorna il collegamento all'interfaccia utente grafica di SnapCenter Server.
6. Aggiornare i valori delle seguenti chiavi in * SnapManager.Web.UI.dll.config* situato in _ /<percorso di installazione>/ NetApp/snapcenter/SnapManagerWeb_ e **SMCoreServiceHost.dll.config** situato in */<percorso di installazione>/ NetApp/snapcenter/SMCore*.

- <add key="SERVICE_CERTIFICATE_PATH" value="<percorso del certificato.pfx>" />
- <add key="SERVICE_CERTIFICATE_PASSWORD" value="<password>"/>

7. Riavviare i seguenti servizi.
   - `systemctl restart smcore.service`
   - `systemctl restart snapmanagerweb.service`
8. Verificare che il certificato sia collegato alla porta web SnapManager .
   `openssl s_client -connect localhost:8146 -brief`
9. Verificare che il certificato sia collegato alla porta smcore.
   `openssl s_client -connect localhost:8145 -brief`
10. Gestisci la password per l'archivio chiavi e l'alias SPL.
    a. Recupera la password predefinita del keystore SPL assegnata alla chiave **SPL_KEYSTORE_PASS** nel file delle proprietà SPL.
    b. Cambia la password del keystore.
       `keytool -storepasswd -keystore keystore.jks`
    c. Cambia la password per tutti gli alias delle voci della chiave privata.
       `keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks`
    d. Aggiornare la stessa password per la chiave **SPL_KEYSTORE_PASS** in *spl.properties*.
    e. Riavviare il servizio.
11. Sull'host Linux del plug-in, aggiungere i certificati radice e intermedi nel keystore del plug-in SPL.
    - `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. Controllare le voci in keystore.jks.
         `keytool -list -v -keystore <path to keystore.jks>`
      ii. Se necessario, rinominare qualsiasi alias.
         `keytool -changealias -alias "old-alias" -destalias "new-alias" -keypass keypass -keystore </path/to/keystore> -storepass storepas`
12. Aggiornare il valore di **SPL_CERTIFICATE_ALIAS** nel file *spl.properties* con l'alias di **certificate.pfx** memorizzato in *keystore.jks* e riavviare il servizio SPL: `systemctl restart spl`
13. Verificare che il certificato sia collegato alla porta smcore.
    `openssl s_client -connect localhost:8145 -brief`

## Abilita la comunicazione SSL sull'host Linux

È possibile abilitare la comunicazione SSL bidirezionale per proteggere la comunicazione reciproca tra SnapCenter Server sull'host Linux e i plug-in utilizzando i comandi di PowerShell.

**Fare un passo**

1. Per abilitare la comunicazione SSL unidirezionale, procedere come segue.
   a. Accedi all'interfaccia grafica utente SnapCenter .
   b. Fare clic su **Impostazioni** > **Impostazioni globali** e selezionare **Abilita convalida certificato su SnapCenter Server**.
   c. Fare clic su **Host** > **Host gestiti** e selezionare l'host del plug-in per il quale si desidera abilitare SSL unidirezionale.
   d. Clic icona, quindi fare clic su **Abilita convalida certificato**.
2. Abilita la comunicazione SSL bidirezionale dall'host Linux di SnapCenter Server.
   - `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"}`

# Configurare Active Directory, LDAP e LDAPS

## Registra domini Active Directory non attendibili

È necessario registrare Active Directory con SnapCenter Server per gestire host, utenti e gruppi da più domini Active Directory non attendibili.

**Prima di iniziare**

**Protocolli LDAP e LDAPS**

- È possibile registrare i domini Active Directory non attendibili utilizzando il protocollo LDAP o LDAPS.
- Dovresti aver abilitato la comunicazione bidirezionale tra gli host del plug-in e il server SnapCenter .
- La risoluzione DNS deve essere impostata dal server SnapCenter agli host del plug-in e viceversa.

**Protocollo LDAP**

- Il nome di dominio completo (FQDN) dovrebbe essere risolvibile da SnapCenter Server.

  È possibile registrare un dominio non attendibile con l'FQDN. Se il nome di dominio completo non è risolvibile dal server SnapCenter , è possibile registrarsi con un indirizzo IP del controller di dominio e questo dovrebbe essere risolvibile dal server SnapCenter .

**Protocollo LDAPS**

- I certificati CA sono necessari affinché LDAPS fornisca la crittografia end-to-end durante la comunicazione con Active Directory.

  "Configurare il certificato client CA per LDAPS"

- I nomi host del controller di dominio (DCHostName) devono essere raggiungibili da SnapCenter Server.

### Informazioni su questo compito

- Per registrare un dominio non attendibile è possibile utilizzare l'interfaccia utente SnapCenter , i cmdlet di PowerShell o l'API REST.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Impostazioni globali, fare clic su **Impostazioni dominio**.
4. Clic per registrare un nuovo dominio.
5. Nella pagina Registra nuovo dominio, seleziona **LDAP** o **LDAPS**.
   a. Se si seleziona **LDAP**, specificare le informazioni necessarie per la registrazione del dominio non attendibile per LDAP:

| Per questo campo… | Fai questo… |
|---|---|
| Nome di dominio | Specificare il nome NetBIOS per il dominio. |
| FQDN del dominio | Specificare il nome di dominio completo (FQDN) e fare clic su **Risolvi**. |
| Indirizzi IP del controller di dominio | Se il nome di dominio completo (FQDN) non è risolvibile dal server SnapCenter , specificare uno o più indirizzi IP del controller di dominio.<br><br>Per ulteriori informazioni, vedere "Aggiungere l'IP del controller di dominio per il dominio non attendibile dalla GUI" . |

   b. Se selezioni **LDAPS**, specifica le informazioni necessarie per registrare il dominio non attendibile per LDAPS:

| Per questo campo… | Fai questo… |
|---|---|
| Nome di dominio | Specificare il nome NetBIOS per il dominio. |
| FQDN del dominio | Specificare il nome di dominio completo (FQDN). |
| Nomi dei controller di dominio | Specificare uno o più nomi di controller di dominio e fare clic su **Risolvi**. |
| Indirizzi IP del controller di dominio | Se i nomi dei controller di dominio non sono risolvibili da SnapCenter Server, è necessario correggere le risoluzioni DNS. |

6. Fare clic su **OK**.

## Configurare i pool di applicazioni IIS per abilitare le autorizzazioni di lettura di Active Directory

È possibile configurare Internet Information Services (IIS) sul server Windows per creare un account Application Pool personalizzato quando è necessario abilitare le autorizzazioni di lettura di Active Directory per SnapCenter.

**Passi**

1. Aprire Gestione IIS sul server Windows in cui è installato SnapCenter .
2. Nel riquadro di navigazione a sinistra, fare clic su **Pool di applicazioni**.
3. Selezionare SnapCenter nell'elenco Pool di applicazioni, quindi fare clic su **Impostazioni avanzate** nel riquadro Azioni.
4. Selezionare Identità, quindi fare clic su **…** per modificare l'identità del pool di applicazioni SnapCenter .
5. Nel campo Account personalizzato, immettere il nome di un account utente di dominio o di un amministratore di dominio con autorizzazione di lettura di Active Directory.
6. Fare clic su OK.

   L'account personalizzato sostituisce l'account ApplicationPoolIdentity integrato per il pool di applicazioni SnapCenter .

## Configurare il certificato client CA per LDAPS

È necessario configurare il certificato client CA per LDAPS sul server SnapCenter quando Windows Active Directory LDAPS è configurato con i certificati CA.

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
| --- | --- |
| Nella seconda pagina della procedura guidata | Fare clic su **Sfoglia**, selezionare il *Certificato radice* e fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

7. Ripetere i passaggi 5 e 6 per i certificati intermedi.

# Proteggere i database di Microsoft SQL Server

## Plug-in SnapCenter per Microsoft SQL Server

### Panoramica del plug-in SnapCenter per Microsoft SQL Server

Il plug-in SnapCenter per Microsoft SQL Server è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni dei database Microsoft SQL Server. Il plug-in per SQL Server automatizza le operazioni di backup, verifica, ripristino e clonazione del database SQL Server nel tuo ambiente SnapCenter .

Una volta installato il plug-in per SQL Server, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replicazione di backup da disco a disco per conformità agli standard o per scopi di archiviazione.

- Automatizza le operazioni di backup, ripristino e clonazione basate sulle applicazioni per i database Microsoft SQL Server nel tuo ambiente SnapCenter .
- Supporta i database Microsoft SQL Server su VMDK e LUN RDM (raw device mapping) quando si distribuisce il SnapCenter Plug-in for VMware vSphere e si registra il plug-in con SnapCenter
- Supporta solo il provisioning delle condivisioni SMB. Non è previsto il supporto per il backup dei database SQL Server su condivisioni SMB.
- Supporta l'importazione di backup da SnapManager per Microsoft SQL Server a SnapCenter.

### Cosa puoi fare con il plug-in SnapCenter per Microsoft SQL Server

Una volta installato il plug-in SnapCenter per Microsoft SQL Server nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database SQL Server.

È possibile eseguire le seguenti attività che supportano operazioni di backup, operazioni di ripristino e operazioni di clonazione di database e risorse di database di SQL Server:

- Eseguire il backup dei database di SQL Server e dei registri delle transazioni associati

  Non è possibile creare un backup del log per i database di sistema master e msdb. Tuttavia, è possibile creare backup del log per il database del sistema modello.

- Ripristinare le risorse del database
  - È possibile ripristinare i database di sistema master, i database di sistema msdb e i database di sistema modello.
  - Non è possibile ripristinare più database, istanze e gruppi di disponibilità.
  - Non è possibile ripristinare il database di sistema in un percorso alternativo.
- Creare cloni point-in-time dei database di produzione

  Non è possibile eseguire operazioni di backup, ripristino, clonazione e ciclo di vita della clonazione sui database di sistema tempdb.

- Verificare immediatamente le operazioni di backup o rimandare la verifica a un momento successivo

  La verifica del database di sistema SQL Server non è supportata. SnapCenter clona i database per eseguire operazioni di verifica. SnapCenter non può clonare i database di sistema di SQL Server e pertanto la verifica di questi database non è supportata.

- Pianificare le operazioni di backup e le operazioni di clonazione
- Monitorare le operazioni di backup, ripristino e clonazione

Il plug-in per SQL Server non supporta il backup e il ripristino dei database SQL Server su condivisioni SMB.

## Funzionalità del plug-in SnapCenter per Microsoft SQL Server

Il plug-in per SQL Server si integra con Microsoft SQL Server sull'host Windows e con la tecnologia NetApp Snapshot sul sistema di storage. Per lavorare con il plug-in per SQL Server, utilizzare l'interfaccia SnapCenter .

Il plug-in per SQL Server include le seguenti funzionalità principali:

- **Interfaccia utente grafica unificata basata su SnapCenter**

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare processi di backup e ripristino coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in. SnapCenter offre inoltre una pianificazione centralizzata e una gestione delle policy per supportare le operazioni di backup e clonazione.

- **Amministrazione centrale automatizzata**

  È possibile pianificare backup di routine di SQL Server, configurare la conservazione dei backup basata su criteri e impostare operazioni di ripristino puntuali e aggiornate al minuto. È anche possibile monitorare in modo proattivo l'ambiente SQL Server configurando SnapCenter per l'invio di avvisi tramite e-mail.

- **Tecnologia NetApp Snapshot non disruptiva**

  Il plug-in per SQL Server utilizza la tecnologia NetApp Snapshot con il plug-in NetApp SnapCenter per Microsoft Windows. Ciò consente di eseguire il backup dei database in pochi secondi e di ripristinarli rapidamente senza dover disconnettere SQL Server. Gli snapshot occupano uno spazio di archiviazione minimo.

Oltre a queste funzionalità principali, il plug-in per SQL Server offre i seguenti vantaggi:

- Supporto per il flusso di lavoro di backup, ripristino, clonazione e verifica
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli
- Creazione di copie point-in-time e a basso consumo di spazio dei database di produzione per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È richiesta una licenza FlexClone sul sistema di archiviazione che contiene il clone.

- Verifica del backup automatizzata e non distruttiva

- Possibilità di eseguire più backup contemporaneamente su più server
- Cmdlet di PowerShell per la creazione di script per operazioni di backup, verifica, ripristino e clonazione
- Supporto per gruppi di disponibilità AlwaysOn (AG) in SQL Server per accelerare le operazioni di configurazione, backup e ripristino degli AG
- Database in memoria e Buffer Pool Extension (BPE) come parte di SQL Server 2014
- Supporto per il backup di LUN e dischi di macchine virtuali (VMDK)
- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per iSCSI, Fibre Channel, FCoE, raw device mapping (RDM) e VMDK su NFS e VMFS

> I volumi NAS dovrebbero avere una politica di esportazione predefinita nella macchina virtuale di archiviazione (SVM).

- Supporto per FileStream e file group nei database autonomi di SQL Server.
- Supporto per la memoria non volatile express (NVMe) su Windows Server 2022
  - Flussi di lavoro di backup, ripristino, clonazione e verifica su layout VMDK creati su NVMe tramite TCP/IP.
  - Supporta il firmware NVMe versione 1.3 a partire dall'aggiornamento 2 di ESX 8.0 e richiede l'hardware virtuale versione 21.
  - Windows Server Failover Clustering (WSFC) non è supportato per le applicazioni su VMDK su NVMe su TCP/IP.
- Supporta la sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]) che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

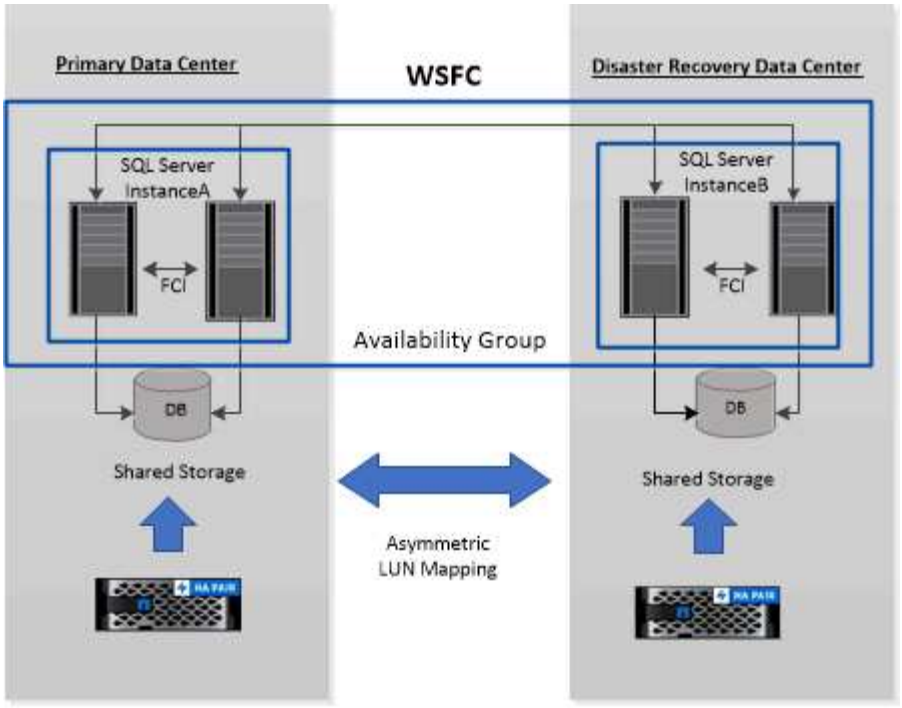
## Supporto per il mapping LUN asimmetrico nei cluster Windows

Il plug-in SnapCenter per Microsoft SQL Server supporta l'individuazione in SQL Server 2012 e versioni successive, configurazioni ALM (Asymmetric LUN Mapping) per elevata disponibilità e gruppi di disponibilità per il ripristino di emergenza. Durante la scoperta delle risorse, SnapCenter rileva i database sugli host locali e sugli host remoti nelle configurazioni ALM.

Una configurazione ALM è un singolo cluster di failover del server Windows che contiene uno o più nodi in un data center primario e uno o più nodi in un centro di ripristino di emergenza.

Di seguito è riportato un esempio di configurazione ALM:

- Due istanze di cluster di failover (FCI) in un data center multi-sito
- FCI per alta disponibilità locale (HA) e gruppo di disponibilità (AG) per il ripristino di emergenza con un'istanza autonoma nel sito di ripristino di emergenza




WSFC----Windows Server Failover Cluster

Lo storage nel data center primario è condiviso tra i nodi FCI presenti nel data center primario. Lo storage nel data center di disaster recovery è condiviso tra i nodi FCI presenti nel data center di disaster recovery.

Lo storage nel datacenter primario non è visibile ai nodi nel datacenter di disaster recovery e viceversa.

L'architettura ALM combina due soluzioni di storage condivise utilizzate da FCI con una soluzione di storage non condivisa o dedicata utilizzata da SQL AG. La soluzione AG utilizza lettere di unità identiche per le risorse disco condivise nei data center. Questa disposizione di archiviazione, in cui un disco del cluster è condiviso tra un sottoinsieme di nodi all'interno di un WSFC, è denominata ALM.

## Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft SQL Server

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali. Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il supporto per il provisioning e la protezione dei dati SnapCenter è disponibile su Windows Server. Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
|---|---|---|---|
| Server fisico | LUN connesse a FC | Interfaccia utente grafica (GUI) SnapCenter o cmdlet di PowerShell | |

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
|---|---|---|---|
| Server fisico | LUN connesse tramite iSCSI | Cmdlet GUI di SnapCenter o PowerShell | |
| Server fisico | Condivisioni SMB3 (CIFS) residenti su una macchina virtuale di archiviazione (SVM) | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning. |
| VMware VM | LUN RDM connesse tramite un HBA FC o iSCSI | Cmdlet di PowerShell | |
| VMware VM | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | |
| VMware VM | Sistemi di file di macchine virtuali (VMFS) o datastore NFS | VMware vSphere | |
| VMware VM | Un sistema guest connesso a condivisioni SMB3 residenti su una SVM | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning. |
| VMware VM | Datastore vVol sia su NFS che su SAN | Strumenti ONTAP per VMware vSphere | |
| Macchina virtuale Hyper-V | LUN FC virtuali (vFC) connesse tramite uno switch Fibre Channel virtuale | Cmdlet GUI di SnapCenter o PowerShell | È necessario utilizzare Hyper-V Manager per eseguire il provisioning di LUN Virtual FC (vFC) connesse tramite uno switch Fibre Channel virtuale.<br>I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
|---|---|---|---|
| Macchina virtuale Hyper-V | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |
| Macchina virtuale Hyper-V | Un sistema guest connesso a condivisioni SMB3 residenti su una SVM | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning.<br>I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |

## Raccomandazioni sul layout di archiviazione per il plug-in SnapCenter per Microsoft SQL Server

Un layout di archiviazione ben progettato consente a SnapCenter Server di eseguire il backup dei database per soddisfare gli obiettivi di ripristino. Quando si definisce il layout di archiviazione, è necessario considerare diversi fattori, tra cui le dimensioni del database, la velocità di modifica del database e la frequenza con cui si eseguono i backup.

Nelle sezioni seguenti vengono definiti i consigli e le restrizioni sul layout di archiviazione per LUN e dischi di macchine virtuali (VMDK) con il plug-in SnapCenter per Microsoft SQL Server installato nel tuo ambiente.

In questo caso, le LUN possono includere dischi VMware RDM e LUN collegate direttamente iSCSI mappate sul guest.

### Requisiti LUN e VMDK

Facoltativamente, è possibile utilizzare LUN o VMDK dedicati per prestazioni e gestione ottimali dei seguenti database:

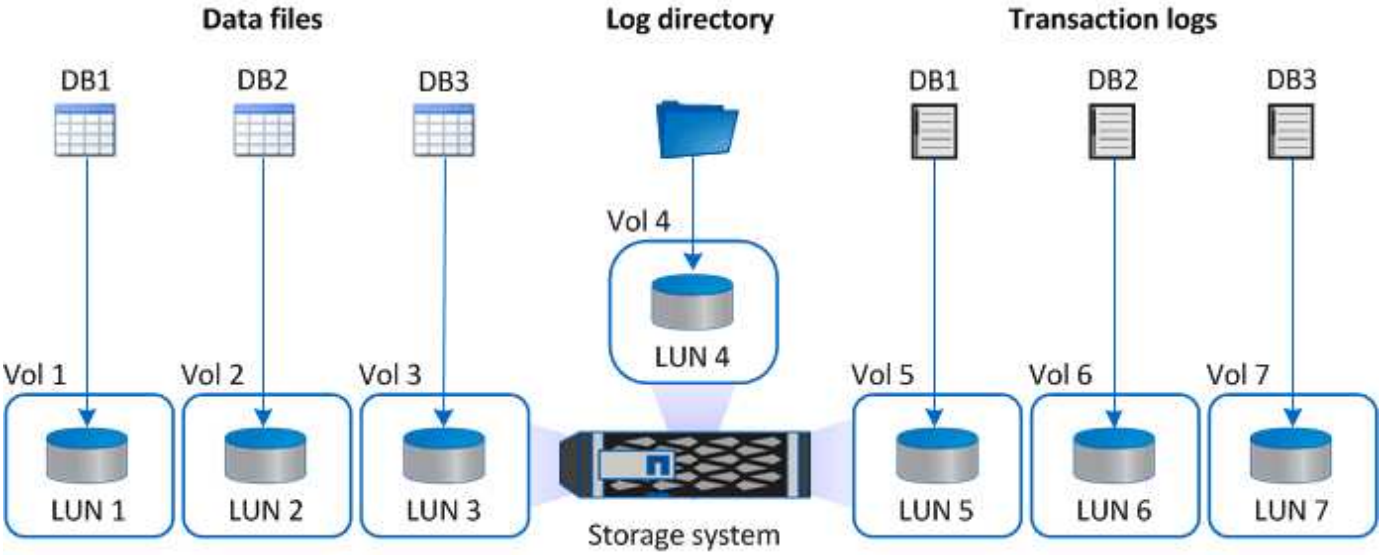
- Database di sistema master e modello
- Database temporaneo
- File di database utente (.mdf e .ndf)
- File di registro delle transazioni del database utente (.ldf)
- Directory dei registri

Per ripristinare database di grandi dimensioni, la procedura consigliata è quella di utilizzare LUN o VMDK dedicati. Il tempo impiegato per ripristinare un LUN o un VMDK completo è inferiore al tempo impiegato per ripristinare i singoli file archiviati nel LUN o nel VMDK.

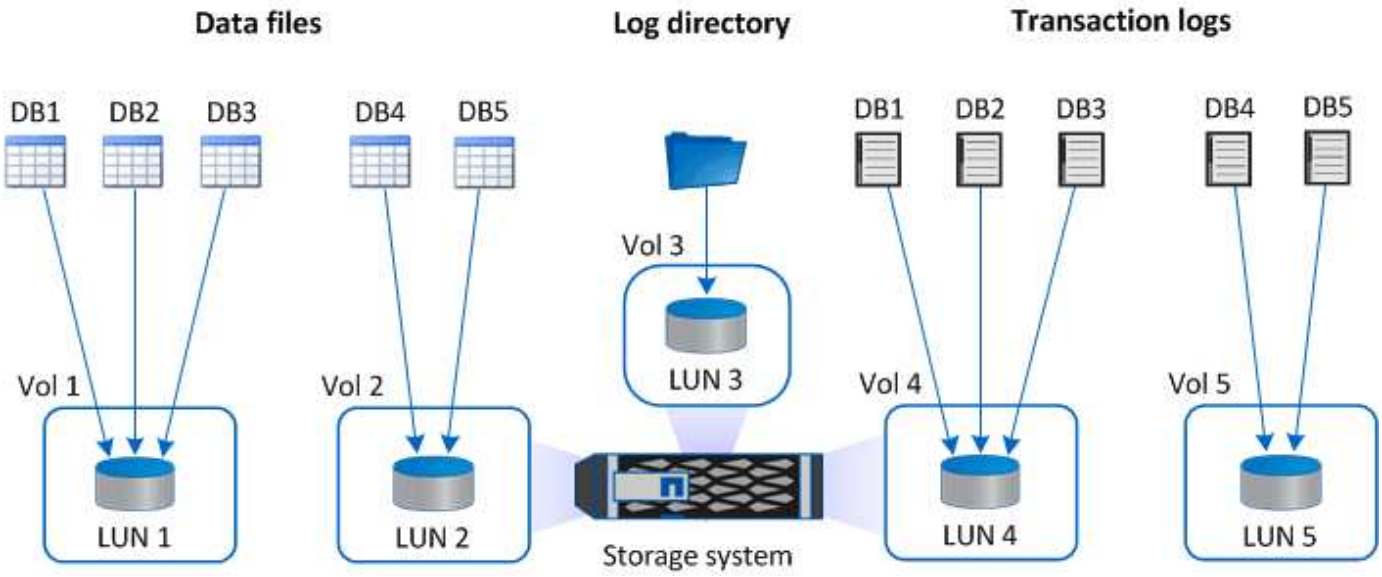
Per la directory del registro, è necessario creare un LUN o un VMDK separato in modo che vi sia spazio libero sufficiente nei dischi dei file di dati o di registro.

### Layout di esempio LUN e VMDK

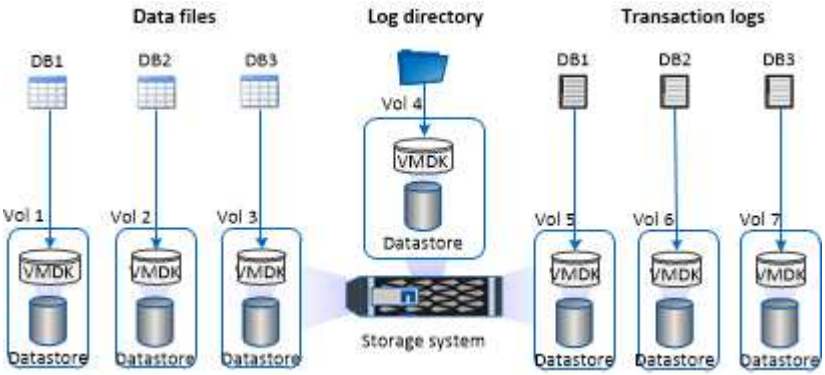
Il seguente grafico mostra come configurare il layout di archiviazione per database di grandi dimensioni su LUN:



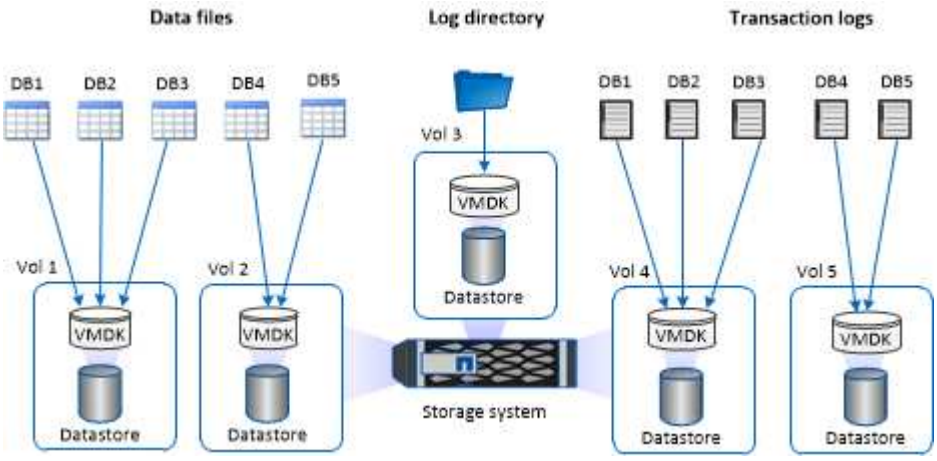

Il seguente grafico mostra come configurare il layout di archiviazione per database di medie o piccole dimensioni su LUN:




Il seguente grafico mostra come configurare il layout di archiviazione per database di grandi dimensioni su VMDK:




Il seguente grafico mostra come configurare il layout di archiviazione per database di medie o piccole dimensioni su VMDK:




## Privilegi ONTAP minimi richiesti per il plug-in SQL

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun cancella
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina
  - rinomina lun igroup
  - spettacolo di gruppo lun
  - mappatura lun aggiungi-nodi-di-segnalazione
  - creazione di mappatura lun
  - eliminazione della mappatura LUN
  - rimozione-nodi-di-segnalazione-mapping-lun
  - spettacolo di mappatura lun
  - lun modifica
  - lun sposta-in-volume
  - lun offline
  - lun online
  - ridimensionamento lun
  - serie lun
  - spettacolo di lunedì
  - aggiunta regola politica snapmirror
  - modifica regola policy snapmirror
  - regola di rimozione della policy di SnapMirror
  - mostra politica di SnapMirror
  - ripristino snapmirror
  - spettacolo snapmirror
  - snapmirror mostra-cronologia
  - aggiornamento snapmirror
  - snapmirror update-ls-set
  - elenco-destinazioni snapmirror
  - versione
  - creazione di cloni di volume
  - spettacolo di clonazione del volume

- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online
- modifica del volume
- creazione di volume qtree
- eliminazione del volume qtree
- modifica del volume qtree
- volume qtree mostra
- limitazione del volume
- spettacolo di volume
- creazione di snapshot del volume
- eliminazione snapshot volume
- modifica snapshot volume
- rinomina snapshot volume
- ripristino snapshot del volume
- file di ripristino dello snapshot del volume
- mostra snapshot del volume
- smontare il volume
- server virtuale cifs
- vserver cifs share create
- vserver cifs share delete
- vserver cifs shadowcopy mostra
- vserver cifs share show
- spettacolo cifs del server virtuale
- politica di esportazione del server virtuale
- creazione di criteri di esportazione vserver
- eliminazione della policy di esportazione del server virtuale
- creazione regola policy di esportazione vserver
- regola di esportazione-politica del vserver mostra
- mostra politica di esportazione vserver
- server virtuale iscsi
- visualizzazione della connessione vserver iscsi

- spettacolo vserver
- interfaccia di rete
- mostra interfaccia di rete
- server virtuale
- spettacolo metrocluster

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per il plug-in per SQL Server

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter . Se si utilizza SnapMirror ActiveSync, utilizzare le pianificazioni predefinite SnapMirror o SnapVault sia per SnapMirror ActiveSync che per le relazioni asincrone.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Strategia di backup per le risorse di SQL Server

### Definire una strategia di backup per le risorse di SQL Server

Definire una strategia di backup prima di creare i processi di backup aiuta a garantire di disporre dei backup necessari per ripristinare o clonare correttamente i database. Il Service Level Agreement (SLA), il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO) determinano in larga misura la strategia di backup.

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di backup.

**Tipo di backup supportati**

Per eseguire il backup dei database utente e di sistema di SQL Server tramite SnapCenter, è necessario scegliere il tipo di risorsa, ad esempio database, istanze di SQL Server e gruppi di disponibilità (AG). La tecnologia snapshot viene sfruttata per creare copie online di sola lettura dei volumi su cui risiedono le risorse.

È possibile selezionare l'opzione di sola copia per specificare che SQL Server non tronchi i registri delle transazioni. È consigliabile utilizzare questa opzione quando si gestisce SQL Server anche con altre applicazioni di backup. Mantenere intatti i registri delle transazioni consente a qualsiasi applicazione di backup di ripristinare i database di sistema. I backup di sola copia sono indipendenti dalla sequenza dei backup pianificati e non influiscono sulle procedure di backup e ripristino del database.

| Tipo di backup | Descrizione | Opzione di sola copia con tipo di backup |
|---|---|---|
| Backup completo e backup del registro | Esegue il backup del database di sistema e tronca i registri delle transazioni.<br><br>SQL Server tronca i registri delle transazioni rimuovendo le voci già salvate nel database.<br><br>Una volta completato il backup completo, questa opzione crea un registro delle transazioni che cattura le informazioni sulle transazioni. In genere, dovresti scegliere questa opzione. Tuttavia, se il tempo di backup è breve, è possibile scegliere di non eseguire un backup del registro delle transazioni con un backup completo.<br><br>Non è possibile creare un backup del log per i database di sistema master e msdb. Tuttavia, è possibile creare backup del log per il database del sistema modello. | Esegue il backup dei file del database di sistema e dei registri delle transazioni senza troncare i registri.<br><br>Un backup di sola copia non può fungere da base differenziale o backup differenziale e non influisce sulla base differenziale. Il ripristino di un backup completo di sola copia è uguale al ripristino di qualsiasi altro backup completo. |
| Backup completo del database | Esegue il backup dei file del database di sistema.<br><br>È possibile creare un backup completo del database per i database di sistema master, model e msdb. | Esegue il backup dei file del database di sistema. |

| Tipo di backup | Descrizione | Opzione di sola copia con tipo di backup |
| --- | --- | --- |
| Backup del registro delle transazioni | Esegue il backup dei registri delle transazioni troncati, copiando solo le transazioni eseguite dopo il backup del registro delle transazioni più recente.<br><br>Se si pianificano backup frequenti del registro delle transazioni insieme a backup completi del database, è possibile scegliere punti di ripristino granulari. | Esegue il backup dei registri delle transazioni senza troncarli.<br><br>Questo tipo di backup non influisce sulla sequenza dei backup regolari del registro. I backup del log di sola copia sono utili per eseguire operazioni di ripristino online. |

**Pianificazioni di backup per il plug-in per SQL Server**

La frequenza del backup (tipo di pianificazione) è specificata nei criteri; una pianificazione del backup è specificata nella configurazione del gruppo di risorse. Il fattore più critico nella determinazione della frequenza o della pianificazione di un backup è la velocità di modifica della risorsa e l'importanza dei dati. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. L'SLA e l'RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, potrebbero essere sufficienti backup regolari del registro delle transazioni per garantire di disporre dei backup necessari. Quanto più spesso si esegue il backup dei database, tanto minore sarà il numero di registri delle transazioni che SnapCenter dovrà utilizzare al momento del ripristino, il che può comportare operazioni di ripristino più rapide.

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup

  La frequenza di backup (la frequenza con cui devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte della configurazione di una policy. È possibile selezionare la frequenza di backup oraria, giornaliera, settimanale o mensile per la policy. Se non si seleziona nessuna di queste frequenze, la policy creata sarà una policy solo on-demand. È possibile accedere alle policy facendo clic su **Impostazioni** > **Policy**.

- Pianificazioni di backup

  Le pianificazioni dei backup (ovvero quando devono essere eseguiti esattamente) fanno parte della configurazione di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per backup settimanali, è possibile configurare la pianificazione in modo che il backup venga

eseguito ogni giovedì alle 22:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **Risorse** > **Gruppi di risorse**.

#### Numero di processi di backup necessari per i database

I fattori che determinano il numero di processi di backup necessari includono le dimensioni del database, il numero di volumi utilizzati, la frequenza di modifica del database e il contratto di servizio (SLA).

Per i backup del database, il numero di processi di backup scelti dipende in genere dal numero di volumi su cui sono posizionati i database. Ad esempio, se si posiziona un gruppo di database di piccole dimensioni su un volume e un database di grandi dimensioni su un altro volume, è possibile creare un processo di backup per i database di piccole dimensioni e un processo di backup per il database di grandi dimensioni.

#### Convenzioni di denominazione del backup per il plug-in per SQL Server

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

#### Opzioni di conservazione del backup per il plug-in per SQL Server

È possibile scegliere il numero di giorni per cui conservare le copie di backup oppure specificare il numero di copie di backup che si desidera conservare, fino a un massimo ONTAP di 255 copie. Ad esempio, la tua organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica SnapMirror , il criterio di conservazione viene replicato sul volume di destinazione.

SnapCenter elimina i backup conservati che hanno etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero comunque rimanere sul sistema.

Per la conservazione a lungo termine delle copie di backup, è consigliabile utilizzare il backup SnapVault .

**Per quanto tempo conservare i backup del registro delle transazioni sul sistema di archiviazione di origine**

Il plug-in SnapCenter per Microsoft SQL Server necessita di backup del registro delle transazioni per eseguire operazioni di ripristino aggiornate al minuto, che ripristinano il database a un orario compreso tra due backup completi.

Ad esempio, se Plug-in per SQL Server ha eseguito un backup completo alle 8:00 e un altro backup completo alle 17:00, potrebbe utilizzare l'ultimo backup del registro delle transazioni per ripristinare il database a un orario qualsiasi compreso tra le 8:00 e le 17:00. Se i registri delle transazioni non sono disponibili, Plug-in per SQL Server può eseguire solo operazioni di ripristino temporizzato, che ripristinano un database all'orario in cui Plug-in per SQL Server ha completato un backup completo.

In genere, sono necessarie operazioni di ripristino aggiornate solo per uno o due giorni. Per impostazione predefinita, SnapCenter conserva un minimo di due giorni.

**Più database sullo stesso volume**

È possibile posizionare tutti i database sullo stesso volume, poiché la policy di backup prevede un'opzione per impostare il numero massimo di database per backup (il valore predefinito è 100).

Ad esempio, se si hanno 200 database nello stesso volume, vengono creati due snapshot con 100 database in ciascuno dei due snapshot.

**Verifica della copia di backup tramite il volume di archiviazione primario o secondario per il plug-in per SQL Server**

È possibile verificare le copie di backup sul volume di archiviazione primario o sul volume di archiviazione secondario SnapMirror o SnapVault . La verifica tramite un volume di archiviazione secondario riduce il carico sul volume di archiviazione primario.

Quando si verifica un backup presente sul volume di archiviazione primario o secondario, tutti gli snapshot primari e secondari vengono contrassegnati come verificati.

Per verificare le copie di backup sui volumi di archiviazione secondari SnapMirror e SnapVault è necessaria la licenza SnapRestore .

**Quando pianificare i lavori di verifica**

Sebbene SnapCenter possa verificare i backup subito dopo averli creati, questa operazione può aumentare significativamente il tempo necessario per completare il processo di backup e richiede molte risorse. Pertanto, è quasi sempre meglio

programmare la verifica in un lavoro separato, da svolgere in un secondo momento. Ad esempio, se esegui il backup di un database alle 17:00 ogni giorno, potresti pianificare la verifica in modo che avvenga un'ora dopo, alle 18:00.

Per lo stesso motivo, solitamente non è necessario eseguire la verifica del backup ogni volta che si esegue un backup. Di solito, per garantire l'integrità del backup è sufficiente eseguire la verifica a intervalli regolari ma meno frequenti. Un singolo processo di verifica può verificare più backup contemporaneamente.

## Strategia di ripristino per SQL Server

### Origini e destinazioni per un'operazione di ripristino

È possibile ripristinare un database SQL Server da una copia di backup su un archivio primario o secondario. È anche possibile ripristinare il database in destinazioni diverse oltre alla sua posizione originale, consentendo di scegliere la destinazione che supporta le proprie esigenze.

#### Fonti per un'operazione di ripristino

È possibile ripristinare i database dall'archiviazione primaria o secondaria.

#### Destinazioni per un'operazione di ripristino

È possibile ripristinare i database in diverse destinazioni:

| Destinazione | Descrizione |
|---|---|
| La posizione originale | Per impostazione predefinita, SnapCenter ripristina il database nella stessa posizione sulla stessa istanza di SQL Server. |
| Una posizione diversa | È possibile ripristinare il database in una posizione diversa su qualsiasi istanza di SQL Server all'interno dello stesso host. |
| Posizione originale o diversa utilizzando nomi di database diversi | È possibile ripristinare il database con un nome diverso su qualsiasi istanza di SQL Server sullo stesso host in cui è stato creato il backup. |

Il ripristino su host alternativi tra server ESX per database SQL su VMDK (datastore NFS e VMFS) non è supportato.

### Modelli di ripristino di SQL Server supportati da SnapCenter

Per impostazione predefinita, a ciascun tipo di database vengono assegnati modelli di ripristino specifici. L'amministratore del database SQL Server può riassegnare ciascun database a un modello di recupero diverso.

SnapCenter supporta tre tipi di modelli di ripristino di SQL Server:

- Modello di recupero semplice

  Quando si utilizza il modello di recupero semplice, non è possibile eseguire il backup dei registri delle transazioni.

- Modello di recupero completo

  Utilizzando il modello di recupero completo, è possibile ripristinare un database allo stato precedente al momento dell'errore.

- Modello di recupero con registrazione in blocco

  Quando si utilizza il modello di recupero con registrazione in blocco, è necessario eseguire nuovamente manualmente l'operazione di registrazione in blocco. È necessario eseguire l'operazione di registrazione in blocco se il registro delle transazioni contenente il record di commit dell'operazione non è stato sottoposto a backup prima del ripristino. Se l'operazione di registrazione in blocco inserisce 10 milioni di righe in un database e il database si blocca prima che venga eseguito il backup del registro delle transazioni, il database ripristinato non conterrà le righe inserite dall'operazione di registrazione in blocco.

### Tipi di operazioni di ripristino

È possibile utilizzare SnapCenter per eseguire diversi tipi di operazioni di ripristino sulle risorse di SQL Server.

- Ripristinare all'ultimo minuto
- Ripristina un punto precedente nel tempo

È possibile ripristinare fino al minuto precedente o ripristinare un punto precedente nel tempo nelle seguenti situazioni:

- Ripristina da SnapMirror o SnapVault , archivio secondario
- Ripristina il percorso alternativo (posizione)

SnapCenter non supporta SnapRestore basato sul volume.

#### Ripristina fino al minuto

In un'operazione di ripristino immediato (selezionata per impostazione predefinita), i database vengono ripristinati fino al punto di errore. SnapCenter realizza questo risultato eseguendo la seguente sequenza:

1. Esegue il backup dell'ultimo registro delle transazioni attive prima di ripristinare il database.
2. Ripristina i database dal backup completo del database selezionato.
3. Applica tutti i registri delle transazioni che non sono stati salvati nei database (inclusi i registri delle transazioni dei backup dal momento in cui è stato creato il backup fino al momento più recente).

   I registri delle transazioni vengono spostati in avanti e applicati a tutti i database selezionati.

Un'operazione di ripristino aggiornata richiede un set contiguo di registri delle transazioni.

Poiché SnapCenter non è in grado di ripristinare i log delle transazioni del database SQL Server dai file di backup del log shipping (il log shipping consente di inviare automaticamente i backup del log delle transazioni

da un database primario su un'istanza del server primario a uno o più database secondari su istanze del server secondario separate), non è possibile eseguire un'operazione di ripristino aggiornata dai backup del log delle transazioni. Per questo motivo, dovresti utilizzare SnapCenter per eseguire il backup dei file di registro delle transazioni del database SQL Server.

Se non è necessario mantenere la capacità di ripristino aggiornata per tutti i backup, è possibile configurare la conservazione del backup del registro delle transazioni del sistema tramite i criteri di backup.

#### Esempio di un'operazione di ripristino aggiornata

Supponiamo di eseguire il backup di SQL Server ogni giorno a mezzogiorno e di dover eseguire il ripristino da un backup mercoledì alle 16:00. Per qualche motivo, la verifica del backup di mercoledì a mezzogiorno non è riuscita, quindi decidi di ripristinare dal backup di martedì a mezzogiorno. Dopodiché, se il backup viene ripristinato, tutti i registri delle transazioni vengono spostati in avanti e applicati ai database ripristinati, iniziando da quelli che non erano stati salvati quando è stato creato il backup di martedì e continuando fino all'ultimo registro delle transazioni scritto mercoledì alle 16:00 (se è stato eseguito il backup dei registri delle transazioni).

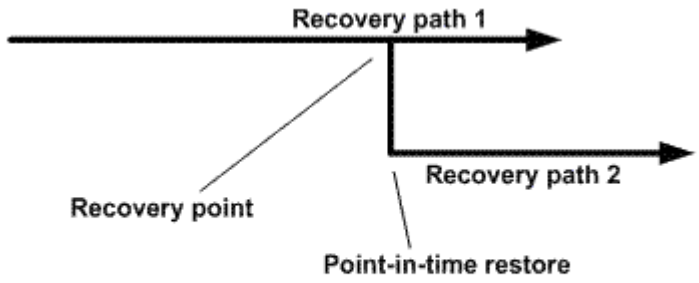
#### Ripristina un punto precedente nel tempo

In un'operazione di ripristino point-in-time, i database vengono ripristinati solo a un momento specifico del passato. Un'operazione di ripristino point-in-time si verifica nelle seguenti situazioni di ripristino:

- Il database viene ripristinato a un orario specificato in un registro delle transazioni sottoposto a backup.
- Il database viene ripristinato e ad esso viene applicato solo un sottoinsieme dei registri delle transazioni sottoposti a backup.

Il ripristino di un database a un punto nel tempo determina la creazione di un nuovo percorso di ripristino.

L'immagine seguente illustra i problemi che si verificano quando viene eseguita un'operazione di ripristino in un dato momento:




Nell'immagine, il percorso di ripristino 1 è costituito da un backup completo seguito da diversi backup del registro delle transazioni. Si ripristina il database a un punto nel tempo. Dopo l'operazione di ripristino point-in-time vengono creati nuovi backup del registro delle transazioni, che determina il percorso di ripristino 2. I nuovi backup del registro delle transazioni vengono creati senza creare un nuovo backup completo. A causa del danneggiamento dei dati o di altri problemi, non è possibile ripristinare il database corrente finché non viene creato un nuovo backup completo. Inoltre, non è possibile applicare i registri delle transazioni creati nel percorso di ripristino 2 al backup completo appartenente al percorso di ripristino 1.

Se si applicano backup del registro delle transazioni, è anche possibile specificare una data e un'ora specifiche in cui si desidera interrompere l'applicazione delle transazioni sottoposte a backup. Per fare ciò, basta specificare una data e un'ora comprese nell'intervallo disponibile e SnapCenter rimuoverà tutte le transazioni non eseguite prima di quel momento. È possibile utilizzare questo metodo per ripristinare i database a un punto nel tempo precedente al verificarsi di un danneggiamento oppure per ripristinare un database o una tabella eliminati accidentalmente.

#### Esempio di un'operazione di ripristino point-in-time

Supponiamo di eseguire backup completi del database una volta a mezzanotte e un backup del registro delle transazioni ogni ora. Il database si blocca alle 9:45, ma si esegue comunque il backup dei registri delle transazioni del database in errore. È possibile scegliere tra questi scenari di ripristino temporizzato:

- Ripristinare il backup completo del database effettuato a mezzanotte e accettare la perdita delle modifiche apportate al database successivamente. (Opzione: Nessuna)
- Ripristina il backup completo del database e applica tutti i backup del registro delle transazioni fino alle 9:45 (opzione: Registra fino a)
- Ripristina il backup completo del database e applica i backup del registro delle transazioni, specificando l'ora in cui desideri che le transazioni vengano ripristinate dall'ultimo set di backup del registro delle transazioni. (Opzione: entro un orario specifico)

In questo caso, dovresti calcolare la data e l'ora in cui è stato segnalato un determinato errore. Tutte le transazioni non eseguite prima della data e dell'ora specificate verranno rimosse.

## Definire una strategia di clonazione per SQL Server

Definire una strategia di clonazione consente di clonare il database con successo.

1. Esaminare le limitazioni relative alle operazioni di clonazione.
2. Decidi il tipo di clone di cui hai bisogno.

#### Limitazioni delle operazioni di clonazione

Prima di clonare i database, è necessario essere consapevoli dei limiti delle operazioni di clonazione.

- Se si utilizza una versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di clonazione sarà bloccata quando si esegue il comando *renamedg*. Per risolvere questo problema, è possibile applicare la patch Oracle 19544733.
- La clonazione di database da una LUN direttamente collegata a un host (ad esempio, utilizzando Microsoft iSCSI Initiator su un host Windows) a un VMDK o a una LUN RDM sullo stesso host Windows o su un altro host Windows, o viceversa, non è supportata.
- La directory radice del punto di montaggio del volume non può essere una directory condivisa.
- Se si sposta una LUN contenente un clone in un nuovo volume, il clone non potrà essere eliminato.

#### Tipi di operazioni di clonazione

È possibile utilizzare SnapCenter per clonare un backup del database SQL Server o un database di produzione.

- Clonazione da un backup del database

  Il database clonato può fungere da base per lo sviluppo di nuove applicazioni e aiutare a isolare gli errori

applicativi che si verificano nell'ambiente di produzione. Il database clonato può essere utilizzato anche per il ripristino da errori software del database.

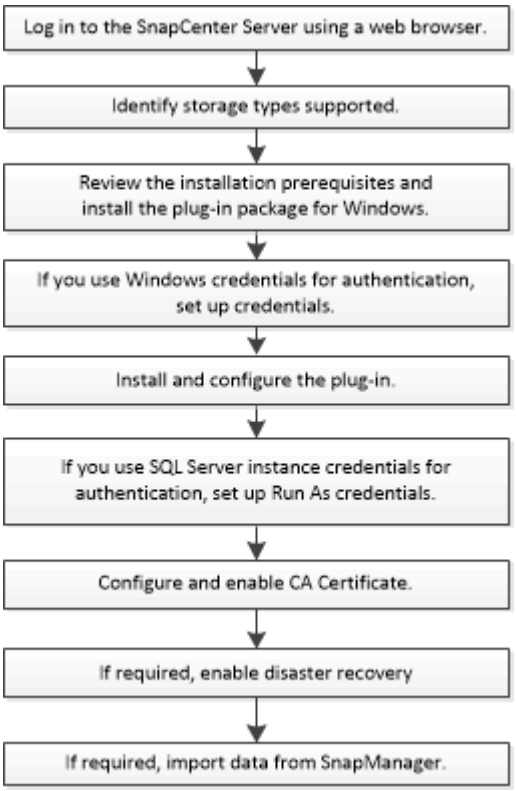
- Ciclo di vita del clone

  È possibile utilizzare SnapCenter per pianificare attività di clonazione ricorrenti che verranno eseguite quando il database di produzione non è occupato.

# Prepararsi all'installazione del plug-in SnapCenter per Microsoft SQL Server

## Flusso di lavoro di installazione per il plug-in SnapCenter per Microsoft SQL Server

Se si desidera proteggere i database di SQL Server, è necessario installare e configurare il plug-in SnapCenter per Microsoft SQL Server.




## Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft SQL Server

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario disporre di un utente con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.

- È necessario disporre di un utente con autorizzazioni di amministratore di sistema su SQL Server.

  Il plug-in SnapCenter per Microsoft SQL Server utilizza Microsoft VDI Framework, che richiede l'accesso come amministratore di sistema.

  "Articolo del supporto Microsoft 2926557: le operazioni di backup e ripristino di SQL Server VDI richiedono privilegi di amministratore di sistema"

- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- Se SnapManager per Microsoft SQL Server è installato, è necessario aver arrestato o disabilitato il servizio e le pianificazioni.

  Se si prevede di importare processi di backup o clonazione in SnapCenter, non disinstallare SnapManager per Microsoft SQL Server.

- L'host deve essere risolvibile nel nome di dominio completo (FQDN) dal server.

  Se il file hosts viene modificato per renderlo risolvibile e se sia il nome breve che l'FQDN sono specificati nel file hosts, creare una voce nel file hosts SnapCenter nel seguente formato: <indirizzo_ip> <fqdn_host> <nome_host>

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br><br>Java 11 Oracle Java e OpenJDK sono richiesti solo per SAP HANA, IBM Db2, PostgreSQL, MySQL, i plug-in supportati NetApp e altre applicazioni personalizzate che possono essere installate su host Windows.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Imposta le credenziali per il pacchetto plug-in SnapCenter per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su database o file system Windows.

**Prima di iniziare**

- Prima di installare i plug-in è necessario impostare le credenziali di Windows.
- È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.
- Autenticazione SQL su host Windows

  Dopo aver installato i plug-in, è necessario impostare le credenziali SQL.

  Se si distribuisce il plug-in SnapCenter per Microsoft SQL Server, è necessario impostare le credenziali SQL dopo aver installato i plug-in. Impostare le credenziali per un utente con autorizzazioni di amministratore di sistema di SQL Server.

  Il metodo di autenticazione SQL esegue l'autenticazione su un'istanza di SQL Server. Ciò significa che un'istanza di SQL Server deve essere individuata in SnapCenter. Pertanto, prima di aggiungere una credenziale SQL, è necessario aggiungere un host, installare pacchetti plug-in e aggiornare le risorse. Per eseguire operazioni quali la pianificazione o l'individuazione di risorse è necessaria l'autenticazione di SQL Server.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.

2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per la credenziale. |
| Nome utente/Password | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio<br>Specificare l'amministratore di dominio sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: `UserName`<br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare. Se si seleziona la modalità di autenticazione SQL, è necessario specificare anche l'istanza del server SQL e l'host in cui si trova l'istanza SQL. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare le credenziali per una singola risorsa di SQL Server

È possibile configurare le credenziali per eseguire processi di protezione dei dati su singole risorse di SQL Server per ciascun utente. Sebbene sia possibile configurare le credenziali a livello globale, potrebbe essere opportuno farlo solo per una risorsa specifica.

**Informazioni su questo compito**

- Se si utilizzano le credenziali di Windows per l'autenticazione, è necessario impostare le credenziali prima di installare i plug-in.

  Tuttavia, se si utilizza un'istanza di SQL Server per l'autenticazione, è necessario aggiungere le credenziali dopo aver installato i plug-in.

- Se hai abilitato l'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database individuato viene visualizzato con un'icona a forma di lucchetto rosso.

  Se viene visualizzata l'icona del lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

- È necessario assegnare le credenziali a un utente con controllo degli accessi basato sui ruoli (RBAC) senza accesso sysadmin quando sono soddisfatte le seguenti condizioni:
  - La credenziale viene assegnata a un'istanza SQL.
  - L'istanza o l'host SQL viene assegnato a un utente RBAC.

    L'utente deve disporre sia dei privilegi di gruppo di risorse che di backup.

**Passaggio 1: aggiungere e configurare le credenziali**

1. Nel riquadro di navigazione a sinistra, seleziona **Impostazioni**.
2. Nella pagina Impostazioni, seleziona **Credenziali**.
   a. Per aggiungere una nuova credenziale, seleziona **Nuovo**.
   b. Nella pagina Credenziali, configura le credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome utente | Immettere il nome utente utilizzato per l'autenticazione di SQL Server.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori Specificare l'amministratore di dominio o qualsiasi membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo **Nome utente** sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro) Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale integrato nel sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo **Nome utente** è: *NomeUtente* |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Selezionare la modalità di autenticazione di SQL Server. È anche possibile scegliere l'autenticazione Windows se l'utente Windows dispone dei privilegi di amministratore di sistema sul server SQL. |
| Ospite | Selezionare l'host. |
| Istanza di SQL Server | Selezionare l'istanza di SQL Server. |

c. Selezionare **OK** per aggiungere le credenziali.

**Passaggio 2: configurare le istanze**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**.
2. Nella pagina Risorse, seleziona **Istanza** dall'elenco **Visualizza**.
   a. Selezionare image::../media/filter_icon.png[icona filtro], quindi selezionare il nome host per filtrare le istanze.
   b. Selezionare image::../media/filter_icon.png[icona filtro] per chiudere il riquadro filtro.
3. Nella pagina Protezione istanza, proteggi l'istanza e, se necessario, seleziona **Configura credenziali**.

   Se l'utente che ha effettuato l'accesso a SnapCenter Server non ha accesso a SnapCenter Plugin per Microsoft SQL Server, dovrà configurare le credenziali.

   L'opzione delle credenziali non si applica ai database e ai gruppi di disponibilità.

4. Seleziona **Aggiorna risorse**.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:
   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Installa il plug-in SnapCenter per Microsoft SQL Server

### Aggiungi host e installa il pacchetto plug-in SnapCenter per Windows

Per aggiungere host e installare il pacchetto plug-in, è necessario utilizzare la pagina **Aggiungi host** SnapCenter . I plug-in vengono installati automaticamente sugli host remoti.

#### Prima di iniziare

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata, è necessario disabilitare UAC sull'host.

- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per SQL"

**Informazioni su questo compito**

Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster. Se si installano i plug-in su un cluster o su Windows Server Failover Clustering (WSFC), i plug-in vengono installati su tutti i nodi del cluster.

Per informazioni sulla gestione degli host, vedere"Gestisci gli host" .

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Selezionare **Aggiungi**.
4. Nella pagina Host procedi come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Selezionare Windows come tipo di host.<br>SnapCenter Server aggiunge l'host e quindi installa il plug-in per Windows se il plug-in non è già installato sull'host.<br><br>Se si seleziona l'opzione Microsoft SQL Server nella pagina Plug-in, SnapCenter Server installa il plug-in per SQL Server. |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. L'indirizzo IP è supportato per gli host di dominio non attendibili solo se si risolve nel nome di dominio completo (FQDN).<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>È possibile immettere gli indirizzi IP o il nome di dominio completo di uno dei seguenti:<br><br>• Host autonomo<br>• WSFC Se si aggiunge un host tramite SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

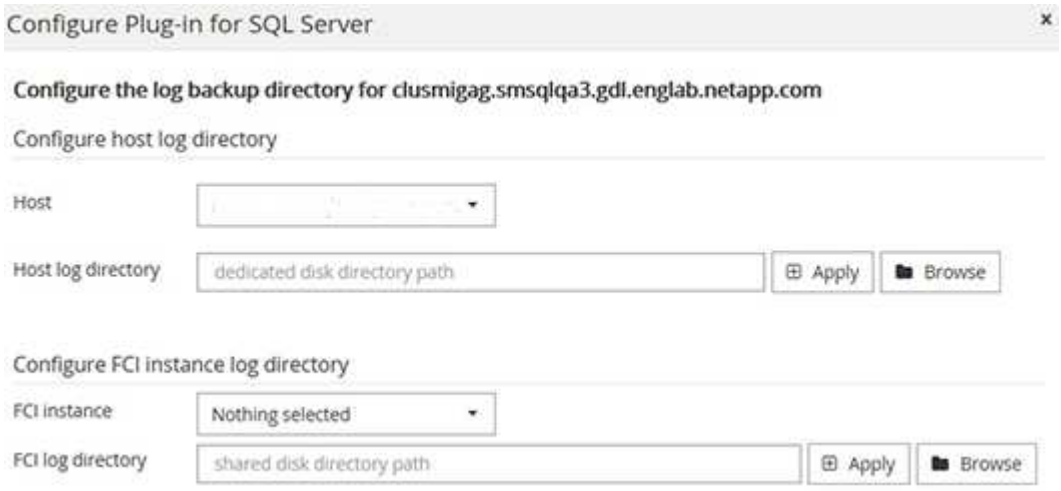
5. Nella sezione **Seleziona i plug-in da installare**, seleziona i plug-in da installare.
6. Seleziona **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, è possibile personalizzare il percorso. |
| Aggiungi tutti gli host nel cluster | Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC o in un gruppo di disponibilità SQL. Se si desidera gestire e identificare più gruppi di disponibilità SQL disponibili all'interno di un cluster, è necessario aggiungere tutti i nodi del cluster selezionando la casella di controllo del cluster appropriata nell'interfaccia utente grafica. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br><br>Fornire il nome gMSA nel seguente formato: domainName\accountName$.<br><br>Se l'host viene aggiunto con gMSA e se gMSA dispone di privilegi di accesso e di amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL. |

7. Seleziona **Invia**.
8. Per il plug-in SQL, selezionare l'host per configurare la directory di registro.
   a. Selezionare **Configura directory di registro** e nella pagina Configura directory di registro host, selezionare **Sfoglia** e completare i seguenti passaggi:

      Sono elencati per la selezione solo i LUN (unità) NetApp . SnapCenter esegue il backup e la replica della directory del registro host come parte dell'operazione di backup.




      i. Selezionare la lettera dell'unità o il punto di montaggio sull'host in cui verrà archiviato il registro dell'host.
      ii. Se necessario, selezionare una sottodirectory.
      iii. Seleziona **Salva**.
9. Seleziona **Invia**.

Se non hai selezionato la casella di controllo **Salta controlli preliminari**, l'host viene convalidato per

verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

10. Monitorare l'avanzamento dell'installazione.

#### Installa il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando i cmdlet

## È possibile installare il plug-in SnapCenter per Microsoft SQL Server su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

#### Prima di iniziare

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

#### Passi

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in SnapCenter per Microsoft SQL Server su più host remoti utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

#### Installare il plug-in SnapCenter per Microsoft SQL Server in modo silenzioso dalla riga di comando

## È necessario installare il plug-in SnapCenter per Microsoft SQL Server dall'interfaccia utente SnapCenter . Tuttavia, se per qualche motivo non è possibile, è possibile eseguire il programma di installazione del plug-in per SQL Server in modalità automatica dalla riga di comando di Windows.

#### Prima di iniziare

- Prima di procedere all'installazione, è necessario eliminare la versione precedente del plug-in SnapCenter per Microsoft SQL Server.

  Per ulteriori informazioni, vedere "Come installare manualmente un plug-in SnapCenter direttamente

dall'host del plug-in" .

**Passi**

1. Verificare se la cartella C:\temp esiste sull'host del plug-in e se l'utente connesso ha pieno accesso ad essa.
2. Scaricare il plug-in per il software SQL Server da C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.
3. Copiare il file di installazione sull'host su cui si desidera installare il plug-in.
4. Da un prompt dei comandi di Windows sull'host locale, accedere alla directory in cui sono stati salvati i file di installazione del plug-in.
5. Installare il plug-in per il software SQL Server:

   ```
   "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
   ```

   Sostituisci i valori segnaposto con i tuoi dati

   - Debug_Log_Path è il nome e il percorso del file di registro del programma di installazione della suite.
   - Log_Path è la posizione dei log di installazione dei componenti del plug-in (SCW, SCSQL e SMCore).
   - Num è la porta su cui SnapCenter comunica con SMCore
   - Install_Directory_Path è la directory di installazione del pacchetto plug-in host.
   - domain\administrator è l'account del servizio Web del plug-in SnapCenter per Microsoft Windows.
   - password è la password per l'account del servizio Web del plug-in SnapCenter per Microsoft Windows.
     ```
     "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
     ```

   Tutti i parametri passati durante l'installazione del plug-in per SQL Server fanno distinzione tra maiuscole e minuscole.
6. Monitorare l'utilità di pianificazione di Windows, il file di registro di installazione principale C:\Installdebug.log e i file di installazione aggiuntivi in C:\Temp.
7. Monitorare la directory %temp% per verificare che i programmi di installazione msiexe.exe installino il software senza errori.

   L'installazione del plug-in per SQL Server registra il plug-in sull'host e non sul server SnapCenter . È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Dopo aver aggiunto l'host, il plug-in viene rilevato automaticamente.

### Monitorare lo stato di installazione del plug-in per SQL Server

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

#### Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

#### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

**Configurare il certificato CA con i servizi plug-in host di Windows**

## È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

#### Abilita i certificati CA per i plug-in

## È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

## Configurare il ripristino di emergenza

#### Ripristino di emergenza del plug-in SnapCenter per SQL Server

## Quando il plug-in SnapCenter per SQL Server non è attivo, utilizzare i passaggi seguenti per passare a un host SQL diverso e ripristinare i dati.

**Prima di iniziare**

- L'host secondario deve avere lo stesso sistema operativo, la stessa applicazione e lo stesso nome host dell'host primario.
- Inviare il plug-in SnapCenter per SQL Server a un host alternativo utilizzando la pagina **Aggiungi host** o **Modifica host**. Vedere "Gestisci gli host" per maggiori informazioni.

**Passi**

1. Selezionare l'host dalla pagina **Host** per modificare e installare il plug-in SnapCenter per SQL Server.
2. (Facoltativo) Sostituire il plug-in SnapCenter per i file di configurazione di SQL Server dal backup di disaster recovery (DR) al nuovo computer.
3. Importare le pianificazioni Windows e SQL dalla cartella del plug-in SnapCenter per SQL Server dal backup DR.

**Informazioni correlate**

Vedi il"API di disaster recovery" video.

### Ripristino di emergenza (DR) dell'archiviazione per il plug-in SnapCenter per SQL Server

## È possibile ripristinare il plug-in SnapCenter per l'archiviazione di SQL Server abilitando la modalità DR per l'archiviazione nella pagina Impostazioni globali.

**Prima di iniziare**

- Assicurarsi che i plug-in siano in modalità di manutenzione.
- Interrompere la relazione SnapMirror/ SnapVault ."Interruzione delle relazioni SnapMirror"
- Collegare la LUN dal secondario alla macchina host con la stessa lettera di unità.
- Assicurarsi che tutti i dischi siano collegati utilizzando le stesse lettere di unità utilizzate prima del DR.
- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo online.

**Informazioni su questo compito**

Il ripristino di emergenza (DR) non è supportato nelle configurazioni VMDK e RDM.

**Passi**

1. Nella pagina Impostazioni, vai su **Impostazioni** > **Impostazioni globali** > **Ripristino di emergenza**.
2. Selezionare **Abilita ripristino di emergenza**.
3. Fare clic su **Applica**.
4. Verificare se il processo DR è abilitato o meno facendo clic su **Monitor** > **Processi**.

**Dopo aver finito**

- Se vengono creati nuovi database dopo il failover, i database saranno in modalità non-DR.

  I nuovi database continueranno a funzionare come prima del failover.

- I nuovi backup creati in modalità DR verranno elencati in SnapMirror o SnapVault (secondario) nella pagina Topologia.

  Accanto ai nuovi backup viene visualizzata un'icona "i" per indicare che sono stati creati durante la modalità DR.

- È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creati durante il failover tramite l'interfaccia utente o il seguente cmdlet: `Remove-SmBackup`
- Dopo il failover, se si desidera che alcune risorse siano in modalità non DR, utilizzare il seguente cmdlet: `Remove-SmResourceDRMode`

  Per maggiori informazioni fare riferimento al "Guida di riferimento ai cmdlet del software SnapCenter" .
- SnapCenter Server gestirà le singole risorse di archiviazione (database SQL) che sono in modalità DR o non DR, ma non il gruppo di risorse con risorse di archiviazione che sono in modalità DR o non DR.

**Failback dal plug-in SnapCenter per l'archiviazione secondaria di SQL Server all'archiviazione primaria**

Dopo che il plug-in SnapCenter per l'archiviazione primaria di SQL Server è di nuovo online, è necessario eseguire il failback all'archiviazione primaria.

**Prima di iniziare**

- Impostare il plug-in SnapCenter per SQL Server in modalità **Manutenzione** dalla pagina Host gestiti.
- Scollegare l'archiviazione secondaria dall'host e connettersi dall'archiviazione primaria.
- Per eseguire il failback sullo storage primario, assicurarsi che la direzione della relazione rimanga la stessa di prima del failover eseguendo l'operazione di risincronizzazione inversa.

  Per mantenere i ruoli di storage primario e secondario dopo l'operazione di risincronizzazione inversa, eseguire nuovamente l'operazione di risincronizzazione inversa.

  Per maggiori informazioni vedere"Relazioni speculari di risincronizzazione inversa"
- Riavviare il servizio del server MSSQL.
- Assicurarsi che le risorse SQL siano di nuovo online.

> Durante il failover o il failback del plug-in, lo stato generale del plug-in non viene aggiornato immediatamente. Lo stato generale dell'host e del plug-in viene aggiornato durante la successiva operazione di aggiornamento dell'host.

**Passi**

1. Nella pagina Impostazioni, vai su **Impostazioni** > **Impostazioni globali** > **Ripristino di emergenza**.
2. Deseleziona **Abilita ripristino di emergenza**.
3. Fare clic su **Applica**.
4. Verificare se il processo DR è abilitato o meno facendo clic su **Monitor** > **Processi**.

**Dopo aver finito**

È possibile eliminare il plug-in SnapCenter per i backup di SQL Server creati durante il failover tramite l'interfaccia utente o il seguente cmdlet: `Remove-SmDRFailoverBackups`

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

### Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

### Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

# Prepararsi alla protezione dei dati

## Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft SQL Server

Prima di iniziare a utilizzare il plug-in per SQL Server, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo o assegnando connessioni al sistema di archiviazione e creando credenziali.

  SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportato da SnapCenter deve avere un nome univoco.

- Aggiungere host, installare i plug-in, scoprire (aggiornare) le risorse e configurare i plug-in.
- Spostare un database Microsoft SQL Server esistente da un disco locale a una LUN NetApp o viceversa eseguendo Invoke-SmConfigureResources.

  Per informazioni sull'esecuzione del cmdlet, vedere "Guida di riferimento ai cmdlet del software SnapCenter"

- Se si utilizza SnapCenter Server per proteggere i database SQL che risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter. Per ulteriori informazioni, consultare la documentazione SnapCenter Plug-in for VMware vSphere .

  "Documentazione SnapCenter Plug-in for VMware vSphere"

- Eseguire il provisioning dello storage lato host utilizzando il plug-in SnapCenter per Microsoft Windows.
- Se si desidera la replica del backup, impostare le relazioni SnapMirror e SnapVault .

Per maggiori dettagli, vedere le informazioni sull'installazione SnapCenter .

Per gli utenti SnapCenter 4.1.1, la documentazione SnapCenter Plug-in for VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti SnapCenter 4.2.x,

NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione di database e file system virtualizzati mediante il SnapCenter Plug-in for VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato Open Virtual Appliance). Per gli utenti SnapCenter 4.3.x, la documentazione SnapCenter Plug-in for VMware vSphere 4.3 contiene informazioni sulla protezione di database e file system virtualizzati mediante l'appliance virtuale SnapCenter Plug-in for VMware vSphere basata su Linux (formato Open Virtual Appliance).

"Documentazione SnapCenter Plug-in for VMware vSphere"

## Come vengono utilizzate risorse, gruppi di risorse e criteri per proteggere SQL Server

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere database, istanze di database o gruppi di disponibilità di Microsoft SQL Server di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host o cluster.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

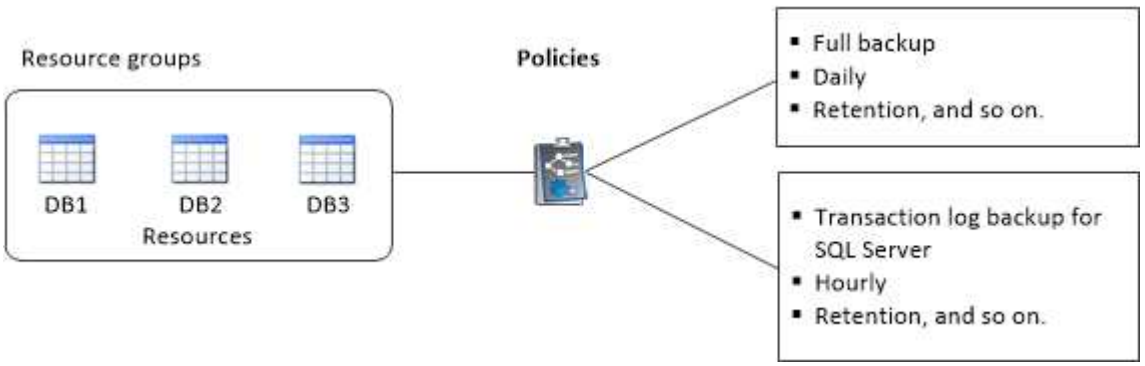
  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy specificano la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

Pensa a un gruppo di risorse come a qualcosa che definisce *cosa* vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una politica come a qualcosa che definisce *come* vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o tutti i file system nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno e un'altra pianificazione che esegua backup del registro ogni ora.

L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



# Eseguire il backup del database, dell'istanza o del gruppo di disponibilità di SQL Server

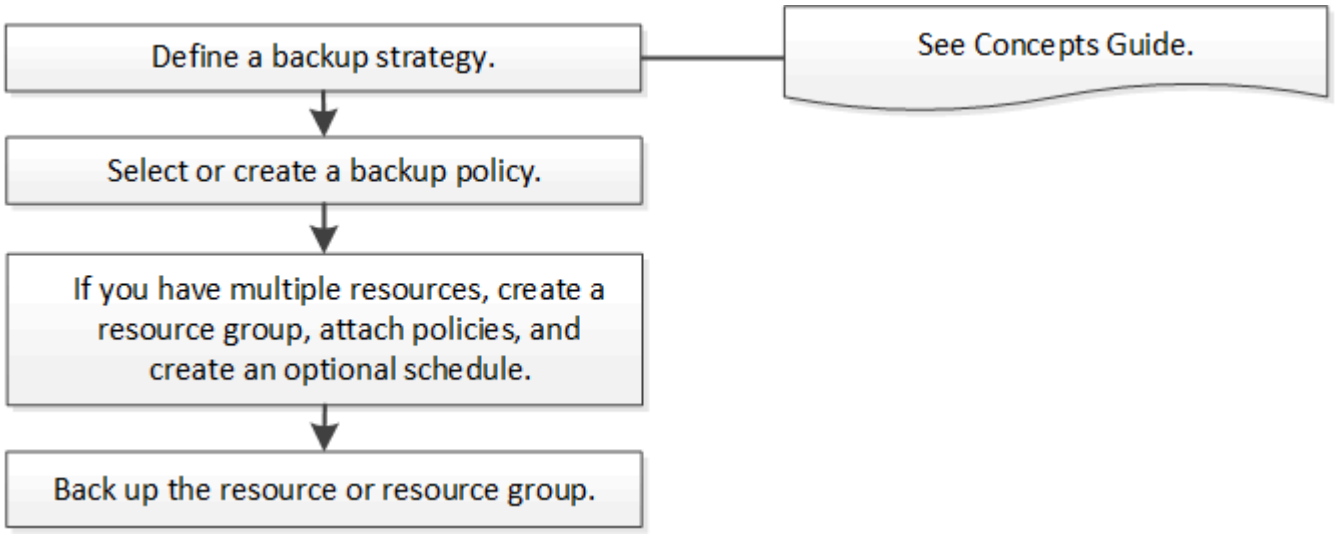
## Flusso di lavoro di backup

Quando installi il plug-in SnapCenter per Microsoft SQL Server nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server.

È possibile pianificare più backup da eseguire contemporaneamente su più server.

Le operazioni di backup e ripristino non possono essere eseguite contemporaneamente sulla stessa risorsa.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di backup:




Le opzioni Esegui backup ora, Ripristina, Gestisci backup e Clona nella pagina Risorse sono disabilitate se si seleziona un LUN non NetApp , un database danneggiato o un database in fase di ripristino.

È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, recupero, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter"

### Come SnapCenter esegue il backup dei database

SnapCenter utilizza la tecnologia Snapshot per eseguire il backup dei database SQL Server che risiedono su LUN o VMDK. SnapCenter crea il backup creando snapshot dei database.

Quando si seleziona un database per un backup completo dalla pagina Risorse, SnapCenter seleziona automaticamente tutti gli altri database che risiedono sullo stesso volume di archiviazione. Se il LUN o il VMDK memorizza un solo database, è possibile cancellare o riselezionare il database singolarmente. Se la LUN o il VMDK ospita più database, è necessario cancellare o riselezionare i database come gruppo.

Tutti i database che risiedono su un singolo volume vengono sottoposti a backup contemporaneamente tramite snapshot. Se il numero massimo di database di backup simultanei è 35 e se in un volume di archiviazione risiedono più di 35 database, il numero totale di snapshot creati è uguale al numero di database diviso per 35.

È possibile configurare il numero massimo di database per ogni snapshot nella policy di backup.

Quando SnapCenter crea uno Snapshot, l'intero volume del sistema di archiviazione viene catturato nello Snapshot. Tuttavia, il backup è valido solo per il server host SQL per il quale è stato creato.

Se i dati provenienti da altri server host SQL risiedono sullo stesso volume, non è possibile ripristinarli dallo snapshot.

**Trova maggiori informazioni**

"Le operazioni di quiesce o di raggruppamento delle risorse falliscono"

## Determinare se le risorse sono disponibili per il backup

Le risorse sono i database, le istanze delle applicazioni, i gruppi di disponibilità e componenti simili gestiti dai plug-in installati. È possibile aggiungere tali risorse ai gruppi di risorse in modo da poter eseguire attività di protezione dei dati, ma prima è necessario identificare quali risorse sono disponibili. La determinazione delle risorse disponibili verifica anche che l'installazione del plug-in sia stata completata correttamente.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la creazione di connessioni al sistema di archiviazione e l'aggiunta di credenziali.
- Per scoprire i database Microsoft SQL, deve essere soddisfatta una delle seguenti condizioni.
  - L'utente utilizzato per aggiungere l'host del plug-in a SnapCenter Server deve disporre delle autorizzazioni richieste (sysadmin) su Microsoft SQL Server.
  - Se la condizione di cui sopra non è soddisfatta, in SnapCenter Server è necessario configurare l'utente che dispone delle autorizzazioni richieste (sysadmin) su Microsoft SQL Server. L'utente deve essere configurato a livello di istanza di Microsoft SQL Server e può essere un utente SQL o Windows.
- Per scoprire i database Microsoft SQL in un cluster Windows, è necessario sbloccare la porta TCP/IP dell'istanza del cluster di failover (FCI).
- Se i database risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.

  Per maggiori informazioni, vedere "Distribuisci il SnapCenter Plug-in for VMware vSphere"

- Se l'host viene aggiunto con gMSA e se gMSA dispone di privilegi di accesso e di amministratore di sistema, gMSA verrà utilizzato per connettersi all'istanza SQL.

**Informazioni su questo compito**

Non è possibile eseguire il backup dei database quando l'opzione **Stato generale** nella pagina Dettagli è impostata su Non disponibile per il backup. L'opzione **Stato generale** è impostata su Non disponibile per il backup quando si verifica una delle seguenti condizioni:

- I database non si trovano su una LUN NetApp .
- I database non sono in stato normale.

  I database non sono in stato normale quando sono offline, in fase di ripristino, in attesa di recupero, sospetti e così via.

- I database non hanno privilegi sufficienti.

  Ad esempio, se un utente ha solo accesso di visualizzazione al database, i file e le proprietà del database non possono essere identificati e quindi non possono essere sottoposti a backup.

SnapCenter può eseguire il backup solo del database primario se si dispone di una configurazione di gruppo di disponibilità su SQL Server Standard Edition.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse seleziona **Database**, **Istanza** o **Gruppo di disponibilità** dall'elenco a discesa **Visualizza**.

   Clic e seleziona il nome host e l'istanza di SQL Server per filtrare le risorse. Puoi quindi fare clic per chiudere il riquadro del filtro.

3. Fare clic su **Aggiorna risorse**.

   Le risorse appena aggiunte, rinominate o eliminate vengono aggiornate nell'inventario di SnapCenter Server.

   È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome dell'host o del cluster, gruppi di risorse associati, tipo di backup, policy e stato generale.

   - Se il database si trova su uno storage non NetApp , `Not available for backup` viene visualizzato nella colonna **Stato generale**.

     Non è possibile eseguire operazioni di protezione dei dati su un database che si trova su un archivio non NetApp .

   - Se il database si trova su uno storage NetApp e non è protetto, `Not protected` viene visualizzato nella colonna **Stato generale**.
   - Se il database si trova su un sistema di archiviazione NetApp ed è protetto, l'interfaccia utente visualizza `Backup not run` messaggio nella colonna **Stato generale**.
   - Se il database si trova su un sistema di archiviazione NetApp ed è protetto e se il backup viene attivato per il database, l'interfaccia utente visualizza `Backup succeeded` messaggio nella colonna **Stato generale**.

Se è stata abilitata un'autenticazione SQL durante la configurazione delle credenziali, l'istanza o il database individuato viene visualizzato con un'icona a forma di lucchetto rosso. Se viene visualizzata l'icona del lucchetto, è necessario specificare le credenziali dell'istanza o del database per aggiungere correttamente l'istanza o il database a un gruppo di risorse.

1. Dopo che l'amministratore SnapCenter ha assegnato le risorse a un utente RBAC, l'utente RBAC deve effettuare l'accesso e fare clic su **Aggiorna risorse** per visualizzare lo **Stato generale** più recente delle risorse.

## Migrare le risorse al sistema di archiviazione NetApp

Dopo aver eseguito il provisioning del sistema di storage NetApp tramite il plug-in SnapCenter per Microsoft Windows, è possibile migrare le risorse al sistema di storage NetApp o da una LUN NetApp a un'altra LUN NetApp tramite l'interfaccia utente grafica (GUI) SnapCenter o i cmdlet di PowerShell.

**Prima di iniziare**

- È necessario aver aggiunto sistemi di archiviazione a SnapCenter Server.
- È necessario aver aggiornato (rilevato) le risorse di SQL Server.

La maggior parte dei campi presenti in queste pagine della procedura guidata sono autoesplicativi. Le seguenti informazioni descrivono alcuni dei campi per i quali potresti aver bisogno di assistenza.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Istanza** dall'elenco a discesa **Visualizza**.
3. Selezionare il database o l'istanza dall'elenco e fare clic su **Migra**.
4. Nella pagina Risorse, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| **Nome del database** (facoltativo) | Se hai selezionato un'istanza per la migrazione, devi selezionare i database di tale istanza dall'elenco a discesa **Database**. |
| **Scegli le destinazioni** | Selezionare la posizione di destinazione per i file di dati e di registro.<br><br>I file di dati e di registro vengono spostati rispettivamente nelle cartelle Dati e Registro nell'unità NetApp selezionata. Se una cartella nella struttura delle cartelle non è presente, viene creata una cartella e la risorsa viene migrata. |
| **Mostra i dettagli del file del database** (facoltativo) | Selezionare questa opzione quando si desidera migrare più file di un singolo database.<br><br>Questa opzione non viene visualizzata quando si seleziona la risorsa **Istanza**. |
| **Opzioni** | Selezionare **Elimina copia del database migrato nella posizione originale** per eliminare la copia del database dall'origine.<br><br>Facoltativo: **ESEGUIRE AGGIORNA STATISTICHE sulle tabelle prima di scollegare il database**. |

5. Nella pagina Verifica, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| **Opzioni di controllo della coerenza del database** | Selezionare **Esegui prima** per verificare l'integrità del database prima della migrazione. Selezionare **Esegui dopo** per verificare l'integrità del database dopo la migrazione. |
| **Opzioni DBCC CHECKDB** | • Selezionare l'opzione **PHYSICAL_ONLY** per limitare il controllo di integrità alla struttura fisica del database e per rilevare pagine danneggiate, errori di checksum e guasti hardware comuni che hanno un impatto sul database.<br>• Selezionare l'opzione **NO_INFOMSGS** per sopprimere tutti i messaggi informativi.<br>• Selezionare l'opzione **ALL_ERRORMSGS** per visualizzare tutti gli errori segnalati per oggetto.<br>• Selezionare l'opzione **NOINDEX** se non si desidera controllare gli indici non cluster.<br>Il database di SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità logica e fisica degli oggetti nel database.<br>Potresti voler selezionare questa opzione per ridurre il tempo di esecuzione.<br>• Selezionare l'opzione **TABLOCK** per limitare i controlli e ottenere blocchi anziché utilizzare uno Snapshot del database interno. |

6. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare criteri di backup per i database di SQL Server

È possibile creare un criterio di backup per la risorsa o il gruppo di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server oppure è possibile creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

**Prima di iniziare**

- Devi aver definito la tua strategia di protezione dei dati.
- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione SnapCenter, l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di archiviazione.
- È necessario aver configurato la directory del registro host per il backup del registro.

- È necessario aver aggiornato (rilevato) le risorse di SQL Server.
- Se si replicano gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le macchine virtuali di archiviazione (SVM) sia per i volumi di origine che per quelli di destinazione.

  Per informazioni su come gli amministratori assegnano le risorse agli utenti, consultare le informazioni sull'installazione SnapCenter .

- Se si desidera eseguire gli script di PowerShell in prescript e postscript, è necessario impostare il valore del parametro usePowershellProcessforScripts su true nel file web.config.

  Il valore predefinito è falso.

- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

- Una policy di backup è un insieme di regole che regolano il modo in cui vengono gestiti e conservati i backup, nonché la frequenza con cui viene eseguito il backup della risorsa o del gruppo di risorse. Inoltre, è possibile specificare le impostazioni di replica e script. Specificare le opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

  SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.

    Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.

  Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

### Passaggio 1: creare il nome della policy

1. Nel riquadro di navigazione a sinistra, seleziona **Impostazioni**.
2. Nella pagina Impostazioni, seleziona **Criteri**.
3. Seleziona **Nuovo**.
4. Nella pagina **Nome**, inserisci il nome e i dettagli della polizza.

### Passaggio 2: configurare le opzioni dei criteri

1. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Seleziona l'ambito della tua policy.

**Backup completo e backup del registro**

Eseguire il backup dei file del database e dei registri delle transazioni e troncare i registri delle transazioni.

i. Selezionare **Backup completo e Backup del registro**.
ii. Immettere il numero massimo di database di cui eseguire il backup per ogni snapshot.

> È necessario aumentare questo valore se si desidera eseguire più operazioni di backup contemporaneamente.

**Backup completo**

Eseguire il backup dei file del database.

i. Selezionare **Backup completo**.
ii. Immettere il numero massimo di database di cui eseguire il backup per ogni snapshot. Il valore predefinito è 100

> È necessario aumentare questo valore se si desidera eseguire più operazioni di backup contemporaneamente.

**Backup del registro**

i. Eseguire il backup dei registri delle transazioni.
ii. Selezionare **Backup del registro**.

**Copia solo backup**

i. Se si esegue il backup delle risorse utilizzando un'altra applicazione di backup, selezionare **Copia solo backup**.

Mantenere intatti i registri delle transazioni consente a qualsiasi applicazione di backup di ripristinare i database. In genere non dovresti usare l'opzione "solo copia" in nessun'altra circostanza.

> Microsoft SQL non supporta l'opzione **Backup solo copia** insieme all'opzione **Backup completo e Backup del registro** per l'archiviazione secondaria.

### Passaggio 3: configurare le impostazioni del gruppo di disponibilità

1. Nella sezione Impostazioni gruppo di disponibilità, eseguire le seguenti azioni:
   a. Backup solo sulla replica di backup preferita.

Selezionare questa opzione per eseguire il backup solo sulla replica di backup preferita. La replica di backup preferita viene decisa dalle preferenze di backup configurate per l'AG in SQL Server.

b. Selezionare le repliche per il backup.

   Selezionare la replica AG primaria o la replica AG secondaria per il backup.

c. Seleziona la priorità di backup (priorità di backup minima e massima)

   Specificare un numero minimo e un numero massimo di priorità di backup che decidano la replica AG per il backup. Ad esempio, è possibile avere una priorità minima di 10 e una priorità massima di 50. In questo caso, vengono prese in considerazione per il backup tutte le repliche AG con priorità superiore a 10 e inferiore a 50.

   Per impostazione predefinita, la priorità minima è 1 e quella massima è 100.

Nelle configurazioni cluster, i backup vengono conservati in ciascun nodo del cluster in base alle impostazioni di conservazione definite nella policy. Se cambia il nodo proprietario dell'AG, i backup vengono eseguiti in base alle impostazioni di conservazione e verranno conservati i backup del nodo proprietario precedente. La conservazione per AG è applicabile solo a livello di nodo.

**Passaggio 4: configurare le impostazioni di snapshot e replica**

1. Nella pagina Snapshot e replica, procedere come segue:

   a. Specificare il tipo di pianificazione selezionando **Su richiesta**, **Ora**, **Giornaliera**, **Settimanale** o **Mensile**.

      È possibile selezionare un solo tipo di pianificazione per una policy.

      È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente di assegnare pianificazioni di backup diverse a ciascuna policy.

Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

**Passaggio 5: configura le impostazioni di conservazione aggiornate**

1. Nella sezione Impostazioni di conservazione aggiornate, a seconda del tipo di backup selezionato nella pagina Tipo di backup, eseguire una o più delle seguenti azioni:

**Numero specifico di copie**

Conserva solo un numero specifico di snapshot.

1. Selezionare l'opzione **Mantieni i backup del registro applicabili agli ultimi <numero> giorni** e specificare il numero di giorni da conservare. Se ti avvicini a questo limite, potresti voler eliminare le copie più vecchie.

**Numero specifico di giorni**

Conservare le copie di backup per un numero specifico di giorni.

1. Selezionare l'opzione **Mantieni i backup del registro applicabili agli ultimi <numero> giorni di backup completi** e specificare il numero di giorni per cui conservare le copie di backup del registro.

**Passaggio 6: configurare le impostazioni di Snapshot**

1. Per le impostazioni di conservazione del backup completo, eseguire le seguenti azioni:
   a. Specificare il numero totale di snapshot da conservare
      i. Per specificare il numero di snapshot da conservare, selezionare **Copie da conservare**.
      ii. Se il numero di snapshot supera il numero specificato, gli snapshot vengono eliminati partendo dalle copie più vecchie.

> Per impostazione predefinita, il valore del conteggio di conservazione è impostato su 2. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo snapshot è lo snapshot di riferimento per la relazione SnapVault finché uno snapshot più recente non viene replicato sulla destinazione.

> Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione di NetApp ONTAP sottostante.

2. Periodo di tempo per conservare gli snapshot
   a. Se si desidera specificare il numero di giorni per cui conservare gli snapshot prima di eliminarli, selezionare **Conserva copie per**.
3. Selezionare **Periodo di blocco della copia snapshot** e specificare la durata in giorni, mesi o anni.

   Il periodo di conservazione di Snaplock dovrebbe essere inferiore a 100 anni.

4. Selezionare un'etichetta di criterio.

> È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

### Passaggio 7: configurare le opzioni di replicazione secondaria

1. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

**Aggiorna SnapMirror**

Aggiorna SnapMirror dopo aver creato una copia Snapshot locale.

1. Selezionare questa opzione per creare copie mirror dei set di backup su un altro volume (SnapMirror).

   Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror .

   Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.

   Vedere "Visualizza i backup e i cloni di SQL Server nella pagina Topologia" .

**Aggiorna SnapVault**

Aggiorna SnapVault dopo aver creato una copia Snapshot.

1. Selezionare questa opzione per eseguire la replica del backup da disco a disco.

   Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.

   Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.

   Per maggiori informazioni su SnapLock Vault vedere "Eseguire il commit delle copie Snapshot su WORM in una destinazione vault"

   Vedere "Visualizza i backup e i cloni di SQL Server nella pagina Topologia" .

**Errore conteggio tentativi**

1. Immettere il numero di tentativi di replica che devono essere eseguiti prima che il processo si interrompa.

### Passaggio 8: configurare le impostazioni dello script

1. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di backup.

   Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi e inviare i registri.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

È necessario configurare il criterio di conservazione SnapMirror in ONTAP in modo che l'archiviazione secondaria non raggiunga il limite massimo di snapshot.

**Passaggio 9: configurare le impostazioni di verifica**

Nella pagina Verifica, procedere come segue:

1. Nella sezione Esegui verifica per le seguenti pianificazioni di backup, seleziona la frequenza della pianificazione.
2. Nella sezione Opzioni di controllo della coerenza del database, eseguire le seguenti azioni:
   a. Limitare la struttura di integrità alla struttura fisica del database (PHYSICAL_ONLY)
      i. Selezionare **Limita la struttura di integrità alla struttura fisica del database (PHYSICAL_ONLY)** per limitare il controllo di integrità alla struttura fisica del database e per rilevare pagine danneggiate, errori di checksum e guasti hardware comuni che hanno un impatto sul database.
   b. Sopprimi tutti i messaggi informativi (NO INFOMSGS)
      i. Selezionare **Sopprimi tutti i messaggi informativi (NO_INFOMSGS)** per sopprimere tutti i messaggi informativi. Selezionato per impostazione predefinita.
   c. Visualizza tutti i messaggi di errore segnalati per oggetto (ALL_ERRORMSGS)
      i. Selezionare **Visualizza tutti i messaggi di errore segnalati per oggetto (ALL_ERRORMSGS)** per visualizzare tutti gli errori segnalati per oggetto.
   d. Non controllare gli indici non cluster (NOINDEX)
      i. Selezionare **Non controllare gli indici non cluster (NOINDEX)** se non si desidera controllare gli indici non cluster. Il database di SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità logica e fisica degli oggetti nel database.
   e. Limitare i controlli e ottenere i blocchi invece di utilizzare uno Snapshot del database interno (TABLOCK)
      i. Selezionare **Limita i controlli e ottieni i blocchi anziché utilizzare una copia Snapshot del database interno (TABLOCK)** per limitare i controlli e ottenere i blocchi anziché utilizzare una copia Snapshot del database interno.
3. Nella sezione **Backup del registro**, seleziona **Verifica il backup del registro al completamento** per verificare il backup del registro al completamento.
4. Nella sezione **Impostazioni script di verifica**, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di verifica.

Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

**Fase 10: Riepilogo della revisione**

1. Rivedi il riepilogo e seleziona **Fine**.

## Creare gruppi di risorse e associare criteri per SQL Server

Un gruppo di risorse è un contenitore al quale si aggiungono le risorse di cui si desidera eseguire il backup e che si desidera proteggere insieme. Un gruppo di risorse consente

di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

È possibile proteggere le risorse singolarmente senza creare un nuovo gruppo di risorse. È possibile eseguire backup sulla risorsa protetta.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi database senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.

   Se hai aggiunto di recente una risorsa a SnapCenter, fai clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.

3. Fare clic su **Nuovo gruppo di risorse**.
4. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Immettere il nome del gruppo di risorse.<br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Facoltativo: inserisci un nome e un formato personalizzati per lo snapshot. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

5. Nella pagina Risorse, procedere come segue:

a. Selezionare il nome host, il tipo di risorsa e l'istanza di SQL Server dagli elenchi a discesa per filtrare l'elenco delle risorse.

> Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle Risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

b. Per spostare le risorse dalla sezione **Risorse disponibili** alla sezione Risorse selezionate, eseguire uno dei seguenti passaggi:
   - Selezionare **Seleziona automaticamente tutte le risorse sullo stesso volume di archiviazione** per spostare tutte le risorse sullo stesso volume nella sezione Risorse selezionate.
   - Seleziona le risorse dalla sezione **Risorse disponibili** e poi clicca sulla freccia a destra per spostarle nella sezione **Risorse selezionate**.

6. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

> Puoi anche creare una policy cliccando * + *.

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Nella sezione Configura pianificazioni per policy selezionate, fai clic su * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare la pianificazione.

c. Nella finestra di dialogo Aggiungi pianificazioni per la policy *nome_policy*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **OK**.

È necessario effettuare questa operazione per ogni frequenza indicata nella polizza. Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate nella sezione **Configura pianificazioni per policy selezionate**.

d. Selezionare lo scheduler di Microsoft SQL Server.

È inoltre necessario selezionare un'istanza dello scheduler da associare al criterio di pianificazione.

Se non si seleziona lo scheduler di Microsoft SQL Server, l'impostazione predefinita è lo scheduler di Microsoft Windows.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter . Non modificare le pianificazioni né rinominare il processo di backup creato nello scheduler di Windows o nell'agente di SQL Server.

7. Nella pagina Verifica, procedere come segue:

a. Selezionare il server di verifica dall'elenco a discesa **Server di verifica**.

L'elenco include tutti i server SQL aggiunti in SnapCenter. È possibile selezionare più server di verifica (host locale o host remoto).

> La versione del server di verifica deve corrispondere alla versione e all'edizione del server SQL che ospita il database primario.

a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror e SnapVault ed eseguire la verifica sull'archiviazione secondaria.

b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi fai clic su * + *.

c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**. |

d. Fare clic su **OK**.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate. Puoi rivedere e poi modificare cliccando * * o elimina cliccando * ✖ *.

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

ⓘ Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

**Informazioni correlate**

"Creare criteri di backup per i database di SQL Server"

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse di Microsoft SQL Server sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.

- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

      Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una

pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

a. Selezionare il tipo di criterio di replica.

La politica di replica sincrona non è supportata.

b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:

a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| **Se lo desidera…** | **Fai questo…** |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

e. Fare clic su **OK**.

Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Requisiti per il backup delle risorse SQL

Prima di eseguire il backup di una risorsa SQL, è necessario assicurarsi che siano soddisfatti diversi requisiti.

- È necessario aver migrato una risorsa da un sistema di archiviazione non NetApp a un sistema di archiviazione NetApp .
- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- L'operazione di backup avviata da un utente di Active Directory (AD) fallisce se le credenziali dell'istanza SQL non sono assegnate all'utente o al gruppo AD. È necessario assegnare le credenziali dell'istanza SQL all'utente o al gruppo AD dalla pagina **Impostazioni** > **Accesso utente**.
- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se un gruppo di risorse ha più database da host diversi, l'operazione di backup su alcuni host potrebbe essere avviata in ritardo a causa di problemi di rete. È necessario configurare il valore di FMaxRetryForUninitializedHosts in web.config utilizzando il cmdlet PS Set-SmConfigSettings.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire operazioni di protezione dei dati.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell Core utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione di PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di archiviazione:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio crea una nuova credenziale denominata FinanceAdmin con credenziali Windows:

   ```
   PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup delle risorse SQL

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Informazioni su questo compito**

- Per ottimizzare l'operazione di backup, è necessario creare un record di ricerca inversa dei nomi dei cluster Windows e degli indirizzi IP nel server DNS.
- Per l'autenticazione delle credenziali di Windows, è necessario impostare le proprie credenziali prima di installare i plug-in.
- Per l'autenticazione dell'istanza di SQL Server, è necessario aggiungere le credenziali dopo aver installato i plug-in.
- Per l'autenticazione gMSA, è necessario configurare gMSA durante la registrazione dell'host con SnapCenter nella pagina **Aggiungi host** o **Modifica host** per abilitare e utilizzare gMSA.

- Se l’host viene aggiunto con gMSA e se gMSA dispone di privilegi di accesso e di amministratore di sistema, allora gMSA può connettersi all’istanza SQL.
  - SnapCenter verificherà se l’autenticazione per le istanze SQL è configurata. Se l’autenticazione è configurata, l’accesso all’istanza SQL avverrà tramite questa credenziale.
  - Se l’autenticazione non è configurata, utilizzare gMSA per verificare se il plug-in SQL è attualmente in funzione. Se il plug-in è in funzione, verrà utilizzato per stabilire una connessione all’istanza SQL.
  - L’accesso all’istanza SQL avverrà tramite autenticazione delle credenziali di Windows quando l’autenticazione per le istanze SQL non è configurata e il plug-in non è operativo.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database**, **Istanza** o **Gruppo di disponibilità** dall'elenco a discesa **Visualizza**.

   a. Selezionare il database, l'istanza o il gruppo di disponibilità di cui si desidera eseguire il backup.

      Quando si esegue un backup di un'istanza, le informazioni sullo stato dell'ultimo backup o il timestamp di tale istanza non saranno disponibili nella pagina delle risorse.

   Nella vista topologia non è possibile distinguere se lo stato del backup, il timestamp o il backup riguardano un'istanza o un database.

3. Nella pagina Risorse, seleziona la casella di controllo **formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, customtext_policy_hostname o resource_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

4. Nella pagina Criteri, eseguire le seguenti attività:

   a. Nella sezione Criteri, seleziona uno o più criteri dall'elenco a discesa.

      Puoi creare una policy selezionando * * per avviare la procedura guidata dei criteri.

      Nella sezione **Configura pianificazioni per policy selezionate** vengono elencate le policy selezionate.

   b. Seleziona * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. In **Aggiungi pianificazioni per la policy** `policy_name` finestra di dialogo, configurare la pianificazione e quindi selezionare **OK**.

      Qui `policy_name` è il nome della policy che hai selezionato.

   Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

   a. Selezionare **Usa scheduler Microsoft SQL Server**, quindi selezionare l'istanza dello scheduler dall'elenco a discesa **Istanza scheduler** associata al criterio di pianificazione.

5. Nella pagina Verifica, procedere come segue:

   a. Selezionare il server di verifica dall'elenco a discesa **Server di verifica**.

      È possibile selezionare più server di verifica (host locale o host remoto).

   La versione del server di verifica deve essere uguale o superiore alla versione dell'edizione del server SQL che ospita il database primario.

a. Selezionare **Carica localizzatori secondari per verificare i backup sul sistema di archiviazione secondario** per verificare i backup sul sistema di archiviazione secondario.

b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi seleziona * + *.

c. Nella finestra di dialogo Aggiungi pianificazioni di verifica *nome_policy*, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**. |

Se il server di verifica non dispone di una connessione di archiviazione, l'operazione di verifica fallisce con l'errore: Impossibile montare il disco.

d. Selezionare **OK**.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

6. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

7. Rivedi il riepilogo e seleziona **Fine**.

Viene visualizzata la pagina della topologia del database.

8. Seleziona **Esegui backup adesso**.
9. Nella pagina Backup, procedere come segue:

a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

b. Seleziona **Verifica dopo il backup** per verificare il backup.

c. Selezionare **Backup**.

Non rinominare il processo di backup creato nello scheduler di Windows o nell'agente di SQL Server.

Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

Viene creato un gruppo di risorse implicito. È possibile visualizzarlo selezionando l'utente o il gruppo corrispondente dalla pagina Accesso utente. Il tipo di gruppo di risorse implicito è "Resource".

10. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

**Dopo aver finito**

- Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

  "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

- Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire. Per aumentare la dimensione dell'heap Java, individuare il file di script /opt/netapp/init_scripts/scvservice. In quella sceneggiatura, il `do_start method` Il comando avvia il servizio plug-in SnapCenter VMware. Aggiorna quel comando come segue: `Java -jar -Xmx8192M -Xms4096M`.

**Informazioni correlate**

"Creare criteri di backup per i database di SQL Server"

"Le operazioni di backup falliscono con un errore di connessione MySQL a causa del ritardo nel TCP_TIMEOUT"

"Il backup non riesce con un errore di pianificazione di Windows"

"Le operazioni di quiesce o di raggruppamento delle risorse falliscono"

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea un nuovo criterio di backup con un tipo di backup SQL di FullBackup:

   ```
   PS C:\> Add-SmPolicy -PolicyName TESTPolicy
   -PluginPolicyType SCSQL -PolicyType Backup
   -SqlBackupType FullBackup -Verbose
   ```

   Questo esempio crea un nuovo criterio di backup con un tipo di backup del file system Windows

CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Scopri le risorse host utilizzando il cmdlet Get-SmResources.

   Questo esempio rileva le risorse per il plug-in Microsoft SQL sull'host specificato:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   Questo esempio rileva le risorse per i file system Windows sull'host specificato:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse di backup del database SQL con i criteri e le risorse specificati:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   Questo esempio crea un nuovo gruppo di risorse di backup del file system di Windows con i criteri e le risorse specificati:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

Questo esempio visualizza un report riepilogativo di tutti i lavori eseguiti nella data specificata:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse di SQL Server

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando e quindi selezionando il tag. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Dopo il backup, seleziona **Verifica** per verificare il backup su richiesta.

      L'opzione **Verifica** nella policy si applica solo ai lavori pianificati.

   c. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

**Informazioni correlate**

"Creare criteri di backup per i database di SQL Server"

"Creare gruppi di risorse e associare criteri per SQL Server"

"Le operazioni di backup falliscono con un errore di connessione MySQL a causa del ritardo nel TCP_TIMEOUT"

"Il backup non riesce con un errore di pianificazione di Windows"

## Monitorare le operazioni di backup delle risorse SQL nella pagina SnapCenter Jobs

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

### Monitorare le operazioni di protezione dei dati sulle risorse SQL nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annullare il plug-in SnapCenter per le operazioni di backup di Microsoft SQL Server

È possibile annullare le operazioni di backup in esecuzione, in coda o che non rispondono. Quando si annulla un'operazione di backup, SnapCenter Server interrompe l'operazione e rimuove tutti gli snapshot dall'archivio se il backup creato non è registrato con SnapCenter Server. Se il backup è già registrato con SnapCenter Server, non verrà eseguito il rollback dello Snapshot già creato, anche dopo l'attivazione dell'annullamento.

**Prima di iniziare**

- Per annullare le operazioni di ripristino, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.
- È possibile annullare solo le operazioni di backup completo o di registro in coda o in esecuzione.
- Non è possibile annullare l'operazione dopo l'avvio della verifica.

  Se si annulla l'operazione prima della verifica, l'operazione viene annullata e la verifica non verrà eseguita.
- È possibile annullare un'operazione di backup dalla pagina Monitor o dal riquadro Attività.
- Oltre a utilizzare l'interfaccia utente grafica SnapCenter , è possibile utilizzare i cmdlet di PowerShell per annullare le operazioni.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, seleziona **Monitor** > **Jobs**.<br>2. Selezionare il lavoro e selezionare **Annulla lavoro**. |

| Dal… | Azione |
| --- | --- |
| Riquadro attività | 1. Dopo aver avviato il processo di backup, selezionare nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, seleziona **Annulla lavoro**. |

**Risultato**

L'operazione viene annullata e la risorsa torna allo stato precedente. Se l'operazione annullata non risponde nello stato di annullamento o di esecuzione, è necessario eseguire `Cancel-SmJob -JobID <int> -Force` cmdlet per interrompere forzatamente l'operazione di backup.

## Visualizza i backup e i cloni di SQL Server nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista **Gestisci copie** per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .
  - Il numero di backup visualizzato include i backup eliminati dall'archivio secondario.

    Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

> I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come

SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa selezionata è un database clonato, proteggere il database clonato; l'origine del clone viene visualizzata nella pagina Topologia. Fare clic su **Dettagli** per visualizzare il backup utilizzato per la clonazione.

   Se la risorsa è protetta, viene visualizzata la pagina Topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Scheda riepilogativa** mostra il numero totale di backup e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

   - Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista **Gestisci copie**, fai clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, ridenominazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

7. Selezionare un clone dalla tabella e fare clic su **Clone Split**.
8. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .

### Pulisci il conteggio dei backup secondari utilizzando i cmdlet di PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per ripulire il conteggio dei backup secondari privi di snapshot. Potrebbe essere necessario utilizzare questo cmdlet quando il numero totale di snapshot visualizzati nella topologia Gestisci copie non corrisponde all'impostazione di conservazione degli snapshot dell'archiviazione secondaria.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Pulisci il conteggio dei backup secondari utilizzando il parametro -CleanupSecondaryBackups.

   Questo esempio pulisce il conteggio dei backup per i backup secondari senza snapshot:

```
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"):
```

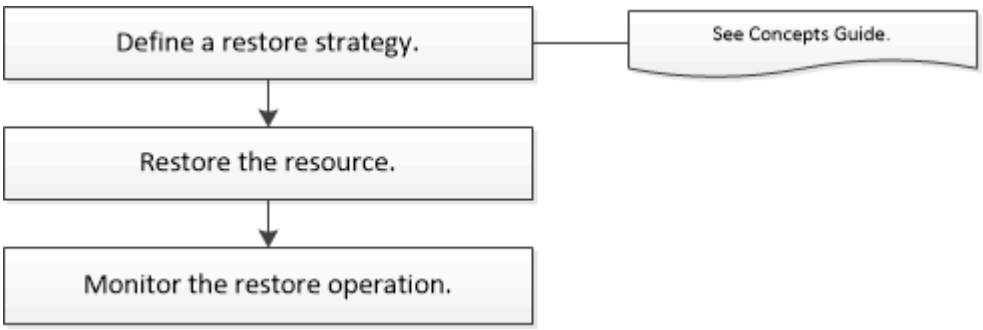
# Ripristinare le risorse di SQL Server

### Ripristina flusso di lavoro

È possibile utilizzare SnapCenter per ripristinare i database di SQL Server ripristinando i dati da uno o più backup sul file system attivo e quindi recuperando il database. È anche possibile ripristinare i database presenti nei gruppi di disponibilità e quindi aggiungere i database ripristinati al gruppo di disponibilità. Prima di ripristinare un database SQL

Server, è necessario eseguire diverse attività preparatorie.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di ripristino del database:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, recupero, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter"

**Trova maggiori informazioni**

"Ripristinare un database SQL Server da un archivio secondario"

"Ripristinare e recuperare risorse utilizzando i cmdlet di PowerShell"

"L'operazione di ripristino potrebbe non riuscire su Windows 2008 R2"

## Requisiti per il ripristino di un database

Prima di ripristinare un database SQL Server da un backup del plug-in SnapCenter per Microsoft SQL Server, è necessario assicurarsi che siano soddisfatti diversi requisiti.

- Prima di poter ripristinare un database, l'istanza di SQL Server di destinazione deve essere online e in esecuzione.

  Ciò vale sia per le operazioni di ripristino del database utente sia per quelle di ripristino del database di sistema.

- Le operazioni SnapCenter pianificate per l'esecuzione sui dati di SQL Server che si stanno ripristinando devono essere disabilitate, compresi tutti i processi pianificati sui server di gestione remota o di verifica remota.
- Se i database di sistema non funzionano, è necessario prima ricostruirli utilizzando un'utilità SQL Server.
- Se si installa il plug-in, assicurarsi di concedere le autorizzazioni ad altri ruoli per ripristinare i backup del gruppo di disponibilità (AG).

  Il ripristino di AG fallisce quando si verifica una delle seguenti condizioni:

  - Se il plug-in è installato dall'utente RBAC e un amministratore tenta di ripristinare un backup AG
  - Se il plug-in viene installato da un amministratore e un utente RBAC tenta di ripristinare un backup AG
- Se si ripristinano backup di directory di log personalizzati su un host alternativo, è necessario che sul server SnapCenter e sull'host del plug-in sia installata la stessa versione SnapCenter .
- È necessario aver installato l'hotfix Microsoft KB2887595. Il sito di supporto Microsoft contiene ulteriori

informazioni su KB2887595.

"Articolo del supporto Microsoft 2887595: Aggiornamento cumulativo per Windows RT 8.1, Windows 8.1 e Windows Server 2012 R2: novembre 2013"

- È necessario aver eseguito il backup dei gruppi di risorse o del database.
- Se si replicano gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le macchine virtuali di archiviazione (SVM) sia per i volumi di origine che per quelli di destinazione.

  Per informazioni su come gli amministratori assegnano le risorse agli utenti, consultare le informazioni sull'installazione SnapCenter .

- Tutti i processi di backup e clonazione devono essere interrotti prima di ripristinare il database.
- L'operazione di ripristino potrebbe scadere se la dimensione del database è espressa in terabyte (TB).

  È necessario aumentare il valore del parametro RESTTimeout di SnapCenter Server a 20000000 ms eseguendo il seguente comando: Set-SmConfigSettings -Agent -configSettings @{"RESTTimeout" = "20000000"}. A seconda delle dimensioni del database, il valore di timeout può essere modificato e il valore massimo che è possibile impostare è 86400000 ms.

Se si desidera effettuare il ripristino mentre i database sono online, è necessario abilitare l'opzione di ripristino online nella pagina Ripristina.

## Ripristinare i backup del database di SQL Server

È possibile utilizzare SnapCenter per ripristinare i database SQL Server sottoposti a backup. Il ripristino del database è un processo multifase che copia tutti i dati e le pagine di registro da un backup di SQL Server specificato a un database specificato.

**Informazioni su questo compito**

- È possibile ripristinare i database SQL Server sottoposti a backup in un'istanza diversa di SQL Server sullo stesso host in cui è stato creato il backup.

  È possibile utilizzare SnapCenter per ripristinare i database SQL Server sottoposti a backup in un percorso alternativo, in modo da non dover sostituire una versione di produzione.

- SnapCenter può ripristinare i database in un cluster Windows senza disconnettere il gruppo di cluster SQL Server.
- Se si verifica un errore del cluster (un'operazione di spostamento di un gruppo di cluster) durante un'operazione di ripristino (ad esempio, se il nodo proprietario delle risorse si arresta), è necessario riconnettersi all'istanza di SQL Server e quindi riavviare l'operazione di ripristino.
- Non è possibile ripristinare il database quando gli utenti o i processi di SQL Server Agent accedono al database.
- Non è possibile ripristinare i database di sistema in un percorso alternativo.
- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

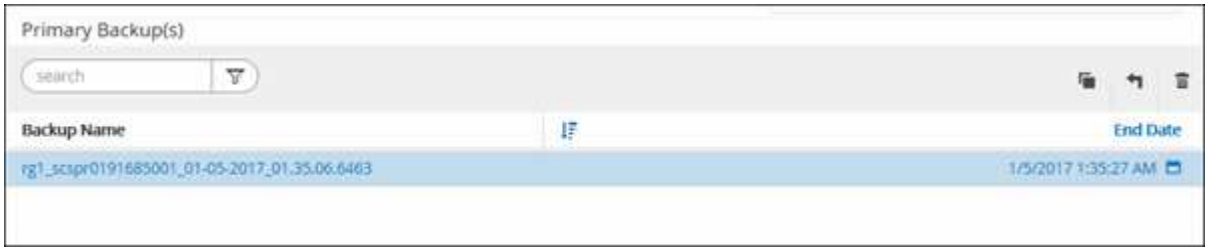
- La maggior parte dei campi nelle pagine della procedura guidata di ripristino sono autoesplicativi. Le seguenti informazioni descrivono i campi per i quali potresti aver bisogno di assistenza.
- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.
- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia.
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione.
5. Selezionare il backup dalla tabella, quindi fare clic su icona.




6. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:

| Opzione | Descrizione |
|---|---|
| Ripristinare il database sullo stesso host in cui è stato creato il backup | Selezionare questa opzione se si desidera ripristinare il database sullo stesso server SQL in cui vengono eseguiti i backup. |
| Ripristinare il database su un host alternativo | Selezionare questa opzione se si desidera che il database venga ripristinato su un server SQL diverso nello stesso host o in uno diverso in cui vengono eseguiti i backup.<br><br>Selezionare un nome host, fornire un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino.<br><br>L'estensione del file fornita nel percorso alternativo deve essere la stessa dell'estensione del file del database originale.<br><br>Se l'opzione **Ripristina il database su un host alternativo** non viene visualizzata nella pagina Ambito di ripristino, cancellare la cache del browser. |

| Opzione | Descrizione |
| --- | --- |
| Ripristinare il database utilizzando i file di database esistenti | Selezionare questa opzione se si desidera che il database venga ripristinato su un SQL Server alternativo nello stesso host o in uno diverso in cui vengono eseguiti i backup.<br><br>I file del database devono essere già presenti nei percorsi dei file esistenti specificati. Selezionare un nome host, fornire un nome di database (facoltativo), selezionare un'istanza e specificare i percorsi di ripristino. |

7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:

| Opzione | Descrizione |
| --- | --- |
| Nessuno | Selezionare **Nessuno** quando è necessario ripristinare solo il backup completo senza alcun registro. |
| Tutti i backup del registro | Selezionare l'operazione di ripristino del backup aggiornato **Tutti i backup del registro** per ripristinare tutti i backup del registro disponibili dopo il backup completo. |
| Tramite backup del registro fino a | Selezionare **Tramite backup del registro** per eseguire un'operazione di ripristino in un punto temporale specifico, che ripristina il database in base ai registri di backup fino al registro di backup con la data selezionata. |
| Entro una data specifica fino a | Selezionare **In base a una data specifica fino a** per specificare la data e l'ora dopo le quali i registri delle transazioni non vengono applicati al database ripristinato.<br><br>Questa operazione di ripristino in un dato momento interrompe il ripristino delle voci del registro delle transazioni registrate dopo la data e l'ora specificate. |

| Opzione | Descrizione |
| --- | --- |
| Utilizza directory di registro personalizzata | Se hai selezionato **Tutti i backup dei log**, **Per backup dei log** o **Per data specifica fino a** e i log si trovano in una posizione personalizzata, seleziona **Usa directory dei log personalizzata**, quindi specifica la posizione del log.<br><br>L'opzione **Usa directory di registro personalizzata** è disponibile solo se è stata selezionata l'opzione **Ripristina il database su un host alternativo** o **Ripristina il database utilizzando i file di database esistenti**. È anche possibile utilizzare il percorso condiviso, ma assicurarsi che sia accessibile all'utente SQL.<br><br>La directory di registro personalizzata non è supportata per il database del gruppo di disponibilità. |

8. Nella pagina Pre Ops, eseguire i seguenti passaggi:

   a. Nella pagina Opzioni pre-ripristino, seleziona una delle seguenti opzioni:

      - Selezionare **Sovrascrivi il database con lo stesso nome durante il ripristino** per ripristinare il database con lo stesso nome.
      - Selezionare **Mantieni impostazioni di replica del database SQL** per ripristinare il database e mantenere le impostazioni di replica esistenti.
      - Selezionare **Crea backup del registro delle transazioni prima del ripristino** per creare un registro delle transazioni prima dell'inizio dell'operazione di ripristino.
      - Selezionare **Interrompi ripristino se il backup del registro delle transazioni prima del ripristino non riesce** per interrompere l'operazione di ripristino se il backup del registro delle transazioni non riesce.

   b. Specificare gli script facoltativi da eseguire prima di eseguire un processo di ripristino.

      Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

      Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

9. Nella pagina Post Ops, eseguire i seguenti passaggi:

   a. Nella sezione Scegli lo stato del database al termine del ripristino, seleziona una delle seguenti opzioni:

      - Selezionare **Operativo, ma non disponibile per il ripristino di registri delle transazioni aggiuntivi** se si desidera ripristinare tutti i backup necessari in questo momento.

        Questo è il comportamento predefinito, che lascia il database pronto per l'uso eseguendo il rollback delle transazioni non confermate. Non è possibile ripristinare ulteriori registri delle

transazioni finché non si crea un backup.

- Selezionare **Non operativo, ma disponibile per il ripristino di ulteriori log transazionali** per lasciare il database non operativo senza eseguire il rollback delle transazioni non confermate.

  È possibile ripristinare ulteriori registri delle transazioni. Non è possibile utilizzare il database finché non viene ripristinato.

- Selezionare **Modalità di sola lettura, disponibile per il ripristino di registri transazionali aggiuntivi** per lasciare il database in modalità di sola lettura.

  Questa opzione annulla le transazioni non eseguite, ma salva le azioni annullate in un file di standby in modo che gli effetti del ripristino possano essere annullati.

Se l'opzione Annulla directory è abilitata, vengono ripristinati più registri delle transazioni. Se l'operazione di ripristino del registro delle transazioni non riesce, è possibile annullare le modifiche. Per ulteriori informazioni, consultare la documentazione di SQL Server.

b. Specificare gli script facoltativi da eseguire dopo aver eseguito un processo di ripristino.

Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

> Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

    È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristinare un database SQL Server da un archivio secondario

È possibile ripristinare i database SQL Server sottoposti a backup dai LUN fisici (RDM, iSCSI o FCP) su un sistema di archiviazione secondario. La funzionalità di ripristino è un processo multifase che copia tutti i dati e le pagine di registro da un backup di SQL Server specificato, residente sul sistema di archiviazione secondario, a un database specificato.

**Prima di iniziare**

- È necessario aver replicato gli snapshot dal sistema di archiviazione primario a quello secondario.

- È necessario assicurarsi che SnapCenter Server e l'host del plug-in siano in grado di connettersi al sistema di archiviazione secondario.
- La maggior parte dei campi nelle pagine della procedura guidata di ripristino sono spiegati nel processo di ripristino di base. Le seguenti informazioni descrivono alcuni dei campi per i quali potresti aver bisogno di assistenza.

**Informazioni su questo compito**

Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare **Plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco a discesa **Visualizza**.
3. Selezionare il database o il gruppo di risorse.

   Viene visualizzata la pagina della topologia del database o del gruppo di risorse.
4. Nella sezione Gestisci copie, seleziona **Backup** dal sistema di archiviazione secondario (con mirroring o vault).
5. Selezionare il backup dall'elenco, quindi fare clic su .
6. Nella pagina Posizione, seleziona il volume di destinazione per il ripristino della risorsa selezionata.
7. Completare la procedura guidata di ripristino, rivedere il riepilogo e quindi fare clic su **Fine**.

Se hai ripristinato un database in un percorso diverso condiviso da altri database, dovresti eseguire un backup completo e una verifica del backup per confermare che il database ripristinato non presenti danneggiamenti a livello fisico.

## Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   PS C:\> Open-Smconnection
   ```
2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Reseed dei database del gruppo di disponibilità

Il reseeding è un'opzione per ripristinare i database dei gruppi di disponibilità (AG). Se un database secondario perde la sincronizzazione con il database primario in un AG, è possibile effettuare il seeding del database secondario.

**Prima di iniziare**

- È necessario aver creato un backup del database AG secondario che si desidera ripristinare.
- Il server SnapCenter e l'host del plug-in devono avere installata la stessa versione SnapCenter .

**Informazioni su questo compito**

- Non è possibile eseguire operazioni di reseeding sui database primari.

- Non è possibile eseguire un'operazione di reseeding se il database replica è stato rimosso dal gruppo di disponibilità. Quando la replica viene rimossa, l'operazione di reseeding fallisce.
- Durante l'esecuzione dell'operazione di reseeding sul database del gruppo di disponibilità SQL, non è necessario attivare backup del log sui database replica di tale database del gruppo di disponibilità. Se si attivano i backup del log durante l'operazione di reseeding, l'operazione di reseeding fallisce e viene visualizzato il messaggio di errore Il database mirror "database_name" non dispone di dati di log delle transazioni sufficienti per preservare la catena di backup del log del database principale.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare **Plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.
3. Selezionare il database AG secondario dall'elenco.
4. Fare clic su **Reseed**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di ripristino delle risorse SQL

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.

e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.

4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

## Annulla le operazioni di ripristino delle risorse SQL

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di ripristino in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla processo** è disabilitato per le operazioni di ripristino che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di ripristino in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Seleziona il lavoro e clicca su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di ripristino, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

# Clona le risorse del database SQL Server

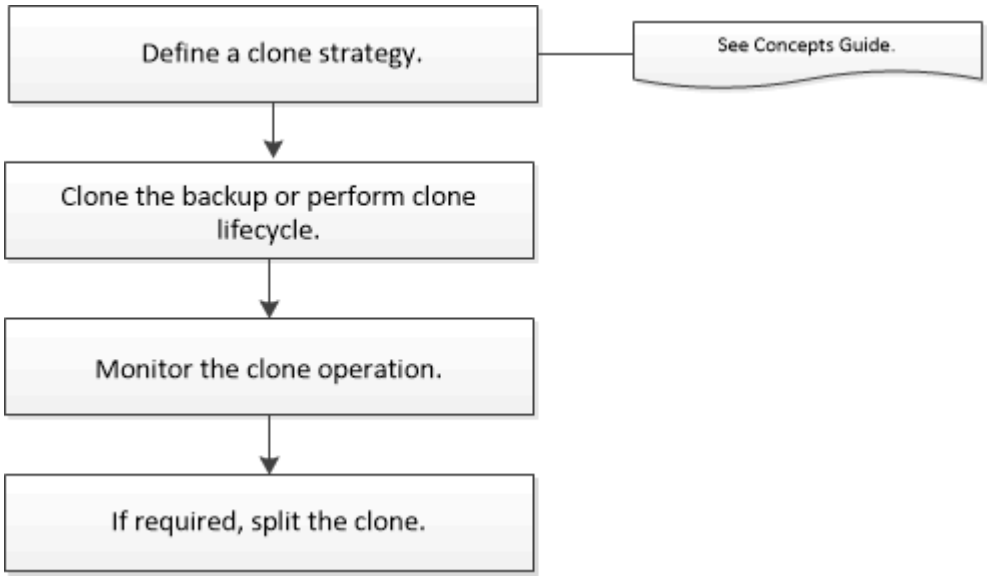
## Flusso di lavoro di clonazione

Prima di clonare le risorse del database da un backup, è necessario eseguire diverse attività utilizzando SnapCenter Server. La clonazione del database è il processo di

creazione di una copia puntuale di un database di produzione o del suo set di backup. È possibile clonare i database per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo delle applicazioni, per utilizzare gli strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse o per recuperare dati che sono stati eliminati o modificati per errore.

Un'operazione di clonazione del database genera report basati sugli ID dei processi.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino, recupero, verifica e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter"

**Trova maggiori informazioni**

"Clonazione da un backup del database SQL Server"

"Eseguire il ciclo di vita della clonazione"

"L'operazione di clonazione potrebbe non riuscire o richiedere più tempo per essere completata con il valore TCP_TIMEOUT predefinito"

## Clonazione da un backup del database SQL Server

È possibile utilizzare SnapCenter per clonare un backup del database SQL Server. Se si desidera accedere o ripristinare una versione precedente dei dati, è possibile clonare i backup del database su richiesta.

**Prima di iniziare**

- Dovresti aver preparato la protezione dei dati completando attività quali l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di archiviazione.
- Avresti dovuto eseguire il backup dei database o dei gruppi di risorse.

- Il tipo di protezione, ad esempio mirror, vault o mirror-vault per LUN dati e LUN log, deve essere lo stesso per individuare localizzatori secondari durante la clonazione su un host alternativo mediante backup log.
- Se l'unità clone montata non viene trovata durante un'operazione di clonazione SnapCenter , è necessario modificare il parametro CloneRetryTimeout di SnapCenter Server su 300.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).

**Informazioni su questo compito**

- Durante la clonazione su un'istanza di database autonoma, assicurarsi che il percorso del punto di montaggio esista e che si tratti di un disco dedicato.
- Durante la clonazione su un'istanza del cluster di failover (FCI), assicurarsi che i punti di montaggio esistano, che si tratti di un disco condiviso e che il percorso e l'FCI appartengano allo stesso gruppo di risorse SQL.
- Assicurarsi che a ciascun host sia collegato un solo vFC o FC Initiator. Questo perché SnapCenter supporta un solo iniziatore per host.
- Se il database di origine o l'istanza di destinazione si trova su un volume condiviso del cluster (csv), il database clonato si troverà sul csv.
- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

  Per gli ambienti virtuali (VMDK/RDM), assicurarsi che il punto di montaggio sia un disco dedicato.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona **Plug-in SnapCenter per SQL Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.

   La clonazione di un backup di un'istanza non è supportata.

3. Selezionare il database o il gruppo di risorse.
4. Dalla pagina di visualizzazione **Gestisci copie**, seleziona il backup dal sistema di archiviazione primario o secondario (con mirroring o in vault).
5. Seleziona il backup, quindi seleziona * *.
6. Nella pagina **Opzioni di clonazione**, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Scegliere un host su cui creare il clone. |
| Istanza clonata | Selezionare un'istanza clone su cui si desidera clonare il backup del database.<br><br>Questa istanza SQL deve trovarsi nel server clone specificato. |
| Suffisso clone | Immettere un suffisso che verrà aggiunto al nome del file clone per identificare che il database è un clone.<br><br>Ad esempio, *db1_clone*. Se si esegue la clonazione nella stessa posizione del database originale, è necessario fornire un suffisso per differenziare il database clonato da quello originale. In caso contrario, l'operazione fallisce. |
| Assegna automaticamente il punto di montaggio o Assegna automaticamente il punto di montaggio del volume nel percorso | Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume in un percorso.<br><br>Assegna automaticamente il punto di montaggio del volume in base al percorso: il punto di montaggio in base a un percorso consente di specificare una directory specifica. I punti di montaggio verranno creati all'interno di quella directory. Prima di scegliere questa opzione, è necessario assicurarsi che la directory sia vuota. Se nella directory è presente un database, dopo l'operazione di montaggio il database sarà in uno stato non valido. |

7. Nella pagina Registri, seleziona una delle seguenti opzioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nessuno | Selezionare questa opzione quando si desidera clonare solo il backup completo senza alcun registro. |
| Tutti i backup del registro | Selezionare questa opzione per clonare tutti i backup di log disponibili con data successiva al backup completo. |
| Tramite backup del registro fino a | Selezionare questa opzione per clonare il database in base ai log di backup creati fino al log di backup con la data selezionata. |
| Entro una data specifica fino a | Specificare la data e l'ora dopo le quali i registri delle transazioni non vengono applicati al database clonato.<br><br>Questa clonazione puntuale interrompe la clonazione delle voci del registro delle transazioni registrate dopo la data e l'ora specificate. |

8. Nella pagina **Script**, immettere il timeout dello script, il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.

   Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

   > Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

   Il timeout predefinito dello script è 60 secondi.

9. Nella pagina **Notifica**, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

   > Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

   Per EMS, puoi fare riferimento a "Gestire la raccolta dati EMS"

10. Rivedi il riepilogo e seleziona **Fine**.
11. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

**Dopo aver finito**

Una volta creato il clone, non dovresti mai rinominarlo.

**Informazioni correlate**

"L'operazione di clonazione potrebbe non riuscire o richiedere più tempo per essere completata con il valore TCP_TIMEOUT predefinito"

"Il clone del database dell'istanza del cluster di failover non riesce"

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Elenca i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   Questo esempio visualizza informazioni su un gruppo di risorse specificato, sulle sue risorse e sui criteri associati:

```
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. Avviare un'operazione di clonazione da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

```
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
```

Questo esempio crea un clone di un'istanza specificata di Microsoft SQL Server:

```
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. Visualizzare lo stato del processo di clonazione utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report di clonazione per l'ID processo specificato:

```
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}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il ciclo di vita della clonazione

Utilizzando SnapCenter, è possibile creare cloni da un gruppo di risorse o da un database. È possibile eseguire la clonazione su richiesta oppure pianificare operazioni di clonazione ricorrenti di un gruppo di risorse o di un database. Se si clona periodicamente un backup, è possibile utilizzare il clone per sviluppare applicazioni, popolare dati o recuperare dati.

SnapCenter consente di pianificare più operazioni di clonazione da eseguire simultaneamente su più server.

**Prima di iniziare**

- Durante la clonazione su un'istanza di database autonoma, assicurarsi che il percorso del punto di montaggio esista e che si tratti di un disco dedicato.
- Durante la clonazione su un'istanza del cluster di failover (FCI), assicurarsi che i punti di montaggio esistano, che si tratti di un disco condiviso e che il percorso e l'FCI appartengano allo stesso gruppo di risorse SQL.
- Se il database di origine o l'istanza di destinazione si trova su un volume condiviso del cluster (csv), il database clonato si troverà sul csv.

Per gli ambienti virtuali (VMDK/RDM), assicurarsi che il punto di montaggio sia un disco dedicato.

**Informazioni su questo compito**

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- La maggior parte dei campi nelle pagine della procedura guidata del ciclo di vita della clonazione sono autoesplicativi. Le seguenti informazioni descrivono i campi per i quali potresti aver bisogno di assistenza.
- Per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco Snapshot, i cloni creati dagli Snapshot antimanomissione erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il gruppo di risorse o il database, quindi fare clic su **Clona ciclo di vita**.
4. Nella pagina Opzioni, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome del lavoro clonato | Specificare il nome del processo del ciclo di vita del clone che aiuta a monitorare e modificare il processo del ciclo di vita del clone. |
| Server clone | Scegliere l'host su cui posizionare il clone. |
| Istanza clonata | Selezionare l'istanza clone in cui si desidera clonare il database. Questa istanza SQL deve trovarsi nel server clone specificato. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Suffisso clone | Immettere un suffisso che verrà aggiunto al database dei cloni per identificare che si tratta di un clone. Ogni istanza SQL utilizzata per creare un gruppo di risorse clone deve avere un nome di database univoco. Ad esempio, se il gruppo di risorse clone contiene un database di origine “db1” da un’istanza SQL “inst1” e se “db1” viene clonato in “inst1”, il nome del database clone dovrebbe essere “db1*clone”. “*clone” è un suffisso obbligatorio definito dall’utente perché il database viene clonato nella stessa istanza. Se “db1” viene clonato nell’istanza SQL “inst2”, il nome del database clone può rimanere “db1” (il suffisso è facoltativo) perché il database viene clonato in un’istanza diversa. |
| Assegna automaticamente il punto di montaggio o Assegna automaticamente il punto di montaggio del volume nel percorso | Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume in un percorso. Scegliendo di assegnare automaticamente un punto di montaggio del volume in un percorso è possibile specificare una directory specifica. I punti di montaggio verranno creati all’interno di quella directory. Prima di scegliere questa opzione, è necessario assicurarsi che la directory sia vuota. Se nella directory è presente un database, dopo l’operazione di montaggio il database sarà in uno stato non valido. |

5. Nella pagina Posizione, seleziona una posizione di archiviazione per creare un clone.
6. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l’operazione di clonazione.

   Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

   > Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

   Il timeout predefinito dello script è 60 secondi.

7. Nella pagina Pianificazione, eseguire una delle seguenti azioni:
   - Selezionare **Esegui ora** se si desidera eseguire immediatamente il processo di clonazione.
   - Selezionare **Configura pianificazione** quando si desidera determinare la frequenza con cui deve avvenire l’operazione di clonazione, quando deve iniziare la pianificazione della clonazione, in quale giorno deve avvenire l’operazione di clonazione, quando deve scadere la pianificazione e se i cloni devono essere eliminati dopo la scadenza della pianificazione.
8. Nella pagina Notifica, dall’elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l’oggetto dell’email.

Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

Per EMS, puoi fare riferimento a "Gestire la raccolta dati EMS"

9. Rivedi il riepilogo e poi clicca su **Fine**.

È necessario monitorare il processo di clonazione tramite la pagina **Monitor** > **Jobs**.

## Monitorare le operazioni di clonazione del database SQL

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Annulla le operazioni di clonazione delle risorse SQL

È possibile annullare le operazioni di clonazione in coda.

Per annullare le operazioni di clonazione, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di clonazione in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di clonazione in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di clonazione in coda.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di clonazione in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Selezionare l'operazione e fare clic su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di clonazione, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina **Dettagli lavoro**, fare clic su **Annulla lavoro**. |

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .

- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

**Informazioni correlate**

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

# Proteggere i database SAP HANA

## Plug-in SnapCenter per database SAP HANA

### Panoramica del plug-in SnapCenter per il database SAP HANA

Il plug-in SnapCenter per il database SAP HANA è un componente lato host del software NetApp SnapCenter software che consente la gestione della protezione dei dati basata sulle applicazioni dei database SAP HANA. Il plug-in per il database SAP HANA automatizza il backup, il ripristino e la clonazione dei database SAP HANA nel tuo ambiente SnapCenter .

SnapCenter supporta contenitori di database singoli e multi-tenant (MDC). È possibile utilizzare il plug-in per il database SAP HANA sia in ambienti Windows che Linux. Il plug-in non installato sull'host del database HANA è noto come plug-in host centralizzato. Il plug-in host centralizzato può gestire più database HANA su host diversi.

Una volta installato il plug-in per il database SAP HANA, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard.

Il plug-in per il database SAP HANA supporta la sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando le applicazioni per il failover trasparente tramite una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

### Cosa puoi fare utilizzando il plug-in SnapCenter per il database SAP HANA

Quando installi il plug-in per il database SAP HANA nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database SAP HANA e delle relative risorse. È anche possibile eseguire attività di supporto a tali operazioni.

- Aggiungere database.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

### Funzionalità del plug-in SnapCenter per il database SAP HANA

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp sul sistema di storage. Per lavorare con il plug-in per il database SAP HANA, utilizzare l'interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare operazioni di backup, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- **Tecnologia di copia snapshot NetApp non disruptive**

  SnapCenter utilizza la tecnologia NetApp Snapshot con il plug-in per il database SAP HANA per eseguire il backup delle risorse.

L'utilizzo del plug-in per il database SAP HANA offre inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di autorizzazioni a livello di applicazione.

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità Snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per il backup basato su file.
- Supporto per Linux LVM sul file system XFS.

## Tipi di archiviazione supportati dal plug-in SnapCenter per il database SAP HANA

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali (VM). È necessario verificare il supporto per il tipo di archiviazione in uso prima di installare il plug-in SnapCenter per il database SAP HANA.

| Macchina | Tipo di archiviazione |
| --- | --- |
| Server fisico | • LUN connesse a FC<br>• LUN connesse tramite iSCSI<br>• Volumi connessi tramite NFS |
| VMware ESXi | • LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host.<br><br>È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES.<br><br>• LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI<br>• VMDK su datastore NFS<br>• VMDK creati su VMFS<br>• Volumi NFS connessi direttamente al sistema guest<br>• Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

## Privilegi ONTAP minimi richiesti per il plug-in SAP HANA

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea
  - lun crea

- lun cancella
- lun igroup aggiungi
- lun igroup create
- lun igroup elimina
- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume

    - creazione di clonazione di file di volume
    - file di volume mostra-utilizzo-disco
    - volume offline
    - volume online
    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete

- mostra interfaccia di rete
- server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per i database SAP HANA

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter . Se si utilizza SnapMirror ActiveSync, utilizzare le pianificazioni predefinite SnapMirror o SnapVault sia per SnapMirror ActiveSync che per le relazioni asincrone.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Strategia di backup per database SAP HANA

### Definire una strategia di backup per i database SAP HANA

Definire una strategia di backup prima di creare i processi di backup ti aiuta a disporre dei backup necessari per ripristinare o clonare correttamente le tue risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

#### Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

#### Passi

1. Determina quando eseguire il backup delle tue risorse.

2. Decidi quanti processi di backup ti servono.
3. Decidi come denominare i tuoi backup.
4. Decidi se vuoi creare una policy basata sulla copia di snapshot per eseguire il backup di snapshot coerenti con l'applicazione del database.
5. Decidi se vuoi verificare l'integrità del database.
6. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
7. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
8. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

**Rilevamento automatico delle risorse sull'host Linux**

Le risorse sono i database SAP HANA e il volume non dati sull'host Linux gestiti da SnapCenter. Dopo aver installato il plug-in SnapCenter per il database SAP HANA, i database SAP HANA presenti sull'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.

La scoperta automatica è supportata per le seguenti risorse SAP HANA:

- Contenitori singoli

  Dopo aver installato o aggiornato il plug-in, le singole risorse del contenitore situate su un plug-in host centralizzato continueranno a essere aggiunte manualmente.

  Dopo l'installazione o l'aggiornamento del plug-in, i database SAP HANA vengono rilevati automaticamente solo sugli host SAP HANA Linux, registrati direttamente in SnapCenter.

- Contenitore di database multi-tenant (MDC)

  Dopo aver installato o aggiornato il plug-in, le risorse MDC presenti su un plug-in host centralizzato continueranno a essere aggiunte manualmente.

  Dopo l'aggiornamento a SnapCenter 4.3, è necessario continuare ad aggiungere manualmente le risorse MDC sul plug-in host centralizzato.

  Per gli host SAP HANA Linux registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in attiverà un rilevamento automatico delle risorse sull'host. Dopo aver aggiornato il plug-in, per ogni risorsa MDC presente sull'host del plug-in, verrà automaticamente rilevata un'altra risorsa MDC con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà bloccata.

  Ad esempio, in SnapCenter 4.2, se la risorsa E90 MDC si trovava sull'host del plug-in ed era stata registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa E90 MDC con un GUID diverso verrà rilevata e registrata in SnapCenter.

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

Nel caso in cui vengano scoperte le risorse di cui sopra, le operazioni di protezione dei dati non saranno supportate su tali risorse.

- Configurazione multi-host HANA
- Più istanze sullo stesso host
- Replicazione del sistema HANA con scalabilità multilivello
- Ambiente di replica a cascata in modalità di replicazione del sistema

**Tipo di backup supportati**

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta i tipi di backup basati su file e copie snapshot per i database SAP HANA.

**Backup basato su file**

I backup basati su file verificano l'integrità del database. È possibile pianificare l'esecuzione dell'operazione di backup basata su file a intervalli specifici. Viene eseguito il backup solo dei tenant attivi. Non è possibile ripristinare e clonare backup basati su file da SnapCenter.

**Backup basato su copia snapshot**

I backup basati su copie snapshot sfruttano la tecnologia NetApp Snapshot per creare copie online di sola lettura dei volumi su cui risiedono i database SAP HANA.

**Come il plug-in SnapCenter per il database SAP HANA utilizza gli snapshot del gruppo di coerenza**

È possibile utilizzare il plug-in per creare snapshot di gruppi di coerenza per gruppi di risorse. Un gruppo di coerenza è un contenitore che può ospitare più volumi, in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da snapshot simultanei di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È anche possibile specificare il tempo di attesa affinché il controller di archiviazione raggruppi in modo coerente gli snapshot. Le opzioni di tempo di attesa disponibili sono **Urgente**, **Medio** e **Rilassato**. È anche possibile abilitare o disabilitare la sincronizzazione Write Anywhere File Layout (WAFL) durante l'operazione Snapshot di gruppo coerente. La sincronizzazione WAFL migliora le prestazioni di uno Snapshot di gruppo di coerenza.

**Come SnapCenter gestisce la manutenzione dei backup dei registri e dei dati**

SnapCenter gestisce la manutenzione dei backup dei registri e dei dati a livello di sistema di archiviazione e file system e all'interno del catalogo di backup SAP HANA.

Gli snapshot sullo storage primario o secondario e le voci corrispondenti nel catalogo SAP HANA vengono eliminati in base alle impostazioni di conservazione. Anche le voci del catalogo SAP HANA vengono eliminate durante il backup e l'eliminazione del gruppo di risorse.

**Considerazioni per la determinazione delle pianificazioni di backup per il database SAP HANA**

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di modifica della risorsa. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora,

mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup (con quale frequenza devono essere eseguiti i backup)

  La frequenza di backup, detta anche tipo di pianificazione per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza del backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (esattamente quando devono essere eseguiti i backup

  Le pianificazioni di backup fanno parte della configurazione di una risorsa o di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00.

#### Numero di processi di backup necessari per i database SAP HANA

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

#### Convenzioni di denominazione del backup per plug-in per database SAP HANA

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

# Strategia di ripristino e recupero per database SAP HANA

## Definire una strategia di ripristino e recupero per le risorse SAP HANA

È necessario definire una strategia prima di ripristinare e recuperare il database, in modo da poter eseguire correttamente le operazioni di ripristino e recupero.

### Passi

1. Determinare le strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i database SAP HANA rilevati automaticamente
3. Decidi il tipo di operazioni di ripristino che vuoi eseguire.

## Tipi di strategie di ripristino supportate per le risorse SAP HANA aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse SAP HANA aggiunte manualmente. Non è possibile recuperare le risorse SAP HANA aggiunte manualmente.

Non è possibile recuperare le risorse SAP HANA aggiunte manualmente.

### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

### Ripristino a livello di file

- Ripristina i file da volumi, qtree o directory
- Ripristina solo i LUN selezionati

## Tipi di strategie di ripristino supportate per i database SAP HANA rilevati automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per i database SAP HANA rilevati automaticamente.

### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa
  - Per ripristinare l'intero volume, è necessario selezionare l'opzione **Ripristina volume**.

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

#### Database degli inquilini

- Ripristina il database del tenant

Se è selezionata l'opzione **Database tenant**, per eseguire l'operazione di ripristino è necessario utilizzare HANA Studio o script di ripristino HANA esterni a SnapCenter .

### Tipi di operazioni di ripristino per database SAP HANA rilevati automaticamente

SnapCenter supporta i tipi di ripristino SnapRestore basati su volume (VBSR), SnapRestore su singolo file e di tipo "connect-and-copy" per i database SAP HANA rilevati automaticamente.

#### SnapRestore basato su volume (VBSR) viene eseguito negli ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito su versioni precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **Completa risorsa**
- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata l'opzione **Ripristino volume**

#### Single File SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e se è selezionata solo l'opzione **Risorsa completa**
- Per i contenitori di database multi-tenant (MDC), quando il backup selezionato per il ripristino viene eseguito su SnapCenter 4.3 e l'opzione **Database tenant** è selezionata
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

#### Single File SnapRestore viene eseguito in ambienti SAN per i seguenti scenari:

- Quando i backup vengono eseguiti su versioni precedenti a SnapCenter 4.3 e solo se è selezionata l'opzione **Completa risorsa**
- Quando i backup vengono eseguiti in SnapCenter 4.3 e solo se è selezionata l'opzione **Risorsa completa**
- Quando il backup viene selezionato da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

#### Il ripristino basato su connessione e copia viene eseguito negli ambienti SAN per il seguente scenario:

- Per MDC, quando il backup selezionato per il ripristino viene eseguito in SnapCenter 4.3 e l'opzione **Database tenant** è selezionata

Le opzioni **Risorsa completa**, **Ripristino volume** e **Database tenant** sono disponibili nella pagina Ambito di ripristino.

### Tipi di operazioni di ripristino supportate per i database SAP HANA

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i database SAP HANA.

- Ripristina il database fino allo stato più recente

- Ripristina il database fino a un punto specifico nel tempo

  È necessario specificare la data e l'ora del ripristino.

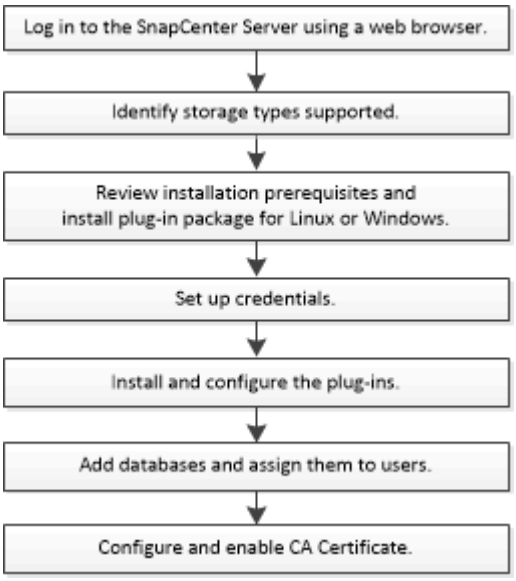
- Ripristinare il database fino a un backup di dati specifico

SnapCenter offre anche l'opzione Nessun ripristino per i database SAP HANA.

# Prepararsi all'installazione del plug-in SnapCenter per il database SAP HANA

## Flusso di lavoro di installazione del plug-in SnapCenter per il database SAP HANA

Se si desidera proteggere i database SAP HANA, è necessario installare e configurare il plug-in SnapCenter per il database SAP HANA.




## Prerequisiti per l'aggiunta di host e l'installazione del plug-in SnapCenter per il database SAP HANA

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. Il plug-in SnapCenter per il database SAP HANA è disponibile sia negli ambienti Windows che Linux.

- Devi aver installato Java 11 sul tuo host.

  IBM Java non è supportato su host Windows e Linux.

- È necessario aver installato il terminale interattivo del database SAP HANA (client HDBSQL) sull'host.
- Per Windows, il plug-in Creator Service dovrebbe essere eseguito utilizzando l'utente Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per il database SAP HANA è installato come amministratore di dominio.
- Per Windows, le chiavi dell'archivio utente devono essere create come utente SYSTEM.

- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in SAP HANA sugli host Windows.
- Per gli host Linux, l'accesso alle chiavi HDB Secure User Store avviene come utente del sistema operativo HDBSQL.
- SnapCenter Server deve avere accesso alla porta 8145 o personalizzata del plug-in per l'host del database SAP HANA.

**Host Windows**

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per il database SAP HANA su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Windows.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

**Host Linux**

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

- Per i database SAP HANA in esecuzione su un host Linux, durante l'installazione del plug-in per il database SAP HANA, viene installato automaticamente il plug-in SnapCenter per UNIX.
- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

**Comandi supplementari**

Per eseguire un comando supplementare sul plug-in SnapCenter per SAP HANA, è necessario includerlo nel file *allowed_commands.config*.

- Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Per consentire comandi supplementari sull'host del plug-in, aprire il file *allowed_commands.config* in un editor. Immettere ogni comando su una riga separata e i comandi non fanno distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e di racchiuderlo tra virgolette (") se contiene spazi.

Per esempio:

comando: monta

comando: smonta

comando: "C:\Programmi\ NetApp\SnapCreator commands\sdcli.exe"

comando: myscript.bat

Se il file *allowed_commands.config* non è presente, l'esecuzione dei comandi o degli script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in *allowed_commands.config*, l'esecuzione del comando o dello script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Non dovresti usare un carattere jolly (*) per consentire tutti i comandi.

**Configurare i privilegi sudo per gli utenti non root per l'host Linux**

SnapCenter 2.0 e le versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

**Cosa ti servirà**

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*LINUX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux. .

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br><br>Java 11 Oracle Java e OpenJDK sono richiesti solo per SAP HANA, IBM Db2, PostgreSQL, MySQL, i plug-in supportati NetApp e altre applicazioni personalizzate che possono essere installate su host Windows.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario acquisire familiarità con alcuni requisiti di base relativi allo spazio e alle dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |

| Articolo | Requisiti |
| --- | --- |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 Oracle Java e OpenJDK<br><br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

## Imposta le credenziali per il plug-in SnapCenter per il database SAP HANA

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su database o file system Windows.

**Informazioni su questo compito**

- Host Linux

  È necessario impostare le credenziali per installare i plug-in sugli host Linux.

  Per installare e avviare il processo del plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root dotato di privilegi sudo.

  **Procedura consigliata:** Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

- Host Windows

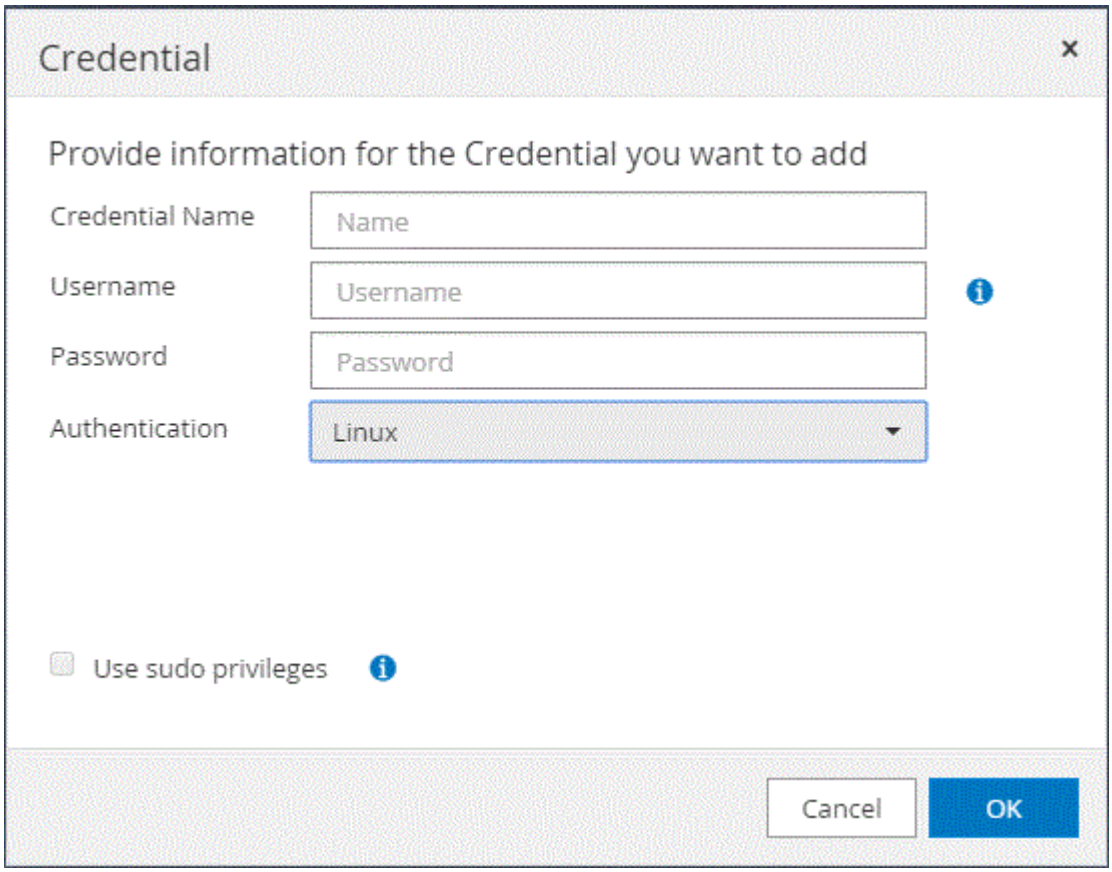
  Prima di installare i plug-in è necessario impostare le credenziali di Windows.

È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.




4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome utente | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName*<br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.<br>Applicabile solo agli utenti Linux. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:
   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Installa il plug-in SnapCenter per i database SAP HANA

### Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.

**Prima di iniziare**

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se

l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.

- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account di servizio gestito del gruppo su Windows Server 2016 o versioni successive per SAP HANA"

**Informazioni su questo compito**

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.
- Per consentire a SAP HANA System Replication di rilevare risorse sia sui sistemi primari che su quelli secondari, si consiglia di aggiungere entrambi i sistemi utilizzando l'utente root o sudo.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Tipo di host | Seleziona il tipo di host:<br>• Finestre<br>• Linux<br>Il plug-in per SAP HANA è installato sull'host client HDBSQL, che può trovarsi su un sistema Windows o Linux. |
| Nome host | Immettere il nome host della comunicazione. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br>È necessario configurare il client HDBSQL e HDBUserStore su questo host. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>Puoi visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale che hai fornito.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.
6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il plug-in per SAP HANA è installato sull'host client HDBSQL, che può trovarsi su un sistema Windows o Linux.<br><br>• Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, puoi personalizzare il percorso.<br>• Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/ NetApp/snapcenter. Facoltativamente, puoi personalizzare il percorso. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br>Fornire il nome gMSA nel seguente formato: domainName\accountName$.<br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo "Ignora controlli preliminari", l'host verrà convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di registro specifici dell'installazione si trovano in /custom_location/snapcenter/logs.

### Installa i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host

contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

**Prima di iniziare**

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

### Installa il plug-in SnapCenter per il database SAP HANA su host Linux utilizzando l'interfaccia della riga di comando

È necessario installare il plug-in SnapCenter per il database SAP HANA utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare il plug-in per il database SAP HANA in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

**Prima di iniziare**

- È necessario installare il plug-in per il database SAP HANA su ciascun host Linux in cui risiede il client HDBSQL.
- L'host Linux su cui si installa il plug-in SnapCenter per il database SAP HANA deve soddisfare i requisiti software, del database e del sistema operativo dipendenti.

  Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  https://imt.netapp.com/matrix/imt.jsp?components=121029;&solution=1259&isHWU&src=IMT

- Il plug-in SnapCenter per il database SAP HANA fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

**Passi**

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\ NetApp\ SnapCenter\Package Repository all'host in cui si desidera installare il plug-in per il database SAP HANA.

   È possibile accedere a questo percorso dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa il plug-in: `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 specifica la porta di comunicazione HTTPS di SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter .
   - -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter .
   - -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto plug-in SnapCenter per Linux.
   - DINSTALL_LOG_NAME specifica il nome del file di registro.

```
/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. Modificare il file /<directory di installazione>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = hana:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

### Monitora lo stato di installazione del plug-in per SAP HANA

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

#### Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.

3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

#### Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.

6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

#### Configurare il certificato CA con i servizi plug-in host di Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare

il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

#### Configurare il certificato CA per il servizio SnapCenter SAP HANA Plug-ins sull'host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio attendibile che come archivio chiavi.

##### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungi un certificato radice o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi per collegare trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elenca i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurare il nome alias dal certificato CA nel file
agent.properties.
```

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

**Informazioni su questo compito**

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è ' opt/ NetApp/snapcenter/scc/etc/crl'.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Configurare il certificato CA per il servizio SnapCenter SAP HANA Plug-ins sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato,

configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   *keytool -storepasswd -keystore keystore.jks*

   > Se il comando "keytool" non viene riconosciuto nel prompt dei comandi di Windows, sostituire il comando keytool con il suo percorso completo.

   *C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungi un certificato radice o intermedio:

   *keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks*

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

> Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   *keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS*

5. Elenca i certificati aggiunti nel keystore.

   *keytool -list -v -keystore keystore.jks*

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   *keytool -keypasswd -alias "nome_alias_in_CA_cert" -keystore keystore.jks*

8. Configurare il nome alias dal certificato CA nel file *agent.properties*.

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

**Informazioni su questo compito**

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .
- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.

2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

### Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

### Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

# Prepararsi alla protezione dei dati

## Prerequisiti per l'utilizzo del plug-in SnapCenter per il database SAP HANA

Prima di utilizzare il plug-in SnapCenter per il database SAP HANA, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.
- Installa Java 11 sul tuo host Linux o Windows.

  È necessario impostare il percorso Java nella variabile del percorso ambientale della macchina host.
- Se desideri la replica del backup, imposta SnapMirror e SnapVault.
- Installare il client HDBSQL sull'host in cui verrà installato il plug-in per il database SAP HANA.

  Configurare le chiavi di archivio utente per i nodi SAP HANA che verranno gestiti tramite questo host.
- Per il database SAP HANA 2.0SPS05, se si utilizza un account utente del database SAP HANA, assicurarsi di disporre delle seguenti autorizzazioni per eseguire operazioni di backup, ripristino e clonazione in SnapCenter Server:
  - Amministratore di backup
  - Catalogo letto
  - Amministratore del backup del database
  - Operatore di recupero database

## Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere i database SAP HANA

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere database SAP HANA di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

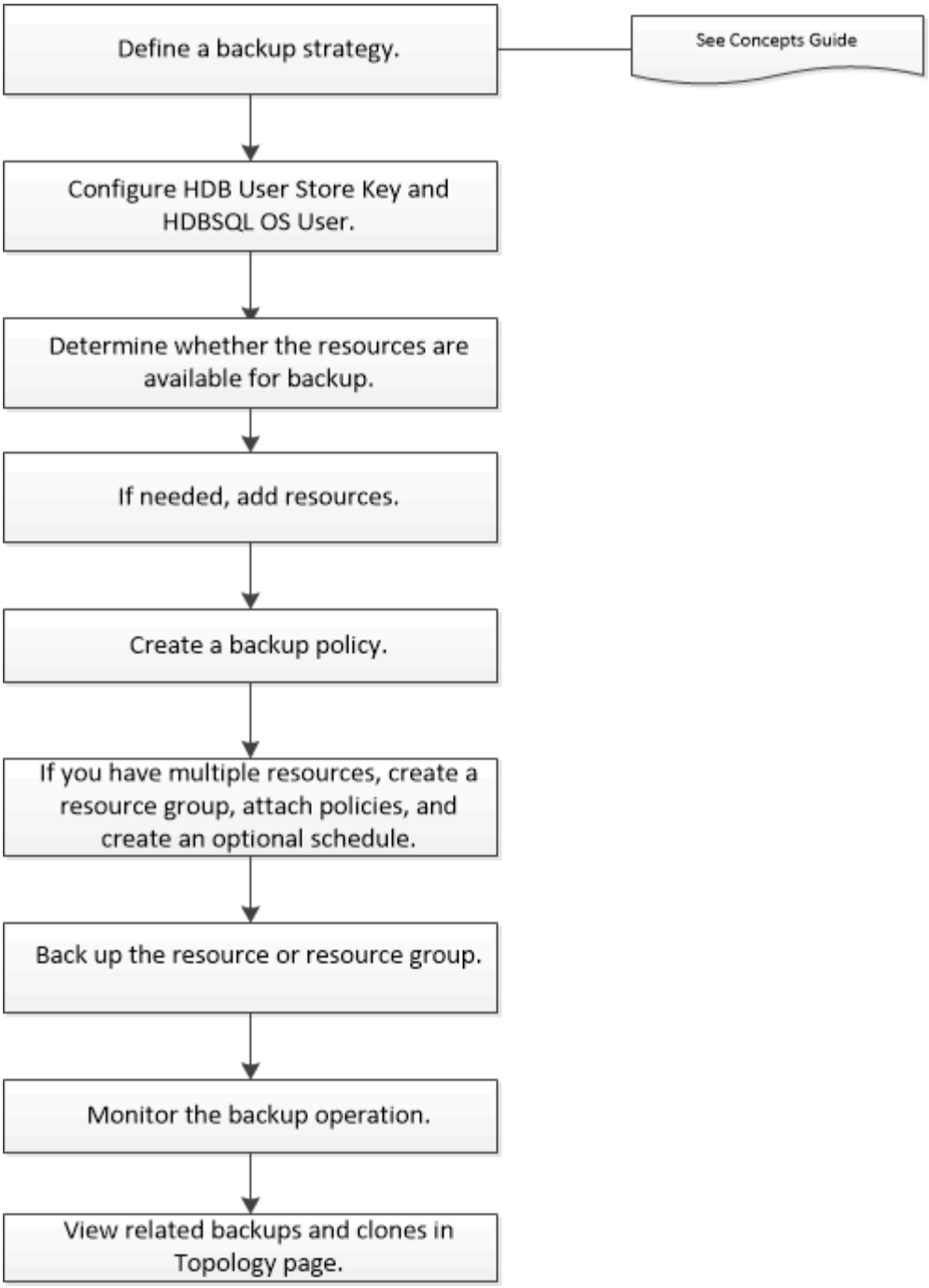
Pensa a un gruppo di risorse come a qualcosa che definisce cosa vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una polizza come a qualcosa che definisce il modo in cui vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database, è possibile creare un gruppo di risorse che includa tutti i database nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

# Eseguire il backup delle risorse SAP HANA

## Eseguire il backup delle risorse SAP HANA

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei database per il backup, la gestione dei criteri di backup, la creazione di gruppi di risorse e l'associazione di criteri, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento ai cmdlet del software SnapCenter" .

## Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA

È necessario configurare HDB User Store Key e HDBSQL OS User per eseguire operazioni di protezione dei dati sui database SAP HANA.

**Prima di iniziare**

- Se nel database SAP HANA non sono configurati né la chiave HDB Secure User Store né l'utente HDB SQL OS, viene visualizzata un'icona a forma di lucchetto rosso solo per le risorse rilevate automaticamente. Se durante una successiva operazione di individuazione, la chiave HDB Secure User Store configurata risulta errata o non consente l'accesso al database stesso, l'icona del lucchetto rosso riapparirà.
- È necessario configurare la chiave HDB Secure User Store e l'utente HDB SQL OS per poter proteggere il database o aggiungerlo a un gruppo di risorse per eseguire operazioni di protezione dei dati.
- È necessario configurare HDB SQL OS User per accedere al database di sistema. Se l'utente HDB SQL OS è configurato per accedere solo al database tenant, l'operazione di individuazione non riuscirà.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse** e quindi selezionare SnapCenter Plug-in per database SAP HANA dall'elenco.
2. Nella pagina Risorse, seleziona il tipo di risorsa dall'elenco **Visualizza**.
3. (Facoltativo) Fare clic e seleziona il nome host.

   Puoi quindi fare clic per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Configura database**.
5. Nella sezione Configura impostazioni database, immettere la chiave HDB Secure User Store.

   Viene visualizzato il nome host del plug-in e l'utente del sistema operativo HDB SQL viene automaticamente inserito in <sid>adm.
6. Fare clic su **OK**.

È possibile modificare la configurazione del database dalla pagina Topologia.

## Scopri le risorse e prepara i contenitori di database multitenant per la protezione dei dati

### Scopri automaticamente i database

Le risorse sono i database SAP HANA e il volume non dati sull'host Linux gestiti da SnapCenter. È possibile aggiungere queste risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database SAP HANA disponibili.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta della chiave di archiviazione utente HDB, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- È necessario aver configurato la chiave HDB Secure User Store e l'utente HDB SQL OS sull'host Linux.
  - È necessario configurare la chiave dell'archivio utenti HDB con SID adm user. Ad esempio, per il sistema HANA con A22 come SID, la chiave di archiviazione utente HDB deve essere configurata con a22adm.
- Il plug-in SnapCenter per il database SAP HANA non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK. È necessario fornire le informazioni di archiviazione per gli ambienti virtuali durante l'aggiunta manuale dei database.

**Informazioni su questo compito**

Dopo aver installato il plug-in, tutte le risorse presenti sull'host Linux vengono automaticamente rilevate e visualizzate nella pagina Risorse.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in per il database SAP HANA dall'elenco.
2. Nella pagina Risorse seleziona il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) Fai clic su * * , quindi selezionare il nome host.

   Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

4. Fare clic su **Aggiorna risorse** per scoprire le risorse disponibili sull'host.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il database si trova su un archivio NetApp e non è protetto, nella colonna Stato generale viene visualizzato Non protetto.
   - Se il database si trova su un sistema di archiviazione NetApp ed è protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup non eseguito. In caso contrario, lo stato cambierà in Backup non riuscito o Backup riuscito in base allo stato dell'ultimo backup.

Se nel database SAP HANA non è configurata una chiave HDB Secure User Store, accanto alla risorsa viene visualizzata un'icona a forma di lucchetto rosso. Se durante una successiva operazione di individuazione, la chiave HDB Secure User Store configurata risulta errata o non consente l'accesso al database stesso, l'icona del lucchetto rosso riapparirà.

È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

**Dopo aver finito**

È necessario configurare la chiave HDB Secure User Store e l'utente HDBSQL OS per poter proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

"Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA"

**Preparare contenitori di database multitenant per la protezione dei dati**

Per gli host SAP HANA registrati direttamente in SnapCenter, l'installazione o l'aggiornamento del plug-in SnapCenter per il database SAP HANA attiverà un rilevamento automatico delle risorse sull'host. Dopo aver installato o aggiornato il plug-in, per ogni risorsa MDC (Multitenant Database Container) presente sull'host del plug-in, verrà automaticamente rilevata un'altra risorsa MDC con un formato GUID diverso e registrata in SnapCenter. La nuova risorsa sarà nello stato "bloccato".

**Informazioni su questo compito**

Ad esempio, in SnapCenter 4.2, se la risorsa E90 MDC si trovava sull'host del plug-in ed era stata registrata manualmente, dopo l'aggiornamento a SnapCenter 4.3, un'altra risorsa E90 MDC con un GUID diverso verrà rilevata e registrata in SnapCenter.

> I backup associati alla risorsa di SnapCenter 4.2 e versioni precedenti devono essere conservati fino alla scadenza del periodo di conservazione. Una volta scaduto il periodo di conservazione, è possibile eliminare la vecchia risorsa MDC e continuare a gestire la nuova risorsa MDC rilevata automaticamente.

`Old MDC resource`è la risorsa MDC per un host plug-in aggiunto manualmente in SnapCenter 4.2 o versioni precedenti.

Per iniziare a utilizzare la nuova risorsa individuata in SnapCenter 4.3 per le operazioni di protezione dei dati, procedere come segue:

**Passi**

1. Nella pagina Risorse, seleziona la vecchia risorsa MDC con i backup aggiunti alla versione precedente SnapCenter e mettila in "modalità di manutenzione" dalla pagina Topologia.

   Se la risorsa fa parte di un gruppo di risorse, impostare il gruppo di risorse in "modalità di manutenzione".

2. Configurare la nuova risorsa MDC rilevata dopo l'aggiornamento a SnapCenter 4.3 selezionando la nuova risorsa dalla pagina Risorse.

   "Nuova risorsa MDC" è la nuova risorsa MDC scoperta dopo che SnapCenter Server e l'host del plug-in sono stati aggiornati alla versione 4.3. La nuova risorsa MDC può essere identificata come una risorsa con lo stesso SID della vecchia risorsa MDC, per un dato host e con un'icona a forma di lucchetto rosso accanto nella pagina Risorse.

3. Proteggi la nuova risorsa MDC scoperta dopo l'aggiornamento a SnapCenter 4.3 selezionando criteri di protezione, pianificazioni e impostazioni di notifica.
4. Eliminare i backup eseguiti in SnapCenter 4.2 o versioni precedenti in base alle impostazioni di conservazione.
5. Eliminare il gruppo di risorse dalla pagina Topologia.
6. Eliminare la vecchia risorsa MDC dalla pagina Risorse.

   Ad esempio, se il periodo di conservazione degli snapshot primari è di 7 giorni e quello degli snapshot secondari è di 45 giorni, una volta trascorsi 45 giorni e dopo l'eliminazione di tutti i backup, è necessario eliminare il gruppo di risorse e la vecchia risorsa MDC.

**Informazioni correlate**

"Configurare la chiave di archivio utente HDB e l'utente del sistema operativo HDBSQL per il database SAP HANA"

"Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia"

## Aggiungere manualmente le risorse all'host del plug-in

La scoperta automatica non è supportata per alcune istanze HANA. È necessario aggiungere queste risorse manualmente.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta della chiave di archiviazione utente HDB.
- Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse di tale sistema HANA in un gruppo di risorse ed eseguire un backup del gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.

"Crea gruppi di risorse e allega criteri" .

**Informazioni su questo compito**

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

> Nel caso in cui vengano scoperte le risorse di cui sopra, le operazioni di protezione dei dati non saranno supportate su tali risorse.

- Configurazione multi-host HANA
- Più istanze sullo stesso host
- Replicazione del sistema HANA con scalabilità multilivello
- Ambiente di replica a cascata in modalità di replicazione del sistema

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fai clic su **Risorse**.
2. Nella pagina Risorse, fare clic su **Aggiungi database SAP HANA**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Tipo di risorsa | Inserisci il tipo di risorsa. I tipi di risorsa sono Contenitore singolo, Contenitore di database multitenant (MDC) e Volume non dati. |
| Nome del sistema HANA | Immettere il nome descrittivo del sistema SAP HANA. Questa opzione è disponibile solo se sono stati selezionati i tipi di risorsa Contenitore singolo o MDC. |
| SID | Inserire l'ID del sistema (SID). Il sistema SAP HANA installato è identificato da un singolo SID. |
| Host plug-in | Selezionare l'host del plug-in. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Chiavi di archiviazione utente protette HDB | Inserisci la chiave per connetterti al sistema SAP HANA.<br><br>La chiave contiene le informazioni di accesso per connettersi al database.<br><br>Per la replica del sistema SAP HANA, la chiave utente secondaria non viene convalidata. Verrà utilizzato durante l'acquisizione. |
| Utente del sistema operativo HDBSQL | Immettere il nome utente per il quale è configurata la chiave HDB Secure User Store. Per Windows, è obbligatorio che l'utente del sistema operativo HDBSQL sia l'utente SYSTEM. Pertanto, è necessario configurare la chiave HDB Secure User Store per l'utente SYSTEM. |

4. Nella pagina Fornisci impronta di archiviazione, seleziona un sistema di archiviazione e scegli uno o più volumi, LUN e qtree, quindi fai clic su **Salva**.

   Facoltativo: puoi cliccare su * + * icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

5. Rivedi il riepilogo e poi clicca su **Fine**.

   I database vengono visualizzati insieme a informazioni quali SID, host del plug-in, gruppi di risorse e policy associati e stato generale

Se si desidera consentire agli utenti di accedere alle risorse, è necessario assegnare le risorse agli utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

"Aggiungi un utente o un gruppo e assegna ruoli e risorse"

Dopo aver aggiunto i database, è possibile modificare i dettagli del database SAP HANA.

Non è possibile modificare quanto segue se sono presenti backup associati alla risorsa SAP HANA:

- Contenitori di database multi-tenant (MDC): SID o host client (plug-in) HDBSQL
- Contenitore singolo: host client (plug-in) SID o HDBSQL
- Volume non dati: nome della risorsa, SID associato o host del plug-in

## Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse del database SAP HANA, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup.

  Per maggiori dettagli, consultare le informazioni sulla definizione di una strategia di protezione dei dati per i database SAP HANA.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta di risorse.
- Se si stanno replicando gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

  Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

- Replica del sistema SAP HANA
  - È possibile proteggere il sistema SAP HANA primario e possono essere eseguite tutte le operazioni di protezione dei dati.
  - È possibile proteggere il sistema SAP HANA secondario, ma non è possibile creare backup.

    Dopo il failover, tutte le operazioni di protezione dei dati possono essere eseguite poiché il sistema SAP HANA secondario diventa il sistema SAP HANA primario.

  Non è possibile creare un backup per il volume dati SAP HANA, ma SnapCenter continua a proteggere i volumi non dati (NDV).

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   - Scegli il tipo di archiviazione
   - Scegli il tipo di backup:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Crea un backup utilizzando la tecnologia Snapshot | Selezionare **Basato su snapshot**. |
| Eseguire un controllo di integrità del database | Selezionare **Backup basato su file**. Viene eseguito il backup solo dei tenant attivi. |

6. Nella pagina Snapshot e replica, procedere come segue:
   - Specificare il tipo di pianificazione selezionando **Su richiesta**, **Ora**, **Giornaliera**, **Settimanale** o **Mensile**.

     È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente anche di assegnare pianificazioni di backup diverse a ciascuna policy.

     Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

7. Nella pagina Snapshot e replica, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Tipo di backup:

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot più vecchi vengono eliminati per primi.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP .<br><br>Per i backup basati su copie Snapshot, è necessario impostare il conteggio di conservazione su 2 o superiore se si prevede di abilitare la replica SnapVault . Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.<br><br>Per la replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un unico gruppo di risorse. In questo modo si garantisce che venga conservato il numero corretto di backup.<br><br>Per la replica del sistema SAP HANA, il numero totale di snapshot acquisiti sarà pari al set di conservazione per il gruppo di risorse. La rimozione dello Snapshot più vecchio si basa sul nodo in cui si trova lo Snapshot più vecchio. Ad esempio, la conservazione è impostata su 7 per un gruppo di risorse con SAP HANA System Replication primario e SAP HANA System Replication secondario. È possibile acquisire un massimo di 7 snapshot alla volta, inclusi sia SAP HANA System Replication primario che SAP HANA System Replication secondario. |

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

8. Selezionare un'etichetta Snapshot.

> È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

9. Per i backup basati su copie snapshot, nella sezione Seleziona opzioni di replica secondaria, seleziona una o entrambe le seguenti opzioni di replica secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapMirror dopo aver creato una copia Snapshot locale** | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror .<br><br>Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e si seleziona solo questa opzione, lo Snapshot creato sul primario non verrà trasferito alla destinazione, ma verrà elencato nella destinazione. Se si seleziona questo snapshot dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il messaggio di errore "La posizione secondaria non è disponibile per il backup con vault/mirroring selezionato".<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia" . |

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapVault dopo aver creato una copia Snapshot locale** | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ).<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per maggiori informazioni su SnapLock Vault vedere "Eseguire il commit delle copie Snapshot su WORM in una destinazione vault"<br><br>Vedere "Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia" . |
| **Errore nel conteggio dei nuovi tentativi** | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

10. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Informazioni su questo compito**

- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

- L'aggiunta di nuovi database senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse.<br><br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br><br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.

   Ciò aiuta a filtrare le informazioni sullo schermo.

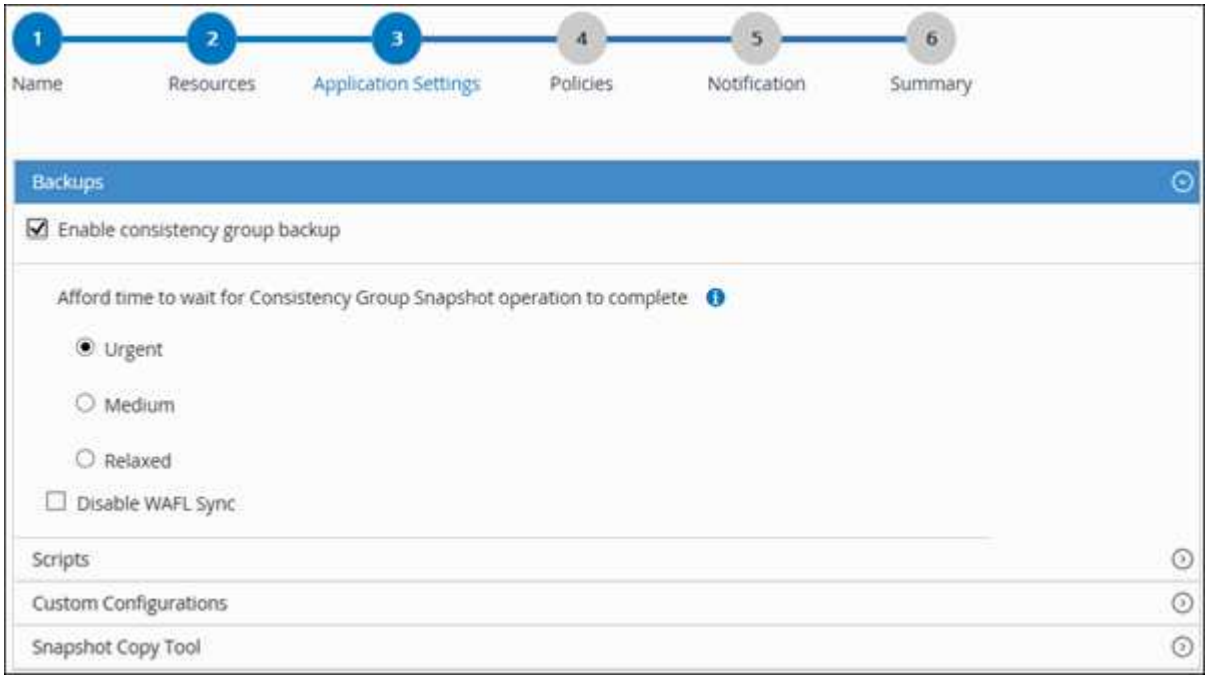
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Concediti del tempo per attendere il completamento dell'operazione Consistency Group Snapshot | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione Snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+




a. Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, Snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

b. Fare clic sulla freccia **Configurazioni personalizzate** e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

| Parametro | Collocamento | Descrizione |
| --- | --- | --- |
| ARCHIVE_LOG_ENABLE | (S/N) | Abilita la gestione dei log di archivio per eliminare i log di archivio. |

| Parametro | Collocamento | Descrizione |
| --- | --- | --- |
| CONSERVAZIONE_ARCHIVIO_LOG | numero_di_giorni | Specifica il numero di giorni per cui vengono conservati i registri di archivio.<br><br>Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Specifica il percorso della directory che contiene i log di archivio. |
| ARCHIVE_LOG_EXT | estensione_file | Specifica la lunghezza dell'estensione del file di registro dell'archivio.<br><br>Ad esempio, se il registro di archivio è log_backup_0_0_0_0.16151855 1942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (S/N) | Consente la gestione dei log di archivio all'interno delle sottodirectory.<br><br>È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory. |

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in Linux SAP HANA e non sono supportate per il database SAP HANA registrato come plug-in centralizzato di Windows.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows e impostare il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile. | Selezionare * SnapCenter con coerenza del file system*.<br><br>Questa opzione non è applicabile al plug-in SnapCenter per il database SAP HANA. |
| SnapCenter per creare uno Snapshot del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| Per immettere il comando da eseguire sull'host per creare copie Snapshot. | Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare uno snapshot. |

7. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

   b. Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

      Dove policy_name è il nome della policy selezionata.

      Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse SAP HANA sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza

primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.

- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

      Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai

clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:
   a. Selezionare il tipo di criterio di replica.

      La politica di replica sincrona non è supportata.

   b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.
   c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

      Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| **Se lo desidera…** | **Fai questo…** |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per il database SAP HANA

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei database SAP HANA.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmStorageConnection
```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Aggiungere l'host di comunicazione SAP HANA a SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode hana
```

5. Installare il pacchetto e il plug-in SnapCenter per il database SAP HANA sull'host.

   Per Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
hana
```

   Per Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode hana
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Imposta il percorso per il client HDBSQL.

   Per Windows:

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
hana -configSettings @{"HANA_HDBSQL_CMD" = "C:\Program
Files\sap\hdbclient\hdbsql.exe"}
```

   Per Linux:

```
Set-SmConfigSettings -Plugin -HostName scs-hana.gdl.englab.netapp.com
-PluginCode hana -configSettings
@{"HANA_HDBSQL_CMD"="/usr/sap/hdbclient/hdbsql"}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei database SAP HANA

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il

backup dalla pagina Risorse.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per l'operazione di backup basata su copia snapshot, assicurarsi che tutti i database tenant siano validi e attivi.
- Per creare backup di replica del sistema SAP HANA, si consiglia di aggiungere tutte le risorse del sistema SAP HANA in un gruppo di risorse. Ciò garantisce un backup senza interruzioni durante la modalità takeover-failback.

  "Crea gruppi di risorse e allega criteri" .

  "Eseguire il backup dei gruppi di risorse"

- Se si desidera creare un backup basato su file quando uno o più database tenant sono inattivi, impostare il parametro ALLOW_FILE_BASED_BACKUP_IFINACTIVE_TENANTS_PRESENT su **YES** nel file delle proprietà HANA utilizzando `Set-SmConfigSettings` cmdlet.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter"

- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Seleziona * * , quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

     Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
|---|---|
| Concediti del tempo per attendere il completamento dell'operazione "Consistency Group Snapshot" | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

   - Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.

     È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .
   - Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   - Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter per creare uno Snapshot a livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare uno Snapshot | Selezionare * SnapCenter con coerenza del file system*. |
| Per immettere il comando per creare uno Snapshot | Selezionare **Altro**, quindi immettere il comando per creare uno Snapshot. |

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
    - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

      Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

    - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

      Per aumentare la dimensione dell'heap Java, individuare il file di script */opt/netapp/init_scripts/scvservice*. In quello script, il comando *do_start method* avvia il servizio plug-in SnapCenter VMware. Aggiornare il comando come segue: *Java -jar -Xmx8192M -Xms4096M*

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse utilizzando il cmdlet Add-SmResources.

   Questo esempio mostra come aggiungere un database SAP HANA di tipo SingleContainer:

```
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_'
```

Questo esempio mostra come aggiungere un database SAP HANA di tipo MultipleContainers:

```
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'
```

Questo esempio mostra come creare una risorsa di volume non dati:

```
C:\PS> Add-SmResource -HostName 'SNAPCENTERN42.sccore.test.com'
-PluginCode 'hana' -ResourceName NonDataVolume -ResourceType
NonDataVolume -StorageFootPrint
(@{"VolumeName"="ng_pvol";"StorageSystem"="vserver_scauto_primary"})
-sid 'S10'
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea un criterio di backup per un backup basato su copia Snapshot:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_snapshotbased -PolicyType
   Backup -PluginPolicyType hana -BackupType SnapShotBasedBackup
   ```

   Questo esempio crea un criterio di backup per un backup basato su file:

   ```
   C:\PS> Add-SmPolicy -PolicyName hana_Filebased -PolicyType Backup
   -PluginPolicyType hana -BackupType FileBasedBackup
   ```

4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio protegge una singola risorsa contenitore:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="SID"} -Description
test -usesnapcenterwithoutfilesystemconsistency
```

Questo esempio protegge una risorsa composta da più contenitori:

```
C:\PS> Add-SmProtectResource -PluginCode HANA  -Policies
hana_snapshotbased,hana_Filebased
 -Resources @{"Host"="host.example.com";"UID"="MDC\SID"}
-Description test -usesnapcenterwithoutfilesystemconsistency
```

Questo esempio crea un nuovo gruppo di risorse con i criteri e le risorse specificati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Resources
@(@{"Host"="sccorelinux61.sccore.test.com";"Uid"="SID"},@{"Host"="sc
corelinux62.sccore.test.com";"Uid"="MDC\SID"})
  -Policies hana_snapshotbased,hana_Filebased
-usesnapcenterwithoutfilesystemconsistency  -plugincode 'HANA'
```

Questo esempio crea un gruppo di risorse di volume non dati:

```
C:\PS> Add-SmResourceGroup -ResourceGroupName
'Mixed_RG_backup_when_Remove_Backup_throguh_BackupName_windows'
-Resources
@(@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="H11";"PluginName"=
"hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="MDC\H31";"Pl
uginName"="hana"},@{"Host"="SNAPCENTERN42.sccore.test.com";"Uid"="No
nDataVolume\S10\NonDataVolume";"PluginName"="hana"}) -Policies
hanaprimary
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

   Questo esempio mostra come eseguire il backup di un gruppo di risorse:

```
C:\PS> New-SMBackup -ResourceGroupName
'ResourceGroup_with_SingleContainer_MultipleContainers_Resources'
-Policy hana_snapshotbased
```

   Questo esempio esegue il backup di una risorsa protetta:

```
C:\PS> New-SMBackup -Resources
@{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
-Policy hana_Filebased
```

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet Get-smJobSummaryReport.

```
PS C:\> Get-smJobSummaryReport -JobID 123
```

7. Monitorare i dettagli del processo di backup, come ID del backup e nome del backup, per eseguire operazioni di ripristino o clonazione utilizzando il cmdlet Get-SmBackupReport.

```
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 :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Informazioni su questo compito**

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando e quindi selezionando il tag. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di backup dei database SAP HANA

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso

- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni di protezione dei dati sui database SAP HANA nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup per SAP HANA

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni del database SAP HANA nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario

mediante la tecnologia SnapMirror .

- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

  Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la **scheda Riepilogo** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Scheda riepilogativa** mostra il numero totale di backup basati su file, backup basati su copie snapshot e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di

scadenza SnapLock più lungo viene recuperato da ONTAP.

Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

- Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
- Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

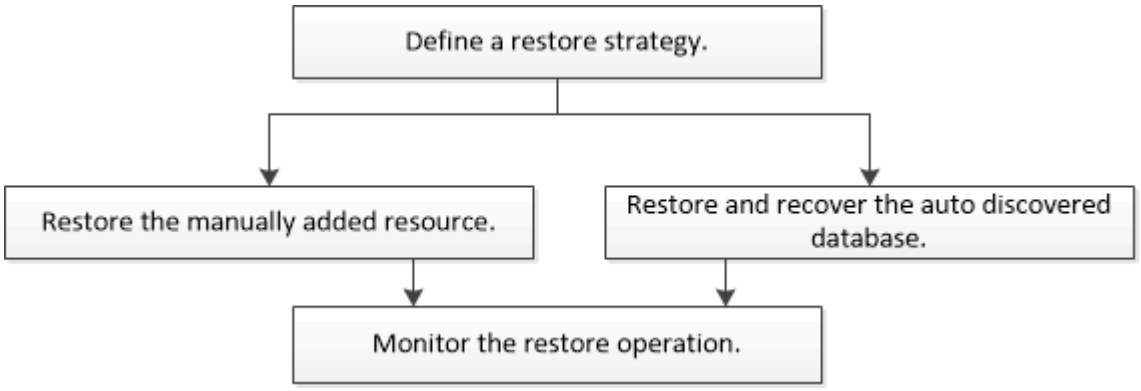
7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su .

# Ripristinare i database SAP HANA

## Ripristina flusso di lavoro

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup di risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non recuperati. Per ripristinare i backup eseguiti in SnapCenter 4.2 è necessario utilizzare HANA Studio o script di ripristino HANA esterni a SnapCenter .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

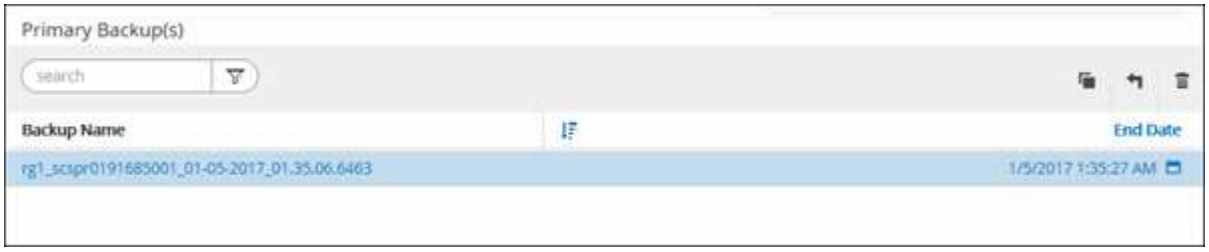
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * .




6. Nella pagina Ambito di ripristino, selezionare **Risorsa completa** o **Livello file**.

   a. Se si seleziona **Risorsa completa**, verranno ripristinati tutti i volumi di dati configurati del database SAP HANA.

      Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

   b. Se selezioni **Livello file**, puoi selezionare **Tutti** oppure selezionare i volumi o i qtree specifici, quindi immettere il percorso relativo a tali volumi o qtree, separati da virgole

      - È possibile selezionare più volumi e qtree.
      - Se il tipo di risorsa è LUN, viene ripristinato l'intero LUN.

        È possibile selezionare più LUN.

Se si seleziona **Tutti**, verranno ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup del database rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in*

*Creator\etc\allowed_commands.config*

- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Dopo l'aggiornamento a SnapCenter 4.3, i backup eseguiti in SnapCenter 4.2 possono essere ripristinati ma non recuperati. Per ripristinare i backup eseguiti in SnapCenter 4.2 è necessario utilizzare HANA Studio o script di ripristino HANA esterni a SnapCenter .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

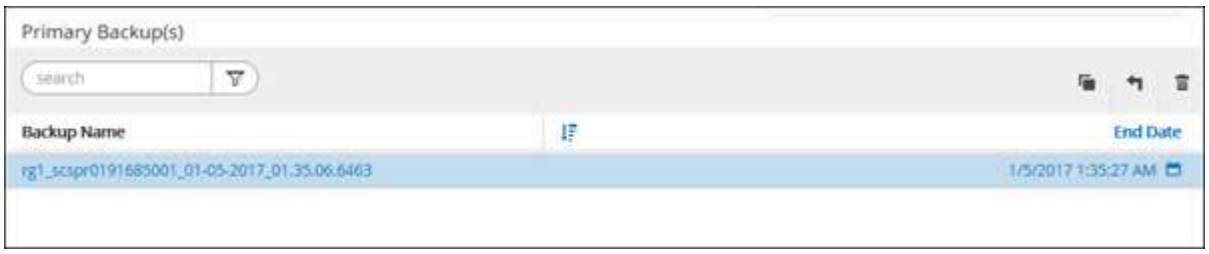
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.




6. Nella pagina Ripristina ambito, seleziona **Risorsa completa** per ripristinare i volumi di dati configurati del database SAP HANA.

È possibile selezionare **Risorsa completa** (con o senza **Ripristino volume**) oppure **Database tenant**.

L'operazione di ripristino non è supportata da SnapCenter Server per più tenant quando l'utente seleziona l'opzione **Database tenant** o **Ripristino completo**. Per eseguire l'operazione di ripristino è necessario utilizzare HANA Studio o lo script Python HANA.

a. Selezionare **Ripristina volume** se si desidera ripristinare l'intero volume.

   Questa opzione è disponibile per i backup eseguiti in SnapCenter 4.3 in ambienti NFS.

   Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata. Questa opzione è applicabile quando per il ripristino è selezionata l'opzione **Completa risorsa** con **Ripristino volume**.

b. Selezionare **Database tenant**.

   Questa opzione è disponibile solo per le risorse MDC.

   Assicurarsi di arrestare il database tenant prima di eseguire l'operazione di ripristino.

Se si seleziona l'opzione **Database tenant**, è necessario utilizzare HANA Studio o script di ripristino HANA esterni a SnapCenter per eseguire l'operazione di ripristino.

7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:

| Se tu… | Fai questo… |
|---|---|
| Vuoi recuperare il più vicino possibile all'ora corrente | Seleziona **Ripristina allo stato più recente**. Per le risorse di un singolo contenitore, specificare una o più posizioni di backup di log e cataloghi.<br><br>Per le risorse del contenitore di database multi-tenant (MDC), specificare una o più posizioni di backup del log e la posizione del catalogo di backup.<br><br>Per le risorse MDC, il percorso deve contenere sia i log del database di sistema che quelli del database tenant. |

| Se tu… | Fai questo… |
| --- | --- |
| Vuoi ripristinare il punto temporale specificato | Seleziona **Recupera fino a un punto nel tempo**.<br><br>a. Seleziona il fuso orario.<br><br>Il fuso orario del browser è popolato per impostazione predefinita.<br><br>Il fuso orario selezionato insieme all'ora immessa vengono convertiti in GMT assoluto.<br><br>b. Inserisci data e ora. Ad esempio, l'host HANA Linux si trova a Sunnyvale, CA e l'utente a Raleigh, NC sta recuperando i log in SnapCenter.<br><br>La differenza oraria tra queste due località è di 3 ore e, poiché l'utente ha effettuato l'accesso da Raleigh, NC, il fuso orario predefinito del browser che verrà selezionato nella GUI è GMT-04:00.<br><br>Se l'utente desidera eseguire un ripristino alle 5 del mattino a Sunnyvale, CA, deve impostare il fuso orario del browser sul fuso orario dell'host Linux HANA, ovvero GMT-07:00, e specificare la data e l'ora come 5:00.<br><br>Per le risorse di un singolo contenitore, specificare una o più posizioni di backup di log e cataloghi.<br><br>Per le risorse MDC, specificare una o più posizioni di backup del registro e la posizione del catalogo di backup.<br><br>Per le risorse MDC, il percorso deve contenere sia i log del database di sistema che quelli del database tenant. |
| Vuoi ripristinare un backup di dati specifico | Selezionare **Ripristina nel backup dei dati specificato**. |
| Non voglio recuperare | Selezionare **Nessun recupero**. È necessario eseguire manualmente l'operazione di ripristino dallo studio HANA. |

È possibile ripristinare solo i backup eseguiti dopo l'aggiornamento a SnapCenter 4.3, a condizione che sia l'host sia il plug-in siano stati aggiornati a SnapCenter 4.3 e che i backup selezionati per il ripristino siano stati eseguiti dopo che la risorsa è stata convertita o rilevata come risorsa rilevata automaticamente.

8. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un

processo di ripristino.

I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

    È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di ripristino dei database SAP HANA

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clona i backup delle risorse SAP HANA

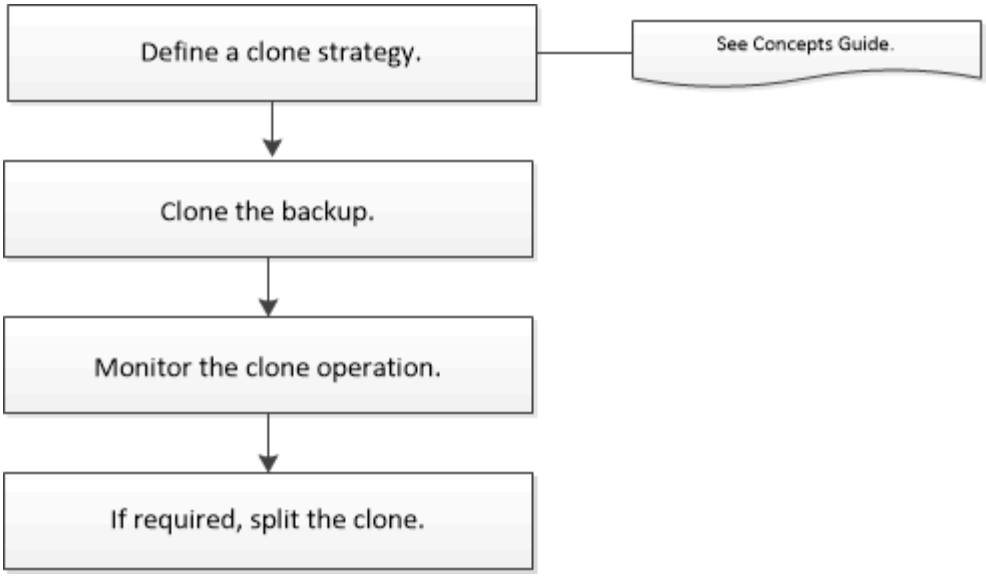
## Flusso di lavoro di clonazione

Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

**Informazioni su questo compito**

- È possibile clonare sul server SAP HANA di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione
  - Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
  - Per recuperare dati che sono stati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

## Clonare un backup del database SAP HANA

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

**Prima di iniziare**

- Avresti dovuto eseguire il backup delle risorse o del gruppo di risorse.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Non è possibile clonare backup basati su file.
- Il server clone di destinazione deve avere lo stesso SID dell'istanza SAP HANA fornito nel campo SID clone di destinazione.
- Per i comandi pre-clone o post-clone, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Per Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Per Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per informazioni sulle limitazioni dell'operazione di divisione del clone, vedere "Guida alla gestione dell'archiviazione logica ONTAP 9" .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, host, gruppi di risorse e policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Host del plug-in | Selezionare l'host su cui montare il clone e il plug-in verrà installato. |
| SID clone di destinazione | Immettere l'ID dell'istanza SAP HANA da clonare dai backup esistenti. |
| Indirizzo IP di esportazione NFS | Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati. |
| Iniziatore iSCSI | Immettere il nome dell'iniziatore iSCSI dell'host su cui vengono esportati i LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN. |
| Protocollo | Inserire il protocollo LUN. Questa opzione è disponibile solo se è stato selezionato il tipo di risorsa LUN. |

   Se la risorsa selezionata è una LUN e si sta clonando da un backup secondario, vengono elencati i volumi di destinazione. Una singola origine può avere più volumi di destinazione.

   Prima di procedere alla clonazione, è necessario assicurarsi che l'iniziatore iSCSI o l'FCP siano presenti, configurati e registrati in host alternativi.

7. Nella pagina Script, procedere come segue:

Gli script vengono eseguiti sull'host del plug-in.

a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
   - Comando pre-clone: elimina i database esistenti con lo stesso nome
   - Comando post-clonazione: verifica un database o avvia un database.

b. Immettere il comando mount per montare un file system su un host.

   Comando di montaggio per un volume o qtree su una macchina Linux:

Esempio per NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Recuperare i backup per eseguire l'operazione di clonazione utilizzando il cmdlet Get-SmBackup.

   Questo esempio mostra che sono disponibili due backup per la clonazione:

```
 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. Avvia un'operazione di clonazione da un backup esistente e specifica gli indirizzi IP di esportazione NFS su cui vengono esportati i volumi clonati.

Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs pari a 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
shivscc4.sccore.test.com -mountcommand 'mount
10.232.206.169:%hana73data_Clone /hana83data'
-preclonecreatecommands '/home/scripts/scpre_clone.sh'
-postclonecreatecommands '/home/scripts/scpost_clone.sh'
```

Se NFSExportIPs non è specificato, l'impostazione predefinita è l'esportazione nell'host di destinazione del clone.

4. Verificare che i backup siano stati clonati correttamente utilizzando il cmdlet Get-SmCloneReport per visualizzare i dettagli del processo di clonazione.

   È possibile visualizzare dettagli quali ID clone, data e ora di inizio, data e ora di fine.

```
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          :
```

## Monitorare le operazioni di clonazione del database SAP HANA

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

**Informazioni correlate**

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

## Eliminare o dividere i cloni del database SAP HANA dopo l'aggiornamento SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non saranno più visibili. È possibile eliminare il clone o dividere i cloni dalla pagina Topologia della risorsa da cui sono stati creati i cloni.

### Informazioni su questo compito

Se si desidera individuare l'impronta di archiviazione dei cloni nascosti, eseguire il seguente comando: `Get-SmClone -ListStorageFootprint`

### Passi

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-smresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa padre dalla pagina Risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Gestisci copie, selezionare i cloni dai sistemi di archiviazione primari o secondari (con mirroring o replica).
6. Seleziona i cloni e poi clicca per eliminare i cloni o fare clic per dividere i cloni.
7. Fare clic su **OK**.

# Proteggere i database Oracle

## Panoramica del plug-in SnapCenter per Oracle Database

### Cosa puoi fare con il plug-in per Oracle Database

Il plug-in SnapCenter per Oracle Database è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni dei database Oracle.

Il plug-in per Oracle Database automatizza il backup, la catalogazione e la decatalogazione con Oracle Recovery Manager (RMAN), la verifica, il montaggio, lo smontaggio, il ripristino, il recupero e la clonazione dei database Oracle nel tuo ambiente SnapCenter . Il plug-in per Oracle Database installa il plug-in SnapCenter per UNIX per eseguire tutte le operazioni di protezione dei dati.

È possibile utilizzare il plug-in per Oracle Database per gestire i backup dei database Oracle che eseguono applicazioni SAP. Tuttavia, l'integrazione con SAP BR*Tools non è supportata.

- Eseguire il backup dei file di dati, dei file di controllo e dei file di registro di archivio.

  Il backup è supportato solo a livello di database contenitore (CDB).

- Ripristino e recupero di database, CDB e database collegabili (PDB).

  Il ripristino incompleto dei PDB non è supportato.

- Creare cloni di database di produzione fino a un determinato punto nel tempo.

  La clonazione è supportata solo a livello CDB.

- Verificare immediatamente i backup.
- Montare e smontare i backup dei dati e dei log per le operazioni di ripristino.
- Pianificare le operazioni di backup e verifica.
- Monitorare tutte le operazioni.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.
- Automatizza le operazioni di backup, ripristino, recupero, verifica, montaggio, smontaggio e clonazione basate sulle applicazioni per i database Oracle nel tuo ambiente SnapCenter
- Supporta i database Oracle per SAP, tuttavia l'integrazione con SAP BR*Tools non è fornita

### Caratteristiche del plug-in per Oracle Database

Il plug-in per Oracle Database si integra con il database Oracle sull'host Linux o AIX e con le tecnologie NetApp sul sistema di storage.

- Interfaccia utente grafica unificata

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino, recupero e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli

accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- Amministrazione centrale automatizzata

  È possibile pianificare operazioni di backup e clonazione, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- Tecnologia NetApp Snapshot non disruptiva

  SnapCenter utilizza la tecnologia NetApp Snapshot con il plug-in per Oracle Database e il plug-in per UNIX per eseguire il backup dei database. Gli snapshot occupano uno spazio di archiviazione minimo.

Il plug-in per Oracle Database offre inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino, clonazione, montaggio, smontaggio e verifica
- Rilevamento automatico dei database Oracle configurati sull'host
- Supporto per la catalogazione e la decatalogazione tramite Oracle Recovery Manager (RMAN)
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di autorizzazioni a livello di applicazione.

- Supporto per Archive Log Management (ALM) per operazioni di ripristino e clonazione
- Creazione di copie puntuali e a basso consumo di spazio dei database di produzione per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità di gruppo di coerenza (CG) di ONTAP come parte della creazione di backup in ambienti SAN e ASM
- Verifica del backup automatizzata e non distruttiva
- Capacità di eseguire più backup contemporaneamente su più host di database

  In un'unica operazione, gli snapshot vengono consolidati quando i database in un singolo host condividono lo stesso volume.

- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per NFS, iSCSI, Fibre Channel (FC), RDM, VMDK su NFS e VMFS e ASM su NFS, SAN, RDM e VMDK
- Supporto per la funzionalità Selective LUN Map (SLM) di ONTAP

  Abilitata per impostazione predefinita, la funzionalità SLM rileva periodicamente i LUN che non dispongono di percorsi ottimizzati e li corregge. È possibile configurare SLM modificando i parametri nel file scu.properties che si trova in /var/opt/snapcenter/scu/etc.

  - È possibile disabilitare questa funzione impostando il valore del parametro ENABLE_LUNPATH_MONITORING su false.
  - È possibile specificare la frequenza con cui i percorsi LUN verranno corretti automaticamente assegnando il valore (in ore) al parametro LUNPATH_MONITORING_INTERVAL. Per informazioni su SLM, vedere "Sezione Amministrazione SAN ONTAP 9" .

- Supporto per la memoria non volatile express (NVMe) su Linux
  - L'utilità NVMe deve essere installata sull'host.

    È necessario installare l'utilità NVMe per clonare o montare su un host alternativo.
  - Le operazioni di backup, ripristino, clonazione, montaggio, smontaggio, catalogazione, decatalogazione e verifica sono supportate sull'hardware NVMe, ad eccezione degli ambienti virtualizzati come RDM.

    Le operazioni sopra descritte sono supportate su dispositivi senza partizioni o con una sola partizione.

    > È possibile configurare una soluzione multipathing per i dispositivi NVMe impostando l'opzione multipathing nativa nel kernel. Il multipathing Device Mapper (DM) non è supportato.
  - I flussi di lavoro di backup, ripristino, clonazione, montaggio, smontaggio, catalogazione, decatalogazione e verifica sono supportati su NVMe tramite TCP/IP.
  - I flussi di lavoro di backup, ripristino, clonazione, montaggio, smontaggio, catalogazione, decatalogazione e verifica sono supportati sul layout VMDK creato su NVMe tramite TCP/IP.
- Supporta la sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]) che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.
- Supporta qualsiasi utente non predefinito anziché Oracle e Grid.

  Per supportare gli utenti non predefiniti, è necessario impostarli modificando i valori dei parametri nel file **sco.properties** situato in *file /var/opt/snapcenter/sco/etc/*.

  I valori predefiniti dei parametri sono impostati come oracle e grid.
  - DB_USER=oracolo
  - DB_GROUP=oinstall
  - GI_USER=griglia
  - GI_GROUP=oinstall

## Tipi di archiviazione supportati dal plug-in per Oracle Database

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che virtuali. È necessario verificare il supporto per il tipo di archiviazione in uso prima di installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX.

SnapCenter non supporta il provisioning dello storage per Linux e AIX.

### Tipi di archiviazione supportati su Linux

Nella tabella seguente sono elencati i tipi di archiviazione supportati su Linux.

| Macchina | Tipo di archiviazione |
| --- | --- |
| Server fisico | • LUN connesse a FC<br>• LUN connesse tramite iSCSI<br>• Volumi connessi tramite NFS<br>• NVMe-FC<br>• NVMe/TCP |
| VMware ESXi | • LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host.<br><br>È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES.<br><br>• LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI<br>• VMDK su datastore NFS<br>• VMDK su VMFS creati tramite NVMe/TCP<br><br>RAC è supportato su ESX 8.0U2 che supporta VMDK condiviso<br><br>• Volumi NFS connessi direttamente al sistema guest<br>• Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

### Tipi di archiviazione supportati su AIX

Nella tabella seguente sono elencati i tipi di archiviazione supportati su AIX.

| Macchina | Tipo di archiviazione |
| --- | --- |
| Server fisico | • LUN connesse tramite FC e tramite iSCSI.<br><br>In un ambiente SAN sono supportati i file system ASM, LVM e SAN.<br><br>NFS su AIX e sul file system non è supportato.<br><br>• Sistema di file journaling avanzato (JFS2)<br><br>Supporta la registrazione in linea sui file system SAN e sul layout LVM. |

IL "Strumento matrice di interoperabilità NetApp" contiene le informazioni più recenti sulle versioni supportate.

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per Plug-in per Oracle

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter . Se si utilizza SnapMirror ActiveSync, utilizzare le pianificazioni predefinite SnapMirror o SnapVault sia per SnapMirror ActiveSync che per le relazioni asincrone.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Privilegi ONTAP minimi richiesti per il plug-in per Oracle

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

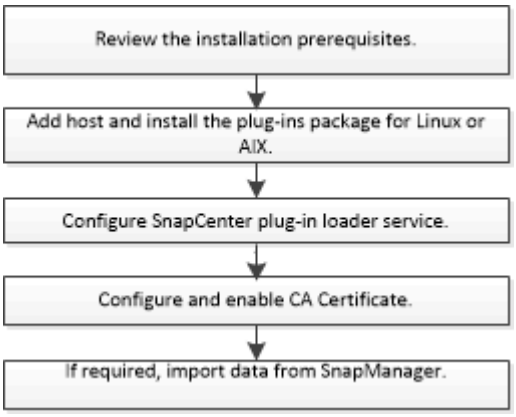
- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - spettacolo attributo lun
  - lun crea
  - lun cancella
  - geometria lun
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina
  - rinomina lun igroup
  - spettacolo di gruppo lun
  - mappatura lun aggiungi-nodi-di-segnalazione
  - creazione di mappatura lun
  - eliminazione della mappatura LUN
  - rimozione-nodi-di-segnalazione-mapping-lun
  - spettacolo di mappatura lun
  - lun modifica
  - lun sposta-in-volume
  - lun offline
  - lun online
  - lun persistent-reservation clear
  - ridimensionamento lun
  - serie lun
  - spettacolo di lunedì
  - aggiunta regola politica snapmirror
  - modifica regola policy snapmirror
  - regola di rimozione della policy di SnapMirror
  - mostra politica di SnapMirror
  - ripristino snapmirror
  - spettacolo snapmirror
  - snapmirror mostra-cronologia
  - aggiornamento snapmirror
  - snapmirror update-ls-set
  - elenco-destinazioni snapmirror

- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online
- modifica del volume
- creazione di volume qtree
- eliminazione del volume qtree
- modifica del volume qtree
- volume qtree mostra
- limitazione del volume
- spettacolo di volume
- creazione di snapshot del volume
- eliminazione snapshot volume
- modifica snapshot volume
- rinomina snapshot volume
- ripristino snapshot del volume
- file di ripristino dello snapshot del volume
- mostra snapshot del volume
- smontare il volume
- server virtuale
- server virtuale cifs
- vserver cifs shadowcopy mostra
- spettacolo vserver
- interfaccia di rete
- mostra interfaccia di rete
- spettacolo metrocluster

# Installa il plug-in SnapCenter per Oracle Database

## Flusso di lavoro di installazione del plug-in SnapCenter per Oracle Database

Se si desidera proteggere i database Oracle, è necessario installare e configurare il plug-in SnapCenter per Oracle Database.




## Prerequisiti per l'aggiunta di host e l'installazione del pacchetto plug-in per Linux o AIX

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.

  Il plug-in SnapCenter per Oracle Database può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo del plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utente non root.

- Se si installa il pacchetto di plug-in SnapCenter per AIX su un host AIX, è necessario aver risolto manualmente i collegamenti simbolici a livello di directory.

  Il pacchetto di plug-in SnapCenter per AIX risolve automaticamente il collegamento simbolico a livello di file, ma non i collegamenti simbolici a livello di directory, per ottenere il percorso assoluto JAVA_HOME.

- Creare credenziali con modalità di autenticazione Linux o AIX per l'utente installatore.
- È necessario aver installato Java 11 sul proprio host Linux o AIX.
  - Java di Oracle e OpenJDK è supportato per Linux
  - IBM Java per AIX. Puoi scaricare da "Download di IBM Semeru Runtimes"

    Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.

- Per i database Oracle in esecuzione su un host Linux o AIX, è necessario installare sia SnapCenter Plug-in per Oracle Database sia SnapCenter Plug-in per UNIX.

  È possibile utilizzare il plug-in per Oracle Database anche per gestire i database Oracle per SAP. Tuttavia, l'integrazione con SAP BR*Tools non è supportata.

- Se si utilizza il database Oracle 11.2.0.3 o versione successiva, è necessario installare la patch Oracle

13366202.

La mappatura UUID nel file /etc/fstab non è supportata da SnapCenter.

- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

### Requisiti dell'host Linux

Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario assicurarsi che l'host soddisfi i requisiti.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | • Red Hat Enterprise Linux<br>• Oracle Linux<br>Se si utilizza il database Oracle su LVM nei sistemi operativi Oracle Linux o Red Hat Enterprise Linux 6.6 o 7.0, è necessario installare la versione più recente di Logical Volume Manager (LVM).<br>• SUSE Linux Enterprise Server (SLES) |
| RAM minima per il plug-in SnapCenter sull'host | 2 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | Java 11 Oracle e OpenJDK<br><br>Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.<br><br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. |

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

#### Configurare i privilegi sudo per gli utenti non root per l'host Linux

SnapCenter 2.0 e le versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

### Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*LINUX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

### Requisiti dell'host AIX

Prima di installare il pacchetto di plug-in SnapCenter per AIX, è necessario assicurarsi che l'host soddisfi i requisiti.

Il plug-in SnapCenter per UNIX, che fa parte del pacchetto di plug-in SnapCenter per AIX, non supporta gruppi di volumi simultanei.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | AIX 7.1 o successivo |
| RAM minima per il plug-in SnapCenter sull'host | 4 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 IBM Java<br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. |

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

#### Configurare i privilegi sudo per gli utenti non root per l'host AIX

SnapCenter 4.4 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per AIX e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

#### Cosa ti servirà

- Sudo versione 1.8.7 o successiva.

- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedere all'host AIX su cui si desidera installare il pacchetto plug-in SnapCenter per AIX.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*AIX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

### Imposta le credenziali

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare le credenziali per installare il pacchetto plug-in su host Linux o AIX.

### Informazioni su questo compito

Le credenziali vengono create per l'utente root o per un utente non root che dispone dei privilegi sudo per installare e avviare il processo del plug-in.

Per informazioni, vedere:Configurare i privilegi sudo per gli utenti non root per l'host Linux OConfigurare i privilegi sudo per gli utenti non root per l'host AIX

**Procedura consigliata:** Sebbene sia consentito creare credenziali dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, inserisci le informazioni sulle credenziali:

| Per questo campo… | Fai questo… |
|---|---|
| Nome della credenziale | Inserisci un nome per le credenziali. |
| Nome utente/Password | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio<br>Specificare l'amministratore di dominio sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName* |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare.<br>A seconda del sistema operativo dell'host del plug-in, selezionare Linux o AIX. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina **Utente e accesso**.

### Configurare le credenziali per un database Oracle

È necessario configurare le credenziali utilizzate per eseguire operazioni di protezione dei dati sui database Oracle.

### Informazioni su questo compito

Dovresti esaminare i diversi metodi di autenticazione supportati per il database Oracle. Per informazioni, vedere"Metodi di autenticazione per le tue credenziali" .

Se si impostano credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, il nome utente deve disporre almeno dei privilegi di gruppo di risorse e di backup.

Se hai abilitato l'autenticazione del database Oracle, nella vista delle risorse verrà visualizzata un'icona a forma di lucchetto rosso. È necessario configurare le credenziali del database per poter proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

Se durante la creazione di una credenziale si specificano dati errati, verrà visualizzato un messaggio di errore. È necessario fare clic su **Annulla** e riprovare.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.
3. Clic , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   Puoi quindi fare clic per chiudere il riquadro del filtro.
4. Selezionare il database, quindi fare clic su **Impostazioni database** > **Configura database**.
5. Nella sezione Configura impostazioni database, dall'elenco a discesa **Usa credenziali esistenti**, seleziona le credenziali da utilizzare per eseguire processi di protezione dei dati sul database Oracle.

   L'utente Oracle deve disporre dei privilegi sysdba.

   Puoi anche creare una credenziale cliccando .
6. Nella sezione Configura impostazioni ASM, dall'elenco a discesa **Usa credenziali esistenti**, seleziona le credenziali da utilizzare per eseguire processi di protezione dei dati sull'istanza ASM.

   L'utente ASM deve avere il privilegio sysasm.

   Puoi anche creare una credenziale cliccando .
7. Nella sezione Configura impostazioni catalogo RMAN, dall'elenco a discesa **Usa credenziale esistente**, selezionare la credenziale da utilizzare per eseguire processi di protezione dei dati sul database del catalogo Oracle Recovery Manager (RMAN).

Puoi anche creare una credenziale cliccando + .

Nel campo **TNSName**, immettere il nome del file Transparent Network Substrate (TNS) che verrà utilizzato da SnapCenter Server per comunicare con il database.

8. Nel campo **Nodi RAC preferiti**, specificare i nodi RAC (Real Application Cluster) preferiti per il backup.

   I nodi preferiti potrebbero essere uno o tutti i nodi del cluster in cui sono presenti le istanze del database RAC. L'operazione di backup viene attivata solo su questi nodi preferiti, nell'ordine di preferenza.

   In RAC One Node, solo un nodo è elencato tra i nodi preferiti e questo nodo preferito è il nodo in cui è attualmente ospitato il database.

   Dopo il failover o la rilocazione del database RAC One Node, l'aggiornamento delle risorse nella pagina Risorse SnapCenter rimuoverà l'host dall'elenco **Nodi RAC preferiti** in cui era precedentemente ospitato il database. Il nodo RAC in cui viene trasferito il database verrà elencato in **Nodi RAC** e dovrà essere configurato manualmente come nodo RAC preferito.

   Per ulteriori informazioni, consultare "Nodi preferiti nella configurazione RAC" .

9. Fare clic su **OK**.

## Aggiungi host e installa il pacchetto plug-in per Linux o AIX utilizzando l'interfaccia grafica

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX. I plug-in vengono installati automaticamente sugli host remoti.

### Informazioni su questo compito

È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster. Se si installa il plug-in su un cluster (Oracle RAC), il plug-in viene installato su tutti i nodi del cluster. Per Oracle RAC One Node, è necessario installare il plug-in sia sui nodi attivi che su quelli passivi.

Quando si installa il plug-in su un Oracle RAC, è supportata solo l'autenticazione basata su password. L'autenticazione basata sulla chiave SSH non è supportata.

Dovresti essere assegnato a un ruolo che disponga delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .

Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Selezionare **Linux** o **AIX** come tipo di host.<br><br>SnapCenter Server aggiunge l'host e quindi installa il plug-in per Oracle Database e il plug-in per UNIX se i plug-in non sono già installati sull'host. |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>È possibile immettere gli indirizzi IP o il nome di dominio completo di uno dei seguenti:<br><br>• Host autonomo<br>• Qualsiasi nodo nell'ambiente Oracle Real Application Clusters (RAC)<br><br>Il nodo VIP o l'IP di scansione non sono supportati<br><br>Se si aggiunge un host tramite SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN. |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove.<br><br>La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.
6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta.<br><br>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il percorso predefinito è */opt/ NetApp/snapcenter*.<br><br>Facoltativamente, è possibile personalizzare il percorso. |
| Aggiungere tutti gli host in Oracle RAC | Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un Oracle RAC.<br><br>In una configurazione Flex ASM, verranno aggiunti tutti i nodi, indipendentemente dal fatto che si tratti di un nodo Hub o Leaf. |
| Salta i controlli di preinstallazione facoltativi | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo Salta controlli preliminari, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in.

   Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

   Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati. Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config situato in *C:\Programmi\ NetApp\ SnapCenter WebApp* per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, dovresti risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

SnapCenter non supporta l'algoritmo ECDSA.

La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di registro specifici dell'installazione si trovano in */custom_location/snapcenter/logs*.

**Risultato**

Tutti i database sull'host vengono rilevati automaticamente e visualizzati nella pagina Risorse. Se non viene visualizzato nulla, fare clic su **Aggiorna risorse**.

**Monitorare lo stato dell'installazione**

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Metodi alternativi per installare il pacchetto Plug-in per Linux o AIX

È anche possibile installare manualmente il pacchetto Plug-in per Linux o AIX utilizzando i cmdlet o le CLI.

Prima di installare manualmente il plug-in, è necessario convalidare la firma del pacchetto binario utilizzando la chiave **snapcenter_public_key.pub** e **snapcenter_linux_host_plugin.bin.sig** che si trovano in *C:\ProgramData\ NetApp\ SnapCenter\Package Repository*.

Assicurarsi che **OpenSSL 1.0.2g** sia installato sull'host in cui si desidera installare il plug-in.

Convalidare la firma del pacchetto binario eseguendo il comando:

- Per host Linux: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_linux_host_plugin.bin.sig snapcenter_linux_host_plugin.bin`
- Per host AIX: `openssl dgst -sha256 -verify snapcenter_public_key.pub -signature snapcenter_aix_host_plugin.bsx.sig snapcenter_aix_host_plugin.bsx`

### Installa su più host remoti utilizzando cmdlet

Per installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su più host, è necessario utilizzare il cmdlet PowerShell *Install-SmHostPackage*.

### Cosa ti servirà

È necessario effettuare l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

### Passi

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
3. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX utilizzando il cmdlet *Install-SmHostPackage* e i parametri richiesti.

   È possibile utilizzare l'opzione *-skipprecheck* quando i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

   Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

4. Inserisci le tue credenziali per l'installazione remota.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

### Installa sull'host del cluster

È necessario installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.

Ciascuno dei nodi dell'host del cluster ha due IP. Uno degli IP sarà l'IP pubblico dei rispettivi nodi e il secondo IP sarà l'IP del cluster condiviso tra entrambi i nodi.

**Passi**

1. Installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX su entrambi i nodi dell'host del cluster.
2. Verificare che i valori corretti per i parametri SNAPCENTER_SERVER_HOST, SPL_PORT, SNAPCENTER_SERVER_PORT e SPL_ENABLED_PLUGINS siano specificati nel file spl.properties situato in */var/opt/snapcenter/spl/etc/*.

   Se SPL_ENABLED_PLUGINS non è specificato in spl.properties, è possibile aggiungerlo e assegnare il valore SCO,SCU.

3. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
4. In ciascuno dei nodi, impostare gli IP preferiti del nodo utilizzando il comando *Set-PreferredHostIPsInStorageExportPolicy* sccli e i parametri richiesti.
5. Nell'host del server SnapCenter , aggiungere una voce per l'IP del cluster e il nome DNS corrispondente in *C:\Windows\System32\drivers\etc\hosts*.
6. Aggiungere il nodo al server SnapCenter utilizzando il cmdlet *Add-SmHost* specificando l'IP del cluster per il nome host.

Individuare il database Oracle sul nodo 1 (supponendo che l'IP del cluster sia ospitato sul nodo 1) e creare un backup del database. In caso di failover, è possibile utilizzare il backup creato sul nodo 1 per ripristinare il database sul nodo 2. È anche possibile utilizzare il backup creato sul nodo 1 per creare un clone sul nodo 2.

Se il failover avviene mentre sono in esecuzione altre operazioni SnapCenter , saranno presenti volumi, directory e file di blocco obsoleti.

### Installa il pacchetto Plug-in per Linux in modalità silenziosa

È possibile installare il pacchetto di plug-in SnapCenter per Linux in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

**Cosa ti servirà**

- Dovresti rivedere i prerequisiti per l'installazione del pacchetto plug-in.
- È necessario assicurarsi che la variabile d'ambiente DISPLAY non sia impostata.

  Se la variabile d'ambiente DISPLAY è impostata, dovresti eseguire unset DISPLAY e quindi provare a installare manualmente il plug-in.

**Informazioni su questo compito**

Durante l'installazione in modalità console è necessario fornire le informazioni di installazione necessarie, mentre nell'installazione in modalità silenziosa non è necessario fornire alcuna informazione di installazione.

**Passi**

1. Scaricare il pacchetto di plug-in SnapCenter per Linux dal percorso di installazione di SnapCenter Server.

Il percorso di installazione predefinito è *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.
3. Correre

```
./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. Modificare il file spl.properties situato in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio SnapCenter Plug-in Loader .

> L'installazione del pacchetto plug-in registra i plug-in sull'host e non sul server SnapCenter . È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, seleziona "Nessuno" come credenziale. Dopo aver aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

### Installa il pacchetto Plug-in per AIX in modalità silenziosa

È possibile installare il pacchetto di plug-in SnapCenter per AIX in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

#### Cosa ti servirà

- Dovresti rivedere i prerequisiti per l'installazione del pacchetto plug-in.
- È necessario assicurarsi che la variabile d'ambiente DISPLAY non sia impostata.

  Se la variabile d'ambiente DISPLAY è impostata, dovresti eseguire unset DISPLAY e quindi provare a installare manualmente il plug-in.

#### Passi

1. Scaricare il pacchetto di plug-in SnapCenter per AIX dal percorso di installazione di SnapCenter Server.

   Il percorso di installazione predefinito è *C:\ProgramData\ NetApp\ SnapCenter\PackageRepository*. Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.
3. Correre

```
./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. Modificare il file spl.properties situato in */var/opt/snapcenter/spl/etc/* per aggiungere SPL_ENABLED_PLUGINS=SCO,SCU, quindi riavviare il servizio SnapCenter Plug-in Loader .

L'installazione del pacchetto plug-in registra i plug-in sull'host e non sul server SnapCenter . È necessario registrare i plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Durante l'aggiunta dell'host, seleziona "Nessuno" come credenziale. Dopo aver aggiunto l'host, i plug-in installati vengono rilevati automaticamente.

## Configurare il servizio SnapCenter Plug-in Loader

Il servizio SnapCenter Plug-in Loader carica il pacchetto plug-in per Linux o AIX per interagire con SnapCenter Server. Il servizio SnapCenter Plug-in Loader viene installato quando si installa il pacchetto SnapCenter Plug-ins per Linux o il pacchetto SnapCenter Plug-ins per AIX.

### Informazioni su questo compito

Dopo aver installato il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX, il servizio SnapCenter Plug-in Loader si avvia automaticamente. Se il servizio SnapCenter Plug-in Loader non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui è in esecuzione il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file spl.properties, che si trova in */custom_location/ NetApp/snapcenter/spl/etc/*, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

| Nome del parametro | Descrizione |
|---|---|
| LOG_LEVEL | Visualizza i livelli di registro supportati.<br><br>I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR e FATAL. |
| SPL_PROTOCOL | Visualizza il protocollo supportato da SnapCenter Plug-in Loader.<br><br>È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito. |
| PROTOCOLLO_SERVER_SNAPCENTER | Visualizza il protocollo supportato da SnapCenter Server.<br><br>È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito. |
| SKIP_JAVAHOME_UPDATE | Per impostazione predefinita, il servizio SPL rileva il percorso Java e aggiorna il parametro JAVA_HOME.<br><br>Pertanto il valore predefinito è impostato su FALSE. È possibile impostare su TRUE se si desidera disabilitare il comportamento predefinito e correggere manualmente il percorso Java. |

| Nome del parametro | Descrizione |
| --- | --- |
| SPL_KEYSTORE_PASS | Visualizza la password del file keystore.<br><br>È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore. |
| SPL_PORT | Visualizza il numero di porta su cui è in esecuzione il servizio SnapCenter Plug-in Loader .<br><br>È possibile aggiungere il valore se manca il valore predefinito.<br><br>Non modificare il valore dopo aver installato i plug-in. |
| SNAPCENTER_SERVER_HOST | Visualizza l'indirizzo IP o il nome host del server SnapCenter . |
| SPL_KEYSTORE_PATH | Visualizza il percorso assoluto del file keystore. |
| SNAPCENTER_SERVER_PORT | Visualizza il numero di porta su cui è in esecuzione SnapCenter Server. |
| LOGS_MAX_COUNT | Visualizza il numero di file di registro di SnapCenter Plug-in Loader conservati nella cartella */custom_location/snapcenter/spl/logs*.<br><br>Il valore predefinito è impostato su 5000. Se il conteggio è superiore al valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio SnapCenter Plug-in Loader .<br><br>Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999. |
| JAVA_HOME | Visualizza il percorso assoluto della directory JAVA_HOME utilizzata per avviare il servizio SPL.<br><br>Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL. |

| Nome del parametro | Descrizione |
| --- | --- |
| LOG_MAX_SIZE | Visualizza la dimensione massima del file di registro dei lavori.<br><br>Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file di quel processo. |
| CONSERVA_I_LOG_DEGLI_ULTIMI_GIORNI | Visualizza il numero di giorni per i quali vengono conservati i registri. |
| ABILITA_VALIDAZIONE_CERTIFICATO | Visualizza true quando la convalida del certificato CA è abilitata per l'host.<br><br>È possibile abilitare o disabilitare questo parametro modificando spl.properties oppure utilizzando l'interfaccia utente grafica o il cmdlet SnapCenter . |

Se uno qualsiasi di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, è necessario riavviare il servizio SnapCenter Plug-in Loader .

**Passi**

1. Eseguire una delle seguenti azioni, a seconda delle necessità:
   - Avviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Arrestare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     È possibile utilizzare l'opzione -force con il comando stop per arrestare forzatamente il servizio SnapCenter Plug-in Loader . Tuttavia, è necessario procedere con cautela prima di procedere, poiché ciò interrompe anche le operazioni in corso.

   - Riavviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Trova lo stato del servizio SnapCenter Plug-in Loader :

- Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
- Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`

◦ Trova la modifica nel servizio SnapCenter Plug-in Loader :

- Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
- Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

## Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per l'archivio attendibile SPL e configurare la coppia di chiavi firmata dalla CA per l'archivio attendibile SPL con il servizio SnapCenter Plug-in Loader per attivare il certificato digitale installato.

SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come archivio attendibile che come archivio chiavi.

### Gestisci la password per il keystore SPL e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL.

   È il valore corrispondente alla chiave 'SPL_KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore SPL e per tutte le password alias associate della chiave privata devono essere le stesse.

### Configurare i certificati radice o intermedi per l'archivio attendibile SPL

È necessario configurare i certificati radice o intermedi senza la chiave privata nell'archivio attendibile SPL.

**Passi**

1. Passare alla cartella contenente il keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungi un certificato radice o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi su SPL trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

**Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL**

È necessario configurare la coppia di chiavi firmata dalla CA nell'archivio attendibile SPL.

**Passi**

1. Passare alla cartella contenente il keystore dell'SPL /var/opt/snapcenter/spl/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave sia privata che pubblica.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elenca i certificati aggiunti nel keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verificare che il keystore contenga l'alias corrispondente al nuovo
certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il
certificato CA con la password del keystore.
```

La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS nel file

spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore situato nel file
spl.properties.
```

Aggiornare questo valore in base alla chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL.

#### Configurare l'elenco di revoche dei certificati (CRL) per SPL

Dovresti configurare il CRL per SPL

#### Informazioni su questo compito

- SPL cercherà i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per SPL è */var/opt/snapcenter/spl/etc/crl*.

#### Passi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

## Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

#### Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

## Importa dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter

### Importando i dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter è possibile continuare a utilizzare i dati delle versioni precedenti.

È possibile importare dati da SnapManager per Oracle e SnapManager per SAP in SnapCenter eseguendo lo strumento di importazione dall'interfaccia della riga di comando (CLI host Linux).

Lo strumento di importazione crea policy e gruppi di risorse in SnapCenter. Le policy e i gruppi di risorse creati in SnapCenter corrispondono ai profili e alle operazioni eseguite utilizzando tali profili in SnapManager per Oracle e SnapManager per SAP. Lo strumento di importazione SnapCenter interagisce con i database del repository SnapManager per Oracle e SnapManager per SAP e con il database che si desidera importare.

- Recupera tutti i profili, le pianificazioni e le operazioni eseguite utilizzando i profili.
- Crea una policy di backup SnapCenter per ogni operazione univoca e ogni pianificazione associata a un profilo.
- Crea un gruppo di risorse per ciascun database di destinazione.

È possibile eseguire lo strumento di importazione eseguendo lo script sc-migrate che si trova in */opt/ NetApp/snapcenter/spl/bin*. Quando si installa il pacchetto di plug-in SnapCenter per Linux sull'host del database che si desidera importare, lo script sc-migrate viene copiato in */opt/ NetApp/snapcenter/spl/bin*.

L'importazione dei dati non è supportata dall'interfaccia utente grafica (GUI) SnapCenter .

SnapCenter non supporta Data ONTAP funzionante in modalità 7. È possibile utilizzare lo strumento di transizione a 7 modalità per migrare dati e configurazioni archiviati su un sistema che esegue Data ONTAP in modalità 7 modalità verso un sistema ONTAP .

### Configurazioni supportate per l'importazione dei dati

Prima di importare dati da SnapManager 3.4.x per Oracle e SnapManager 3.4.x per SAP in SnapCenter, è necessario conoscere le configurazioni supportate dal plug-in SnapCenter per Oracle Database.

Le configurazioni supportate con il plug-in SnapCenter per Oracle Database sono elencate in "Strumento matrice di interoperabilità NetApp" .

### Cosa viene importato in SnapCenter

È possibile importare profili, pianificazioni e operazioni eseguite utilizzando i profili.

| Da SnapManager per Oracle e SnapManager per SAP | Per SnapCenter |
|---|---|
| Profili senza alcuna operazione e programmazione | Viene creato un criterio con tipo di backup predefinito come Online e ambito di backup come Completo. |
| Profili con una o più operazioni | Vengono create più policy in base a una combinazione univoca di un profilo e di operazioni eseguite utilizzando tale profilo.<br><br>I criteri creati in SnapCenter contengono i dettagli di conservazione e potatura del registro di archivio recuperati dal profilo e dalle operazioni corrispondenti. |
| Profili con configurazione Oracle Recovery Manager (RMAN) | Le policy vengono create con l'opzione **Backup del catalogo con Oracle Recovery Manager** abilitata.<br><br>Se in SnapManager è stata utilizzata la catalogazione RMAN esterna, è necessario configurare le impostazioni del catalogo RMAN in SnapCenter. È possibile selezionare le credenziali esistenti oppure crearne di nuove.<br><br>Se RMAN è stato configurato tramite il file di controllo in SnapManager, non è necessario configurare RMAN in SnapCenter. |
| Programma allegato a un profilo | Viene creata una policy specifica per la pianificazione. |
| Banca dati | Per ogni database importato viene creato un gruppo di risorse.<br><br>In una configurazione RAC (Real Application Clusters), il nodo su cui si esegue lo strumento di importazione diventa il nodo preferito dopo l'importazione e per tale nodo viene creato il gruppo di risorse. |

Quando si importa un profilo, viene creata una policy di verifica insieme alla policy di backup.

Quando i profili, le pianificazioni e tutte le operazioni eseguite tramite i profili SnapManager per Oracle e SnapManager per SAP vengono importati in SnapCenter, vengono importati anche i diversi valori dei parametri.

| Parametri e valori SnapManager per Oracle e SnapManager per SAP | Parametro e valori SnapCenter | Note |
|---|---|---|
| Ambito di backup<br>• Pieno<br>• Dati<br>• Tronco d'albero | Ambito di backup<br>• Pieno<br>• Dati<br>• Tronco d'albero | |
| Modalità di backup<br>• Auto<br>• In linea<br>• Fuori linea | Tipo di backup<br>• In linea<br>• Arresto offline | Se la modalità di backup è Auto, lo strumento di importazione controlla lo stato del database al momento dell'esecuzione dell'operazione e imposta opportunamente il tipo di backup su Arresto online o Arresto offline. |
| Conservazione<br>• Giorni<br>• Conti | Conservazione<br>• Giorni<br>• Conti | SnapManager per Oracle e SnapManager per SAP utilizzano sia Giorni che Conteggi per impostare la conservazione.<br>In SnapCenter, ci sono Giorni *O* Conteggi. Pertanto, la conservazione è impostata in base ai giorni, poiché in SnapManager per Oracle e SnapManager per SAP i giorni hanno la precedenza sui conteggi. |
| Potatura per programmi<br>• Tutto<br>• numero di modifica del sistema (SCN)<br>• Data<br>• Registri creati prima di ore, giorni, settimane e mesi specificati | Potatura per programmi<br>• Tutto<br>• Registri creati prima delle ore e dei giorni specificati | SnapCenter non supporta la potatura basata su SCN, data, settimane e mesi. |

| Parametri e valori SnapManager per Oracle e SnapManager per SAP | Parametro e valori SnapCenter | Note |
|---|---|---|
| Notifica<br>• Email inviate solo per operazioni riuscite<br>• Email inviate solo per operazioni non riuscite<br>• Email inviate sia per operazioni riuscite che non riuscite | Notifica<br>• Sempre<br>• In caso di fallimento<br>• Avvertimento<br>• Errore | Le notifiche e-mail vengono importate.<br>Tuttavia, è necessario aggiornare manualmente il server SMTP tramite l'interfaccia grafica utente SnapCenter . L'oggetto dell'e-mail viene lasciato vuoto per consentirti di configurarlo. |

### Cosa non viene importato in SnapCenter

Lo strumento di importazione non importa tutto in SnapCenter.

Non è possibile importare quanto segue in SnapCenter:

- Metadati di backup
- Backup parziali
- Backup relativi a Raw Device Mapping (RDM) e Virtual Storage Console (VSC)
- Ruoli o credenziali disponibili nel repository SnapManager per Oracle e SnapManager per SAP
- Dati relativi alle operazioni di verifica, ripristino e clonazione
- Potatura per operazioni
- Dettagli di replicazione specificati nel profilo SnapManager per Oracle e SnapManager per SAP

  Dopo l'importazione, è necessario modificare manualmente il criterio corrispondente creato in SnapCenter per includere i dettagli di replica.

- Informazioni di backup catalogate

### Prepararsi all'importazione dei dati

Prima di importare i dati in SnapCenter, è necessario eseguire determinate attività per eseguire correttamente l'operazione di importazione.

### Passi

1. Identifica il database che vuoi importare.
2. Utilizzando SnapCenter, aggiungere l'host del database e installare il pacchetto plug-in SnapCenter per Linux.
3. Utilizzando SnapCenter, impostare le connessioni per le macchine virtuali di archiviazione (SVM) utilizzate dai database sull'host.
4. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
5. Nella pagina Risorse, assicurati che il database da importare sia stato individuato e visualizzato.

Quando si desidera eseguire lo strumento di importazione, il database deve essere accessibile, altrimenti la creazione del gruppo di risorse non riesce.

Se il database ha credenziali configurate, è necessario creare una credenziale corrispondente in SnapCenter, assegnare la credenziale al database e quindi eseguire nuovamente l'individuazione del database. Se il database risiede su Automatic Storage Management (ASM), è necessario creare le credenziali per l'istanza ASM e assegnarle al database.

6. Assicurarsi che l'utente che esegue lo strumento di importazione disponga di privilegi sufficienti per eseguire i comandi SnapManager per Oracle o SnapManager per SAP CLI (ad esempio il comando per sospendere le pianificazioni) dall'host SnapManager per Oracle o SnapManager per SAP.
7. Eseguire i seguenti comandi sull'host SnapManager per Oracle o SnapManager per SAP per sospendere le pianificazioni:
   a. Se si desidera sospendere le pianificazioni sull'host SnapManager per Oracle, eseguire:
      - `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`

        È necessario eseguire il comando smo credential set per ciascun profilo sull'host.

   b. Se si desidera sospendere le pianificazioni sull'host SnapManager per SAP, eseguire:
      - `smsap credential set -repository -dbname repository_database_name -host host_name -port port_number -login -username user_name_for_repository_database`
      - `smsap profile sync -repository -dbname repository_database_name -host host_name -port port_number -login -username host_user_name_for_repository_database`
      - `smsap credential set -profile -name profile_name`

        È necessario eseguire il comando smsap credential set per ciascun profilo sull'host.

8. Assicurarsi che il nome di dominio completo (FQDN) dell'host del database venga visualizzato quando si esegue hostname -f.

   Se il nome di dominio completo (FQDN) non viene visualizzato, è necessario modificare /etc/hosts per specificare il nome di dominio completo (FQDN) dell'host.

### Importa dati

È possibile importare i dati eseguendo lo strumento di importazione dall'host del database.

### Informazioni su questo compito

I criteri di backup SnapCenter creati dopo l'importazione hanno formati di denominazione diversi:

- I criteri creati per i profili senza alcuna operazione e pianificazione hanno il formato SM_PROFILENAME_ONLINE_FULL_DEFAULT_MIGRATED.

  Quando non viene eseguita alcuna operazione utilizzando un profilo, viene creato il criterio corrispondente con il tipo di backup predefinito online e l'ambito del backup completo.

- I criteri creati per i profili con una o più operazioni hanno il formato SM_PROFILENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.
- I criteri creati per le pianificazioni associate ai profili hanno il formato SM_PROFILENAME_SMOSCHEDULENAME_BACKUPMODE_BACKUPSCOPE_MIGRATED.

**Passi**

1. Accedi all'host del database che desideri importare.
2. Eseguire lo strumento di importazione eseguendo lo script sc-migrate che si trova in */opt/NetApp/snapcenter/spl/bin*.
3. Immettere il nome utente e la password di SnapCenter Server.

   Dopo aver convalidato le credenziali, viene stabilita una connessione con SnapCenter.

4. Immettere i dettagli del database del repository SnapManager per Oracle o SnapManager per SAP.

   Il database del repository elenca i database disponibili sull'host.

5. Inserisci i dettagli del database di destinazione.

   Se si desidera importare tutti i database sull'host, immettere all.

6. Se si desidera generare un registro di sistema o inviare messaggi ASUP per operazioni non riuscite, è necessario abilitarli eseguendo il comando *Add-SmStorageConnection* o *Set-SmStorageConnection*.

> Se si desidera annullare un'operazione di importazione, durante l'esecuzione dello strumento di importazione o dopo l'importazione, è necessario eliminare manualmente i criteri, le credenziali e i gruppi di risorse SnapCenter creati come parte dell'operazione di importazione.

**Risultati**

I criteri di backup SnapCenter vengono creati per profili, pianificazioni e operazioni eseguite utilizzando i profili. Vengono creati anche gruppi di risorse per ogni database di destinazione.

Dopo aver importato correttamente i dati, le pianificazioni associate al database importato vengono sospese in SnapManager per Oracle e SnapManager per SAP.

> Dopo l'importazione, è necessario gestire il database o il file system importato utilizzando SnapCenter.

I log di ogni esecuzione dello strumento di importazione vengono archiviati nella directory */var/opt/snapcenter/spl/logs* con il nome spl_migration_timestamp.log. È possibile fare riferimento a questo registro per esaminare gli errori di importazione e risolverli.

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

## Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

## Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

# Prepararsi alla protezione dei database Oracle

Prima di eseguire qualsiasi operazione di protezione dei dati, come backup, clonazione o ripristino, è necessario definire la strategia e configurare l'ambiente. È anche possibile configurare SnapCenter Server per utilizzare le tecnologie SnapMirror e SnapVault .

Per sfruttare i vantaggi della tecnologia SnapVault e SnapMirror , è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di archiviazione. Per eseguire queste attività è possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di archiviazione.

Prima di utilizzare il plug-in per Oracle Database, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server."Saperne di più"
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione."Saperne di più"

> SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM registrato con SnapCenter tramite la registrazione SVM o la registrazione cluster deve essere univoco.

- Creare credenziali con modalità di autenticazione Linux o AIX per l'utente installatore."Saperne di più"
- Aggiungi host, installa i plug-in e scopri le risorse.
- Se si utilizza SnapCenter Server per proteggere i database Oracle che risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.
- Installa Java sul tuo host Linux o AIX.

  Vedere"Requisiti host Linux" O"Requisiti dell'host AIX" per maggiori informazioni.

- Dovresti impostare il valore di timeout del firewall dell'applicazione su 3 ore o più.
- Se si dispone di database Oracle in ambienti NFS, è necessario aver configurato almeno un LIF di dati NFS per l'archiviazione primaria o secondaria per eseguire operazioni di montaggio, clonazione, verifica e ripristino.
- Se si dispone di più percorsi dati (LIF) o di una configurazione dNFS, è possibile eseguire le seguenti operazioni utilizzando la CLI SnapCenter sull'host del database:
  - Per impostazione predefinita, tutti gli indirizzi IP dell'host del database vengono aggiunti alla policy di esportazione dell'archiviazione NFS nella macchina virtuale di archiviazione (SVM) per i volumi clonati. Se si desidera avere un indirizzo IP specifico o limitarsi a un sottoinsieme di indirizzi IP, eseguire la CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se in SVM sono presenti più percorsi dati (LIF), SnapCenter sceglie il percorso dati (LIF) appropriato per il montaggio del volume clonato NFS. Tuttavia, se si desidera specificare un percorso dati specifico (LIF), è necessario eseguire la CLI Set-SvmPreferredDataPath. Per maggiori informazioni, consultare la guida di riferimento ai comandi.
- Se si dispone di database Oracle in ambienti SAN, assicurarsi che l'ambiente SAN sia configurato secondo le raccomandazioni menzionate nelle seguenti guide:
  - "Utilizzo di host Linux con storage ONTAP"
  - "Impostazioni host interessate dalle utilità host AIX"
- Se si dispone di database Oracle su LVM nei sistemi operativi Oracle Linux o RHEL, installare la versione più recente di Logical Volume Management (LVM).
- Se si utilizza SnapManager per Oracle e si desidera migrare al plug-in SnapCenter per Oracle Database, è possibile migrare i profili alle policy e ai gruppi di risorse di SnapCenter utilizzando il comando sccli sc-migrate.
- Configura SnapMirror e SnapVault su ONTAP, se desideri la replica del backup

Per gli utenti SnapCenter 4.1.1, la documentazione SnapCenter Plug-in for VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione di database e file system virtualizzati mediante il SnapCenter Plug-in for VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato Open Virtual Appliance). Per gli utenti SnapCenter 4.3.x, la documentazione SnapCenter Plug-in for VMware vSphere 4.3 contiene informazioni sulla protezione di database e file system virtualizzati mediante l'appliance virtuale SnapCenter Plug-in for VMware vSphere basata su Linux (formato Open Virtual Appliance).

**Trova maggiori informazioni**

- "Strumento di matrice di interoperabilità"
- "Documentazione SnapCenter Plug-in for VMware vSphere"
- "L'operazione di protezione dei dati fallisce in un ambiente non multipath in RHEL 7 e versioni successive"

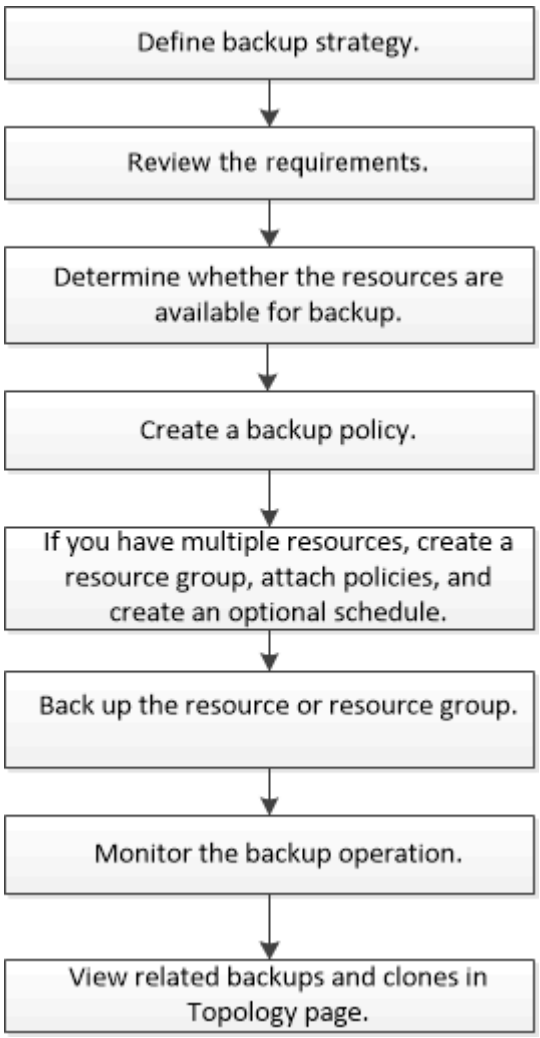
# Eseguire il backup dei database Oracle

## Panoramica della procedura di backup

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. La procedura di backup include la pianificazione, l'identificazione delle risorse per il backup, la creazione di policy di backup, la creazione di gruppi di risorse e l'associazione di policy,

la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




Durante la creazione di un backup per i database Oracle, viene creato un file di blocco operativo (*.sm_lock_dbsid*) sull'host del database Oracle nella directory */var/opt/snapcenter/sco/lock* per evitare che vengano eseguite più operazioni sul database. Dopo aver eseguito il backup del database, il file di blocco operativo viene rimosso automaticamente.

Tuttavia, se il backup precedente è stato completato con un avviso, il file di blocco operativo potrebbe non essere eliminato e la successiva operazione di backup potrebbe essere inserita nella coda di attesa. Potrebbe eventualmente essere annullato se il file **.sm_lock_dbsid** non viene eliminato. In tale scenario, è necessario eliminare manualmente il file di blocco operativo eseguendo i seguenti passaggi:

1. Dal prompt dei comandi, vai a */var/opt/snapcenter/sco/lock*.
2. Eliminare il blocco operativo:`rm -rf .sm_lock_dbsid.`

## Informazioni sulla configurazione del backup

#### Configurazioni del database Oracle supportate per i backup

SnapCenter supporta il backup di diverse configurazioni di database Oracle.

- Oracle autonomo
- Cluster di applicazioni reali Oracle (RAC)
- Oracle Standalone Legacy
- Database contenitore autonomo Oracle (CDB)
- Oracle Data Guard in standby

  È possibile creare solo backup offline dei database standby di Data Guard. Il backup con arresto offline, il backup del solo registro di archivio e il backup completo non sono supportati.

- Oracle Active Data Guard standby

  È possibile creare backup online solo dei database standby di Active Data Guard. Non sono supportati il backup del solo registro di archivio e il backup completo.

  Prima di creare un backup del database Data Guard standby o Active Data Guard standby, il processo di ripristino gestito (MRP) viene arrestato e, una volta creato il backup, MRP viene avviato.

- Gestione automatica dell'archiviazione (ASM)
  - ASM standalone e ASM RAC su disco macchina virtuale (VMDK)

    Tra tutti i metodi di ripristino supportati per i database Oracle, è possibile eseguire solo il ripristino di tipo connect-and-copy dei database ASM RAC su VMDK.

  - ASM standalone e ASM RAC su Raw Device Mapping (RDM) + È possibile eseguire operazioni di backup, ripristino e clonazione su database Oracle su ASM, con o senza ASMLib.
  - Driver filtro Oracle ASM (ASMFD)

    Le operazioni di migrazione e clonazione PDB non sono supportate.

  - Oracle Flex ASM

Per le informazioni più recenti sulle versioni Oracle supportate, vedere "Strumento matrice di interoperabilità NetApp" .

**Tipi di backup supportati per i database Oracle**

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta tipi di backup online e offline per i database Oracle.

**Backup online**

Un backup creato quando il database è online è detto backup online. Chiamato anche backup a caldo, il backup online consente di creare un backup del database senza doverlo arrestare.

Come parte del backup online, puoi creare un backup dei seguenti file:

- Solo file di dati e file di controllo
- Archivia solo i file di registro (in questo scenario il database non viene portato in modalità di backup)
- Database completo che include file di dati, file di controllo e file di registro di archivio

#### Backup offline

Un backup creato quando il database è in stato di montaggio o di spegnimento è chiamato backup offline. Un backup offline è anche chiamato backup a freddo. Nei backup offline è possibile includere solo file di dati e file di controllo. È possibile creare un backup di montaggio offline o di arresto offline.

- Quando si crea un backup di montaggio offline, è necessario assicurarsi che il database sia in uno stato montato.

  Se il database si trova in uno stato diverso, l'operazione di backup fallisce.

- Quando si crea un backup di arresto offline, il database può trovarsi in qualsiasi stato.

  Lo stato del database viene modificato nello stato richiesto per creare un backup. Dopo aver creato il backup, lo stato del database viene ripristinato allo stato originale.

### Come SnapCenter scopre i database Oracle

Le risorse sono database Oracle sull'host gestiti da SnapCenter. È possibile aggiungere questi database ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database disponibili.

Nelle sezioni seguenti viene descritto il processo utilizzato da SnapCenter per individuare diversi tipi e versioni di database Oracle.

#### Per le versioni di Oracle da 11*g* a 12*c*R1

**Banca dati RAC**

I database RAC vengono scoperti solo sulla base delle voci /etc/oratab`. Le voci del database dovrebbero essere nel file /etc/oratab.

**Autonomo**

I database autonomi vengono scoperti solo sulla base delle voci /etc/oratab.

**ASM**

La voce dell'istanza ASM dovrebbe essere disponibile nel file /etc/oratab.

**RAC One Node**

I database RAC One Node vengono rilevati solo sulla base delle voci /etc/oratab. I database devono essere nello stato nomount, mount o open. Le voci del database dovrebbero essere nel file /etc/oratab.

Lo stato del database RAC One Node verrà contrassegnato come rinominato o eliminato se il database è già stato rilevato e sono associati backup al database.

Se il database viene spostato, è necessario eseguire i seguenti passaggi:

1. Aggiungere manualmente la voce del database riposizionato nel file /etc/oratab sul nodo RAC sottoposto a failover.
2. Aggiorna manualmente le risorse.
3. Selezionare il database RAC One Node dalla pagina delle risorse, quindi fare clic su Impostazioni database.
4. Configurare il database per impostare i nodi del cluster preferiti sul nodo RAC che attualmente ospita il

database.

5. Eseguire le operazioni SnapCenter .
6. Se hai spostato un database da un nodo a un altro e la voce oratab nel nodo precedente non è stata eliminata, elimina manualmente la voce oratab per evitare che lo stesso database venga visualizzato due volte.

#### Per le versioni di Oracle da 12cR2 a 18c, 19c o 21c

**Banca dati RAC**

I database RAC vengono rilevati tramite il comando srvctl config. Le voci del database dovrebbero essere nel file /etc/oratab.

**Autonomo**

I database autonomi vengono rilevati in base alle voci nel file /etc/oratab e all'output del comando srvctl config.

**ASM**

La voce dell'istanza ASM non deve necessariamente trovarsi nel file /etc/oratab.

**RAC One Node**

I database RAC One Node vengono rilevati solo tramite il comando srvctl config. I database devono essere nello stato nomount, mount o open. Lo stato del database RAC One Node verrà contrassegnato come rinominato o eliminato se il database è già stato rilevato e sono associati backup al database.

Se il database viene spostato, è necessario eseguire i seguenti passaggi: . Aggiorna manualmente le risorse. . Selezionare il database RAC One Node dalla pagina delle risorse, quindi fare clic su Impostazioni database. . Configurare il database per impostare i nodi del cluster preferiti sul nodo RAC che attualmente ospita il database. . Eseguire le operazioni SnapCenter .

> Se nel file /etc/oratab sono presenti voci di database Oracle 12*c*R2 e 18*c* e lo stesso database è registrato con il comando srvctl config, SnapCenter eliminerà le voci di database duplicate. Se sono presenti voci obsolete nel database, il database verrà rilevato ma non sarà raggiungibile e lo stato sarà offline.

**Nodi preferiti nella configurazione RAC**

Nella configurazione di Oracle Real Application Clusters (RAC), è possibile specificare i nodi preferiti che SnapCenter utilizza per eseguire l'operazione di backup. Se non si specifica il nodo preferito, SnapCenter assegna automaticamente un nodo come preferito e su tale nodo viene creato un backup.

I nodi preferiti potrebbero essere uno o tutti i nodi del cluster in cui sono presenti le istanze del database RAC. L'operazione di backup viene attivata solo su questi nodi preferiti, nell'ordine di preferenza.

**Esempio**

Il database RAC cdbrac ha tre istanze: cdbrac1 sul nodo 1, cdbrac2 sul nodo 2 e cdbrac3 sul nodo 3.

Le istanze node1 e node2 sono configurate per essere i nodi preferiti, con node2 come prima preferenza e node1 come seconda preferenza. Quando si esegue un'operazione di backup, l'operazione viene tentata prima sul nodo 2 perché è il primo nodo preferito.

Se node2 non è nello stato di backup, il che potrebbe essere dovuto a molteplici motivi, ad esempio l'agente

plug-in non è in esecuzione sull'host, l'istanza del database sull'host non è nello stato richiesto per il tipo di backup specificato o l'istanza del database su node2 in una configurazione FlexASM non è servita dall'istanza ASM locale; l'operazione verrà tentata su node1.

Il nodo3 non verrà utilizzato per il backup perché non è presente nell'elenco dei nodi preferiti.

#### Configurazione Flex ASM

In una configurazione Flex ASM, i nodi Leaf non verranno elencati come nodi preferiti se la cardinalità è inferiore al numero di nodi nel cluster RAC. Se si verificano modifiche nei ruoli dei nodi del cluster Flex ASM, è necessario rilevarle manualmente in modo che i nodi preferiti vengano aggiornati.

#### Stato del database richiesto

Affinché il backup venga completato correttamente, le istanze del database RAC sui nodi preferiti devono essere nello stato richiesto:

- Per creare un backup online, una delle istanze del database RAC nei nodi preferiti configurati deve essere nello stato aperto.
- Una delle istanze del database RAC nei nodi preferiti configurati deve essere nello stato di montaggio e tutte le altre istanze, inclusi gli altri nodi preferiti, devono essere nello stato di montaggio o in uno stato inferiore per creare un backup di montaggio offline.
- Le istanze del database RAC possono trovarsi in qualsiasi stato, ma è necessario specificare i nodi preferiti per creare un backup di arresto offline.

### Come catalogare i backup con Oracle Recovery Manager

## È possibile catalogare i backup dei database Oracle utilizzando Oracle Recovery Manager (RMAN) per archiviare le informazioni di backup nel repository Oracle RMAN.

I backup catalogati possono essere utilizzati in seguito per operazioni di ripristino a livello di blocco o di ripristino point-in-time dello spazio tabella. Quando non hai bisogno di questi backup catalogati, puoi rimuovere le informazioni del catalogo.

Per la catalogazione, il database deve essere montato o in uno stato superiore. È possibile eseguire la catalogazione su backup di dati, backup di log di archivio e backup completi. Se la catalogazione è abilitata per un backup di un gruppo di risorse che dispone di più database, la catalogazione viene eseguita per ciascun database. Per i database Oracle RAC, la catalogazione verrà eseguita sul nodo preferito in cui il database è almeno nello stato montato.

Se si desidera catalogare i backup di un database RAC, assicurarsi che non sia in esecuzione nessun altro processo per quel database. Se è in esecuzione un altro processo, l'operazione di catalogazione fallisce anziché essere messa in coda.

#### Database di catalogo esterno

Per impostazione predefinita, per la catalogazione viene utilizzato il file di controllo del database di destinazione. Se si desidera aggiungere un database di catalogo esterno, è possibile configurarlo specificando le credenziali e il nome del substrato di rete trasparente (TNS) del catalogo esterno tramite la procedura guidata Impostazioni database dall'interfaccia utente grafica (GUI) di SnapCenter . È anche possibile configurare il database del catalogo esterno dalla CLI eseguendo il comando Configure-SmOracleDatabase con le opzioni -OracleRmanCatalogCredentialName e -OracleRmanCatalogTnsName.

#### comando RMAN

Se è stata abilitata l'opzione di catalogazione durante la creazione di un criterio di backup Oracle dalla GUI SnapCenter , i backup vengono catalogati utilizzando Oracle RMAN come parte dell'operazione di backup. È anche possibile eseguire la catalogazione differita dei backup eseguendo il comando `Catalog-SmBackupWithOracleRMAN` comando.

Dopo aver catalogato i backup, è possibile eseguire il `Get-SmBackupDetails` comando per ottenere le informazioni di backup catalogate, come il tag per i file di dati catalogati, il percorso del catalogo dei file di controllo e le posizioni dei registri di archivio catalogati.

#### Formato di denominazione

Se il nome del gruppo di dischi ASM è maggiore o uguale a 16 caratteri, da SnapCenter 3.0, il formato di denominazione utilizzato per il backup è SC_HASHCODEofDISKGROUP_DBSID_BACKUPID. Tuttavia, se il nome del gruppo di dischi è inferiore a 16 caratteri, il formato di denominazione utilizzato per il backup è DISKGROUPNAME_DBSID_BACKUPID, che è lo stesso formato utilizzato in SnapCenter 2.0.

HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM.

#### Operazioni di controllo incrociato

È possibile eseguire controlli incrociati per aggiornare le informazioni obsolete del repository RMAN sui backup i cui record del repository non corrispondono al loro stato fisico. Ad esempio, se un utente rimuove i registri archiviati dal disco con un comando del sistema operativo, il file di controllo indica comunque che i registri sono sul disco, quando in realtà non è così.

L'operazione di controllo incrociato consente di aggiornare il file di controllo con le informazioni. È possibile abilitare il controllo incrociato eseguendo il comando Set-SmConfigSettings e assegnando il valore TRUE al parametro ENABLE_CROSSCHECK. Il valore predefinito è impostato su FALSE.

```
sccli Set-SmConfigSettings-ConfigSettingsTypePlugin-PluginCodeSCO-ConfigSettings
"KEY=ENABLE_CROSSCHECK, VALUE=TRUE"
```

#### Rimuovere le informazioni del catalogo

È possibile rimuovere le informazioni del catalogo eseguendo il comando Uncatalog-SmBackupWithOracleRMAN. Non è possibile rimuovere le informazioni del catalogo utilizzando l'interfaccia utente grafica SnapCenter . Tuttavia, le informazioni di un backup catalogato vengono rimosse durante l'eliminazione del backup o durante l'eliminazione del gruppo di conservazione e di risorse associato a tale backup catalogato.

> Quando si forza l'eliminazione dell'host SnapCenter , le informazioni dei backup catalogati associati a tale host non vengono rimosse. È necessario rimuovere le informazioni di tutti i backup catalogati per quell'host prima di forzare l'eliminazione dell'host.

Se la catalogazione e la decatalogazione non riescono perché il tempo dell'operazione ha superato il valore di timeout specificato per il parametro ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT, è necessario modificare il valore del parametro eseguendo il seguente comando:

```
/opt/Netapp/snapcenter/spl/bin/sccli Set-SmConfigSettings-ConfigSettingsType
Plugin -PluginCode SCO-ConfigSettings
"KEY=ORACLE_PLUGIN_RMAN_CATALOG_TIMEOUT,VALUE=user_defined_value"
```

Dopo aver modificato il valore del parametro, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il seguente comando:

```
/opt/NetApp/snapcenter/spl/bin/spl restart
```

Le informazioni sui parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help nome_comando. In alternativa, è possibile fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

### Variabili di ambiente predefinite per il backup di prescript e postscript specifici

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript durante la creazione di policy di backup. Questa funzionalità è supportata per tutte le configurazioni Oracle, ad eccezione di VMDK.

SnapCenter predefinisce i valori dei parametri che saranno direttamente accessibili nell'ambiente in cui vengono eseguiti gli script della shell. Non è necessario specificare manualmente i valori di questi parametri durante l'esecuzione degli script.

#### Variabili di ambiente predefinite supportate per la creazione di criteri di backup

- **SC_JOB_ID** specifica l'ID del processo dell'operazione.

  Esempio: 256

- **SC_ORACLE_SID** specifica l'identificativo di sistema del database.

  Se l'operazione coinvolge più database, il parametro conterrà i nomi dei database separati da una barra verticale.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: NFSB32|NFSB31

- **SC_HOST** specifica il nome host del database.

  Per RAC, il nome host sarà il nome dell'host su cui viene eseguito il backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** specifica il proprietario del sistema operativo del database.

  I dati saranno formattati come <db1>@<osuser1>|<db2>@<osuser2>.

  Esempio: NFSB31@oracle|NFSB32@oracle

- **SC_OS_GROUP** specifica il gruppo del sistema operativo del database.

  I dati saranno formattati come <db1>@<osgroup1>|<db2>@<osgroup2>.

  Esempio: NFSB31@install|NFSB32@oinstall

- **SC_BACKUP_TYPE**" specifica il tipo di backup (online completo, dati online, registro online, arresto

offline, montaggio offline)

Esempi:

- Per il backup completo: ONLINEFULL
- backup solo dati: ONLINEDATA
- Per il backup solo del registro: ONLINELOG

- **SC_BACKUP_NAME** specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: 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** specifica l'ID del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: DATI@203|LOG@205|AV@207

- **SC_ORACLE_HOME** specifica il percorso della directory home di Oracle.

  Esempio: NFSB32@/ora01/app/oracle/product/18.1.0/db_1|NFSB31@/ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_RETENTION** specifica il periodo di conservazione definito nella policy.

  Esempi:

  - Per backup completo: Orario|DATA@DAYS:3|LOG@COUNT:4
  - Solo per il backup dei dati su richiesta: Ondemand|DATA@COUNT:2
  - Solo per il backup del registro su richiesta: Ondemand|LOG@COUNT:2

- **SC_RESOURCE_GROUP_NAME** specifica il nome del gruppo di risorse.

  Esempio: RG1

- **SC_BACKUP_POLICY_NAME** specifica il nome del criterio di backup.

  Esempio: backup_policy

- **SC_AV_NAME** specifica i nomi dei volumi dell'applicazione.

  Esempio: AV1|AV2

- **SC_PRIMARY_DATA_VOLUME_FULL_PATH** specifica la mappatura dell'archiviazione di SVM sul volume per la directory dei file di dati. Sarà il nome del volume padre per LUN e Qtree.

  I dati saranno formattati come <db1>@<SVM1:volume1>|<db2>@<SVM2:volume2>.

  Esempi:

  - Per 2 database nello stesso gruppo di risorse:

NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_DATA|NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA

  - Per un singolo database con file di dati distribuiti su più volumi: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_DATA,herculus:/vol/scspr2417819002_NFS
- **SC_PRIMARY_ARCHIVELOGS_VOLUME_FULL_PATH** specifica la mappatura dell'archiviazione di SVM sul volume per la directory dei file di registro. Sarà il nome del volume padre per LUN e Qtree.

  Esempi:

  - Per una singola istanza del database: buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO
  - Per più istanze di database: NFSB31@buck:/vol/scspr2417819002_NFS_CDB_NFSB31_REDO|NFSB32@buck:/vol/scspr2417819002_NFS_CDB_NFSB32_REDO
- **SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG** specifica l'elenco di snapshot contenenti il nome del sistema di archiviazione e il nome del volume.

  Esempi:

  - Per una singola istanza di database: 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
  - Per più istanze di database: 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
- **SC_PRIMARY_SNAPSHOT_NAMES** specifica i nomi degli snapshot primari creati durante il backup.

  Esempi:

  - Per istanza di database singola: RG2_scspr2417819002_07-21-2021_02.28.26.3973_0,RG2_scspr2417819002_07-21-2021_02.28.26.3973_1
  - Per più istanze di database: 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_02.28.26.3973_1
  - Per gli snapshot di gruppo di coerenza che coinvolgono 2 volumi: cg3_R80404CBEF5V1_04-05-2021_03.08.03.4945_0_bfc279cc-28ad-465c-9d60-5487ac17b25d_2021_4_5_3_8_58_350
- **SC_PRIMARY_MOUNT_POINTS** specifica i dettagli del punto di montaggio che fanno parte del backup.

  I dettagli includono la directory su cui sono montati i volumi e non il padre immediato del file sottoposto a backup. Per una configurazione ASM, è il nome del gruppo di dischi.

  I dati saranno formattati come <db1>@<mountpoint1,mountpoint2>|<db2>@<mountpoint1,mountpoint2>.

  Esempi:

  - Per una singola istanza di database: /mnt/nfsdb3_data,/mnt/nfsdb3_log,/mnt/nfsdb3_data1

- Per più istanze di database: NFSB31@/mnt/nfsdb31_data,/mnt/nfsdb31_log,/mnt/nfsdb31_data1|NFSB32@/mnt/nfsdb32_data,/mnt/nfsdb32_log,/mnt/nfsdb32_data1
- Per ASM: +DATA2DG,+LOG2DG

- **SC_PRIMARY_SNAPSHOTS_AND_MOUNT_POINTS** specifica i nomi degli snapshot creati durante il backup di ciascuno dei punti di montaggio.

  Esempi:

  - Per una singola istanza del database: 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
  - Per più istanze di database: 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** specifica la posizione della directory dei registri di archivio.

  I nomi delle directory saranno il padre immediato dei file di registro dell'archivio. Se i registri di archivio vengono posizionati in più posizioni, verranno acquisite tutte le posizioni. Ciò include anche gli scenari FRA. Se per la directory vengono utilizzati i softlink, questi verranno popolati.

  Esempi:

  - Per un singolo database su NFS: /mnt/nfsdb2_log
  - Per più database su NFS e per i registri di archivio del database NFSB31 che si trovano in due posizioni diverse: NFSB31@/mnt/nfsdb31_log1,/mnt/nfsdb31_log2|NFSB32@/mnt/nfsdb32_log
  - Per ASM: +LOG2DG/ASMDB2/ARCHIVELOG/2021_07_15
- **SC_REDO_LOGS_LOCATIONS** specifica la posizione della directory dei redo log.

  I nomi delle directory saranno il padre immediato dei file redo log. Se per la directory vengono utilizzati i softlink, questi verranno popolati.

  Esempi:

  - Per un singolo database su NFS: /mnt/nfsdb2_data/newdb1
  - Per più database su NFS: NFSB31@/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/newdb32
  - Per ASM: +LOG2DG/ASMDB2/ONLINELOG
- **SC_CONTROL_FILES_LOCATIONS** specifica la posizione della directory dei file di controllo.

  I nomi delle directory saranno il genitore immediato dei file di controllo. Se per la directory vengono utilizzati i softlink, questi verranno popolati.

  Esempi:

  - Per un singolo database su NFS: /mnt/nfsdb2_data/fra/newdb1,/mnt/nfsdb2_data/newdb1
  - Per più database su NFS: NFSB31@/mnt/nfsdb31_data/fra/newdb31,/mnt/nfsdb31_data/newdb31|NFSB32@/mnt/nfsdb32_data/f

ra/newdb32,/mnt/nfsdb32_data/newdb32

- Per ASM: +LOG2DG/ASMDB2/CONTROLFILE

- **SC_DATA_FILES_LOCATIONS**" specifica la posizione della directory dei file di dati.

  I nomi delle directory saranno il genitore immediato dei file di dati. Se per la directory vengono utilizzati i softlink, questi verranno popolati.

  Esempi:

  - Per un singolo database su NFS: /mnt/nfsdb3_data1,/mnt/nfsdb3_data/NEWDB3/datafile
  - Per più database su NFS: NFSB31@/mnt/nfsdb31_data1,/mnt/nfsdb31_data/NEWDB31/datafile|NFSB32@/mnt/nfsdb32_data1,/mnt/nfsdb32_data/NEWDB32/datafile
  - Per ASM: +DATA2DG/ASMDB2/DATAFILE,+DATA2DG/ASMDB2/TEMPFILE

- **SC_SNAPSHOT_LABEL** specifica il nome delle etichette secondarie.

  Esempi: etichetta oraria, giornaliera, settimanale, mensile o personalizzata.

#### Delimitatori supportati

- **:** viene utilizzato per separare il nome SVM dal nome del volume

  Esempio: 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

- **@** viene utilizzato per separare i dati dal nome del database e per separare il valore dalla sua chiave.

  Esempi:

  - 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

- **|** viene utilizzato per separare i dati tra due database diversi e per separare i dati tra due entità diverse per i parametri SC_BACKUP_ID, SC_BACKUP_RETENTION e SC_BACKUP_NAME.

  Esempi:

  - DATI@203|LOG@205
  - Ogni ora|DATI@GIORNI:3|LOG@CONTEGGIO:4
  - DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1

- **/** viene utilizzato per separare il nome del volume dal suo Snapshot per i parametri SC_PRIMARY_SNAPSHOT_NAMES e SC_PRIMARY_FULL_SNAPSHOT_NAME_FOR_TAG.

  Esempio: 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

- **,** viene utilizzato per separare un insieme di variabili per lo stesso DB.

  Esempio: 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

**Opzioni di conservazione del backup**

È possibile scegliere il numero di giorni per cui conservare le copie di backup oppure specificare il numero di copie di backup che si desidera conservare, fino a un massimo ONTAP di 255 copie. Ad esempio, la tua organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica SnapMirror , il criterio di conservazione viene replicato sul volume di destinazione.

SnapCenter elimina i backup conservati che hanno etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero comunque rimanere sul sistema.

Per la conservazione a lungo termine delle copie di backup, è consigliabile utilizzare il backup SnapVault .

**Pianificazioni di backup**

La frequenza del backup (tipo di pianificazione) è specificata nei criteri; una pianificazione del backup è specificata nella configurazione del gruppo di risorse. Il fattore più critico nella determinazione della frequenza o della pianificazione di un backup è la velocità di modifica della risorsa e l'importanza dei dati. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. L'SLA e l'RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, potrebbero essere sufficienti backup regolari del registro delle transazioni per garantire di

disporre dei backup necessari. Quanto più spesso si esegue il backup dei database, tanto minore sarà il numero di registri delle transazioni che SnapCenter dovrà utilizzare al momento del ripristino, il che può comportare operazioni di ripristino più rapide.

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup

  La frequenza di backup (la frequenza con cui devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte della configurazione di una policy. È possibile selezionare la frequenza di backup oraria, giornaliera, settimanale o mensile per la policy. Se non si seleziona nessuna di queste frequenze, la policy creata sarà una policy solo on-demand. È possibile accedere alle policy facendo clic su **Impostazioni** > **Policy**.

- Pianificazioni di backup

  Le pianificazioni dei backup (ovvero quando devono essere eseguiti esattamente) fanno parte della configurazione di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **Risorse** > **Gruppi di risorse**.

#### Convenzioni di denominazione del backup

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

## Requisiti per il backup di un database Oracle

Prima di eseguire il backup di un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- È necessario aver assegnato l'aggregato utilizzato dall'operazione di backup alla macchina virtuale di archiviazione (SVM) utilizzata dal database.
- Se per quel database è abilitata la protezione secondaria, dovresti aver verificato che tutti i volumi di dati e i volumi di registro di archivio appartenenti al database siano protetti.
- Avresti dovuto verificare che il database che contiene file sui gruppi di dischi ASM fosse nello stato "MOUNT" o "OPEN" per verificare i suoi backup utilizzando l'utilità Oracle DBVERIFY.
- Dovresti aver verificato che la lunghezza del punto di montaggio del volume non superi i 240 caratteri.
- Se il database sottoposto a backup è di grandi dimensioni (dimensioni in TB), è necessario aumentare il valore di RESTTimeout a 86400000 ms nel file *C:\Program Files\ NetApp \SMCore\SMCoreServiceHost.exe.config* nell'host del server SnapCenter .

  Durante la modifica dei valori, assicurarsi che non vi siano processi in esecuzione e riavviare il servizio SnapCenter SMCore dopo aver aumentato il valore.

## Scopri i database Oracle disponibili per il backup

Le risorse sono database Oracle sull'host gestiti da SnapCenter. È possibile aggiungere questi database ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database disponibili.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la creazione di connessioni al sistema di archiviazione e l'aggiunta di credenziali.
- Se i database risiedono su un disco di macchina virtuale (VMDK) o su un mapping di dispositivi raw (RDM), è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Distribuisci il SnapCenter Plug-in for VMware vSphere" .
- Se i database risiedono su un file system VMDK, è necessario aver effettuato l'accesso a vCenter e aver selezionato **Opzioni VM** > **Avanzate** > **Modifica configurazione** per impostare il valore di *disk.enableUUID* su true per la VM.
- È necessario aver esaminato il processo seguito da SnapCenter per individuare diversi tipi e versioni di database Oracle.

**Passaggio 1: impedire a SnapCenter di rilevare voci non di database**

È possibile impedire a SnapCenter di rilevare voci non di database aggiunte nel file oratab.

**Passi**

1. Dopo aver installato il plug-in per Oracle, l'utente root deve creare il file **sc_oratab.config** nella directory */var/opt/snapcenter/sco/etc/*.

   Concedere l'autorizzazione di scrittura al proprietario e al gruppo del binario Oracle in modo che il file possa essere gestito in futuro.

2. L'amministratore del database dovrebbe aggiungere le voci non relative al database nel file **sc_oratab.config**.

   Si consiglia di mantenere lo stesso formato definito per le voci non di database nel file */etc/oratab* oppure l'utente può semplicemente aggiungere la stringa dell'entità non di database.

   > La stringa è sensibile alle maiuscole e alle minuscole. Qualsiasi testo che inizia con # viene considerato un commento. Il commento può essere aggiunto dopo il nome non appartenente al database.

   ```
   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. Scopri le risorse.

   Le voci non di database aggiunte in **sc_oratab.config** non verranno elencate nella pagina Risorse.

> Si consiglia sempre di eseguire un backup del file sc_oratab.config prima di aggiornare il plug-in SnapCenter .

**Fase 2: Scopri le risorse**

Dopo aver installato il plug-in, tutti i database presenti su quell'host vengono automaticamente rilevati e visualizzati nella pagina Risorse.

Affinché la scoperta dei database abbia successo, è necessario che i database siano almeno nello stato montato o superiore. In un ambiente Oracle Real Application Clusters (RAC), l'istanza del database RAC nell'host in cui viene eseguita la scoperta deve essere almeno nello stato montato o superiore affinché la scoperta dell'istanza del database abbia esito positivo. Solo i database scoperti correttamente possono essere aggiunti ai gruppi di risorse.

Se hai eliminato un database Oracle sull'host, SnapCenter Server non ne sarà a conoscenza e elencherà il database eliminato. È necessario aggiornare manualmente le risorse per aggiornare l'elenco delle risorse SnapCenter .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.

   Clic icona filtro], quindi selezionare il nome host e il tipo di database per filtrare le risorse. È quindi possibile fare clic sull'icona imagfilter_icon.gif[icona filtro]_icon.png[] per chiudere il riquadro filtro.
3. Fare clic su **Aggiorna risorse**.

   In uno scenario RAC One Node, il database viene rilevato come database RAC sul nodo in cui è attualmente ospitato.

**Risultati**

I database vengono visualizzati insieme a informazioni quali tipo di database, nome host o cluster, gruppi di risorse e policy associati e stato.

È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

- Se il database si trova su un sistema di archiviazione non NetApp , l'interfaccia utente visualizza il messaggio Non disponibile per il backup nella colonna Stato generale.

  Non è possibile eseguire operazioni di protezione dei dati sul database che si trova su un sistema di archiviazione non NetApp .
- Se il database si trova su un sistema di archiviazione NetApp e non è protetto, l'interfaccia utente visualizza il messaggio Non protetto nella colonna Stato generale.
- Se il database si trova su un sistema di archiviazione NetApp ed è protetto, l'interfaccia utente visualizza un messaggio Disponibile per il backup nella colonna Stato generale.

Se hai abilitato l'autenticazione del database Oracle, nella vista delle risorse viene visualizzata un'icona a forma di lucchetto rosso. È necessario configurare le credenziali del database per poter proteggere il database o aggiungerlo al gruppo di risorse per eseguire operazioni di protezione dei dati.

## Creare policy di backup per i database Oracle

Prima di utilizzare SnapCenter per eseguire il backup delle risorse del database Oracle, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup. È inoltre possibile specificare le impostazioni relative a replica, script e tipo di backup. La creazione di un criterio consente di risparmiare tempo quando si desidera riutilizzarlo su un'altra risorsa o un altro gruppo di risorse.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup.
- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione SnapCenter, l'aggiunta di host, l'individuazione di database e la creazione di connessioni al sistema di archiviazione.

- Se si replicano gli snapshot su un mirror o su un archivio secondario vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.
- Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.
- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.

+ Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.

+ Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare **Oracle Database** dall'elenco a discesa.
4. Fare clic su **Nuovo**.
5. Nella pagina Nome, immettere il nome e i dettagli della policy.
6. Nella pagina Tipo di policy, procedere come segue:

    a. Seleziona il tipo di archiviazione.

    b. Seleziona l'ambito della policy:

        - Se vuoi **creare un backup online**, seleziona **Backup online**.

          È necessario specificare se si desidera eseguire il backup di tutti i file di dati, dei file di controllo e dei file di registro di archivio, solo dei file di dati e dei file di controllo o solo dei file di registro di archivio.

        - Se vuoi **creare un backup offline**, seleziona **Backup offline**, quindi seleziona una delle seguenti opzioni:
            - Se si desidera creare un backup offline quando il database è montato, selezionare **Monta**.
            - Se si desidera creare un backup di arresto offline modificando lo stato del database in stato di arresto, selezionare **Arresto**.

              Se si dispone di database collegabili (PDB) e si desidera salvare lo stato dei PDB prima di creare il backup, è necessario selezionare **Salva stato dei PDB**. Ciò consente di riportare i PDB al loro stato originale dopo la creazione del backup.

    c. Se si desidera catalogare il backup utilizzando Oracle Recovery Manager (RMAN), selezionare **Catalog backup with Oracle Recovery Manager (RMAN)**.

       È possibile eseguire la catalogazione differita per un backup alla volta utilizzando l'interfaccia utente

grafica (GUI) o il comando Catalog-SmBackupWithOracleRMAN della CLI SnapCenter .

> Se si desidera catalogare i backup di un database RAC, assicurarsi che non sia in esecuzione nessun altro processo per quel database. Se è in esecuzione un altro processo, l'operazione di catalogazione fallisce anziché essere messa in coda.

d. Se si desidera eliminare i log di archivio dopo il backup, selezionare **Elimina log di archivio dopo il backup**.

> L'eliminazione dei log di archivio dalla destinazione del log di archivio non configurata nel database verrà ignorata.

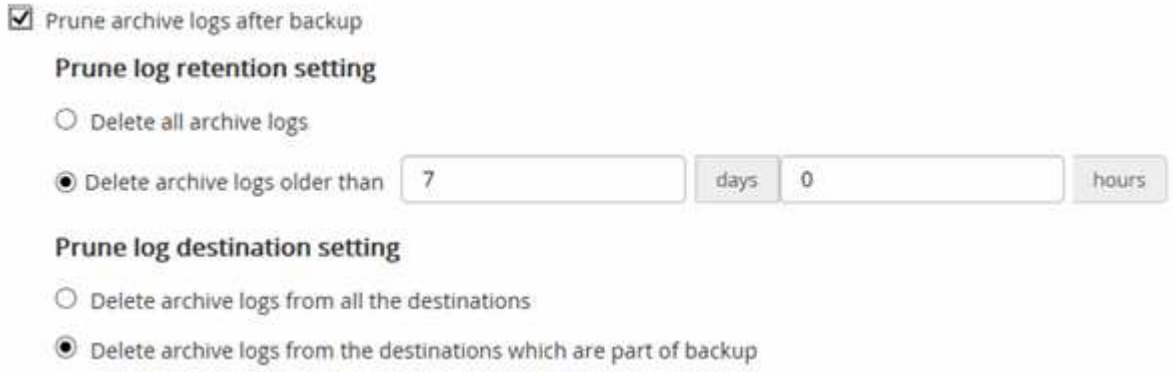
> Se si utilizza Oracle Standard Edition, è possibile utilizzare i parametri LOG_ARCHIVE_DEST e LOG_ARCHIVE_DUPLEX_DEST durante l'esecuzione del backup del log di archivio.

- È possibile eliminare i registri di archivio solo se sono stati selezionati i file di registro di archivio come parte del backup.

> Affinché l'operazione di eliminazione abbia esito positivo, è necessario assicurarsi che tutti i nodi in un ambiente RAC possano accedere a tutte le posizioni dei registri di archivio.

| **Se lo desidera…** | **Poi…** |
|---|---|
| Elimina tutti i registri di archivio | Seleziona **Elimina tutti i registri di archivio**. |
| Elimina i registri di archivio più vecchi | Selezionare **Elimina i registri di archivio più vecchi di**, quindi specificare l'età dei registri di archivio da eliminare in giorni e ore. |
| Elimina i log di archivio da tutte le destinazioni | Selezionare **Elimina i log di archivio da tutte le destinazioni**. |
| Eliminare i log di archivio dalle destinazioni dei log che fanno parte del backup | Selezionare **Elimina i registri di archivio dalle destinazioni che fanno parte del backup**. |

+



7. Nella pagina Snapshot e replica, procedere come segue:

   a. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.

      È possibile specificare la pianificazione (data di inizio e data di fine) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente di assegnare pianificazioni di backup diverse a ciascuna policy.

      Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

   a. Nella sezione Impostazioni di conservazione degli snapshot dei dati, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Tipo di backup:

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |

| | |
|---|---|
| Periodo di blocco della copia snapshot | Selezionare il **Periodo di blocco della copia snapshot** e specificare la durata in giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

b. Nella sezione Impostazioni di conservazione degli snapshot del registro di archivio, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Tipo di backup:

| Se lo desidera… | Poi… |
|---|---|
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare il **Periodo di blocco della copia snapshot** e specificare la durata in giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

c. Seleziona l'etichetta della policy.

> È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

8. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

> Per rendere effettivo il **Periodo di blocco della copia snapshot secondaria**, è necessario selezionare le opzioni di replica secondaria.

| Per questo campo… | Fai questo… |
|---|---|
| Aggiorna SnapMirror dopo aver creato uno Snapshot locale | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror .<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP. |
| Aggiorna SnapVault dopo aver creato uno Snapshot locale | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ).<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per maggiori informazioni su SnapLock Vault vedere "Eseguire il commit delle copie Snapshot su WORM in una destinazione vault"<br><br>Vedere "Visualizza i backup e i cloni del database Oracle nella pagina Topologia" . |
| Errore nel conteggio dei tentativi | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

9. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.

   È necessario memorizzare i prescript e i postscript in */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

   È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

10. Nella pagina Verifica, procedere come segue:

    a. Selezionare la pianificazione del backup per la quale si desidera eseguire l'operazione di verifica.
    b. Nella sezione Comandi dello script di verifica, immettere il percorso e gli argomenti del prescript o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di verifica.

       È necessario memorizzare i prescript e i postscript in */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

    È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

11. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega policy per i database Oracle

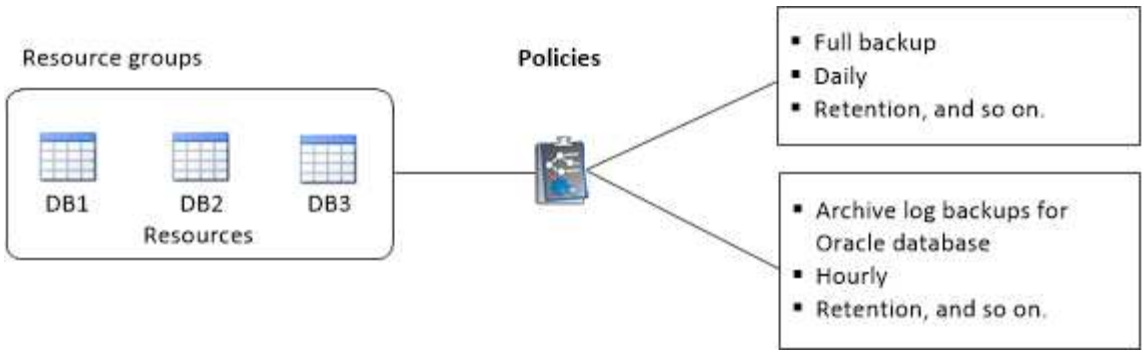
Un gruppo di risorse è un contenitore in cui aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione.

**Informazioni su questo compito**

- Un database con file in gruppi di dischi ASM deve essere nello stato "MOUNT" o "OPEN" per verificare i propri backup utilizzando l'utilità Oracle DBVERIFY.

  Allegare una o più policy al gruppo di risorse per definire il tipo di attività di protezione dei dati che si desidera eseguire.

  L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:




- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi database senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

      Dovresti usare esattamente la stessa destinazione impostata in Oracle, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona un nome host del database Oracle dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Seleziona le risorse dalla sezione Risorse disponibili e spostale nella sezione Risorse selezionate.

   È possibile aggiungere database da host Linux e AIX in un singolo gruppo di risorse.

6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

      Dove *policy_name* è il nome della policy selezionata.

      Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Verifica, procedere come segue:

   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| **Se lo desidera…** | **Fai questo…** |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

   e. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare

le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

10. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse Oracle sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per

impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

> Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

> Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

> Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

a. Selezionare il tipo di criterio di replica.

> La politica di replica sincrona non è supportata.

b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

> Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

   Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Eseguire il backup delle risorse Oracle

Se una risorsa non fa parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco Visualizza.
3. Clic , quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   Puoi quindi fare clic per chiudere il riquadro del filtro.

4. Selezionare il database di cui si desidera eseguire il backup.

   Viene visualizzata la pagina Database-Protect.

5. Nella pagina Risorse, procedere come segue:
   a. Selezionare la casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Per esempio, `customtext_policy_hostname` O `resource_hostname` . Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   b. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.
6. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per configurare una pianificazione per la policy desiderata.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione e quindi seleziona `OK` .

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault per verificare l'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio. + Nella finestra di dialogo Aggiungi pianificazioni di verifica *nome_policy*, è possibile eseguire i seguenti passaggi:
   c. Selezionare **Esegui verifica dopo il backup**.
   d. Selezionare **Esegui verifica pianificata** e selezionare il tipo di pianificazione dall'elenco a discesa.

      In una configurazione Flex ASM, non è possibile eseguire operazioni di verifica sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

   e. Seleziona **Verifica su posizione secondaria** per verificare i backup su un archivio secondario.
   f. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

8. Nella pagina Notifica, seleziona gli scenari in cui desideri inviare le email dall'elenco a discesa **Preferenza email**.

È necessario specificare gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Allega report attività**.

Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente o il comando PowerShell `Set-SmSmtpServer` .

9. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia del database.

10. Fare clic su **Esegui backup ora**.
11. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa Criterio seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Dopo aver finito**

- Nella configurazione AIX, è possibile utilizzare `lkdev` comando per bloccare e il `rendev` comando per rinominare i dischi su cui risiedeva il database sottoposto a backup.

  Il blocco o la ridenominazione dei dispositivi non influirà sull'operazione di ripristino quando si esegue il ripristino utilizzando tale backup.

- Se l'operazione di backup non riesce perché il tempo di esecuzione della query del database ha superato il valore di timeout, è necessario modificare il valore dei parametri ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT eseguendo il comando `Set-SmConfigSettings` cmdlet:

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il seguente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se il file non è accessibile e il punto di montaggio non è disponibile durante il processo di verifica, l'operazione potrebbe non riuscire con il codice di errore DBV-00100 nel file specificato. È necessario modificare i valori dei parametri VERIFICATION_DELAY e VERIFICATION_RETRY_COUNT in sco.properties.

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il seguente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.
- Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

  Per aumentare la dimensione dell'heap Java, individuare il file di script */opt/netapp/init_scripts/scvservice*. In quella sceneggiatura, il `do_start method` Il comando avvia il servizio plug-in SnapCenter VMware.

Aggiorna quel comando come segue: `Java -jar -Xmx8192M -Xms4096M .`

**Trova maggiori informazioni**

- "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"
- "Il database Oracle RAC One Node viene ignorato per l'esecuzione delle operazioni SnapCenter"
- "Impossibile modificare lo stato di un database Oracle 12c ASM"
- "Parametri personalizzabili per le operazioni di backup, ripristino e clonazione sui sistemi AIX"(Richiede l'accesso)

## Eseguire il backup dei gruppi di risorse del database Oracle

Un gruppo di risorse è una raccolta di risorse su un host o cluster. L'operazione di backup viene eseguita su tutte le risorse definite nel gruppo di risorse.

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono creati in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Inserisci il nome del gruppo di risorse nella casella di ricerca oppure fai clic su e seleziona il tag.

   Clic per chiudere il riquadro del filtro.

4. Nella pagina Gruppo di risorse, seleziona il gruppo di risorse di cui eseguire il backup.

   Se si dispone di un gruppo di risorse federato con due database e uno dei due contiene dati su uno storage non NetApp , l'operazione di backup viene interrotta anche se l'altro database si trova su uno storage NetApp .

5. Nella pagina Backup, procedere come segue:
   a. Se al gruppo di risorse sono associati più criteri, selezionare il criterio di backup che si desidera utilizzare dall'elenco a discesa **Criterio**.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
6. Monitorare l'avanzamento selezionando **Monitoraggio > Lavori**.

**Dopo aver finito**

- Nella configurazione AIX, è possibile utilizzare `lkdev` comando per bloccare e il `rendev` comando per rinominare i dischi su cui risiedeva il database sottoposto a backup.

  Il blocco o la ridenominazione dei dispositivi non influirà sull'operazione di ripristino quando si esegue il ripristino utilizzando tale backup.

- Se l'operazione di backup non riesce perché il tempo di esecuzione della query del database ha superato il valore di timeout, è necessario modificare il valore dei parametri ORACLE_SQL_QUERY_TIMEOUT e ORACLE_PLUGIN_SQL_QUERY_TIMEOUT eseguendo il comando `Set-SmConfigSettings` cmdlet:

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il seguente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

- Se il file non è accessibile e il punto di montaggio non è disponibile durante il processo di verifica, l'operazione potrebbe non riuscire con il codice di errore DBV-00100 nel file specificato. È necessario modificare i valori dei parametri VERIFICATION_DELAY_ e VERIFICATION_RETRY_COUNT in sco.properties.

  Dopo aver modificato il valore dei parametri, riavviare il servizio SnapCenter Plug-in Loader (SPL) eseguendo il seguente comando `/opt/NetApp/snapcenter/spl/bin/spl restart`

## Monitorare il backup del database Oracle

Scopri come monitorare l'avanzamento delle operazioni di backup e di protezione dei dati.

### Monitorare le operazioni di backup del database Oracle

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

#### Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.

e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.

4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

> Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni di protezione dei dati nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Altre operazioni di backup

#### Eseguire il backup dei database Oracle utilizzando i comandi UNIX

Il flusso di lavoro del backup include la pianificazione, l'identificazione delle risorse per il backup, la creazione di policy di backup, la creazione di gruppi di risorse e l'associazione di policy, la creazione di backup e il monitoraggio delle operazioni.

**Cosa ti servirà**

- Dovresti aver aggiunto le connessioni al sistema di archiviazione e creato le credenziali utilizzando i comandi *Add-SmStorageConnection* e *Add-SmCredential*.
- Dovresti aver stabilito la sessione di connessione con SnapCenter Server utilizzando il comando *Open-SmConnection*.

  È possibile avere una sola sessione di accesso all'account SnapCenter e il token viene archiviato nella directory home dell'utente.

> La sessione di connessione è valida solo per 24 ore. Tuttavia, è possibile creare un token con l'opzione TokenNeverExpires per creare un token che non scade mai e la sessione sarà sempre valida.

**Informazioni su questo compito**

È necessario eseguire i seguenti comandi per stabilire la connessione con SnapCenter Server, individuare le istanze del database Oracle, aggiungere policy e gruppo di risorse, eseguire il backup e verificare il backup.

Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

**Passi**

1. Avvia una sessione di connessione con il server SnapCenter per un utente specificato: *Open-SmConnection*
2. Eseguire l'operazione di rilevamento delle risorse host: *Get-SmResources*
3. Configurare le credenziali del database Oracle e i nodi preferiti per l'operazione di backup di un database Real Application Cluster (RAC): *Configure-SmOracleDatabase*
4. Crea una policy di backup: *Add-SmPolicy*
5. Recupera le informazioni sulla posizione di archiviazione secondaria (SnapVault o SnapMirror): *Get-SmSecondaryDetails*

   Questo comando recupera i dettagli di mappatura dello storage primario e secondario di una risorsa specificata. È possibile utilizzare i dettagli di mappatura per configurare le impostazioni di verifica secondaria durante la creazione di un gruppo di risorse di backup.
6. Aggiungi un gruppo di risorse a SnapCenter: *Add-SmResourceGroup*
7. Crea un backup: *New-SmBackup*

   È possibile interrogare il processo utilizzando l'opzione WaitForCompletion. Se questa opzione è specificata, il comando continua a interrogare il server fino al completamento del processo di backup.
8. Recupera i log da SnapCenter: *Get-SmLogs*

**Annullare le operazioni di backup dei database Oracle**

## È possibile annullare le operazioni di backup in esecuzione, in coda o che non rispondono.

Per annullare le operazioni di backup, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

Quando si annulla un'operazione di backup, SnapCenter Server interrompe l'operazione e rimuove tutti gli snapshot dall'archivio se il backup creato non è registrato con SnapCenter Server. Se il backup è già registrato con SnapCenter Server, non verrà eseguito il rollback dello Snapshot già creato, anche dopo l'attivazione dell'annullamento.

- È possibile annullare solo il registro o l'operazione di backup completo in coda o in esecuzione.
- Non è possibile annullare l'operazione dopo l'avvio della verifica.

  Se si annulla l'operazione prima della verifica, l'operazione viene annullata e la verifica non verrà eseguita.
- Non è possibile annullare l'operazione di backup dopo l'avvio delle operazioni di catalogo.

- È possibile annullare un'operazione di backup dalla pagina Monitor o dal riquadro Attività.
- Oltre a utilizzare l'interfaccia grafica utente SnapCenter , è possibile utilizzare i comandi CLI per annullare le operazioni.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Selezionare l'operazione e fare clic su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato il processo di backup, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

**Risultati**

L'operazione viene annullata e la risorsa viene ripristinata allo stato originale.

Se l'operazione annullata non risponde nello stato di annullamento o di esecuzione, è necessario eseguire Cancel-SmJob -JobID <int> -Force per interrompere forzatamente l'operazione di backup.

### Visualizza i backup e i cloni del database Oracle nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

-

visualizza il numero di backup e cloni disponibili sullo storage primario.

- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

  Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina Topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   Nella sezione Scheda riepilogativa viene visualizzato il numero totale di backup e cloni e il numero totale di backup del registro.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

- Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
- Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, montaggio, smontaggio, ridenominazione, catalogazione, decatalogazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

   - Se hai selezionato un backup del log, puoi eseguire solo operazioni di ridenominazione, montaggio, smontaggio, catalogazione, decatalogazione ed eliminazione.
   - Se il backup è stato catalogato tramite Oracle Recovery Manager (RMAN), non è possibile rinominare i backup catalogati.

7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .

Se il valore assegnato a SnapmirrorStatusUpdateWaitTime è inferiore, le copie di backup Mirror e Vault non vengono elencate nella pagina della topologia, anche se i volumi di dati e log sono protetti correttamente. Dovresti aumentare il valore assegnato a SnapmirrorStatusUpdateWaitTime utilizzando il cmdlet PowerShell *Set-SmConfigSettings*.

Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*.

In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" O "Guida di riferimento ai cmdlet del software SnapCenter" .

# Montare e smontare i backup del database

È possibile montare uno o più backup di dati e solo di registro se si desidera accedere ai file nel backup. È possibile montare il backup sullo stesso host in cui è stato creato oppure su un host remoto con lo stesso tipo di configurazione Oracle e host. Se hai montato manualmente i backup, dovresti smontarli manualmente dopo aver completato l'operazione. In qualsiasi momento, è possibile montare un backup di un database su uno qualsiasi degli host. Durante l'esecuzione di un'operazione, è possibile montare un solo

backup.

In una configurazione Flex ASM, non è possibile eseguire operazioni di montaggio sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

## Montare un backup del database

Se si desidera accedere ai file nel backup, è necessario montare manualmente un backup del database.

### Cosa ti servirà

- Se si dispone di un'istanza del database Automatic Storage Management (ASM) in un ambiente NFS e si desidera montare i backup ASM, è necessario aggiungere il percorso del disco ASM */var/opt/snapcenter/sco/backup*/*/*/*/** al percorso esistente definito nel parametro asm_diskstring.
- Se si dispone di un'istanza del database ASM in un ambiente NFS e si desidera montare i backup del log ASM come parte di un'operazione di ripristino, è necessario aggiungere il percorso del disco ASM */var/opt/snapcenter/scu/clones/*/*_* al percorso esistente definito nel parametro asm_diskstring.
- Nel parametro asm_diskstring, dovresti configurare *AFD:** se stai utilizzando ASMFD o configurare *ORCL:** se stai utilizzando ASMLIB.

Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere percorsi disco a asm_diskstring" .

- È necessario configurare le credenziali ASM e la porta ASM se differiscono da quelle dell'host del database di origine durante il montaggio del backup.
- Se si desidera effettuare il montaggio su un host alternativo, è necessario verificare che l'host alternativo soddisfi i seguenti requisiti:
  - UID e GID uguali a quelli dell'host originale
  - Stessa versione di Oracle dell'host originale
  - Stessa distribuzione e versione del sistema operativo dell'host originale
  - Per NVMe, è necessario installare NVMe util
- È necessario assicurarsi che la LUN non sia mappata sull'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "L'operazione fallisce con errore Impossibile rilevare il dispositivo per LUN" .

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione primario o secondario (con mirroring o replica).
5. Selezionare il backup dalla tabella, quindi fare clic su .

6. Nella pagina Monta backup, seleziona l'host su cui desideri montare il backup dall'elenco a discesa **Scegli l'host su cui montare il backup**.

   Viene visualizzato il percorso di montaggio */var/opt/snapcenter/sco/backup_mount/backup_name/database_name*.

   Se si sta montando il backup di un database ASM, viene visualizzato il percorso di montaggio +diskgroupname_SID_backupid.

7. Fare clic su **Monta**.

**Dopo aver finito**

- È possibile eseguire il seguente comando per recuperare le informazioni relative al backup montato:

  ```
  ./sccli Get-SmBackup -BackupName backup_name -ListMountInfo
  ```

- Se hai montato un database ASM, puoi eseguire il seguente comando per recuperare le informazioni relative al backup montato:

  ```
  ./sccli Get-Smbackup -BackupNamediskgroupname_SID_backupid-listmountinfo
  ```

- Per recuperare l'ID del backup, eseguire il seguente comando:

  ```
  ./sccli Get-Smbackup-BackupNamebackup_name
  ```

  Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

## Smontare un backup del database

È possibile smontare manualmente un backup del database montato quando non si desidera più accedere ai file presenti sul backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

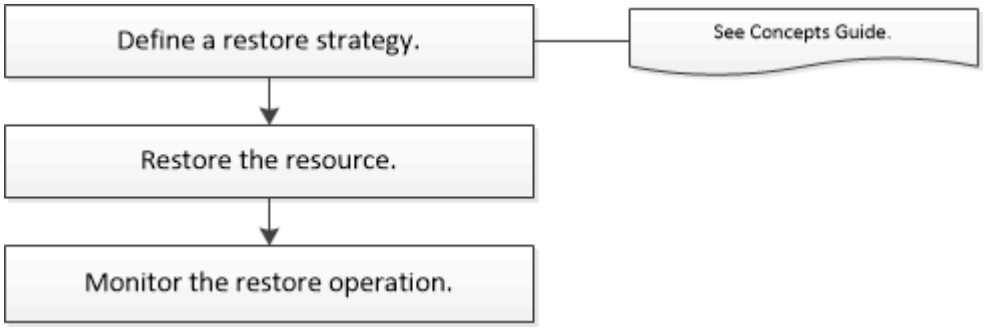
4. Selezionare il backup montato, quindi fare clic su .
5. Fare clic su **OK**.

# Ripristinare e recuperare i database Oracle

## Ripristina flusso di lavoro

Il flusso di lavoro di ripristino include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




## Definire una strategia di ripristino e recupero per i database Oracle

È necessario definire una strategia prima di ripristinare e recuperare il database, in modo da poter eseguire correttamente le operazioni di ripristino e recupero.

### Tipi di backup supportati per le operazioni di ripristino e recupero

SnapCenter supporta il ripristino e il recupero di diversi tipi di backup del database Oracle.

- Backup dei dati online
- Backup dei dati di arresto offline
- Backup dei dati di montaggio offline

> Se si ripristina un backup dei dati di arresto offline o di montaggio offline, SnapCenter lascia il database nello stato offline. Dovresti ripristinare manualmente il database e reimpostare i log.

- Backup completo
- Backup offline dei database standby di Data Guard
- Backup online dei soli dati dei database di standby di Active Data Guard

> Non è possibile eseguire il ripristino dei database standby di Active Data Guard.

- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione Real Application Clusters (RAC)
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione di gestione automatica dell'archiviazione (ASM)

### Tipi di metodi di ripristino supportati per i database Oracle

SnapCenter supporta la connessione e la copia o il ripristino sul posto per i database Oracle. Durante un'operazione di ripristino, SnapCenter determina il metodo di ripristino più appropriato per il file system da utilizzare per il ripristino senza alcuna perdita di dati.

SnapCenter non supporta SnapRestore basato sul volume.

#### Ripristino tramite connessione e copia

Se il layout del database è diverso dal backup o se sono presenti nuovi file dopo la creazione del backup, viene eseguito il ripristino tramite connessione e copia. Nel metodo di ripristino tramite connessione e copia vengono eseguite le seguenti attività:

### Passi

1. Il volume viene clonato dallo Snapshot e lo stack del file system viene creato sull'host utilizzando i LUN o i volumi clonati.
2. I file vengono copiati dai file system clonati ai file system originali.
3. I file system clonati vengono quindi smontati dall'host e i volumi clonati vengono eliminati da ONTAP.

Per una configurazione Flex ASM (in cui la cardinalità è inferiore al numero di nodi nel cluster RAC) o per database ASM RAC su VMDK o RDM, è supportato solo il metodo di ripristino con connessione e copia.

Anche se hai abilitato forzatamente il ripristino sul posto, SnapCenter esegue il ripristino con connessione e copia nei seguenti scenari:

- Ripristina dal sistema di archiviazione secondario
- Ripristino dei gruppi di dischi ASM presenti sui nodi di una configurazione Oracle RAC su cui l'istanza del database non è configurata
- Nella configurazione di Oracle RAC, su uno qualsiasi dei nodi peer se l'istanza ASM o l'istanza del cluster non è in esecuzione o se il nodo peer è inattivo
- Ripristino solo dei file di controllo
- Ripristina un sottoinsieme di tablespace residenti su un gruppo di dischi ASM
- Il gruppo di dischi è condiviso tra file di dati, file sp e file di password
- Il servizio SnapCenter Plug-in Loader (SPL) non è installato o non è in esecuzione sul nodo remoto in un ambiente RAC
- Vengono aggiunti nuovi nodi a Oracle RAC e SnapCenter Server non è a conoscenza dei nuovi nodi aggiunti

#### Ripristino sul posto

Se il layout del database è simile al backup e non ha subito alcuna modifica di configurazione sullo stack di archiviazione e database, viene eseguito un ripristino sul posto, in cui il ripristino del file o della LUN viene eseguito su ONTAP. SnapCenter supporta solo Single File SnapRestore (SFSR) come parte del metodo di ripristino sul posto.

NetApp ONTAP supporta il ripristino sul posto da una posizione secondaria.

Se si desidera eseguire un ripristino sul posto del database, assicurarsi di avere solo file di dati sul gruppo di dischi ASM. È necessario creare un backup dopo aver apportato modifiche al gruppo di dischi ASM o alla struttura fisica del database. Dopo aver eseguito il ripristino sul posto, il gruppo di dischi conterrà lo stesso numero di file di dati presenti al momento del backup.

Il ripristino sul posto verrà applicato automaticamente quando il gruppo di dischi o il punto di montaggio corrisponde ai seguenti criteri:

- Nessun nuovo file di dati viene aggiunto dopo il backup (controllo file esterni)
- Nessuna aggiunta, eliminazione o ricreazione del disco ASM o LUN dopo il backup (controllo delle modifiche strutturali del gruppo di dischi ASM)
- Nessuna aggiunta, eliminazione o ricreazione di LUN nel gruppo di dischi LVM (controllo delle modifiche strutturali del gruppo di dischi LVM)

È anche possibile abilitare forzatamente il ripristino sul posto tramite GUI, SnapCenter CLI o cmdlet PowerShell per ignorare il controllo dei file esterni e il controllo delle modifiche strutturali del gruppo di dischi LVM.

**Esecuzione del ripristino sul posto su ASM RAC**

In SnapCenter, il nodo su cui si esegue il ripristino è definito nodo primario, mentre tutti gli altri nodi del RAC su cui risiede il gruppo di dischi ASM sono denominati nodi peer. SnapCenter modifica lo stato del gruppo di dischi ASM per smontarlo su tutti i nodi in cui il gruppo di dischi ASM è in stato di montaggio prima di eseguire l'operazione di ripristino dell'archiviazione. Una volta completato il ripristino dell'archiviazione, SnapCenter modifica lo stato del gruppo di dischi ASM rispetto a quello precedente all'operazione di ripristino.

Negli ambienti SAN, SnapCenter rimuove i dispositivi da tutti i nodi peer ed esegue l'operazione di unmap LUN prima dell'operazione di ripristino dell'archiviazione. Dopo l'operazione di ripristino dell'archiviazione, SnapCenter esegue l'operazione di mappatura LUN e crea dispositivi su tutti i nodi peer. In un ambiente SAN, se il layout Oracle RAC ASM risiede su LUN, durante il ripristino SnapCenter esegue operazioni di unmap LUN, ripristino LUN e mappatura LUN su tutti i nodi del cluster RAC in cui risiede il gruppo di dischi ASM. Prima del ripristino, anche se non tutti gli iniziatori dei nodi RAC sono stati utilizzati per le LUN, dopo il ripristino SnapCenter crea un nuovo iGroup con tutti gli iniziatori di tutti i nodi RAC.

- Se si verifica un errore durante l'attività di pre-ripristino sui nodi peer, SnapCenter ripristina automaticamente lo stato del gruppo di dischi ASM così come era prima dell'esecuzione del ripristino sui nodi peer su cui l'operazione di pre-ripristino ha avuto esito positivo. Il rollback non è supportato per il nodo primario e per il nodo peer su cui l'operazione non è riuscita. Prima di tentare un altro ripristino, è necessario risolvere manualmente il problema sul nodo peer e riportare il gruppo di dischi ASM sul nodo primario allo stato di montaggio.
- Se si verifica un errore durante l'attività di ripristino, l'operazione di ripristino fallisce e non viene eseguito alcun rollback. Prima di tentare un altro ripristino, è necessario risolvere manualmente il problema di ripristino dell'archiviazione e riportare il gruppo di dischi ASM sul nodo primario allo stato di montaggio.
- Se si verifica un errore durante l'attività di post-ripristino su uno qualsiasi dei nodi peer, SnapCenter continua con l'operazione di ripristino sugli altri nodi peer. È necessario risolvere manualmente il problema di ripristino successivo sul nodo peer.

**Tipi di operazioni di ripristino supportate per i database Oracle**

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i database Oracle.

Prima di ripristinare il database, i backup vengono convalidati per identificare eventuali file mancanti rispetto ai file effettivi del database.

**Ripristino completo**

- Ripristina solo i file di dati

- Ripristina solo i file di controllo
- Ripristina i file di dati e i file di controllo
- Ripristina i file di dati, i file di controllo e i file di registro redo nei database standby di Data Guard e Active Data Guard

#### Ripristino parziale

- Ripristina solo gli spazi tabella selezionati
- Ripristina solo i database collegabili selezionati (PDB)
- Ripristina solo gli spazi tabella selezionati di un PDB

### Tipi di operazioni di ripristino supportate per i database Oracle

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i database Oracle.

- Il database fino all'ultima transazione (tutti i log)
- Il database fino a un numero di modifica del sistema specifico (SCN)
- Il database fino a una data e un'ora specifiche

  È necessario specificare la data e l'ora per il ripristino in base al fuso orario dell'host del database.

  SnapCenter offre anche l'opzione Nessun ripristino per i database Oracle.

> Il plug-in per il database Oracle non supporta il ripristino se è stato eseguito utilizzando un backup creato con il ruolo del database come standby. Per i database fisici in standby è sempre necessario eseguire il ripristino manuale.

### Limitazioni relative al ripristino e al recupero dei database Oracle

Prima di eseguire operazioni di ripristino e recupero, è necessario essere consapevoli delle limitazioni.

Se si utilizza una versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di ripristino sarà bloccata quando si esegue il comando *renamedg*. Per risolvere questo problema, è possibile applicare la patch Oracle 19544733.

Le seguenti operazioni di ripristino e recupero non sono supportate:

- Ripristino e recupero degli spazi tabella del database contenitore radice (CDB)
- Ripristino di tablespace temporanei e tablespace temporanei associati ai PDB
- Ripristino e recupero di tablespace da più PDB contemporaneamente
- Ripristino dei backup del log
- Ripristino dei backup in una posizione diversa
- Ripristino dei file di registro redo in qualsiasi configurazione diversa dai database standby di Data Guard o Active Data Guard
- Ripristino del file SPFILE e password
- Quando si esegue un'operazione di ripristino su un database che è stato ricreato utilizzando il nome del database preesistente sullo stesso host, era gestito da SnapCenter e aveva backup validi, l'operazione di ripristino sovrascrive i file del database appena creati anche se i DBID sono diversi.

È possibile evitare questo inconveniente eseguendo una delle seguenti azioni:

- Scopri le risorse SnapCenter dopo che il database è stato ricreato
- Creare un backup del database ricreato

### Limitazioni relative al ripristino point-in-time degli spazi tabella

- Il ripristino point-in-time (PITR) degli spazi tabella SYSTEM, SYSAUX e UNDO non è supportato
- Il PITR degli spazi tabella non può essere eseguito insieme ad altri tipi di ripristino
- Se uno spazio di tabella viene rinominato e si desidera ripristinarlo a un punto precedente alla sua ridenominazione, è necessario specificare il nome precedente dello spazio di tabella.
- Se i vincoli per le tabelle in un tablespace sono contenuti in un altro tablespace, è necessario ripristinare entrambi i tablespace
- Se una tabella e i suoi indici sono archiviati in tablespace diversi, gli indici devono essere eliminati prima di eseguire PITR
- PITR non può essere utilizzato per recuperare l'attuale tablespace predefinito
- PITR non può essere utilizzato per recuperare tablespace contenenti uno qualsiasi dei seguenti oggetti:
  - Oggetti con oggetti sottostanti (ad esempio viste materializzate) o oggetti contenuti (ad esempio tabelle partizionate), a meno che tutti gli oggetti sottostanti o contenuti non siano nel set di ripristino

    Inoltre, se le partizioni di una tabella partizionata sono archiviate in tablespace diversi, è necessario eliminare la tabella prima di eseguire PITR oppure spostare tutte le partizioni nello stesso tablespace prima di eseguire PITR.

  - Annulla o ripristina i segmenti
  - Code avanzate compatibili con Oracle 8 con più destinatari
  - Oggetti di proprietà dell'utente SYS

    Esempi di questi tipi di oggetti sono PL/SQL, classi Java, programmi di chiamata, viste, sinonimi, utenti, privilegi, dimensioni, directory e sequenze.

### Origini e destinazioni per il ripristino dei database Oracle

È possibile ripristinare un database Oracle da una copia di backup su un archivio primario o secondario. È possibile ripristinare i database solo nella stessa posizione sulla stessa istanza del database. Tuttavia, nella configurazione Real Application Cluster (RAC), è possibile ripristinare i database su altri nodi.

#### Fonti per le operazioni di ripristino

È possibile ripristinare i database da un backup su un archivio primario o secondario. Se si desidera eseguire il ripristino da un backup sullo storage secondario in una configurazione con più mirror, è possibile selezionare il mirror dello storage secondario come origine.

#### Destinazioni per le operazioni di ripristino

È possibile ripristinare i database solo nella stessa posizione sulla stessa istanza del database.

In una configurazione RAC, è possibile ripristinare i database RAC da qualsiasi nodo del cluster.

## Variabili di ambiente predefinite per ripristinare specifici prescript e postscript

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript durante il ripristino di un database.

#### Variabili di ambiente predefinite supportate per il ripristino di un database

- **SC_JOB_ID** specifica l'ID del processo dell'operazione.

  Esempio: 257

- **SC_ORACLE_SID** specifica l'identificativo di sistema del database.

  Se l'operazione coinvolge più database, questo conterrà i nomi dei database separati da una barra verticale.

  Esempio: NFSB31

- **SC_HOST** specifica il nome host del database.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: scsmohost2.gdl.englabe.netapp.com

- **SC_OS_USER** specifica il proprietario del sistema operativo del database.

  Esempio: oracolo

- **SC_OS_GROUP** specifica il gruppo del sistema operativo del database.

  Esempio: oinstall

- **SC_BACKUP_NAME** specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

  - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se il database è in esecuzione in modalità ARCHIVELOG: 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_1

- **SC_BACKUP_ID** specifica l'ID del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

  - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@203|LOG@205
  - Se il database è in esecuzione in modalità ARCHIVELOG: DATA@203|LOG@205,206,207

- **SC_RESOURCE_GROUP_NAME** specifica il nome del gruppo di risorse.

Esempio: RG1

- **SC_ORACLE_HOME** specifica il percorso della directory home di Oracle.

  Esempio: /ora01/app/oracle/product/18.1.0/db_1

- **SC_RECOVERY_TYPE** specifica i file che vengono recuperati e anche l'ambito del recupero.

  Esempio:
  RESTORESCOPE:usingBackupControlfile=false|RECOVERYSCOPE:allLogs=true,noLogs=false,untiltime=false,untilscn=false.

Per informazioni sui delimitatori, vedere"Delimitatori supportati" .

## Requisiti per il ripristino di un database Oracle

Prima di ripristinare un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- Dovresti aver definito la tua strategia di ripristino e recupero.
- Se si stanno replicando snapshot su un mirror o un vault, l'amministratore SnapCenter dovrebbe aver assegnato le macchine virtuali di archiviazione (SVM) sia per i volumi di origine che per quelli di destinazione.
- Se i registri di archivio vengono eliminati durante il backup, è necessario montare manualmente i backup dei registri di archivio richiesti.
- Se si desidera ripristinare i database Oracle che risiedono su un disco di macchina virtuale (VMDK), è necessario assicurarsi che la macchina guest disponga del numero richiesto di slot liberi per l'allocazione dei VMDK clonati.
- Se per quel database è abilitata la protezione secondaria, è necessario assicurarsi che tutti i volumi di dati e i volumi di registro di archivio appartenenti al database siano protetti.
- È necessario assicurarsi che il database RAC One Node sia nello stato "nomount" per eseguire il ripristino del file di controllo o del database completo.
- Se si dispone di un'istanza del database ASM in ambiente NFS, è necessario aggiungere il percorso del disco ASM */var/opt/snapcenter/scu/clones/*/** al percorso esistente definito nel parametro asm_diskstring per montare correttamente i backup del log ASM come parte dell'operazione di ripristino.
- Nel parametro asm_diskstring, dovresti configurare *AFD:** se stai utilizzando ASMFD o configurare *ORCL:** se stai utilizzando ASMLIB.

  Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere percorsi disco a asm_diskstring"

- Se hai disabilitato l'autenticazione del sistema operativo e abilitato l'autenticazione del database Oracle per un database Oracle e desideri ripristinare i file di dati e i file di controllo di tale database, dovresti configurare l'ascoltatore statico nel file **listener.ora** disponibile in *$ORACLE_HOME/network/admin* per i database non ASM e in *$GRID_HOME/network/admin* per i database ASM.
- Se la dimensione del database è in terabyte (TB), è necessario aumentare il valore del parametro SCORestoreTimeout eseguendo il comando Set-SmConfigSettings.
- È necessario assicurarsi che tutte le licenze richieste per vCenter siano installate e aggiornate.

Se le licenze non sono installate o aggiornate, viene visualizzato un messaggio di avviso. Se si ignora l'avviso e si procede, il ripristino da RDM fallisce.

- È necessario assicurarsi che la LUN non sia mappata sull'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "L'operazione fallisce con errore Impossibile rilevare il dispositivo per LUN" .

## Ripristinare e recuperare il database Oracle

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i dati da uno o più backup sul file system attivo e quindi recuperare il database.

### Prima di iniziare

Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.

### Informazioni su questo compito

- Il ripristino viene eseguito utilizzando i registri di archivio disponibili nella posizione del registro di archivio configurata. Se il database è in esecuzione in modalità ARCHIVELOG, il database Oracle salva i gruppi compilati di file di redo log in una o più destinazioni offline, note collettivamente come redo log archiviato. SnapCenter identifica e monta il numero ottimale di backup dei log in base all'SCN specificato, alla data e all'ora selezionate o all'opzione di tutti i log. Se i log di archivio necessari per il ripristino non sono disponibili nella posizione configurata, è necessario montare lo Snapshot contenente i log e specificare il percorso come log di archivio esterno.

  Se si esegue la migrazione del database ASM da ASMLIB ad ASMFD, i backup creati con ASMLIB non potranno essere utilizzati per ripristinare il database. Dovresti creare dei backup nella configurazione ASMFD e utilizzare tali backup per il ripristino. Allo stesso modo, se il database ASM viene migrato da ASMFD ad ASMLIB, è necessario creare dei backup nella configurazione ASMLIB per il ripristino.

  Quando si ripristina un database, viene creato un file di blocco operativo (.sm_lock_dbsid) sull'host del database Oracle nella directory */var/opt/snapcenter/sco/lock* per evitare che vengano eseguite più operazioni sul database. Dopo il ripristino del database, il file di blocco operativo viene rimosso automaticamente.

  Il ripristino dei file SPFILE e Password non è supportato.

- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primario o secondario (con mirroring o replica).
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
   a. Se è stato selezionato un backup di un database in un ambiente Real Application Clusters (RAC), selezionare il nodo RAC.
   b. Quando selezioni dati mirrorati o vault:
      - se non sono presenti backup del log nel mirror o nel vault, non viene selezionato nulla e i localizzatori sono vuoti.
      - se i backup del log sono presenti nel mirror o nel vault, viene selezionato l'ultimo backup del log e viene visualizzato il localizzatore corrispondente.

      Se il backup del log selezionato esiste sia nella posizione mirror che in quella vault, vengono visualizzati entrambi i localizzatori.

   c. Eseguire le seguenti azioni:

| **Se vuoi ripristinare…** | **Fai questo…** |
|---|---|
| Tutti i file di dati del database | Seleziona **Tutti i file di dati**.<br><br>Vengono ripristinati solo i file di dati del database. I file di controllo, i log di archivio o i file di redo log non vengono ripristinati. |
| Tablespace | Selezionare **Tablespace**.<br><br>È possibile specificare gli spazi tabella che si desidera ripristinare. |
| File di controllo | Selezionare **File di controllo**.<br><br>Durante il ripristino dei file di controllo, assicurarsi che la struttura della directory esista o debba essere creata con le corrette proprietà utente e di gruppo, se presenti, per consentire la copia dei file nella posizione di destinazione tramite il processo di ripristino. Se la directory non esiste, il processo di ripristino non riuscirà. |

| Se vuoi ripristinare… | Fai questo… |
| --- | --- |
| File di registro redo | Selezionare **File di registro redo**.<br><br>Questa opzione è disponibile solo per i database Data Guard standby o Active Data Guard standby.<br><br>I file di redo log non vengono sottoposti a backup per i database non Data Guard. Per i database non Data Guard il ripristino viene eseguito utilizzando i log di archivio. |
| Database collegabili (PDB) | Selezionare **Database collegabili**, quindi specificare i PDB che si desidera ripristinare. |
| Tablespace del database collegabile (PDB) | Selezionare **Spazi tabella del database collegabile (PDB)**, quindi specificare il PDB e gli spazi tabella di quel PDB che si desidera ripristinare.<br><br>Questa opzione è disponibile solo se è stato selezionato un PDB per il ripristino. |

d. Selezionare **Modifica stato del database se necessario per il ripristino e il recupero** per modificare lo stato del database nello stato richiesto per eseguire operazioni di ripristino e recupero.

   I vari stati di un database, dal più alto al più basso, sono aperto, montato, avviato e spento. È necessario selezionare questa casella di controllo se il database si trova in uno stato superiore ma è necessario modificarlo in uno inferiore per eseguire un'operazione di ripristino. Se il database si trova in uno stato inferiore ma è necessario modificarlo in uno superiore per eseguire l'operazione di ripristino, lo stato del database viene modificato automaticamente anche se non si seleziona la casella di controllo.

Se un database è nello stato aperto e per ripristinarlo è necessario che sia nello stato montato, lo stato del database viene modificato solo se si seleziona questa casella di controllo.

a. Selezionare **Forza ripristino sul posto** se si desidera eseguire il ripristino sul posto negli scenari in cui vengono aggiunti nuovi file di dati dopo il backup o quando i LUN vengono aggiunti, eliminati o ricreati in un gruppo di dischi LVM.

7. Nella pagina Ambito di ripristino, eseguire le seguenti azioni:

| Se tu… | Fai questo… |
| --- | --- |
| Vuoi recuperare l'ultima transazione | Seleziona **Tutti i registri**. |
| Desideri ripristinare un numero di modifica del sistema (SCN) specifico | Selezionare **Fino a SCN (numero di modifica del sistema)**. |

| Se tu… | Fai questo… |
| --- | --- |
| Vuoi ripristinare una data e un'ora specifiche | Selezionare **Data e ora**.<br><br>È necessario specificare la data e l'ora del fuso orario dell'host del database. |
| Non voglio recuperare | Selezionare **Nessun recupero**. |
| Vuoi specificare eventuali posizioni di registro di archivio esterno | Se il database è in esecuzione in modalità ARCHIVELOG, SnapCenter identifica e monta il numero ottimale di backup dei log in base all'SCN specificato, alla data e all'ora selezionate o all'opzione di tutti i log.<br><br>Se si desidera comunque specificare la posizione dei file di registro dell'archivio esterno, selezionare **Specifica posizioni registro archivio esterno**.<br><br>Se i registri di archivio vengono eliminati come parte del backup e sono stati montati manualmente i backup dei registri di archivio richiesti, è necessario specificare il percorso del backup montato come posizione del registro di archivio esterno per il ripristino.<br><br>È necessario verificare il percorso e il contenuto del percorso di montaggio prima di elencarlo come posizione di registro esterno.<br><br>• "Protezione dei dati Oracle con ONTAP"<br>• "L'operazione fallisce con l'errore ORA-00308" |

Non è possibile eseguire il ripristino con recupero da backup secondari se i volumi di registro di archivio non sono protetti ma i volumi di dati lo sono. È possibile effettuare il ripristino solo selezionando **Nessun ripristino**.

Se si sta ripristinando un database RAC con l'opzione di apertura del database selezionata, solo l'istanza RAC in cui è stata avviata l'operazione di ripristino viene riportata allo stato aperto.

Il ripristino non è supportato per i database Data Guard standby e Active Data Guard standby.

8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   È necessario memorizzare i prescript nel percorso */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

9. Nella pagina PostOps, eseguire i seguenti passaggi:

   a. Immettere il percorso e gli argomenti del PostScript che si desidera eseguire dopo l'operazione di ripristino.

      È necessario memorizzare i postscript in */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

      Se l'operazione di ripristino fallisce, i postscript non verranno eseguiti e le attività di pulizia verranno avviate direttamente.

   b. Selezionare la casella di controllo se si desidera aprire il database dopo il ripristino.

      Dopo aver ripristinato un database contenitore (CDB) con o senza file di controllo, oppure dopo aver ripristinato solo i file di controllo CDB, se si specifica di aprire il database dopo il ripristino, verrà aperto solo il CDB e non i database collegabili (PDB) in quel CDB.

      In una configurazione RAC, dopo il ripristino viene aperta solo l'istanza RAC utilizzata per il ripristino.

      Dopo aver ripristinato uno spazio tabella utente con file di controllo, uno spazio tabella di sistema con o senza file di controllo o un PDB con o senza file di controllo, solo lo stato del PDB relativo all'operazione di ripristino viene modificato nello stato originale. Lo stato degli altri PDB non utilizzati per il ripristino non viene riportato allo stato originale perché lo stato di tali PDB non è stato salvato. È necessario modificare manualmente lo stato dei PDB che non sono stati utilizzati per il ripristino.

10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le notifiche e-mail.

    È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di ripristino eseguita, è necessario selezionare **Allega report lavoro**.

    Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Per maggiori informazioni**

- "Il database Oracle RAC One Node viene ignorato per l'esecuzione delle operazioni SnapCenter"
- "Impossibile ripristinare da una posizione secondaria SnapMirror o SnapVault"
- "Impossibile ripristinare da un backup di un'incarnazione orfana"
- "Parametri personalizzabili per le operazioni di backup, ripristino e clonazione sui sistemi AIX"

## Ripristina e recupera gli spazi tabella utilizzando il ripristino point-in-time

È possibile ripristinare un sottoinsieme di tablespace danneggiati o eliminati senza influire sugli altri tablespace nel database. SnapCenter utilizza RMAN per eseguire il ripristino point-in-time (PITR) degli spazi tabella.

### Prima di iniziare

- I backup necessari per eseguire il PITR degli spazi tabella devono essere catalogati e montati.
- Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.

### Informazioni su questo compito

Durante l'operazione PITR, RMAN crea un'istanza ausiliaria nella destinazione ausiliaria specificata. La destinazione ausiliaria potrebbe essere un punto di montaggio o un gruppo di dischi ASM. Se lo spazio nella posizione di montaggio è sufficiente, è possibile riutilizzare una delle posizioni di montaggio anziché un punto di montaggio dedicato.

È necessario specificare la data e l'ora o l'SCN e lo spazio di tabella verrà ripristinato sul database di origine.

È possibile selezionare e ripristinare più tablespace residenti in ambienti ASM, NFS e SAN. Ad esempio, se gli spazi tabella TS2 e TS3 risiedono su NFS e TS4 su SAN, è possibile eseguire una singola operazione PITR per ripristinare tutti gli spazi tabella.

In una configurazione RAC, è possibile eseguire PITR di tablespace da qualsiasi nodo del RAC.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database di tipo istanza singola (multitenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primario o secondario (con mirroring o replica).

   Se il backup non è catalogato, selezionarlo e fare clic su **Catalogo**.

5. Seleziona il backup catalogato, quindi fai clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
   a. Se è stato selezionato un backup di un database in un ambiente Real Application Clusters (RAC), selezionare il nodo RAC.
   b. Selezionare **Tablespace**, quindi specificare i tablespace che si desidera ripristinare.

      Non è possibile eseguire PITR sugli spazi tabella SYSAUX, SYSTEM e UNDO.

c. Selezionare **Modifica stato del database se necessario per il ripristino e il recupero** per modificare lo stato del database nello stato richiesto per eseguire operazioni di ripristino e recupero.

7. Nella pagina Ambito di ripristino, eseguire una delle seguenti azioni:
   - Se si desidera ripristinare un numero di modifica del sistema (SCN) specifico, selezionare **Fino a SCN** e specificare l'SCN e la destinazione ausiliaria.
   - Se si desidera ripristinare una data e un'ora specifiche, selezionare **Data e ora** e specificare la data, l'ora e la destinazione ausiliaria.

     SnapCenter identifica e quindi monta e cataloga il numero ottimale di backup di dati e log necessari per eseguire PITR in base allo SCN specificato o alla data e all'ora selezionate.

8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   Dovresti memorizzare i prescript nel percorso /var/opt/snapcenter/spl/scripts o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso /var/opt/snapcenter/spl/scripts. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

   È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

9. Nella pagina PostOps, eseguire i seguenti passaggi:
   a. Immettere il percorso e gli argomenti del PostScript che si desidera eseguire dopo l'operazione di ripristino.

      Se l'operazione di ripristino fallisce, i postscript non verranno eseguiti e le attività di pulizia verranno avviate direttamente.

   b. Selezionare la casella di controllo se si desidera aprire il database dopo il ripristino.
10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le notifiche e-mail.
11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Ripristina e recupera il database collegabile utilizzando il ripristino point-in-time

È possibile ripristinare e recuperare un database collegabile (PDB) danneggiato o eliminato senza influire sugli altri PDB nel database contenitore (CDB). SnapCenter utilizza RMAN per eseguire il ripristino point-in-time (PITR) del PDB.

### Prima di iniziare

- I backup necessari per eseguire il PITR di un PDB devono essere catalogati e montati.

  In una configurazione RAC, è necessario chiudere manualmente il PDB (modificando lo stato in MOUNTED) su tutti i nodi della configurazione RAC.

- Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.

**Informazioni su questo compito**

Durante l'operazione PITR, RMAN crea un'istanza ausiliaria nella destinazione ausiliaria specificata. La destinazione ausiliaria potrebbe essere un punto di montaggio o un gruppo di dischi ASM. Se lo spazio nella posizione di montaggio è sufficiente, è possibile riutilizzare una delle posizioni di montaggio anziché un punto di montaggio dedicato.

È necessario specificare la data e l'ora o l'SCN per eseguire il PITR del PDB. RMAN può recuperare i PDB in LETTURA/SCRITTURA, SOLA LETTURA o eliminati, inclusi i file di dati.

È possibile ripristinare e recuperare solo:

- un PDB alla volta
- uno spazio di tabella in un PDB
- più tablespace dello stesso PDB

In una configurazione RAC, è possibile eseguire PITR di tablespace da qualsiasi nodo del RAC.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database di tipo istanza singola (multitenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primario o secondario (con mirroring o replica).

   Se il backup non è catalogato, selezionarlo e fare clic su **Catalogo**.

5. Seleziona il backup catalogato, quindi fai clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
   a. Se è stato selezionato un backup di un database in un ambiente Real Application Clusters (RAC), selezionare il nodo RAC.
   b. A seconda che si desideri ripristinare il PDB o gli spazi tabella in un PDB, eseguire una delle seguenti azioni:

| Se lo desidera… | Passi… |
| --- | --- |

| | |
|---|---|
| Ripristinare un PDB | i. Selezionare **Database collegabili (PDB)**.<br>ii. Specificare il PDB che si desidera ripristinare.<br>Non è possibile eseguire PITR sul database PDB$SEED. |
| Ripristinare gli spazi tabella in un PDB | i. Selezionare **Spazi tabella database collegabili (PDB)**.<br>ii. Specificare il PDB.<br>iii. Specificare uno o più tablespace che si desidera ripristinare.<br>Non è possibile eseguire PITR sugli spazi tabella SYSAUX, SYSTEM e UNDO. |

c. Selezionare **Modifica stato del database se necessario per il ripristino e il recupero** per modificare lo stato del database nello stato richiesto per eseguire operazioni di ripristino e recupero.

7. Nella pagina Ambito di ripristino, eseguire una delle seguenti azioni:
   - Se si desidera ripristinare un numero di modifica del sistema (SCN) specifico, selezionare **Fino a SCN** e specificare l'SCN e la destinazione ausiliaria.
   - Se si desidera ripristinare una data e un'ora specifiche, selezionare **Data e ora** e specificare la data, l'ora e la destinazione ausiliaria.

     SnapCenter identifica e quindi monta e cataloga il numero ottimale di backup di dati e log necessari per eseguire PITR in base allo SCN specificato o alla data e all'ora selezionate.

8. Nella pagina PreOps, immettere il percorso e gli argomenti della prescrizione che si desidera eseguire prima dell'operazione di ripristino.

   Dovresti memorizzare i prescript nel percorso /var/opt/snapcenter/spl/scripts o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso /var/opt/snapcenter/spl/scripts. Se hai creato delle cartelle all'interno di questo percorso per archiviare gli script, devi specificare tali cartelle nel percorso.

   È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

9. Nella pagina PostOps, eseguire i seguenti passaggi:
   a. Immettere il percorso e gli argomenti del PostScript che si desidera eseguire dopo l'operazione di ripristino.

      Se l'operazione di ripristino fallisce, i postscript non verranno eseguiti e le attività di pulizia verranno avviate direttamente.

b. Selezionare la casella di controllo se si desidera aprire il database dopo il ripristino.

   In una configurazione RAC, il PDB verrà aperto solo sul nodo in cui è stato recuperato il database. Dovresti aprire manualmente il PDB recuperato su tutti gli altri nodi della configurazione RAC.

10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le notifiche e-mail.
11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Ripristinare e recuperare i database Oracle utilizzando i comandi UNIX

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e recupero e il monitoraggio delle operazioni.

### Informazioni su questo compito

- È necessario eseguire i seguenti comandi per stabilire la connessione con SnapCenter Server, elencare i backup e recuperarne le informazioni, quindi ripristinare il backup.

  Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

### Passi

1. Avvia una sessione di connessione con il server SnapCenter per un utente specificato: *Open-SmConnection*
2. Recupera le informazioni sui backup che desideri ripristinare: *Get-SmBackup*
3. Recupera le informazioni dettagliate sul backup specificato: *Get-SmBackupDetails*

   Questo comando recupera le informazioni dettagliate sul backup di una risorsa specificata con un dato ID di backup. Le informazioni includono il nome del database, la versione, l'home, l'SCN iniziale e finale, gli spazi tabella, i database collegabili e i relativi spazi tabella.

4. Ripristina i dati dal backup: *Restore-SmBackup*

## Monitorare le operazioni di ripristino del database Oracle

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

## Annulla le operazioni di ripristino del database Oracle

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di ripristino in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla processo** è disabilitato per le operazioni di ripristino che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di ripristino in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Seleziona il lavoro e clicca su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di ripristino, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

# Clona il database Oracle

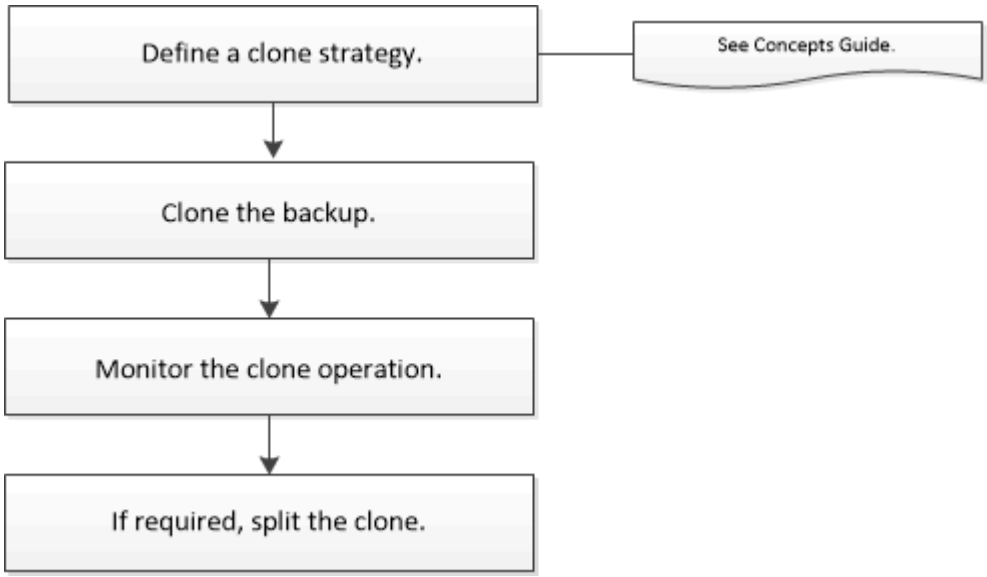
## Flusso di lavoro di clonazione

Il flusso di lavoro della clonazione comprende la pianificazione, l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

È possibile clonare i database per i seguenti motivi:

- Per testare le funzionalità che devono essere implementate utilizzando la struttura e il contenuto del database corrente durante i cicli di sviluppo delle applicazioni.
- Per popolare i data warehouse utilizzando strumenti di estrazione e manipolazione dei dati.
- Per recuperare dati cancellati o modificati per errore.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:



## Definire una strategia di clonazione per i database Oracle

Definire una strategia prima di clonare il database garantisce il successo dell'operazione.

### Tipi di backup supportati per la clonazione

SnapCenter supporta la clonazione di diversi tipi di backup dei database Oracle.

- Backup dei dati online
- Backup completo online
- Backup del montaggio offline
- Backup di arresto offline
- Backup dei database standby di Data Guard e dei database standby di Active Data Guard
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione Real Application Clusters (RAC)
- Backup dei dati online, backup completi online, backup di montaggio offline e backup di arresto offline in una configurazione di gestione automatica dell'archiviazione (ASM)

> Le configurazioni SAN non sono supportate se l'opzione user_friendly_names nel file di configurazione multipath è impostata su yes.

> La clonazione dei backup dei log di archivio non è supportata.

### Tipi di clonazione supportati per i database Oracle

In un ambiente di database Oracle, SnapCenter supporta la clonazione di un backup del database. È possibile clonare il backup dai sistemi di archiviazione primari e secondari.

SnapCenter Server utilizza la tecnologia NetApp FlexClone per clonare i backup.

È possibile aggiornare un clone eseguendo il comando "Refresh-SmClone". Questo comando crea un backup del database, elimina il clone esistente e crea un clone con lo stesso nome.

> L'operazione di aggiornamento del clone può essere eseguita solo utilizzando i comandi UNIX.

### Convenzioni di denominazione dei cloni per i database Oracle

A partire da SnapCenter 3.0, la convenzione di denominazione utilizzata per i cloni dei file system è diversa da quella utilizzata per i cloni dei gruppi di dischi ASM.

- La convenzione di denominazione per i file system SAN o NFS è FileSystemNameofsourcedatabase_CLONESID.
- La convenzione di denominazione per i gruppi di dischi ASM è SC_HASHCODEofDISKGROUP_CLONESID.

  HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ciascun gruppo di dischi ASM.

#### Limitazioni della clonazione dei database Oracle

Prima di clonare i database, è necessario essere consapevoli dei limiti delle operazioni di clonazione.

- Se si utilizza una versione di Oracle dalla 11.2.0.4 alla 12.1.0.1, l'operazione di clonazione sarà bloccata quando si esegue il comando *renamedg*. Per risolvere questo problema, è possibile applicare la patch Oracle 19544733.
- La clonazione di database da una LUN direttamente collegata a un host (ad esempio, utilizzando Microsoft iSCSI Initiator su un host Windows) a un VMDK o a una LUN RDM sullo stesso host Windows o su un altro host Windows, o viceversa, non è supportata.
- La directory radice del punto di montaggio del volume non può essere una directory condivisa.
- Se si sposta una LUN contenente un clone in un nuovo volume, il clone non potrà essere eliminato.

## Variabili di ambiente predefinite per prescript e postscript specifici del clone

SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript durante la clonazione di un database.

#### Variabili di ambiente predefinite supportate per la clonazione di un database

- **SC_ORIGINAL_SID** specifica il SID del database di origine.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: NFSB32

- **SC_ORIGINAL_HOST** specifica il nome dell'host di origine.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: asmrac1.gdl.englab.netapp.com

- **SC_ORACLE_HOME** specifica il percorso della directory home Oracle del database di destinazione.

  Esempio: /ora01/app/oracle/product/18.1.0/db_1

- **SC_BACKUP_NAME**" specifica il nome del backup.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempi:

  - Se il database non è in esecuzione in modalità ARCHIVELOG: DATA@RG2_scspr2417819002_07-20-2021_12.16.48.9267_0|LOG@RG2_scspr2417819002_07-20-2021_12.16.48.9267_1
  - Se il database è in esecuzione in modalità ARCHIVELOG: 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_1

- **SC_AV_NAME** specifica i nomi dei volumi dell'applicazione.

  Esempio: AV1|AV2

- **SC_ORIGINAL_OS_USER** specifica il proprietario del sistema operativo del database di origine.

  Esempio: oracolo

- **SC_ORIGINAL_OS_GROUP** specifica il gruppo del sistema operativo del database di origine.

  Esempio: oinstall

- **SC_TARGET_SID**" specifica il SID del database clonato.

  Per il flusso di lavoro di clonazione PDB, il valore di questo parametro non sarà predefinito.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: clonedb

- **SC_TARGET_HOST** specifica il nome dell'host in cui verrà clonato il database.

  Questo parametro verrà popolato per i volumi dell'applicazione.

  Esempio: asmrac1.gdl.englab.netapp.com

- **SC_TARGET_OS_USER** specifica il proprietario del sistema operativo del database clonato.

  Per il flusso di lavoro di clonazione PDB, il valore di questo parametro non sarà predefinito.

  Esempio: oracolo

- **SC_TARGET_OS_GROUP** specifica il gruppo del sistema operativo del database clonato.

  Per il flusso di lavoro di clonazione PDB, il valore di questo parametro non sarà predefinito.

  Esempio: oinstall

- **SC_TARGET_DB_PORT** specifica la porta del database clonato.

  Per il flusso di lavoro di clonazione PDB, il valore di questo parametro non sarà predefinito.

  Esempio: 1521

Per informazioni sui delimitatori, vedere"Delimitatori supportati" .

## Requisiti per la clonazione di un database Oracle

Prima di clonare un database Oracle, è necessario assicurarsi che i prerequisiti siano stati completati.

- Avresti dovuto creare un backup del database utilizzando SnapCenter.

  Per far sì che l'operazione di clonazione vada a buon fine, è necessario aver creato correttamente backup dei dati e dei log online oppure backup offline (montaggio o arresto).

- Se si desidera personalizzare i percorsi del file di controllo o del file di registro redo, è necessario aver predisposto il file system richiesto o il gruppo di dischi Automatic Storage Management (ASM).

Per impostazione predefinita, i file di controllo e di redo log del database clonato vengono creati sul gruppo di dischi ASM o sul file system fornito da SnapCenter per i file di dati del database clone.

- Se si utilizza ASM su NFS, è necessario aggiungere */var/opt/snapcenter/scu/clones/*/** al percorso esistente definito nel parametro asm_diskstring.
- Nel parametro asm_diskstring, dovresti configurare *AFD:** se stai utilizzando ASMFD o configurare *ORCL:** se stai utilizzando ASMLIB.

  Per informazioni su come modificare il parametro asm_diskstring, vedere "Come aggiungere percorsi disco a asm_diskstring" .

- Se si crea il clone su un host alternativo, quest'ultimo deve soddisfare i seguenti requisiti:
  - Il plug-in SnapCenter per Oracle Database deve essere installato sull'host alternativo.
  - L'host clone dovrebbe essere in grado di rilevare le LUN dall'archiviazione primaria o secondaria.
    - Se si esegue la clonazione da un archivio primario o secondario (Vault o Mirror) a un host alternativo, assicurarsi che sia stabilita una sessione iSCSI tra l'archivio secondario e l'host alternativo oppure che sia suddivisa in zone appropriate per FC.
    - Se si esegue la clonazione da un archivio Vault o Mirror sullo stesso host, assicurarsi che sia stata stabilita una sessione iSCSI tra l'archivio Vault o Mirror e l'host oppure che sia stata suddivisa in zone appropriate per FC.
    - Se si esegue la clonazione in un ambiente virtualizzato, assicurarsi che sia stabilita una sessione iSCSI tra l'archiviazione primaria o secondaria e il server ESX che ospita l'host alternativo oppure che sia suddivisa in zone appropriate per FC.

      Per informazioni, fare riferimento a "documentazione delle utilità host" .

  - Se il database di origine è un database ASM:
    - L'istanza ASM deve essere attiva e funzionante sull'host in cui verrà eseguita la clonazione.
    - Se si desidera posizionare i file di registro di archivio del database clonato in un gruppo di dischi ASM dedicato, è necessario predisporre il gruppo di dischi ASM prima dell'operazione di clonazione.
    - È possibile configurare il nome del gruppo di dischi dati, ma assicurarsi che il nome non sia utilizzato da nessun altro gruppo di dischi ASM sull'host in cui verrà eseguita la clonazione.

      I file di dati residenti sul gruppo di dischi ASM vengono forniti come parte del flusso di lavoro di clonazione SnapCenter .

  - Per NVMe, è necessario installare NVMe util
- Il tipo di protezione per la LUN dei dati e la LUN del registro, ad esempio mirror, vault o mirror-vault, deve essere lo stesso per individuare i localizzatori secondari durante la clonazione su un host alternativo mediante backup del registro.
- È necessario impostare il valore di exclude_seed_cdb_view su FALSE nel file dei parametri del database di origine per recuperare le informazioni relative al seed PDB per la clonazione di un backup del database 12_c_.

  Il seed PDB è un modello fornito dal sistema che il CDB può utilizzare per creare i PDB. Il seed PDB è denominato PDB$SEED. Per informazioni su PDB$SEED, vedere Oracle Doc ID 1940806.1.

  È necessario impostare il valore prima di eseguire il backup del database 12_c_.

- SnapCenter supporta il backup dei file system gestiti dal sottosistema autofs. Se si sta clonando il database, assicurarsi che i punti di montaggio dei dati non si trovino nella radice del punto di montaggio autofs, perché l'utente root dell'host del plug-in non ha l'autorizzazione per creare directory nella radice del punto di montaggio autofs.

  Se i file di controllo e di redo log si trovano nel punto di montaggio dei dati, è necessario modificare il percorso del file di controllo e quindi il percorso del file di redo log di conseguenza.

  ⓘ È possibile registrare manualmente i nuovi punti di montaggio clonati con il sottosistema autofs. I nuovi punti di montaggio clonati non verranno registrati automaticamente.

- Se si dispone di un TDE (accesso automatico) e si desidera clonare il database sullo stesso host o su uno alternativo, è necessario copiare il portafoglio (file chiave) in */etc/ORACLE/WALLET/$ORACLE_SID* dal database di origine al database clonato.
- È necessario impostare il valore di use_lvmetad = 0 in */etc/lvm/lvm.conf* e arrestare il servizio lvm2-lvmetad per eseguire correttamente la clonazione in ambienti SAN (Storage Area Network) su Oracle Linux 7 o versioni successive o Red Hat Enterprise Linux (RHEL) 7 o versioni successive.
- Se si utilizza il database Oracle 11.2.0.3 o versione successiva e l'ID del database per l'istanza ausiliaria viene modificato tramite uno script NID, è necessario installare la patch Oracle 13366202.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Per NVMe, se una porta di destinazione deve essere esclusa dalla connessione, è necessario aggiungere il nome del nodo di destinazione e il nome della porta nel file /var/opt/snapcenter/scu/etc/nvme.conf.

  Se il file non esiste, dovresti crearlo come mostrato nell'esempio seguente:

  ```
  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>
  }
  ```

- È necessario assicurarsi che la LUN non sia mappata sull'host AIX utilizzando iGroup costituito da protocolli misti iSCSI e FC. Per ulteriori informazioni, vedere "L'operazione fallisce con errore Impossibile rilevare il dispositivo per LUN" .

## Clonare un backup del database Oracle

È possibile utilizzare SnapCenter per clonare un database Oracle utilizzando il backup del database.

### Prima di iniziare

Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.

### Informazioni su questo compito

- L'operazione di clonazione crea una copia dei file di dati del database e crea nuovi file di redo log online e file di controllo. Facoltativamente, è possibile ripristinare il database a un orario specificato, in base alle

opzioni di ripristino specificate.

> La clonazione non riesce se si tenta di clonare un backup creato su un host Linux su un host AIX o viceversa.

SnapCenter crea un database autonomo quando viene clonato da un backup del database Oracle RAC. SnapCenter supporta la creazione di cloni dal backup di un database standby di Data Guard e di un database standby di Active Data Guard.

Durante la clonazione, SnapCenter monta il numero ottimale di backup del log in base a SCN o data e ora per le operazioni di ripristino. Dopo il ripristino, il backup del registro viene smontato. Tutti questi cloni vengono montati in */var/opt/snapcenter/scu/clones/*. Se si utilizza ASM su NFS, è necessario aggiungere */var/opt/snapcenter/scu/clones/*/** al percorso esistente definito nel parametro asm_diskstring.

Durante la clonazione di un backup di un database ASM in un ambiente SAN, le regole udev per i dispositivi host clonati vengono create in */etc/udev/rules.d/999-scu-netapp.rules*. Le regole udev associate ai dispositivi host clonati vengono eliminate quando si elimina il clone.

> In una configurazione Flex ASM, non è possibile eseguire operazioni di clonazione sui nodi Leaf se la cardinalità è inferiore al numero di nodi nel cluster RAC.

- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Gestisci copie, seleziona i backup tra Copie locali (primarie), Copie mirror (secondarie) o Copie vault (secondarie).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su * *.
6. Nella pagina Nome, eseguire una delle seguenti azioni:

| Se lo desidera… | Passi… |
| --- | --- |
| Clonare un database (CDB o non CDB) | a. Specificare il SID del clone.<br><br>Il SID clone non è disponibile per impostazione predefinita e la lunghezza massima del SID è di 8 caratteri.<br><br>È necessario assicurarsi che non esista alcun database con lo stesso SID sull'host in cui verrà creato il clone. |
| Clonare un database collegabile (PDB) | a. Selezionare **Clona PDB**.<br>b. Specificare il PDB che si desidera clonare.<br>c. Specificare il nome del PDB clonato. Per i passaggi dettagliati per clonare un PDB, vedere"Clonare un database collegabile" . |

Quando selezioni dati mirrorati o vault:

- se non sono presenti backup del log nel mirror o nel vault, non viene selezionato nulla e i localizzatori sono vuoti.
- se i backup del log sono presenti nel mirror o nel vault, viene selezionato l'ultimo backup del log e viene visualizzato il localizzatore corrispondente.

Se il backup del log selezionato esiste sia nella posizione mirror che in quella vault, vengono visualizzati entrambi i localizzatori.

7. Nella pagina Posizioni, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Clone host | Per impostazione predefinita, viene popolato l'host del database di origine.<br><br>Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e sistema operativo dell'host del database di origine. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Posizioni dei file di dati | Per impostazione predefinita, il percorso del file di dati è popolato.<br><br>La convenzione di denominazione predefinita di SnapCenter per i file system SAN o NFS è FileSystemNameofsourcedatabase_CLONESID.<br><br>La convenzione di denominazione predefinita SnapCenter per i gruppi di dischi ASM è SC_HASHCODEofDISKGROUP_CLONESID. HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ogni gruppo di dischi ASM.<br><br>Se si personalizza il nome del gruppo di dischi ASM, assicurarsi che la lunghezza del nome rispetti la lunghezza massima supportata da Oracle.<br><br>Se si desidera specificare un percorso diverso, è necessario immettere i punti di montaggio del file di dati o i nomi dei gruppi di dischi ASM per il database clone. Quando si personalizza il percorso del file di dati, è necessario modificare anche i nomi dei gruppi di dischi ASM o del file system del file di controllo e del file di registro redo con lo stesso nome utilizzato per i file di dati oppure con un gruppo di dischi ASM o un file system esistente. |

| Per questo campo… | Fai questo… |
| --- | --- |
| File di controllo | Per impostazione predefinita, il percorso del file di controllo è compilato.<br><br>I file di controllo vengono posizionati nello stesso gruppo di dischi ASM o file system dei file di dati. Se si desidera sovrascrivere il percorso del file di controllo, è possibile specificare un percorso diverso.<br><br>Il file system o il gruppo di dischi ASM devono essere presenti sull'host.<br><br>Per impostazione predefinita, il numero di file di controllo sarà uguale a quello del database di origine. È possibile modificare il numero di file di controllo, ma per clonare il database è necessario almeno un file di controllo.<br><br>È possibile personalizzare il percorso del file di controllo su un file system diverso (esistente) rispetto a quello del database di origine. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Redo log | Per impostazione predefinita, vengono popolati il gruppo di file del redo log, il percorso e le relative dimensioni.<br><br>I redo log vengono inseriti nello stesso gruppo di dischi ASM o file system dei file di dati del database clonato. Se si desidera sovrascrivere il percorso del file redo log, è possibile personalizzare il percorso del file redo log impostandolo su un file system diverso da quello del database di origine.<br><br>Il nuovo file system o il gruppo di dischi ASM dovrebbe essere presente sull'host.<br><br>Per impostazione predefinita, il numero di gruppi di redo log, di file di redo log e le relative dimensioni saranno gli stessi del database di origine. È possibile modificare i seguenti parametri:<br><br>• Numero di gruppi di redo log<br><br>Per clonare il database sono necessari almeno due gruppi di redo log.<br><br>• Redo log dei file in ogni gruppo e il loro percorso<br><br>È possibile personalizzare il percorso del file del redo log su un file system diverso (esistente) rispetto a quello del database di origine.<br><br>Per clonare il database è necessario almeno un file redo log nel gruppo redo log.<br><br>• Dimensioni del file redo log |

8. Nella pagina Credenziali, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome delle credenziali per l'utente sys | Selezionare le credenziali da utilizzare per definire la password dell'utente di sistema del database clone.<br><br>Se SQLNET.AUTHENTICATION_SERVICES è impostato su NONE nel file sqlnet.ora sull'host di destinazione, non selezionare **None** come Credenziale nell'interfaccia utente grafica SnapCenter . |
| Nome delle credenziali dell'istanza ASM | Selezionare **Nessuno** se l'autenticazione del sistema operativo è abilitata per la connessione all'istanza ASM sull'host clone.<br><br>In caso contrario, selezionare le credenziali Oracle ASM configurate con l'utente "sys" o un utente con privilegio "sysasm" applicabile all'host clone. |

I dettagli relativi alla home page di Oracle, al nome utente e al gruppo vengono automaticamente inseriti dal database di origine. È possibile modificare i valori in base all'ambiente Oracle dell'host in cui verrà creato il clone.

9. Nella pagina PreOps, eseguire i seguenti passaggi:

   a. Immettere il percorso e gli argomenti del prescript che si desidera eseguire prima dell'operazione di clonazione.

      È necessario memorizzare la prescrizione in */var/opt/snapcenter/spl/scripts* o in una qualsiasi cartella all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai inserito lo script in una cartella all'interno di questo percorso, devi fornire il percorso completo fino alla cartella in cui è inserito lo script.

      SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

   b. Nella sezione Impostazioni parametri database, modificare i valori dei parametri del database precompilati utilizzati per inizializzare il database.

      Puoi aggiungere parametri aggiuntivi cliccando * + *.

      Se si utilizza Oracle Standard Edition e il database è in esecuzione in modalità di registro di archivio o si desidera ripristinare un database dal registro di ripristino dell'archivio, aggiungere i parametri e specificare il percorso.

      - LOG_ARCHIVE_DEST
      - LOG_ARCHIVE_DUPLEX_DEST

      > ⓘ L'area di ripristino rapido (FRA) non è definita nei parametri del database precompilati. È possibile configurare FRA aggiungendo i parametri correlati.

Il valore predefinito di log_archive_dest_1 è $ORACLE_HOME/clone_sid e i log di archivio del database clonato verranno creati in questa posizione. Se è stato eliminato il parametro log_archive_dest_1, la posizione del log di archivio viene determinata da Oracle. È possibile definire una nuova posizione per il registro di archivio modificando log_archive_dest_1, ma assicurarsi che il file system o il gruppo di dischi sia esistente e reso disponibile sull'host.

a. Fare clic su **Reimposta** per ripristinare le impostazioni predefinite dei parametri del database.

10. Nella pagina PostOps, **Recupera database** e **Fino all'annullamento** sono selezionati per impostazione predefinita per eseguire il ripristino del database clonato.

    SnapCenter esegue il ripristino montando l'ultimo backup del registro che presenta la sequenza ininterrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione. Il backup dei dati e del registro deve essere eseguito sullo storage primario per eseguire la clonazione sullo storage primario, mentre il backup dei dati e del registro deve essere eseguito sullo storage secondario per eseguire la clonazione sullo storage secondario.

    Le opzioni **Recupera database** e **Fino all'annullamento** non sono selezionate se SnapCenter non riesce a trovare i backup del registro appropriati. È possibile specificare la posizione del registro di archivio esterno se il backup del registro non è disponibile in **Specificare le posizioni del registro di archivio esterno**. È possibile specificare più posizioni di registro.

    Se si desidera clonare un database di origine configurato per supportare Flash Recovery Area (FRA) e Oracle Managed Files (OMF), anche la destinazione del log per il ripristino deve rispettare la struttura di directory OMF.

    La pagina PostOps non viene visualizzata se il database di origine è un database standby di Data Guard o un database standby di Active Data Guard. Per un database Data Guard standby o Active Data Guard standby, SnapCenter non fornisce un'opzione per selezionare il tipo di ripristino nell'interfaccia utente grafica SnapCenter , ma il database viene ripristinato utilizzando il tipo di ripristino Fino all'annullamento senza applicare alcun registro.

| Nome del campo | Descrizione |
|---|---|
| Fino a quando non verrà annullato | SnapCenter esegue il ripristino montando l'ultimo backup del registro contenente la sequenza ininterrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione. Il database clonato viene recuperato fino al file di registro mancante o danneggiato. |
| Data e ora | SnapCenter recupera il database fino a una data e un'ora specificate. Il formato accettato è mm/gg/aaaa hh:mm:ss.<br>L'ora può essere specificata nel formato 24 ore. |
| Fino a SCN (numero di modifica del sistema) | SnapCenter recupera il database fino a un numero di modifica del sistema (SCN) specificato. |

| Nome del campo | Descrizione |
| --- | --- |
| Specificare le posizioni dei registri di archivio esterni | Se il database è in esecuzione in modalità ARCHIVELOG, SnapCenter identifica e monta il numero ottimale di backup del log in base all'SCN specificato o alla data e all'ora selezionate.<br><br>È anche possibile specificare la posizione del registro di archivio esterno.<br><br>SnapCenter non identificherà e monterà automaticamente i backup del registro se hai selezionato Fino all'annullamento. |
| Crea un nuovo DBID | Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** è selezionata per generare un numero univoco (DBID) per il database clonato, differenziandolo dal database di origine.<br><br>Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui è già registrato il database di origine, l'operazione fallisce. |
| Crea un file temporaneo per lo spazio tabella temporaneo | Selezionare la casella di controllo se si desidera creare un file temporaneo per lo spazio tabella temporaneo predefinito del database clonato.<br><br>Se la casella di controllo non è selezionata, il clone del database verrà creato senza il file temporaneo. |
| Inserisci le voci SQL da applicare quando viene creato il clone | Aggiungere le voci SQL che si desidera applicare quando viene creato il clone. |

| Nome del campo | Descrizione |
| --- | --- |
| Inserisci gli script da eseguire dopo l'operazione di clonazione | Specificare il percorso e gli argomenti del PostScript che si desidera eseguire dopo l'operazione di clonazione.<br><br>Dovresti memorizzare il postscript in */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*.<br><br>Se hai inserito lo script in una cartella all'interno di questo percorso, devi fornire il percorso completo fino alla cartella in cui è inserito lo script.<br><br>Se l'operazione di clonazione fallisce, i postscript non verranno eseguiti e le attività di pulizia verranno attivate direttamente. |

11. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

    È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

    Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

12. Rivedi il riepilogo e poi clicca su **Fine**.

    Durante l'esecuzione del ripristino come parte dell'operazione di creazione del clone, anche se il ripristino fallisce, il clone viene creato con un avviso. È possibile eseguire il ripristino manuale su questo clone per riportare il database del clone a uno stato coerente.

13. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Risultato**

Dopo aver clonato il database, puoi aggiornare la pagina delle risorse per elencare il database clonato come una delle risorse disponibili per il backup. Il database clonato può essere protetto come qualsiasi altro database utilizzando il flusso di lavoro di backup standard oppure può essere incluso in un gruppo di risorse (di nuova creazione o esistente). Il database clonato può essere ulteriormente clonato (clone di cloni).

Dopo la clonazione, non dovresti mai rinominare il database clonato.

Se non è stato eseguito il ripristino durante la clonazione, il backup del database clonato potrebbe non riuscire a causa di un ripristino non corretto e potrebbe essere necessario eseguire un ripristino manuale. Il backup del registro potrebbe non riuscire anche se la posizione predefinita popolata per i registri di archivio si trova su un archivio non NetApp o se il sistema di archiviazione non è configurato con SnapCenter.

Nella configurazione di AIX, è possibile utilizzare il comando lkdev per bloccare e il comando rendev per rinominare i dischi su cui risiedeva il database clonato.

Il blocco o la ridenominazione dei dispositivi non influirà sull'operazione di eliminazione del clone. Per i layout AIX LVM creati su dispositivi SAN, la ridenominazione dei dispositivi non sarà supportata per i dispositivi SAN clonati.

**Trova maggiori informazioni**

- "Il ripristino o la clonazione falliscono con il messaggio di errore ORA-00308"
- "Impossibile recuperare un database clonato"
- "Parametri personalizzabili per le operazioni di backup, ripristino e clonazione sui sistemi AIX"

**Aggiorna l'IP preferito sull'host**

Una volta completata l'operazione di clonazione, il percorso fornito dal SAL (Storage Access Layer) al clone sarà nel formato *<nfs_lif_IP>:<JunctionPath>*. Per fornire l'IP preferito, è necessario configurarlo sull'host utilizzando i comandi SCCLI.

**Passi**

1. Accedi all'host del database.
2. Avvia una sessione di connessione PowerShell con SnapCenter per un utente specificato.

   Open-SmConnection

3. Crea un file vuoto.

   tocca /var/opt/snapcenter/scu/etc/storagepreference.properties

4. Configurare il LIF dati preferito per l'SVM.

   Add-SvmPreferredDataPath -SVM <Nome SVM> -DataPath <Indirizzo IP o FQDN>

5. Verificare il percorso preferito.

   Ottieni-SvmPreferredDataPath

## Clonare un database collegabile

È possibile clonare un database collegabile (PDB) su un CDB di destinazione diverso o uguale sullo stesso host o su un host alternativo. È anche possibile ripristinare il PDB clonato in un SCN o in una data e ora desiderati.

**Prima di iniziare**

Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione alle directory prescript e postscript.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.

2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database di tipo istanza singola (multitenant) dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del database.

4. Dalla vista Gestisci copie, seleziona i backup tra Copie locali (primarie), Copie mirror (secondarie) o Copie vault (secondarie).
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Nome, eseguire le seguenti azioni:
   a. Selezionare **Clona PDB**.
   b. Specificare il PDB che si desidera clonare.

      È possibile clonare solo un PDB alla volta.

   c. Specificare il nome del PDB clone.
7. Nella pagina Posizioni, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Clone host | Per impostazione predefinita, viene popolato l'host del database di origine.<br><br>Se si desidera creare il clone su un host alternativo, selezionare l'host con la stessa versione di Oracle e sistema operativo dell'host del database di origine. |
| Obiettivo CDB | Selezionare il CDB in cui si desidera includere il PDB clonato.<br><br>È necessario assicurarsi che il CDB di destinazione sia in esecuzione. |
| Stato del database | Selezionare la casella di controllo **Apri il PDB clonato in modalità LETTURA-SCRITTURA** se si desidera aprire il PDB in modalità LETTURA-SCRITTURA. |

| | |
|---|---|
| Posizioni dei file di dati | Per impostazione predefinita, il percorso del file di dati è popolato.<br><br>La convenzione di denominazione predefinita di SnapCenter per i file system SAN o NFS è FileSystemNameofsourcedatabase_SCJOBID.<br><br>La convenzione di denominazione predefinita SnapCenter per i gruppi di dischi ASM è SC_HASHCODEofDISKGROUP_SCJOBID. HASHCODEofDISKGROUP è un numero generato automaticamente (da 2 a 10 cifre) univoco per ogni gruppo di dischi ASM.<br><br>Se si personalizza il nome del gruppo di dischi ASM, assicurarsi che la lunghezza del nome rispetti la lunghezza massima supportata da Oracle.<br><br>Se si desidera specificare un percorso diverso, è necessario immettere i punti di montaggio del file di dati o i nomi dei gruppi di dischi ASM per il database clone. |

I dettagli relativi alla home page di Oracle, al nome utente e al gruppo vengono automaticamente inseriti dal database di origine. È possibile modificare i valori in base all'ambiente Oracle dell'host in cui verrà creato il clone.

8. Nella pagina PreOps, eseguire i seguenti passaggi:

   a. Immettere il percorso e gli argomenti del prescript che si desidera eseguire prima dell'operazione di clonazione.

      Dovresti memorizzare il prescript in /var/opt/snapcenter/spl/scripts o in una cartella qualsiasi all'interno di questo percorso. Per impostazione predefinita, viene compilato il percorso /var/opt/snapcenter/spl/scripts. Se hai inserito lo script in una cartella all'interno di questo percorso, devi fornire il percorso completo fino alla cartella in cui è inserito lo script.

   SnapCenter consente di utilizzare le variabili di ambiente predefinite quando si eseguono prescript e postscript."Saperne di più"

   a. Nella sezione Impostazioni parametri database clone CDB ausiliario, modificare i valori dei parametri database precompilati utilizzati per inizializzare il database.

9. Fare clic su **Reimposta** per ripristinare le impostazioni predefinite dei parametri del database.
10. Nella pagina PostOps, **Fino all'annullamento** è selezionato per impostazione predefinita per eseguire il ripristino del database clonato.

    L'opzione **Fino all'annullamento** non è selezionata se SnapCenter non riesce a trovare i backup del registro appropriati. È possibile specificare la posizione del registro di archivio esterno se il backup del registro non è disponibile in **Specificare le posizioni del registro di archivio esterno**. È possibile specificare più posizioni di registro.

Se si desidera clonare un database di origine configurato per supportare Flash Recovery Area (FRA) e Oracle Managed Files (OMF), anche la destinazione del log per il ripristino deve rispettare la struttura di directory OMF.

| Nome del campo | Descrizione |
|---|---|
| Fino a quando non verrà annullato | SnapCenter esegue il ripristino montando l'ultimo backup del registro contenente la sequenza ininterrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione.<br><br>Il backup dei dati e del registro deve essere eseguito sullo storage primario per eseguire la clonazione sullo storage primario, mentre il backup dei dati e del registro deve essere eseguito sullo storage secondario per eseguire la clonazione sullo storage secondario. Il database clonato viene recuperato fino al file di registro mancante o danneggiato. |
| Data e ora | SnapCenter recupera il database fino a una data e un'ora specificate.<br><br>L'ora può essere specificata nel formato 24 ore. |
| Fino a SCN (numero di modifica del sistema) | SnapCenter recupera il database fino a un numero di modifica del sistema (SCN) specificato. |
| Specificare le posizioni dei registri di archivio esterni | Specificare la posizione del registro di archivio esterno. |
| Crea un nuovo DBID | Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** non è selezionata per il database clone ausiliario.<br><br>Selezionare la casella di controllo se si desidera generare un numero univoco (DBID) per il database clonato ausiliario, differenziandolo dal database di origine. |
| Crea un file temporaneo per lo spazio tabella temporaneo | Selezionare la casella di controllo se si desidera creare un file temporaneo per lo spazio tabella temporaneo predefinito del database clonato.<br><br>Se la casella di controllo non è selezionata, il clone del database verrà creato senza il file temporaneo. |
| Inserisci le voci SQL da applicare quando viene creato il clone | Aggiungere le voci SQL che si desidera applicare quando viene creato il clone. |

| Nome del campo | Descrizione |
| --- | --- |
| Inserisci gli script da eseguire dopo l'operazione di clonazione | Specificare il percorso e gli argomenti del PostScript che si desidera eseguire dopo l'operazione di clonazione.<br><br>Dovresti memorizzare il postscript in */var/opt/snapcenter/spl/scripts* o in una cartella qualsiasi all'interno di questo percorso.<br><br>Per impostazione predefinita, viene compilato il percorso */var/opt/snapcenter/spl/scripts*. Se hai inserito lo script in una cartella all'interno di questo percorso, devi fornire il percorso completo fino alla cartella in cui è inserito lo script.<br><br>Se l'operazione di clonazione fallisce, i postscript non verranno eseguiti e le attività di pulizia verranno attivate direttamente. |

11. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

    È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

    Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

12. Rivedi il riepilogo e poi clicca su **Fine**.
13. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Dopo aver finito**

Se si desidera creare un backup del PDB clonato, è necessario eseguire il backup del CDB di destinazione in cui è clonato il PDB, poiché non è possibile eseguire il backup solo del PDB clonato. Se si desidera creare il backup con una relazione secondaria, è necessario creare una relazione secondaria per il CDB di destinazione.

In una configurazione RAC, l'archiviazione per il PDB clonato è collegata solo al nodo in cui è stata eseguita la clonazione del PDB. I PDB sugli altri nodi del RAC sono nello stato MOUNT. Se si desidera che il PDB clonato sia accessibile dagli altri nodi, è necessario collegare manualmente lo storage agli altri nodi.

**Trova maggiori informazioni**

- "Il ripristino o la clonazione falliscono con il messaggio di errore ORA-00308"
- "Parametri personalizzabili per le operazioni di backup, ripristino e clonazione sui sistemi AIX"

## Clonare i backup del database Oracle utilizzando i comandi UNIX

Il flusso di lavoro della clonazione comprende la pianificazione, l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

### Informazioni su questo compito

È necessario eseguire i seguenti comandi per creare il file di specifica del clone del database Oracle e avviare l'operazione di clonazione.

Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

### Passi

1. Crea una specifica di clone del database Oracle da un backup specificato: *New-SmOracleCloneSpecification*

   Se il criterio di protezione dei dati secondari è mirror-vault unificato, specificare solo -IncludeSecondaryDetails. Non è necessario specificare -SecondaryStorageType.

   Questo comando crea automaticamente un file di specifica del clone del database Oracle per il database di origine specificato e il relativo backup. È inoltre necessario fornire un SID del database clone in modo che il file di specifiche creato contenga i valori generati automaticamente per il database clone che verrà creato.

   Il file di specifica del clone viene creato in */var/opt/snapcenter/sco/clone_specs*.

2. Avvia un'operazione di clonazione da un gruppo di risorse di clonazione o da un backup esistente: *New-SmClone*

   Questo comando avvia un'operazione di clonazione. È inoltre necessario fornire un percorso del file di specifica del clone Oracle per l'operazione di clonazione. È inoltre possibile specificare le opzioni di ripristino, l'host su cui eseguire l'operazione di clonazione, i prescript, i postscript e altri dettagli.

   Per impostazione predefinita, il file di destinazione del registro di archivio per il database clone viene automaticamente popolato in *$ORACLE_HOME/CLONE_SIDs*.

## Dividi un clone di database Oracle

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

### Informazioni su questo compito

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup del clone vengono eliminate.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere,https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividere un volume FlexClone dal suo volume padre"]
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.
3. Selezionare la risorsa clonata (ad esempio, il database o il LUN) e quindi fare clic su .
4. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato e i database su cui è stata eseguita l'operazione di suddivisione del clone sono elencati come cloni nella pagina Risorse. È necessario eseguire il cmdlet *Stop-SmJob* per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro CloneSplitStatusCheckPollTime nel file SMCoreServiceHost.exe.config per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio,

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

> L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

## Clone diviso di un database collegabile

È possibile utilizzare SnapCenter per dividere un database collegabile clonato (PDB).

**Informazioni su questo compito**

Se hai creato un backup del CDB di destinazione in cui è clonato il PDB, quando dividi il clone del PDB, il PDB clonato viene rimosso anche da tutti i backup del CDB di destinazione contenenti il PDB clonato.

> I cloni PDB non vengono visualizzati nella vista inventario o risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Selezionare il database del contenitore di origine (CDB) dalla vista delle risorse o dei gruppi di risorse.
3. Dalla vista Gestisci copie, seleziona **Cloni** dai sistemi di archiviazione primari o secondari (con mirroring o replica).
4. Selezionare il clone PDB (targetCDB:PDBClone) e quindi fare clic su .
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di clonazione del database Oracle

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Aggiorna un clone

È possibile aggiornare il clone eseguendo il comando *Refresh-SmClone*. Questo comando crea un backup del database, elimina il clone esistente e crea un clone con lo stesso nome.

Non è possibile aggiornare un clone PDB.

**Cosa ti servirà**

- Crea un backup completo online o un criterio di backup dei dati offline senza abilitare backup pianificati.
- Configurare la notifica e-mail nel criterio solo per gli errori di backup.
- Definire in modo appropriato il conteggio di conservazione per i backup su richiesta per garantire che non vi siano backup indesiderati.
- Assicurarsi che solo un backup completo online o un criterio di backup dei dati offline sia associato al gruppo di risorse identificato per l'operazione di clonazione di aggiornamento.
- Creare un gruppo di risorse con un solo database.
- Se viene creato un cron job per il comando clone refresh, assicurarsi che le pianificazioni SnapCenter e le pianificazioni cron non si sovrappongano per il gruppo di risorse del database.

  Per un cron job creato per il comando clone refresh, assicurarsi di eseguire Open-SmConnection ogni 24 ore.

- Assicurarsi che il SID del clone sia univoco per un host.

  Se più operazioni di clonazione di aggiornamento utilizzano lo stesso file di specifica del clone o utilizzano il file di specifica del clone con lo stesso SID del clone, il clone esistente con lo stesso SID sull'host verrà eliminato e quindi verrà creato il clone.

- Assicurarsi che il criterio di backup sia abilitato con protezione secondaria e che il file di specifica del clone sia creato con "-IncludeSecondaryDetails" per creare i cloni utilizzando backup secondari.
  - Se viene specificato il file di specifica del clone primario ma il criterio ha selezionato l'opzione di aggiornamento secondario, il backup verrà creato e l'aggiornamento verrà trasferito al secondario. Tuttavia, il clone verrà creato dal backup primario.
  - Se viene specificato il file di specifica del clone primario e il criterio non ha selezionato l'opzione di aggiornamento secondario, il backup verrà creato sul primario e il clone verrà creato dal primario.

**Passi**

1. Avvia una sessione di connessione con il server SnapCenter per un utente specificato: *Open-SmConnection*
2. Crea una specifica di clone del database Oracle da un backup specificato: *New-SmOracleCloneSpecification*

   Se il criterio di protezione dei dati secondari è mirror-vault unificato, specificare solo -IncludeSecondaryDetails. Non è necessario specificare -SecondaryStorageType.

   Questo comando crea automaticamente un file di specifica del clone del database Oracle per il database di origine specificato e il relativo backup. È inoltre necessario fornire un SID del database clone in modo che il file di specifiche creato contenga i valori generati automaticamente per il database clone che verrà

creato.

Il file di specifica del clone viene creato in */var/opt/snapcenter/sco/clone_specs*.

3. Eseguire *Refresh-SmClone*.

   Se l'operazione fallisce con il messaggio di errore "PL-SCO-20032: operazione canExecute non riuscita con errore: PL-SCO-30031: il file di registro redo +SC_2959770772_clmdb/clmdb/redolog/redo01_01.log esiste", specificare un valore più alto per *-WaitToTriggerClone*.

   Per informazioni dettagliate sui comandi UNIX, vedere "Guida di riferimento ai comandi del software SnapCenter" .

### Elimina il clone di un database collegabile

È possibile eliminare il clone di un database collegabile (PDB) se non ne hai più bisogno.

Se hai creato un backup del CDB di destinazione in cui è clonato il PDB, quando elimini il clone del PDB, anche il PDB clonato viene rimosso dal backup del CDB di destinazione.

I cloni PDB non vengono visualizzati nella vista inventario o risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Selezionare il database del contenitore di origine (CDB) dalla vista delle risorse o dei gruppi di risorse.
3. Dalla vista Gestisci copie, seleziona **Cloni** dai sistemi di archiviazione primari o secondari (con mirroring o replica).
4. Selezionare il clone PDB (targetCDB:PDBClone) e quindi fare clic su .
5. Fare clic su **OK**.

# Gestire i volumi delle applicazioni

### Cosa sono i volumi di applicazione

I volumi applicativi sono l'archiviazione in cui vengono archiviate informazioni quali la configurazione, il programma di installazione e altri file non di dati relativi al database Oracle.

Il plug-in SnapCenter per Oracle Database consente di creare backup coerenti dei volumi delle applicazioni (volumi non di dati) insieme ai database Oracle.

Il plug-in automatizza il backup e la clonazione dei volumi delle applicazioni.

- Proteggere i volumi delle applicazioni insieme ai volumi del database Oracle in un unico gruppo di risorse.
- Creare backup dei volumi delle applicazioni.
- Creare backup dei database Oracle insieme ai volumi delle applicazioni.

- Crea cloni di database insieme a volumi di applicazioni fino a un determinato punto nel tempo.
- Pianificare le operazioni di backup.
- Monitorare tutte le operazioni.
- Visualizza i report delle operazioni di backup e clonazione.

## Aggiungere volumi di applicazione

SnapCenter supporta il backup e la clonazione dei volumi applicativi del database Oracle. Dovresti aggiungere manualmente i volumi dell'applicazione. Il rilevamento automatico dei volumi delle applicazioni non è supportato.

I volumi applicativi supportano solo connessioni NFS dirette e iSCSI dirette.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Fare clic su **Aggiungi volume applicazione**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   - Nel campo Nome, immettere il nome del volume dell'applicazione.
   - Nel campo Nome host, immettere il nome dell'host.
4. Nella pagina Storage Footprint, immettere il nome del sistema di archiviazione, selezionare uno o più volumi e specificare i LUN o i Qtree associati.

   È possibile aggiungere più sistemi di archiviazione.

5. Rivedi il riepilogo e poi clicca su **Fine**.
6. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza** per visualizzare tutti i volumi applicazione che hai aggiunto.

### Modificare il volume dell'applicazione

Se non vengono creati backup, è possibile modificare tutti i valori specificati durante l'aggiunta del volume dell'applicazione. Se il backup viene creato, è possibile modificare solo i dettagli del sistema di archiviazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza**.
3. Clic per modificare i valori.
4. Clic per modificare i valori.

### Elimina il volume dell'applicazione

Quando si elimina un volume applicativo, se sono presenti backup associati al volume applicativo, il volume applicativo verrà messo in modalità di manutenzione e non verranno creati nuovi backup né conservati i backup precedenti. Se non sono presenti backup associati, tutti i metadati verranno eliminati.

Se necessario, SnapCenter consente di annullare l'operazione di eliminazione.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza**.
3. Clic [elimina icona] per modificare i valori.

## Volumi di applicazione di backup

### Eseguire il backup del volume dell'applicazione

Se il volume dell'applicazione non fa parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

#### Informazioni su questo compito

Per impostazione predefinita, vengono creati backup di gruppi di coerenza (CG). Se si desidera creare backup basati su volumi, è necessario impostare il valore di **EnableOracleNdvVolumeBasedBackup** su true nel file *web.config*.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza**.
3. Clicca * *, quindi selezionare il nome host e il tipo di database per filtrare le risorse.

   Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

4. Selezionare il volume dell'applicazione di cui si desidera eseguire il backup.

   Viene visualizzata la pagina Protezione volume applicazione.

5. Nella pagina Risorsa, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo, quindi immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, customtext__policy_hostname o resource_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |
| Escludi le destinazioni dei registri di archivio dal backup | Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup. |

6. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Allega report attività**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

8. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia del volume dell'applicazione.

9. Fare clic su **Esegui backup ora**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

b. Fare clic su **Backup**.

11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

#### Eseguire il backup del gruppo di risorse dei volumi dell'applicazione

È possibile eseguire il backup del gruppo di risorse contenente solo volumi di applicazioni o una combinazione di volumi di applicazioni e database. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

Se il gruppo di risorse ha più volumi applicativi, tutti i volumi applicativi devono avere un criterio di replica SnapMirror o SnapVault .

#### Informazioni su questo compito

Per impostazione predefinita, vengono creati backup di gruppi di coerenza (CG). Se si desidera creare backup basati su volumi, è necessario impostare il valore di **EnableOracleNdvVolumeBasedBackup** su true nel file *web.config*.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su * *, quindi selezionando il tag. Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi fai clic su **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

> L'operazione di verifica verrà eseguita solo per i database e non per i volumi dell'applicazione.

## Backup del volume dell'applicazione clonata

È possibile utilizzare SnapCenter per clonare i backup del volume dell'applicazione.

#### Prima di iniziare

Se hai installato il plug-in come utente non root, dovresti assegnare manualmente i permessi di esecuzione

alle directory prescript e postscript.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza**.
3. Selezionare il volume dell'applicazione dalla vista dei dettagli del volume dell'applicazione o dalla vista dei dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia del volume dell'applicazione.

4. Dalla vista Gestisci copie, seleziona i backup tra Copie locali (primarie), Copie mirror (secondarie) o Copie vault (secondarie).
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Host del plug-in | Seleziona l'host in cui vuoi creare il clone. |
| Nome della risorsa di destinazione | Specificare il nome della risorsa. |

7. Nella pagina Script, specificare i nomi degli script da eseguire prima della clonazione, i comandi per montare un file system e i nomi degli script da eseguire dopo la clonazione.
8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

### Dividi un clone del volume dell'applicazione

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall'elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall'elenco **Visualizza**.
3. Seleziona la risorsa clonata e fai clic .
4. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.

5. Monitorare l’avanzamento dell’operazione cliccando su **Monitoraggio** > **Lavori**.

### Elimina un clone del volume dell’applicazione

Puoi eliminare i cloni se ritieni che non siano più necessari. Non è possibile eliminare i cloni che fungono da origine per altri cloni.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Oracle Database dall’elenco.
2. Nella pagina Risorse, seleziona **Volume applicazione** dall’elenco **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall’elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Cloni** dai sistemi di archiviazione primari o secondari (con mirroring o replica).
5. Seleziona il clone e poi clicca .
6. Nella pagina Elimina clone, eseguire le seguenti azioni:
   a. Nel campo **Eliminazione pre-clone**, immettere i nomi degli script da eseguire prima di eliminare il clone.
   b. Nel campo **Smonta**, immettere i comandi per smontare il clone prima di eliminarlo.
7. Fare clic su **OK**.

# Proteggere i file system di Windows

## Plug-in SnapCenter per concetti di Microsoft Windows

### Panoramica del plug-in SnapCenter per Microsoft Windows

Il plug-in SnapCenter per Microsoft Windows è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni delle risorse del file system Microsoft. Inoltre, fornisce provisioning di storage, coerenza degli snapshot e recupero di spazio per i file system di Windows. Il plug-in per Windows automatizza le operazioni di backup, ripristino e clonazione del file system nell'ambiente SnapCenter .

Una volta installato il plug-in per Windows, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replicazione del backup da disco a disco per l'archiviazione o la conformità agli standard.

- Abilita la protezione dei dati basata sulle applicazioni per altri plug-in in esecuzione negli host Windows nell'ambiente SnapCenter
- Automatizza le operazioni di backup, ripristino e clonazione basate sulle applicazioni per i file system Microsoft nel tuo ambiente SnapCenter
- Supporta il provisioning dello storage, la coerenza degli snapshot e il recupero dello spazio per gli host Windows

> Il plug-in per Windows esegue il provisioning di condivisioni SMB e file system Windows su LUN fisiche e RDM, ma non supporta operazioni di backup per file system Windows su condivisioni SMB.

### Cosa puoi fare con il plug-in SnapCenter per Microsoft Windows

Una volta installato il plug-in per Windows nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei file system di Windows. È anche possibile eseguire attività di supporto a tali operazioni.

- Scopri le risorse
- Eseguire il backup dei file system di Windows
- Pianificare le operazioni di backup
- Ripristinare i backup del file system
- Clonazione dei backup del file system
- Monitorare le operazioni di backup, ripristino e clonazione

> Il plug-in per Windows non supporta il backup e il ripristino dei file system sulle condivisioni SMB.

## Funzionalità del plug-in SnapCenter per Windows

Il plug-in per Windows si integra con la tecnologia NetApp Snapshot sul sistema di storage. Per lavorare con il plug-in per Windows, utilizzare l'interfaccia SnapCenter .

Il plug-in per Windows include le seguenti funzionalità principali:

- **Interfaccia utente grafica unificata basata su SnapCenter**

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare processi di backup e ripristino coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in. SnapCenter offre inoltre una pianificazione centralizzata e una gestione delle policy per supportare le operazioni di backup e clonazione.

- **Amministrazione centrale automatizzata**

  È possibile pianificare backup di routine del file system, configurare la conservazione dei backup basata su criteri e impostare operazioni di ripristino. È anche possibile monitorare in modo proattivo l'ambiente del file system configurando SnapCenter per l'invio di avvisi tramite e-mail.

- **Tecnologia NetApp Snapshot non disruptiva**

  Il plug-in per Windows utilizza la tecnologia NetApp Snapshot. Ciò consente di eseguire il backup dei file system in pochi secondi e di ripristinarli rapidamente senza dover disconnettere l'host. Gli snapshot occupano uno spazio di archiviazione minimo.

Oltre a queste caratteristiche principali, il plug-in per Windows offre i seguenti vantaggi:

- Supporto per il flusso di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli
- Creazione di copie efficienti in termini di spazio dei file system di produzione per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  Per informazioni sulla licenza FlexClone , vedere"Licenze SnapCenter" .

- Possibilità di eseguire più backup contemporaneamente su più server
- Cmdlet di PowerShell per la creazione di script per operazioni di backup, ripristino e clonazione
- Supporto per il backup di file system e dischi di macchine virtuali (VMDK)
- Supporto per infrastrutture fisiche e virtualizzate
- Supporto per iSCSI, Fibre Channel, FCoE, raw device mapping (RDM), Asymmetric LUN Mapping (ALM), VMDK su NFS e VMFS e FC virtuale
- Supporto per la memoria non volatile express (NVMe) su Windows Server 2022
  - Flussi di lavoro di backup, ripristino, clonazione e verifica su layout VMDK creati su NVMe tramite TCP/IP.
  - Supporta il firmware NVMe versione 1.3 a partire dall'aggiornamento 2 di ESX 8.0 e richiede l'hardware virtuale versione 21.
  - Windows Server Failover Clustering (WSFC) non è supportato per le applicazioni su VMDK su NVMe su TCP/IP.

- Supporta la sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]) che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

## Come SnapCenter esegue il backup dei file system di Windows

SnapCenter utilizza la tecnologia Snapshot per eseguire il backup delle risorse del file system di Windows che risiedono su LUN, CSV (volumi condivisi del cluster), volumi RDM (raw device mapping), ALM (asymmetric LUN mapping) nei cluster Windows e VMDK basati su VMFS/NFS (VMware Virtual Machine File System che utilizza NFS).

SnapCenter crea backup creando snapshot dei file system. I backup federati, in cui un volume contiene LUN da più host, sono più rapidi ed efficienti dei backup di ogni singola LUN perché viene creato un solo snapshot del volume rispetto ai singoli snapshot di ciascun file system.

Quando SnapCenter crea uno Snapshot, l'intero volume del sistema di archiviazione viene catturato nello Snapshot. Tuttavia, il backup è valido solo per il server host per il quale è stato creato.

Se i dati di altri server host risiedono sullo stesso volume, non è possibile ripristinarli dallo Snapshot.

Se un file system di Windows contiene un database, eseguire il backup del file system non è la stessa cosa che eseguire il backup del database. Per eseguire il backup di un database, è necessario utilizzare uno dei plug-in del database.

## Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft Windows

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali. Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il supporto per il provisioning e la protezione dei dati SnapCenter è disponibile su Windows Server. Per le informazioni più recenti sulle versioni supportate, vederehttps://imt.netapp.com/matrix/imt.jsp?components=121074;&solution=1257&isHWU&src=IMT["Strumento matrice di interoperabilità NetApp"^] .

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
|---|---|---|---|
| Server fisico | LUN connesse a FC | Interfaccia utente grafica (GUI) SnapCenter o cmdlet di PowerShell | |
| Server fisico | LUN connesse tramite iSCSI | Cmdlet GUI di SnapCenter o PowerShell | |
| Server fisico | Condivisioni SMB3 (CIFS) residenti su una macchina virtuale di archiviazione (SVM) | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning. |

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
| --- | --- | --- | --- |
| VMware VM | LUN RDM connesse tramite un HBA FC o iSCSI | Cmdlet di PowerShell | |
| VMware VM | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | |
| VMware VM | Sistemi di file di macchine virtuali (VMFS) o datastore NFS | VMware vSphere | |
| VMware VM | Un sistema guest connesso a condivisioni SMB3 residenti su una SVM | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning. |
| VMware VM | Datastore vVol sia su NFS che su SAN | Strumenti ONTAP per VMware vSphere | |
| Macchina virtuale Hyper-V | LUN FC virtuali (vFC) connesse tramite uno switch Fibre Channel virtuale | Cmdlet GUI di SnapCenter o PowerShell | È necessario utilizzare Hyper-V Manager per eseguire il provisioning di LUN Virtual FC (vFC) connesse tramite uno switch Fibre Channel virtuale.<br>I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
| --- | --- | --- | --- |
| Macchina virtuale Hyper-V | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |
| Macchina virtuale Hyper-V | Un sistema guest connesso a condivisioni SMB3 residenti su una SVM | Cmdlet GUI di SnapCenter o PowerShell | Supporto solo per il provisioning.<br>I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |

## Privilegi ONTAP minimi richiesti per il plug-in di Windows

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun cancella
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina

- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online
- modifica del volume
- creazione di volume qtree

    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - mostra interfaccia di rete
    - server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è

necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter . Se si utilizza SnapMirror ActiveSync, utilizzare le pianificazioni predefinite SnapMirror o SnapVault sia per SnapMirror ActiveSync che per le relazioni asincrone.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Definire una strategia di backup per i file system di Windows

Definire una strategia di backup prima di creare i backup ti fornisce i backup necessari per ripristinare o clonare correttamente i tuoi file system. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

### Pianificazioni di backup per i file system di Windows

La frequenza del backup è specificata nei criteri; una pianificazione del backup è specificata nella configurazione del gruppo di risorse. Il fattore più critico nella determinazione della frequenza o della pianificazione di un backup è la velocità di modifica della risorsa e l'importanza dei dati. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. L'SLA e l'RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno.

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup

  La frequenza di backup (la frequenza con cui devono essere eseguiti i backup), denominata *tipo di pianificazione* per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza di backup come oraria, giornaliera, settimanale o mensile, oppure specificare **Nessuno**, che rende il criterio un criterio solo su richiesta. È possibile accedere alle policy facendo clic su **Impostazioni** > **Policy**.

- Pianificazioni di backup

  Le pianificazioni dei backup (ovvero quando devono essere eseguiti esattamente) fanno parte della configurazione di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **Risorse** > **Gruppi di risorse**.

#### Numero di backup necessari per i file system di Windows

I fattori che determinano il numero di backup necessari includono le dimensioni del file system di Windows, il numero di volumi utilizzati, la velocità di modifica del file system e il contratto di servizio (SLA).

#### Convenzione di denominazione del backup per i file system di Windows

I backup del file system di Windows utilizzano la convenzione di denominazione predefinita Snapshot. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:
resourcegroupname_hostname_timestamp

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- `dts1`è il nome del gruppo di risorse.
- `mach1x88`è il nome host.
- `03-12-2016_23.17.26`è la data e l'ora.

Quando si crea un backup, è anche possibile aggiungere un tag descrittivo per facilitare l'identificazione del backup. Al contrario, se si desidera utilizzare una convenzione di denominazione personalizzata per il backup, è necessario rinominare il backup al termine dell'operazione di backup.

#### Opzioni di conservazione del backup

È possibile scegliere il numero di giorni per cui conservare le copie di backup oppure specificare il numero di copie di backup che si desidera conservare, fino a un massimo ONTAP di 255 copie. Ad esempio, la tua organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica SnapMirror , il criterio di conservazione viene replicato sul volume di destinazione.

SnapCenter elimina i backup conservati che hanno etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero comunque rimanere sul sistema.

Per la conservazione a lungo termine delle copie di backup, è consigliabile utilizzare il backup SnapVault .

### Origini e destinazioni dei cloni per i file system di Windows

È possibile clonare un backup del file system da un archivio primario o secondario. Puoi anche scegliere la destinazione che supporta le tue esigenze: la posizione di backup originale o una destinazione diversa sullo stesso host o su un host diverso. La destinazione deve trovarsi sullo stesso volume del backup di origine del clone.

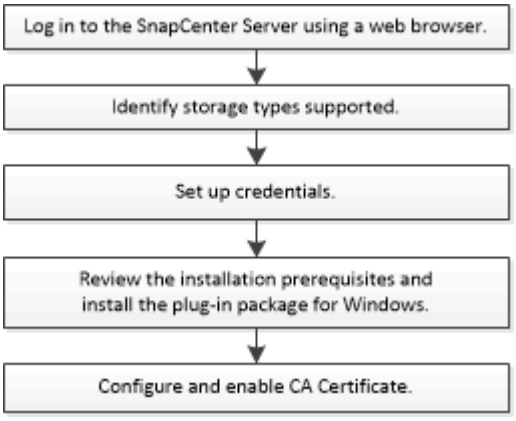
| Destinazione del clone | Descrizione |
|---|---|
| Originale, fonte, posizione | Per impostazione predefinita, SnapCenter memorizza il clone nella stessa posizione e sullo stesso host del backup che viene clonato. |
| Posizione diversa | È possibile archiviare il clone in una posizione diversa sullo stesso host o su un host diverso. L'host deve disporre di una connessione configurata alla macchina virtuale di archiviazione (SVM). |

Una volta completata l'operazione di clonazione, è possibile rinominare il clone.

# Installa il plug-in SnapCenter per Microsoft Windows

### Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Windows

Se si desidera proteggere i file di Windows che non sono file di database, è necessario installare e configurare il plug-in SnapCenter per Microsoft Windows.



## Requisiti di installazione per il plug-in SnapCenter per Microsoft Windows

Prima di installare il plug-in per Windows, è necessario conoscere alcuni requisiti di installazione.

Prima di iniziare a utilizzare il plug-in per Windows, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Per installare il plug-in per Windows è necessario disporre dei privilegi di amministratore SnapCenter .

  Il ruolo di amministratore SnapCenter deve disporre di privilegi di amministratore.

- È necessario aver installato e configurato SnapCenter Server.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- Se si desidera la replica del backup, è necessario configurare SnapMirror e SnapVault .

### Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Se si utilizza un cluster Windows, è necessario installare e configurare anche Windows Remote Management (WinRM). |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

### Imposta le tue credenziali per il plug-in per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare le credenziali per l'installazione dei plug-in di SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati sui file system di Windows.

### Cosa ti servirà

- Prima di installare i plug-in è necessario impostare le credenziali di Windows.
- È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore, sull'host remoto.
- Se si impostano credenziali per singoli gruppi di risorse e l'utente non dispone di privilegi di amministratore completi, è necessario assegnare all'utente almeno i privilegi di gruppo di risorse e di backup.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, procedi come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome utente/Password | Inserisci il nome utente e la password utilizzati per l'autenticazione.<br><br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br><br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono i seguenti:<br><br>◦ `NetBIOS\UserName`<br><br>◦ `Domain FQDN\UserName`<br><br>◦ `UserName@upn`<br><br>• Amministratore locale (solo per gruppi di lavoro)<br><br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è il seguente: `UserName`<br><br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |
| Password | Inserisci la password utilizzata per l'autenticazione. |

5. Fare clic su **OK**.

   Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

### Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

#### Prima di iniziare

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:
   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Aggiungi host e installa il plug-in SnapCenter per Microsoft Windows

È possibile utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host Windows. Il plug-in SnapCenter per Microsoft Windows viene installato automaticamente sull'host specificato. Questo è il metodo consigliato per installare i plug-in. È possibile aggiungere un host e installare un plug-in per un singolo host o per un cluster.

**Prima di iniziare**

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- L'utente SnapCenter dovrebbe essere aggiunto al ruolo "Accedi come servizio" di Windows Server.

- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per Windows File System"

**Informazioni su questo compito**

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.
- Plug-in di Windows
  - Microsoft Windows
  - Microsoft Exchange Server
  - Microsoft SQL Server
  - SAP HANA
- Installazione di plug-in su un cluster

  Se si installano plug-in su un cluster (WSFC, Oracle RAC o Exchange DAG), questi vengono installati su tutti i nodi del cluster.

- Archiviazione serie E

  Non è possibile installare il plug-in per Windows su un host Windows connesso all'archiviazione serie E.

SnapCenter non supporta l'aggiunta dello stesso host (host plug-in) a SnapCenter se l'host fa già parte di un gruppo di lavoro ed è stato modificato in un altro dominio o viceversa. Se si desidera aggiungere lo stesso host, è necessario rimuoverlo da SnapCenter e aggiungerlo nuovamente.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Assicurarsi che in alto sia selezionato **Host gestiti**.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, procedi come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Selezionare il tipo di host **Windows**.<br><br>SnapCenter Server aggiunge l'host e quindi installa il plug-in per Windows se non è già installato sull'host. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>È possibile immettere gli indirizzi IP o il nome di dominio completo di uno dei seguenti:<br><br>• Host autonomo<br>• Clustering di failover di Windows Server (WSFC)<br><br>Se si aggiunge un host tramite SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN. |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove.<br><br>La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, vedere le informazioni sulla creazione di una credenziale.<br><br>I dettagli sulle credenziali, tra cui nome utente, dominio e tipo di host, vengono visualizzati posizionando il cursore sul nome della credenziale fornito.<br><br>La modalità di autenticazione è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Per le nuove distribuzioni non sono elencati pacchetti plug-in.

6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta.<br><br>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter.<br><br>Facoltativamente, è possibile personalizzare il percorso. Per il pacchetto plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Tuttavia, se lo desideri, puoi personalizzare il percorso predefinito. |
| Aggiungi tutti gli host nel cluster | Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster in un WSFC. |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br><br>Fornire il nome gMSA nel seguente formato: *nomedominio\nomeaccount$*.<br><br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo **Salta controlli preliminari**, l'host verrà convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET e la posizione vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in `C:\Program Files\NetApp\SnapCenter` WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Monitorare l'avanzamento dell'installazione.

## Installa il plug-in SnapCenter per Microsoft Windows su più host remoti utilizzando i cmdlet di PowerShell

Se si desidera installare il plug-in SnapCenter per Microsoft Windows su più host contemporaneamente, è possibile farlo utilizzando `Install-SmHostPackage` Cmdlet di PowerShell.

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare i plug-in.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando `Open-SmConnection` cmdlet, quindi immettere le credenziali.
3. Aggiungere l'host autonomo o il cluster a SnapCenter utilizzando `Add-SmHost` cmdlet e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

4. Installare il plug-in su più host utilizzando `Install-SmHostPackage` cmdlet e i parametri richiesti.

   Puoi usare il `-skipprecheck` opzione quando hai installato i plug-in manualmente e non vuoi verificare se l'host soddisfa i requisiti per installare il plug-in.

## Installare il plug-in SnapCenter per Microsoft Windows in modo silenzioso dalla riga di comando

Se non è possibile installare il plug-in in remoto dall'interfaccia utente grafica SnapCenter SnapCenter , è possibile installarlo localmente su un host Windows. È possibile eseguire il programma di installazione del plug-in SnapCenter per Microsoft Windows senza intervento dell'utente, in modalità silenziosa, dalla riga di comando di Windows.

**Prima di iniziare**

- È necessario aver installato ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) Hosting Bundle.
- È necessario aver installato PowerShell 7.4.2 o versione successiva.
- Devi essere un amministratore locale sull'host.

**Passi**

1. Scarica il plug-in SnapCenter per Microsoft Windows dal percorso di installazione.

   Ad esempio, il percorso di installazione predefinito è C:\ProgramData\ NetApp\ SnapCenter\Package Repository.

   Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.

2. Copiare il file di installazione sull'host su cui si desidera installare il plug-in.
3. Dal prompt dei comandi, accedi alla directory in cui hai scaricato il file di installazione.
4. Inserisci il seguente comando, sostituendo le variabili con i tuoi dati:

   ```
   "snapcenter_windows_host_plugin.exe"/silent / debuglog"" /log""
   BI_SNAPCENTER_PORT= SUITE_INSTALLDIR="" BI_SERVICEACCOUNT= BI_SERVICEPWD=
   ISFeatureInstall=SCW
   ```

   Per esempio:

   ```
   `"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`
   ```

   Tutti i parametri passati durante l'installazione del plug-in per Windows sono sensibili alle maiuscole e alle minuscole.

   Inserisci i valori per le seguenti variabili:

| Variabile | Valore |
|---|---|
| */debuglog"<Percorso_registro_debug>* | Specificare il nome e il percorso del file di registro del programma di installazione della suite, come nell'esempio seguente: Setup.exe /debuglog"C:\PathToLog\setupexe.log". |
| BI_SNAPCENTER_PORT | Specificare la porta su cui SnapCenter comunica con SMCore. |
| SUITE_INSTALLDIR | Specificare la directory di installazione del pacchetto plug-in host. |
| BI_SERVICEACCOUNT | Specificare il plug-in SnapCenter per l'account del servizio Web di Microsoft Windows. |
| BI_SERVICEPWD | Specificare la password per l'account del servizio Web SnapCenter Plug-in per Microsoft Windows. |

| Variabile | Valore |
| --- | --- |
| ISFeatureInstall | Specificare la soluzione da distribuire tramite SnapCenter sull'host remoto. |

Il parametro *debuglog* include il percorso del file di registro per SnapCenter. La scrittura in questo file di registro è il metodo preferito per ottenere informazioni sulla risoluzione dei problemi, poiché il file contiene i risultati dei controlli eseguiti dall'installazione per i prerequisiti del plug-in.

Se necessario, è possibile trovare ulteriori informazioni sulla risoluzione dei problemi nel file di registro del pacchetto SnapCenter per Windows. I file di registro per il pacchetto sono elencati (dal più vecchio) nella cartella *%Temp%*, ad esempio, *C:\temp*\.

L'installazione del plug-in per Windows registra il plug-in sull'host e non sul server SnapCenter . È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Dopo aver aggiunto l'host, il plug-in viene rilevato automaticamente.

## Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.

5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

#### Configurare il certificato CA con i servizi plug-in host di Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il

seguente comando:

```
> netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
```

Per esempio:

```
 > netsh http delete sslcert ipport=0.0.0.0:8145
. Associare il certificato appena installato ai servizi plug-in host di
Windows eseguendo i seguenti comandi:
```

```
> $cert = "_<certificate thumbprint>_"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

Per esempio:

```
> $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

#### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della

connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

## Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

## Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

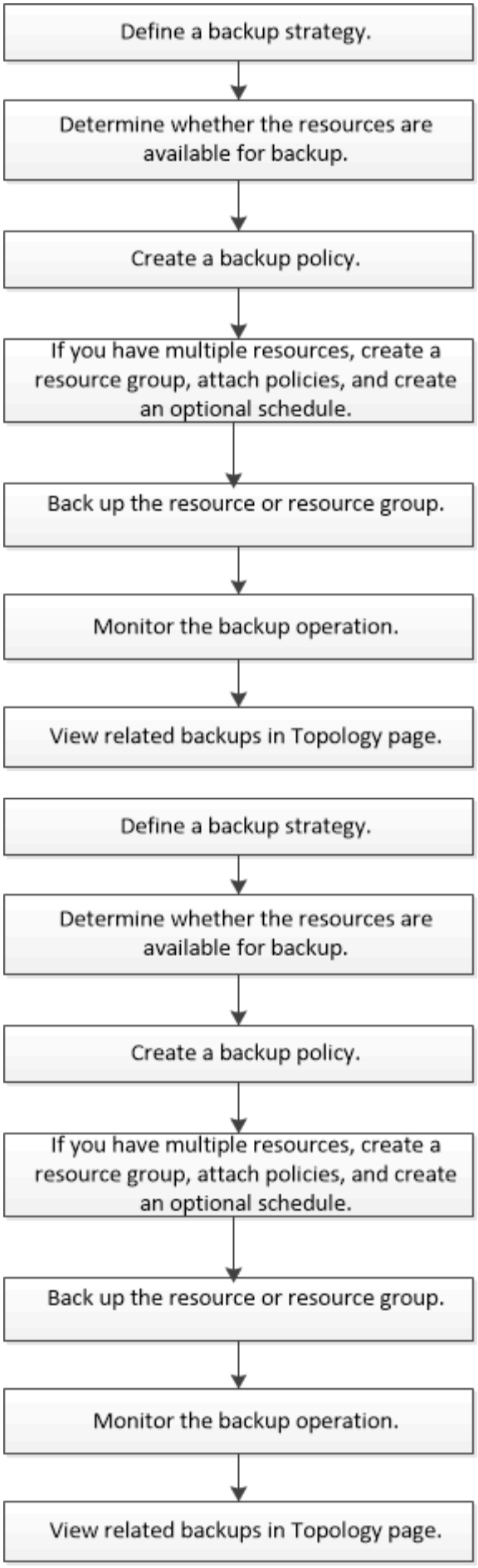
# Eseguire il backup dei file system di Windows

## Eseguire il backup dei file system di Windows

Quando installi il plug-in SnapCenter per Microsoft Windows nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup dei file system di Windows. È possibile eseguire il backup di un singolo file system o di un gruppo di risorse contenente più file system. È possibile eseguire il backup su richiesta o in base a un programma di protezione definito.

È possibile pianificare più backup da eseguire contemporaneamente su più server. Le operazioni di backup e ripristino non possono essere eseguite contemporaneamente sulla stessa risorsa.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di backup:


Define a backup strategy.
Determine whether the resources are available for backup.
Create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
Monitor the backup operation.
View related backups in Topology page.
Define a backup strategy.
Determine whether the resources are available for backup.
Create a backup policy.
If you have multiple resources, create a resource group, attach policies, and create an optional schedule.
Back up the resource or resource group.
Monitor the backup operation.
View related backups in Topology page.

È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter o "Guida di riferimento ai cmdlet del software SnapCenter" contiene informazioni dettagliate sui cmdlet di PowerShell.

## Determinare la disponibilità delle risorse per i file system di Windows

Le risorse sono i LUN e componenti simili nel file system gestiti dai plug-in installati. È possibile aggiungere tali risorse a gruppi di risorse in modo da poter eseguire attività di protezione dei dati su più risorse, ma prima è necessario identificare quali risorse sono disponibili. La scoperta delle risorse disponibili verifica anche che l'installazione del plug-in sia stata completata correttamente.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la creazione di connessioni alla macchina virtuale di archiviazione (SVM) e l'aggiunta di credenziali.
- Se i file risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter. Per ulteriori informazioni, vedere "Documentazione SnapCenter Plug-in for VMware vSphere" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **File System** dall'elenco.
3. Selezionare l'host per filtrare l'elenco delle risorse, quindi fare clic su **Aggiorna risorse**.

   I file system appena aggiunti, rinominati o eliminati vengono aggiornati nell'inventario di SnapCenter Server.

   ⓘ È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

## Creare criteri di backup per i file system di Windows

È possibile creare un nuovo criterio di backup per le risorse prima di utilizzare SnapCenter per eseguire il backup dei file system di Windows oppure è possibile creare un nuovo criterio di backup al momento della creazione di un gruppo di risorse o quando si esegue il backup di una risorsa.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup."Saperne di più"
- È necessario essere preparati alla protezione dei dati.

  Per preparare la protezione dei dati, è necessario completare attività quali l'installazione di SnapCenter, l'aggiunta di host, l'individuazione delle risorse e la creazione di connessioni alla macchina virtuale di archiviazione (SVM).

- Se si replicano gli snapshot su un mirror o su un archivio secondario vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

- Se si desidera eseguire gli script di PowerShell in prescript e postscript, è necessario impostare il valore del parametro usePowershellProcessforScripts su true nel file web.config.

  Il valore predefinito è falso

- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Impostazioni**.
2. Nella pagina Impostazioni, seleziona **Criteri**.
3. Seleziona **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Backup e replica, eseguire le seguenti attività:

   a. Selezionare un'impostazione di backup.

| Opzione | Descrizione |
|---|---|
| Backup coerente con il file system | Selezionare questa opzione se si desidera che SnapCenter metta in pausa l'unità disco su cui risiede il file system prima dell'inizio dell'operazione di backup e poi riprenda l'unità disco al termine dell'operazione di backup. |
| Backup coerente con l'arresto anomalo del file system | Selezionare questa opzione se non si desidera che SnapCenter metta in pausa l'unità disco su cui risiede il file system. |

b. Selezionare una frequenza di pianificazione (detta anche tipo di policy).

   La policy specifica solo la frequenza del backup. La pianificazione specifica della protezione per il backup è definita nel gruppo di risorse. Pertanto, due o più gruppi di risorse possono condividere la stessa policy e la stessa frequenza di backup, ma avere pianificazioni di backup diverse.

   Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

c. Seleziona un'etichetta di criterio.

   A seconda dell'etichetta Snapshot selezionata, ONTAP applica il criterio di conservazione Snapshot secondario corrispondente all'etichetta.

   Se hai selezionato **Aggiorna SnapMirror dopo aver creato una copia Snapshot locale**, puoi facoltativamente specificare l'etichetta del criterio secondario. Tuttavia, se hai selezionato **Aggiorna SnapVault dopo aver creato una copia Snapshot locale**, dovresti specificare l'etichetta del criterio secondario.

6. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| Aggiorna SnapMirror dopo aver creato una copia Snapshot locale | Selezionare questa opzione per creare copie mirror dei set di backup su un altro volume (SnapMirror).<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva di SnapSnapMirror.<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup e i cloni correlati nella pagina Topologia" . |

| Per questo campo… | Fai questo… |
| --- | --- |
| Aggiorna SnapVault dopo aver creato una copia Snapshot | Selezionare questa opzione per eseguire la replica del backup da disco a disco.<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante Aggiorna nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante Aggiorna nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per maggiori informazioni su SnapLock Vault vedere "Eseguire il commit delle copie Snapshot su WORM in una destinazione vault" |
| Errore nel conteggio dei tentativi | Immettere il numero di tentativi di replica che devono essere eseguiti prima che il processo si interrompa. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

7. Nella pagina Impostazioni di conservazione, specificare le impostazioni di conservazione per i backup su richiesta e per ogni frequenza di pianificazione selezionata.

| Opzione | Descrizione |
| --- | --- |
| Numero totale di copie Snapshot da conservare | Selezionare questa opzione se si desidera specificare il numero di snapshot che SnapCenter memorizza prima di eliminarli automaticamente. |
| Conserva le copie Snapshot per | Selezionare questa opzione se si desidera specificare il numero di giorni in cui SnapCenter conserva una copia di backup prima di eliminarla. |
| Periodo di blocco della copia snapshot | Selezionare il periodo di blocco degli snapshot e specificare la durata in giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

Dovresti impostare il conteggio di conservazione su 2 o superiore. Il valore minimo per il conteggio di conservazione è 2.

Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP .

8. Nella pagina Script, immettere il percorso del prescript o del postscript che si desidera che SnapCenter Server esegua rispettivamente prima o dopo l'operazione di backup e un limite di tempo che SnapCenter attende per l'esecuzione dello script prima del timeout.

   Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi e inviare i registri.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare gruppi di risorse per i file system di Windows

Un gruppo di risorse è il contenitore a cui è possibile aggiungere più file system che si desidera proteggere. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire e quindi specificare la pianificazione del backup.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi file system senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi file system a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **File System** dall'elenco.

   Se hai aggiunto di recente un file system a SnapCenter, fai clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.

3. Fare clic su **Nuovo gruppo di risorse**.
4. Nella pagina Nome della procedura guidata, procedere come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere il nome del gruppo di risorse.<br><br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Facoltativo: inserisci un nome e un formato personalizzati per lo snapshot.<br><br>Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |
| Etichetta | Inserisci un tag descrittivo per aiutarti a trovare un gruppo di risorse. |

5. Nella pagina Risorse, esegui le seguenti attività:

   a. Selezionare l'host per filtrare l'elenco delle risorse.

      Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

   b. Nella sezione Risorse disponibili, fare clic sui file system di cui si desidera eseguire il backup, quindi fare clic sulla freccia destra per spostarli nella sezione Aggiunti.

      Se si seleziona l'opzione **Seleziona automaticamente tutte le risorse sullo stesso volume di archiviazione**, vengono selezionate tutte le risorse sullo stesso volume. Quando le sposti nella sezione Aggiunti, tutte le risorse presenti su quel volume vengono spostate insieme.

   Per aggiungere un singolo file system, deselezionare l'opzione **Seleziona automaticamente tutte le risorse sullo stesso volume di archiviazione**, quindi selezionare i file system che si desidera spostare nella sezione Aggiunti.

6. Nella pagina Criteri, eseguire le seguenti attività:

   a. Selezionare una o più policy dall'elenco a discesa.

      È possibile selezionare qualsiasi policy esistente e fare clic su **Dettagli** per determinare se è possibile utilizzarla.

      Se nessuna policy esistente soddisfa i tuoi requisiti, puoi crearne una nuova cliccando su * + * per avviare la procedura guidata dei criteri.

      I criteri selezionati sono elencati nella colonna Criterio nella sezione Configura pianificazioni per i criteri selezionati.

   b. Nella sezione Configura pianificazioni per policy selezionate, fai clic su * + * nella colonna Configura

pianificazioni per il criterio per il quale si desidera configurare la pianificazione.

c. Se il criterio è associato a più tipi di pianificazione (frequenze), selezionare la frequenza che si desidera configurare.

d. Nella finestra di dialogo Aggiungi pianificazioni per la policy *nome_policy*, configura la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fai clic su **Fine**.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate nella sezione Configura pianificazioni per policy selezionate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter . Non modificare le pianificazioni dall'Utilità di pianificazione di Windows e da SQL Server Agent.

7. Nella pagina Notifiche, fornire le seguenti informazioni di notifica:

| Per questo campo… | Fai questo… |
|---|---|
| Preferenza e-mail | Selezionare **Sempre**, **In caso di errore** o **In caso di errore o avviso** per inviare e-mail ai destinatari dopo aver creato gruppi di risorse di backup, allegato criteri e configurato pianificazioni. Inserisci il server SMTP, l'oggetto predefinito dell'e-mail e gli indirizzi e-mail del mittente e del mittente. |
| Da | Indirizzo e-mail |
| A | Inviare un'e-mail all'indirizzo |
| Soggetto | Riga dell'oggetto e-mail predefinita |

8. Rivedi il riepilogo e poi clicca su **Fine**.

È possibile eseguire un backup su richiesta oppure attendere che venga eseguito il backup pianificato.

## Crea gruppi di risorse e abilita la protezione secondaria per i file system Windows sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.

- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

      Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una

pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:
   a. Selezionare il tipo di criterio di replica.

      La politica di replica sincrona non è supportata.

   b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.
   c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

      Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire operazioni di protezione dei dati.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell Core utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione di PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di archiviazione:

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio crea una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup di una singola risorsa su richiesta per i file system di Windows

Se una risorsa non si trova in un gruppo di risorse, è possibile eseguirne il backup su richiesta dalla pagina Risorse.

**Informazioni su questo compito**

Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con l'archiviazione secondaria, il ruolo assegnato all'utente dell'archiviazione deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

Durante il backup di un file system, SnapCenter non esegue il backup delle LUN montate su un punto di montaggio del volume (VMP) nel file system sottoposto a backup.

Se si lavora in un contesto di file system Windows, non eseguire il backup dei file del database. In questo modo si crea un backup incoerente e si rischia la perdita di dati durante il ripristino. Per proteggere i file del database, è necessario utilizzare il plug-in SnapCenter appropriato per il database (ad esempio, il plug-in SnapCenter per Microsoft SQL Server o il plug-in SnapCenter per Microsoft Exchange Server).

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona il tipo di risorsa File System, quindi seleziona la risorsa di cui vuoi eseguire il backup.
3. Se la procedura guidata File System - Proteggi non si avvia automaticamente, fare clic su **Proteggi** per avviare la procedura guidata.

   Specificare le impostazioni di protezione, come descritto nelle attività Creazione di gruppi di risorse.

4. Facoltativo: nella pagina Risorsa della procedura guidata, immettere un formato di nome personalizzato per lo Snapshot.

   Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

5. Nella pagina Criteri, eseguire le seguenti attività:

   a. Selezionare una o più policy dall'elenco a discesa.

      È possibile selezionare qualsiasi criterio esistente e quindi fare clic su **Dettagli** per determinare se è possibile utilizzare tale criterio.

      Se nessuna policy esistente soddisfa i tuoi requisiti, puoi copiare una policy esistente e modificarla oppure puoi creare una nuova policy facendo clic su per avviare la procedura guidata dei criteri. Se nessuna policy esistente soddisfa i tuoi requisiti, puoi copiare una policy esistente e modificarla oppure puoi creare una nuova policy facendo clic su per avviare la procedura guidata dei criteri.

      I criteri selezionati sono elencati nella colonna Criterio nella sezione Configura pianificazioni per i criteri selezionati.

   b. Nella sezione Configura pianificazioni per policy selezionate, fare clic su nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare la pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per la policy *nome_policy*, configura la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fai clic su **Fine**.

      Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate nella sezione Configura pianificazioni per policy selezionate.

   "Le operazioni pianificate potrebbero fallire"

6. Nella pagina Notifiche, eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Preferenza e-mail | Selezionare **Sempre**, **In caso di errore** o **In caso di errore o avviso** per inviare e-mail ai destinatari dopo aver creato gruppi di risorse di backup, allegato criteri e configurato pianificazioni.<br><br>Inserisci le informazioni del server SMTP, l'oggetto predefinito dell'e-mail e gli indirizzi e-mail "A" e "Da". |
| Da | Indirizzo e-mail |
| A | Inviare un'e-mail all'indirizzo |
| Soggetto | Riga dell'oggetto e-mail predefinita |

7. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia del database.

8. Fare clic su **Esegui backup ora**.
9. Nella pagina Backup, procedere come segue:
   a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa Criterio seleziona il criterio che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   Open-smconnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea un nuovo criterio di backup con un tipo di backup SQL di FullBackup:

```
PS C:\> Add-SmPolicy -PolicyName TESTPolicy
-PluginPolicyType SCSQL -PolicyType Backup
-SqlBackupType FullBackup -Verbose
```

Questo esempio crea un nuovo criterio di backup con un tipo di backup del file system Windows CrashConsistent:

```
PS C:\> Add-SmPolicy -PolicyName FileSystemBackupPolicy
-PluginPolicyType SCW -PolicyType Backup
-ScwBackupType CrashConsistent -Verbose
```

3. Scopri le risorse host utilizzando il cmdlet Get-SmResources.

   Questo esempio rileva le risorse per il plug-in Microsoft SQL sull'host specificato:

```
C:\PS>PS C:\> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCSQL
```

   Questo esempio rileva le risorse per i file system Windows sull'host specificato:

```
C:\PS>PS C:\> Get-SmResources -HostName vise2-f6.sddev.mycompany.com
-PluginCode SCW
```

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse di backup del database SQL con i criteri e le risorse specificati:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName AccountingResource
-Resources @{"Host"="visef6.org.com";
"Type"="SQL Database";"Names"="vise-f6\PayrollDatabase"}
-Policies "BackupPolicy"
```

   Questo esempio crea un nuovo gruppo di risorse di backup del file system di Windows con i criteri e le risorse specificati:

```
PS C:\> Add-SmResourceGroup -ResourceGroupName EngineeringResource
-PluginCode SCW -Resources @{"Host"="WIN-VOK20IKID5I";
"Type"="Windows Filesystem";"Names"="E:\"}
-Policies "EngineeringBackupPolicy"
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
PS C:> New-SmBackup -ResourceGroupName PayrollDataset -Policy
FinancePolicy
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

   Questo esempio visualizza un report riepilogativo di tutti i lavori eseguiti nella data specificata:

```
PS C:\> Get-SmJobSummaryReport -Date '1/27/2016'
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse per i file system di Windows

Un gruppo di risorse è una raccolta di risorse su un host o cluster. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse. È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con l'archiviazione secondaria, il ruolo assegnato all'utente dell'archiviazione deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se un gruppo di risorse ha più database da host diversi, l'operazione di backup su alcuni host potrebbe essere avviata in ritardo a causa di problemi di rete. Dovresti configurare il valore di MaxRetryForUninitializedHosts in web.config utilizzando il cmdlet PowerShell Set-SmConfigSettings

Durante il backup di un file system, SnapCenter non esegue il backup delle LUN montate su un punto di montaggio del volume (VMP) nel file system sottoposto a backup.

Se si lavora in un contesto di file system Windows, non eseguire il backup dei file del database. In questo modo si crea un backup incoerente e si rischia la perdita di dati durante il ripristino. Per proteggere i file del database, è necessario utilizzare il plug-in SnapCenter appropriato per il database (ad esempio, il plug-in SnapCenter per Microsoft SQL Server o il plug-in SnapCenter per Microsoft Exchange Server).

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su e selezionando il tag. Puoi quindi fare clic per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi fai clic su **Esegui backup ora**.

> Per il plug-in SnapCenter per Oracle Database, se si dispone di un gruppo di risorse federato con due database e uno dei database ha un file di dati su uno storage non NetApp , l'operazione di backup viene interrotta anche se l'altro database si trova su uno storage NetApp .

4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
   - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

     "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

   - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire. Per aumentare la dimensione dell'heap Java, individuare il file di script `/opt/netapp/init_scripts/scvservice` . In quella sceneggiatura, il `do_start method` Il comando avvia il servizio plug-in SnapCenter VMware. Aggiorna quel comando come segue: `Java -jar -Xmx8192M -Xms4096M` .

## Monitorare le operazioni di backup

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.

- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni correlati nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, è possibile visualizzare una rappresentazione grafica di tutti i backup e i cloni nell'archiviazione primaria e secondaria. Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

**Informazioni su questo compito**

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .
  - Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato sarà 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   Nella sezione Scheda riepilogativa viene visualizzato il numero totale di backup e cloni. Solo per il database Oracle, la sezione Scheda riepilogativa mostra anche il numero totale di backup del log.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di

backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

- Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
- Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, ridenominazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti sul sistema di archiviazione secondario.

7. Se vuoi eliminare un clone, seleziona il clone dalla tabella e fai clic su per eliminare il clone.

**Esempio che mostra backup e cloni sullo storage primario**

## Pulisci il conteggio dei backup secondari utilizzando i cmdlet di PowerShell

È possibile utilizzare il cmdlet Remove-SmBackup per ripulire il conteggio dei backup secondari privi di snapshot. Potrebbe essere necessario utilizzare questo cmdlet quando il numero totale di snapshot visualizzati nella topologia Gestisci copie non corrisponde all'impostazione di conservazione degli snapshot dell'archiviazione secondaria.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Pulisci il conteggio dei backup secondari utilizzando il parametro -CleanupSecondaryBackups.

   Questo esempio pulisce il conteggio dei backup per i backup secondari senza snapshot:

```
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"):
```

# Ripristinare i file system di Windows

## Ripristinare i backup del file system di Windows

È possibile utilizzare SnapCenter per ripristinare i backup del file system. Il ripristino del file system è un processo multifase che copia tutti i dati da un backup specificato nella posizione originale del file system.

**Prima di iniziare**

- È necessario aver eseguito il backup del file system.
- Se è in corso un'operazione pianificata, ad esempio un'operazione di backup, per un file system, è necessario annullare tale operazione prima di poter avviare un'operazione di ripristino.
- È possibile ripristinare un backup del file system solo nella posizione originale, non in un percorso alternativo.

  Non è possibile ripristinare un singolo file da un backup perché il file system ripristinato sovrascrive tutti i dati presenti nella posizione originale del file system. Per ripristinare un singolo file da un backup del file system, è necessario clonare il backup e accedere al file nel clone.

- Non è possibile ripristinare un volume di sistema o di avvio.
- SnapCenter può ripristinare i file system in un cluster Windows senza disconnettere il gruppo di cluster.

**Informazioni su questo compito**

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Per filtrare l'elenco delle risorse, selezionare le opzioni File System e Gruppo di risorse.
3. Selezionare un gruppo di risorse dall'elenco, quindi fare clic su **Ripristina**.
4. Nella pagina Backup, seleziona se desideri effettuare il ripristino dai sistemi di archiviazione primari o secondari, quindi seleziona un backup da ripristinare.
5. Seleziona le opzioni desiderate nella procedura guidata di ripristino.
6. È possibile immettere il percorso e gli argomenti del prescript o del postscript che si desidera che SnapCenter esegua rispettivamente prima o dopo l'operazione di ripristino.

   Ad esempio, è possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

7. Nella pagina Notifiche, seleziona una delle seguenti opzioni:

| Per questo campo… | Fai questo… |
|---|---|
| Registra gli eventi del server SnapCenter nel sistema di archiviazione syslog | Selezionare questa opzione per registrare gli eventi di SnapCenter Server nel syslog del sistema di archiviazione. |
| Invia notifica AutoSupport per operazioni non riuscite al sistema di archiviazione | Selezionare questa opzione per inviare informazioni su eventuali operazioni non riuscite a NetApp tramite AutoSupport. |
| Preferenza e-mail | Selezionare **Sempre**, **In caso di errore** o **In caso di errore o avviso** per inviare messaggi di posta elettronica ai destinatari dopo il ripristino dei backup. Inserisci il server SMTP, l'oggetto predefinito dell'e-mail e gli indirizzi e-mail A e Da. |

8. Rivedi il riepilogo e poi clicca su **Fine**.
9. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   Se il file system ripristinato contiene un database, è necessario ripristinare anche il database. Se non si ripristina il database, è possibile che lo stato del database non sia valido. Per informazioni sul ripristino dei database, consultare la Guida alla protezione dei dati per quel database.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il

cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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           :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di ripristino

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

## Annulla le operazioni di ripristino

È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di ripristino in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla processo** è disabilitato per le operazioni di ripristino che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di ripristino in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Seleziona il lavoro e clicca su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di ripristino, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

# Clonare i file system di Windows

## Clona da un backup del file system di Windows

È possibile utilizzare SnapCenter per clonare un backup del file system di Windows. Se desideri una copia di un singolo file che è stato eliminato o modificato per errore, puoi clonare un backup e accedere a quel file nel clone.

**Prima di iniziare**

- Dovresti aver preparato la protezione dei dati completando attività quali l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni alla macchina virtuale di archiviazione (SVM).
- Dovresti avere un backup del file system.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Non è possibile clonare un gruppo di risorse. È possibile clonare solo singoli backup del file system.
- Se un backup risiede su una macchina virtuale con un disco VMDK, SnapCenter non può clonare il backup su un server fisico.
- Se si clona un cluster Windows (ad esempio, un LUN condiviso o un LUN di un volume condiviso del cluster (CSV)), il clone viene archiviato come LUN dedicato sull'host specificato.
- Per un'operazione di clonazione, la directory radice del punto di montaggio del volume non può essere una directory condivisa.
- Non è possibile creare un clone su un nodo che non sia il nodo home dell'aggregato.
- Non è possibile pianificare operazioni di clonazione ricorrenti (ciclo di vita della clonazione) per i file system Windows; è possibile clonare un backup solo su richiesta.
- Se si sposta una LUN contenente un clone in un nuovo volume, SnapCenter non potrà più supportare il clone. Ad esempio, non è possibile utilizzare SnapCenter per eliminare quel clone.
- Non è possibile clonare tra ambienti diversi. Ad esempio, la clonazione da un disco fisico a un disco virtuale o viceversa.

**Informazioni su questo compito**

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **File System** dall'elenco.
3. Selezionare l'host.

   La vista topologica viene visualizzata automaticamente se la risorsa è protetta.
4. Dall'elenco delle risorse, seleziona il backup che desideri clonare, quindi fai clic sull'icona di clonazione.
5. Nella pagina Opzioni, procedi come segue:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Selezionare l'host su cui creare il clone. |
| "Assegna automaticamente il punto di montaggio" o "Assegna automaticamente il punto di montaggio del volume nel percorso" | Scegliere se assegnare automaticamente un punto di montaggio o un punto di montaggio del volume in un percorso.<br><br>Assegnazione automatica del punto di montaggio del volume in base al percorso: il punto di montaggio in base a un percorso consente di specificare una directory specifica in cui verranno creati i punti di montaggio. Prima di scegliere questa opzione, è necessario verificare che la directory sia vuota. Se nella directory è presente un backup, il backup sarà in uno stato non valido dopo l'operazione di montaggio. |
| Posizione dell'archivio | Se si sta clonando un backup secondario, scegliere una posizione di archivio. |

6. Nella pagina Script, specificare eventuali prescript o postscript che si desidera eseguire.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.
7. Rivedi il riepilogo e poi clicca su **Fine**.
8. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Elenca i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                    BackupTime   BackupType
--------   ----------                    ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

   Questo esempio visualizza informazioni su un gruppo di risorse specificato, sulle sue risorse e sui criteri associati:

```
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. Avviare un'operazione di clonazione da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

```
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
```

   Questo esempio crea un clone di un'istanza specificata di Microsoft SQL Server:

```
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. Visualizzare lo stato del processo di clonazione utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report di clonazione per l'ID processo specificato:

```
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}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di clonazione

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Annulla le operazioni di clonazione

È possibile annullare le operazioni di clonazione in coda.

Per annullare le operazioni di clonazione, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di clonazione in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di clonazione in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di clonazione in coda.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di clonazione in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Selezionare l'operazione e fare clic su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di clonazione, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina **Dettagli lavoro**, fare clic su **Annulla lavoro**. |

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
| --- | --- |
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

**Informazioni correlate**

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

# Proteggere i database di Microsoft Exchange Server

## Concetti del plug-in SnapCenter per Microsoft Exchange Server

### Panoramica del plug-in SnapCenter per Microsoft Exchange Server

Il plug-in SnapCenter per Microsoft Exchange Server è un componente lato host del software NetApp SnapCenter che consente la gestione della protezione dei dati basata sulle applicazioni dei database di Exchange. Il plug-in per Exchange automatizza il backup e il ripristino dei database di Exchange nell'ambiente SnapCenter .

Una volta installato il plug-in per Exchange, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia NetApp SnapVault per eseguire la replicazione di backup da disco a disco per conformità agli standard o per scopi di archiviazione.

Se si desidera ripristinare e recuperare e-mail o cassette postali anziché l'intero database di Exchange, è possibile utilizzare il software Single Mailbox Recovery (SMBR). NetApp® Single Mailbox Recovery ha raggiunto la fine della disponibilità (EOA) il 12 maggio 2023. NetApp continuerà a supportare i clienti che hanno acquistato capacità di casella di posta, manutenzione e supporto tramite i codici prodotto di marketing introdotti il 24 giugno 2020, per tutta la durata del diritto al supporto.

NetApp Single Mailbox Recovery è un prodotto partner fornito da Ontrack. Ontrack PowerControls offre funzionalità simili a quelle di NetApp Single Mailbox Recovery. I clienti possono acquistare nuove licenze software Ontrack PowerControls e rinnovi di manutenzione e supporto Ontrack PowerControls da Ontrack (tramite licensingteam@ontrack.com) per il ripristino granulare delle caselle di posta.

Il plug-in per Exchange supporta la sincronizzazione attiva SnapMirror (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), che consente ai servizi aziendali di continuare a funzionare anche in caso di guasto completo del sito, supportando il failover delle applicazioni in modo trasparente utilizzando una copia secondaria. Per attivare un failover con SnapMirror ActiveSync non è necessario alcun intervento manuale né scripting aggiuntivo.

Supporta la modalità asimmetrica, failover o non duplex di SnapMirror Active Sync. Si riferisce alla soluzione in cui il percorso ottimizzato parte solo dal nodo proprietario della LUN sul lato primario. Qualsiasi I/O in arrivo sui percorsi del cluster secondario viene gestito tramite proxy sul cluster primario. La replicazione sincrona è unidirezionale, nella direzione da primaria a secondaria.

- Automatizza le operazioni di backup e ripristino basate sulle applicazioni per i database di Microsoft Exchange Server e i gruppi di disponibilità del database (DAG) nel tuo ambiente SnapCenter
- Supporta server Exchange virtualizzati su LUN RDM quando si distribuisce il SnapCenter Plug-in for VMware vSphere e si registra il plug-in con SnapCenter.

### Cosa puoi fare con il plug-in SnapCenter per Microsoft Exchange Server

È possibile utilizzare il plug-in per Exchange per eseguire il backup e il ripristino dei database di Exchange Server.

- Visualizza e gestisci un inventario attivo di gruppi di disponibilità del database di Exchange (DAG), database e set di repliche
- Definire le policy che forniscono le impostazioni di protezione per l'automazione del backup
- Assegnare policy ai gruppi di risorse
- Proteggere singoli DAG e database
- Eseguire il backup dei database delle cassette postali di Exchange primari e secondari
- Ripristinare i database dai backup primari e secondari

## Tipi di archiviazione supportati dal plug-in SnapCenter per Microsoft Windows e per Microsoft Exchange Server

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali. Prima di installare il pacchetto per l'host, è necessario verificare se il supporto è disponibile per il tipo di storage in uso.

Il supporto per il provisioning e la protezione dei dati SnapCenter è disponibile su Windows Server. Per le informazioni più recenti sulle versioni supportate, vedere https://imt.netapp.com/matrix/imt.jsp?components=121031;&solution=1259&isHWU&src=IMT [Strumento matrice di interoperabilità NetApp ^].

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
|---|---|---|---|
| Server fisico | LUN connesse a FC | Interfaccia utente grafica (GUI) SnapCenter o cmdlet di PowerShell | |
| Server fisico | LUN connesse tramite iSCSI | Cmdlet GUI di SnapCenter o PowerShell | |
| VMware VM | LUN RDM connesse tramite un HBA FC o iSCSI | Cmdlet di PowerShell | Solo compatibilità fisica<br>I VMDK non sono supportati. |
| VMware VM | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | I VMDK non sono supportati. |

| Macchina | Tipo di archiviazione | Fornitura tramite | Note di supporto |
| --- | --- | --- | --- |
| Macchina virtuale Hyper-V | LUN FC virtuali (vFC) connesse tramite uno switch Fibre Channel virtuale | Cmdlet GUI di SnapCenter o PowerShell | È necessario utilizzare Hyper-V Manager per eseguire il provisioning di LUN Virtual FC (vFC) connesse tramite uno switch Fibre Channel virtuale.<br>I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |
| Macchina virtuale Hyper-V | LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI | Cmdlet GUI di SnapCenter o PowerShell | I dischi pass-through Hyper-V e il backup dei database su VHD(x) forniti su storage NetApp non sono supportati. |

## Privilegi ONTAP minimi richiesti per il plug-in di Exchange

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea

- lun crea
- lun cancella
- lun igroup aggiungi
- lun igroup create
- lun igroup elimina
- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume

    - distruzione del volume
    - creazione di clonazione di file di volume
    - file di volume mostra-utilizzo-disco
    - volume offline
    - volume online
    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive

- interfaccia di rete
- mostra interfaccia di rete
- server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter . Se si utilizza SnapMirror ActiveSync, utilizzare le pianificazioni predefinite SnapMirror o SnapVault sia per SnapMirror ActiveSync che per le relazioni asincrone.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Definire una strategia di backup per le risorse di Exchange Server

Definire una strategia di backup prima di creare i processi di backup aiuta a garantire di disporre dei backup necessari per ripristinare correttamente i database. Il Service Level Agreement (SLA), il Recovery Time Objective (RTO) e il Recovery Point Objective (RPO) determinano in larga misura la strategia di backup.

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di backup.

### Tipi di backup supportati per il database di Exchange

Per eseguire il backup delle cassette postali di Exchange tramite SnapCenter è necessario scegliere il tipo di risorsa, ad esempio database e gruppi di disponibilità del database (DAG). La tecnologia snapshot viene sfruttata per creare copie online di sola lettura dei volumi su cui risiedono le risorse.

| Tipo di backup | Descrizione |
| --- | --- |
| Backup completo e del registro | Esegue il backup dei database e di tutti i registri delle transazioni, compresi i registri troncati.<br><br>Una volta completato un backup completo, Exchange Server tronca i registri delle transazioni già salvati nel database.<br><br>In genere, dovresti scegliere questa opzione. Tuttavia, se il tempo di backup è breve, è possibile scegliere di non eseguire un backup del registro delle transazioni con un backup completo. |
| Backup completo | Esegue il backup dei database e dei registri delle transazioni.<br><br>I registri delle transazioni troncati non vengono sottoposti a backup. |
| Backup del registro | Esegue il backup di tutti i registri delle transazioni.<br><br>I log troncati che sono già stati salvati nel database non vengono sottoposti a backup. Se si pianificano backup frequenti del registro delle transazioni tra backup completi del database, è possibile scegliere punti di ripristino granulari. |

**Pianificazioni di backup per i plug-in del database**

La frequenza del backup (tipo di pianificazione) è specificata nei criteri; una pianificazione del backup è specificata nella configurazione del gruppo di risorse. Il fattore più critico nella determinazione della frequenza o della pianificazione di un backup è la velocità di modifica della risorsa e l'importanza dei dati. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo Service Level Agreement (SLA) e il tuo Recover Point Objective (RPO).

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. Un RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. L'SLA e l'RPO contribuiscono alla strategia di protezione dei dati.

Anche per una risorsa molto utilizzata, non è necessario eseguire un backup completo più di una o due volte al giorno. Ad esempio, potrebbero essere sufficienti backup regolari del registro delle transazioni per garantire di disporre dei backup necessari. Quanto più spesso si esegue il backup dei database, tanto minore sarà il numero di registri delle transazioni che SnapCenter dovrà utilizzare al momento del ripristino, il che può comportare operazioni di ripristino più rapide.

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup

  La frequenza di backup (la frequenza con cui devono essere eseguiti i backup), denominata *tipo di*

*pianificazione* per alcuni plug-in, fa parte della configurazione di una policy. È possibile selezionare la frequenza di backup oraria, giornaliera, settimanale o mensile per la policy. Se non si seleziona nessuna di queste frequenze, la policy creata sarà una policy solo on-demand. È possibile accedere alle policy facendo clic su **Impostazioni** > **Policy**.

- Pianificazioni di backup

  Le pianificazioni dei backup (ovvero quando devono essere eseguiti esattamente) fanno parte della configurazione di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00. È possibile accedere alle pianificazioni dei gruppi di risorse facendo clic su **Risorse** > **Gruppi di risorse**.

### Numero di processi di backup necessari per i database

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

### Convenzioni di denominazione del backup

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

### Opzioni di conservazione del backup

È possibile scegliere il numero di giorni per cui conservare le copie di backup oppure specificare il numero di copie di backup che si desidera conservare, fino a un massimo ONTAP di 255 copie. Ad esempio, la tua organizzazione potrebbe richiedere di conservare 10 giorni di copie di backup o 130 copie di backup.

Durante la creazione di un criterio, è possibile specificare le opzioni di conservazione per il tipo di backup e il tipo di pianificazione.

Se si imposta la replica SnapMirror , il criterio di conservazione viene replicato sul volume di destinazione.

SnapCenter elimina i backup conservati che hanno etichette di conservazione corrispondenti al tipo di pianificazione. Se il tipo di pianificazione è stato modificato per la risorsa o il gruppo di risorse, i backup con la vecchia etichetta del tipo di pianificazione potrebbero comunque rimanere sul sistema.

Per la conservazione a lungo termine delle copie di backup, è consigliabile utilizzare il backup SnapVault .

#### Per quanto tempo conservare i backup del registro delle transazioni sul volume di archiviazione di origine per Exchange Server

Il plug-in SnapCenter per Microsoft Exchange Server necessita di backup del registro delle transazioni per eseguire operazioni di ripristino aggiornate al minuto, che ripristinano il database a un orario compreso tra due backup completi.

Ad esempio, se Plug-in per Exchange ha eseguito un backup completo del registro delle transazioni alle 8:00 e un altro backup completo del registro delle transazioni alle 17:00, potrebbe utilizzare l'ultimo backup del registro delle transazioni per ripristinare il database a un orario qualsiasi compreso tra le 8:00 e le 17:00. Se i registri delle transazioni non sono disponibili, Plug-in per Exchange può eseguire solo operazioni di ripristino temporizzato, che ripristinano un database all'orario in cui Plug-in per Exchange ha completato un backup completo.

In genere, sono necessarie operazioni di ripristino aggiornate solo per uno o due giorni. Per impostazione predefinita, SnapCenter conserva un minimo di due giorni.

## Definire una strategia di ripristino per i database di Exchange

Definire una strategia di ripristino per Exchange Server consente di ripristinare correttamente il database.

#### Origini per un'operazione di ripristino in Exchange Server

È possibile ripristinare un database di Exchange Server da una copia di backup su un archivio primario.

È possibile ripristinare i database solo dall'archiviazione primaria.

#### Tipi di operazioni di ripristino supportate per Exchange Server

È possibile utilizzare SnapCenter per eseguire diversi tipi di operazioni di ripristino sulle risorse di Exchange.

- Ripristinare all'ultimo minuto
- Ripristina un punto precedente nel tempo

##### Ripristina fino al minuto

In un'operazione di ripristino all'ultimo minuto, i database vengono ripristinati fino al punto di errore. SnapCenter realizza questo risultato eseguendo la seguente sequenza:

1. Ripristina i database dal backup completo del database selezionato.
2. Applica tutti i registri delle transazioni sottoposti a backup, nonché tutti i nuovi registri creati dall'ultimo backup.

I registri delle transazioni vengono spostati in avanti e applicati a tutti i database selezionati.

Al termine di un ripristino, Exchange crea una nuova catena di registri.

**Procedura consigliata:** si consiglia di eseguire un nuovo backup completo e del registro dopo il completamento di un ripristino.

Un'operazione di ripristino aggiornata richiede un set contiguo di registri delle transazioni.

Dopo aver eseguito un ripristino aggiornato, il backup utilizzato per il ripristino è disponibile solo per le operazioni di ripristino point-in-time.

Se non è necessario mantenere la capacità di ripristino aggiornata per tutti i backup, è possibile configurare la conservazione del backup del registro delle transazioni del sistema tramite i criteri di backup.

#### Ripristina un punto precedente nel tempo

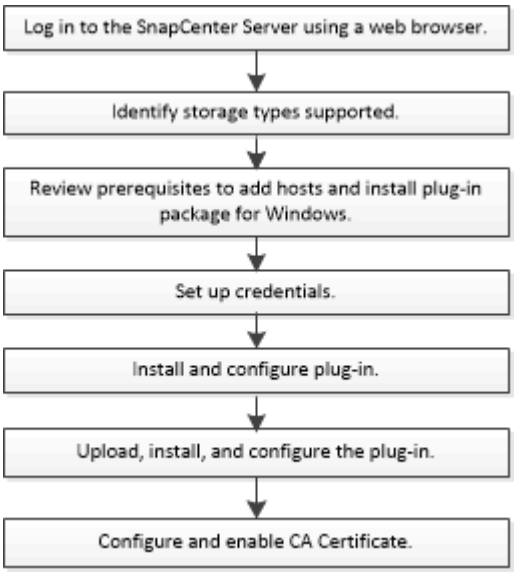
In un'operazione di ripristino point-in-time, i database vengono ripristinati solo a un momento specifico del passato. Un'operazione di ripristino point-in-time si verifica nelle seguenti situazioni di ripristino:

- Il database viene ripristinato a un orario specificato in un registro delle transazioni sottoposto a backup.
- Il database viene ripristinato e ad esso viene applicato solo un sottoinsieme dei registri delle transazioni sottoposti a backup.

# Installa il plug-in SnapCenter per Microsoft Exchange Server

## Flusso di lavoro di installazione del plug-in SnapCenter per Microsoft Exchange Server

Se si desidera proteggere i database di Exchange, è necessario installare e configurare il plug-in SnapCenter per Microsoft Exchange Server.



## Prerequisiti per aggiungere host e installare il plug-in SnapCenter per Microsoft Exchange Server

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Per le configurazioni autonome e del gruppo di disponibilità del database è necessario utilizzare Microsoft Exchange Server 2013, 2016 o 2019.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente del gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.
- È necessario disporre di un utente con autorizzazioni amministrative su Exchange Server.
- Se SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati, è necessario annullare la registrazione del provider hardware VSS utilizzato da SnapDrive per Windows prima di installare il plug-in per Exchange sullo stesso Exchange Server per garantire una protezione dei dati efficace tramite SnapCenter.
- Se SnapManager per Microsoft Exchange Server e Plug-in per Exchange sono installati sullo stesso server, è necessario sospendere o eliminare dallo scheduler di Windows tutte le pianificazioni create da SnapManager per Microsoft Exchange Server.
- L'host deve essere risolvibile nel nome di dominio completo (FQDN) dal server. Se il file hosts viene modificato per renderlo risolvibile e se nel file hosts sono specificati sia il nome breve che l'FQDN, creare una voce nel file hosts SnapCenter nel seguente formato: *<indirizzo_ip> <fqdn_host> <nome_host>*.
- Assicurarsi che le seguenti porte non siano bloccate nel firewall, altrimenti l'operazione di aggiunta dell'host fallirà. Per risolvere questo problema, è necessario configurare l'intervallo di porte dinamiche. Per ulteriori informazioni, vedere "Documentazione Microsoft" .
  - Intervallo di porte 50000 - 51000 per Windows 2016 ed Exchange 2016
  - Intervallo di porte 6000 - 6500 per Windows 2012 R2 ed Exchange 2013
  - Intervallo di porte 49152 - 65536 per Windows 2019

> Per identificare l'intervallo di porte, eseguire i seguenti comandi:
>
> - netsh int ipv4 mostra porta dinamica tcp
> - netsh int ipv4 mostra porta dinamica udp
> - netsh int ipv6 mostra porta dinamica tcp
> - netsh int ipv6 mostra porta dinamica udp

### Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br><br>Java 11 Oracle Java e OpenJDK sono richiesti solo per SAP HANA, IBM Db2, PostgreSQL, MySQL, i plug-in supportati NetApp e altre applicazioni personalizzate che possono essere installate su host Windows.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

**Sono richiesti privilegi di Exchange Server**

Per consentire a SnapCenter di aggiungere Exchange Server o DAG e di installare il plug-in SnapCenter per Microsoft Exchange Server su un host o DAG, è necessario configurare SnapCenter con le credenziali di un utente con un set minimo di privilegi e autorizzazioni.

È necessario disporre di un utente di dominio con privilegi di amministratore locale e con autorizzazioni di

accesso locale sull'host Exchange remoto, nonché autorizzazioni amministrative su tutti i nodi del DAG. L'utente del dominio necessita delle seguenti autorizzazioni minime:

- Aggiungi-MailboxDatabaseCopy
- Smonta-Database
- Ottieni-AdServerSettings
- Ottieni-DatabaseAvailabilityGroup
- Ottieni-ExchangeServer
- Ottieni-MailboxDatabase
- Get-MailboxDatabaseCopyStatus
- Get-MailboxServer
- Ottieni-Statistiche-della-Casella-Di-Posta
- Ottieni-PublicFolderDatabase
- Sposta-ActiveMailboxDatabase
- Move-DatabasePath -ConfigurationOnly:$true
- Mount-Database
- Nuovo database delle cassette postali
- Nuovo database cartella pubblica
- Rimuovi-MailboxDatabase
- Rimuovi-MailboxDatabaseCopy
- Rimuovi-DatabaseCartellaPubblica
- Riprendi-MailboxDatabaseCopy
- Set-AdServerSettings
- Set-MailboxDatabase -allowfilerestore:$true
- Set-MailboxDatabaseCopy
- Set-PublicFolderDatabase
- Sospendi-MailboxDatabaseCopy
- Aggiorna-MailboxDatabaseCopy

### Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

| Articolo | Requisiti |
| --- | --- |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br><br>Java 11 Oracle Java e OpenJDK sono richiesti solo per SAP HANA, IBM Db2, PostgreSQL, MySQL, i plug-in supportati NetApp e altre applicazioni personalizzate che possono essere installate su host Windows.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Imposta le credenziali per il plug-in SnapCenter per Windows

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare le credenziali per l'installazione del pacchetto plug-in e credenziali aggiuntive per eseguire operazioni di protezione dei dati sui database.

### Informazioni su questo compito

È necessario impostare le credenziali per l'installazione dei plug-in sugli host Windows. Sebbene sia possibile creare credenziali per Windows dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

Impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.

   Viene visualizzata la finestra Credenziali.

4. Nella pagina Credenziali, procedi come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per la credenziale. |
| Nome utente | Inserisci il nome utente utilizzato per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ `NetBIOS\UserName`<br>◦ `Domain FQDN\UserName`<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: `UserName` |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Autenticazione | Selezionare Windows come modalità di autenticazione. |

5. Fare clic su **OK**.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:
   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

   Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Aggiungi host e installa il plug-in per Exchange

È possibile utilizzare la pagina Aggiungi host di SnapCenter per aggiungere host Windows. Il plug-in per Exchange viene installato automaticamente sull'host specificato. Questo è il metodo consigliato per installare i plug-in. È possibile aggiungere un host e installare un plug-in per un singolo host o per un cluster.

**Prima di iniziare**

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio SnapCenter Admin.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- Il servizio di accodamento dei messaggi deve essere in esecuzione.

- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi. Per informazioni, vedere"Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per Microsoft Exchange Server" .

**Informazioni su questo compito**

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.
- È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.
- Se un nodo di scambio fa parte di un DAG, non è possibile aggiungere un solo nodo al server SnapCenter .
- Se si installano plug-in su un cluster (Exchange DAG), questi vengono installati su tutti i nodi del cluster, anche se alcuni nodi non dispongono di database su LUN NetApp .

A partire da SnapCenter 4.6, SCE supporta il multi-tenancy ed è possibile aggiungere un host utilizzando i seguenti metodi:

| Aggiungi operazione host | 4.5 e precedenti | 4.6 e versioni successive |
|---|---|---|
| Aggiungi DAG senza IP in domini diversi o incrociati | Non supportato | Supportato |
| Aggiungi più IP DAG con nomi univoci, residenti nello stesso dominio o in domini diversi | Supportato | Supportato |
| Aggiungere più DAG IP o senza IP che hanno gli stessi nomi host e/o nomi DB in domini incrociati | Non supportato | Supportato |
| Aggiungi più DAG IP/senza IP con lo stesso nome e dominio incrociato | Non supportato | Supportato |
| Aggiungi più host autonomi con lo stesso nome e dominio incrociato | Non supportato | Supportato |

Il plug-in per Exchange dipende dal pacchetto plug-in SnapCenter per Windows e le versioni devono essere le stesse. Durante l'installazione del plug-in per Exchange, il pacchetto plug-in SnapCenter per Windows è selezionato per impostazione predefinita e viene installato insieme al provider hardware VSS.

Se SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati e si desidera installare Plug-in per Exchange sullo stesso Exchange Server, è necessario annullare la registrazione del provider hardware VSS utilizzato da SnapDrive per Windows perché non è compatibile con il provider hardware VSS installato con Plug-in per Exchange e SnapCenter Plug-ins Package per Windows. Per ulteriori informazioni, vedere "Come registrare manualmente il fornitore hardware Data ONTAP VSS" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che in alto sia selezionato **Host gestiti**.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, procedi come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Selezionare **Windows** come tipo di host.<br><br>SnapCenter Server aggiunge l'host e quindi installa sull'host il plug-in per Windows e il plug-in per Exchange, se non sono già installati.<br><br>Il plug-in per Windows e il plug-in per Exchange devono avere la stessa versione. Se in precedenza era installata una versione diversa del plug-in per Windows, SnapCenter aggiorna la versione come parte dell'installazione. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>Un indirizzo IP è supportato per gli host di dominio non attendibili solo se si risolve nel nome di dominio completo (FQDN).<br><br>Se si aggiunge un host tramite SnapCenter e fa parte di un sottodominio, è necessario fornire l'FQDN.<br><br>È possibile immettere gli indirizzi IP o il nome di dominio completo di uno dei seguenti:<br><br>• Host autonomo<br>• Exchange DAG<br><br>Per un Exchange DAG, è possibile:<br><br>◦ Aggiungere un DAG specificando il nome del DAG, l'indirizzo IP del DAG, il nome del nodo o l'indirizzo IP del nodo.<br>◦ Aggiungere il cluster DAG senza IP fornendo l'indirizzo IP o il nome di dominio completo (FQDN) di uno dei nodi del cluster DAG.<br>◦ Aggiungere un DAG senza IP che risiede nello stesso dominio o in un dominio diverso. È anche possibile aggiungere più DAG IP/IPless con lo stesso nome ma domini diversi.<br><br>Per un host autonomo o un Exchange DAG (tra domini o nello stesso dominio), si consiglia di fornire il nome di dominio completo (FQDN) o l'indirizzo IP dell'host o del DAG. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove.<br><br>La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, vedere le informazioni sulla creazione di una credenziale.<br><br>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Quando si seleziona Plug-in per Exchange, il plug-in SnapCenter per Microsoft SQL Server viene deselezionato automaticamente. Microsoft consiglia di non installare SQL Server ed Exchange Server sullo stesso sistema a causa della quantità di memoria utilizzata e dell'utilizzo di altre risorse richieste da Exchange.

6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta.<br><br>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il percorso predefinito è `C:\Program Files\NetApp\SnapCenter`.<br><br>Facoltativamente, è possibile personalizzare il percorso. |
| Aggiungi tutti gli host nel DAG | Selezionare questa casella di controllo quando si aggiunge un DAG. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br><br>Fornire il nome gMSA nel seguente formato: *nomedominio\nomeaccount$*.<br><br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo "Ignora controlli preliminari", l'host verrà convalidato per determinare se soddisfa i requisiti per l'installazione del plug-in. Se i requisiti minimi non vengono soddisfatti, verranno visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in `C:\Program Files\NetApp\SnapCenter` WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Monitorare l'avanzamento dell'installazione.

### Configura la porta personalizzata per la comunicazione NET TCP

Per impostazione predefinita, a partire dalla versione SnapCenter 6.0, il plug-in SnapCenter per Windows utilizza la porta 909 per la comunicazione NET TCP. Se la porta 909 è in uso, è possibile configurare un'altra porta per la comunicazione NET TCP.

**Passi**

1. Modificare il valore della chiave *NetTCPPort* situata in *C:\Programmi\ NetApp\ SnapCenter\ SnapCenter Plug-in per Microsoft Windows\vssproviders\navssprv.exe.config* con il numero di porta richiesto.
   `<add key="NetTCPPort" value="new_port_number" />`
2. Modificare il valore della chiave *NetTCPPort* situata in *C:\Programmi\ NetApp\ SnapCenter\ SnapCenter Plug-in per Microsoft Windows\SnapDriveService.dll.config* con il numero di porta richiesto.
   `<add key="NetTCPPort" value="new_port_number" />`
3. Annullare la registrazione del servizio *Data ONTAP VSS Hardware Provider* eseguendo il comando seguente:
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\navssprv.exe" -r service -u`

Verificare che il servizio non sia visualizzato nell'elenco dei servizi in *services.msc*.

4. Registrare il servizio *Data ONTAP VSS Hardware Provider* eseguendo il comando seguente:
   `"C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft Windows\vssproviders\navssprv.exe" -r service -a ".\LocalSystem"`

   Verificare se il servizio è ora visualizzato nell'elenco dei servizi in *services.msc*.

5. Riavviare il servizio *Plug-in per Windows*.

## Installa il plug-in per Exchange dall'host del server SnapCenter utilizzando i cmdlet di PowerShell

Dovresti installare il plug-in per Exchange dall'interfaccia utente grafica SnapCenter . Se non si desidera utilizzare l'interfaccia utente grafica, è possibile utilizzare i cmdlet di PowerShell sull'host del server SnapCenter o su un host remoto.

**Prima di iniziare**

- SnapCenter Server deve essere installato e configurato.
- Devi essere un amministratore locale sull'host o un utente con privilegi amministrativi.
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni per plug-in, installazione e disinstallazione, ad esempio SnapCenter Admin.
- Prima di installare il plug-in per Exchange, è necessario esaminare i requisiti di installazione e i tipi di configurazioni supportate.
- L'host su cui si desidera installare il plug-in per Exchange deve essere un host Windows.

**Passi**

1. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
2. Aggiungere l'host su cui si desidera installare il plug-in per Exchange utilizzando il cmdlet *Add-SmHost* con i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   L'host può essere un host autonomo o un DAG. Se si specifica un DAG, è obbligatorio il parametro *-IsDAG*.

3. Installare il plug-in per Exchange utilizzando il cmdlet *Install-SmHostPackage* con i parametri richiesti.

   Questo comando installa il plug-in per Exchange sull'host specificato e quindi registra il plug-in con SnapCenter.

## Installare il plug-in SnapCenter per Exchange in modo silenzioso dalla riga di comando

Dovresti installare il plug-in per Exchange dall'interfaccia utente SnapCenter . Tuttavia, se per qualche motivo non è possibile, è possibile eseguire il programma di installazione del

plug-in per Exchange in modalità automatica dalla riga di comando di Windows.

**Prima di iniziare**

- È necessario aver eseguito il backup delle risorse di Microsoft Exchange Server.
- È necessario aver installato i pacchetti plug-in SnapCenter .
- Prima di procedere all'installazione, è necessario eliminare la versione precedente del plug-in SnapCenter per Microsoft SQL Server.

  Per ulteriori informazioni, vedere "Come installare manualmente un plug-in SnapCenter direttamente dall'host del plug-in" .

**Passi**

1. Verificare se la cartella *C:\temp* esiste sull'host del plug-in e se l'utente connesso ha pieno accesso ad essa.
2. Scaricare il plug-in SnapCenter per Microsoft Windows da *C:\ProgramData\ NetApp\ SnapCenter\Package* Repository.

   Questo percorso è accessibile dall'host in cui è installato SnapCenter Server.
3. Copiare il file di installazione sull'host su cui si desidera installare il plug-in.
4. Da un prompt dei comandi di Windows sull'host locale, accedere alla directory in cui sono stati salvati i file di installazione del plug-in.
5. Immettere il seguente comando per installare il plug-in.

   *snapcenter_windows_host_plugin.exe"/silent /debuglog"<Percorso_Registro_Debug>" /log"<Percorso_Registro>" BI_SNAPCENTER_PORT=<Num> SUITE_INSTALLDIR="<Percorso_Directory_Installazione>" BI_SERVICEACCOUNT=<dominio\amministratore> BI_SERVICEPWD=<password> ISFeatureInstall=HPPW,SCW,SCE*

   Per esempio:

   *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\snapcenter_windows_host_plugin.exe"/silent /debuglog"C:\HPPW_SCSQL_Install.log" /log"C:\temp" BI_SNAPCENTER_PORT=8145 SUITE_INSTALLDIR="C:\Programmi\ NetApp\ SnapCenter" BI_SERVICEACCOUNT=dominio\amministratore BI_SERVICEPWD=password ISFeatureInstall=HPPW,SCW,SCE*

   Tutti i parametri passati durante l'installazione del plug-in per Exchange sono sensibili alle maiuscole e alle minuscole.

   Inserire i seguenti valori per le variabili:

| Variabile | Valore |
|---|---|
| */debuglog"<Percorso_registro_debug>* | Specificare il nome e il percorso del file di registro del programma di installazione della suite, come nell'esempio seguente:<br><br>*Setup.exe /debuglog"C:\PercorsoRegistro\setupexe.log* |
| BI_SNAPCENTER_PORT | Specificare la porta su cui SnapCenter comunica con SMCore. |
| SUITE_INSTALLDIR | Specificare la directory di installazione del pacchetto plug-in host. |
| BI_SERVICEACCOUNT | Specificare il plug-in SnapCenter per l'account del servizio Web di Microsoft Windows. |
| BI_SERVICEPWD | Specificare la password per l'account del servizio Web SnapCenter Plug-in per Microsoft Windows. |
| ISFeatureInstall | Specificare la soluzione da distribuire tramite SnapCenter sull'host remoto. |

6. Monitorare l'utilità di pianificazione di Windows, il file di registro di installazione principale *C:\Installdebug.log* e i file di installazione aggiuntivi in *C:\Temp*.
7. Monitorare la directory *%temp%* per verificare se i programmi di installazione *msiexe.exe* installano il software senza errori.

L'installazione del plug-in per Exchange registra il plug-in sull'host e non sul server SnapCenter . È possibile registrare il plug-in sul server SnapCenter aggiungendo l'host tramite l'interfaccia utente grafica SnapCenter o il cmdlet PowerShell. Dopo aver aggiunto l'host, il plug-in viene rilevato automaticamente.

## Monitorare lo stato di installazione del pacchetto plug-in SnapCenter

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
-

Completato con avvisi o non è stato possibile avviarlo a causa di avvisi

- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

> Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

#### Passi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e

identificare il certificato installato di recente tramite il nome dell'oggetto.

*Get-ChildItem -Percorso Cert:\LocalMachine\My*

b. Copia l'impronta digitale.

**Configurare il certificato CA con i servizi plug-in host di Windows**

## È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

**Abilita i certificati CA per i plug-in**

## È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.

- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

## Configurare SnapManager 7.x affinché Exchange e SnapCenter coesistano

Per consentire la coesistenza del plug-in SnapCenter per Microsoft Exchange Server con SnapManager per Microsoft Exchange Server, è necessario installare il plug-in SnapCenter per Microsoft Exchange Server sullo stesso Exchange Server su cui è installato SnapManager per Microsoft Exchange Server, disabilitare le pianificazioni di SnapManager per Exchange e configurare nuove pianificazioni e backup utilizzando il plug-in SnapCenter per Microsoft Exchange Server.

**Prima di iniziare**

- SnapManager per Microsoft Exchange Server e SnapDrive per Windows sono già installati e i backup di SnapManager per Microsoft Exchange Server sono presenti sul sistema e nella directory SnapInfo.
- Dovresti aver eliminato o recuperato i backup eseguiti da SnapManager per Microsoft Exchange Server che non ti servono più.
- Avresti dovuto sospendere o eliminare tutte le pianificazioni create da SnapManager per Microsoft Exchange Server dallo scheduler di Windows.
- Il plug-in SnapCenter per Microsoft Exchange Server e SnapManager per Microsoft Exchange Server possono coesistere sullo stesso Exchange Server, ma non è possibile aggiornare le installazioni esistenti SnapManager per Microsoft Exchange Server a SnapCenter.

  SnapCenter non fornisce un'opzione per l'aggiornamento.

- SnapCenter non supporta il ripristino dei database di Exchange da SnapManager per il backup di Microsoft Exchange Server.

  Se non si disinstalla SnapManager per Microsoft Exchange Server dopo l'installazione del plug-in SnapCenter per Microsoft Exchange Server e in seguito si desidera ripristinare un backup di SnapManager per Microsoft Exchange Server, è necessario eseguire passaggi aggiuntivi.

**Passi**

1. Utilizzando PowerShell su tutti i nodi DAG, determinare se SnapDrive per Windows VSS Hardware Provider è registrato: *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. Dalla directory SnapDrive , annullare la registrazione del provider hardware VSS da SnapDrive per Windows: *navssprv.exe -r service –u*
3. Verificare che il provider hardware VSS sia stato rimosso: *vssadmin list providers*
4. Aggiungere l'host di Exchange a SnapCenter, quindi installare il plug-in SnapCenter per Microsoft Windows e il plug-in SnapCenter per Microsoft Exchange Server.
5. Dalla directory del plug-in SnapCenter per Microsoft Windows su tutti i nodi DAG, verificare che il provider hardware VSS sia registrato: *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. Interrompere le pianificazioni di backup di SnapManager per Microsoft Exchange Server.
7. Utilizzando l'interfaccia utente grafica SnapCenter , è possibile creare backup su richiesta, configurare backup pianificati e configurare le impostazioni di conservazione.
8. Disinstallare SnapManager per Microsoft Exchange Server.

   Se non si disinstalla SnapManager per Microsoft Exchange Server ora e in seguito si desidera ripristinare

un backup SnapManager per Microsoft Exchange Server:

a. Annullare la registrazione del plug-in SnapCenter per Microsoft Exchange Server da tutti i nodi DAG: *navssprv.exe -r service -u*

```
C:\Program Files\NetApp\SnapCenter\SnapCenter Plug-in for Microsoft
Windows>navssprv.exe -r service -u
```

b. Dalla directory *C:\Programmi\ NetApp\ SnapDrive*, registrare SnapDrive per Windows su tutti i nodi DAG: *navssprv.exe -r service -a hostname\\username -p password*

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

## Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

## Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

# Prepararsi alla protezione dei dati

Prima di eseguire qualsiasi operazione di protezione dei dati, come backup, clonazione o ripristino, è necessario definire la strategia e configurare l'ambiente. È anche possibile configurare SnapCenter Server per utilizzare le tecnologie SnapMirror e SnapVault .

Per sfruttare i vantaggi della tecnologia SnapVault e SnapMirror , è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di archiviazione. Per eseguire queste attività è possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di archiviazione.

**Trova maggiori informazioni**

"Introduzione all'API REST"

## Prerequisiti per l'utilizzo del plug-in SnapCenter per Microsoft Exchange Server

Prima di utilizzare il plug-in per Exchange, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter.
- Configurare l'ambiente SnapCenter aggiungendo o assegnando connessioni al sistema di archiviazione e creando una credenziale.

  SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM supportato da SnapCenter deve avere un nome univoco.

- Aggiungere host, installare il plug-in SnapCenter per Microsoft Windows e il plug-in SnapCenter per Microsoft Exchange Server e scoprire (aggiornare) le risorse.
- Eseguire il provisioning dello storage lato host utilizzando il plug-in SnapCenter per Microsoft Windows.
- Se si utilizza SnapCenter Server per proteggere i database di Exchange che risiedono su VMware RDM LUN, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter. Per ulteriori informazioni, consultare la documentazione SnapCenter Plug-in for VMware vSphere .

  I VMDK non sono supportati.

- Spostare un database Microsoft Exchange Server esistente da un disco locale a un archivio supportato utilizzando gli strumenti di Microsoft Exchange.
- Se si desidera la replica del backup, impostare le relazioni SnapMirror e SnapVault .

Per gli utenti SnapCenter 4.1.1, la documentazione SnapCenter Plug-in for VMware vSphere 4.1.1 contiene informazioni sulla protezione dei database e dei file system virtualizzati. Per gli utenti SnapCenter 4.2.x, NetApp Data Broker 1.0 e 1.0.1, la documentazione contiene informazioni sulla protezione di database e file system virtualizzati mediante il SnapCenter Plug-in for VMware vSphere fornito dall'appliance virtuale NetApp Data Broker basata su Linux (formato Open Virtual Appliance). Per gli utenti SnapCenter 4.3.x, la documentazione SnapCenter Plug-in for VMware vSphere 4.3 contiene informazioni sulla protezione di database e file system virtualizzati mediante l'appliance virtuale SnapCenter Plug-in for VMware vSphere basata su Linux (formato Open Virtual Appliance).

"Documentazione SnapCenter Plug-in for VMware vSphere"

## Come vengono utilizzate risorse, gruppi di risorse e criteri per proteggere Exchange Server

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, ripristino e reseeding che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere database di cassette postali o gruppi di disponibilità del database (DAG) di Microsoft Exchange di cui si esegue il backup con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host o Exchange DAG e può includere un intero DAG o singoli database.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse

definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

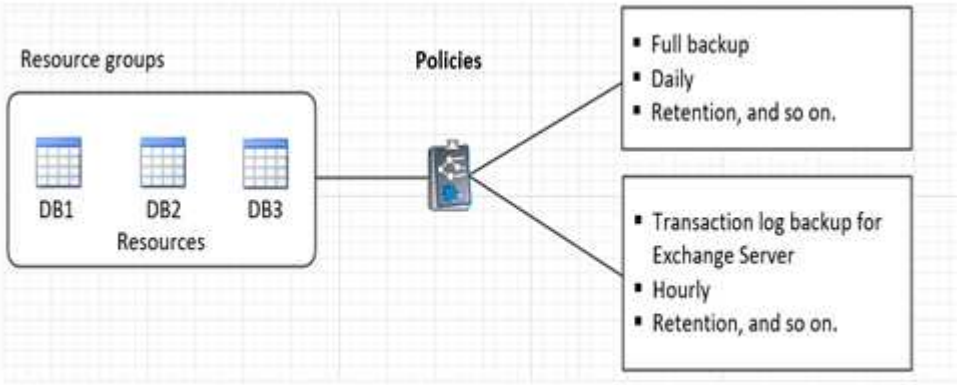
È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

In precedenza i gruppi di risorse erano noti come set di dati.

- Le policy specificano la frequenza di backup, la conservazione delle copie, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare una o più policy quando si esegue un backup su richiesta per una singola risorsa.

Pensa a un gruppo di risorse come a qualcosa che definisce *cosa* vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una politica come a qualcosa che definisce *come* vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database di un host, è possibile creare un gruppo di risorse che includa tutti i database nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno e un'altra pianificazione che esegua backup del registro ogni ora. L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:



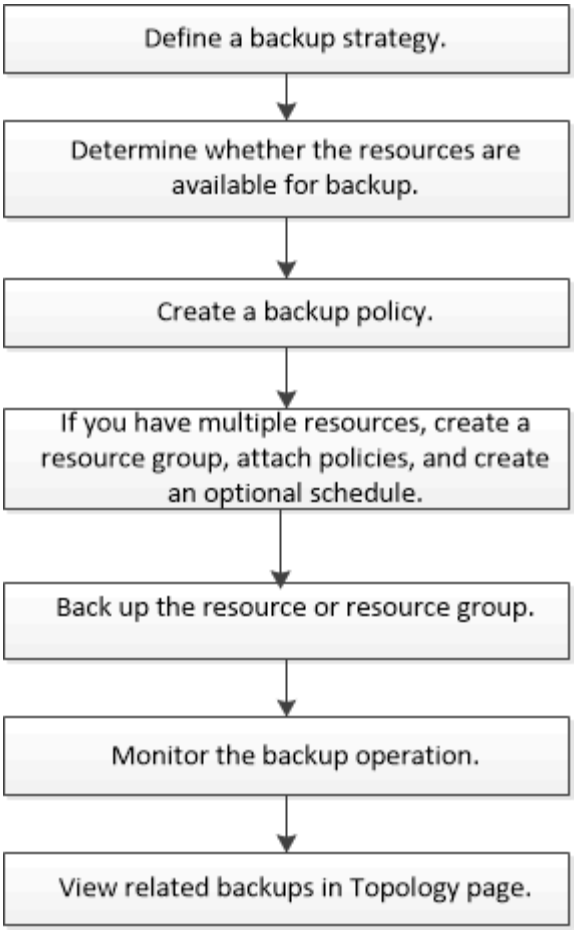

# Eseguire il backup delle risorse di Exchange

## Flusso di lavoro di backup

Quando installi il plug-in SnapCenter per Microsoft Exchange Server nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup delle risorse di Exchange.

È possibile pianificare più backup da eseguire contemporaneamente su più server. Le operazioni di backup e ripristino non possono essere eseguite contemporaneamente sulla stessa risorsa. Non sono supportate copie di backup attive e passive sullo stesso volume.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




## Verifica del database di Exchange e del backup

Il plug-in SnapCenter per Microsoft Exchange Server non fornisce la verifica del backup; tuttavia, è possibile utilizzare lo strumento Eseutil fornito con Exchange per verificare i database e i backup di Exchange.

Lo strumento Microsoft Exchange Eseutil è un'utilità della riga di comando inclusa nel server Exchange. L'utilità consente di eseguire controlli di coerenza per verificare l'integrità dei database e dei backup di Exchange.

**Procedura consigliata:** non è necessario eseguire controlli di coerenza sui database che fanno parte di una configurazione DAG (Database Availability Group) con almeno due repliche.

Per ulteriori informazioni, vedere "Documentazione di Microsoft Exchange Server" .

## Determina se le risorse di Exchange sono disponibili per il backup

Le risorse sono i database, i gruppi di disponibilità del database di Exchange gestiti dai plug-in installati. È possibile aggiungere tali risorse ai gruppi di risorse in modo da poter eseguire attività di protezione dei dati, ma prima è necessario identificare quali risorse sono disponibili. La determinazione delle risorse disponibili verifica anche che l'installazione del plug-in sia stata completata correttamente.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la creazione di connessioni al sistema di archiviazione, l'aggiunta di credenziali e l'installazione del plug-in per Exchange.
- Per sfruttare le funzionalità del software Single Mailbox Recovery, è necessario aver individuato il database attivo sul server Exchange in cui è installato il software Single Mailbox Recovery.
- Se i database risiedono su LUN VMware RDM, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter. IL "Documentazione SnapCenter Plug-in for VMware vSphere" ha più informazioni.

**Informazioni su questo compito**

- Non è possibile eseguire il backup dei database quando l'opzione **Stato generale** nella pagina Dettagli è impostata su Non disponibile per il backup. L'opzione **Stato generale** è impostata su Non disponibile per il backup quando si verifica una delle seguenti condizioni:
  - I database non si trovano su una LUN NetApp .
  - I database non sono in stato normale.

    I database non sono in stato normale quando si trovano nello stato di montaggio, smontaggio, risemina o ripristino in sospeso.
- Se si dispone di un gruppo di disponibilità del database (DAG), è possibile eseguire il backup di tutti i database nel gruppo eseguendo il processo di backup dal DAG.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare **Microsoft Exchange Server** dall'elenco a discesa dei plug-in situato nell'angolo in alto a sinistra della pagina Risorse.
2. Nella pagina Risorse, seleziona **Database**, **Gruppo di disponibilità del database** o **Gruppo di risorse** dall'elenco a discesa **Visualizza**.

   Tutti i database e i DAG vengono visualizzati con i rispettivi DAG o nomi host in formato FQDN, in modo da poter distinguere tra più database.

   Clic e seleziona il nome host e il server Exchange per filtrare le risorse. Puoi quindi fare clic per chiudere il riquadro del filtro.
3. Fare clic su **Aggiorna risorse**.

   Le risorse appena aggiunte, rinominate o eliminate vengono aggiornate nell'inventario di SnapCenter Server.

   È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

   Le risorse vengono visualizzate insieme a informazioni quali il nome della risorsa, il nome del gruppo di disponibilità del database, il server in cui il database è attualmente attivo, il server con copie, l'ora dell'ultimo backup e lo stato generale.

   - Se il database si trova su un archivio non NetApp , nella colonna Stato generale viene visualizzato Non disponibile per il backup.

     In un DAG, se la copia attiva del database si trova su un archivio non NetApp e se almeno una copia passiva del database si trova su un archivio NetApp , nella colonna **Stato generale** viene visualizzato Non protetto.

Non è possibile eseguire operazioni di protezione dei dati su un database che si trova su un tipo di archiviazione non NetApp .

- Se il database si trova su un archivio NetApp e non è protetto, nella colonna **Stato generale** viene visualizzato Non protetto.
- Se il database si trova su un sistema di archiviazione NetApp ed è protetto, l'interfaccia utente visualizza il messaggio Backup non eseguito nella colonna **Stato generale**.
- Se il database si trova su un sistema di archiviazione NetApp ed è protetto e se il backup è attivato per il database, l'interfaccia utente visualizza il messaggio Backup riuscito nella colonna **Stato generale**.

## Creare criteri di backup per i database di Exchange Server

È possibile creare un criterio di backup per le risorse di Exchange o per i gruppi di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di Microsoft Exchange Server oppure è possibile creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

**Prima di iniziare**

- Devi aver definito la tua strategia di protezione dei dati.

  Per maggiori dettagli, vedere le informazioni sulla definizione di una strategia di protezione dei dati per i database di Exchange.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione SnapCenter, l'aggiunta di host, l'identificazione delle risorse e la creazione di connessioni al sistema di archiviazione.
- È necessario aver aggiornato (rilevato) le risorse di Exchange Server.
- Se si replicano gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le macchine virtuali di archiviazione (SVM) sia per i volumi di origine che per quelli di destinazione.
- Se si desidera eseguire gli script di PowerShell in prescript e postscript, è necessario impostare il valore di `usePowershellProcessforScripts` parametro su true nel `web.config` file.

  Il valore predefinito è falso.

- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

- Una policy di backup è un insieme di regole che regolano il modo in cui vengono gestiti e conservati i backup, nonché la frequenza con cui viene eseguito il backup della risorsa o del gruppo di risorse. Inoltre, è possibile specificare le impostazioni dello script. Specificare le opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.
- La conservazione completa del backup è specifica di una determinata policy. Un database o una risorsa che utilizza la policy A con una conservazione del backup completo pari a 4 conserva 4 backup completi e non ha alcun effetto sulla policy B per lo stesso database o risorsa, che potrebbe avere una conservazione pari a 3 per conservare 3 backup completi.
- La conservazione del backup del log è efficace per tutte le policy e si applica a tutti i backup del log per un database o una risorsa. Pertanto, quando si esegue un backup completo utilizzando il criterio B, l'impostazione di conservazione del registro influisce sui backup del registro creati dal criterio A sullo stesso database o risorsa. Allo stesso modo, l'impostazione di conservazione dei log per la policy A influisce sui backup dei log creati dalla policy B sullo stesso database.

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

  **Procedura consigliata:** è consigliabile configurare il criterio di conservazione secondario in base al numero complessivo di backup completi e di registro che si desidera conservare. Quando si configurano criteri di conservazione secondari, tenere presente che quando i database e i log si trovano in volumi diversi, ogni backup può avere tre snapshot e quando i database e i log si trovano nello stesso volume, ogni backup può avere due snapshot.

- SnapLock

  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.

    Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.

  Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di backup e replica, procedere come segue:

   a. Scegli il tipo di backup:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Eseguire il backup dei file del database e dei registri delle transazioni richiesti | Selezionare **Backup completo e Backup del registro**.<br><br>Il backup dei database viene eseguito con il troncamento del log e tutti i log, compresi quelli troncati, vengono sottoposti a backup.<br><br>Questo è il tipo di backup consigliato. |

| Se lo desidera… | Fai questo… |
| --- | --- |
| Eseguire il backup dei file del database e dei registri delle transazioni non confermate | Selezionare **Backup completo**.<br><br>I database vengono sottoposti a backup con troncamento del log, mentre i log troncati non vengono sottoposti a backup. |
| Eseguire il backup di tutti i registri delle transazioni | Selezionare **Backup del registro**.<br><br>Viene eseguito il backup di tutti i registri delle transazioni sul file system attivo e non avviene alcun troncamento dei registri.<br><br>Una directory *scebackupinfo* viene creata sullo stesso disco del registro live. Questa directory contiene il puntatore alle modifiche incrementali per il database di Exchange e non è equivalente ai file di registro completi. |
| Eseguire il backup di tutti i file del database e dei registri delle transazioni senza troncare i file del registro delle transazioni | Selezionare **Copia backup**.<br><br>Viene eseguito il backup di tutti i database e di tutti i log e non viene effettuato alcun troncamento dei log. In genere questo tipo di backup viene utilizzato per effettuare il reseeding di una replica o per testare o diagnosticare un problema. |

ⓘ È necessario definire lo spazio necessario per i backup del registro in base alla conservazione completa dei backup e non in base alla conservazione Up-to-the-minute (UTM).

ⓘ Creare criteri di vault separati per registri e database quando si gestiscono volumi di Exchange (LUN) e impostare la conservazione per il criterio di registro su un numero doppio per ogni etichetta rispetto al criterio del database, utilizzando le stesse etichette. Per maggiori informazioni vedere, "I backup SnapCenter per Exchange conservano solo metà degli snapshot sul volume del registro di destinazione del Vault"

b. Nella sezione Impostazioni gruppo di disponibilità del database, seleziona un'azione:

| Per questo campo… | Fai questo… |
| --- | --- |
| Eseguire il backup delle copie attive | Selezionare questa opzione per eseguire il backup solo delle copie attive del database selezionato.<br><br>Per i gruppi di disponibilità del database (DAG), questa opzione esegue il backup solo delle copie attive di tutti i database nel DAG.<br><br>Le copie passive non vengono sottoposte a backup. |
| Copie di backup sui server da selezionare al momento della creazione del processo di backup | Selezionare questa opzione per eseguire il backup di tutte le copie dei database sui server selezionati, sia attivi che passivi.<br><br>Per i DAG, questa opzione esegue il backup delle copie attive e passive di tutti i database sui server selezionati. |

Nelle configurazioni cluster, i backup vengono conservati in ciascun nodo del cluster in base alle impostazioni di conservazione definite nella policy. Se il nodo proprietario del cluster cambia, verranno conservati i backup del nodo proprietario precedente. La conservazione è applicabile solo a livello di nodo.

c. Nella sezione Frequenza di pianificazione, seleziona uno o più tipi di frequenza: **Su richiesta**, **Oraria**, **Giornaliera**, **Settimanale** e **Mensile**.

È possibile specificare la pianificazione (data di inizio, data di fine) per le operazioni di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente di assegnare pianificazioni di backup diverse a ciascuna policy.

Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

a. Selezionare l'etichetta Criterio.

È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

b. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| Aggiorna SnapMirror dopo aver creato uno Snapshot locale | Selezionare questa opzione per conservare copie speculari dei set di backup su un altro volume (SnapMirror).<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror .<br><br>Il criterio solo primario non può essere utilizzato se SnapMirror ActiveSync è configurato per i volumi Exchange ONTAP . SnapCenter non lo consente. Dovresti abilitare l'opzione "Mirror".<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup di Exchange nella pagina Topologia" . |
| Aggiorna SnapVault dopo aver creato uno Snapshot locale | Selezionare questa opzione per eseguire la replica del backup da disco a disco. |
| Errore nel conteggio dei tentativi | Immettere il numero di tentativi di replica che devono essere eseguiti prima che il processo si interrompa. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

6. Nella pagina Conservazione, configura le impostazioni di conservazione.

   Le opzioni visualizzate dipendono dal tipo di backup e dalla frequenza selezionati in precedenza.

   Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante.

   Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.

a. Nella sezione Impostazioni di conservazione dei backup del registro, seleziona una delle seguenti opzioni:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Conservare solo un numero specifico di backup del registro | Selezionare **Numero di backup completi per i quali vengono conservati i registri** e specificare il numero di backup completi per i quali si desidera un ripristino aggiornato.<br><br>La conservazione aggiornata al minuto (UTM) si applica al backup del registro creato tramite backup completo o del registro. Ad esempio, se le impostazioni di conservazione UTM sono configurate per conservare i backup del registro degli ultimi 5 backup completi, verranno conservati i backup del registro degli ultimi 5 backup completi.<br><br>Le cartelle di registro create come parte dei backup completi e dei registri vengono eliminate automaticamente come parte di UTM. Non è possibile eliminare manualmente le cartelle di registro. Ad esempio, se l'impostazione di conservazione del backup completo o completo e del registro è impostata su 1 mese e la conservazione UTM è impostata su 10 giorni, la cartella del registro creata come parte di questi backup verrà eliminata come da UTM. Di conseguenza, saranno presenti solo le cartelle di registro degli ultimi 10 giorni e tutti gli altri backup saranno contrassegnati per il ripristino in un dato momento.<br><br>È possibile impostare il valore di conservazione UTM su 0 se non si desidera eseguire un ripristino aggiornato. Ciò consentirà l'operazione di ripristino in un dato momento.<br><br>**Procedura consigliata:** è preferibile che l'impostazione sia uguale all'impostazione per Snapshot totali (backup completi) nella sezione Impostazioni di conservazione dei backup completi. Ciò garantisce che i file di registro vengano conservati per ogni backup completo. |
| Conservare le copie di backup per un numero specifico di giorni | Selezionare l'opzione **Conserva i backup del registro per ultimi** e specificare il numero di giorni per cui conservare le copie di backup del registro.<br><br>Vengono conservati i backup del log fino al numero di giorni dei backup completi. |

| Se lo desidera… | Fai questo… |
| --- | --- |
| Periodo di blocco degli snapshot | Selezionare **Periodo di blocco della copia snapshot** e selezionare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

Se hai selezionato **Backup del registro** come tipo di backup, i backup del registro vengono conservati come parte delle impostazioni di conservazione aggiornate per i backup completi.

b. Nella sezione Impostazioni di conservazione del backup completo, seleziona una delle seguenti opzioni per i backup su richiesta, quindi selezionane un'altra per i backup completi:

| Per questo campo… | Fai questo… |
| --- | --- |
| Conserva solo un numero specifico di snapshot | Se si desidera specificare il numero di backup completi da conservare, selezionare l'opzione **Numero totale di copie snapshot da conservare** e specificare il numero di snapshot (backup completi) da conservare.<br><br>Se il numero di backup completi supera il numero specificato, i backup completi che superano il numero specificato vengono eliminati, partendo dalle copie più vecchie. |
| Conservare i backup completi per un numero specifico di giorni | Selezionare l'opzione **Conserva copie snapshot per** e specificare il numero di giorni per cui conservare gli snapshot (backup completi). |
| Periodo di blocco dello snapshot primario | Selezionare **Periodo di blocco della copia snapshot primaria** e selezionare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |
| Periodo di blocco dello snapshot secondario | Selezionare **Periodo di blocco della copia snapshot secondaria** e selezionare giorni, mesi o anni. |

Se si dispone di un database con solo backup del log e nessun backup completo su un host in una configurazione DAG, i backup del log vengono conservati nei seguenti modi:

- Per impostazione predefinita, SnapCenter trova il backup completo più vecchio per questo database in tutti gli altri host del DAG ed elimina tutti i backup del registro su questo host eseguiti prima del backup completo.
- È possibile ignorare il comportamento di conservazione predefinito sopra indicato per un database su un host in un DAG con solo backup del log aggiungendo la chiave **MaxLogBackupOnlyCountWithoutFullBackup** nel file *C:\Program Files\ NetApp\ SnapCenter*

*WebApp\web.config*.

```
<add key="MaxLogBackupOnlyCountWithoutFullBackup" value="10">
```

Nell'esempio, il valore 10 significa che si conservano fino a 10 backup del log sull'host.

7. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di backup.
   - Gli argomenti di backup predefiniti includono "$Database" e "$ServerInstance".
   - Gli argomenti di backup PostScript includono "$Database", "$ServerInstance", "$BackupName", "$LogDirectory" e "$LogSnapshot".

     È possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

8. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare gruppi di risorse e allegare criteri per i server Exchange

Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire e la pianificazione della protezione.

**Informazioni su questo compito**

- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi database senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi database a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in Microsoft Exchange Server dall'elenco.

2. Nella pagina Risorse, seleziona **Database** dall'elenco **Visualizza**.

   Se hai aggiunto di recente una risorsa a SnapCenter, fai clic su **Aggiorna risorse** per visualizzare la risorsa appena aggiunta.

3. Fare clic su **Nuovo gruppo di risorse**.
4. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere il nome del gruppo di risorse.<br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Facoltativo: inserisci un nome e un formato personalizzati per lo snapshot.<br>Ad esempio, *customtext_resourcegroup_policy_hostname* o *resourcegroup_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

5. Nella pagina Risorse, procedere come segue:
   a. Selezionare il tipo di risorsa e il gruppo di disponibilità del database dagli elenchi a discesa per filtrare l'elenco delle risorse disponibili.

      Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle Risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

      Nelle sezioni Risorse disponibili e Risorse selezionate, il nome del database viene visualizzato con l'FQDN dell'host. Questo FQDN indica solo che il database è attivo su quell'host specifico e potrebbe non eseguire il backup su questo host. È necessario selezionare uno o più server di backup dall'opzione Selezione server, dove si desidera eseguire il backup nel caso in cui sia stata selezionata l'opzione **Copie di backup sui server da selezionare al momento della creazione del processo di backup** nella policy.

   b. Digita il nome della risorsa nella casella di testo di ricerca oppure scorri per individuare una risorsa.
   c. Per spostare le risorse dalla sezione Risorse disponibili alla sezione Risorse selezionate, eseguire uno dei seguenti passaggi:
      - Selezionare **Seleziona automaticamente tutte le risorse sullo stesso volume di archiviazione** per spostare tutte le risorse sullo stesso volume nella sezione Risorse selezionate.

- Selezionare le risorse dalla sezione Risorse disponibili, quindi fare clic sulla freccia destra per spostarle nella sezione Risorse selezionate.

  I gruppi di risorse di SnapCenter per Microsoft Exchange Server non possono avere più di 30 database per snapshot. Se in un gruppo di risorse sono presenti più di 30 database, viene creato un secondo Snapshot per i database aggiuntivi. Pertanto, vengono creati 2 sotto-processi sotto il processo di backup principale. Per i backup con replica secondaria, mentre è in corso l'aggiornamento SnapMirror o SnapVault , potrebbero verificarsi scenari in cui l'aggiornamento di entrambi i sottoprocessi si sovrappone. Il processo di backup principale continua a essere eseguito all'infinito, anche se i registri indicano che il processo è stato completato.

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Se un criterio contiene l'opzione **Esegui copie di backup sui server da selezionare al momento della creazione del processo di backup**, viene visualizzata un'opzione di selezione del server per selezionare uno o più server. L'opzione di selezione del server elencherà solo il server in cui si trova il database selezionato nello storage NetApp .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Nella sezione Configura pianificazioni per policy selezionate, fai clic su + **nella colonna *Configura pianificazioni** per la policy per la quale si desidera configurare la pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per la policy *nome_policy*, configurare la pianificazione specificando la data di inizio, la data di scadenza e la frequenza, quindi fare clic su **OK**.

      È necessario effettuare questa operazione per ogni frequenza indicata nella polizza. Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate** nella sezione Configura pianificazioni per policy selezionate.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente o il comando PowerShell `Set-SmSmtpServer` .

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

8. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per Exchange Server

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup e il ripristino.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell utilizzando `Open-SmConnection` cmdlet.

   Questo esempio apre una sessione di PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Creare una nuova connessione al sistema di archiviazione utilizzando `Add-SmStorageConnection` cmdlet.

   Questo esempio crea una nuova connessione al sistema di archiviazione:

   ```
   PS C:\> Add-SmStorageConnection -SVM test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Crea un nuovo account Esegui come utilizzando `Add-Credential` cmdlet.

   Questo esempio crea un nuovo account RunAs denominato ExchangeAdmin con credenziali Windows:

   ```
   PS C:> Add-SmCredential -Name ExchangeAdmin -AuthMode Windows
   -Credential sddev\administrator
   ```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni

possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei database di Exchange

Se un database non fa parte di alcun gruppo di risorse, è possibile eseguire il backup del database o del gruppo di disponibilità del database dalla pagina Risorse.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- È necessario aver assegnato l'aggregato utilizzato dall'operazione di backup all'SVM utilizzato dal database.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se si desidera eseguire il backup di un database o di un gruppo di disponibilità del database che dispone di una copia del database attiva/passiva su uno storage NetApp e non NetApp e si è selezionata l'opzione **Esegui backup copie attive** o **Esegui backup copie sui server da selezionare durante la creazione del processo di backup** nella policy, i processi di backup entreranno in stato di avviso. Il backup avrà esito positivo per la copia del database attivo/passivo su storage NetApp , mentre non avrà esito positivo per la copia del database attivo/passivo su storage non NetApp .

**Migliore pratica:** non eseguire backup di database attivi e passivi contemporaneamente. Potrebbe verificarsi una condizione di competizione e uno dei backup potrebbe non riuscire.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il **plug-in di Microsoft Exchange Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di disponibilità del database** dall'elenco **Visualizza**.

   Nella pagina Risorse, il L'icona indica che il database si trova su un archivio non NetApp .

   In un DAG, se una copia attiva del database si trova su uno storage non NetApp e almeno una copia passiva del database risiede su uno storage NetApp , è possibile proteggere il database.

   Clicca * *, quindi selezionare il nome host e il tipo di database per filtrare le risorse. Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

   - Se si desidera eseguire il backup di un database, fare clic sul nome del database.
     i. Se è visualizzata la vista Topologia, fare clic su **Proteggi**.
     ii. Se viene visualizzata la procedura guidata Database - Proteggi risorsa, procedere al passaggio 3.
   - Se si desidera eseguire il backup di un gruppo di disponibilità del database, fare clic sul nome del gruppo di disponibilità del database.
3. Se si desidera specificare un nome Snapshot personalizzato, nella pagina Risorse selezionare la casella di controllo **Usa formato nome personalizzato per copia Snapshot**, quindi immettere un formato nome personalizzato che si desidera utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
4. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * *.

      Se un criterio contiene l'opzione **Esegui copie di backup sui server da selezionare al momento della creazione del processo di backup**, viene visualizzata un'opzione di selezione del server per selezionare uno o più server. L'opzione di selezione del server elencherà solo il server in cui si trova il database selezionato su uno storage NetApp .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clicca * * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

   Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

5. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Allega report attività**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

6. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia del database.

7. Fare clic su **Esegui backup ora**.
8. Nella pagina Backup, procedere come segue:
   a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
9. Monitorare l'avanzamento del backup facendo doppio clic sul processo nel riquadro Attività nella parte inferiore della pagina per visualizzare la pagina Dettagli processo.
   - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

     Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

   - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

     Per aumentare la dimensione dell'heap Java, individuare il file di script */opt/netapp/init_scripts/scvservice*. In quello script, il comando *do_start method* avvia il servizio plug-in SnapCenter VMware. Aggiornare il comando come segue: *Java -jar -Xmx8192M -Xms4096M*

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

Viene visualizzata la richiesta di nome utente e password.

2. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea un nuovo criterio di backup con un backup completo e un backup del registro di tipo Exchange:

```
C:\PS> Add-SmPolicy -PolicyName SCE_w2k12_Full_Log_bkp_Policy
-PolicyType Backup -PluginPolicytype SCE -SceBackupType
FullBackupAndLogBackup -BackupActiveCopies
```

   Questo esempio crea un nuovo criterio di backup con un backup completo orario e un backup del registro di tipo Exchange:

```
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'}
```

   Questo esempio crea un nuovo criterio di backup per eseguire il backup solo dei registri di Exchange:

```
Add-SmPolicy -PolicyName SCE_w2k12_Log_bkp_Policy -PolicyType Backup
-PluginPolicytype SCE -SceBackupType LogBackup -BackupActiveCopies
```

3. Scopri le risorse host utilizzando il cmdlet Get-SmResources.

   Questo esempio rileva le risorse per il plug-in di Microsoft Exchange Server sull'host specificato:

```
C:\PS> Get-SmResources -HostName vise-f6.sddev.mycompany.com
-PluginCode SCE
```

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse di backup del database di Exchange Server con i criteri e le risorse specificati:

```
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_Lo
g_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'}
```

Questo esempio crea un nuovo gruppo di risorse di backup del gruppo di disponibilità del database di Exchange (DAG) con i criteri e le risorse specificati:

```
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_Lo
g_bkp_Policy -Resources @{"Host"="DAGSCE0102";"Type"="Database
Availability Group";"Names"="DAGSCE0102"}
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
C:\PS> New-SmBackup -ResourceGroupName SCE_w2k12_bkp_RG -Policy
SCE_w2k12_Full_Log_bkp_Policy
```

Questo esempio crea un nuovo backup su un archivio secondario:

```
New-SMBackup -DatasetName ResourceGroup1 -Policy
Secondary_Backup_Policy4
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

Questo esempio visualizza un report riepilogativo di tutti i lavori eseguiti nella data specificata:

```
C:\PS> Get-SmJobSummaryReport -Date ?1/27/2018?
```

Questo esempio visualizza un report riepilogativo del lavoro per un ID lavoro specifico:

```
C:\PS> Get-SmJobSummaryReport -JobId 168
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse di Exchange

Un gruppo di risorse è una raccolta di risorse su un host o un Exchange DAG e può includere un intero DAG o singoli database. È possibile eseguire il backup dei gruppi di risorse dalla pagina Risorse.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- È necessario aver assegnato l'aggregato utilizzato dall'operazione di backup alla macchina virtuale di archiviazione (SVM) utilizzata dal database.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Se un gruppo di risorse ha più database da host diversi, l'operazione di backup su alcuni host potrebbe iniziare in ritardo a causa di problemi di rete. Dovresti configurare il valore di `MaxRetryForUninitializedHosts` In `web.config` utilizzando il `Set-SmConfigSettings` Cmdlet di PowerShell.
- In un gruppo di risorse, se si include un database o un gruppo di disponibilità del database che ha una copia del database attiva/passiva su uno storage NetApp e non NetApp e si è selezionata l'opzione **Esegui backup copie attive** o **Esegui backup copie sui server da selezionare durante la creazione del processo di backup** nella policy, i processi di backup entreranno in stato di avviso.

  Il backup avrà esito positivo per la copia del database attivo/passivo su storage NetApp , mentre non avrà esito positivo per la copia del database attivo/passivo su storage non NetApp .

**Informazioni su questo compito**

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il **plug-in di Microsoft Exchange Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su * *, quindi selezionando il tag. Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi fai clic su **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

b. Fare clic su **Backup**.

5. Monitorare l'avanzamento del backup facendo doppio clic sul processo nel riquadro Attività nella parte inferiore della pagina per visualizzare la pagina Dettagli processo.

## Monitorare le operazioni di backup

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

### Monitorare le operazioni nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup per il database di Exchange

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup di Exchange nella pagina Topologia

Quando ci si prepara a eseguire il backup di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup sugli archivi primari e secondari.

**Informazioni su questo compito**

Nella pagina Topologia è possibile visualizzare tutti i backup disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e quindi selezionarli per eseguire operazioni di protezione dei dati.

È possibile esaminare l'icona seguente nella vista Gestisci copie per determinare se i backup sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup disponibili sullo storage primario.
- visualizza il numero di backup replicati sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup replicati sullo storage secondario mediante la tecnologia SnapVault .
  - Il numero di backup visualizzato include i backup eliminati dall'archivio secondario.

    Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

> **Procedura consigliata:** per garantire che venga visualizzato il numero corretto di backup replicati, consigliamo di aggiornare la topologia.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona il database, la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli del database o dalla vista dei dettagli del gruppo di risorse.

Se la risorsa è protetta, viene visualizzata la pagina Topologia della risorsa selezionata.

4. Consultare la sezione della scheda Riepilogo per visualizzare un riepilogo del numero di backup disponibili sullo storage primario e secondario.

   Nella sezione Scheda Riepilogo vengono visualizzati il numero totale di backup e il numero totale di backup del registro.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

   - Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault viene configurato automaticamente sulla nuova destinazione primaria dopo il failover.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** dall'archivio primario o secondario per visualizzare i dettagli di un backup.

   I dettagli dei backup vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, ridenominazione ed eliminazione.

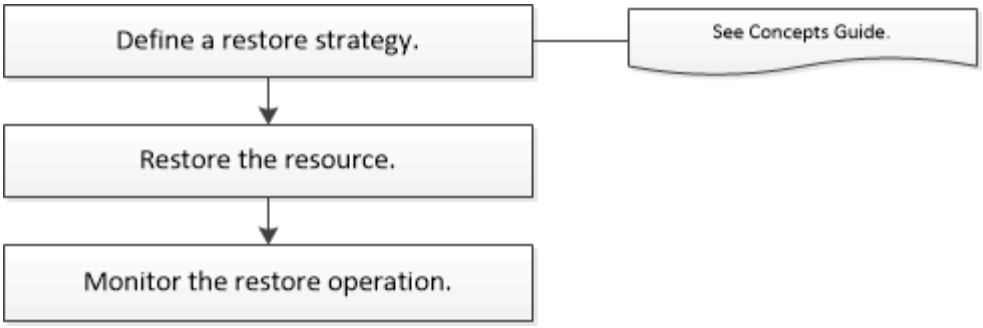
   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario. L'eliminazione degli snapshot è gestita dalle impostazioni di conservazione ONTAP .

# Ripristinare le risorse di Exchange

## Ripristina flusso di lavoro

È possibile utilizzare SnapCenter per ripristinare i database di Exchange ripristinando uno o più backup nel file system attivo.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire le operazioni di ripristino del database di Exchange:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup e ripristino. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

## Requisiti per il ripristino di un database di Exchange

Prima di ripristinare un database di Exchange Server da un backup del plug-in SnapCenter per Microsoft Exchange Server, è necessario assicurarsi che siano soddisfatti diversi requisiti.

Per utilizzare completamente la funzionalità di ripristino, è necessario aggiornare sia SnapCenter Server che SnapCenter Plug-in per il database di Exchange alla versione 4.6.

- Prima di poter ripristinare un database, Exchange Server deve essere online e in esecuzione.
- I database devono essere presenti sul server Exchange.

  Il ripristino dei database eliminati non è supportato.

- Le pianificazioni SnapCenter per il database devono essere sospese.
- Il server SnapCenter e l'host del plug-in SnapCenter per Microsoft Exchange Server devono essere connessi allo storage primario e secondario che contiene i backup che si desidera ripristinare.

## Ripristinare i database di Exchange

È possibile utilizzare SnapCenter per ripristinare i database Exchange sottoposti a backup.

**Prima di iniziare**

- È necessario aver eseguito il backup dei gruppi di risorse, del database o dei gruppi di disponibilità del database (DAG).
- Quando il database di Exchange viene migrato in un'altra posizione, l'operazione di ripristino non funziona per i vecchi backup.
- Se si replicano gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato gli SVM sia per i volumi di origine che per quelli di destinazione.
- In un DAG, se una copia attiva del database si trova su uno storage non NetApp e si desidera eseguire il ripristino dal backup della copia passiva del database che si trova su uno storage NetApp , è necessario rendere la copia passiva (storage NetApp ) come copia attiva, aggiornare le risorse ed eseguire l'operazione di ripristino.

Esegui il `Move-ActiveMailboxDatabase` comando per trasformare la copia passiva del database in una copia attiva del database.

IL "Documentazione Microsoft" contiene informazioni su questo comando.

**Informazioni su questo compito**

- Quando si esegue un'operazione di ripristino su un database, il database viene rimontato sullo stesso host e non viene creato alcun nuovo volume.
- I backup a livello di DAG devono essere ripristinati dai singoli database.
- Il ripristino completo del disco non è supportato quando sono presenti file diversi dal file del database di Exchange (.edb).

  Il plug-in per Exchange non esegue un ripristino completo su un disco se il disco contiene file di Exchange come quelli utilizzati per la replica. Quando un ripristino completo potrebbe avere ripercussioni sulla funzionalità di Exchange, il plug-in per Exchange esegue una singola operazione di ripristino del file.

- Il plug-in per Exchange non è in grado di ripristinare le unità crittografate con BitLocker.
- SCRIPTS_PATH viene definito utilizzando la chiave PredefinedWindowsScriptsDirectory che si trova nel file SMCoreServiceHost.exe.Config dell'host del plug-in.

  Se necessario, è possibile modificare questo percorso e riavviare il servizio SMcore. Per motivi di sicurezza, si consiglia di utilizzare il percorso predefinito.

  Il valore della chiave può essere visualizzato da Swagger tramite l'API: API /4.7/configsettings

  È possibile utilizzare l'API GET per visualizzare il valore della chiave. L'API SET non è supportata.

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse** nell'angolo in alto a sinistra della pagina Risorse.
2. Selezionare il plug-in Exchange Server dall'elenco a discesa.
3. Nella pagina Risorse, seleziona **Database** dall'elenco Visualizza.
4. Selezionare il database dall'elenco.
5. Dalla vista Gestisci copie, seleziona **Backup** dalla tabella Backup primari, quindi fai clic su * *.
6. Nella pagina Opzioni, seleziona una delle seguenti opzioni di backup del registro:

| Opzione | Descrizione |
|---|---|
| Tutti i backup del registro | Selezionare **Tutti i backup del registro** per eseguire un'operazione di ripristino del backup aggiornata al minuto per ripristinare tutti i backup del registro disponibili dopo il backup completo. |
| Tramite backup del registro fino a | Selezionare **Per backup del log fino a** per eseguire un'operazione di ripristino in un punto temporale specifico, che ripristina il database in base ai backup del log fino al log selezionato.<br>Il numero di log visualizzati nell'elenco a discesa si basa su UTM. Ad esempio, se la conservazione del backup completo è 5 e la conservazione UTM è 3, il numero di backup del log disponibili è 5, ma nel menu a discesa saranno elencati solo 3 log per eseguire l'operazione di ripristino. |
| Entro una data specifica fino a | Selezionare **In base a una data specifica fino a** per specificare la data e l'ora fino alle quali i registri delle transazioni vengono applicati al database ripristinato. Questa operazione di ripristino in un dato momento ripristina le voci del registro delle transazioni registrate fino all'ultimo backup nella data e ora specificate. |
| Nessuno | Selezionare **Nessuno** quando è necessario ripristinare solo il backup completo senza alcun backup del registro. |

È possibile eseguire una delle seguenti azioni:

- **Recupera e monta il database dopo il ripristino** - Questa opzione è selezionata per impostazione predefinita.
- **Non verificare l'integrità dei registri delle transazioni nel backup prima del ripristino** - Per impostazione predefinita, SnapCenter verifica l'integrità dei registri delle transazioni in un backup prima di eseguire un'operazione di ripristino.

  **Migliore pratica:** non selezionare questa opzione.

7. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di ripristino.

   Gli argomenti predefiniti per il ripristino includono $Database e $ServerInstance.

   Gli argomenti PostScript da ripristinare includono $Database, $ServerInstance, $BackupName, $LogDirectory e $TargetServerInstance.

   È possibile eseguire uno script per aggiornare le trap SNMP, automatizzare gli avvisi, inviare registri e così via.

   Il percorso prescripts o postscripts non deve includere unità o condivisioni. Il percorso dovrebbe essere relativo a SCRIPTS_PATH.

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. È possibile visualizzare lo stato del processo di ripristino espandendo il pannello Attività nella parte inferiore della pagina.

    È necessario monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

Quando si ripristina un database attivo da un backup, il database passivo potrebbe entrare in stato di sospensione o errore se c'è un ritardo tra la replica e il database attivo.

Il cambiamento di stato può verificarsi quando la catena di log del database attivo si biforca e inizia una nuova diramazione che interrompe la replicazione. Exchange Server tenta di riparare la replica, ma se non ci riesce, dopo il ripristino è necessario creare un nuovo backup e quindi ripetere il seeding della replica.

**Cmdlet di PowerShell**

**Passi**

1. Avviare una sessione di connessione con il server SnapCenter per un utente specificato utilizzando `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl
https://snapctr.demo.netapp.com:8146/
```

2. Recupera le informazioni su uno o più backup che desideri ripristinare utilizzando `Get-SmBackup` cmdlet.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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. Ripristinare i dati dal backup utilizzando `Restore-SmBackup` cmdlet.

   Questo esempio ripristina un backup aggiornato:

```
C:\PS> Restore-SmBackup -PluginCode SCE -AppObjectId 'sce-w2k12-
exch.sceqa.com\sce-w2k12-exch_DB_2' -BackupId 341
-IsRecoverMount:$true
```

   Questo esempio ripristina un backup puntuale:

```
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
```

   Questo esempio ripristina un backup su un archivio secondario nella storia primaria:

```
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
```

   IL `-archive` Il parametro consente di specificare i volumi primario e secondario che si desidera utilizzare per il ripristino.

IL `-IsRecoverMount:$true` Il parametro consente di montare il database dopo il ripristino.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Recupero granulare di e-mail e caselle di posta

Il software Single Mailbox Recovery (SMBR) consente di ripristinare e recuperare e-mail o cassette postali anziché l'intero database di Exchange.

Ripristinare l'intero database solo per recuperare una singola e-mail richiederebbe molto tempo e risorse. SMBR aiuta a recuperare rapidamente le e-mail creando una copia clone dello Snapshot e quindi utilizzando le API Microsoft per montare la casella di posta in SMBR. Per informazioni su come utilizzare SMBR, vedere "Guida all'amministrazione SMBR" .

Per ulteriori informazioni su SMBR, fare riferimento a quanto segue:

- "Come ripristinare manualmente un singolo elemento con SMBR (applicabile anche ai ripristini di Ontrack Power Control)"
- "Come ripristinare da un archivio secondario in SMBR con SnapCenter"
- "Recupero della posta di Microsoft Exchange da SnapVault tramite SMBR"

## Ripristinare un database di Exchange Server da un archivio secondario

È possibile ripristinare un database di Exchange Server sottoposto a backup da un archivio secondario (mirror o vault).

È necessario aver replicato gli snapshot dall'archivio primario a un archivio secondario.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare **Plug-in di Microsoft Exchange Server** dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco a discesa **Visualizza**.
3. Selezionare il database o il gruppo di risorse.

   Viene visualizzata la pagina della topologia del database o del gruppo di risorse.
4. Nella sezione Gestisci copie, seleziona **Backup** dal sistema di archiviazione secondario (mirror o vault).
5. Selezionare il backup dall'elenco, quindi fare clic su .

6. Nella pagina Posizione, seleziona il volume di destinazione per il ripristino della risorsa selezionata.
7. Completare la procedura guidata di ripristino, rivedere il riepilogo e quindi fare clic su **Fine**.

## Reinizializzare una replica di un nodo Exchange passivo

Se è necessario effettuare il reseeding di una copia replica, ad esempio quando una copia è danneggiata, è possibile effettuare il reseeding all'ultimo backup utilizzando la funzionalità di reseeding in SnapCenter.

**Prima di iniziare**

È necessario aver creato un backup del database di cui si desidera effettuare il reinizializzazione.

+ Per evitare ritardi tra i nodi, è possibile creare un nuovo backup prima di eseguire un'operazione di reseeding oppure scegliere l'host con il backup più recente.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare **Plug-in di Microsoft Exchange Server** dall'elenco.
2. Nella pagina Risorse, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per effettuare il reseeding di un singolo database | Selezionare **Database** dall'elenco Visualizza. |
| Per effettuare il reseeding dei database in un DAG | Selezionare **Gruppo di disponibilità del database** dall'elenco Visualizza. |

3. Seleziona la risorsa che vuoi riseminare.
4. Nella pagina Gestisci copie, fare clic su **Reseed**.
5. Dall'elenco delle copie di database non integre nella procedura guidata Reseed, seleziona quella di cui vuoi effettuare il reseeding, quindi fai clic su **Avanti**.
6. Nella finestra Host, seleziona l'host con il backup da cui vuoi effettuare il reseeding, quindi fai clic su **Avanti**.
7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

8. Rivedi il riepilogo e poi clicca su **Fine**.
9. È possibile visualizzare lo stato del lavoro espandendo il pannello Attività nella parte inferiore della pagina.

> L'operazione di reseeding non è supportata se la copia passiva del database risiede su uno storage non NetApp .

## Ripristinare il seeding di una replica utilizzando i cmdlet di PowerShell per il database di Exchange

È possibile utilizzare i cmdlet di PowerShell per ripristinare una replica non integra utilizzando la copia più recente sullo stesso host oppure la copia più recente da un host alternativo.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Avviare una sessione di connessione con il server SnapCenter per un utente specificato utilizzando `Open-SmConnection` cmdlet.

```
Open-smconnection  -SMSbaseurl  https:\\snapctr.demo.netapp.com:8146/
```

2. Ripristinare il database utilizzando `reseed-SmDagReplicaCopy` cmdlet.

   In questo esempio viene effettuata la reinizializzazione della copia non riuscita del database denominata execdb sull'host "mva-rx200.netapp.com" utilizzando l'ultimo backup presente su tale host.

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb
```

   Questo esempio effettua il seeding della copia non riuscita del database denominata execdb utilizzando l'ultimo backup del database (produzione/copia) su un host alternativo "mva-rx201.netapp.com".

```
reseed-SmDagReplicaCopy -ReplicaHost "mva-rx200.netapp.com" -Database
execdb -BackupHost "mva-rx201.netapp.com"
```

## Monitorare le operazioni di ripristino

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso

- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

## Annulla le operazioni di ripristino per il database di Exchange

### È possibile annullare i processi di ripristino in coda.

Per annullare le operazioni di ripristino, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del processo.

**Informazioni su questo compito**

- È possibile annullare un'operazione di ripristino in coda dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di ripristino in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di ripristino in coda.
- Il pulsante **Annulla processo** è disabilitato per le operazioni di ripristino che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di ripristino in coda degli altri membri mentre utilizzi quel ruolo.

**Fare un passo**

Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | 1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>2. Seleziona il lavoro e clicca su **Annulla lavoro**. |
| Riquadro attività | 1. Dopo aver avviato l'operazione di ripristino, fare clic su nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>2. Selezionare l'operazione.<br>3. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

# Proteggi IBM Db2

## Plug-in SnapCenter per IBM Db2

### Panoramica del plug-in SnapCenter per IBM Db2

Il plug-in SnapCenter per IBM Db2 Database è un componente lato host del software NetApp SnapCenter software che consente la gestione della protezione dei dati basata sulle applicazioni dei database IBM Db2. Il plug-in per IBM Db2 Database automatizza il backup, il ripristino e la clonazione dei database IBM Db2 nel tuo ambiente SnapCenter .

- SnapCenter 6.0 supporta IBM Db2 10.5 e versioni successive.
- SnapCenter 6.0.1 supporta IBM Db2 9.7.x e versioni successive. Inoltre, a partire da SnapCenter 6.0.1, è supportato IBM Db2 su AIX.

SnapCenter supporta configurazioni Db2 a istanza singola e multi-istanza. È possibile utilizzare il plug-in per IBM Db2 Database sia in ambienti Linux che Windows. Negli ambienti Windows, Db2 sarà supportato come risorsa manuale.

L'ambiente Db2 pureScale e i sistemi Db2 multi-nodo (DPF) non sono supportati.

Una volta installato il plug-in per IBM Db2 Database, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror di set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard.

Il plug-in SnapCenter per Db2 supporta NFS e SAN su layout di archiviazione ONTAP e Azure NetApp File.

Sono supportati i layout di archiviazione virtuale VMDK, vVol e RDM.

### Cosa puoi fare utilizzando il plug-in SnapCenter per IBM Db2

Quando installi il plug-in per IBM Db2 Database nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei database IBM Db2 e delle relative risorse. È anche possibile eseguire attività di supporto a tali operazioni.

- Aggiungere database.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

### Funzionalità del plug-in SnapCenter per IBM Db2

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp sul sistema

di storage. Per lavorare con il plug-in per IBM Db2 Database, utilizzare l'interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare operazioni di backup, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- **Tecnologia di copia snapshot NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia snapshot NetApp con il plug-in per il database IBM Db2 per eseguire il backup delle risorse.

L'utilizzo del plug-in per IBM Db2 offre inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di autorizzazioni a livello di applicazione.

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per Linux LVM sul file system XFS.

## Tipi di archiviazione supportati dal plug-in SnapCenter per IBM Db2

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali (VM). Prima di installare il plug-in SnapCenter per IBM Db2, è necessario verificare il supporto per il tipo di storage in uso.

| Macchina | Tipo di archiviazione |
| --- | --- |
| Server fisico | • LUN connesse a FC<br>• LUN connesse tramite iSCSI<br>• Volumi connessi tramite NFS |
| VMware ESXi | • LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host.<br><br>È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES.<br><br>• LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI<br>• VMDK su datastore NFS<br>• VMDK creati su VMFS<br>• Volumi NFS connessi direttamente al sistema guest<br>• Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

## Privilegi ONTAP minimi richiesti per il plug-in IBM Db2

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea
  - lun crea

- lun cancella
- lun igroup aggiungi
- lun igroup create
- lun igroup elimina
- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume

    - creazione di clonazione di file di volume
    - file di volume mostra-utilizzo-disco
    - volume offline
    - volume online
    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete

- mostra interfaccia di rete
- server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per IBM Db2

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter ; non creare una pianificazione ONTAP separata.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Strategia di backup per IBM Db2

### Definire una strategia di backup per IBM Db2

Definire una strategia di backup prima di creare i processi di backup ti aiuta a disporre dei backup necessari per ripristinare o clonare correttamente le tue risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

#### Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

#### Passi

1. Determina quando eseguire il backup delle tue risorse.
2. Decidi quanti processi di backup ti servono.

3. Decidi come denominare i tuoi backup.
4. Decidi se vuoi creare una policy basata sulla copia Snapshot per eseguire il backup di snapshot del database coerenti con l'applicazione.
5. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
7. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

#### Rilevamento automatico delle risorse sull'host Linux

Le risorse sono database IBM Db2 e istanze sull'host Linux gestite da SnapCenter. Dopo aver installato il plug-in SnapCenter per IBM Db2, i database IBM Db2 di tutte le istanze su quell'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.

#### Tipo di backup supportati

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta il tipo di backup basato sulla copia snapshot per i database IBM Db2.

##### Backup basato su copia snapshot

I backup basati su copie snapshot sfruttano la tecnologia snapshot NetApp per creare copie online di sola lettura dei volumi su cui risiedono i database IBM Db2.

#### Come il plug-in SnapCenter per IBM Db2 utilizza gli snapshot del gruppo di coerenza

È possibile utilizzare il plug-in per creare snapshot di gruppi di coerenza per i gruppi di risorse. Un gruppo di coerenza è un contenitore che può ospitare più volumi, in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da snapshot simultanei di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È anche possibile specificare il tempo di attesa affinché il controller di archiviazione raggruppi in modo coerente gli snapshot. Le opzioni di tempo di attesa disponibili sono **Urgente**, **Medio** e **Rilassato**. È anche possibile abilitare o disabilitare la sincronizzazione Write Anywhere File Layout (WAFL) durante l'operazione di snapshot di gruppo coerente. La sincronizzazione WAFL migliora le prestazioni di uno snapshot del gruppo di coerenza.

#### Come SnapCenter gestisce la manutenzione dei backup dei dati

SnapCenter gestisce la manutenzione dei backup dei dati a livello di sistema di archiviazione e di file system.

Gli snapshot sullo storage primario o secondario e le voci corrispondenti nel catalogo IBM Db2 vengono eliminati in base alle impostazioni di conservazione.

#### Considerazioni per la determinazione delle pianificazioni di backup per IBM Db2

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di

modifica della risorsa. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup (con quale frequenza devono essere eseguiti i backup)

  La frequenza di backup, detta anche tipo di pianificazione per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza del backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (quando esattamente devono essere eseguiti i backup)

  Le pianificazioni di backup fanno parte della configurazione di una risorsa o di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00.

#### Numero di processi di backup necessari per IBM Db2

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

#### Convenzioni di denominazione del backup per il plug-in per i database IBM Db2

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione

predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

## Strategia di ripristino e recupero per IBM Db2

### Definire una strategia di ripristino e recupero per le risorse IBM Db2

È necessario definire una strategia prima di ripristinare e recuperare il database, in modo da poter eseguire correttamente le operazioni di ripristino e recupero.

È supportato solo il ripristino manuale del database.

**Passi**

1. Determinare le strategie di ripristino supportate per le risorse IBM Db2 aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i database IBM Db2 rilevati automaticamente

### Tipi di strategie di ripristino supportate per le risorse IBM Db2 aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse IBM Db2 aggiunte manualmente.

Non è possibile recuperare manualmente le risorse IBM Db2 aggiunte.

#### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

### Tipo di strategia di ripristino supportata per IBM Db2 rilevato automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Il ripristino completo delle risorse è la strategia di ripristino supportata per i database IBM Db2 rilevati automaticamente. Ripristina tutti i volumi, i qtree e i LUN di una risorsa.

### Tipi di operazioni di ripristino per IBM Db2 rilevato automaticamente

Il plug-in SnapCenter per IBM Db2 supporta i tipi di ripristino Single File SnapRestore e Connect-and-copy per i database IBM Db2 rilevati automaticamente.

#### Single File SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

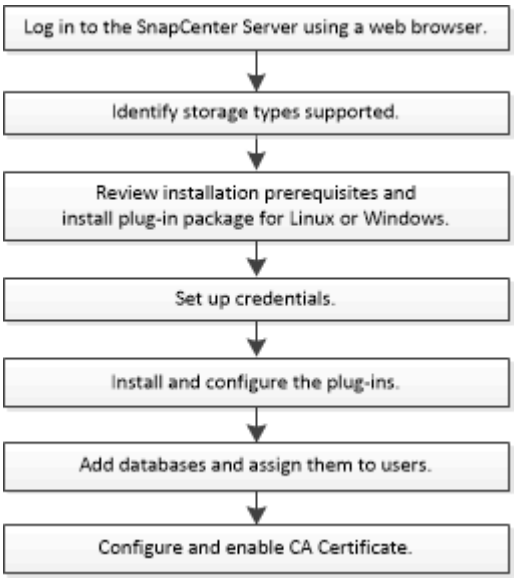
**Single File SnapRestore viene eseguito in ambienti SAN per i seguenti scenari:**

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup viene selezionato da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

# Prepararsi all'installazione del plug-in SnapCenter per IBM Db2

## Flusso di lavoro di installazione del plug-in SnapCenter per IBM Db2

Se si desidera proteggere i database IBM Db2, è necessario installare e configurare il plug-in SnapCenter per IBM Db2.




## Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Windows, Linux o AIX

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. Plug-in SnapCenter per IBM Db2 supportato negli ambienti Windows, Linux e AIX.

- Devi aver installato Java 11 sul tuo host.

  IBM Java non è supportato su host Windows e Linux.

- Per Windows, il plug-in Creator Service dovrebbe essere eseguito utilizzando l'utente Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per IBM Db2 è installato come amministratore di dominio.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in IBM Db2 sugli host Windows.

- SnapCenter Server deve avere accesso alla porta 8145 o personalizzata del plug-in per l'host IBM Db2.

**Host Windows**

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per IBM Db2 su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Windows.

  "Scarica JAVA per Windows"

  "Strumento matrice di interoperabilità NetApp"

**Host Linux e AIX**

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  "Scarica JAVA per Linux"

  "Scarica JAVA per AIX"

  "Strumento matrice di interoperabilità NetApp"

- Per i database IBM Db2 in esecuzione su un host Linux, durante l'installazione del plug-in per IBM Db2, viene installato automaticamente il plug-in SnapCenter per UNIX.
- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

**Comandi supplementari**

Per eseguire un comando supplementare sul plug-in SnapCenter per IBM Db2, è necessario includerlo nel file *allowed_commands.config*.

- Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Per consentire comandi supplementari sull'host del plug-in, aprire il file *allowed_commands.config* in un editor. Immettere ogni comando su una riga separata e i comandi non fanno distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e di racchiuderlo tra virgolette (") se contiene spazi.

Per esempio:

comando: monta

comando: smonta

comando: "C:\Programmi\ NetApp\SnapCreator commands\sdcli.exe"

comando: myscript.bat

Se il file *allowed_commands.config* non è presente, l'esecuzione dei comandi o degli script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in *allowed_commands.config*, l'esecuzione del comando o dello script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Non dovresti usare un carattere jolly (*) per consentire tutti i comandi.

**Configurare i privilegi sudo per gli utenti non root per l'host Linux**

SnapCenter consente a un utente non root di installare il pacchetto plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

**Cosa ti servirà**

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin

- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*LINUX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

### Configurare i privilegi sudo per gli utenti non root per l'host AIX

SnapCenter 4.4 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per AIX e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

#### Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

#### Informazioni su questo compito

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

#### Passi

1. Accedere all'host AIX su cui si desidera installare il pacchetto plug-in SnapCenter per AIX.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*AIX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

| Articolo | Requisiti |
| --- | --- |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario acquisire familiarità con alcuni requisiti di base relativi allo spazio e alle dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |

| Articolo | Requisiti |
| --- | --- |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 Oracle Java e OpenJDK<br><br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

## Imposta le credenziali per il plug-in SnapCenter per IBM Db2

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su database o file system Windows.

**Informazioni su questo compito**

- Host Linux

  È necessario impostare le credenziali per installare i plug-in sugli host Linux.

  Per installare e avviare il processo del plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root dotato di privilegi sudo.

  **Procedura consigliata:** Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

- Host Windows

  Prima di installare i plug-in è necessario impostare le credenziali di Windows.

È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |
| Nome utente | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName*<br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.<br>Applicabile solo agli utenti Linux. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:

   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

      Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

   b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

   c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.

6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Installa il plug-in SnapCenter per IBM Db2

### Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster.

#### Prima di iniziare

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per IBM Db2"

#### Informazioni su questo compito

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Seleziona il tipo di host:<br>• Finestre<br>• Linux<br>Il plug-in per IBM Db2 è installato sull'host client IBM Db2, che può trovarsi su un sistema Windows o Linux. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome host | Immettere il nome host della comunicazione. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN). |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>Puoi visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale che hai fornito.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Quando si utilizza l'API REST per installare il plug-in per Db2, è necessario passare la versione come 3.0. Ad esempio, Db2:3.0

6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Percorso di installazione | Il plug-in per IBM Db2 è installato sull'host client IBM Db2, che può trovarsi su un sistema Windows o Linux.<br>• Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, puoi personalizzare il percorso.<br>• Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/ NetApp/snapcenter. Facoltativamente, puoi personalizzare il percorso. |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br>Fornire il nome gMSA nel seguente formato: domainName\accountName$.<br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Fare clic su **Invia**.

   Se non è stata selezionata la casella di controllo "Ignora controlli preliminari", l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e Java 11 (sia per i plug-in Windows che per quelli Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

> La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.
   - Per il plug-in di Windows, i registri di installazione e aggiornamento si trovano in: *C:\Windows\SnapCenter plugin\Install*<JOBID>\
   - Per il plug-in Linux, i registri di installazione si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log e i registri di aggiornamento si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log

**Dopo aver finito**

Se si desidera eseguire l'aggiornamento a SnapCenter 6.0 o versione successiva, il plug-in basato su PERL esistente per Db2 verrà disinstallato dal server plug-in remoto.

### Installa i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

**Prima di iniziare**

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

### Installare il plug-in SnapCenter per IBM Db2 su host Linux utilizzando l'interfaccia della riga di comando

È necessario installare il plug-in SnapCenter per IBM Db2 Database utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare il plug-in per IBM Db2 Database in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

**Prima di iniziare**

- È necessario installare il plug-in per il database IBM Db2 su ciascun host Linux in cui risiede il client IBM Db2.
- L'host Linux su cui si installa il plug-in SnapCenter per IBM Db2 Database deve soddisfare i requisiti software, del database e del sistema operativo dipendenti.

  Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Strumento matrice di interoperabilità NetApp"

- Il plug-in SnapCenter per IBM Db2 Database fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

**Informazioni su questo compito**

Se i parametri non vengono menzionati, SnapCenter viene installato con i valori predefiniti.

**Passi**

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\ NetApp\ SnapCenter\Package Repository all'host in cui si desidera installare il plug-in per IBM Db2.

   È possibile accedere a questo percorso dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa il plug-in: `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 specifica la porta di comunicazione HTTPS di SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter .
   - -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter .
   - -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto plug-in SnapCenter per Linux.
   - DINSTALL_LOG_NAME specifica il nome del file di registro.

   ```
   /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. Modificare il file /<directory di installazione>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = DB2:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento

a "Guida di riferimento ai cmdlet del software SnapCenter" .

#### Monitorare lo stato di installazione del plug-in per IBM Db2

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

#### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

#### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

**Configurare il certificato CA con i servizi plug-in host di Windows**

## È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

```
> $cert = “a909502dd82ae41433e6f83886b00d4277a32a7b”
> $guid = [guid]::NewGuid().ToString("B")
> netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
appid="$guid"
```

#### Configurare il certificato CA per il servizio SnapCenter IBM Db2 Plug-ins sull’host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio attendibile che come archivio chiavi.

##### Gestisci la password per il keystore del plug-in e l’alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell’agente del plug-in.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Modificare la password per tutti gli alias delle voci di chiave
   privata nel keystore con la stessa password utilizzata per il keystore:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

> La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

##### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.

3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungi un certificato radice o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi per collegare trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elenca i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurare il nome alias dal certificato CA nel file
agent.properties.
```

Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

**Informazioni su questo compito**

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è ' opt/ NetApp/snapcenter/scc/etc/crl'.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Configurare il certificato CA per il servizio SnapCenter IBM Db2 Plug-ins sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   *keytool -storepasswd -keystore keystore.jks*

   > Se il comando "keytool" non viene riconosciuto nel prompt dei comandi di Windows, sostituire il comando keytool con il suo percorso completo.

   *C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungi un certificato radice o intermedio:

   *keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks*

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

   Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   *keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS*

5. Elenca i certificati aggiunti nel keystore.

   *keytool -list -v -keystore keystore.jks*

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   *keytool -keypasswd -alias "nome_alias_in_CA_cert" -keystore keystore.jks*

8. Configurare il nome alias dal certificato CA nel file *agent.properties*.

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

**Informazioni su questo compito**

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .
- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Prepararsi alla protezione dei dati

## Prerequisiti per l'utilizzo del plug-in SnapCenter per IBM Db2

Prima di utilizzare il plug-in SnapCenter per IBM Db2, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività prerequisite.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.
- Installa Java 11 sul tuo host Linux o Windows.

  È necessario impostare il percorso Java nella variabile del percorso ambientale della macchina host.

- Se desideri la replica del backup, imposta SnapMirror e SnapVault.

## Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere IBM Db2

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere database IBM Db2 di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile

selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

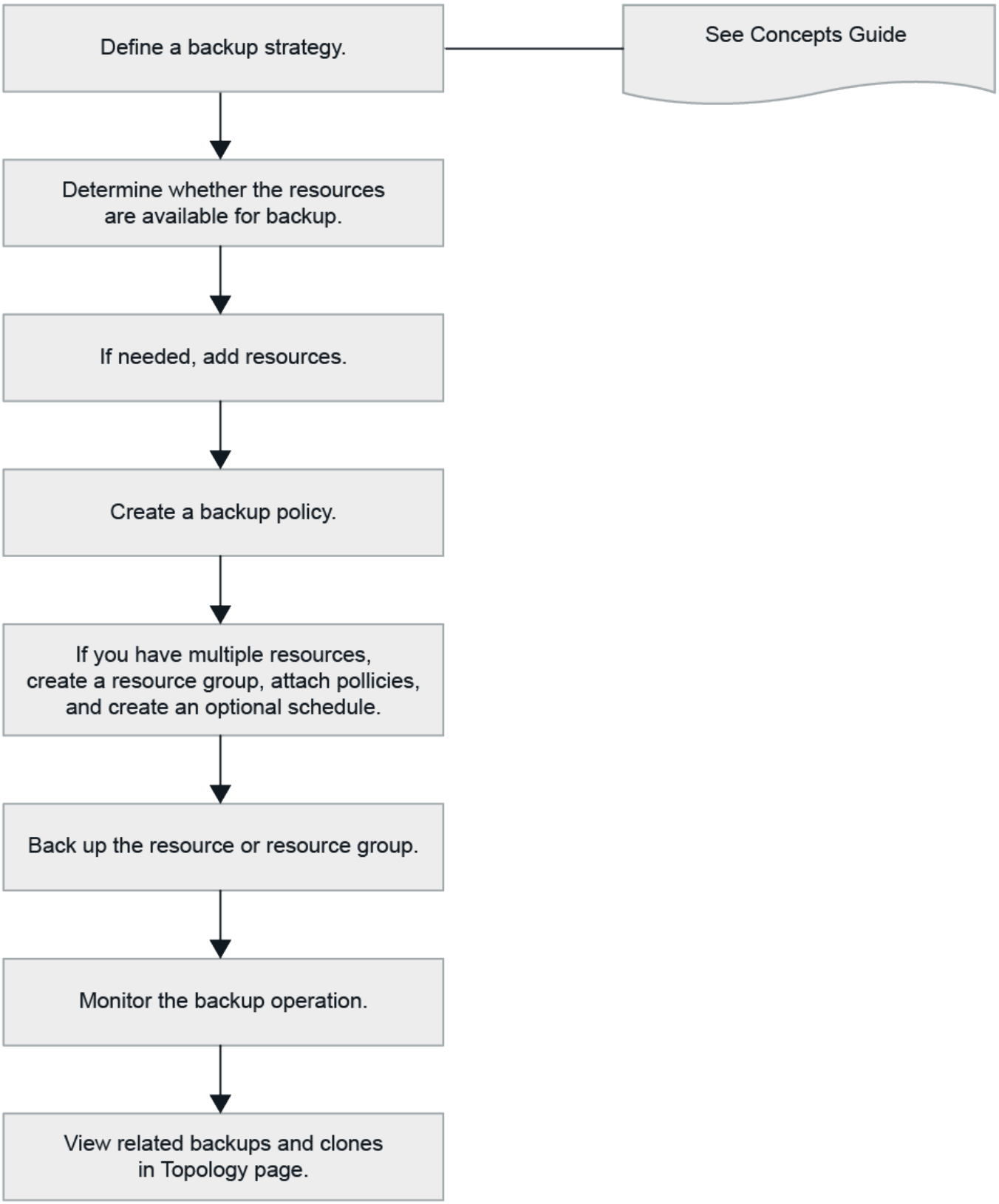
Pensa a un gruppo di risorse come a qualcosa che definisce cosa vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una polizza come a qualcosa che definisce il modo in cui vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database, è possibile creare un gruppo di risorse che includa tutti i database nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

# Eseguire il backup delle risorse IBM Db2

## Eseguire il backup delle risorse IBM Db2

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei database per il backup, la gestione dei criteri di backup, la creazione di gruppi di risorse e l'associazione di criteri, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento ai cmdlet del software SnapCenter" .

## Scopri automaticamente i database

Le risorse sono database IBM Db2 sull'host Linux gestiti da SnapCenter. È possibile aggiungere le risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database IBM Db2 disponibili.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- Il plug-in SnapCenter per IBM Db2 non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK. È necessario fornire le informazioni di archiviazione per gli ambienti virtuali durante l'aggiunta manuale dei database.

**Informazioni su questo compito**

- Dopo aver installato il plug-in, tutti i database presenti sull'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.
- Solo i database vengono rilevati automaticamente.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in per IBM Db2 dall'elenco.
2. Nella pagina Risorse seleziona il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) Fai clic su * * , quindi selezionare il nome host.

   Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

4. Fare clic su **Aggiorna risorse** per scoprire le risorse disponibili sull'host.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il database si trova su un archivio NetApp e non è protetto, nella colonna Stato generale viene visualizzato Non protetto.
   - Se il database si trova su un sistema di archiviazione NetApp ed è protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup non eseguito. In caso contrario, lo stato cambierà in Backup non riuscito o Backup riuscito in base allo stato dell'ultimo backup.

È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

## Aggiungere manualmente le risorse all'host del plug-in

Il rilevamento automatico non è supportato sull'host Windows. È necessario aggiungere manualmente le istanze Db2 e le risorse del database.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni al sistema di archiviazione.

**Informazioni su questo compito**

La rilevazione manuale non è supportata per le seguenti configurazioni:

- Layout RDM e VMDK

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in SnapCenter per IBM Db2 dall'elenco a discesa.
2. Nella pagina Risorse, fare clic su **Aggiungi risorsa IBM DB2**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Specificare il nome del database. |
| Nome host | Inserisci il nome host. |
| Tipo | Seleziona database o istanza. |
| Esempio | Specificare il nome dell'istanza, che è quella padre del database. |
| Credenziali | Seleziona le credenziali o aggiungi informazioni per le credenziali.<br><br>Questo è facoltativo. |

4. Nella pagina Fornisci impronta di archiviazione, seleziona un tipo di archiviazione e scegli uno o più volumi, LUN e qtree, quindi fai clic su **Salva**.

   Facoltativo: puoi cliccare su * * icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

5. Facoltativo: nella pagina Impostazioni risorse, per le risorse sull'host Windows, immettere coppie chiave-valore personalizzate per il plug-in IBM Db2
6. Rivedi il riepilogo e poi clicca su **Fine**.

   I database vengono visualizzati insieme a informazioni quali il nome host, i gruppi di risorse e le policy associate e lo stato generale

Se si desidera consentire agli utenti di accedere alle risorse, è necessario assegnare le risorse agli utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

"Aggiungi un utente o un gruppo e assegna ruoli e risorse"

Dopo aver aggiunto i database, è possibile modificare i dettagli del database IBM Db2.

## Creare policy di backup per IBM Db2

Prima di utilizzare SnapCenter per eseguire il backup delle risorse IBM Db2, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup.

  Per maggiori dettagli, consultare le informazioni sulla definizione di una strategia di protezione dei dati per i database IBM Db2.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta di risorse.
- Se si stanno replicando snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

  Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

**Informazioni su questo compito**

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Nella sezione **Impostazioni di backup personalizzate**, specificare eventuali impostazioni di backup specifiche che devono essere trasmesse al plug-in in formato chiave-valore.

      È possibile fornire più valori-chiave da passare al plug-in.

6. Nella pagina Snapshot e replica, eseguire le seguenti azioni.

   a. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.

È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente anche di assegnare pianificazioni di backup diverse a ciascuna policy.

Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

a. Nella sezione Impostazioni snapshot, eseguire le seguenti azioni:

| **Se lo desidera…** | **Poi…** |
|---|---|
| Conserva un certo numero di istantanee | Selezionare **Copie da conservare**, quindi specificare il numero di snapshot che si desidera conservare.<br><br>Se il numero di snapshot supera il numero specificato, gli snapshot vengono eliminati partendo dalle copie più vecchie. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare giorni, mesi o anni.<br><br>Il periodo di conservazione di Snaplock dovrebbe essere inferiore a 100 anni. |

Per i backup basati su copie Snapshot, è necessario impostare il conteggio di conservazione su 2 o superiore se si prevede di abilitare la replica SnapVault . Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo snapshot è lo snapshot di riferimento per la relazione SnapVault finché uno snapshot più recente non viene replicato sulla destinazione.

b. Specificare l'etichetta della policy.

   È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

7. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| Aggiorna SnapMirror dopo aver creato una copia Snapshot locale | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror . |
| Aggiorna SnapVault dopo aver creato una copia Snapshot locale | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ). |
| Errore nel conteggio dei tentativi | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

8. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse.<br><br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br><br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato del nome personalizzato per la copia snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.

   Ciò aiuta a filtrare le informazioni sullo schermo.

5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Concediti del tempo per attendere il completamento dell'operazione di snapshot del gruppo di coerenza | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione di snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+

a. Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

b. Fare clic sulla freccia **Configurazioni personalizzate** e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

| Parametro | Collocamento | Descrizione |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Abilita la gestione dei log di archivio per eliminare i log di archivio. |
| CONSERVAZIONE_ARCHIVIO_LOG | numero_di_giorni | Specifica il numero di giorni per cui vengono conservati i registri di archivio.<br><br>Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Specifica il percorso della directory che contiene i log di archivio. |

| Parametro | Collocamento | Descrizione |
|---|---|---|
| ARCHIVE_LOG_EXT | estensione_file | Specifica la lunghezza dell'estensione del file di registro dell'archivio.<br><br>Ad esempio, se il registro di archivio è log_backup_0_0_0_0.16151855 1942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151. |
| ARCHIVE_LOG_RECURSIVE_ SE ARCH | (S/N) | Consente la gestione dei log di archivio all'interno delle sottodirectory.<br><br>È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory. |

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in IBM Db2 Linux e non sono supportate per il database IBM Db2 registrato come plug-in centralizzato di Windows.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter utilizza il plug-in per Windows e imposta il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile. | Selezionare * SnapCenter con coerenza del file system*. |
| SnapCenter per creare uno snapshot del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |
| Per immettere il comando da eseguire sull'host per creare copie snapshot. | Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare uno snapshot. |

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando * + *.

I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

b.

Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove policy_name è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse IBM Db2 sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

a. Selezionare il tipo di criterio di replica.

La politica di replica sincrona non è supportata.

b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

> Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

> Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:

a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| **Se lo desidera…** | **Fai questo…** |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

e. Fare clic su **OK**.

Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

> Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per IBM Db2

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e

una credenziale prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei database IBM Db2.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Passi**

1. Fare clic su **SnapCenterPS** per avviare PowerShell Core.
2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -StorageType DataOntap -Type DataOntap
-OntapStorage 'scsnfssvm' -Protocol Https -Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:\> Add-SmCredential -Name 'FinanceAdmin' -Type Linux
-AuthenticationType PasswordBased -Credential db2hostuser
-EnableSudoPrevileges:$true
```

4. Aggiungere l'host di comunicazione IBM Db2 a SnapCenter Server.

   Per Linux:

```
PS C:\> Add-SmHost -HostType Linux -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

   Per Windows:

```
PS C:\> Add-SmHost -HostType Windows -HostName '10.232.204.61'
-CredentialName 'defaultcreds'
```

5. Installare il pacchetto e il plug-in SnapCenter per IBM Db2 sull'host.

   Per Linux:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2
   ```

   Per Windows:

   ```
   PS C:\> Install-SmHostPackage -HostNames '10.232.204.61' -PluginCodes
   DB2,SCW
   ```

6. Imposta il percorso per SQLLIB.

   Per Windows, il plug-in Db2 utilizzerà il percorso predefinito per la cartella SQLLIB: "C:\Programmi\IBM\SQLLIB\BIN"

   Se si desidera sovrascrivere il percorso predefinito, utilizzare il seguente comando.

   ```
   PS C:\> Set-SmConfigSettings -Plugin -HostName '10.232.204.61'
   -PluginCode DB2 -configSettings
   @{"DB2_SQLLIB_CMD"="<custom_path>\IBM\SQLLIB\BIN"}
   ```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei database Db2

Il backup di un database include la creazione di una connessione con SnapCenter Server, l'aggiunta di risorse, l'aggiunta di un criterio, la creazione di un gruppo di risorse di backup e l'esecuzione del backup.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per l'operazione di backup basata su copia snapshot, assicurarsi che tutti i database tenant siano validi e attivi.

- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Selezionare , quindi seleziona il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

     Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
|---|---|
| Concediti del tempo per attendere il completamento dell'operazione "Consistency Group Snapshot" | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

   - Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.

     È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .
   - Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   - Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter per creare uno Snapshot a livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare uno Snapshot | Selezionare * SnapCenter con coerenza del file system*. |
| Per immettere il comando per creare uno Snapshot | Selezionare **Altro**, quindi immettere il comando per creare uno Snapshot. |

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
    - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

      Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   PS C:\> Open-SmConnection
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse manuali utilizzando il cmdlet Add-SmResources.

   Questo esempio mostra come aggiungere un'istanza IBM Db2:

   ```
   PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
   -ResourceType Instance -ResourceName db2inst1 -StorageFootPrint
   (@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
   geSystem"="scsnfssvm"}) -MountPoints "D:\"
   ```

   Per il database Db2:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode DB2
-ResourceType Database -ResourceName SALESDB -StorageFootPrint
(@{"VolumeName"="windb201_data01";"LUNName"="windb201_data01";"Stora
geSystem"="scsnfssvm"}) -MountPoints "D:\" -Instance DB2
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.
4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.
5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

   Questo esempio mostra come eseguire il backup di un gruppo di risorse:

   ```
   C:\PS> New-SMBackup -ResourceGroupName
   'ResourceGroup_with_Db2_Resources' -Policy db2_policy1
   ```

   Questo esempio esegue il backup di un'istanza Db2:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1";"PluginName"="DB2"} -Policy
   db2_policy
   ```

   Questo esempio esegue il backup di un database Db2:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.32.212.13";"Uid"="DB2INST1\WINARCDB";"PluginName"="DB2"
   } -Policy db2_policy
   ```

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet Get-smJobSummaryReport.

```
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. Monitorare i dettagli del processo di backup, come ID del backup e nome del backup, per eseguire operazioni di ripristino o clonazione utilizzando il cmdlet Get-SmBackupReport.

```
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
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio

secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Informazioni su questo compito**

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando e quindi selezionando il tag. Puoi quindi selezionare per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di backup di IBM Db2

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni di protezione dei dati sui database IBM Db2 nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup per IBM Db2

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.

- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
|---|---|
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni di IBM Db2 nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la **scheda Riepilogo** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Scheda riepilogativa** mostra il numero totale di backup basati su copie snapshot e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Aggiorna** si aggiornano i dettagli del backup o del clone.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

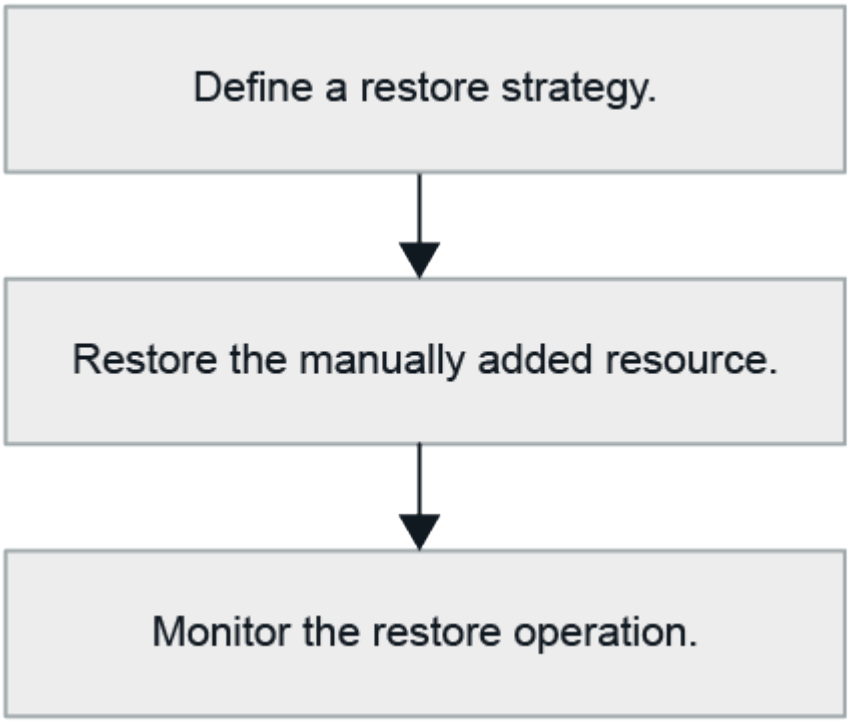
7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su .

# Ripristina IBM Db2

## Ripristina flusso di lavoro

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina un backup di risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

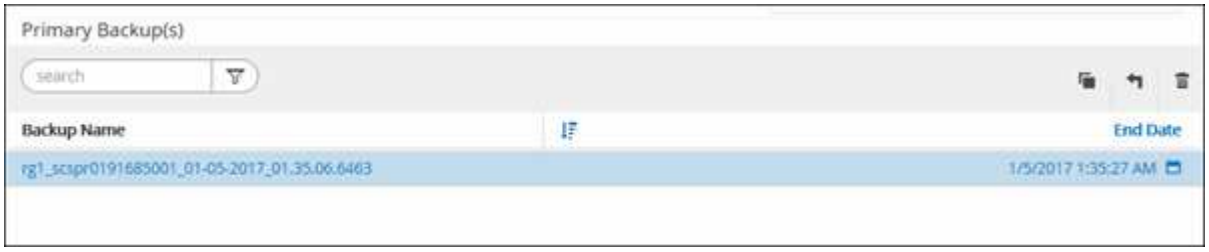
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.




6. Nella pagina Ambito di ripristino, seleziona **Risorsa completa**.

   a. Se si seleziona **Risorsa completa**, verranno ripristinati tutti i volumi di dati configurati del database IBM Db2.

      Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

      È possibile selezionare più LUN.

      Se si seleziona **Tutti**, verranno ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.
8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un

processo di ripristino.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Dopo aver finito**

Il ripristino è possibile solo se lo stato Rollforward è "DB in sospeso". Questo stato è applicabile ai database Db2 con la registrazione degli archivi abilitata.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Identificare il backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio mostra che sono disponibili due backup per il ripristino:

```
 PS C:\> Get-SmBackup -AppObjectId
cn24.sccore.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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

> AppObjectId è "Host\Plugin\UID", dove UID = <nome_istanza> è per la risorsa dell'istanza DB2 rilevata manualmente e UID = <nome_istanza>\<nome_databse> è per la risorsa del database IBM Db2. È possibile ottenere ResourceID dal cmdlet Get-smResources.

```
Get-smResources  -HostName cn24.sccore.test.com  -PluginCode DB2
```

Questo esempio mostra come ripristinare il database dall'archivio primario:

```
Restore-SmBackup -PluginCode DB2 -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 3
```

Questo esempio mostra come ripristinare il database dall'archivio secondario:

```
Restore-SmBackup -PluginCode 'DB2' -AppObjectId
cn24.sccore.test.com\DB2\db2inst1\DB01 -BackupId 399 -Confirm:$false
-Archive @( @{"Primary"="<Primary
Vserver>:<PrimaryVolume>";"Secondary"="<Secondary
Vserver>:<SecondaryVolume>"})
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup del database rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per le risorse rilevate automaticamente, il ripristino è supportato con SFSR.
- Il ripristino automatico non è supportato.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

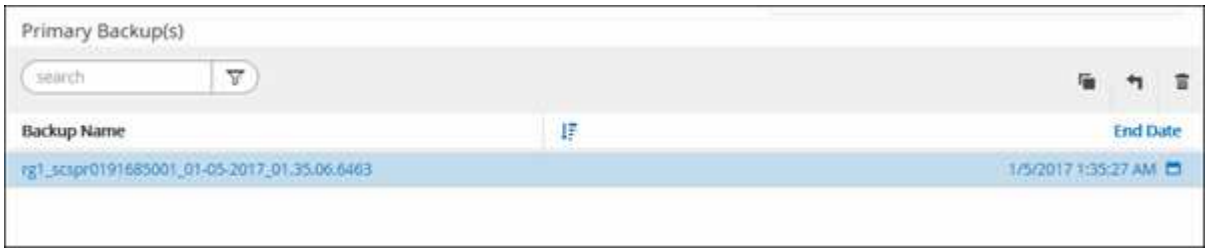
Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato “Non protetto”. Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * .




6. Nella pagina Ripristina ambito, seleziona **Risorsa completa** per ripristinare i volumi di dati configurati del database IBM Db2.
7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono necessari per le risorse rilevate automaticamente.

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono necessari per le risorse rilevate automaticamente.

9. Nella pagina Notifica, dall’elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l’oggetto dell’e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l’avanzamento dell’operazione cliccando su **Monitoraggio** > **Lavori**.

**Dopo aver finito**

Il ripristino è possibile solo se lo stato Rollforward è "DB in sospeso". Questo stato è applicabile ai database Db2 con la registrazione degli archivi abilitata.

## Monitorare le operazioni di ripristino di IBM Db2

È possibile monitorare l’avanzamento delle diverse operazioni di ripristino SnapCenter

utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clona i backup delle risorse IBM Db2

## Flusso di lavoro di clonazione

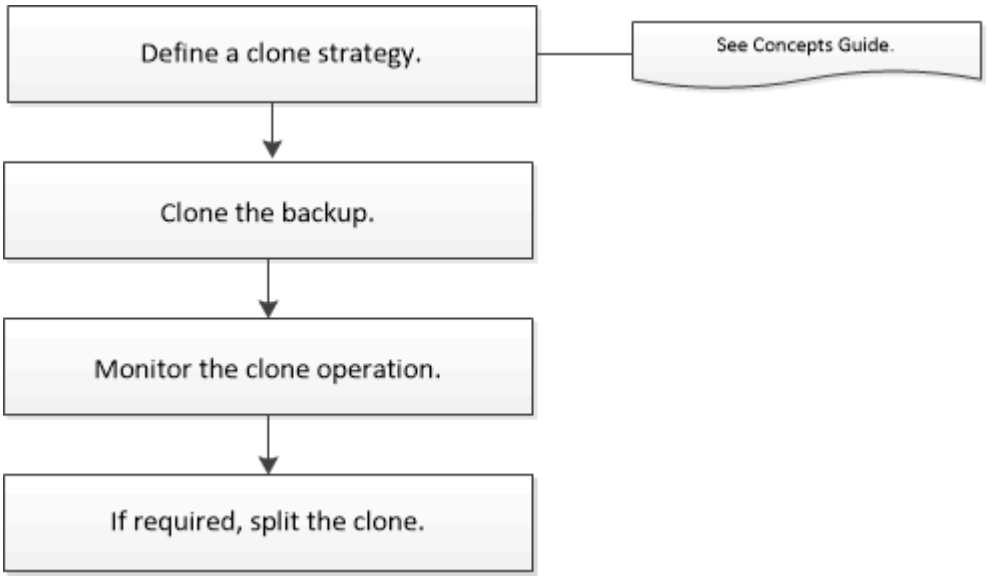
Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

**Informazioni su questo compito**

- È possibile clonare sul server IBM Db2 di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione

- Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
- Per recuperare dati che sono stati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

**Dopo aver finito**

Dopo aver clonato le risorse Db2 rilevate automaticamente, la risorsa clonata viene contrassegnata come risorsa manuale. Fare clic su **Aggiorna risorse** per recuperare la risorsa Db2 clonata. Quando si elimina il clone, vengono ripuliti anche l'archivio e l'host.

Se non si aggiornano le risorse dopo l'operazione di clonazione e si tenta di eliminare il clone, l'archiviazione e l'host non verranno ripuliti. È necessario eliminare manualmente le voci in fstab.

## Clonare un backup IBM Db2

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

**Prima di iniziare**

- Avresti dovuto eseguire il backup delle risorse o del gruppo di risorse.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Durante la creazione di un clone per Db2 su un host alternativo, è necessario creare una struttura di directory n-1 per il percorso di montaggio del clone, uguale al percorso di montaggio originale sull'altro host. Il percorso di montaggio dovrebbe avere l'autorizzazione di esecuzione *755*.
- Per i comandi pre-clone o post-clone, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*

◦ Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere,https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividere un volume FlexClone dal suo volume padre"] .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, host, gruppi di risorse e policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Scegliere un host su cui creare il clone. |
| Istanza clone di destinazione | Immettere l'ID dell'istanza clone Db2 di destinazione da clonare dai backup esistenti.<br><br>Ciò è applicabile solo per le risorse di tipo storage ANF. |
| Nome clone di destinazione | Inserisci il nome del clone.<br><br>Questo è applicabile solo alle risorse del database Db2. |
| Indirizzo IP di esportazione NFS | Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati.<br><br>Questo è applicabile solo alle risorse di tipo archiviazione NFS. |
| Capacità massima del pool (MiB/s) | Immettere la capacità massima di un pool di capacità. |

7. Nella pagina Script, procedere come segue:

   Gli script vengono eseguiti sull'host del plug-in.

a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
   - Comando pre-clone: elimina i database esistenti con lo stesso nome
   - Comando post-clonazione: verifica un database o avvia un database.

b. Immettere il comando mount per montare un file system su un host.

   Comando di montaggio per un volume o qtree su una macchina Linux:

Esempio per NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Dopo aver finito**

Dopo aver clonato le risorse Db2 rilevate automaticamente, la risorsa clonata viene contrassegnata come risorsa manuale. Fare clic su **Aggiorna risorse** per recuperare la risorsa Db2 clonata. Quando si elimina il clone, vengono ripuliti anche l'archivio e l'host.

Se non si aggiornano le risorse dopo l'operazione di clonazione e si tenta di eliminare il clone, l'archiviazione e l'host non verranno ripuliti. È necessario eliminare manualmente le voci in fstab.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl  https://snapctr.demo.netapp.com:8146
```

2. Elenca i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
C:\PS>PS C:\> Get-SmBackup

BackupId   BackupName                      BackupTime   BackupType
--------   ----------                      ----------   ----------
1          Payroll Dataset_vise-f6_08...  8/4/2015     Full Backup
                                          11:02:32 AM

2          Payroll Dataset_vise-f6_08...  8/4/2015
                                          11:23:17 AM
```

Questo esempio visualizza informazioni su un gruppo di risorse specificato, sulle sue risorse e sui criteri associati:

```
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. Avviare un'operazione di clonazione da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

```
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
```

   Questo esempio crea un clone di un'istanza specificata di Microsoft SQL Server:

```
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. Visualizzare lo stato del processo di clonazione utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report di clonazione per l'ID processo specificato:

```
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}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di clonazione IBM Db2

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

**Informazioni correlate**

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

## Eliminare o dividere i cloni del database IBM Db2 dopo l'aggiornamento SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non saranno più visibili. È possibile eliminare il clone o dividere i cloni dalla pagina Topologia della risorsa da cui sono stati creati i cloni.

**Informazioni su questo compito**

Se si desidera individuare l'impronta di archiviazione dei cloni nascosti, eseguire il seguente comando: `Get-SmClone -ListStorageFootprint`

**Passi**

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-smresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa padre dalla pagina Risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Gestisci copie, selezionare i cloni dai sistemi di archiviazione primari o secondari (con mirroring o replica).
6. Seleziona i cloni e poi clicca per eliminare i cloni o fare clic per dividere i cloni.

7. Fare clic su **OK**.

# Proteggere PostgreSQL

## Plug-in SnapCenter per PostgreSQL

### Panoramica del plug-in SnapCenter per PostgreSQL

Il plug-in SnapCenter per cluster PostgreSQL è un componente lato host del software NetApp SnapCenter software che consente la gestione della protezione dei dati basata sulle applicazioni dei cluster PostgreSQL. Il plug-in per il cluster PostgreSQL automatizza il backup, il ripristino e la clonazione dei cluster PostgreSQL nel tuo ambiente SnapCenter .

SnapCenter supporta configurazioni PostgreSQL a cluster singolo e multi-cluster. È possibile utilizzare il plug-in per i cluster PostgreSQL sia in ambienti Linux che Windows. Negli ambienti Windows, PostgreSQL sarà supportato come risorsa manuale.

Una volta installato il plug-in per il cluster PostgreSQL, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard.

Il plug-in SnapCenter per PostgreSQL supporta NFS e SAN su layout di archiviazione ONTAP e Azure NetApp File.

Sono supportati i layout di archiviazione virtuale VMDK, vVol e RDM.

### Cosa puoi fare utilizzando il plug-in SnapCenter per PostgreSQL

Quando installi il plug-in per il cluster PostgreSQL nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei cluster PostgreSQL e delle relative risorse. È anche possibile eseguire attività di supporto a tali operazioni.

- Aggiungere cluster.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

### Funzionalità del plug-in SnapCenter per PostgreSQL

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp sul sistema di storage. Per lavorare con il plug-in per PostgreSQL Cluster, è necessario utilizzare l'interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare operazioni di backup, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- **Tecnologia di copia snapshot NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia snapshot NetApp con il plug-in per il cluster PostgreSQL per eseguire il backup delle risorse.

L'utilizzo del plug-in per PostgreSQL offre inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di autorizzazioni a livello di applicazione.

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per Linux LVM sul file system XFS.

## Tipi di archiviazione supportati dal plug-in SnapCenter per PostgreSQL

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali (VM). Prima di installare il plug-in SnapCenter per PostgreSQL, è necessario verificare il supporto per il tipo di archiviazione in uso.

| Macchina | Tipo di archiviazione |
|---|---|
| Server fisico | • LUN connesse a FC<br>• LUN connesse tramite iSCSI<br>• Volumi connessi tramite NFS |

| Macchina | Tipo di archiviazione |
| --- | --- |
| VMware ESXi | • LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host.<br><br>È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES.<br><br>• LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI<br>• VMDK su datastore NFS<br>• VMDK su VMFS<br>• Volumi NFS connessi direttamente al sistema guest<br>• Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

## Privilegi ONTAP minimi richiesti per il plug-in PostgreSQL

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea
  - lun crea
  - lun cancella
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina

- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online

    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - mostra interfaccia di rete
    - server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per PostgreSQL

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter ; non creare una pianificazione ONTAP separata.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Strategia di backup per PostgreSQL

### Definire una strategia di backup per PostgreSQL

Definire una strategia di backup prima di creare i processi di backup ti aiuta a disporre dei backup necessari per ripristinare o clonare correttamente le tue risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

#### Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

#### Passi

1. Determina quando eseguire il backup delle tue risorse.
2. Decidi quanti processi di backup ti servono.
3. Decidi come denominare i tuoi backup.
4. Decidi se vuoi creare una policy basata sulla copia di snapshot per eseguire il backup di snapshot coerenti con l'applicazione del cluster.

5. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
7. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

#### Rilevamento automatico delle risorse sull'host Linux

Le risorse sono cluster e istanze PostgreSQL sull'host Linux gestiti da SnapCenter. Dopo aver installato il plug-in SnapCenter per PostgreSQL, i cluster PostgreSQL di tutte le istanze su quell'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.

#### Tipo di backup supportati

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta il tipo di backup basato sulla copia snapshot per i cluster PostgreSQL.

##### Backup basato su copia snapshot

I backup basati su copie snapshot sfruttano la tecnologia snapshot NetApp per creare copie online di sola lettura dei volumi su cui risiedono i cluster PostgreSQL.

#### Come il plug-in SnapCenter per PostgreSQL utilizza gli snapshot del gruppo di coerenza

È possibile utilizzare il plug-in per creare snapshot di gruppi di coerenza per i gruppi di risorse. Un gruppo di coerenza è un contenitore che può ospitare più volumi, in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da snapshot simultanei di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È anche possibile specificare il tempo di attesa affinché il controller di archiviazione raggruppi in modo coerente gli snapshot. Le opzioni di tempo di attesa disponibili sono **Urgente**, **Medio** e **Rilassato**. È anche possibile abilitare o disabilitare la sincronizzazione Write Anywhere File Layout (WAFL) durante l'operazione di snapshot di gruppo coerente. La sincronizzazione WAFL migliora le prestazioni di uno snapshot del gruppo di coerenza.

#### Come SnapCenter gestisce la manutenzione dei backup dei dati

SnapCenter gestisce la manutenzione dei backup dei dati a livello di sistema di archiviazione e di file system.

Gli snapshot sullo storage primario o secondario e le voci corrispondenti nel catalogo PostgreSQL vengono eliminati in base alle impostazioni di conservazione.

#### Considerazioni per la determinazione delle pianificazioni di backup per PostgreSQL

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di modifica della risorsa. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno.

Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup (con quale frequenza devono essere eseguiti i backup)

  La frequenza di backup, detta anche tipo di pianificazione per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza del backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (quando esattamente devono essere eseguiti i backup)

  Le pianificazioni di backup fanno parte della configurazione di una risorsa o di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00.

#### Numero di processi di backup necessari per PostgreSQL

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

#### Convenzioni di denominazione del backup per i cluster Plug-in per PostgreSQL

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

## Strategia di ripristino e recupero per PostgreSQL

### Definire una strategia di ripristino e recupero per le risorse PostgreSQL

È necessario definire una strategia prima di ripristinare e recuperare il cluster, in modo da poter eseguire correttamente le operazioni di ripristino e recupero.

È supportato solo il ripristino manuale del cluster.

**Passi**

1. Determinare le strategie di ripristino supportate per le risorse PostgreSQL aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i cluster PostgreSQL rilevati automaticamente
3. Decidi il tipo di operazioni di ripristino che vuoi eseguire.

### Tipi di strategie di ripristino supportate per le risorse PostgreSQL aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Non è possibile recuperare le risorse PostgreSQL aggiunte manualmente.

#### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

NOTA: il plug-in per PostgreSQL crea un backup_label e una tablespace_map nella cartella */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ per facilitare il ripristino manuale.

### Tipo di strategia di ripristino supportata per PostgreSQL rilevato automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Il ripristino completo delle risorse è la strategia di ripristino supportata per i cluster PostgreSQL rilevati automaticamente. Ripristina tutti i volumi, i qtree e i LUN di una risorsa.

### Tipi di operazioni di ripristino per PostgreSQL rilevato automaticamente

Il plug-in SnapCenter per PostgreSQL supporta Single File SnapRestore e i tipi di ripristino connect-and-copy per i cluster PostgreSQL rilevati automaticamente.

#### Single File SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione

**Risorsa completa** è selezionata

**Single File SnapRestore viene eseguito in ambienti SAN per i seguenti scenari:**

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup viene selezionato da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

**Tipi di operazioni di ripristino supportate per i cluster PostgreSQL**

SnapCenter consente di eseguire diversi tipi di operazioni di ripristino per i cluster PostgreSQL.

- Ripristina il cluster fino allo stato più recente
- Ripristina il cluster fino a un punto specifico nel tempo

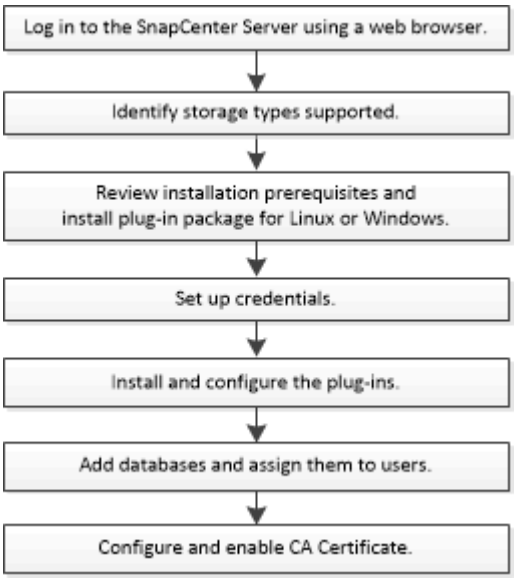
  È necessario specificare la data e l'ora del ripristino.

SnapCenter fornisce anche l'opzione Nessun ripristino per i cluster PostgreSQL.

# Prepararsi all'installazione del plug-in SnapCenter per PostgreSQL

## Flusso di lavoro di installazione del plug-in SnapCenter per PostgreSQL

Se si desidera proteggere i cluster PostgreSQL, è necessario installare e configurare il plug-in SnapCenter per PostgreSQL.




## Prerequisiti per aggiungere host e installare il plug-in SnapCenter per PostgreSQL

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. Il plug-in SnapCenter per PostgreSQL è disponibile sia negli ambienti Windows che Linux.

- Devi aver installato Java 11 sul tuo host.

  IBM Java non è supportato su host Windows e Linux.

- Per Windows, il servizio Creator del plug-in dovrebbe essere eseguito utilizzando l'utente Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per PostgreSQL è installato come amministratore di dominio.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in PostgreSQL sugli host Windows.
- SnapCenter Server dovrebbe avere accesso alla porta 8145 o personalizzata dell'host Plug-in per PostgreSQL.

**Host Windows**

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per PostgreSQL su un host Windows, il plug-in SnapCenter per Microsoft Windows viene installato automaticamente.
- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Windows.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

**Host Linux**

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

- Per i cluster PostgreSQL in esecuzione su un host Linux, durante l'installazione del plug-in per PostgreSQL, viene installato automaticamente il plug-in SnapCenter per UNIX.
- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

**Comandi supplementari**

Per eseguire un comando supplementare sul plug-in SnapCenter per PostgreSQL, è necessario includerlo nel file *allowed_commands.config*.

- Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Per consentire comandi supplementari sull'host del plug-in, aprire il file *allowed_commands.config* in un editor.

Immettere ogni comando su una riga separata e i comandi non fanno distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e di racchiuderlo tra virgolette (") se contiene spazi.

Per esempio:

comando: mount comando: umount comando: "C:\Programmi\ NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

Se il file *allowed_commands.config* non è presente, l'esecuzione dei comandi o degli script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in *allowed_commands.config*, l'esecuzione del comando o dello script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Non dovresti usare un carattere jolly (*) per consentire tutti i comandi.

**Configurare i privilegi sudo per gli utenti non root per l'host Linux**

SnapCenter consente a un utente non root di installare il pacchetto plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

**Cosa ti servirà**

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

*LINUX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario acquisire familiarità con alcuni requisiti di base relativi allo spazio e alle dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | Java 11 Oracle Java e OpenJDK<br><br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

## Imposta le credenziali per il plug-in SnapCenter per PostgreSQL

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su cluster o file system Windows.

**Informazioni su questo compito**

- Host Linux

  È necessario impostare le credenziali per installare i plug-in sugli host Linux.

  Per installare e avviare il processo del plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root dotato di privilegi sudo.

  **Procedura consigliata:** Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

- Host Windows

  Prima di installare i plug-in è necessario impostare le credenziali di Windows.

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |
| Nome utente | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName*<br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.<br>Applicabile solo agli utenti Linux. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:
   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

      Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.
6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Installa il plug-in SnapCenter per PostgreSQL

### Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere l'host e installare pacchetti plug-in per un singolo host.

**Prima di iniziare**

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.

- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per PostgreSQL"

**Informazioni su questo compito**

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Tipo di host | Seleziona il tipo di host:<br>• Finestre<br>• Linux<br>Il plug-in per PostgreSQL viene installato sull'host client PostgreSQL, che può trovarsi sia su un sistema Windows che su un sistema Linux. |
| Nome host | Immettere il nome host della comunicazione. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN). |

| Per questo campo… | Fai questo… |
| --- | --- |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>Puoi visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale che hai fornito.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Quando si utilizza l'API REST per installare il plug-in per PostgreSQL, è necessario passare la versione come 3.0. Ad esempio, PostgreSQL:3.0

6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il plug-in per PostgreSQL viene installato sull'host client PostgreSQL, che può trovarsi sia su un sistema Windows che su un sistema Linux.<br><br>• Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, puoi personalizzare il percorso.<br>• Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/ NetApp/snapcenter. Facoltativamente, puoi personalizzare il percorso. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Aggiungi tutti gli host nel cluster | Selezionare questa casella di controllo per aggiungere tutti i nodi del cluster. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br>Fornire il nome gMSA nel seguente formato: domainName\accountName$.<br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo "Ignora controlli preliminari", l'host verrà convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.
   - Per il plug-in di Windows, i registri di installazione e aggiornamento si trovano in: *C:\Windows\ SnapCenter plugin\Install*<JOBID>_
   - Per il plug-in Linux, i registri di installazione si trovano in:

*/var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ e i registri di aggiornamento si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

### Installa i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

#### Prima di iniziare

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

#### Passi

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

### Installa il plug-in SnapCenter per PostgreSQL su host Linux utilizzando l'interfaccia della riga di comando

È necessario installare il plug-in SnapCenter per il cluster PostgreSQL utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare il plug-in per il cluster PostgreSQL in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

#### Prima di iniziare

- Dovresti installare il plug-in per il cluster PostgreSQL su ciascun host Linux in cui risiede il client PostgreSQL.
- L'host Linux su cui si installa il plug-in SnapCenter per il cluster PostgreSQL deve soddisfare i requisiti software, cluster e sistema operativo dipendenti.

  Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Strumento matrice di interoperabilità NetApp"

- Il plug-in SnapCenter per il cluster PostgreSQL fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

**Passi**

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\ NetApp\ SnapCenter\Package Repository all'host in cui si desidera installare il plug-in per PostgreSQL.

   È possibile accedere a questo percorso dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa il plug-in: `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 specifica la porta di comunicazione HTTPS di SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter .
   - -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter .
   - -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto plug-in SnapCenter per Linux.
   - DINSTALL_LOG_NAME specifica il nome del file di registro.

   ```
   /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. Modificare il file /<directory di installazione>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = PostgreSQL:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

### Monitorare lo stato di installazione del plug-in per PostgreSQL

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
-

Completato con avvisi o non è stato possibile avviarlo a causa di avvisi

- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

> Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

#### Passi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e

identificare il certificato installato di recente tramite il nome dell'oggetto.

*Get-ChildItem -Percorso Cert:\LocalMachine\My*

b. Copia l'impronta digitale.

**Configurare il certificato CA con i servizi plug-in host di Windows**

## È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

**Configurare il certificato CA per il servizio SnapCenter PostgreSQL Plug-ins sull'host Linux**

## È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio

attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

   ```
    keytool -storepasswd -keystore keystore.jks
   . Modificare la password per tutti gli alias delle voci di chiave
   privata nel keystore con la stessa password utilizzata per il keystore:
   ```

   ```
   keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
   ```

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

> La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Aggiungi un certificato radice o intermedio:

   ```
    keytool -import -trustcacerts -alias myRootCA -file
   /root/USERTrustRSA_Root.cer -keystore keystore.jks
   . Riavviare il servizio dopo aver configurato i certificati radice o
   intermedi per collegare trust-store.
   ```

> Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   ```
   keytool -list -v -keystore keystore.jks
   ```

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   ```
   keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
   -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
   ```

5. Elenca i certificati aggiunti nel keystore.

   ```
   keytool -list -v -keystore keystore.jks
   ```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   ```
    keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
   keystore.jks
   . Se il nome alias nel certificato CA è lungo e contiene spazi o
   caratteri speciali ("*",","), modificare il nome alias in un nome
   semplice:
   ```

   ```
    keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
   -keystore keystore.jks
   . Configurare il nome alias dal certificato CA nel file
   agent.properties.
   ```

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

**Informazioni su questo compito**

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è ' opt/ NetApp/snapcenter/scc/etc/crl'.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Configurare il certificato CA per il servizio plug-in SnapCenter PostgreSQL sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   *keytool -storepasswd -keystore keystore.jks*

   > Se il comando "keytool" non viene riconosciuto nel prompt dei comandi di Windows, sostituire il comando keytool con il suo percorso completo.

   *C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*

2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungi un certificato radice o intermedio:

   *keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks*

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

   Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   *keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS*

5. Elenca i certificati aggiunti nel keystore.

   *keytool -list -v -keystore keystore.jks*

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   *keytool -keypasswd -alias "nome_alias_in_CA_cert" -keystore keystore.jks*

8. Configurare il nome alias dal certificato CA nel file *agent.properties*.

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

**Informazioni su questo compito**

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Prepararsi alla protezione dei dati

### Prerequisiti per l'utilizzo del plug-in SnapCenter per PostgreSQL

Prima di utilizzare il plug-in SnapCenter per PostgreSQL, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.
- Installa Java 11 sul tuo host Linux o Windows.

  È necessario impostare il percorso Java nella variabile del percorso ambientale della macchina host.

- Se desideri la replica del backup, imposta SnapMirror e SnapVault.

### Come vengono utilizzate le risorse, i gruppi di risorse e le policy per proteggere PostgreSQL

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere cluster PostgreSQL di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

Pensa a un gruppo di risorse come a qualcosa che definisce cosa vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una polizza come a qualcosa che definisce il modo in cui vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i cluster, è possibile creare un gruppo di risorse che includa tutti i cluster nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

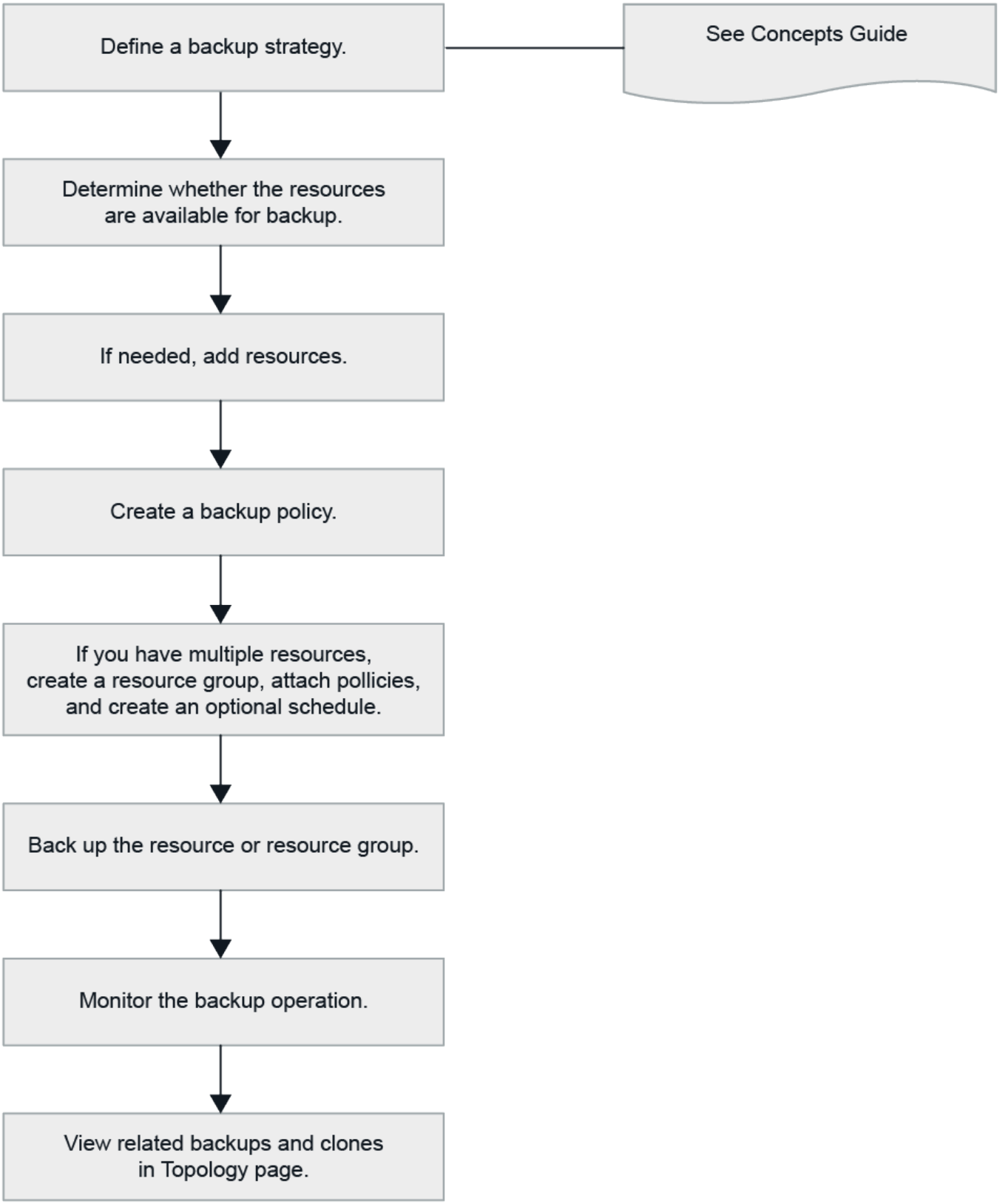
# Eseguire il backup delle risorse PostgreSQL

### Eseguire il backup delle risorse PostgreSQL

È possibile creare un backup di una risorsa (cluster) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei cluster per il backup, la

gestione delle policy di backup, la creazione di gruppi di risorse e l'associazione di policy, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:



È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento ai cmdlet del software SnapCenter" .

## Scopri automaticamente i cluster

Le risorse sono cluster PostgreSQL sull'host Linux gestiti da SnapCenter. È possibile aggiungere le risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i cluster PostgreSQL disponibili.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- Il plug-in SnapCenter per PostgreSQL non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK.

**Informazioni su questo compito**

- Dopo aver installato il plug-in, tutti i cluster presenti sull'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.
- Solo i cluster vengono rilevati automaticamente.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in per PostgreSQL dall'elenco.
2. Nella pagina Risorse seleziona il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) Fai clic su * * , quindi selezionare il nome host.

   Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

4. Fare clic su **Aggiorna risorse** per scoprire le risorse disponibili sull'host.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il cluster si trova su uno storage NetApp e non è protetto, nella colonna Stato generale viene visualizzato Non protetto.
   - Se il cluster si trova su un sistema di archiviazione NetApp ed è protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup non eseguito. In caso contrario, lo stato cambierà in Backup non riuscito o Backup riuscito in base allo stato dell'ultimo backup.

È necessario aggiornare le risorse se i cluster vengono rinominati all'esterno di SnapCenter.

## Aggiungere manualmente le risorse all'host del plug-in

Il rilevamento automatico non è supportato sull'host Windows. È necessario aggiungere manualmente le risorse del cluster Postgresql.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni al sistema di archiviazione.

**Informazioni su questo compito**

Il rilevamento automatico non è supportato per le seguenti configurazioni:

- Layout RDM e VMDK

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona il plug-in SnapCenter per Postgresql dall'elenco a discesa, quindi fai clic su **Risorse**.
2. Nella pagina Risorse, fare clic su **Aggiungi risorse Postgresql**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Specificare il nome del cluster. |
| Nome host | Inserisci il nome host. |
| Tipo | Seleziona cluster. |
| Esempio | Specificare il nome dell'istanza, che è l'istanza padre del cluster. |
| Credenziali | Seleziona le credenziali o aggiungi informazioni per le credenziali.<br><br>Questo è facoltativo. |

4. Nella pagina Fornisci impronta di archiviazione, seleziona un tipo di archiviazione e scegli uno o più volumi, LUN e qtree, quindi fai clic su **Salva**.

   Facoltativo: puoi cliccare su * * icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

5. Facoltativo: nella pagina Impostazioni risorse, per le risorse sull'host Windows, immettere coppie chiave-valore personalizzate per il plug-in PostgreSQL
6. Rivedi il riepilogo e poi clicca su **Fine**.

   I cluster vengono visualizzati insieme a informazioni quali il nome host, i gruppi di risorse e le policy associate e lo stato generale

Se si desidera consentire agli utenti di accedere alle risorse, è necessario assegnare le risorse agli utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

"Aggiungi un utente o un gruppo e assegna ruoli e risorse"

**Dopo aver finito**

- Dopo aver aggiunto i cluster, è possibile modificare i dettagli del cluster PostgreSQL.
- Le risorse migrate (tablespace e cluster) da SnapCenter 5.0 saranno contrassegnate come tipo di cluster PostgreSQL in SnapCenter 6.0.
- Quando si modificano le risorse aggiunte manualmente e migrate da SnapCenter 5.0 o versioni precedenti, procedere come segue nella pagina **Impostazioni risorse** per le coppie chiave-valore personalizzate:
  - Specificare il termine "PORTA" nel campo **Nome**.
  - Specificare il numero di porta nel campo **Valore**.

## Creare policy di backup per PostgreSQL

Prima di utilizzare SnapCenter per eseguire il backup delle risorse PostgreSQL, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup.

  Per maggiori dettagli, vedere le informazioni sulla definizione di una strategia di protezione dei dati per i cluster PostgreSQL.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta di risorse.
- Se si stanno replicando snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

  Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

**Informazioni su questo compito**

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.

5. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Nella sezione **Impostazioni di backup personalizzate**, specificare eventuali impostazioni di backup specifiche che devono essere trasmesse al plug-in in formato chiave-valore.

      È possibile fornire più valori-chiave da passare al plug-in.

6. Nella pagina Backup e replica, eseguire le seguenti azioni:
   a. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.

      È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente anche di assegnare pianificazioni di backup diverse a ciascuna policy.

      Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

   a. Nella sezione Impostazioni snapshot, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina **Tipo di backup**:

| **Se lo desidera…** | **Poi…** |
|---|---|
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP . |

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

7. Selezionare un'etichetta di criterio.

> È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

8. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapMirror dopo aver creato una copia Snapshot locale** | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e si seleziona solo questa opzione, lo Snapshot creato sul primario non verrà trasferito alla destinazione, ma verrà elencato nella destinazione. Se si seleziona questo snapshot dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il seguente messaggio di errore: La posizione secondaria non è disponibile per il backup con vault/mirroring selezionato.<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup e i cloni relativi alle risorse PostgreSQL nella pagina Topologia" . |

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapVault dopo aver creato una copia Snapshot locale** | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ).<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per ulteriori informazioni su SnapLock Vault, vedere Commit Snapshots to WORM su una destinazione vault<br><br>Vedere "Visualizza i backup e i cloni relativi alle risorse PostgreSQL nella pagina Topologia" . |
| **Errore nel conteggio dei nuovi tentativi** | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.

2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse.<br><br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br><br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato del nome personalizzato per la copia snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.

   Ciò aiuta a filtrare le informazioni sullo schermo.

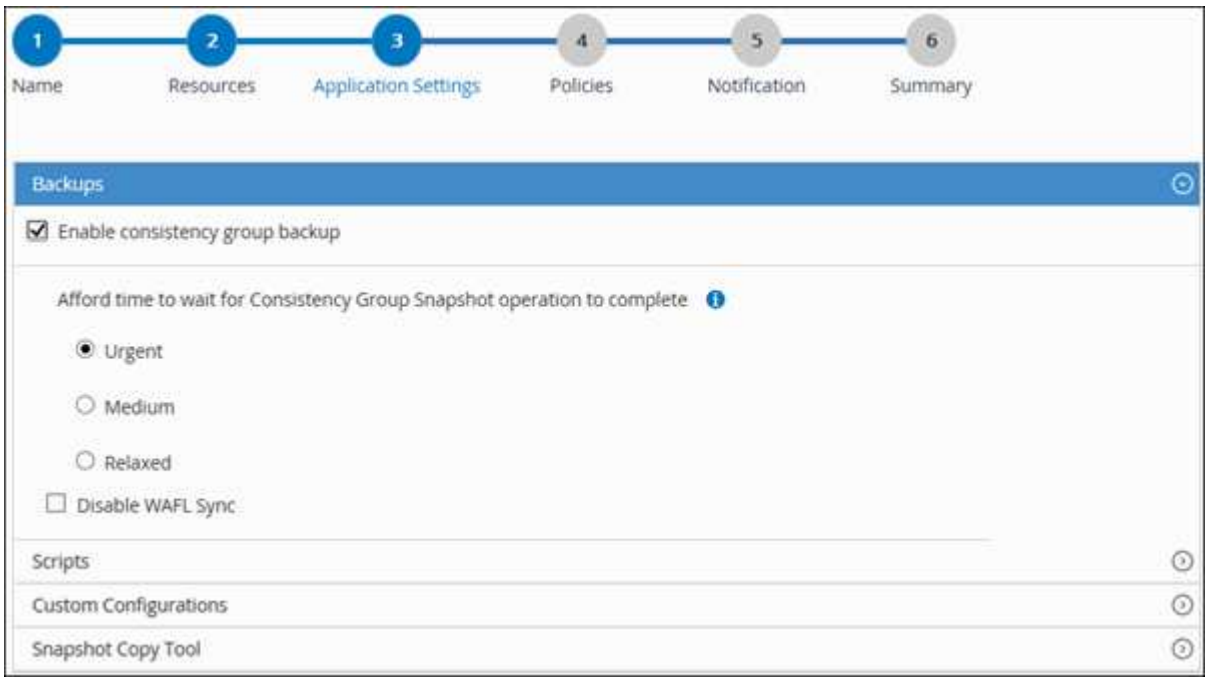
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Concediti del tempo per attendere il completamento dell'operazione di snapshot del gruppo di coerenza | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione di snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+




a. Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

b. Fare clic sulla freccia **Configurazioni personalizzate** e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

| Parametro | Collocamento | Descrizione |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Abilita la gestione dei log di archivio per eliminare i log di archivio. |
| CONSERVAZIONE_ARCHIVIO_LOG | numero_di_giorni | Specifica il numero di giorni per cui vengono conservati i registri di archivio.<br><br>Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Specifica il percorso della directory che contiene i log di archivio. |

| Parametro | Collocamento | Descrizione |
|---|---|---|
| ARCHIVE_LOG_EXT | estensione_file | Specifica la lunghezza dell'estensione del file di registro dell'archivio.<br><br>Ad esempio, se il registro di archivio è log_backup_0_0_0_0.16151855 1942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151. |
| ARCHIVE_LOG_RECURSIVE_ SE ARCH | (S/N) | Consente la gestione dei log di archivio all'interno delle sottodirectory.<br><br>È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory. |

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in Linux PostgreSQL e non sono supportate per i cluster PostgreSQL registrati come plug-in Windows centralizzato.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter utilizza il plug-in per Windows e imposta il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile. | Selezionare * SnapCenter con coerenza del file system*. |
| SnapCenter per creare uno snapshot del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |
| Per immettere il comando da eseguire sull'host per creare copie snapshot. | Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare uno snapshot. |

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando * + *.

I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

b.

Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove policy_name è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse PostgreSQL sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

a. Selezionare il tipo di criterio di replica.

La politica di replica sincrona non è supportata.

b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

> Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

> Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:

   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

   e. Fare clic su **OK**.

   Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   > Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per PostgreSQL

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e

delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei cluster PostgreSQL.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei cluster potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell Core utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Aggiungere l'host di comunicazione PostgreSQL a SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode PostgreSQL
```

5. Installare il pacchetto e il plug-in SnapCenter per PostgreSQL sull'host.

Per Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL
```

Per Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
PostgreSQL -FilesystemCode scw -RunAsName FinanceAdmin
```

6. Imposta il percorso per SQLLIB.

   Per Windows, il plug-in PostgreSQL utilizzerà il percorso predefinito per la cartella SQLLIB: "C:\Programmi\IBM\SQLLIB\BIN"

   Se si desidera sovrascrivere il percorso predefinito, utilizzare il seguente comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
PostgreSQL -configSettings @{“PostgreSQL_SQLLIB_CMD” =
“<custom_path>\IBM\SQLLIB\BIN”}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup di PostgreSQL

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all’utente dell’archivio deve includere il privilegio “snapmirror all”. Tuttavia, se si utilizza il ruolo “vsadmin”, il privilegio “snapmirror all” non è richiesto.
- Per l’operazione di backup basata su copia snapshot, assicurarsi che tutti i cluster tenant siano validi e attivi.
- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell’elenco dei comandi disponibile sull’host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull’host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull’host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell’elenco dei comandi, l’operazione fallirà.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Seleziona * *, quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

     Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
|---|---|
| Concediti del tempo per attendere il completamento dell'operazione "Consistency Group Snapshot" | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

   - Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.

     È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .
   - Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   - Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter per creare uno Snapshot a livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare uno Snapshot | Selezionare * SnapCenter con coerenza del file system*. |
| Per immettere il comando per creare uno Snapshot | Selezionare **Altro**, quindi immettere il comando per creare uno Snapshot. |

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
    - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

      Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

    - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

      Per aumentare la dimensione dell'heap Java, individuare il file di script */opt/netapp/init_scripts/scvservice*. In quello script, il comando *do_start method* avvia il servizio plug-in SnapCenter VMware. Aggiornare il comando come segue: *Java -jar -Xmx8192M -Xms4096M*

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   PS C:\> Open-SmConnection
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse manuali utilizzando il cmdlet Add-SmResources.

   Questo esempio mostra come aggiungere un'istanza PostgreSQL:

```
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. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.
4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.
5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

   Questo esempio mostra come eseguire il backup di un gruppo di risorse:

   ```
   C:\PS> New-SMBackup -ResourceGroupName 'ResourceGroup_wback-up-
   clusters-using-powershell-cmdlets-postgresql.adocith_Resources'
   -Policy postgresql_policy1
   ```

   Questo esempio esegue il backup di una risorsa protetta:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="postgresql"}
   -Policy postgresql_policy2
   ```

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitorare i dettagli del processo di backup, come ID del backup e nome del backup, per eseguire operazioni di ripristino o clonazione utilizzando il cmdlet Get-SmBackupReport.

```
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 :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Informazioni su questo compito**

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in

base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando e quindi selezionando il tag. Puoi quindi selezionare per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di backup di PostgreSQL

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.

b. Specificare le date di inizio e fine.

c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.

d. Dal menu a discesa **Stato**, seleziona lo stato del backup.

e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.

4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

> Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni di protezione dei dati sui cluster PostgreSQL nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup per PostgreSQL

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni di PostgreSQL nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la **scheda Riepilogo** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Scheda riepilogativa** mostra il numero totale di backup basati su copie snapshot e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Aggiorna** si aggiornano i dettagli del backup o del clone.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

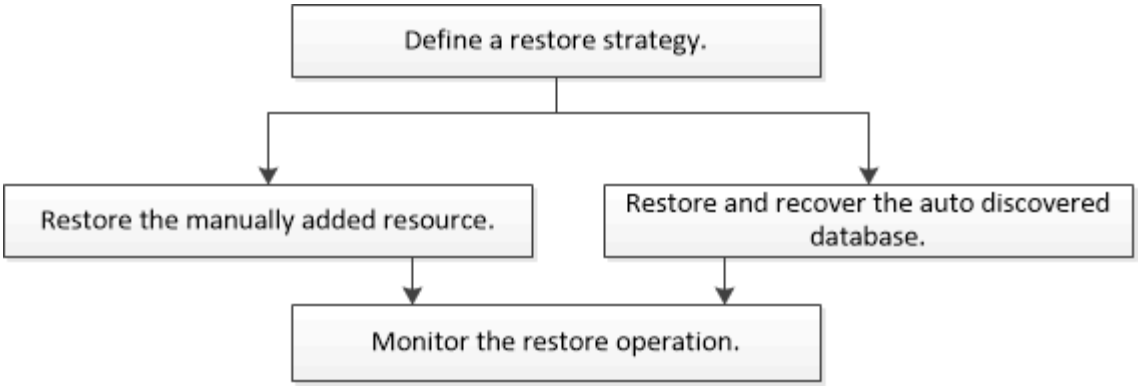
7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su .

# Ripristina PostgreSQL

## Ripristina flusso di lavoro

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup di risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

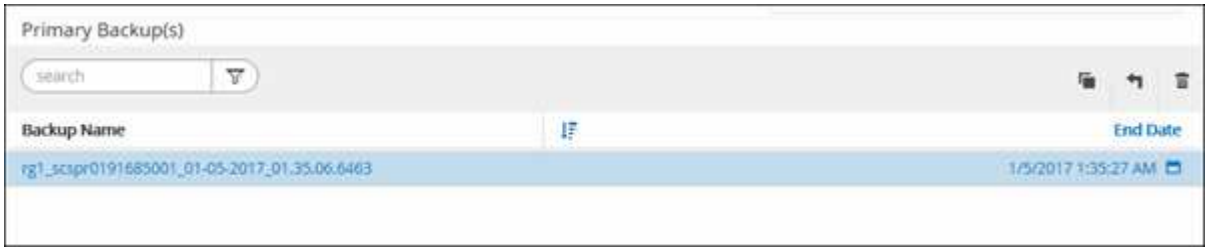
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.




6. Nella pagina Ambito di ripristino, seleziona **Risorsa completa**.

   a. Se si seleziona **Risorsa completa**, verranno ripristinati tutti i volumi di dati configurati del cluster PostgreSQL.

      Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

      È possibile selezionare più LUN.

      Se si seleziona **Tutti**, verranno ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup del cluster rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in*

*Creator\etc\allowed_commands.config*

- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Le copie di backup basate su file non possono essere ripristinate da SnapCenter.
- Per le risorse rilevate automaticamente, il ripristino è supportato con SFSR.
- Il ripristino automatico non è supportato.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

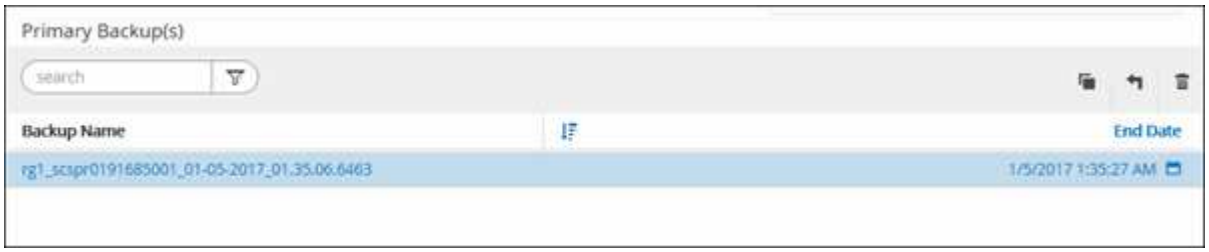
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * .




6. Nella pagina Ripristina ambito, seleziona **Risorsa completa** per ripristinare i volumi di dati configurati del cluster PostgreSQL.
7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:

| Se tu… | Fai questo… |
| --- | --- |

| | |
|---|---|
| Vuoi recuperare il più vicino possibile all'ora corrente | Seleziona **Ripristina allo stato più recente**. Per le risorse di un singolo contenitore, specificare una o più posizioni di backup di log e cataloghi. |
| Vuoi ripristinare il punto temporale specificato | Seleziona **Recupera fino a un punto nel tempo**.<br><br>a. Inserisci data e ora. Inserisci data e ora. Ad esempio, l'host Linux PostgreSQL si trova a Sunnyvale, CA e l'utente a Raleigh, NC sta recuperando i log in SnapCenter.<br><br>Se l'utente desidera eseguire un ripristino alle 5 del mattino a Sunnyvale, CA, deve impostare il fuso orario del browser sul fuso orario dell'host Linux PostgreSQL, ovvero GMT-07:00, e specificare la data e l'ora come 5:00. |
| Non voglio recuperare | Selezionare **Nessun recupero**. |

Non è possibile recuperare le risorse PostgreSQL aggiunte manualmente.

Il plug-in SnapCenter per PostgreSQL crea un backup_label e una tablespace_map nella cartella */<OS_temp_folder>/postgresql_sc_recovery*<Restore_JobId>/_ per facilitare il ripristino manuale.

1. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

2. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

3. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

4. Rivedi il riepilogo e poi clicca su **Fine**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di ripristino di PostgreSQL

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clona i backup delle risorse PostgreSQL

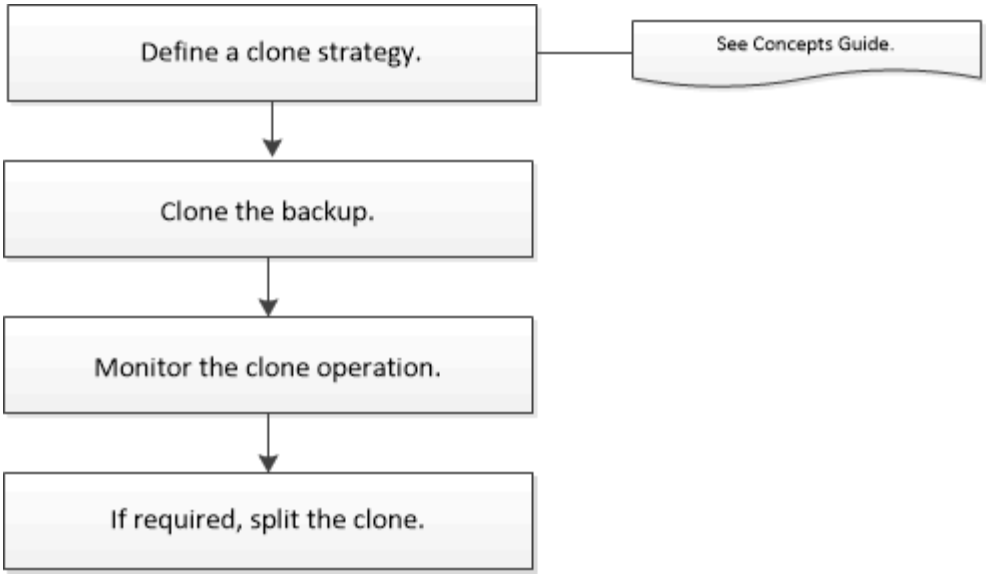
## Flusso di lavoro di clonazione

Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

**Informazioni su questo compito**

- È possibile clonare sul server PostgreSQL di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione
  - Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
  - Per recuperare dati che sono stati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

## Clonare un backup PostgreSQL

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

**Prima di iniziare**

- Avresti dovuto eseguire il backup delle risorse o del gruppo di risorse.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Per i comandi pre-clone o post-clone, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere,https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividere un volume FlexClone dal suo volume padre"] .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, host, gruppi di risorse e policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Scegliere un host su cui creare il clone. |
| Porta di destinazione | Immettere la porta di destinazione PostgreSQL da clonare dai backup esistenti. |
| Indirizzo IP di esportazione NFS | Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati.<br><br>Questo è applicabile solo alle risorse di tipo archiviazione NFS. |
| Capacità massima del pool (MiB/s) | Immettere la capacità massima di un pool di capacità.<br><br>Ciò è applicabile solo per le risorse di tipo storage ANF. |

7. Nella pagina Script, procedere come segue:

   Gli script vengono eseguiti sull'host del plug-in.

   a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
      - Comando pre-clone: elimina i cluster esistenti con lo stesso nome
      - Comando post-clonazione: verifica un cluster o avvia un cluster.

b. Immettere il comando mount per montare un file system su un host.

Comando di montaggio per un volume o qtree su una macchina Linux:

Esempio per NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Recuperare i backup per eseguire l'operazione di clonazione utilizzando il cmdlet Get-SmBackup.

Questo esempio mostra che sono disponibili due backup per la clonazione:

```
 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. Avvia un'operazione di clonazione da un backup esistente e specifica gli indirizzi IP di esportazione NFS su cui vengono esportati i volumi clonati.

Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs pari a 10.32.212.14:

Per il cluster PostgreSQL:

```
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
```

Se NFSExportIPs non è specificato, l'impostazione predefinita è l'esportazione nell'host di destinazione del clone.

4. Verificare che i backup siano stati clonati correttamente utilizzando il cmdlet Get-SmCloneReport per visualizzare i dettagli del processo di clonazione.

   È possibile visualizzare dettagli quali ID clone, data e ora di inizio, data e ora di fine.

```
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          :
```

## Monitorare le operazioni di clonazione di PostgreSQL

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

#### Informazioni correlate

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

## Elimina o dividi i cloni del cluster PostgreSQL dopo l'aggiornamento SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non saranno più visibili. È possibile eliminare il clone o dividere i cloni dalla pagina Topologia della risorsa da cui sono stati creati i cloni.

#### Informazioni su questo compito

Se si desidera individuare l'impronta di archiviazione dei cloni nascosti, eseguire il seguente comando: `Get-`

```
SmClone -ListStorageFootprint
```

**Passi**

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-smresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa padre dalla pagina Risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Gestisci copie, selezionare i cloni dai sistemi di archiviazione primari o secondari (con mirroring o replica).
6. Seleziona i cloni e poi clicca per eliminare i cloni o fare clic per dividere i cloni.
7. Fare clic su **OK**.

# Proteggi MySQL

## Plug-in SnapCenter per MySQL

### Panoramica del plug-in SnapCenter per MySQL

Il plug-in SnapCenter per il database MySQL è un componente lato host del software NetApp SnapCenter software che consente la gestione della protezione dei dati basata sulle applicazioni dei database MySQL. Il plug-in per il database MySQL automatizza il backup, il ripristino e la clonazione dei database MySQL nel tuo ambiente SnapCenter .

SnapCenter supporta configurazioni MySQL a istanza singola. È possibile utilizzare il plug-in per il database MySQL sia in ambienti Linux che Windows. Negli ambienti Windows, MySQL sarà supportato come risorsa manuale.

Una volta installato il plug-in per il database MySQL, è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror dei set di backup su un altro volume. È inoltre possibile utilizzare il plug-in con la tecnologia NetApp SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard.

Il plug-in SnapCenter per MySQL supporta NFS e SAN su layout di archiviazione ONTAP e Azure NetApp File.

Sono supportati i layout di archiviazione virtuale VMDK, vVol e RDM.

I collegamenti simbolici non sono supportati.

### Cosa puoi fare utilizzando il plug-in SnapCenter per MySQL

Quando installi il plug-in per il database MySQL nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione delle istanze MySQL. È anche possibile eseguire attività di supporto a tali operazioni.

- Aggiungi istanze.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

### Funzionalità del plug-in SnapCenter per MySQL

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp sul sistema di storage. Per lavorare con il plug-in per il database MySQL, utilizzare l'interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare operazioni di backup, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- **Tecnologia di copia snapshot NetApp senza interruzioni**

  SnapCenter utilizza la tecnologia snapshot NetApp con il plug-in per il database MySQL per eseguire il backup delle risorse.

L'utilizzo del plug-in per MySQL offre inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di autorizzazioni a livello di applicazione.

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Supporto per Linux LVM sul file system XFS.

## Tipi di archiviazione supportati dal plug-in SnapCenter per MySQL

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che su macchine virtuali (VM). Prima di installare il plug-in SnapCenter per MySQL, è necessario verificare il supporto per il tipo di archiviazione in uso.

| Macchina | Tipo di archiviazione |
|---|---|
| Server fisico | • LUN connesse a FC<br>• LUN connesse tramite iSCSI<br>• Volumi connessi tramite NFS |

| Macchina | Tipo di archiviazione |
| --- | --- |
| VMware ESXi | • LUN RDM connesse tramite FC o iSCSI ESXi HBA. La scansione degli adattatori bus host (HBA) potrebbe richiedere molto tempo perché SnapCenter esegue la scansione di tutti gli adattatori bus host presenti nell'host.<br><br>È possibile modificare il file **LinuxConfig.pm** che si trova in */opt/NetApp/snapcenter/spl/plugins/scu/scucore/modules/SCU/Config* per impostare il valore del parametro **SCSI_HOSTS_OPTIMIZED_RESCAN** su 1 per rieseguire la scansione solo degli HBA elencati in HBA_DRIVER_NAMES.<br><br>• LUN iSCSI collegate direttamente al sistema guest dall'iniziatore iSCSI<br>• VMDK su datastore NFS<br>• VMDK creati su VMFS<br>• Volumi NFS connessi direttamente al sistema guest<br>• Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

## Privilegi ONTAP minimi richiesti per il plug-in MySQL

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro
  - luna
  - lun crea
  - lun crea
  - lun crea
  - lun cancella
  - lun igroup aggiungi
  - lun igroup create
  - lun igroup elimina

- rinomina lun igroup
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- lun persistent-reservation clear
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop
- creazione del volume
- distruzione del volume
- creazione di clonazione di file di volume
- file di volume mostra-utilizzo-disco
- volume offline
- volume online

    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - modifica-scadenza-snaplock-istantanea-volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - politica di esportazione del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - server virtuale iscsi
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete
    - mostra interfaccia di rete
    - server virtuale

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per MySQL

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter ; non creare una pianificazione ONTAP separata.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Strategia di backup per MySQL

### Definire una strategia di backup per MySQL

Definire una strategia di backup prima di creare i processi di backup ti aiuta a disporre dei backup necessari per ripristinare o clonare correttamente le tue risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

#### Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

#### Passi

1. Determina quando eseguire il backup delle tue risorse.
2. Decidi quanti processi di backup ti servono.
3. Decidi come denominare i tuoi backup.
4. Decidi se vuoi creare una policy basata sulla copia Snapshot per eseguire il backup di snapshot del database coerenti con l'applicazione.

5. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.
6. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
7. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

#### Rilevamento automatico delle risorse sull'host Linux

Le risorse sono istanze MySQL sull'host Linux gestite da SnapCenter. Dopo aver installato il plug-in SnapCenter per MySQL, le istanze MySQL su quell'host Linux vengono automaticamente rilevate e visualizzate nella pagina Risorse.

#### Tipo di backup supportati

Tipo di backup specifica il tipo di backup che si desidera creare. SnapCenter supporta il tipo di backup basato sulla copia snapshot per i database MySQL.

##### Backup basato su copia snapshot

I backup basati su copie snapshot sfruttano la tecnologia snapshot NetApp per creare copie online di sola lettura dei volumi su cui risiedono i database MySQL.

#### Come il plug-in SnapCenter per MySQL utilizza gli snapshot del gruppo di coerenza

È possibile utilizzare il plug-in per creare snapshot di gruppi di coerenza per i gruppi di risorse. Un gruppo di coerenza è un contenitore che può ospitare più volumi, in modo da poterli gestire come un'unica entità. Un gruppo di coerenza è costituito da snapshot simultanei di più volumi, che forniscono copie coerenti di un gruppo di volumi.

È anche possibile specificare il tempo di attesa affinché il controller di archiviazione raggruppi in modo coerente gli snapshot. Le opzioni di tempo di attesa disponibili sono **Urgente**, **Medio** e **Rilassato**. È anche possibile abilitare o disabilitare la sincronizzazione Write Anywhere File Layout (WAFL) durante l'operazione di snapshot di gruppo coerente. La sincronizzazione WAFL migliora le prestazioni di uno snapshot del gruppo di coerenza.

#### Come SnapCenter gestisce la manutenzione dei backup dei log

SnapCenter gestisce la manutenzione dei backup dei dati a livello di sistema di archiviazione e di file system.

#### Considerazioni per la determinazione delle pianificazioni di backup per MySQL

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di modifica della risorsa. Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup (con quale frequenza devono essere eseguiti i backup)

  La frequenza di backup, detta anche tipo di pianificazione per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza del backup come oraria, giornaliera, settimanale o mensile.

- Pianificazioni di backup (quando esattamente devono essere eseguiti i backup)

  Le pianificazioni di backup fanno parte della configurazione di una risorsa o di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per i backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00.

#### Numero di processi di backup necessari per MySQL

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

#### Convenzioni di denominazione del backup per plug-in per database MySQL

È possibile utilizzare la convenzione di denominazione predefinita di Snapshot oppure una convenzione di denominazione personalizzata. La convenzione di denominazione predefinita per i backup aggiunge un timestamp ai nomi degli snapshot che consente di identificare quando sono state create le copie.

Lo Snapshot utilizza la seguente convenzione di denominazione predefinita:

```
resourcegroupname_hostname_timestamp
```

Dovresti assegnare nomi logici ai gruppi di risorse di backup, come nell'esempio seguente:

```
dts1_mach1x88_03-12-2015_23.17.26
```

In questo esempio, gli elementi della sintassi hanno i seguenti significati:

- *dts1* è il nome del gruppo di risorse.
- *mach1x88* è il nome host.
- *03-12-2015_23.17.26* è la data e l'ora.

In alternativa, è possibile specificare il formato del nome dello snapshot durante la protezione delle risorse o dei gruppi di risorse selezionando **Usa formato nome personalizzato per la copia dello snapshot**. Ad esempio, customtext_resourcegroup_policy_hostname o resourcegroup_hostname. Per impostazione predefinita, il suffisso timestamp viene aggiunto al nome dello Snapshot.

## Strategia di ripristino e recupero per MySQL

#### Definire una strategia di ripristino e recupero per le risorse MySQL

È necessario definire una strategia prima di ripristinare e recuperare il database, in modo

da poter eseguire correttamente le operazioni di ripristino e recupero.

È supportato solo il ripristino manuale del database.

**Passi**

1. Determinare le strategie di ripristino supportate per le risorse MySQL aggiunte manualmente
2. Determinare le strategie di ripristino supportate per i database MySQL rilevati automaticamente
3. Decidi il tipo di operazioni di ripristino che vuoi eseguire.

#### Tipi di strategie di ripristino supportate per le risorse MySQL aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse MySQL aggiunte manualmente.

Non è possibile recuperare le risorse MySQL aggiunte manualmente.

##### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

#### Tipo di strategia di ripristino supportata per MySQL rilevato automaticamente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter.

Il ripristino completo delle risorse è la strategia di ripristino supportata per i database MySQL rilevati automaticamente. Ripristina tutti i volumi, i qtree e i LUN di una risorsa.

#### Tipi di operazioni di ripristino per MySQL rilevato automaticamente

Il plug-in SnapCenter per MySQL supporta Single File SnapRestore e i tipi di ripristino "connect-and-copy" per i database MySQL rilevati automaticamente.

##### Single File SnapRestore viene eseguito negli ambienti NFS per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup selezionato proviene da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

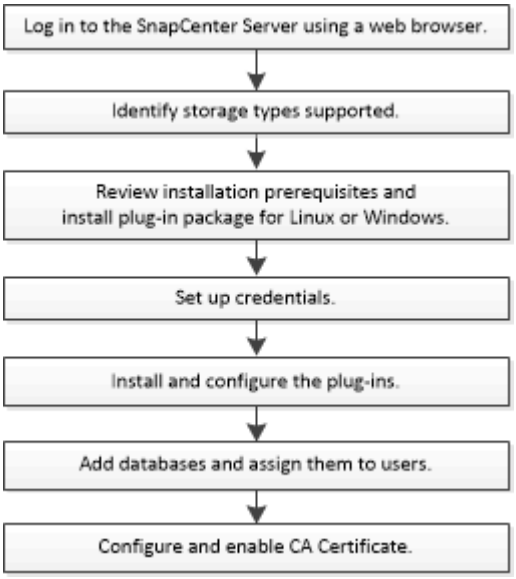
##### Single File SnapRestore viene eseguito in ambienti SAN per i seguenti scenari:

- Se è selezionata solo l'opzione **Completa Risorsa**
- Quando il backup viene selezionato da una posizione secondaria SnapMirror o SnapVault e l'opzione **Risorsa completa** è selezionata

# Preparati a installare il plug-in SnapCenter per MySQL

## Flusso di lavoro di installazione del plug-in SnapCenter per MySQL

Se si desidera proteggere i database MySQL, è necessario installare e configurare il plug-in SnapCenter per MySQL.




## Prerequisiti per aggiungere host e installare il plug-in SnapCenter per MySQL

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. Il plug-in SnapCenter per MySQL è disponibile sia negli ambienti Windows che Linux.

- Devi aver installato Java 11 sul tuo host.

  IBM Java non è supportato su host Windows e Linux.

- Per Windows, il servizio Creator del plug-in dovrebbe essere eseguito utilizzando l'utente Windows "LocalSystem", che è il comportamento predefinito quando il plug-in per MySQL è installato come amministratore di dominio.
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host. Il plug-in SnapCenter per Microsoft Windows verrà distribuito per impostazione predefinita con il plug-in MySQL sugli host Windows.
- SnapCenter Server dovrebbe avere accesso alla porta 8145 o personalizzata del plug-in per l'host MySQL.
- Per MySQL 5.7, binlog deve essere specificato nel file di configurazione mysql (my.cnf o mysql-server.cnf).

### Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Durante l'installazione del plug-in per MySQL su un host Windows, il plug-in SnapCenter per Microsoft

Windows viene installato automaticamente.

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Windows.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

**Host Linux**

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  "Scarica JAVA per tutti i sistemi operativi"

  "Strumento matrice di interoperabilità NetApp"

- Per i database MySQL in esecuzione su un host Linux, durante l'installazione del plug-in per MySQL, viene installato automaticamente il plug-in SnapCenter per UNIX.
- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

**Comandi supplementari**

Per eseguire un comando supplementare sul plug-in SnapCenter per MySQL, è necessario includerlo nel file *allowed_commands.config*.

- Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Per consentire comandi supplementari sull'host del plug-in, aprire il file *allowed_commands.config* in un editor. Immettere ogni comando su una riga separata e i comandi non fanno distinzione tra maiuscole e minuscole. Assicurarsi di specificare il percorso completo e di racchiuderlo tra virgolette (") se contiene spazi.

Per esempio:

comando: mount comando: umount comando: "C:\Programmi\ NetApp\SnapCreator commands\sdcli.exe" comando: myscript.bat

Se il file *allowed_commands.config* non è presente, l'esecuzione dei comandi o degli script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Se il comando o lo script non è presente in *allowed_commands.config*, l'esecuzione del comando o dello script verrà bloccata e il flusso di lavoro non riuscirà con il seguente errore:

"[/mnt/mount -a] esecuzione non consentita. Autorizza aggiungendo il comando nel file %s sull'host del plugin."

Non dovresti usare un carattere jolly (*) per consentire tutti i comandi.

### Configurare i privilegi sudo per gli utenti non root per l'host Linux

SnapCenter consente a un utente non root di installare il pacchetto plug-in SnapCenter per Linux e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

#### Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Se l'umask è 0027, assicurarsi che la cartella java e tutti i file al suo interno abbiano l'autorizzazione 555. In caso contrario l'installazione del plug-in potrebbe non riuscire.
- Per l'utente non root, assicurarsi che il nome dell'utente non root e il nome del gruppo dell'utente siano gli stessi.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

#### Informazioni su questo compito

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*LINUX_USER*/.sc_netapp/snapcenter_linux_host_plugin.bin
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

#### Passi

1. Accedi all'host Linux su cui desideri installare il pacchetto plug-in SnapCenter per Linux.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*LINUX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- _C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Windows.
- _/opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt _ se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux

Prima di installare il pacchetto di plug-in SnapCenter per Linux, è necessario acquisire familiarità con alcuni requisiti di base relativi allo spazio e alle dimensioni del sistema host.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• SUSE Linux Enterprise Server (SLES)<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 Oracle Java e OpenJDK<br><br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |

## Imposta le credenziali per il plug-in SnapCenter per MySQL

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su database o file system Windows.

**Informazioni su questo compito**

- Host Linux

  È necessario impostare le credenziali per installare i plug-in sugli host Linux.

  Per installare e avviare il processo del plug-in, è necessario impostare le credenziali per l'utente root o per

un utente non root dotato di privilegi sudo.

**Procedura consigliata:** Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

- Host Windows

  Prima di installare i plug-in è necessario impostare le credenziali di Windows.

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome della credenziale | Inserisci un nome per le credenziali. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome utente | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName*<br>Non utilizzare virgolette doppie (") o apici inversi (`) nelle password. Non dovresti usare insieme i simboli minore (<) e punto esclamativo (!) nelle password. Ad esempio, lessthan<!10, lessthan10<!, backtick`12. |
| Password | Inserisci la password utilizzata per l'autenticazione. |
| Modalità di autenticazione | Seleziona la modalità di autenticazione che desideri utilizzare. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.<br>Applicabile solo agli utenti Linux. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

# Installa il plug-in SnapCenter per MySQL

## Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere l'host e installare pacchetti plug-in per un singolo host.

### Prima di iniziare

- Se il sistema operativo dell'host del server SnapCenter è Windows 2019 e il sistema operativo dell'host del plug-in è Windows 2022, è necessario eseguire le seguenti operazioni:
  - Aggiorna a Windows Server 2019 (build del sistema operativo 17763.5936) o versione successiva
  - Aggiorna a Windows Server 2022 (build del sistema operativo 20348.2402) o versione successiva
- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- La documentazione di amministrazione contiene informazioni sulla gestione degli host.

### Informazioni su questo compito

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Tipo di host | Seleziona il tipo di host:<br>• Finestre<br>• Linux<br>Il plug-in per MySQL deve essere installato sul server del database MySQL. |
| Nome host | Immettere il nome host della comunicazione. Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host. SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN). |

| Per questo campo… | Fai questo… |
| --- | --- |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove. La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>Puoi visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale che hai fornito.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.

   Quando si utilizza l'API REST per installare il plug-in per MySQL, è necessario passare la versione come 3.0. Ad esempio, MySQL:3.0

6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta. Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il plug-in per MySQL viene installato sull'host client MySQL, che può trovarsi sia su un sistema Windows che su un sistema Linux.<br><br>• Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter. Facoltativamente, puoi personalizzare il percorso.<br>• Per il pacchetto di plug-in SnapCenter per Linux, il percorso predefinito è /opt/ NetApp/snapcenter. Facoltativamente, puoi personalizzare il percorso. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |
| Aggiungi tutti gli host nel cluster | Non applicabile. |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Non applicabile. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo "Ignora controlli preliminari", l'host verrà convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.
   - Per il plug-in di Windows, i registri di installazione e aggiornamento si trovano in: *C:\Windows\ SnapCenter plugin\Install*<JOBID>_
   - Per il plug-in Linux, i registri di installazione si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Install*<JOBID>.log_ e i registri di aggiornamento si trovano in: */var/opt/snapcenter/logs/SnapCenter_Linux_Host_Plug-in_Upgrade*<JOBID>.log_

**Dopo aver finito**

Se si desidera eseguire l'aggiornamento alla versione 6.0 SnapCenter , il plug-in basato su PERL per MySQL verrà disinstallato dal server del plug-in remoto.

#### Installa i pacchetti plug-in SnapCenter per Linux o Windows su più host remoti utilizzando i cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux o Windows su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

**Prima di iniziare**

È necessario aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui si desidera installare il pacchetto plug-in.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

### Installa il plug-in SnapCenter per MySQL su host Linux utilizzando l'interfaccia della riga di comando

È necessario installare il plug-in SnapCenter per il database MySQL utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare il plug-in per il database MySQL in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

**Prima di iniziare**

- Dovresti installare il plug-in per il database MySQL su ciascun host Linux in cui l'istanza MySQL deve essere protetta.
- L'host Linux su cui si installa il plug-in SnapCenter per il database MySQL deve soddisfare i requisiti software, del database e del sistema operativo dipendenti.

  Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sulle configurazioni supportate.

  "Strumento matrice di interoperabilità NetApp"

- Il plug-in SnapCenter per il database MySQL fa parte del pacchetto di plug-in SnapCenter per Linux. Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario aver già installato SnapCenter su un host Windows.

**Passi**

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\ NetApp\ SnapCenter\Package Repository all'host in cui si desidera installare il plug-in per MySQL.

   È possibile accedere a questo percorso dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa il plug-in: `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 specifica la porta di comunicazione HTTPS di SMCore.
- -DSERVER_IP specifica l'indirizzo IP del server SnapCenter .
- -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter .
- -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto plug-in SnapCenter per Linux.
- DINSTALL_LOG_NAME specifica il nome del file di registro.

```
/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. Modificare il file /<directory di installazione>/ NetApp/snapcenter/scc/etc/SC_SMS_Services.properties, quindi aggiungere il parametro PLUGINS_ENABLED = MySQL:3.0.
5. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

### Monitorare lo stato di installazione del plug-in per MySQL

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

#### Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:

a. Fare clic su **Filtro**.
b. Facoltativo: specificare la data di inizio e di fine.
c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.
e. Fare clic su **Applica**.

4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

#### Passi

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

**Passi**

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

#### Configurare il certificato CA con i servizi plug-in host di Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

#### Configurare il certificato CA per il servizio SnapCenter MySQL Plug-ins sull'host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio attendibile che come archivio chiavi.

##### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungi un certificato radice o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi per collegare trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elenca i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurare il nome alias dal certificato CA nel file
agent.properties.
```

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

**Informazioni su questo compito**

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è ' opt/ NetApp/snapcenter/scc/etc/crl'.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Configurare il certificato CA per il servizio SnapCenter MySQL Plug-ins sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei

plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   *keytool -storepasswd -keystore keystore.jks*

   > Se il comando "keytool" non viene riconosciuto nel prompt dei comandi di Windows, sostituire il comando keytool con il suo percorso completo.

   *C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungi un certificato radice o intermedio:

   *keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks*

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   *keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS*

5. Elenca i certificati aggiunti nel keystore.

   *keytool -list -v -keystore keystore.jks*

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   *keytool -keypasswd -alias "nome_alias_in_CA_cert" -keystore keystore.jks*

8. Configurare il nome alias dal certificato CA nel file *agent.properties*.

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

**Informazioni su questo compito**

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .
- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

I certificati in arrivo saranno verificati rispetto a ciascun CRL.

#### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Prepararsi alla protezione dei dati

## Prerequisiti per l'utilizzo del plug-in SnapCenter per MySQL

Prima di utilizzare il plug-in SnapCenter per MySQL, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.

- Installa Java 11 sul tuo host Linux o Windows.

  È necessario impostare il percorso Java nella variabile del percorso ambientale della macchina host.

- Se desideri la replica del backup, imposta SnapMirror e SnapVault.

### Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere MySQL

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere istanze MySQL di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.

- Le policy specificano la frequenza di backup, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

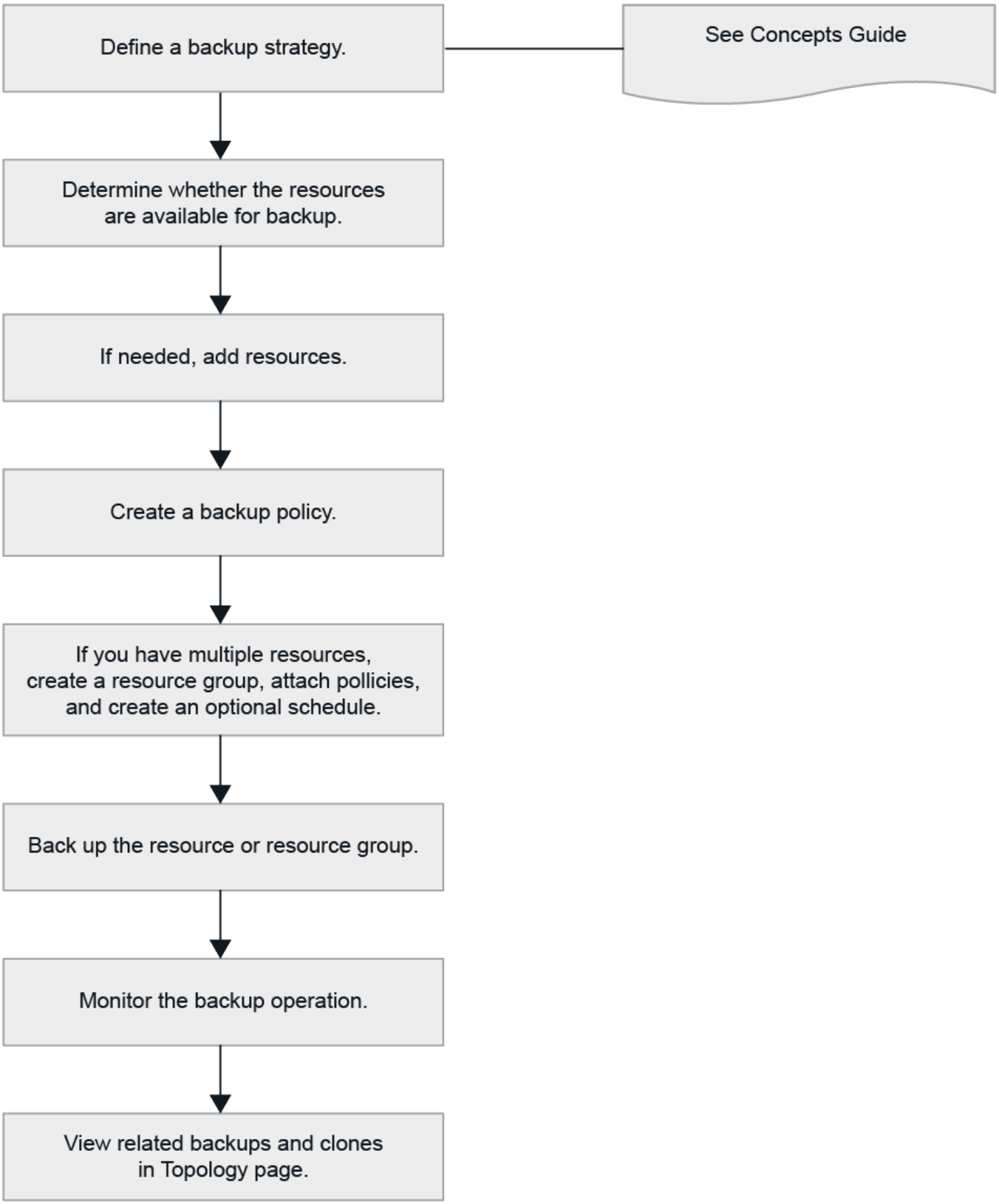
Pensa a un gruppo di risorse come a qualcosa che definisce cosa vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una polizza come a qualcosa che definisce il modo in cui vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database, è possibile creare un gruppo di risorse che includa tutti i database nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse in modo che esegua un backup completo ogni giorno.

# Eseguire il backup delle risorse MySQL

### Eseguire il backup delle risorse MySQL

È possibile creare un backup di una risorsa (database) o di un gruppo di risorse. Il flusso di lavoro del backup include la pianificazione, l'identificazione dei database per il backup, la gestione dei criteri di backup, la creazione di gruppi di risorse e l'associazione di criteri, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell. "Guida di riferimento ai cmdlet del software SnapCenter" .

## Scopri automaticamente i database

Le risorse sono database MySQL sull'host Linux gestiti da SnapCenter. È possibile aggiungere le risorse ai gruppi di risorse per eseguire operazioni di protezione dei dati dopo aver individuato i database MySQL disponibili.

**Prima di iniziare**

- È necessario aver già completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni del sistema di archiviazione.
- Il plug-in SnapCenter per MySQL non supporta il rilevamento automatico delle risorse residenti negli ambienti virtuali RDM/VMDK. È necessario fornire le informazioni di archiviazione per gli ambienti virtuali durante l'aggiunta manuale dei database.

**Informazioni su questo compito**

- Dopo aver installato il plug-in, tutti i database presenti sull'host Linux vengono automaticamente rilevati e visualizzati nella pagina Risorse.
- Solo i database vengono rilevati automaticamente.

Le risorse rilevate automaticamente non possono essere modificate o eliminate.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in per MySQL dall'elenco.
2. Nella pagina Risorse seleziona il tipo di risorsa dall'elenco Visualizza.
3. (Facoltativo) Fai clic su * * , quindi selezionare il nome host.

   Puoi quindi cliccare su * * per chiudere il riquadro del filtro.

4. Fare clic su **Aggiorna risorse** per scoprire le risorse disponibili sull'host.

   Le risorse vengono visualizzate insieme a informazioni quali tipo di risorsa, nome host, gruppi di risorse associati, tipo di backup, criteri e stato generale.

   - Se il database si trova su un archivio NetApp e non è protetto, nella colonna Stato generale viene visualizzato Non protetto.
   - Se il database si trova su un sistema di archiviazione NetApp ed è protetto e non viene eseguita alcuna operazione di backup, nella colonna Stato generale viene visualizzato Backup non eseguito. In caso contrario, lo stato cambierà in Backup non riuscito o Backup riuscito in base allo stato dell'ultimo backup.

È necessario aggiornare le risorse se le istanze vengono rinominate all'esterno di SnapCenter.

## Aggiungere manualmente le risorse all'host del plug-in

Il rilevamento automatico non è supportato sull'host Windows. È necessario aggiungere manualmente le istanze MySQL e le risorse del database.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la configurazione delle connessioni al sistema di archiviazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona il plug-in SnapCenter per MySQL dall'elenco a discesa, quindi fai clic su **Risorse**.
2. Nella pagina Risorse, fare clic su **Aggiungi risorse MySQL**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Specificare il nome del database. |
| Nome host | Inserisci il nome host. |
| Tipo | Seleziona l'istanza. |
| Esempio | Non applicabile. |
| Credenziali | Seleziona le credenziali o aggiungi informazioni per le credenziali.<br><br>Questo è facoltativo. |

4. Nella pagina Fornisci impronta di archiviazione, seleziona un tipo di archiviazione e scegli uno o più volumi, LUN e qtree, quindi fai clic su **Salva**.

   Facoltativo: puoi cliccare su * * icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

5. Facoltativo: nella pagina Impostazioni risorse, immettere coppie chiave-valore personalizzate per il plug-in MySQL.
6. Rivedi il riepilogo e poi clicca su **Fine**.

   I database vengono visualizzati insieme a informazioni quali il nome host, i gruppi di risorse e le policy associate e lo stato generale

Se si desidera consentire agli utenti di accedere alle risorse, è necessario assegnare le risorse agli utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

"Aggiungi un utente o un gruppo e assegna ruoli e risorse"

Dopo aver aggiunto i database, è possibile modificare i dettagli del database MySQL.

## Creare policy di backup per MySQL

Prima di utilizzare SnapCenter per eseguire il backup delle risorse MySQL, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup.

**Prima di iniziare**

- Devi aver definito la tua strategia di backup.

  Per maggiori dettagli, consultare le informazioni sulla definizione di una strategia di protezione dei dati per i database MySQL.

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione di SnapCenter, l'aggiunta di host, la configurazione delle connessioni al sistema di archiviazione e l'aggiunta di risorse.
- Se si stanno replicando snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

  Inoltre, è possibile specificare le impostazioni di replica, script e applicazione nel criterio. Queste opzioni consentono di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.

**Informazioni su questo compito**

- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Nella sezione Impostazioni di backup personalizzate, specificare eventuali impostazioni di backup specifiche che devono essere trasmesse al plug-in in formato chiave-valore.

      È possibile fornire più valori-chiave da passare al plug-in.

6. Nella pagina Snapshot e replica, procedere come segue:

   a. Specificare il tipo di pianificazione selezionando **Su richiesta**, **Ora**, **Giornaliera**, **Settimanale** o **Mensile**.

      È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente di assegnare pianificazioni di backup diverse a ciascuna policy.

Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).

a. Nella sezione Impostazioni snapshot, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina **Tipo di backup**:

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

b. Selezionare un'etichetta di criterio.

È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

7. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapMirror dopo aver creato una copia Snapshot locale** | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e si seleziona solo questa opzione, lo Snapshot creato sul primario non verrà trasferito alla destinazione, ma verrà elencato nella destinazione. Se si seleziona questo snapshot dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il seguente messaggio di errore: La posizione secondaria non è disponibile per il backup con vault/mirroring selezionato.<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup e i cloni relativi alle risorse MySQL nella pagina Topologia" . |
| **Aggiorna SnapVault dopo aver creato una copia Snapshot locale** | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ).<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per ulteriori informazioni su SnapLock Vault, vedere Commit Snapshots to WORM su una destinazione vault<br><br>Vedere "Visualizza i backup e i cloni relativi alle risorse MySQL nella pagina Topologia" . |

| Per questo campo… | Fai questo… |
| --- | --- |
| **Errore nel conteggio dei nuovi tentativi** | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

8. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse.<br>Il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Utilizza il formato del nome personalizzato per la copia snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.

   Ciò aiuta a filtrare le informazioni sullo schermo.

5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Impostazioni applicazione, procedere come segue:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Concediti del tempo per attendere il completamento dell'operazione di snapshot del gruppo di coerenza | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione di snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+

a. Fare clic sulla freccia **Script** e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

b. Fare clic sulla freccia **Configurazioni personalizzate** e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

| Parametro | Collocamento | Descrizione |
|---|---|---|
| ARCHIVE_LOG_ENABLE | (S/N) | Abilita la gestione dei log di archivio per eliminare i log di archivio. |
| CONSERVAZIONE_ARCHIVIO_LOG | numero_di_giorni | Specifica il numero di giorni per cui vengono conservati i registri di archivio.<br><br>Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Specifica il percorso della directory che contiene i log di archivio. |

| Parametro | Collocamento | Descrizione |
| --- | --- | --- |
| ARCHIVE_LOG_EXT | estensione_file | Specifica la lunghezza dell'estensione del file di registro dell'archivio.<br><br>Ad esempio, se il registro di archivio è log_backup_0_0_0_0.16151855 1942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151. |
| ARCHIVE_LOG_RECURSIVE_ SE ARCH | (S/N) | Consente la gestione dei log di archivio all'interno delle sottodirectory.<br><br>È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory. |

Le coppie chiave-valore personalizzate sono supportate per i sistemi plug-in MySQL Linux e non sono supportate per il database MySQL registrato come plug-in centralizzato di Windows.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter utilizza il plug-in per Windows e imposta il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile. | Selezionare * SnapCenter con coerenza del file system*. |
| SnapCenter per creare uno snapshot del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |
| Per immettere il comando da eseguire sull'host per creare copie snapshot. | Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare uno snapshot. |

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando * + *.

I criteri sono elencati nella sezione Configura pianificazioni per i criteri selezionati.

b.

Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove policy_name è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna **Pianificazioni applicate**.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse MySQL sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

a. Selezionare il tipo di criterio di replica.

La politica di replica sincrona non è supportata.

b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

> Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

> Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:

   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.

   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.

   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| **Se lo desidera…** | **Fai questo…** |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.

   e. Fare clic su **OK**.

   Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

> Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell per MySQL

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e

delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire il backup, il ripristino o la clonazione dei database MySQL.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF dati univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell Core utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection
```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

```
PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
-Timeout 60
```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

   Questo esempio mostra come creare una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

4. Aggiungere l'host di comunicazione MySQL a SnapCenter Server.

```
PS C:> Add-SmHost -HostName 10.232.204.61 -OSType Windows -RunAsName
FinanceAdmin -PluginCode mysql
```

5. Installare il pacchetto e il plug-in SnapCenter per MySQL sull'host.

Per Linux:

```
PS C:> Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode
mysql
```

Per Windows:

```
Install-SmHostPackage -HostNames 10.232.204.61 -ApplicationCode mysql
-FilesystemCode scw -RunAsName FinanceAdmin
```

6. Imposta il percorso per SQLLIB.

   Per Windows, il plug-in MySQL utilizzerà il percorso predefinito per la cartella SQLLIB: "C:\Programmi\IBM\SQLLIB\BIN"

   Se si desidera sovrascrivere il percorso predefinito, utilizzare il seguente comando.

```
PS C:> Set-SmConfigSettings -Plugin -HostName 10.232.204.61 -PluginCode
MySQL -configSettings @{"MySQL_SQLLIB_CMD" =
"<custom_path>\IBM\SQLLIB\BIN"}
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup di MySQL

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.
- Per l'operazione di backup basata su copia snapshot, assicurarsi che tutti i database tenant siano validi e attivi.
- Per i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Seleziona * * , quindi selezionare il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi selezionare per chiudere il riquadro del filtro.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive:

     Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
|---|---|
| Concediti del tempo per attendere il completamento dell'operazione "Consistency Group Snapshot" | Selezionare **Urgente**, **Medio** o **Rilassato** per specificare il tempo di attesa per il completamento dell'operazione Snapshot. Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

   - Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.

     È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup. I prescript e i postscript vengono eseguiti nel server SnapCenter .
   - Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   - Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter per creare uno Snapshot a livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi creare uno Snapshot | Selezionare * SnapCenter con coerenza del file system*. |
| Per immettere il comando per creare uno Snapshot | Selezionare **Altro**, quindi immettere il comando per creare uno Snapshot. |

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando * + *.

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.

   Viene visualizzata la pagina della topologia delle risorse.

9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
    - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

      Per informazioni, vedere: "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"

    - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire.

      Per aumentare la dimensione dell'heap Java, individuare il file di script */opt/netapp/init_scripts/scvservice*. In quello script, il comando *do_start method* avvia il servizio plug-in SnapCenter VMware. Aggiornare il comando come segue: *Java -jar -Xmx8192M -Xms4096M*

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   Open-SmConnection  -SMSbaseurl
   https:\\snapctr.demo.netapp.com:8146\
   ```

   Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse manuali utilizzando il cmdlet Add-SmResources.

   Questo esempio mostra come aggiungere un'istanza MySQL:

```
PS C:\> Add-SmResource -HostName 10.32.212.13 -PluginCode MySQL
-ResourceType Instance -ResourceName mysqlinst1 -StorageFootPrint
(@{"VolumeName"="winmysql01_data01";"LUNName"="winmysql01_data01";"S
torageSystem"="scsnfssvm"}) -MountPoints "D:\"
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.
4. Proteggere la risorsa o aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.
5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

   Questo esempio mostra come eseguire il backup di un gruppo di risorse:

   ```
   C:\PS> New-SmBackup -Resources
   @{"Host"="scs000211748.gdl.englab.netapp.com";"Uid"="mysqld_3306";"P
   luginName"="MySQL"} -Policy "MySQL_snapshotbased"
   ```

   Questo esempio esegue il backup di una risorsa protetta:

   ```
   C:\PS> New-SMBackup -Resources
   @{"Host"="10.232.204.42";"Uid"="MDC\SID";"PluginName"="hana"}
   -Policy mysql_policy2
   ```

6. Monitorare lo stato del processo (in esecuzione, completato o non riuscito) utilizzando il cmdlet Get-smJobSummaryReport.

   ```
   PS C:\> Get-smJobSummaryReport -JobID 123
   ```

7. Monitorare i dettagli del processo di backup, come ID del backup e nome del backup, per eseguire operazioni di ripristino o clonazione utilizzando il cmdlet Get-SmBackupReport.

```
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 :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup dei gruppi di risorse

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Informazioni su questo compito**

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in

base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure selezionando e quindi selezionando il tag. Puoi quindi selezionare per chiudere il riquadro del filtro.

3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di backup di MySQL

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.

b. Specificare le date di inizio e fine.

c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.

d. Dal menu a discesa **Stato**, seleziona lo stato del backup.

e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.

4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

> Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

#### Monitorare le operazioni di protezione dei dati sulle istanze MySQL nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Annulla le operazioni di backup per MySQL

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni di MySQL nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario.

**Informazioni su questo compito**

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Consultare la **scheda Riepilogo** per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   La sezione **Scheda riepilogativa** mostra il numero totale di backup basati su copie snapshot e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Aggiorna** si aggiornano i dettagli del backup o del clone.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

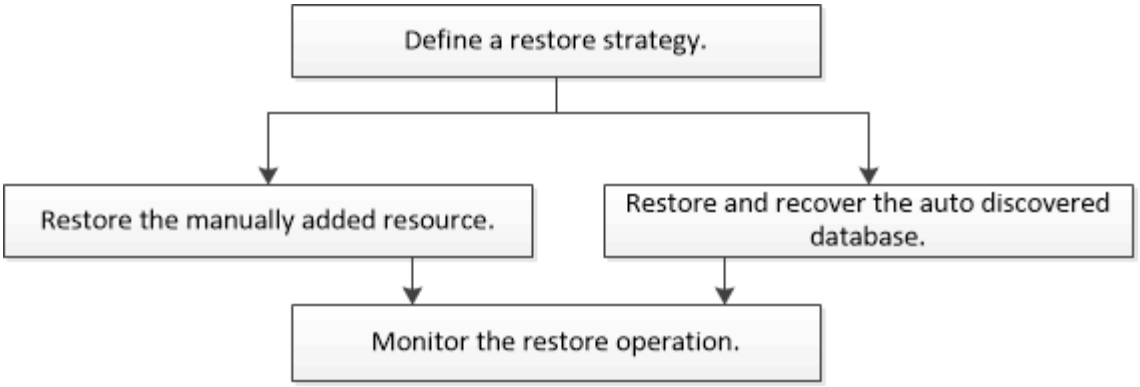
7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .
8. Se vuoi dividere un clone, seleziona il clone dalla tabella, quindi fai clic su .

# Ripristina MySQL

## Ripristina flusso di lavoro

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

"Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup di risorse aggiunto manualmente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

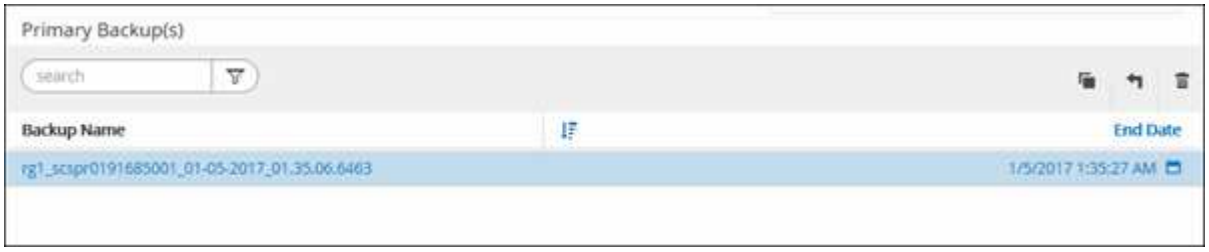
   > Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * * *.




6. Nella pagina Ambito di ripristino, seleziona **Risorsa completa**.

   a. Se si seleziona **Risorsa completa**, verranno ripristinati tutti i volumi di dati configurati del database MySQL.

      Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

      È possibile selezionare più LUN.

      > Se si seleziona **Tutti**, verranno ripristinati tutti i file presenti nei volumi, nei qtree o nei LUN.

7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristina e recupera un backup del database rilevato automaticamente

È possibile utilizzare SnapCenter per ripristinare e recuperare dati da uno o più backup.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- È necessario aver annullato tutte le operazioni di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.
- Per i comandi pre-ripristino, post-ripristino, montaggio e smontaggio, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in*

*Creator\etc\allowed_commands.config*

- Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà.

**Informazioni su questo compito**

- Per le risorse rilevate automaticamente, il ripristino è supportato con SFSR.
- Il ripristino automatico puntuale e aggiornato al minuto non è supportato.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli snapshot SnapLock Vault come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme al tipo, all'host, ai gruppi di risorse associati, ai criteri e allo stato.

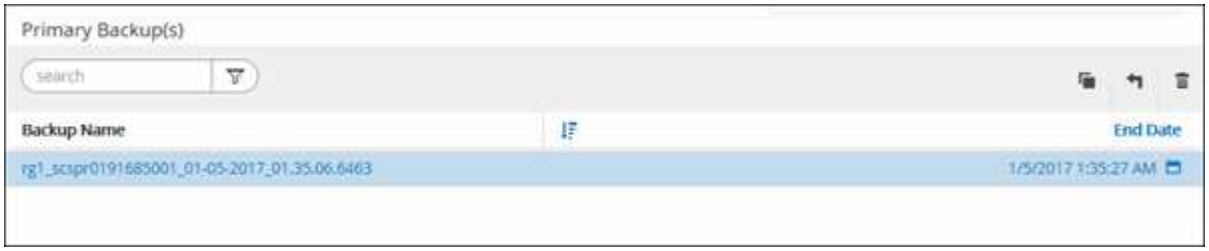
   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

   Se la risorsa non è protetta, nella colonna Stato generale viene visualizzato "Non protetto". Ciò può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * *.




6. Nella pagina Ripristina ambito, seleziona **Risorsa completa** per ripristinare i volumi di dati configurati del database MySQL.
7. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

   I comandi di smontaggio non sono disponibili per le risorse rilevate automaticamente.

8. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.

   I comandi di montaggio non sono disponibili per le risorse rilevate automaticamente.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.

10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Ripristinare le risorse utilizzando i cmdlet di PowerShell

Il ripristino di un backup delle risorse include l'avvio di una sessione di connessione con SnapCenter Server, l'elenco dei backup, il recupero delle informazioni di backup e il ripristino di un backup.

È necessario aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-Smconnection
```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
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
```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitorare le operazioni di ripristino di MySQL

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clona i backup delle risorse MySQL

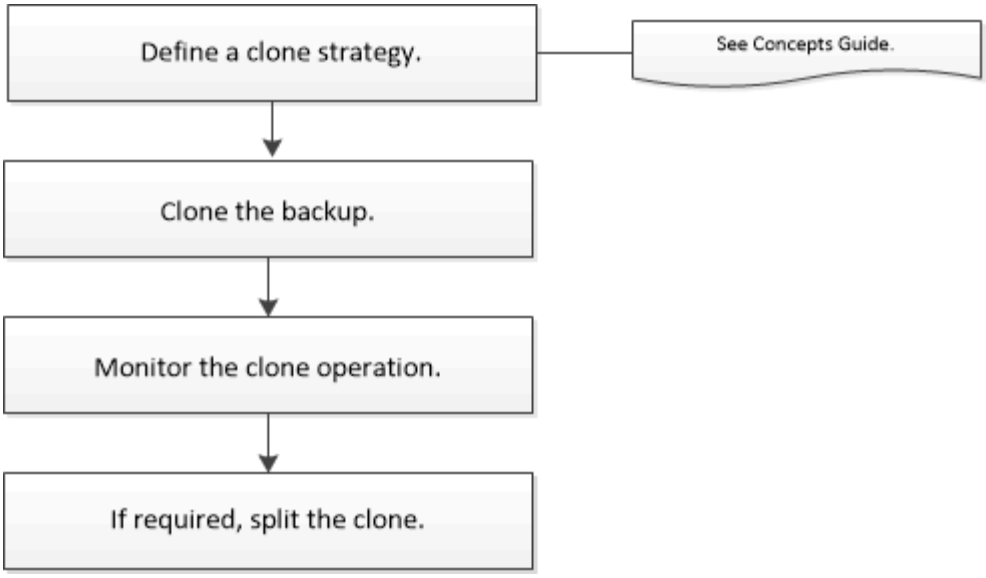
## Flusso di lavoro di clonazione

Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

**Informazioni su questo compito**

- È possibile clonare sul server MySQL di origine.
- È possibile clonare i backup delle risorse per i seguenti motivi:
  - Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione
  - Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
  - Per recuperare dati che sono stati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono informazioni dettagliate sui cmdlet di PowerShell.

## Clonare un backup MySQL

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario.

**Prima di iniziare**

- Avresti dovuto eseguire il backup delle risorse o del gruppo di risorse.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).
- Per i comandi pre-clone o post-clone, è necessario verificare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dai seguenti percorsi:
  - Posizione predefinita sull'host Windows: *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc\allowed_commands.config*
  - Posizione predefinita sull'host Linux: */opt/ NetApp/snapcenter/scc/etc/allowed_commands.config*

Se i comandi non sono presenti nell'elenco dei comandi, l'operazione fallirà. * Per la versione MySQL 5.7, è necessario impostare IGNORE_MYSQLX_PORT = true (per impostazione predefinita false) nel file MySQL. properties.

**Informazioni su questo compito**

- Non è possibile proteggere le istanze MySQL clonate.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere,https://docs.netapp.com/us-en/ontap/volumes/split-flexclone-from-parent-task.html["Dividere un volume FlexClone dal suo volume padre"] .
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, host, gruppi di risorse e policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Scegliere un host su cui creare il clone. |
| Porta | Fornire la porta su cui avviare l'istanza MySQL clonata. |
| Indirizzo IP di esportazione NFS | Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati. |

7. Nella pagina Script, procedere come segue:

   Gli script vengono eseguiti sull'host del plug-in.

   a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
      - Comando pre-clone: elimina i database esistenti con lo stesso nome
      - Comando post-clonazione: verifica un database o avvia un database.
   b. Immettere il comando mount per montare un file system su un host.

      Comando di montaggio per un volume o qtree su una macchina Linux:

   Esempio per NFS: `mount VSERVER_DATA_IP:%VOLUME_NAME_Clone /mnt`

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto

dell'email.

9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
PS C:\> Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Recuperare i backup per eseguire l'operazione di clonazione utilizzando il cmdlet Get-SmBackup.

   Questo esempio mostra che sono disponibili due backup per la clonazione:

```
 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. Avvia un'operazione di clonazione da un backup esistente e specifica gli indirizzi IP di esportazione NFS su cui vengono esportati i volumi clonati.

   Questo esempio mostra che il backup da clonare ha un indirizzo NFSExportIPs pari a 10.32.212.14:

```
PS C:\> New-SmClone -AppPluginCode MySQL -BackupName
"scs000211748_gdl_englab_netapp_com_MySQL_mysqld_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
```

   Se NFSExportIPs non è specificato, l'impostazione predefinita è l'esportazione nell'host di destinazione del clone.

4. Verificare che i backup siano stati clonati correttamente utilizzando il cmdlet Get-SmCloneReport per visualizzare i dettagli del processo di clonazione.

   È possibile visualizzare dettagli quali ID clone, data e ora di inizio, data e ora di fine.

```
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          :
```

## Monitorare le operazioni di clonazione di MySQL

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.

2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su

* *.

5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file *SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

   Per esempio:

   ```
   <add key="CloneSplitStatusCheckPollTime" value="300000" />
   ```

   L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

#### Informazioni correlate

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

## Elimina o dividi i cloni del database MySQL dopo l'aggiornamento SnapCenter

Dopo l'aggiornamento a SnapCenter 4.3, i cloni non saranno più visibili. È possibile eliminare il clone o dividere i cloni dalla pagina Topologia della risorsa da cui sono stati creati i cloni.

#### Informazioni su questo compito

Se si desidera individuare l'impronta di archiviazione dei cloni nascosti, eseguire il seguente comando: `Get-SmClone -ListStorageFootprint`

#### Passi

1. Eliminare i backup delle risorse clonate utilizzando il cmdlet remove-smbackup.
2. Eliminare il gruppo di risorse delle risorse clonate utilizzando il cmdlet remove-smresourcegroup.
3. Rimuovere la protezione della risorsa clonata utilizzando il cmdlet remove-smprotectresource.
4. Selezionare la risorsa padre dalla pagina Risorse.

   Viene visualizzata la pagina della topologia delle risorse.

5. Dalla vista Gestisci copie, selezionare i cloni dai sistemi di archiviazione primari o secondari (con mirroring o replica).
6. Seleziona i cloni e poi clicca per eliminare i cloni o fare clic per dividere i cloni.
7. Fare clic su **OK**.

# Proteggi le applicazioni utilizzando i plug-in supportati NetApp

## Plug-in supportati da NetApp

### Panoramica dei plug-in supportati da NetApp

È possibile utilizzare i plug-in supportati da NetApp , come MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e il plug-in Storage per le applicazioni in uso, quindi utilizzare SnapCenter per eseguire il backup, il ripristino o la clonazione di tali applicazioni. I plug-in supportati NetApp fungono da componenti lato host del software NetApp SnapCenter , consentendo la protezione dei dati e la gestione delle risorse in base alle applicazioni.

Quando sono installati i plug-in supportati NetApp , è possibile utilizzare SnapCenter con la tecnologia NetApp SnapMirror per creare copie mirror di set di backup su un altro volume e utilizzare la tecnologia NetApp SnapVault per eseguire la replica del backup da disco a disco. I plug-in supportati da NetApp possono essere utilizzati sia in ambienti Windows che Linux.

SnapCenterCLI non supporta i comandi dei plug-in supportati NetApp .

NetApp fornisce il plug-in Storage per eseguire operazioni di protezione dei dati del volume di dati sullo storage ONTAP utilizzando il framework plug-in integrato in SnapCenter.

È possibile installare i plug-in supportati da NetApp dalla pagina Aggiungi host.

"Aggiungere host e installare pacchetti plug-in su host remoti."

La politica di supporto SnapCenter coprirà il supporto per il framework dei plug-in, il motore principale e le API associate. Il supporto non coprirà il codice sorgente del plug-in e gli script associati creati sul framework del plug-in.

### Cosa puoi fare con i plug-in supportati da NetApp

È possibile utilizzare i plug-in supportati NetApp , come MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e il plug-in Storage, per le operazioni di protezione dei dati.

- Aggiungere risorse quali database, istanze, documenti o tablespace.
- Creare backup.
- Ripristina dai backup.
- Backup clonati.
- Pianificare le operazioni di backup.
- Monitorare le operazioni di backup, ripristino e clonazione.
- Visualizza i report per le operazioni di backup, ripristino e clonazione.

È possibile utilizzare i plug-in supportati da NetApp per le operazioni di protezione dei dati.

- Acquisisci snapshot di gruppo di coerenza dei volumi di archiviazione nei cluster ONTAP .
- Eseguire il backup delle applicazioni personalizzate utilizzando il framework di pre e post scripting integrato

  È possibile eseguire il backup di un volume ONTAP , di un LUN o di un Qtree.

- Aggiorna gli snapshot acquisiti sul primario su un secondario ONTAP , sfruttando la relazione di replicazione esistente (SnapVault/ SnapMirror/replica unificata) utilizzando la policy SnapCenter

  ONTAP primario e secondario possono essere ONTAP FAS, AFF, ASA, ONTAP Select o Cloud Volumes ONTAP.

- Ripristina il volume ONTAP completo, LUN o file.

  È necessario fornire manualmente il percorso del file corrispondente, poiché le funzionalità di esplorazione o indicizzazione non sono integrate nel prodotto.

  Il ripristino di Qtree o directory non è supportato, ma è possibile clonare ed esportare solo Qtree se l'ambito del backup è definito a livello di Qtree.

## Funzionalità dei plug-in supportati da NetApp

SnapCenter si integra con l'applicazione plug-in e con le tecnologie NetApp sul sistema di storage. Per lavorare con i plug-in supportati NetApp , come MongoDB, ORASCPM (Oracle Applications), SAP ASE, SAP MaxDB e il plug-in Storage, è possibile utilizzare l'interfaccia utente grafica SnapCenter .

- **Interfaccia utente grafica unificata**

  L'interfaccia SnapCenter garantisce standardizzazione e coerenza tra plug-in e ambienti. L'interfaccia SnapCenter consente di completare operazioni di backup, ripristino, recupero e clonazione coerenti su tutti i plug-in, utilizzare report centralizzati, utilizzare viste dashboard immediate, impostare il controllo degli accessi basato sui ruoli (RBAC) e monitorare i processi su tutti i plug-in.

- **Amministrazione centrale automatizzata**

  È possibile pianificare operazioni di backup, configurare la conservazione dei backup basata su criteri ed eseguire operazioni di ripristino. Puoi anche monitorare in modo proattivo il tuo ambiente configurando SnapCenter per inviare avvisi via e-mail.

- **Tecnologia NetApp Snapshot non disruptiva**

  SnapCenter utilizza la tecnologia NetApp Snapshot con i plug-in supportati NetApp per eseguire il backup delle risorse. Gli snapshot occupano uno spazio di archiviazione minimo.

I plug-in supportati da NetApp offrono inoltre i seguenti vantaggi:

- Supporto per flussi di lavoro di backup, ripristino e clonazione
- Sicurezza supportata da RBAC e delega centralizzata dei ruoli

  È anche possibile impostare le credenziali in modo che gli utenti autorizzati SnapCenter dispongano di

autorizzazioni a livello di applicazione.

- Creazione di copie di risorse efficienti in termini di spazio e puntuali per test o estrazione dati utilizzando la tecnologia NetApp FlexClone

  È necessaria una licenza FlexClone sul sistema di archiviazione in cui si desidera creare il clone.

- Supporto per la funzionalità Snapshot del gruppo di coerenza (CG) di ONTAP come parte della creazione di backup.
- Capacità di eseguire più backup contemporaneamente su più host di risorse

  In un'unica operazione, gli snapshot vengono consolidati quando le risorse in un singolo host condividono lo stesso volume.

- Possibilità di creare snapshot utilizzando comandi esterni.
- Capacità di creare snapshot coerenti con il file system in ambienti Windows.

## Tipi di storage supportati dai plug-in supportati da NetApp

SnapCenter supporta un'ampia gamma di tipi di archiviazione sia su macchine fisiche che virtuali. Prima di installare i plug-in supportati NetApp , è necessario verificare il supporto per il tipo di storage in uso.

| Macchina | Tipo di archiviazione |
|---|---|
| Montaggi diretti fisici e NFS sugli host VM (VMDK e LUN RDM non sono supportati). | LUN connesse a FC |
| Montaggi diretti fisici e NFS sugli host VM (VMDK e LUN RDM non sono supportati). | LUN connesse tramite iSCSI |
| Montaggi diretti fisici e NFS sugli host VM (VMDK e LUN RDM non sono supportati). | Volumi connessi tramite NFS |
| VMware ESXi | Datastore vVol sia su NFS che su SAN<br><br>Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |

## Privilegi ONTAP minimi richiesti per il plug-in supportato NetApp

I privilegi ONTAP minimi richiesti variano a seconda dei plug-in SnapCenter utilizzati per la protezione dei dati.

- Comandi di accesso completo: privilegi minimi richiesti per ONTAP 9.12.1 e versioni successive
  - evento genera-autosupport-log
  - spettacolo di storia lavorativa
  - interruzione del lavoro

- spettacolo attributo lun
- lun crea
- lun cancella
- geometria lun
- lun igroup aggiungi
- lun igroup create
- lun igroup elimina
- rinomina lun igroup
- spettacolo di gruppo lun
- mappatura lun aggiungi-nodi-di-segnalazione
- creazione di mappatura lun
- eliminazione della mappatura LUN
- rimozione-nodi-di-segnalazione-mapping-lun
- spettacolo di mappatura lun
- lun modifica
- lun sposta-in-volume
- lun offline
- lun online
- ridimensionamento lun
- serie lun
- spettacolo di lunedì
- interfaccia di rete
- aggiunta regola politica snapmirror
- modifica regola policy snapmirror
- regola di rimozione della policy di SnapMirror
- mostra politica di SnapMirror
- ripristino snapmirror
- spettacolo snapmirror
- snapmirror mostra-cronologia
- aggiornamento snapmirror
- snapmirror update-ls-set
- elenco-destinazioni snapmirror
- versione
- creazione di cloni di volume
- spettacolo di clonazione del volume
- inizio divisione clone volume
- volume clone divisione stop

    - creazione del volume
    - distruzione del volume
    - creazione di clonazione di file di volume
    - file di volume mostra-utilizzo-disco
    - volume offline
    - volume online
    - modifica del volume
    - creazione di volume qtree
    - eliminazione del volume qtree
    - modifica del volume qtree
    - volume qtree mostra
    - limitazione del volume
    - spettacolo di volume
    - creazione di snapshot del volume
    - eliminazione snapshot volume
    - modifica snapshot volume
    - rinomina snapshot volume
    - ripristino snapshot del volume
    - file di ripristino dello snapshot del volume
    - mostra snapshot del volume
    - smontare il volume
    - server virtuale cifs
    - vserver cifs share create
    - vserver cifs share delete
    - vserver cifs shadowcopy mostra
    - vserver cifs share show
    - spettacolo cifs del server virtuale
    - creazione di criteri di esportazione vserver
    - eliminazione della policy di esportazione del server virtuale
    - creazione regola policy di esportazione vserver
    - regola di esportazione-politica del vserver mostra
    - mostra politica di esportazione vserver
    - visualizzazione della connessione vserver iscsi
    - spettacolo vserver
- Comandi di sola lettura: privilegi minimi richiesti per ONTAP 8.3.0 e versioni successive
    - interfaccia di rete

## Preparare i sistemi di archiviazione per la replica SnapMirror e SnapVault per i plug-in supportati da NetApp

È possibile utilizzare un plug-in SnapCenter con la tecnologia ONTAP SnapMirror per creare copie mirror di set di backup su un altro volume e con la tecnologia ONTAP SnapVault per eseguire la replicazione del backup da disco a disco per la conformità agli standard e altri scopi correlati alla governance. Prima di eseguire queste attività, è necessario configurare una relazione di protezione dei dati tra i volumi di origine e di destinazione e inizializzare la relazione.

SnapCenter esegue gli aggiornamenti a SnapMirror e SnapVault dopo aver completato l'operazione Snapshot. Gli aggiornamenti SnapMirror e SnapVault vengono eseguiti come parte del processo SnapCenter ; non creare una pianificazione ONTAP separata.

Se si SnapCenter da un prodotto NetApp SnapManager e si è soddisfatti delle relazioni di protezione dei dati configurate, è possibile saltare questa sezione.

Una relazione di protezione dei dati replica i dati dall'archivio primario (il volume di origine) all'archivio secondario (il volume di destinazione). Quando si inizializza la relazione, ONTAP trasferisce i blocchi di dati a cui si fa riferimento sul volume di origine al volume di destinazione.

SnapCenter non supporta relazioni a cascata tra volumi SnapMirror e SnapVault (**Primario** > **Mirror** > **Vault**). Dovresti usare relazioni fanout.

SnapCenter supporta la gestione delle relazioni SnapMirror flessibili in base alla versione. Per i dettagli sulle relazioni SnapMirror flessibili in base alla versione e su come impostarle, vedere "Documentazione ONTAP" .

## Definire una strategia di backup

Definire una strategia di backup prima di creare i processi di backup garantisce di disporre dei backup necessari per ripristinare o clonare correttamente le risorse. Il contratto di servizio (SLA), l'obiettivo del tempo di ripristino (RTO) e l'obiettivo del punto di ripristino (RPO) determinano in larga misura la strategia di backup.

### Informazioni su questo compito

Un SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. L'RTO è il tempo entro il quale un processo aziendale deve essere ripristinato dopo un'interruzione del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA, RTO e RPO contribuiscono alla strategia di protezione dei dati.

### Passi

1. Determina quando eseguire il backup delle tue risorse.
2. Decidi quanti processi di backup ti servono.
3. Decidi come denominare i tuoi backup.
4. Decidi se desideri gli snapshot del gruppo di coerenza e scegli le opzioni appropriate per eliminarli.
5. Decidi se vuoi utilizzare la tecnologia NetApp SnapMirror per la replica o la tecnologia NetApp SnapVault per la conservazione a lungo termine.

6. Determinare il periodo di conservazione per gli snapshot sul sistema di archiviazione di origine e sulla destinazione SnapMirror .
7. Stabilisci se desideri eseguire dei comandi prima o dopo l'operazione di backup e fornisci un prescript o un postscript.

## Strategia di backup per i plug-in supportati da NetApp

### Pianificazioni di backup delle risorse plug-in supportate NetApp

Il fattore più critico nella determinazione di una pianificazione di backup è la velocità di modifica della risorsa. Quanto più spesso si esegue il backup delle risorse, tanto minore sarà il numero di registri di archivio che SnapCenter dovrà utilizzare per il ripristino, il che può comportare operazioni di ripristino più rapide.

Potresti eseguire il backup di una risorsa molto utilizzata ogni ora, mentre potresti eseguire il backup di una risorsa raramente utilizzata una volta al giorno. Altri fattori includono l'importanza della risorsa per la tua organizzazione, il tuo contratto di servizio (SLA) e il tuo obiettivo del punto di ripristino (RPO).

L'SLA definisce il livello di servizio previsto e affronta molti aspetti correlati al servizio, tra cui la disponibilità e le prestazioni del servizio. RPO definisce la strategia per l'età dei file che devono essere recuperati dall'archivio di backup affinché le normali operazioni possano riprendere dopo un errore. SLA e RPO contribuiscono alla strategia di protezione dei dati.

Le pianificazioni dei backup sono composte da due parti, come segue:

- Frequenza di backup

  La frequenza di backup (la frequenza con cui devono essere eseguiti i backup), chiamata anche tipo di pianificazione per alcuni plug-in, fa parte della configurazione di una policy. Ad esempio, è possibile configurare la frequenza del backup come oraria, giornaliera, settimanale o mensile. È possibile accedere ai criteri nell'interfaccia utente grafica SnapCenter facendo clic su **Impostazioni** > **Criteri**.

- Pianificazioni di backup

  Le pianificazioni dei backup (ovvero il momento esatto in cui devono essere eseguiti i backup) fanno parte della configurazione di una risorsa o di un gruppo di risorse. Ad esempio, se si dispone di un gruppo di risorse con un criterio configurato per backup settimanali, è possibile configurare la pianificazione in modo che il backup venga eseguito ogni giovedì alle 22:00. È possibile accedere alle pianificazioni del gruppo di risorse nell'interfaccia utente grafica SnapCenter facendo clic su **Risorse**, quindi selezionando il plug-in appropriato e facendo clic su **Visualizza** > **Gruppo di risorse**.

### Numero di processi di backup necessari

I fattori che determinano il numero di processi di backup necessari includono la dimensione della risorsa, il numero di volumi utilizzati, la frequenza di modifica della risorsa e il contratto di servizio (SLA).

Il numero di processi di backup scelti dipende in genere dal numero di volumi su cui sono posizionate le risorse. Ad esempio, se si posiziona un gruppo di risorse di piccole dimensioni su un volume e una risorsa di grandi dimensioni su un altro volume, è possibile creare un processo di backup per le risorse di piccole dimensioni e un processo di backup per la risorsa di grandi dimensioni.

### Tipi di strategie di ripristino supportate per le risorse plug-in supportate NetApp aggiunte manualmente

È necessario definire una strategia prima di poter eseguire correttamente le operazioni di ripristino utilizzando SnapCenter. Esistono due tipi di strategie di ripristino per le risorse plug-in supportate NetApp aggiunte manualmente.

Non è possibile recuperare manualmente le risorse plug-in supportate da NetApp .

#### Ripristino completo delle risorse

- Ripristina tutti i volumi, qtree e LUN di una risorsa

Se la risorsa contiene volumi o qtree, gli snapshot acquisiti dopo lo snapshot selezionato per il ripristino su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

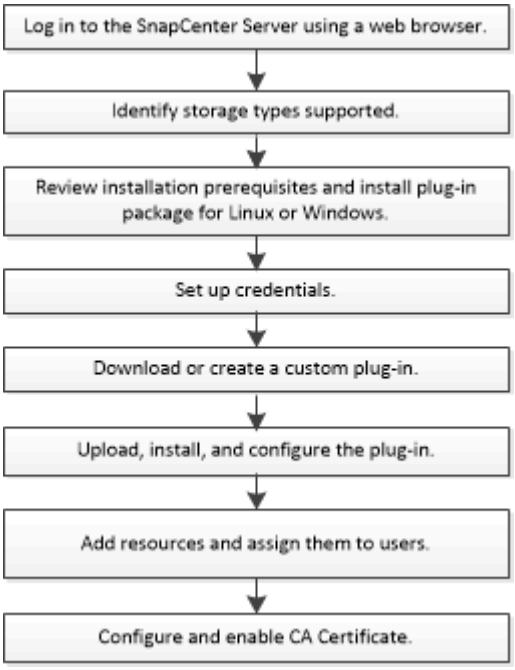
#### Ripristino a livello di file

- Ripristina i file da volumi, qtree o directory
- Ripristina solo i LUN selezionati

# Preparati a installare i plug-in supportati da NetApp

## Flusso di lavoro di installazione dei plug-in supportati da SnapCenter NetApp

Se si desidera proteggere le risorse dei plug-in supportati da NetApp , è necessario installare e configurare i plug-in SnapCenter supportati NetApp .



## Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Windows, Linux o AIX

Prima di aggiungere un host e installare i pacchetti plug-in, è necessario soddisfare tutti i requisiti. I plug-in supportati NetApp sono supportati negli ambienti Windows, Linux e AIX.

Su AIX sono supportate le applicazioni di archiviazione e Oracle.

- È necessario aver installato Java 11 sul proprio host Linux, Windows o AIX.

  IBM Java non è supportato su host Windows e Linux.

- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- I plug-in supportati da NetApp , come MongoDB, ORASCPM, Oracle Applications, SAP ASE, SAP MaxDB e il plug-in Storage, devono essere disponibili sull'host client da cui viene eseguita l'operazione di aggiunta host.

### Generale

Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.

### Host Windows

- È necessario disporre di un utente di dominio con privilegi di amministratore locale e autorizzazioni di accesso locale sull'host remoto.
- Se si gestiscono i nodi del cluster in SnapCenter, è necessario disporre di un utente con privilegi amministrativi per tutti i nodi del cluster.
- È necessario selezionare manualmente il plug-in SnapCenter per Microsoft Windows.

  "Scarica JAVA per Windows"

### Host Linux e AIX

Su AIX sono supportate le applicazioni di archiviazione e Oracle.

- È necessario aver abilitato la connessione SSH basata su password per l'utente root o non root.
- Devi aver installato Java 11 sul tuo host Linux.

  Se si utilizza Windows Server 2019 o Windows Server 2016 per l'host SnapCenter Server, è necessario installare Java 11. Lo strumento Interoperability Matrix (IMT) contiene le informazioni più recenti sui requisiti.

  "Scarica JAVA per Linux"

  "Scarica JAVA per AIX"

  "Strumento matrice di interoperabilità NetApp"

- È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a più percorsi. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

  Assicurati di utilizzare la versione 1.8.7 o successiva di Sudo.

```
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 SCCCMDEXECUTOR =checksum_value==
/opt/NetApp/snapcenter/scc/bin/sccCommandExecutor
LINUX_USER ALL=(ALL) NOPASSWD:SETENV: HPPLCMD, PRECHECKCMD,
CONFIGCHECKCMD, SCCCMDEXECUTOR, SCCMD
Defaults: LINUX_USER env_keep += "IATEMPDIR"
Defaults: LINUX_USER env_keep += "JAVA_HOME"
Defaults: LINUX_USER !visiblepw
Defaults: LINUX_USER !requiretty
```

  *LINUX_USER* è il nome dell'utente non root che hai creato.

  È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

  - *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
  - */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

    L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

### Requisiti dell'host AIX

Prima di installare il pacchetto di plug-in SnapCenter per AIX, è necessario assicurarsi che l'host soddisfi i requisiti.

Su AIX sono supportate le applicazioni di archiviazione e Oracle.

Il plug-in SnapCenter per UNIX, che fa parte del pacchetto di plug-in SnapCenter per AIX, non supporta gruppi di volumi simultanei.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | AIX 7.1 o successivo |
| RAM minima per il plug-in SnapCenter sull'host | 4 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 IBM Java<br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. |

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

#### Configurare i privilegi sudo per gli utenti non root per l'host AIX

SnapCenter 4.4 e versioni successive consentono a un utente non root di installare il pacchetto di plug-in SnapCenter per AIX e di avviare il processo di plug-in. I processi del plug-in verranno eseguiti come utente non root effettivo. È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso a diversi percorsi.

### Cosa ti servirà

- Sudo versione 1.8.7 o successiva.
- Modificare il file */etc/ssh/sshd_config* per configurare gli algoritmi del codice di autenticazione dei messaggi: MAC hmac-sha2-256 e MAC hmac-sha2-512.

  Riavviare il servizio sshd dopo aver aggiornato il file di configurazione.

  Esempio:

```
#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
```

**Informazioni su questo compito**

È necessario configurare i privilegi sudo per l'utente non root per consentire l'accesso ai seguenti percorsi:

- /home/*AIX_USER*/.sc_netapp/snapcenter_aix_host_plugin.bsx
- /custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall
- /posizione_personalizzata/ NetApp/snapcenter/spl/bin/spl

**Passi**

1. Accedere all'host AIX su cui si desidera installare il pacchetto plug-in SnapCenter per AIX.
2. Aggiungere le seguenti righe al file /etc/sudoers utilizzando l'utilità Linux visudo.

```
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
```

Se si dispone di una configurazione RAC, insieme agli altri comandi consentiti, è necessario aggiungere quanto segue al file /etc/sudoers: '/<crs_home>/bin/olsnodes'

È possibile ottenere il valore di *crs_home* dal file */etc/oracle/olr.loc*.

*AIX_USER* è il nome dell'utente non root che hai creato.

È possibile ottenere il valore *checksum_value* dal file **sc_unix_plugins_checksum.txt**, che si trova in:

- *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Windows.
- */opt/ NetApp/snapcenter/SnapManagerWeb/Repository/sc_unix_plugins_checksum.txt* se SnapCenter Server è installato sull'host Linux.

L'esempio deve essere utilizzato solo come riferimento per la creazione dei propri dati.

## Requisiti host per installare il pacchetto plug-in SnapCenter per Windows

Prima di installare il pacchetto di plug-in SnapCenter per Windows, è necessario acquisire familiarità con alcuni requisiti di base di spazio e dimensioni del sistema host.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | Microsoft Windows<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" . |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 5 GB<br><br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |

| Articolo | Requisiti |
| --- | --- |
| Pacchetti software richiesti | • Pacchetto di hosting ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive)<br>• PowerShell Core 7.4.2<br>• Java 11 Oracle Java e OpenJDK<br><br>Java 11 Oracle Java e OpenJDK sono richiesti solo per SAP HANA, IBM Db2, PostgreSQL, MySQL, i plug-in supportati NetApp e altre applicazioni personalizzate che possono essere installate su host Windows.<br><br>Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .<br><br>Per informazioni specifiche sulla risoluzione dei problemi di .NET, vedere "L'aggiornamento o l'installazione SnapCenter non riesce nei sistemi legacy che non dispongono di connettività Internet." |

## Requisiti host per l'installazione del pacchetto plug-in SnapCenter per Linux e AIX

Prima di installare il pacchetto plug-in SnapCenter per Linux o AIX, è necessario assicurarsi che l'host soddisfi i requisiti.

Su AIX sono supportate le applicazioni di archiviazione e Oracle.

| Articolo | Requisiti |
| --- | --- |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| RAM minima per il plug-in SnapCenter sull'host | 1 GB |

| Articolo | Requisiti |
| --- | --- |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 Oracle Java o OpenJDK<br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. |

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp"

## Imposta le credenziali per i plug-in supportati da NetApp

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter . È necessario creare credenziali per l'installazione dei plug-in SnapCenter e credenziali aggiuntive per eseguire operazioni di protezione dei dati su database o file system Windows.

**Prima di iniziare**

- Host Linux o AIX

  È necessario impostare le credenziali per installare i plug-in su host Linux o AIX.

  Per installare e avviare il processo del plug-in, è necessario impostare le credenziali per l'utente root o per un utente non root dotato di privilegi sudo.

  **Procedura consigliata:** Sebbene sia consentito creare credenziali per Linux dopo aver distribuito gli host e installato i plug-in, la procedura consigliata è quella di creare le credenziali dopo aver aggiunto le SVM, prima di distribuire gli host e installare i plug-in.

- Host Windows

  Prima di installare i plug-in è necessario impostare le credenziali di Windows.

  È necessario impostare le credenziali con privilegi di amministratore, inclusi i diritti di amministratore sull'host remoto.

- Applicazioni plug-in supportate NetApp

  Il plug-in utilizza le credenziali selezionate o create durante l'aggiunta di una risorsa. Se una risorsa non richiede credenziali durante le operazioni di protezione dei dati, è possibile impostare le credenziali come **Nessuno**.

**Informazioni su questo compito**

Se si impostano le credenziali per singoli gruppi di risorse e il nome utente non dispone di privilegi di amministratore completi, è necessario assegnare al nome utente almeno i privilegi di gruppo di risorse e di backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina **Credenziali**, specificare le informazioni richieste per la configurazione delle credenziali:

| Per questo campo… | Fai questo… |
|---|---|
| Nome della credenziale | Inserisci un nome per le credenziali. |
| Nome utente | Immettere il nome utente e la password da utilizzare per l'autenticazione.<br>• Amministratore di dominio o qualsiasi membro del gruppo di amministratori<br>Specificare l'amministratore di dominio o un membro del gruppo di amministratori sul sistema su cui si sta installando il plug-in SnapCenter . I formati validi per il campo Nome utente sono:<br>◦ *NetBIOS\NomeUtente*<br>◦ *FQDN dominio\Nome utente*<br>• Amministratore locale (solo per gruppi di lavoro)<br>Per i sistemi che appartengono a un gruppo di lavoro, specificare l'amministratore locale predefinito sul sistema su cui si sta installando il plug-in SnapCenter . È possibile specificare un account utente locale appartenente al gruppo degli amministratori locali se l'account utente dispone di privilegi elevati o se la funzionalità di controllo degli accessi utente è disabilitata sul sistema host. Il formato valido per il campo Nome utente è: *UserName* |
| Password | Inserisci la password utilizzata per l'autenticazione. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di autenticazione | Seleziona il tipo di autenticazione che desideri utilizzare. |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo **Usa privilegi sudo** se si stanno creando credenziali per un utente non root.<br>Applicabile solo agli utenti Linux e AIX. |

5. Fare clic su **OK**.

Dopo aver completato la configurazione delle credenziali, potresti voler assegnare la manutenzione delle credenziali a un utente o a un gruppo di utenti nella pagina Utente e accesso.

## Configurare gMSA su Windows Server 2016 o versioni successive

Windows Server 2016 o versioni successive consente di creare un account di servizio gestito di gruppo (gMSA) che fornisce la gestione automatizzata delle password degli account di servizio da un account di dominio gestito.

**Prima di iniziare**

- Dovresti avere un controller di dominio Windows Server 2016 o versione successiva.
- Dovresti avere un host Windows Server 2016 o versione successiva, che sia membro del dominio.

**Passi**

1. Crea una chiave radice KDS per generare password univoche per ogni oggetto nel tuo gMSA.
2. Per ogni dominio, eseguire il seguente comando dal controller di dominio Windows: Add-KDSRootKey -EffectiveImmediately
3. Crea e configura il tuo gMSA:
   a. Crea un account di gruppo utenti nel seguente formato:

```
 domainName\accountName$
.. Aggiungere oggetti computer al gruppo.
.. Utilizzare il gruppo utenti appena creato per creare il gMSA.
```

   Per esempio,

```
 New-ADServiceAccount -name <ServiceAccountName> -DNSHostName <fqdn>
-PrincipalsAllowedToRetrieveManagedPassword <group>
-ServicePrincipalNames <SPN1,SPN2,…>
.. Correre `Get-ADServiceAccount` comando per verificare l'account di
servizio.
```

4. Configurare gMSA sui tuoi host:

   a. Abilitare il modulo Active Directory per Windows PowerShell sull'host in cui si desidera utilizzare l'account gMSA.

      Per fare ciò, eseguire il seguente comando da PowerShell:

```
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. Riavvia il tuo host.

   b. Installa gMSA sul tuo host eseguendo il seguente comando dal prompt dei comandi di PowerShell: `Install-AdServiceAccount <gMSA>`

   c. Verifica il tuo account gMSA eseguendo il seguente comando: `Test-AdServiceAccount <gMSA>`

5. Assegnare i privilegi amministrativi al gMSA configurato sull'host.

6. Aggiungere l'host Windows specificando l'account gMSA configurato nel server SnapCenter .

   SnapCenter Server installerà i plug-in selezionati sull'host e il gMSA specificato verrà utilizzato come account di accesso al servizio durante l'installazione del plug-in.

## Installa i plug-in supportati da NetApp

#### Aggiungere host e installare pacchetti plug-in su host remoti

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti. È possibile aggiungere un host e installare i pacchetti plug-in per un singolo host o per un cluster.

**Prima di iniziare**

- Dovresti essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .

- È necessario assicurarsi che il servizio di accodamento dei messaggi sia in esecuzione.
- Se si utilizza un account di servizio gestito di gruppo (gMSA), è necessario configurare gMSA con privilegi amministrativi.

  "Configurare l'account del servizio gestito del gruppo su Windows Server 2016 o versioni successive per applicazioni personalizzate"

- Per l'host Windows, è necessario assicurarsi di selezionare il plug-in SnapCenter per Windows.

**Informazioni su questo compito**

- Non è possibile aggiungere uno SnapCenter Server come host plug-in a un altro SnapCenter Server.
- Se si installano i plug-in su un cluster (WSFC), i plug-in vengono installati su tutti i nodi del cluster.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Selezionare **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Tipo di host | Seleziona il tipo di host:<br>• Finestre<br>• Linux<br>• AIX<br>I plug-in supportati da NetApp possono essere utilizzati negli ambienti Windows, Linux e AIX.<br>Su AIX sono supportate le applicazioni di archiviazione e Oracle. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>Per gli ambienti Windows, l'indirizzo IP è supportato per gli host di dominio non attendibili solo se si risolve nel nome di dominio completo (FQDN).<br><br>È possibile immettere gli indirizzi IP o il nome di dominio completo (FQDN) di un host autonomo.<br><br>Se si aggiunge un host tramite SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN. |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove.<br><br>Le credenziali devono disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione **Seleziona i plug-in da installare**, seleziona i plug-in da installare.

   È possibile installare i seguenti plug-in dall'elenco:

   - MongoDB
   - ORASCPM (visualizzato come Oracle Applications)
   - SAP ASE
   - SAP MaxDB
   - Magazzinaggio

6. (Facoltativo) Selezionare **Altre opzioni** per installare gli altri plug-in.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificarne uno nuovo.<br><br>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | I plug-in supportati da NetApp possono essere installati sia su sistemi Windows che Linux.<br><br>• Per il pacchetto di plug-in SnapCenter per Windows, il percorso predefinito è C:\Programmi\ NetApp\ SnapCenter.<br><br>Facoltativamente, puoi personalizzare il percorso.<br><br>• Per il pacchetto di plug-in SnapCenter per Linux e il pacchetto di plug-in SnapCenter per AIX, il percorso predefinito è `/opt/NetApp/snapcenter` .<br><br>Facoltativamente, puoi personalizzare il percorso. |
| Salta i controlli pre-installazione | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in | Per l'host Windows, selezionare questa casella di controllo se si desidera utilizzare l'account di servizio gestito del gruppo (gMSA) per eseguire i servizi plug-in.<br>Fornire il nome gMSA nel seguente formato: domainName\accountName$.<br>gMSA verrà utilizzato come account di accesso al servizio solo per il plug-in SnapCenter per il servizio Windows. |

7. Seleziona **Invia**.

   Se non hai selezionato la casella di controllo **Salta controlli preliminari**, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Lo spazio su disco, la RAM, la versione di PowerShell, la versione di .NET, la posizione (per i plug-in Windows) e la versione di Java (per i plug-in Linux) vengono convalidati rispetto ai requisiti minimi. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati.

   Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config che si trova in `C:\Program Files\NetApp\SnapCenter WebApp` per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, è necessario risolvere il problema.

   In una configurazione HA, se si aggiorna SnapManager.Web.UI.dll.config, è necessario aggiornare il file su entrambi i nodi e riavviare SnapCenter App Pool.

   Il percorso predefinito di Windows è `C:\Program Files\NetApp\SnapCenter WebApp\SnapManager.Web.UI.dll.config`

   Il percorso predefinito di Linux è `/opt/NetApp/snapcenter/SnapManagerWeb/SnapManager.Web.UI.dll.config`

8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi selezionare **Conferma e invia**.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l'avanzamento dell'installazione.

   I file di registro specifici dell'installazione si trovano in `/custom_location/snapcenter/` registri.

#### Installa i pacchetti plug-in SnapCenter per Linux, Windows o AIX su più host remoti utilizzando cmdlet

È possibile installare i pacchetti plug-in SnapCenter per Linux, Windows o AIX su più host contemporaneamente utilizzando il cmdlet Install-SmHostPackage di PowerShell.

**Prima di iniziare**

L'utente che aggiunge un host deve disporre dei diritti amministrativi sull'host.

Su AIX sono supportate le applicazioni di archiviazione e Oracle.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet Open-SmConnection, quindi immettere le credenziali.
3. Installare il plug-in su più host utilizzando il cmdlet Install-SmHostPackage e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

   È possibile utilizzare l'opzione -skipprecheck quando i plug-in sono stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in.

4. Inserisci le tue credenziali per l'installazione remota.

**Installare i plug-in supportati da NetApp sugli host Linux utilizzando l'interfaccia della riga di comando**

È necessario installare i plug-in supportati da NetApp utilizzando l'interfaccia utente (UI) SnapCenter . Se l'ambiente non consente l'installazione remota del plug-in dall'interfaccia utente SnapCenter , è possibile installare i plug-in supportati da NetApp in modalità console o in modalità silenziosa utilizzando l'interfaccia della riga di comando (CLI).

**Passi**

1. Copiare il file di installazione del pacchetto plug-in SnapCenter per Linux (snapcenter_linux_host_plugin.bin) da C:\ProgramData\ NetApp\ SnapCenter\Package Repository all'host in cui si desidera installare i plug-in supportati NetApp .

   È possibile accedere a questo percorso dall'host in cui è installato SnapCenter Server.

2. Dal prompt dei comandi, vai alla directory in cui hai copiato il file di installazione.
3. Installa il plug-in: `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 specifica la porta di comunicazione HTTPS di SMCore.
   - -DSERVER_IP specifica l'indirizzo IP del server SnapCenter .
   - -DSERVER_HTTPS_PORT specifica la porta HTTPS del server SnapCenter .
   - -DUSER_INSTALL_DIR specifica la directory in cui si desidera installare il pacchetto plug-in SnapCenter per Linux.
   - _DINSTALL_LOG_NAME specifica il nome del file di registro.

```
/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. Aggiungere l'host al server SnapCenter utilizzando il cmdlet Add-Smhost e i parametri richiesti.

   Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

5. Accedi a SnapCenter e carica il plug-in supportato da NetApp dall'interfaccia utente o utilizzando i cmdlet di PowerShell.

   È possibile caricare il plug-in supportato da NetApp dall'interfaccia utente facendo riferimento a"Aggiungere host e installare pacchetti plug-in su host remoti" sezione.

   La guida del cmdlet SnapCenter e le informazioni di riferimento sul cmdlet contengono ulteriori informazioni sui cmdlet di PowerShell.

   "Guida di riferimento ai cmdlet del software SnapCenter" .

### Monitorare lo stato di installazione dei plug-in supportati da NetApp

È possibile monitorare l'avanzamento dell'installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l'avanzamento dell'installazione per stabilire quando è completa o se si è verificato un problema.

#### Informazioni su questo compito

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l'elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.

c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.

d. Dal menu a discesa Stato, selezionare lo stato dell'installazione.

e. Fare clic su **Applica**.

4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il certificato CA

### Genera file CSR del certificato CA

È possibile generare una richiesta di firma del certificato (CSR) e importare il certificato che può essere ottenuto da un'autorità di certificazione (CA) utilizzando la CSR generata. Al certificato sarà associata una chiave privata.

CSR è un blocco di testo codificato che viene fornito a un fornitore di certificati autorizzato per ottenere il certificato CA firmato.

La lunghezza della chiave RSA del certificato CA deve essere di almeno 3072 bit.

Per informazioni su come generare un CSR, vedere "Come generare il file CSR del certificato CA" .

Se possiedi il certificato CA per il tuo dominio (*.domain.company.com) o per il tuo sistema (machine1.domain.company.com), puoi saltare la generazione del file CSR del certificato CA. È possibile distribuire il certificato CA esistente con SnapCenter.

Per le configurazioni cluster, il nome del cluster (FQDN del cluster virtuale) e i rispettivi nomi host devono essere menzionati nel certificato CA. È possibile aggiornare il certificato compilando il campo Subject Alternative Name (SAN) prima di ottenere il certificato. Per un certificato con caratteri jolly (*.domain.company.com), il certificato conterrà implicitamente tutti i nomi host del dominio.

### Importa certificati CA

È necessario importare i certificati CA nel server SnapCenter e nei plug-in host Windows utilizzando la console di gestione Microsoft (MMC).

**Passi**

1. Vai alla console di gestione Microsoft (MMC), quindi fai clic su **File** > **Aggiungi/Rimuovi snap-in**.
2. Nella finestra Aggiungi o rimuovi snap-in, seleziona **Certificati** e poi fai clic su **Aggiungi**.
3. Nella finestra snap-in Certificati, selezionare l'opzione **Account computer**, quindi fare clic su **Fine**.
4. Fare clic su **Console Root** > **Certificati – Computer locale** > **Autorità di certificazione radice attendibili** > **Certificati**.
5. Fare clic con il pulsante destro del mouse sulla cartella "Autorità di certificazione radice attendibili", quindi selezionare **Tutte le attività** > **Importa** per avviare la procedura guidata di importazione.
6. Completare la procedura guidata come segue:

| In questa finestra della procedura guidata… | Procedi come segue… |
|---|---|
| Importa chiave privata | Selezionare l'opzione **Sì**, importare la chiave privata, quindi fare clic su **Avanti**. |
| Formato file di importazione | Non apportare modifiche; fare clic su **Avanti**. |
| Sicurezza | Specificare la nuova password da utilizzare per il certificato esportato, quindi fare clic su **Avanti**. |
| Completamento della procedura guidata di importazione del certificato | Rivedi il riepilogo, quindi fai clic su **Fine** per avviare l'importazione. |

Il certificato di importazione deve essere incluso nella chiave privata (i formati supportati sono: *.pfx, *.p12 e *.p7b).

7. Ripetere il passaggio 5 per la cartella "Personale".

#### Ottieni l'impronta digitale del certificato CA

L'impronta digitale di un certificato è una stringa esadecimale che identifica un certificato. L'impronta digitale viene calcolata dal contenuto del certificato utilizzando un algoritmo di identificazione digitale.

#### Passi

1. Eseguire le seguenti operazioni sulla GUI:
   a. Fare doppio clic sul certificato.
   b. Nella finestra di dialogo Certificato, fare clic sulla scheda **Dettagli**.
   c. Scorri l'elenco dei campi e clicca su **Impronta digitale**.
   d. Copia i caratteri esadecimali dalla casella.
   e. Rimuovere gli spazi tra i numeri esadecimali.

      Ad esempio, se l'impronta digitale è: "a9 09 50 2d d8 2a e4 14 33 e6 f8 38 86 b0 0d 42 77 a3 2a 7b", dopo aver rimosso gli spazi, sarà: "a909502dd82ae41433e6f83886b00d4277a32a7b".

2. Eseguire le seguenti operazioni da PowerShell:
   a. Eseguire il seguente comando per elencare l'identificazione personale del certificato installato e identificare il certificato installato di recente tramite il nome dell'oggetto.

      *Get-ChildItem -Percorso Cert:\LocalMachine\My*

   b. Copia l'impronta digitale.

#### Configurare il certificato CA con i servizi plug-in host di Windows

È necessario configurare il certificato CA con i servizi plug-in host di Windows per attivare il certificato digitale installato.

Eseguire i seguenti passaggi sul server SnapCenter e su tutti gli host plug-in in cui sono già distribuiti i certificati CA.

**Passi**

1. Rimuovere l'associazione del certificato esistente con la porta predefinita SMCore 8145, eseguendo il seguente comando:

   ```
   > netsh http delete sslcert ipport=0.0.0.0:_<SMCore Port>
   ```

   Per esempio:

   ```
    > netsh http delete sslcert ipport=0.0.0.0:8145
   . Associare il certificato appena installato ai servizi plug-in host di
   Windows eseguendo i seguenti comandi:
   ```

   ```
   > $cert = "_<certificate thumbprint>_"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

   Per esempio:

   ```
   > $cert = "a909502dd82ae41433e6f83886b00d4277a32a7b"
   > $guid = [guid]::NewGuid().ToString("B")
   > netsh http add sslcert ipport=0.0.0.0: _<SMCore Port>_ certhash=$cert
   appid="$guid"
   ```

#### Configurare il certificato CA per il servizio plug-in supportato da NetApp sull'host Linux

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file 'keystore.jks', che si trova in */opt/ NetApp/snapcenter/scc/etc* sia come archivio attendibile che come archivio chiavi.

##### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave 'KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks
```

Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

3. Riavviare il servizio dopo aver modificato la password.

La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in: /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungi un certificato radice o intermedio:

```
 keytool -import -trustcacerts -alias myRootCA -file
/root/USERTrustRSA_Root.cer -keystore keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi per collegare trust-store.
```

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in /opt/ NetApp/snapcenter/scc/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
keytool -list -v -keystore keystore.jks
```

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

```
keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
```

5. Elenca i certificati aggiunti nel keystore.

```
keytool -list -v -keystore keystore.jks
```

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

```
 keytool -keypasswd -alias "alias_name_in_CA_cert" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "long_alias_name" -destalias "simple_alias"
-keystore keystore.jks
. Configurare il nome alias dal certificato CA nel file
agent.properties.
```

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

8. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in

**Informazioni su questo compito**

- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è ' opt/ NetApp/snapcenter/scc/etc/crl'.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file agent.properties in base alla chiave CRL_PATH.

   È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

### Configurare il certificato CA per il servizio plug-in supportato da NetApp sull'host Windows

È necessario gestire la password del keystore dei plug-in e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per il trust-store dei

plug-in e configurare la coppia di chiavi firmata dalla CA per il trust-store dei plug-in con il servizio plug-in SnapCenter per attivare il certificato digitale installato.

Il plug-in utilizza il file *keystore.jks*, che si trova in *C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc* sia come archivio attendibile che come archivio chiavi.

#### Gestisci la password per il keystore del plug-in e l'alias della coppia di chiavi firmata dalla CA in uso

**Passi**

1. È possibile recuperare la password predefinita del keystore del plug-in dal file delle proprietà dell'agente del plug-in.

   È il valore corrispondente alla chiave *KEYSTORE_PASS*.

2. Cambia la password del keystore:

   *keytool -storepasswd -keystore keystore.jks*

   > Se il comando "keytool" non viene riconosciuto nel prompt dei comandi di Windows, sostituire il comando keytool con il suo percorso completo.

   *C:\Programmi\Java\<versione_jdk>\bin\keytool.exe" -storepasswd -keystore keystore.jks*

3. Modificare la password per tutti gli alias delle voci di chiave privata nel keystore con la stessa password utilizzata per il keystore:

   *keytool -keypasswd -alias "alias_name_in_cert" -keystore keystore.jks*

   Aggiornare lo stesso per la chiave KEYSTORE_PASS nel file *agent.properties*.

4. Riavviare il servizio dopo aver modificato la password.

   > La password per il keystore del plug-in e per tutte le password alias associate alla chiave privata devono essere le stesse.

#### Configurare i certificati radice o intermedi per collegare trust-store

È necessario configurare i certificati radice o intermedi senza la chiave privata per collegare trust-store.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungi un certificato radice o intermedio:

   *keytool -import -trustcacerts -alias myRootCA -file /root/USERTrustRSA_Root.cer -keystore keystore.jks*

5. Riavviare il servizio dopo aver configurato i certificati radice o intermedi per collegare trust-store.

Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

#### Configurare la coppia di chiavi firmata dalla CA per collegare l'archivio attendibile

È necessario configurare la coppia di chiavi firmata dalla CA nel trust-store del plug-in.

**Passi**

1. Passare alla cartella contenente il keystore del plug-in *C:\Programmi\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\etc*
2. Individuare il file *keystore.jks*.
3. Elenca i certificati aggiunti nel keystore:

   *keytool -list -v -keystore keystore.jks*

4. Aggiungere il certificato CA con chiave sia privata che pubblica.

   *keytool -importkeystore -srckeystore /root/snapcenter.ssl.test.netapp.com.pfx -srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS*

5. Elenca i certificati aggiunti nel keystore.

   *keytool -list -v -keystore keystore.jks*

6. Verificare che il keystore contenga l'alias corrispondente al nuovo certificato CA aggiunto al keystore.
7. Modificare la password della chiave privata aggiunta per il certificato CA con la password del keystore.

   La password predefinita del keystore del plug-in è il valore della chiave KEYSTORE_PASS nel file agent.properties.

   *keytool -keypasswd -alias "nome_alias_in_CA_cert" -keystore keystore.jks*

8. Configurare il nome alias dal certificato CA nel file *agent.properties*.

   Aggiornare questo valore in base alla chiave SCC_CERTIFICATE_ALIAS.

9. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA per collegare trust-store.

#### Configurare l'elenco di revoche dei certificati (CRL) per i plug-in SnapCenter

**Informazioni su questo compito**

- Per scaricare l'ultimo file CRL per il certificato CA correlato, vedere "Come aggiornare il file dell'elenco di revoche dei certificati in SnapCenter CA Certificate" .
- I plug-in SnapCenter cercheranno i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per i plug-in SnapCenter è *'C:\Program Files\ NetApp\ SnapCenter\Snapcenter Plug-in Creator\ etc\crl'*.

**Passi**

1. È possibile modificare e aggiornare la directory predefinita nel file *agent.properties* in base alla chiave CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

I certificati in arrivo saranno verificati rispetto a ciascun CRL.

#### Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

**Prima di iniziare**

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

**Dopo aver finito**

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Prepararsi alla protezione dei dati

## Prerequisiti per l'utilizzo dei plug-in supportati NetApp

Prima di utilizzare i plug-in supportati da SnapCenter NetApp , l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server.
- Accedi a SnapCenter Server.
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione e creando credenziali, se applicabile.

- Aggiungi gli host, installa e carica i plug-in.
- Se applicabile, installare Java 11 sull'host del plug-in.
- Se si dispone di più percorsi dati (LIF) o di una configurazione dNFS, è possibile eseguire le seguenti operazioni utilizzando la CLI SnapCenter sull'host del database:
  - Per impostazione predefinita, tutti gli indirizzi IP dell'host del database vengono aggiunti alla policy di esportazione dell'archiviazione NFS nella macchina virtuale di archiviazione (SVM) per i volumi clonati. Se si desidera avere un indirizzo IP specifico o limitarsi a un sottoinsieme di indirizzi IP, eseguire la CLI Set-PreferredHostIPsInStorageExportPolicy.
  - Se sono presenti più percorsi dati (LIF) nelle SVM, SnapCenter sceglie il percorso dati (LIF) appropriato per il montaggio del volume clonato NFS. Tuttavia, se si desidera specificare un percorso dati specifico (LIF), è necessario eseguire la CLI Set-SvmPreferredDataPath. Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo *Get-Help nome_comando*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .
- Se desideri la replica del backup, imposta SnapMirror e SnapVault.
- Assicurarsi che la porta 9090 non sia utilizzata da altre applicazioni sull'host.

  La porta 9090 deve essere riservata per l'uso da parte dei plug-in supportati NetApp , oltre alle altre porte richieste da SnapCenter.

## Come vengono utilizzate risorse, gruppi di risorse e policy per proteggere le risorse dei plug-in supportati da NetApp

Prima di utilizzare SnapCenter, è utile comprendere i concetti di base relativi alle operazioni di backup, clonazione e ripristino che si desidera eseguire. Interagisci con risorse, gruppi di risorse e policy per diverse operazioni.

- Le risorse sono in genere database, file system Windows o macchine virtuali di cui si esegue il backup o la clonazione con SnapCenter.
- Un gruppo di risorse SnapCenter è una raccolta di risorse su un host o cluster.

  Quando si esegue un'operazione su un gruppo di risorse, tale operazione viene eseguita sulle risorse definite nel gruppo di risorse in base alla pianificazione specificata per il gruppo di risorse.

  È possibile eseguire il backup su richiesta di una singola risorsa o di un gruppo di risorse. È anche possibile eseguire backup pianificati per singole risorse e gruppi di risorse.
- Le policy specificano la frequenza di backup, la conservazione delle copie, la replica, gli script e altre caratteristiche delle operazioni di protezione dei dati.

  Quando si crea un gruppo di risorse, si selezionano una o più policy per quel gruppo. È anche possibile selezionare un criterio quando si esegue un backup su richiesta per una singola risorsa.

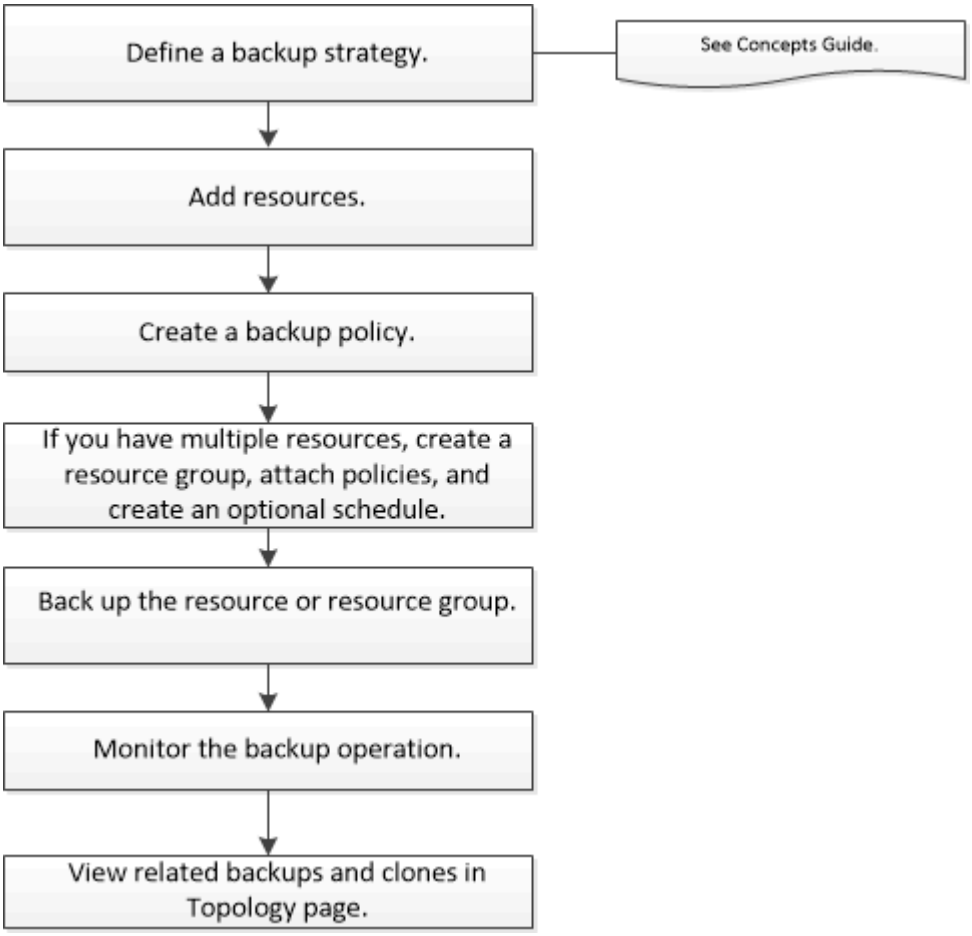
Pensa a un gruppo di risorse come a qualcosa che definisce *cosa* vuoi proteggere e quando vuoi proteggerlo in termini di giorno e ora. Pensa a una politica come a qualcosa che definisce *come* vuoi proteggerla. Ad esempio, se si esegue il backup di tutti i database o di tutti i file system di un host, è possibile creare un gruppo di risorse che includa tutti i database o tutti i file system nell'host. È quindi possibile associare due policy al gruppo di risorse: una policy giornaliera e una policy oraria. Quando si crea il gruppo di risorse e si associano i criteri, è possibile configurare il gruppo di risorse per eseguire un backup basato su file ogni giorno e un'altra pianificazione che esegue un backup basato su snapshot ogni ora.

# Eseguire il backup delle risorse dei plug-in supportati NetApp

## Eseguire il backup delle risorse dei plug-in supportati NetApp

Il flusso di lavoro del backup include la pianificazione, l'identificazione delle risorse per il backup, la gestione dei criteri di backup, la creazione di gruppi di risorse e l'associazione di criteri, la creazione di backup e il monitoraggio delle operazioni.

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di backup:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter"

## Aggiungi risorse ai plug-in supportati da NetApp

È necessario aggiungere le risorse di cui si desidera eseguire il backup o la clonazione. A seconda dell'ambiente, le risorse potrebbero essere istanze di database o raccolte di cui si desidera eseguire il backup o la clonazione.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host, la creazione di connessioni al sistema di archiviazione e l'aggiunta di credenziali.

- È necessario aver caricato i plug-in su SnapCenter Server.

**Passi**

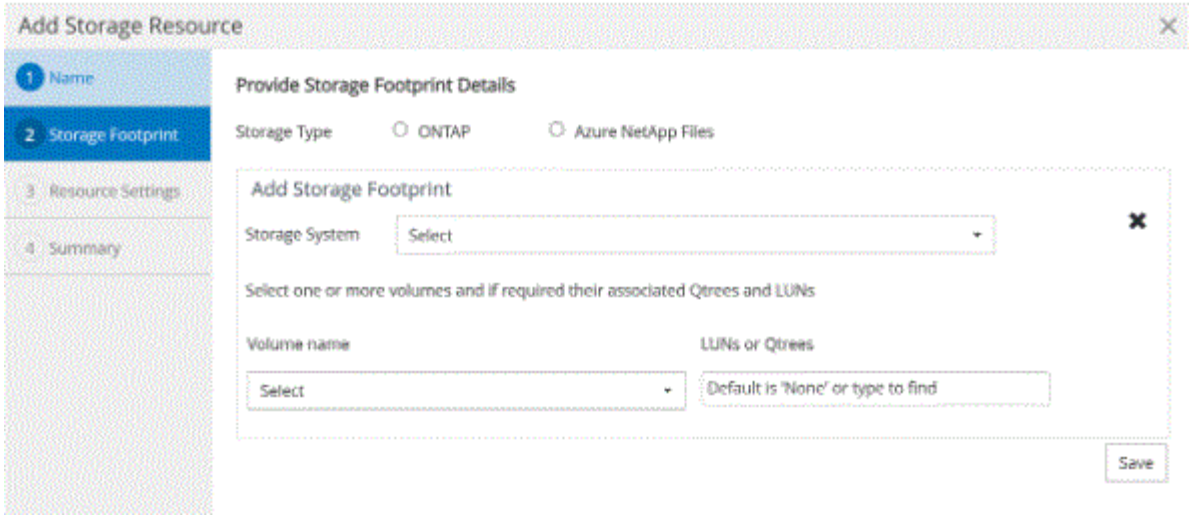
1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Aggiungi risorsa**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Inserisci il nome della risorsa. |
| Nome host | Selezionare l'host. |
| Tipo | Seleziona il tipo. Il tipo è definito dall'utente in base al file di descrizione del plug-in. Ad esempio, database e istanza.<br><br>Nel caso in cui il tipo selezionato abbia un elemento padre, immettere i dettagli dell'elemento padre. Ad esempio, se il tipo è Database e l'elemento padre è Istanza, immettere i dettagli dell'istanza. |
| Nome della credenziale | Seleziona Credenziale o crea una nuova credenziale. |
| Sentieri del Monte | Immettere i percorsi di montaggio in cui è montata la risorsa. Questo è applicabile solo per un host Windows. |

4. Nella pagina Fornisci impronta di archiviazione, seleziona un sistema di archiviazione e scegli uno o più volumi, LUN e qtree, quindi seleziona **Salva**.

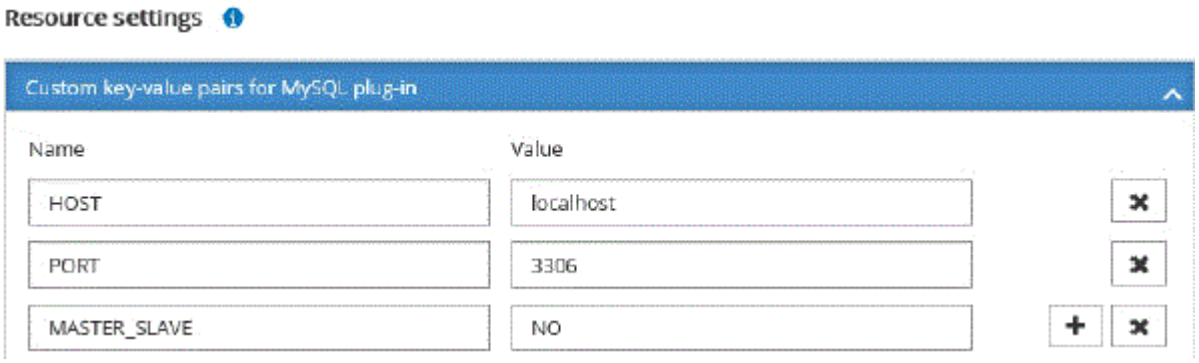
   Facoltativo: seleziona il icona per aggiungere più volumi, LUN e qtree da altri sistemi di archiviazione.

   I plug-in supportati NetApp non supportano il rilevamento automatico delle risorse. Anche i dettagli di archiviazione degli ambienti fisici e virtuali non vengono rilevati automaticamente. Durante la creazione delle risorse è necessario fornire le informazioni di archiviazione per gli ambienti fisici e virtuali.




5. Nella pagina Impostazioni risorsa, fornire coppie chiave-valore personalizzate per la risorsa.

   Assicurarsi che il nome delle chiavi personalizzate sia scritto in maiuscolo.




   Per i rispettivi parametri del plug-in, fare riferimento"Parametri per configurare la risorsa"

6. Rivedi il riepilogo e seleziona **Fine**.

**Risultato**

Le risorse vengono visualizzate insieme a informazioni quali tipo, nome dell'host o del cluster, gruppi di risorse e policy associati e stato generale.

È necessario aggiornare le risorse se i database vengono rinominati all'esterno di SnapCenter.

**Dopo aver finito**

Se si desidera consentire l'accesso alle risorse ad altri utenti, l'amministratore SnapCenter deve assegnare le risorse a tali utenti. Ciò consente agli utenti di eseguire le azioni per le quali dispongono delle autorizzazioni sulle risorse loro assegnate.

Dopo aver aggiunto le risorse, è possibile modificarne i dettagli. Se a una risorsa plug-in supportata NetApp sono associati dei backup, non è possibile modificare i seguenti campi: nome della risorsa, tipo di risorsa e nome host.

### Parametri per configurare la risorsa

Se si aggiungono i plug-in manualmente, è possibile utilizzare i seguenti parametri per configurare la risorsa nella pagina Impostazioni risorsa.

#### Plug-in per MongoDB

Impostazioni delle risorse:

- MONGODB_APP_SERVER=(per tipo di risorsa come cluster shardato) o MONGODB_REPLICASET_SERVER=(per tipo di risorsa come replicaset)
- OPLOG_PATH=(Parametro facoltativo nel caso in cui venga fornito da MongoDB.propertiesfile)
- MONGODB_AUTHENTICATION_TYPE= (PLAIN per l'autenticazione LDAP e None per le altre)

È necessario fornire i seguenti parametri nel file MongoDB.properties:

- DISABILITA_AVVIO_ARRESTO_SERVIZI=
  - N se i servizi di avvio/arresto vengono eseguiti dal plug-in.
  - Y se i servizi di avvio/**arresto vengono eseguiti dall'utente.
  - Il parametro facoltativo come valore predefinito è impostato su N.
- OPLOG_PATH_= (Parametro facoltativo nel caso in cui sia già fornito come coppia chiave-valore personalizzata in SnapCenter).

#### Plug-in per MaxDB

Impostazioni delle risorse:

- XUSER_ENABLE (Y|N) abilita o disabilita l'uso di un xuser per MaxDB in modo che non sia richiesta una password per l'utente del database.
- HANDLE_LOGWRITER (Y|N) esegue le operazioni di sospensione del logwriter (N) o di ripresa del logwriter (Y).
- DBMCLICMD (path_to_dbmcli_cmd) specifica il percorso al comando dbmcli di MaxDB. Se non impostato, viene utilizzato dbmcli sul percorso di ricerca.

  Per l'ambiente Windows, il percorso deve essere racchiuso tra virgolette doppie ("…").

- SQLCLICMD (path_to_sqlcli_cmd) specifica il percorso al comando sqlcli di MaxDB. Se il percorso non è impostato, nel percorso di ricerca viene utilizzato sqlcli.
- MAXDB_UPDATE_HIST_LOG (Y|N) indica al programma di backup di MaxDB se aggiornare il registro cronologico di MaxDB.
- MAXDB_CHECK_SNAPSHOT_DIR: Esempio, SID1:directory[,directory…]; [SID2:directoary[,directory…] verifica che un'operazione di copia Snap Creator Snapshot abbia esito positivo e garantisce che lo snapshot venga creato.

  Questo vale solo per NFS. La directory deve puntare alla posizione che contiene la directory .snapshot. È possibile includere più directory in un elenco separato da virgole.

  In MaxDB 7.8 e versioni successive, la richiesta di backup del database è contrassegnata come Non riuscita nella cronologia dei backup.

- MAXDB_BACKUP_TEMPLATES: specifica un modello di backup per ciascun database.

  Il modello deve esistere ed essere un tipo esterno di modello di backup. Per abilitare l'integrazione degli snapshot per MaxDB 7.8 e versioni successive, è necessario disporre della funzionalità del server in background MaxDB e di un modello di backup MaxDB di tipo ESTERNO già configurato.

- MAXDB_BG_SERVER_PREFIX: specifica il prefisso per il nome del server in background.

  Se è impostato il parametro MAXDB_BACKUP_TEMPLATES, è necessario impostare anche il parametro MAXDB_BG_SERVER_PREFIX. Se non si imposta il prefisso, verrà utilizzato il valore predefinito na_bg_.

#### Plug-in per SAP ASE

Impostazioni delle risorse:

- SYBASE_SERVER (data_server_name) specifica il nome del server dati Sybase (opzione -S nel comando isql). Ad esempio, p_test.
- SYBASE_DATABASES_EXCLUDE (db_name) consente di escludere i database se viene utilizzato il costrutto "ALL".

  È possibile specificare più database utilizzando un elenco separato da punto e virgola. Ad esempio: pubs2;test_db1.

- SYBASE_USER: user_name specifica l'utente del sistema operativo che può eseguire il comando isql.

  Richiesto per UNIX. Questo parametro è obbligatorio se l'utente che esegue i comandi di avvio e arresto di Snap Creator Agent (in genere l'utente root) e l'utente che esegue il comando isql sono diversi.

- SYBASE_TRAN_DUMP db_name:directory_path consente di eseguire un dump delle transazioni Sybase dopo aver creato uno snapshot. Ad esempio, pubs2:/sybasedumps/ pubs2

  È necessario specificare ciascun database per il quale è necessario eseguire il dump delle transazioni.

- SYBASE_TRAN_DUMP_COMPRESS (Y|N ) abilita o disabilita la compressione nativa del dump delle transazioni Sybase.
- SYBASE_ISQL_CMD (ad esempio, /opt/sybase/OCS-15_0/bin/isql) definisce il percorso al comando isql.
- SYBASE_EXCLUDE_TEMPDB (Y|N) consente di escludere automaticamente i database temporanei creati dall'utente.

#### Plug-in per applicazioni Oracle (ORASCPM)

Impostazioni delle risorse:

- SQLPLUS_CMD specifica il percorso per SQLplus.
- ORACLE_DATABASES elenca i database Oracle di cui eseguire il backup e l'utente corrispondente (database:utente).
- CNTL_FILE_BACKUP_DIR specifica la directory per il backup del file di controllo.
- ORA_TEMP specifica la directory per i file temporanei.
- ORACLE_HOME specifica la directory in cui è installato il software Oracle.
- ARCHIVE_LOG_ONLY specifica se eseguire o meno il backup dei log di archivio.

- ORACLE_BACKUPMODE specifica se eseguire il backup online o offline.
- ORACLE_EXPORT_PARAMETERS specifica se le variabili di ambiente definite sopra devono essere riesportate durante l'esecuzione di */bin/su <utente che esegue sqlplus> -c sqlplus /nolog <cmd>*. Questo è in genere il caso in cui l'utente che esegue sqlplus non ha impostato tutte le variabili di ambiente necessarie per connettersi al database tramite *connect / come sysdba*.

## Creare policy per le risorse plug-in supportate NetApp

Prima di utilizzare SnapCenter per eseguire il backup di risorse specifiche dei plug-in supportati NetApp , è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

**Prima di iniziare**

- Avresti dovuto definire la tua strategia di backup.

  Per maggiori dettagli, consultare le informazioni sulla definizione di una strategia di protezione dei dati per i plug-in supportati NetApp .

- Avresti dovuto prepararti alla protezione dei dati.

  La preparazione per la protezione dei dati include attività quali l'installazione di SnapCenter, l'aggiunta di host, la creazione di connessioni al sistema di archiviazione e l'aggiunta di risorse.

- Le macchine virtuali di archiviazione (SVM) devono essere assegnate all'utente per operazioni di mirroring o vault.

  Se si stanno replicando gli snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.

- Avresti dovuto aggiungere manualmente le risorse che desideri proteggere.

**Informazioni su questo compito**

- Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup. Inoltre, è possibile specificare le impostazioni di replica, script e applicazione.
- Specificare le opzioni in un criterio consente di risparmiare tempo quando si desidera riutilizzare il criterio per un altro gruppo di risorse.
- SnapLock
  - Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.
  - Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.
  - Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

> Le impostazioni primarie SnapLock sono gestite nella policy di backup SnapCenter , mentre le impostazioni secondarie SnapLock sono gestite da ONTAP.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e i dettagli della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   a. Seleziona il tipo di archiviazione.
   b. Nella sezione Impostazioni di backup personalizzate, specificare eventuali impostazioni di backup specifiche che devono essere trasmesse al plug-in in formato chiave-valore.

      È possibile fornire più valori-chiave da passare al plug-in.
6. Nella pagina Snapshot e replica, procedere come segue:
   a. Specificare il tipo di pianificazione selezionando **Su richiesta**, **Ora**, **Giornaliera**, **Settimanale** o **Mensile**.

      È possibile specificare la pianificazione (data di inizio, data di fine e frequenza) per l'operazione di backup durante la creazione di un gruppo di risorse. Ciò consente di creare gruppi di risorse che condividono la stessa policy e la stessa frequenza di backup, ma consente di assegnare pianificazioni di backup diverse a ciascuna policy.

      Se hai programmato per le 2:00, la pianificazione non verrà attivata durante l'ora legale (DST).
   a. Nella sezione Impostazioni snapshot, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina **Tipo di backup**:

| Se lo desidera… | Poi… |
| --- | --- |
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare giorni, mesi o anni.<br><br>Il periodo di conservazione SnapLock dovrebbe essere inferiore a 100 anni. |

b. Selezionare un'etichetta di criterio.

È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

7. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
| --- | --- |
| **Aggiorna SnapMirror dopo aver creato una copia Snapshot locale** | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Se la relazione di protezione in ONTAP è di tipo Mirror e Vault e si seleziona solo questa opzione, lo Snapshot creato sul primario non verrà trasferito alla destinazione, ma verrà elencato nella destinazione. Se si seleziona questo snapshot dalla destinazione per eseguire un'operazione di ripristino, viene visualizzato il seguente messaggio di errore: La posizione secondaria non è disponibile per il backup con vault/mirroring selezionato.<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario.<br><br>Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Vedere "Visualizza i backup e i cloni correlati alle risorse dei plug-in supportati da NetApp nella pagina Topologia" . |
| **Aggiorna SnapVault dopo aver creato una copia Snapshot locale** | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ).<br><br>Durante la replicazione secondaria, il tempo di scadenza SnapLock carica il tempo di scadenza SnapLock primario. Facendo clic sul pulsante **Aggiorna** nella pagina Topologia, vengono aggiornati i tempi di scadenza SnapLock secondari e primari recuperati da ONTAP.<br><br>Quando SnapLock è configurato solo sul secondario da ONTAP noto come SnapLock Vault, facendo clic sul pulsante **Aggiorna** nella pagina Topologia si aggiorna il periodo di blocco sul secondario recuperato da ONTAP.<br><br>Per ulteriori informazioni su SnapLock Vault, vedere Commit degli snapshot in WORM su una destinazione vault.<br><br>Vedere "Visualizza i backup e i cloni correlati alle risorse dei plug-in supportati da NetApp nella pagina Topologia" . |

| Per questo campo… | Fai questo… |
| --- | --- |
| **Errore nel conteggio dei nuovi tentativi** | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

È necessario configurare i criteri di conservazione SnapMirror in ONTAP per l'archiviazione secondaria per evitare di raggiungere il limite massimo di snapshot sull'archiviazione secondaria.

8. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega criteri

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Consente di eseguire il backup di tutti i dati associati a una determinata applicazione contemporaneamente. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona Nuovo gruppo di risorse.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse.<br><br>Nota: il nome del gruppo di risorse non deve superare i 250 caratteri. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse.<br><br>Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.<br><br>Ad esempio, *customtext_resource group_policy_hostname o resource group_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp. |

4. Facoltativo: nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa

dall'elenco a discesa **Tipo di risorsa**.

Ciò aiuta a filtrare le informazioni sullo schermo.

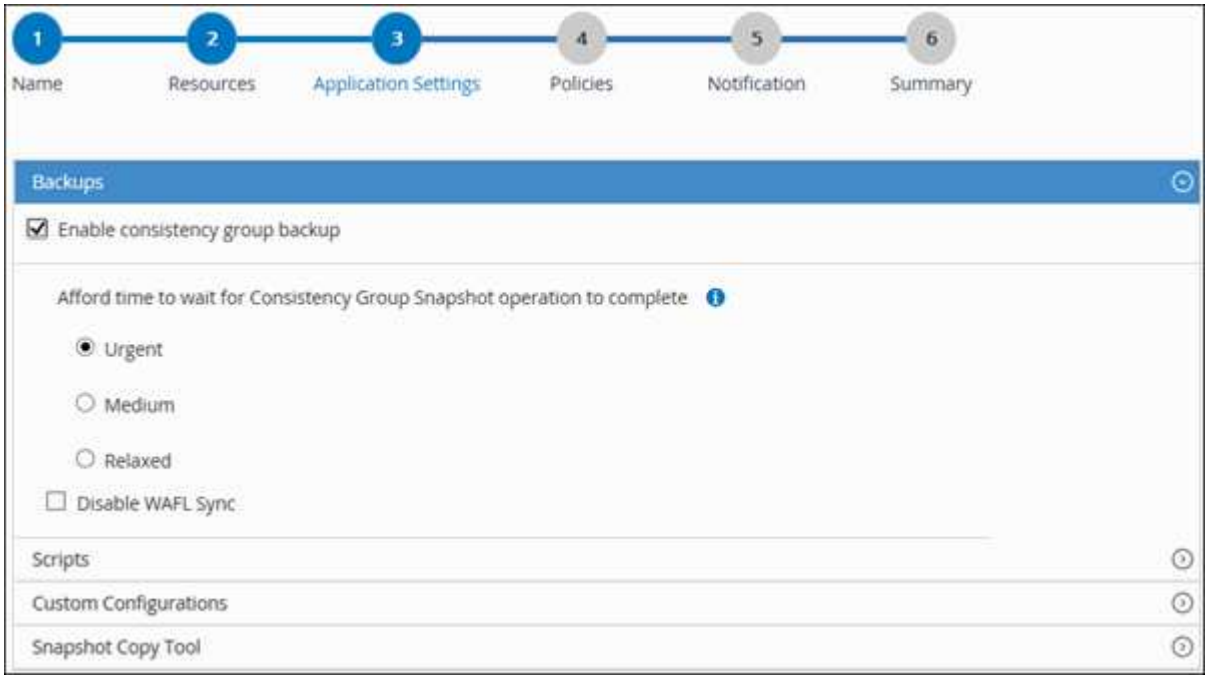
5. Selezionare le risorse dalla sezione **Risorse disponibili**, quindi selezionare la freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Facoltativo: nella pagina **Impostazioni applicazione**, procedere come segue:

   a. Selezionare la freccia Backup per impostare opzioni di backup aggiuntive:

      Abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
| --- | --- |
| Concediti del tempo per attendere il completamento dell'operazione Consistency Group Snapshot | Selezionare Urgente, Medio o Rilassato per specificare il tempo di attesa per il completamento dell'operazione Snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+




   a. Selezionare la freccia Script e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.

   b. Selezionare la freccia Configurazioni personalizzate e immettere le coppie chiave-valore personalizzate richieste per tutte le operazioni di protezione dei dati che utilizzano questa risorsa.

| Parametro | Collocamento | Descrizione |
| --- | --- | --- |
| ARCHIVE_LOG_ENABLE | (S/N) | Abilita la gestione dei log di archivio per eliminare i log di archivio. |
| CONSERVAZIONE_ARCHIVIO_LOG | numero_di_giorni | Specifica il numero di giorni per cui vengono conservati i registri di archivio.<br><br>Questa impostazione deve essere uguale o maggiore di NTAP_SNAPSHOT_RETENTIONS. |
| ARCHIVE_LOG_DIR | change_info_directory/logs | Specifica il percorso della directory che contiene i log di archivio. |
| ARCHIVE_LOG_EXT | estensione_file | Specifica la lunghezza dell'estensione del file di registro dell'archivio.<br><br>Ad esempio, se il registro di archivio è log_backup_0_0_0_0.16151855 1942 9 e se il valore file_extension è 5, l'estensione del registro conserverà 5 cifre, ovvero 16151. |
| ARCHIVE_LOG_RECURSIVE_SE ARCH | (S/N) | Consente la gestione dei log di archivio all'interno delle sottodirectory.<br><br>È necessario utilizzare questo parametro se i registri di archivio si trovano in sottodirectory. |

c. Selezionare la freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
| --- | --- |
| SnapCenter per utilizzare il plug-in per Windows e impostare il file system in uno stato coerente prima di creare uno snapshot. Per le risorse Linux, questa opzione non è applicabile. | Selezionare * SnapCenter con coerenza del file system*.<br><br>Questa opzione non è applicabile al plug-in SnapCenter per il database SAP HANA. |
| SnapCenter per creare uno Snapshot del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |

| Se vuoi… | Poi… |
| --- | --- |
| Per immettere il comando da eseguire sull'host per creare gli snapshot. | Selezionare **Altro**, quindi immettere il comando da eseguire sull'host per creare uno snapshot. |

7. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy selezionando * + *.

      Le policy sono elencate nella sezione **Configura pianificazioni per policy selezionate**.

   b. Nella colonna **Configura pianificazioni**, seleziona * + * per la policy che vuoi configurare.

   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione e selezionare OK.

      Dove policy_name è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate. Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Dall'elenco a discesa **Preferenza e-mail** nella pagina **Notifica**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Il server SMTP deve essere configurato in **Impostazioni** > **Impostazioni globali**.

9. Rivedi il riepilogo e seleziona **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per le risorse sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.

- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

   c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

   d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

      Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:
   a. Selezionare il tipo di criterio di replica.

      La politica di replica sincrona non è supportata.

   b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.
   c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

      Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
| --- | --- |
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

      Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

> Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare una connessione al sistema di archiviazione e una credenziale utilizzando i cmdlet di PowerShell

È necessario creare una connessione alla macchina virtuale di archiviazione (SVM) e delle credenziali prima di utilizzare i cmdlet di PowerShell per eseguire operazioni di protezione dei dati.

**Prima di iniziare**

- Dovresti aver preparato l'ambiente PowerShell per eseguire i cmdlet PowerShell.
- Per creare connessioni di archiviazione è necessario disporre delle autorizzazioni necessarie nel ruolo di amministratore dell'infrastruttura.
- È necessario assicurarsi che non siano in corso installazioni di plug-in.

  Le installazioni di plug-in host non devono essere in corso durante l'aggiunta di una connessione al sistema di storage, poiché la cache host potrebbe non essere aggiornata e lo stato dei database potrebbe essere visualizzato nell'interfaccia utente grafica SnapCenter come "Non disponibile per il backup" o "`Non su storage NetApp ".

- I nomi dei sistemi di archiviazione devono essere univoci.

  SnapCenter non supporta più sistemi di archiviazione con lo stesso nome su cluster diversi. Ogni sistema di archiviazione supportato da SnapCenter deve avere un nome univoco e un indirizzo IP LIF di gestione univoco.

**Passi**

1. Avviare una sessione di connessione PowerShell Core utilizzando il cmdlet Open-SmConnection.

   Questo esempio apre una sessione di PowerShell:

   ```
   PS C:\> Open-SmConnection
   ```

2. Creare una nuova connessione al sistema di archiviazione utilizzando il cmdlet Add-SmStorageConnection.

   Questo esempio crea una nuova connessione al sistema di archiviazione:

   ```
   PS C:\> Add-SmStorageConnection -Storage test_vs1 -Protocol Https
   -Timeout 60
   ```

3. Creare una nuova credenziale utilizzando il cmdlet Add-SmCredential.

Questo esempio crea una nuova credenziale denominata FinanceAdmin con credenziali Windows:

```
PS C:> Add-SmCredential -Name FinanceAdmin -AuthMode Windows
-Credential sddev\administrator
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Eseguire il backup delle singole risorse dei plug-in supportati NetApp

Se una singola risorsa di plug-in supportata NetApp non fa parte di alcun gruppo di risorse, è possibile eseguire il backup della risorsa dalla pagina Risorse. È possibile eseguire il backup della risorsa su richiesta oppure, se alla risorsa è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Prima di iniziare**

- Devi aver creato una policy di backup.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con un archivio secondario, il ruolo ONTAP assegnato all'utente dell'archivio deve includere il privilegio "snapmirror all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Clic , quindi seleziona il nome host e il tipo di risorsa per filtrare le risorse. Puoi quindi fare clic per chiudere il riquadro del filtro.
3. Fare clic sulla risorsa di cui si desidera eseguire il backup.
4. Nella pagina Risorsa, se si desidera utilizzare un nome personalizzato, selezionare la casella di controllo **Usa formato nome personalizzato per copia Snapshot**, quindi immettere un formato nome personalizzato per il nome Snapshot.

   Ad esempio, *customtext_policy_hostname* o *resource_hostname*. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.
5. Nella pagina Impostazioni applicazione, procedere come segue:

   a. Fare clic sulla freccia **Backup** per impostare opzioni di backup aggiuntive:

      Se necessario, abilitare il backup del gruppo di coerenza ed eseguire le seguenti attività:

| Per questo campo… | Fai questo… |
|---|---|
| Concediti del tempo per attendere il completamento dell'operazione Consistency Group Snapshot | Selezionare Urgente, Medio o Rilassato per specificare il tempo di attesa per il completamento dell'operazione Snapshot.<br><br>Urgente = 5 secondi, Medio = 7 secondi e Rilassato = 20 secondi. |
| Disabilita la sincronizzazione WAFL | Selezionare questa opzione per evitare di forzare un punto di coerenza WAFL . |

+

a. Fare clic sulla freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile eseguire i comandi pre prima di uscire dall'operazione di backup.

   I prescript e i postscript vengono eseguiti nel server SnapCenter .

b. Fare clic sulla freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.

c. Fare clic sulla freccia **Strumento Copia snapshot** per selezionare lo strumento per creare snapshot:

| Se vuoi… | Poi… |
|---|---|
| SnapCenter per acquisire un'istantanea del livello di archiviazione | Selezionare * SnapCenter senza coerenza del file system*. |
| SnapCenter per utilizzare il plug-in per Windows per mettere il file system in uno stato coerente e quindi acquisire uno snapshot | Selezionare * SnapCenter con coerenza del file system*. |
| Per immettere il comando per creare uno Snapshot | Selezionare **Altro**, quindi immettere il comando per creare uno Snapshot. |

6. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

   Puoi anche creare una policy cliccando + .

   Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e poi clicca su **Fine**.

Viene visualizzata la pagina della topologia delle risorse.

9. Fare clic su **Esegui backup ora**.
10. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa **Criterio** seleziona il criterio che desideri utilizzare per il backup.

    Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-smconnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146\
```

Viene visualizzata la richiesta di nome utente e password.

2. Aggiungere risorse utilizzando il cmdlet Add-SmResources.

Questo esempio aggiunge risorse:

```
Add-SmResource -HostName 'scc55.sccore.test.com' -PluginCode
'DummyPlugin' -ResourceName QDBVOL1 -ResourceType Database
-StorageFootPrint (
@{"VolumeName"="qtree_vol1_scc55_sccore_test_com";"QTREENAME"="qtree
Vol1";"StorageSystem"="vserver_scauto_primary"}) -Instance QTREE1
```

3. Creare un criterio di backup utilizzando il cmdlet Add-SmPolicy.

   Questo esempio crea una nuova policy di backup:

```
Add-SMPolicy -PolicyName 'test2' -PolicyType 'Backup'
-PluginPolicyType DummyPlugin  -description 'testPolicy'
```

4. Aggiungere un nuovo gruppo di risorse a SnapCenter utilizzando il cmdlet Add-SmResourceGroup.

   Questo esempio crea un nuovo gruppo di risorse con i criteri e le risorse specificati:

```
Add-SmResourceGroup -ResourceGroupName
'Verify_Backup_on_Multiple_Qtree_different_vserver_windows'
-Resources
@(@{"Host"="scc55.sccore.test.com";"Uid"="QTREE2";"PluginName"="Dumm
yPlugin"},@{"Host"="scc55.sccore.test.com";"Uid"="QTREE";"PluginName
"="DummyPlugin"}) -Policies test2 -plugincode 'DummyPlugin'
-usesnapcenterwithoutfilesystemconsistency
```

5. Avviare un nuovo processo di backup utilizzando il cmdlet New-SmBackup.

```
New-SMBackup -DatasetName
Verify_Backup_on_Multiple_Qtree_different_vserver_windows -Policy
test2
```

6. Visualizzare lo stato del processo di backup utilizzando il cmdlet Get-SmBackupReport.

   Questo esempio visualizza un report riepilogativo di tutti i lavori eseguiti nella data specificata:

```
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.sccore.test.com
```

## Eseguire il backup dei gruppi di risorse delle risorse plug-in supportate NetApp

È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono eseguiti automaticamente in base alla pianificazione.

**Prima di iniziare**

- È necessario aver creato un gruppo di risorse con un criterio associato.
- Se si desidera eseguire il backup di una risorsa che ha una relazione SnapMirror con l'archiviazione secondaria, il ruolo ONTAP assegnato all'utente dell'archiviazione deve includere il privilegio "snapmirror

all". Tuttavia, se si utilizza il ruolo "vsadmin", il privilegio "snapmirror all" non è richiesto.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.

   È possibile cercare il gruppo di risorse inserendo il nome del gruppo di risorse nella casella di ricerca oppure facendo clic su e selezionando il tag. Puoi quindi fare clic per chiudere il riquadro del filtro.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi fai clic su **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se hai associato più policy al gruppo di risorse, dall'elenco a discesa **Policy** seleziona la policy che desideri utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Fare clic su **Backup**.
5. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.
   - Nelle configurazioni MetroCluster , SnapCenter potrebbe non essere in grado di rilevare una relazione di protezione dopo un failover.

     "Impossibile rilevare la relazione SnapMirror o SnapVault dopo il failover MetroCluster"
   - Se si esegue il backup dei dati dell'applicazione su VMDK e la dimensione dell'heap Java per il SnapCenter Plug-in for VMware vSphere non è sufficientemente grande, il backup potrebbe non riuscire. Per aumentare la dimensione dell'heap Java, individuare il file di script /opt/netapp/init_scripts/scvservice. In quella sceneggiatura, il `do_start method` Il comando avvia il servizio plug-in SnapCenter VMware. Aggiorna quel comando come segue: `Java -jar -Xmx8192M -Xms4096M`.

## Monitora le operazioni di backup delle risorse plug-in supportate NetApp

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi

- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

## Annulla le operazioni di backup per i plug-in supportati da NetApp

È possibile annullare le operazioni di backup in coda.

**Cosa ti servirà**

- Per annullare le operazioni, è necessario aver effettuato l'accesso come amministratore SnapCenter o come proprietario del lavoro.
- È possibile annullare un'operazione di backup dalla pagina **Monitor** o dal riquadro **Attività**.
- Non è possibile annullare un'operazione di backup in esecuzione.
- È possibile utilizzare l'interfaccia utente grafica SnapCenter , i cmdlet di PowerShell o i comandi CLI per annullare le operazioni di backup.
- Il pulsante **Annulla lavoro** è disabilitato per le operazioni che non possono essere annullate.
- Se hai selezionato **Tutti i membri di questo ruolo possono vedere e operare sugli oggetti degli altri membri** nella pagina Utenti\Gruppi durante la creazione di un ruolo, puoi annullare le operazioni di backup in coda degli altri membri mentre utilizzi quel ruolo.

**Passi**

1. Eseguire una delle seguenti azioni:

| Dal… | Azione |
| --- | --- |
| Pagina di monitoraggio | a. Nel riquadro di navigazione a sinistra, fare clic su **Monitor** > **Lavori**.<br>b. Selezionare l'operazione, quindi fare clic su **Annulla lavoro**. |
| Riquadro attività | a. Dopo aver avviato l'operazione di backup, fare clic su * * nel riquadro Attività per visualizzare le cinque operazioni più recenti.<br>b. Selezionare l'operazione.<br>c. Nella pagina Dettagli lavoro, fare clic su **Annulla lavoro**. |

L'operazione viene annullata e la risorsa torna allo stato precedente.

## Visualizza i backup e i cloni correlati alle risorse dei plug-in supportati da NetApp nella pagina Topologia

Quando ci si prepara a eseguire il backup o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup e i cloni sullo storage primario e secondario. Nella pagina Topologia è possibile visualizzare tutti i backup e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup e cloni e quindi selezionarli per eseguire operazioni di protezione dei dati.

### Informazioni su questo compito

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .

  I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

  Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai

creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato sarà 6.

> I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

   Se la risorsa è protetta, viene visualizzata la pagina della topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   Nella sezione Scheda riepilogativa viene visualizzato il numero totale di backup e cloni.

   Facendo clic sul pulsante Aggiorna viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando la risorsa dell'applicazione è distribuita su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Dopo il backup su richiesta, facendo clic sul pulsante **Aggiorna** si aggiornano i dettagli del backup o del clone.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione, ridenominazione ed eliminazione.

   > Non è possibile rinominare o eliminare i backup presenti sul sistema di archiviazione secondario.

   > Non è possibile rinominare i backup presenti sul sistema di archiviazione primario.

7. Se vuoi eliminare un clone, seleziona il clone dalla tabella e fai clic su per eliminare il clone.

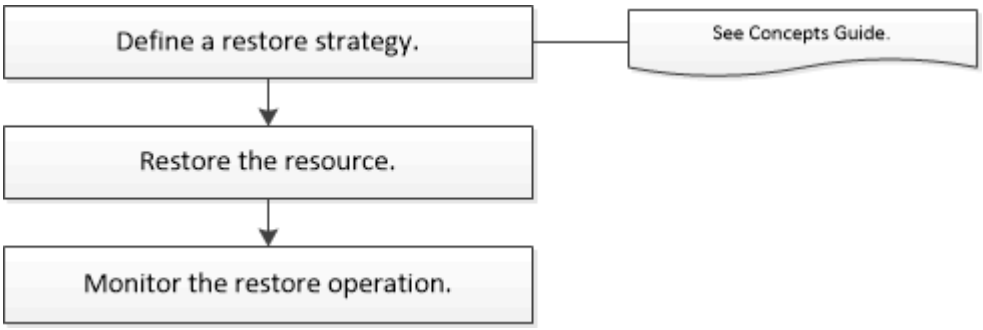
# Ripristina le risorse dei plug-in supportati da NetApp

## Ripristina le risorse dei plug-in supportati da NetApp

Il flusso di lavoro di ripristino e recupero include la pianificazione, l'esecuzione delle operazioni di ripristino e il monitoraggio delle operazioni.

**Informazioni su questo compito**

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di ripristino:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

## Ripristinare un backup delle risorse

È possibile utilizzare SnapCenter per ripristinare le risorse. Le capacità delle operazioni di ripristino dipendono dal plug-in utilizzato.

**Prima di iniziare**

- È necessario aver eseguito il backup della risorsa o dei gruppi di risorse.
- Se si stanno replicando snapshot su un mirror o un vault, l'amministratore SnapCenter deve aver assegnato le macchine virtuali di archiviazione (SVM) sia per i volumi di origine che per quelli di destinazione.
- È necessario aver annullato qualsiasi operazione di backup in corso per la risorsa o il gruppo di risorse che si desidera ripristinare.

**Informazioni su questo compito**

- L'operazione di ripristino predefinita ripristina solo gli oggetti di archiviazione. Le operazioni di ripristino a livello di applicazione possono essere eseguite solo se il plug-in supportato NetApp fornisce tale funzionalità.
- Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, nome dell'host o del cluster, gruppi di risorse e policy associati e stato.

   Sebbene un backup possa riguardare un gruppo di risorse, quando si esegue il ripristino è necessario selezionare le singole risorse che si desidera ripristinare.

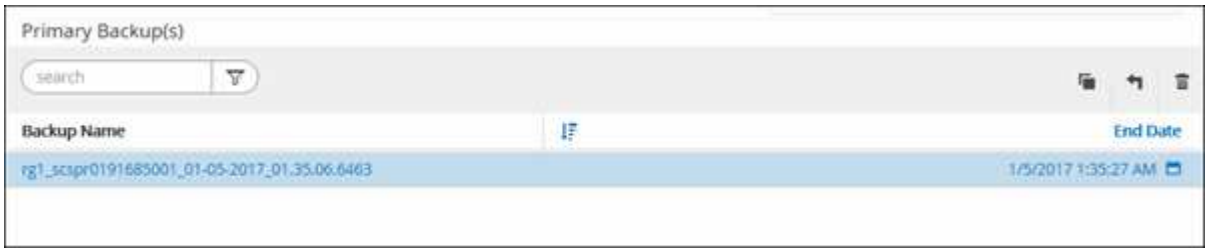
   Se la risorsa non è protetta, nella colonna **Stato generale** viene visualizzato *Non protetto*.

   Lo stato *Non protetto* nella colonna **Stato generale** può significare che la risorsa non è protetta oppure che è stata sottoposta a backup da un utente diverso.

3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su .




6. Nella pagina Ambito di ripristino, selezionare **Risorsa completa** o **Livello file**.
   a. Se hai selezionato **Risorsa completa**, il backup della risorsa verrà ripristinato.

      Se la risorsa contiene volumi o qtree come Storage Footprint, gli snapshot più recenti su tali volumi o qtree vengono eliminati e non possono essere recuperati. Inoltre, se sugli stessi volumi o qtree è ospitata un'altra risorsa, anche tale risorsa verrà eliminata.

   b. Se hai selezionato **Livello file**, puoi selezionare **Tutti** oppure selezionare volumi o qtree, quindi immettere il percorso relativo ai volumi o qtree selezionati, separati da virgole.
      - È possibile selezionare più volumi e qtree.
      - Se il tipo di risorsa è LUN, viene ripristinato l'intero LUN. È possibile selezionare più LUN. + NOTA: se si seleziona **Tutti**, verranno ripristinati tutti i file sui volumi, qtree o LUN.
7. Nella pagina **Pre ops**, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.

8. Nella pagina **Post ops**, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.
9. Nella pagina **Notifica**, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.
10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

   ```
   PS C:\> Open-Smconnection
   ```

2. Recuperare le informazioni su uno o più backup che si desidera ripristinare utilizzando i cmdlet Get-SmBackup e Get-SmBackupReport.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

   ```
   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
   ```

   Questo esempio mostra informazioni dettagliate sul backup dal 29 gennaio 2015 al 3 febbraio 2015:

```
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. Ripristinare i dati dal backup utilizzando il cmdlet Restore-SmBackup.

```
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          :
```

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

## Monitora le operazioni di ripristino delle risorse dei plug-in supportati NetApp

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

#### Informazioni su questo compito

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clona i backup delle risorse dei plug-in supportati NetApp

## Clona i backup delle risorse dei plug-in supportati NetApp

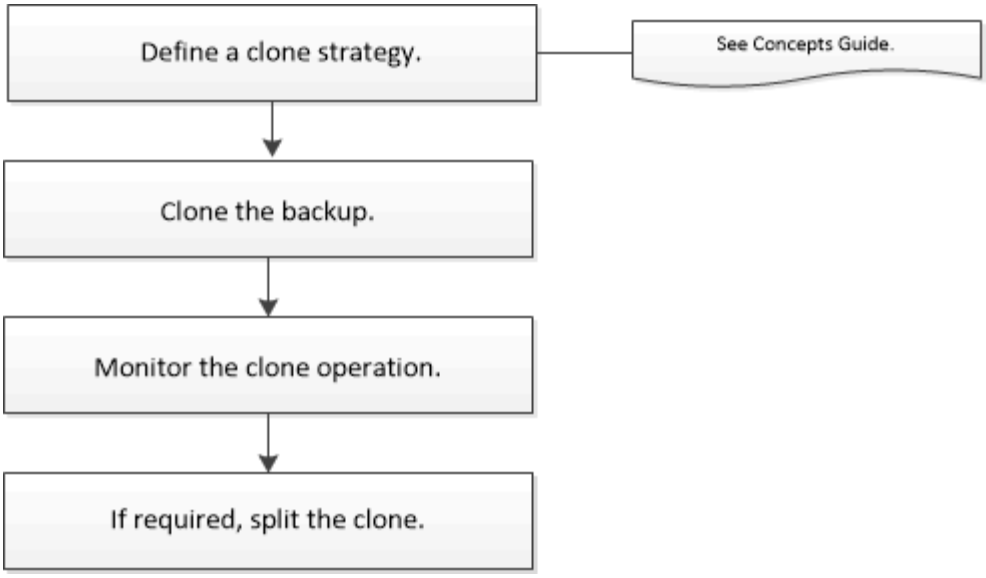
Il flusso di lavoro della clonazione include l'esecuzione dell'operazione di clonazione e il monitoraggio dell'operazione.

**Informazioni su questo compito**

È possibile clonare i backup delle risorse per i seguenti motivi:

- Per testare la funzionalità che deve essere implementata utilizzando la struttura e il contenuto delle risorse correnti durante i cicli di sviluppo dell'applicazione
- Per strumenti di estrazione e manipolazione dei dati durante il popolamento dei data warehouse
- Per recuperare dati che sono stati cancellati o modificati per errore

Il seguente flusso di lavoro mostra la sequenza in cui è necessario eseguire l'operazione di clonazione:




È anche possibile utilizzare i cmdlet di PowerShell manualmente o negli script per eseguire operazioni di backup, ripristino e clonazione. Per informazioni dettagliate sui cmdlet di PowerShell, utilizzare la guida del cmdlet SnapCenter o vedere "Guida di riferimento ai cmdlet del software SnapCenter" .

## Clona da un backup

È possibile utilizzare SnapCenter per clonare un backup. È possibile clonare dal backup primario o secondario. Le capacità delle operazioni di clonazione dipendono dal plug-in utilizzato.

**Prima di iniziare**

- È necessario aver eseguito il backup delle risorse o del gruppo di risorse.
- L'operazione di clonazione predefinita clona solo gli oggetti di archiviazione. Le operazioni di clonazione a livello di applicazione possono essere eseguite solo se il plug-in supportato NetApp fornisce tale funzionalità.
- È necessario assicurarsi che gli aggregati che ospitano i volumi siano presenti nell'elenco degli aggregati assegnati della macchina virtuale di archiviazione (SVM).

**Informazioni su questo compito**

Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Interfaccia utente SnapCenter**

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.

   Le risorse vengono visualizzate insieme a informazioni quali tipo, nome dell'host o del cluster, gruppi di risorse e policy associati e stato.

3. Selezionare la risorsa o il gruppo di risorse.

   Se si seleziona un gruppo di risorse, è necessario selezionare una risorsa.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .
6. Nella pagina Posizioni, procedere come segue:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Per impostazione predefinita, l'host di origine è popolato.<br><br>Se si desidera specificare un host diverso, selezionare l'host su cui deve essere montato il clone e installato il plug-in. |
| Suffisso clone | Questa operazione è obbligatoria quando la destinazione del clone è la stessa della sorgente.<br><br>Immettere un suffisso che verrà aggiunto al nome della risorsa appena clonata. Il suffisso garantisce che la risorsa clonata sia univoca sull'host.<br><br>Ad esempio, rs1_clone. Se si esegue la clonazione sullo stesso host della risorsa originale, è necessario fornire un suffisso per differenziare la risorsa clonata dalla risorsa originale; in caso contrario, l'operazione fallisce. |

   Se la risorsa selezionata è una LUN e si sta clonando da un backup secondario, vengono elencati i volumi di destinazione. Una singola origine può avere più volumi di destinazione.

7. Nella pagina **Impostazioni**, procedere come segue:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome dell'iniziatore | Immettere il nome dell'iniziatore host, che può essere un IQDN o un WWPN. |
| Protocollo Igroup | Selezionare il protocollo Igroup. |

La pagina Impostazioni viene visualizzata solo se il tipo di archiviazione è LUN.

8. Nella pagina Script, immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione. Immettere il comando mount per montare un file system su un host.

   Per esempio:

   - Comando pre-clone: elimina i database esistenti con lo stesso nome
   - Comando post-clonazione: verifica un database o avvia un database.

     Comando di montaggio per un volume o qtree su una macchina Linux: mount<VSERVER_NAME>:%<VOLUME_NAME_Clone /mnt>

9. Nella pagina **Notifica**, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email.

10. Rivedi il riepilogo e clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

**Cmdlet di PowerShell**

**Passi**

1. Avvia una sessione di connessione con SnapCenter Server per un utente specificato utilizzando il cmdlet Open-SmConnection.

```
Open-SmConnection  -SMSbaseurl
https:\\snapctr.demo.netapp.com:8146/
```

2. Elenca i backup che possono essere clonati utilizzando il cmdlet Get-SmBackup o Get-SmResourceGroup.

   Questo esempio visualizza informazioni su tutti i backup disponibili:

```
 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
```

Questo esempio visualizza informazioni su un gruppo di risorse specificato:

```
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                    : {}
    HostResourceMaping          : {}
    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                    : {}
    HostResourceMaping          : {}
    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. Avviare un'operazione di clonazione da un gruppo di risorse di clonazione o da un backup esistente utilizzando il cmdlet New-SmClone.

   Questo esempio crea un clone da un backup specificato con tutti i log:

```
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. Visualizzare lo stato del processo di clonazione utilizzando il cmdlet Get-SmCloneReport.

   Questo esempio visualizza un report di clonazione per l'ID processo specificato:

```
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          :
```

## Monitora le operazioni di clonazione delle risorse plug-in supportate NetApp

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

### Informazioni su questo compito

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.

2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

# Proteggere i file system Unix

## Cosa puoi fare con il plug-in SnapCenter per i file system Unix

Una volta installato il plug-in per i file system Unix nel tuo ambiente, puoi utilizzare SnapCenter per eseguire il backup, il ripristino e la clonazione dei file system Unix. È anche possibile eseguire attività di supporto a tali operazioni.

- Scopri le risorse
- Eseguire il backup dei file system Unix
- Pianificare le operazioni di backup
- Ripristinare i backup del file system
- Clonazione dei backup del file system
- Monitorare le operazioni di backup, ripristino e clonazione

### Configurazioni supportate

| Articolo | Configurazione supportata |
| --- | --- |
| Ambienti | • Server fisico<br>• Server virtuale<br><br>Datastore vVol sia su NFS che su SAN. Il provisioning del datastore vVol può essere effettuato solo con ONTAP Tools per VMware vSphere. |
| Sistemi operativi | • Red Hat Enterprise Linux<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| Sistemi di file | • SAN:<br>◦ Sia i file system basati su LVM che quelli non basati su LVM<br>◦ LVM su VMDK ext3, ext4 e xfs<br>• NFS: NFS v3, NFS v4.x |
| Protocolli | • FC<br>• FCoE<br>• iSCSI<br>• NFS |

| Articolo | Configurazione supportata |
| --- | --- |
| Multipercorso | SÌ |

## Limitazioni

- Non è supportata la combinazione di RDM e dischi virtuali in un gruppo di volumi.
- Il ripristino a livello di file non è supportato.

  Tuttavia, è possibile eseguire manualmente il ripristino a livello di file clonando il backup e quindi copiando manualmente i file.

- Non è supportato il mix di file system distribuiti su VMDK provenienti sia da datastore NFS che VMFS.
- NVMe non è supportato.
- Il provisioning non è supportato.

## Caratteristiche

- Consente al plug-in per Oracle Database di eseguire operazioni di protezione dei dati sui database Oracle gestendo lo stack di archiviazione host sottostante sui sistemi Linux o AIX
- Supporta i protocolli Network File System (NFS) e Storage Area Network (SAN) su un sistema di archiviazione che esegue ONTAP.
- Per i sistemi Linux, i database Oracle su VMDK e RDM LUN sono supportati quando si distribuisce il SnapCenter Plug-in for VMware vSphere e si registra il plug-in con SnapCenter.
- Supporta Mount Guard per AIX su file system SAN e layout LVM.
- Supporta Enhanced Journaled File System (JFS2) con registrazione in linea sui file system SAN e layout LVM solo per sistemi AIX.

  Sono supportati dispositivi SAN nativi, file system e layout LVM creati su dispositivi SAN.

- Automatizza le operazioni di backup, ripristino e clonazione basate sulle applicazioni per i file system UNIX nel tuo ambiente SnapCenter

# Installa il plug-in SnapCenter per i file system Unix

## Prerequisiti per l'aggiunta di host e l'installazione del pacchetto Plug-in per Linux

Prima di aggiungere un host e installare il pacchetto plug-in per Linux, è necessario soddisfare tutti i requisiti.

- Se si utilizza iSCSI, il servizio iSCSI deve essere in esecuzione.
- È possibile utilizzare l'autenticazione basata su password per l'utente root o non root oppure l'autenticazione basata su chiave SSH.

  Il plug-in SnapCenter per i file system Unix può essere installato da un utente non root. Tuttavia, è necessario configurare i privilegi sudo per l'utente non root per installare e avviare il processo del plug-in. Dopo aver installato il plug-in, i processi verranno eseguiti come utente non root.

- Creare credenziali con modalità di autenticazione Linux per l'utente installatore.
- Devi aver installato Java 11 sul tuo host Linux.

  Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.

  Per informazioni su come scaricare JAVA, vedere: "Download Java per tutti i sistemi operativi"

- Dovresti avere **bash** come shell predefinita per l'installazione del plug-in.

### Requisiti dell'host Linux

Prima di installare il pacchetto plug-in SnapCenter per Linux, è necessario assicurarsi che l'host soddisfi i requisiti.

| Articolo | Requisiti |
|---|---|
| Sistemi operativi | • Red Hat Enterprise Linux<br>• Oracle Linux<br>• SUSE Linux Enterprise Server (SLES) |
| RAM minima per il plug-in SnapCenter sull'host | 2 GB |
| Spazio minimo di installazione e registro per il plug-in SnapCenter sull'host | 2 GB<br>È necessario allocare spazio su disco sufficiente e monitorare il consumo di spazio di archiviazione da parte della cartella dei registri. Lo spazio di registro richiesto varia a seconda del numero di entità da proteggere e della frequenza delle operazioni di protezione dei dati. Se non c'è spazio sufficiente sul disco, i registri per le operazioni eseguite di recente non verranno creati. |
| Pacchetti software richiesti | Java 11 Oracle Java e OpenJDK<br>Assicurarsi di aver installato solo l'edizione certificata di JAVA 11 sull'host Linux.<br>Se hai aggiornato JAVA alla versione più recente, devi assicurarti che l'opzione JAVA_HOME situata in /var/opt/snapcenter/spl/etc/spl.properties sia impostata sulla versione JAVA corretta e sul percorso corretto. |

Per le informazioni più recenti sulle versioni supportate, vedere "Strumento matrice di interoperabilità NetApp" .

## Aggiungi host e installa il pacchetto Plug-in per Linux utilizzando l'interfaccia grafica

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto plug-in SnapCenter per Linux. I plug-in vengono installati automaticamente sugli host remoti.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Tipo di host | Selezionare **Linux** come tipo di host. |
| Nome host | Immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.<br><br>SnapCenter dipende dalla corretta configurazione del DNS. Pertanto, la prassi migliore è quella di immettere il nome di dominio completo (FQDN).<br><br>Se si aggiunge un host tramite SnapCenter e l'host fa parte di un sottodominio, è necessario fornire l'FQDN. |
| Credenziali | Seleziona il nome delle credenziali che hai creato oppure creane di nuove.<br><br>La credenziale deve disporre di diritti amministrativi sull'host remoto. Per maggiori dettagli, consultare le informazioni sulla creazione delle credenziali.<br><br>È possibile visualizzare i dettagli sulle credenziali posizionando il cursore sul nome della credenziale specificato.<br><br>La modalità di autenticazione delle credenziali è determinata dal tipo di host specificato nella procedura guidata Aggiungi host. |

5. Nella sezione Seleziona plug-in da installare, seleziona **File System Unix**.
6. (Facoltativo) Fare clic su **Altre opzioni**.

| Per questo campo… | Fai questo… |
| --- | --- |
| Porta | Mantenere il numero di porta predefinito oppure specificare il numero di porta.<br><br>Il numero di porta predefinito è 8145. Se SnapCenter Server è stato installato su una porta personalizzata, tale numero di porta verrà visualizzato come porta predefinita.<br><br>Se hai installato manualmente i plug-in e hai specificato una porta personalizzata, devi specificare la stessa porta. In caso contrario, l'operazione fallisce. |
| Percorso di installazione | Il percorso predefinito è */opt/ NetApp/snapcenter*.<br><br>Facoltativamente, è possibile personalizzare il percorso. Se si utilizza il percorso personalizzato, assicurarsi che il contenuto predefinito dei sudoer venga aggiornato con il percorso personalizzato. |
| Salta i controlli di preinstallazione facoltativi | Selezionare questa casella di controllo se i plug-in sono già stati installati manualmente e non si desidera verificare se l'host soddisfa i requisiti per l'installazione del plug-in. |

7. Fare clic su **Invia**.

   Se non hai selezionato la casella di controllo Salta controlli preliminari, l'host viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in.

   Lo script di pre-controllo non convalida lo stato del firewall della porta del plug-in se è specificato nelle regole di rifiuto del firewall.

   Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati. Se l'errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config situato in *C:\Programmi\ NetApp\ SnapCenter WebApp* per modificare i valori predefiniti. Se l'errore è correlato ad altri parametri, dovresti risolvere il problema.

   In una configurazione HA, se si aggiorna il file web.config, è necessario aggiornare il file su entrambi i nodi.

8. Verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   SnapCenter non supporta l'algoritmo ECDSA.

   La verifica dell'impronta digitale è obbligatoria anche se lo stesso host è stato aggiunto in precedenza a SnapCenter e l'impronta digitale è stata confermata.

9. Monitorare l’avanzamento dell’installazione.

   I file di registro specifici dell’installazione si trovano in */custom_location/snapcenter/logs*.

**Risultato**

Tutti i file system montati sull’host vengono automaticamente rilevati e visualizzati nella pagina Risorse. Se non viene visualizzato nulla, fare clic su **Aggiorna risorse**.

**Monitorare lo stato dell’installazione**

È possibile monitorare l’avanzamento dell’installazione del pacchetto plug-in SnapCenter tramite la pagina Lavori. Potrebbe essere opportuno controllare l’avanzamento dell’installazione per stabilire quando è completa o se si è verificato un problema.

**Informazioni su questo compito**

Le seguenti icone compaiono nella pagina Lavori e indicano lo stato dell’operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, per filtrare l’elenco in modo che vengano elencate solo le operazioni di installazione dei plug-in, procedere come segue:
   a. Fare clic su **Filtro**.
   b. Facoltativo: specificare la data di inizio e di fine.
   c. Dal menu a discesa Tipo, seleziona **Installazione plug-in**.
   d. Dal menu a discesa Stato, selezionare lo stato dell’installazione.
   e. Fare clic su **Applica**.
4. Selezionare il lavoro di installazione e fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

## Configurare il servizio SnapCenter Plug-in Loader

Il servizio SnapCenter Plug-in Loader carica il pacchetto plug-in per consentire a Linux di interagire con SnapCenter Server. Il servizio SnapCenter Plug-in Loader viene installato quando si installa il pacchetto SnapCenter Plug-ins per Linux.

**Informazioni su questo compito**

Dopo aver installato il pacchetto di plug-in SnapCenter per Linux, il servizio SnapCenter Plug-in Loader si avvia automaticamente. Se il servizio SnapCenter Plug-in Loader non si avvia automaticamente, è necessario:

- Assicurarsi che la directory in cui è in esecuzione il plug-in non venga eliminata
- Aumentare lo spazio di memoria assegnato alla Java Virtual Machine

Il file spl.properties, che si trova in */custom_location/ NetApp/snapcenter/spl/etc/*, contiene i seguenti parametri. A questi parametri vengono assegnati valori predefiniti.

| Nome del parametro | Descrizione |
|---|---|
| LOG_LEVEL | Visualizza i livelli di registro supportati.<br><br>I valori possibili sono TRACE, DEBUG, INFO, WARN, ERROR e FATAL. |
| SPL_PROTOCOL | Visualizza il protocollo supportato da SnapCenter Plug-in Loader.<br><br>È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito. |
| PROTOCOLLO_SERVER_SNAPCENTER | Visualizza il protocollo supportato da SnapCenter Server.<br><br>È supportato solo il protocollo HTTPS. È possibile aggiungere il valore se manca il valore predefinito. |
| SKIP_JAVAHOME_UPDATE | Per impostazione predefinita, il servizio SPL rileva il percorso Java e aggiorna il parametro JAVA_HOME.<br><br>Pertanto il valore predefinito è impostato su FALSE. È possibile impostare su TRUE se si desidera disabilitare il comportamento predefinito e correggere manualmente il percorso Java. |
| SPL_KEYSTORE_PASS | Visualizza la password del file keystore.<br><br>È possibile modificare questo valore solo se si modifica la password o si crea un nuovo file keystore. |
| SPL_PORT | Visualizza il numero di porta su cui è in esecuzione il servizio SnapCenter Plug-in Loader .<br><br>È possibile aggiungere il valore se manca il valore predefinito.<br><br>Non modificare il valore dopo aver installato i plug-in. |

| Nome del parametro | Descrizione |
| --- | --- |
| SNAPCENTER_SERVER_HOST | Visualizza l'indirizzo IP o il nome host del server SnapCenter . |
| SPL_KEYSTORE_PATH | Visualizza il percorso assoluto del file keystore. |
| SNAPCENTER_SERVER_PORT | Visualizza il numero di porta su cui è in esecuzione SnapCenter Server. |
| LOGS_MAX_COUNT | Visualizza il numero di file di registro di SnapCenter Plug-in Loader conservati nella cartella */custom_location/snapcenter/spl/logs*.<br><br>Il valore predefinito è impostato su 5000. Se il conteggio è superiore al valore specificato, vengono conservati gli ultimi 5000 file modificati. Il controllo del numero di file viene eseguito automaticamente ogni 24 ore dall'avvio del servizio SnapCenter Plug-in Loader .<br><br>Se si elimina manualmente il file spl.properties, il numero di file da conservare viene impostato su 9999. |
| JAVA_HOME | Visualizza il percorso assoluto della directory JAVA_HOME utilizzata per avviare il servizio SPL.<br><br>Questo percorso viene determinato durante l'installazione e come parte dell'avvio di SPL. |
| LOG_MAX_SIZE | Visualizza la dimensione massima del file di registro dei lavori.<br><br>Una volta raggiunta la dimensione massima, il file di registro viene compresso e i registri vengono scritti nel nuovo file di quel processo. |
| CONSERVA_I_LOG_DEGLI_ULTIMI_GIORNI | Visualizza il numero di giorni per i quali vengono conservati i registri. |
| ABILITA_VALIDAZIONE_CERTIFICATO | Visualizza true quando la convalida del certificato CA è abilitata per l'host.<br><br>È possibile abilitare o disabilitare questo parametro modificando spl.properties oppure utilizzando l'interfaccia utente grafica o il cmdlet SnapCenter . |

Se uno qualsiasi di questi parametri non è assegnato al valore predefinito o se si desidera assegnare o modificare il valore, è possibile modificare il file spl.properties. È inoltre possibile verificare il file spl.properties

e modificarlo per risolvere eventuali problemi relativi ai valori assegnati ai parametri. Dopo aver modificato il file spl.properties, è necessario riavviare il servizio SnapCenter Plug-in Loader .

**Passi**

1. Eseguire una delle seguenti azioni, a seconda delle necessità:
   - Avviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl start`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl start`
   - Arrestare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl stop`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl stop`

     È possibile utilizzare l'opzione -force con il comando stop per arrestare forzatamente il servizio SnapCenter Plug-in Loader . Tuttavia, è necessario procedere con cautela prima di procedere, poiché ciò interrompe anche le operazioni in corso.

   - Riavviare il servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl restart`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl restart`
   - Trova lo stato del servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl status`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl status`
   - Trova la modifica nel servizio SnapCenter Plug-in Loader :
     - Come utente root, esegui: `/custom_location/NetApp/snapcenter/spl/bin/spl change`
     - Come utente non root, esegui: `sudo /custom_location/NetApp/snapcenter/spl/bin/spl change`

## Configurare il certificato CA con il servizio SnapCenter Plug-in Loader (SPL) sull'host Linux

È necessario gestire la password del keystore SPL e il relativo certificato, configurare il certificato CA, configurare i certificati radice o intermedi per l'archivio attendibile SPL e configurare la coppia di chiavi firmata dalla CA per l'archivio attendibile SPL con il servizio SnapCenter Plug-in Loader per attivare il certificato digitale installato.

SPL utilizza il file 'keystore.jks', che si trova in '/var/opt/snapcenter/spl/etc' sia come archivio attendibile che come archivio chiavi.

**Gestisci la password per il keystore SPL e l'alias della coppia di chiavi firmata dalla CA in uso**

**Passi**

1. È possibile recuperare la password predefinita del keystore SPL dal file delle proprietà SPL.

   È il valore corrispondente alla chiave 'SPL_KEYSTORE_PASS'.

2. Cambia la password del keystore:

```
 keytool -storepasswd -keystore keystore.jks
. Modificare la password per tutti gli alias delle voci di chiave
privata nel keystore con la stessa password utilizzata per il keystore:
```

```
keytool -keypasswd -alias "<alias_name>" -keystore keystore.jks
```

   Aggiornare lo stesso per la chiave SPL_KEYSTORE_PASS nel file spl.properties.

3. Riavviare il servizio dopo aver modificato la password.

> La password per il keystore SPL e per tutte le password alias associate della chiave privata devono essere le stesse.

**Configurare i certificati radice o intermedi per l'archivio attendibile SPL**

È necessario configurare i certificati radice o intermedi senza la chiave privata nell'archivio attendibile SPL.

**Passi**

1. Passare alla cartella contenente il keystore SPL: */var/opt/snapcenter/spl/etc*.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungi un certificato radice o intermedio:
```

```
 keytool -import -trustcacerts -alias
<AliasNameForCerticateToBeImported> -file /<CertificatePath> -keystore
keystore.jks
. Riavviare il servizio dopo aver configurato i certificati radice o
intermedi su SPL trust-store.
```

> Dovresti aggiungere il certificato CA radice e poi i certificati CA intermedi.

### Configurare la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL

È necessario configurare la coppia di chiavi firmata dalla CA nell'archivio attendibile SPL.

**Passi**

1. Passare alla cartella contenente il keystore dell'SPL /var/opt/snapcenter/spl/etc.
2. Individuare il file 'keystore.jks'.
3. Elenca i certificati aggiunti nel keystore:

```
 keytool -list -v -keystore keystore.jks
. Aggiungere il certificato CA con chiave sia privata che pubblica.
```

```
 keytool -importkeystore -srckeystore <CertificatePathToImport>
-srcstoretype pkcs12 -destkeystore keystore.jks -deststoretype JKS
. Elenca i certificati aggiunti nel keystore.
```

```
 keytool -list -v -keystore keystore.jks
. Verificare che il keystore contenga l'alias corrispondente al nuovo
certificato CA aggiunto al keystore.
. Modificare la password della chiave privata aggiunta per il
certificato CA con la password del keystore.
```

La password predefinita del keystore SPL è il valore della chiave SPL_KEYSTORE_PASS nel file spl.properties.

```
 keytool -keypasswd -alias "<aliasNameOfAddedCertInKeystore>" -keystore
keystore.jks
. Se il nome alias nel certificato CA è lungo e contiene spazi o
caratteri speciali ("*",","), modificare il nome alias in un nome
semplice:
```

```
 keytool -changealias -alias "<OrignalAliasName>" -destalias
"<NewAliasName>" -keystore keystore.jks
. Configurare il nome alias dal keystore situato nel file
spl.properties.
```

Aggiornare questo valore in base alla chiave SPL_CERTIFICATE_ALIAS.

4. Riavviare il servizio dopo aver configurato la coppia di chiavi firmate dalla CA nell'archivio attendibile SPL.

### Configurare l'elenco di revoche dei certificati (CRL) per SPL

Dovresti configurare il CRL per SPL

#### Informazioni su questo compito

- SPL cercherà i file CRL in una directory preconfigurata.
- La directory predefinita per i file CRL per SPL è */var/opt/snapcenter/spl/etc/crl*.

#### Passi

1. È possibile modificare e aggiornare la directory predefinita nel file spl.properties in base alla chiave SPL_CRL_PATH.
2. È possibile inserire più di un file CRL in questa directory.

   I certificati in arrivo saranno verificati rispetto a ciascun CRL.

## Abilita i certificati CA per i plug-in

È necessario configurare i certificati CA e distribuirli nel server SnapCenter e negli host dei plug-in corrispondenti. Dovresti abilitare la convalida del certificato CA per i plug-in.

#### Prima di iniziare

- È possibile abilitare o disabilitare i certificati CA utilizzando il cmdlet run *Set-SmCertificateSettings*.
- È possibile visualizzare lo stato del certificato per i plug-in utilizzando *Get-SmCertificateSettings*.

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Selezionare uno o più host di plug-in.
4. Fare clic su **Altre opzioni**.
5. Selezionare **Abilita convalida certificato**.

#### Dopo aver finito

Nella scheda Host gestiti viene visualizzato un lucchetto e il colore del lucchetto indica lo stato della connessione tra SnapCenter Server e l'host del plug-in.

- * * indica che il certificato CA non è abilitato né assegnato all'host del plug-in.
- * * indica che il certificato CA è stato convalidato correttamente.
- * * indica che il certificato CA non è stato convalidato.
- * * indica che non è stato possibile recuperare le informazioni di connessione.

> Quando lo stato è giallo o verde, le operazioni di protezione dei dati sono state completate correttamente.

# Installa il SnapCenter Plug-in for VMware vSphere

Se il database o il file system è archiviato su macchine virtuali (VM) o se si desidera proteggere VM e datastore, è necessario distribuire il SnapCenter Plug-in for VMware vSphere .

Per informazioni da distribuire, vedere "Panoramica della distribuzione" .

## Distribuisci il certificato CA

Per configurare il certificato CA con il SnapCenter Plug-in for VMware vSphere, vedere "Crea o importa un certificato SSL" .

## Configurare il file CRL

Il SnapCenter Plug-in for VMware vSphere cerca i file CRL in una directory preconfigurata. La directory predefinita dei file CRL per il SnapCenter Plug-in for VMware vSphere è */opt/netapp/config/crl*.

È possibile inserire più di un file CRL in questa directory. I certificati in arrivo saranno verificati rispetto a ciascun CRL.

# Prepararsi alla protezione dei file system Unix

Prima di eseguire qualsiasi operazione di protezione dei dati, come backup, clonazione o ripristino, è necessario configurare l'ambiente. È anche possibile configurare SnapCenter Server per utilizzare la tecnologia SnapMirror e SnapVault .

Per sfruttare i vantaggi della tecnologia SnapVault e SnapMirror , è necessario configurare e inizializzare una relazione di protezione dei dati tra i volumi di origine e di destinazione sul dispositivo di archiviazione. Per eseguire queste attività è possibile utilizzare NetAppSystem Manager oppure la riga di comando della console di archiviazione.

Prima di utilizzare il plug-in per i file system Unix, l'amministratore SnapCenter deve installare e configurare SnapCenter Server ed eseguire le attività preliminari.

- Installa e configura SnapCenter Server."Saperne di più"
- Configurare l'ambiente SnapCenter aggiungendo connessioni al sistema di archiviazione."Saperne di più"

> SnapCenter non supporta più SVM con lo stesso nome su cluster diversi. Ogni SVM registrato con SnapCenter tramite la registrazione SVM o la registrazione cluster deve essere univoco.

- Aggiungi host, installa i plug-in e scopri le risorse.
- Se si utilizza SnapCenter Server per proteggere i file system Unix che risiedono su VMware RDM LUN o VMDK, è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.
- Installa Java sul tuo host Linux.
- Se si desidera la replica del backup, configurare SnapMirror e SnapVault su ONTAP.

# Eseguire il backup dei file system Unix

## Scopri i file system UNIX disponibili per il backup

Dopo aver installato il plug-in, tutti i file system presenti su quell'host vengono automaticamente rilevati e visualizzati nella pagina Risorse. È possibile aggiungere questi file system ai gruppi di risorse per eseguire operazioni di protezione dei dati.

**Prima di iniziare**

- È necessario aver completato attività quali l'installazione di SnapCenter Server, l'aggiunta di host e la creazione di connessioni al sistema di archiviazione.
- Se i file system risiedono su un disco di macchina virtuale (VMDK) o su un mapping di dispositivi raw (RDM), è necessario distribuire il SnapCenter Plug-in for VMware vSphere e registrare il plug-in con SnapCenter.

  Per ulteriori informazioni, vedere "Distribuisci il SnapCenter Plug-in for VMware vSphere" .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** dall'elenco Visualizza.
3. Fare clic su **Aggiorna risorse**.

   I file system vengono visualizzati insieme a informazioni quali tipo, nome host, gruppi di risorse e policy associati e stato.

## Creare policy di backup per i file system Unix

Prima di utilizzare SnapCenter per eseguire il backup dei file system Unix, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup. Una policy di backup è un insieme di regole che regolano il modo in cui si gestiscono, si pianificano e si conservano i backup. È inoltre possibile specificare le impostazioni relative a replica, script e tipo di backup. La creazione di un criterio consente di risparmiare tempo quando si desidera riutilizzarlo su un'altra risorsa o un altro gruppo di risorse.

**Prima di iniziare**

- È necessario prepararsi alla protezione dei dati completando attività quali l'installazione SnapCenter, l'aggiunta di host, l'individuazione dei file system e la creazione di connessioni al sistema di archiviazione.
- Se si replicano gli snapshot su un mirror o su un archivio secondario vault, l'amministratore SnapCenter deve aver assegnato le SVM sia per il volume di origine che per quello di destinazione.
- Esaminare i prerequisiti e le limitazioni specifici SnapMirror ActiveSync. Per informazioni, fare riferimento "Limiti degli oggetti per la sincronizzazione attiva SnapMirror" .

**Informazioni su questo compito**

- SnapLock

◦ Se è selezionata l'opzione "Conserva le copie di backup per un numero specifico di giorni", il periodo di conservazione SnapLock deve essere inferiore o uguale ai giorni di conservazione indicati.

Specificando un periodo di blocco degli snapshot si impedisce l'eliminazione degli snapshot fino alla scadenza del periodo di conservazione. Ciò potrebbe comportare la conservazione di un numero di snapshot maggiore rispetto al conteggio specificato nella policy.

Per ONTAP 9.12.1 e versioni precedenti, i cloni creati dagli SnapLock Vault Snapshot come parte del ripristino erediteranno il tempo di scadenza SnapLock Vault. L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare **File System Unix** dall'elenco a discesa.
4. Fare clic su **Nuovo**.
5. Nella pagina Nome, immettere il nome e i dettagli della policy.
6. Nella pagina Backup e replica, eseguire le seguenti azioni:
   a. Specificare le impostazioni di backup.
   b. Specificare la frequenza di programmazione selezionando **Su richiesta**, **Ogni ora**, **Giornaliera**, **Settimanale** o **Mensile**.
   c. Nella sezione Seleziona opzioni di replicazione secondaria, seleziona una o entrambe le seguenti opzioni di replicazione secondaria:

| Per questo campo… | Fai questo… |
|---|---|
| Aggiorna SnapMirror dopo aver creato una copia Snapshot locale | Selezionare questo campo per creare copie mirror dei set di backup su un altro volume (replica SnapMirror ).<br><br>Questa opzione dovrebbe essere abilitata per la sincronizzazione attiva SnapMirror . |
| Aggiorna SnapVault dopo aver creato una copia Snapshot locale | Selezionare questa opzione per eseguire la replica del backup da disco a disco (backup SnapVault ). |
| Errore nel conteggio dei tentativi | Immettere il numero massimo di tentativi di replica consentiti prima che l'operazione venga interrotta. |

7. Nella pagina Conservazione, specificare le impostazioni di conservazione per il tipo di backup e il tipo di pianificazione selezionati nella pagina Backup e replica:

| Se lo desidera… | Poi… |
|---|---|

| | |
|---|---|
| Conserva un certo numero di snapshot | Seleziona **Copie da conservare**, quindi specifica il numero di snapshot che desideri conservare.<br><br>Se il numero di Snapshot supera il numero specificato, gli Snapshot vengono eliminati partendo dalle copie più vecchie.<br><br>Il valore massimo di ritenzione è 1018. I backup non riusciranno se la conservazione è impostata su un valore superiore a quello supportato dalla versione ONTAP sottostante.<br><br>Se si prevede di abilitare la replica SnapVault , è necessario impostare il conteggio di conservazione su 2 o su un valore superiore. Se si imposta il conteggio di conservazione su 1, l'operazione di conservazione potrebbe non riuscire perché il primo Snapshot è lo Snapshot di riferimento per la relazione SnapVault finché uno Snapshot più recente non viene replicato sulla destinazione. |
| Conserva gli snapshot per un certo numero di giorni | Selezionare **Conserva copie per**, quindi specificare il numero di giorni per cui si desidera conservare gli snapshot prima di eliminarli. |
| Periodo di blocco della copia snapshot | Selezionare **Periodo di blocco della copia snapshot** e specificare la durata in giorni, mesi o anni.<br><br>Il periodo di conservazione di Snaplock dovrebbe essere inferiore a 100 anni. |

8. Seleziona l'etichetta della policy.

   È possibile assegnare etichette SnapMirror agli snapshot primari per la replica remota, consentendo agli snapshot primari di trasferire l'operazione di replica degli snapshot da SnapCenter ai sistemi secondari ONTAP . Questa operazione può essere eseguita senza abilitare l'opzione SnapMirror o SnapVault nella pagina dei criteri.

9. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.

   Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dal percorso _ /opt/ NetApp/snapcenter/scc/etc/allowed_commands.config_.

È anche possibile specificare il valore di timeout dello script. Il valore predefinito è 60 secondi.

10. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e allega policy per i file system Unix

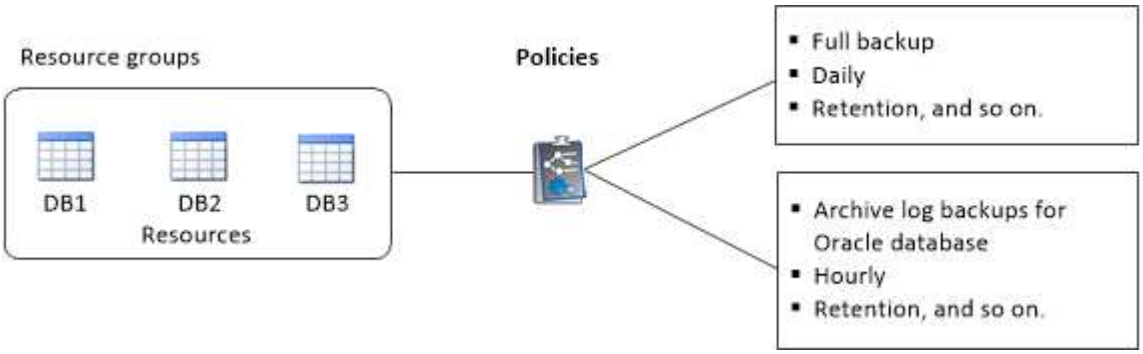
Un gruppo di risorse è un contenitore in cui aggiungere le risorse di cui si desidera eseguire il backup e la protezione. Un gruppo di risorse consente di eseguire il backup di tutti i dati associati ai file system.

**Informazioni su questo compito**

- Un database con file in gruppi di dischi ASM deve essere nello stato "MOUNT" o "OPEN" per verificare i propri backup utilizzando l'utilità Oracle DBVERIFY.

  Allegare una o più policy al gruppo di risorse per definire il tipo di attività di protezione dei dati che si desidera eseguire.

  L'immagine seguente illustra la relazione tra risorse, gruppi di risorse e criteri per i database:




- Per i criteri abilitati per SnapLock , per ONTAP 9.12.1 e versioni precedenti, se si specifica un periodo di blocco degli snapshot, i cloni creati dagli snapshot antimanomissione come parte del ripristino erediteranno il tempo di scadenza SnapLock . L'amministratore dell'archiviazione deve pulire manualmente i cloni dopo la scadenza SnapLock .
- L'aggiunta di nuovi file system senza SnapMirror ActiveSync a un gruppo di risorse esistente che contiene risorse con SnapMirror ActiveSync non è supportata.
- L'aggiunta di nuovi file system a un gruppo di risorse esistente in modalità failover di SnapMirror ActiveSync non è supportata. È possibile aggiungere risorse al gruppo di risorse solo nello stato normale o di failback.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare la casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

4. Nella pagina Risorse, seleziona un nome host del file system Unix dall'elenco a discesa **Host**.

Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Seleziona le risorse dalla sezione Risorse disponibili e spostale nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia Script e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.
   - Selezionare una delle opzioni di coerenza del backup:
     - Selezionare **File System Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup e che non siano consentite operazioni di input o output sul file system durante la creazione del backup.

Per la coerenza del file system, verranno acquisiti snapshot del gruppo di coerenza per i LUN coinvolti nel gruppo di volumi.

     - Selezionare **Crash Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup.

Se hai aggiunto diversi file system nel gruppo di risorse, tutti i volumi provenienti da diversi file system nel gruppo di risorse verranno inseriti in un gruppo di coerenza.

7. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

Puoi anche creare una policy cliccando + .

Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

Dove *policy_name* è il nome della policy selezionata.

Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

## Crea gruppi di risorse e abilita la protezione secondaria per i file system Unix sui sistemi ASA r2

È necessario creare il gruppo di risorse per aggiungere le risorse presenti sui sistemi ASA r2. È anche possibile predisporre la protezione secondaria durante la creazione del gruppo di risorse.

**Prima di iniziare**

- È necessario assicurarsi di non aggiungere risorse ONTAP 9.x e risorse ASA r2 allo stesso gruppo di risorse.
- È necessario assicurarsi di non disporre di un database con risorse ONTAP 9.x e risorse ASA r2.

**Informazioni su questo compito**

- La protezione secondaria è disponibile solo se all'utente connesso è assegnato il ruolo per cui è abilitata la funzionalità **SecondaryProtection**.
- Se è stata abilitata la protezione secondaria, il gruppo di risorse viene messo in modalità di manutenzione durante la creazione dei gruppi di coerenza primario e secondario. Dopo aver creato i gruppi di coerenza primari e secondari, il gruppo di risorse esce dalla modalità di manutenzione.
- SnapCenter non supporta la protezione secondaria per una risorsa clone.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:
   a. Immettere un nome per il gruppo di risorse nel campo Nome.

      Il nome del gruppo di risorse non deve superare i 250 caratteri.

   b. Inserisci una o più etichette nel campo Tag per aiutarti a cercare il gruppo di risorse in un secondo momento.

      Ad esempio, se aggiungi HR come tag a più gruppi di risorse, potrai successivamente trovare tutti i gruppi di risorse associati al tag HR.

c. Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

   Ad esempio, customtext_resource group_policy_hostname o resource group_hostname. Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

d. Specificare le destinazioni dei file di registro dell'archivio di cui non si desidera eseguire il backup.

   Dovresti usare esattamente la stessa destinazione impostata nell'applicazione, incluso il prefisso, se necessario.

4. Nella pagina Risorse, seleziona il nome host del database dall'elenco a discesa **Host**.

   Le risorse vengono elencate nella sezione Risorse disponibili solo se la risorsa viene rilevata correttamente. Se hai aggiunto risorse di recente, queste appariranno nell'elenco delle risorse disponibili solo dopo aver aggiornato l'elenco delle risorse.

5. Selezionare le risorse ASA r2 dalla sezione Risorse disponibili e spostarle nella sezione Risorse selezionate.
6. Nella pagina Impostazioni applicazione, seleziona l'opzione di backup.
7. Nella pagina Criteri, procedere come segue:

   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi anche creare una policy cliccando + .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic + nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.

   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione, quindi fai clic su **OK**.

      Dove *policy_name* è il nome della policy selezionata.

      Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

   Le pianificazioni di backup di terze parti non sono supportate quando si sovrappongono alle pianificazioni di backup SnapCenter .

8. Se la protezione secondaria è abilitata per il criterio selezionato, viene visualizzata la pagina Protezione secondaria ed è necessario eseguire i seguenti passaggi:

   a. Selezionare il tipo di criterio di replica.

      La politica di replica sincrona non è supportata.

   b. Specificare il suffisso del gruppo di coerenza che si desidera utilizzare.

   c. Dai menu a discesa Cluster di destinazione e SVM di destinazione, seleziona il cluster peer e l'SVM che desideri utilizzare.

Il cluster e il peering SVM non sono supportati da SnapCenter. Per eseguire il peering di cluster e SVM, è necessario utilizzare System Manager o ONTAP CLI.

Se le risorse sono già protette all'esterno di SnapCenter, verranno visualizzate nella sezione Risorse secondarie protette.

1. Nella pagina Verifica, procedere come segue:
   a. Fare clic su **Carica localizzatori** per caricare i volumi SnapMirror o SnapVault ed eseguire la verifica sull'archiviazione secondaria.
   b. Clic + nella colonna Configura pianificazioni per configurare la pianificazione di verifica per tutti i tipi di pianificazione del criterio.
   c. Nella finestra di dialogo Aggiungi pianificazioni di verifica policy_name, eseguire le seguenti azioni:

| Se lo desidera… | Fai questo… |
|---|---|
| Esegui la verifica dopo il backup | Selezionare **Esegui verifica dopo il backup**. |
| Pianifica una verifica | Selezionare **Esegui verifica pianificata**, quindi selezionare il tipo di pianificazione dall'elenco a discesa. |

   d. Seleziona **Verifica su posizione secondaria** per verificare i backup sul sistema di archiviazione secondario.
   e. Fare clic su **OK**.

   Le pianificazioni di verifica configurate sono elencate nella colonna Pianificazioni applicate.

2. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione eseguita sul gruppo di risorse, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

3. Rivedi il riepilogo e poi clicca su **Fine**.

## Eseguire il backup dei file system Unix

Se una risorsa non fa parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** dall'elenco Visualizza.

3. Clic , quindi selezionare il nome host e i file system Unix per filtrare le risorse.
4. Selezionare il file system di cui si desidera eseguire il backup.
5. Nella pagina Risorse puoi eseguire i seguenti passaggi:
   a. Selezionare la casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot.

      Per esempio, `customtext_policy_hostname` O `resource_hostname` . Per impostazione predefinita, al nome dello snapshot viene aggiunto un timestamp.

6. Nella pagina Impostazioni applicazione, procedere come segue:
   - Selezionare la freccia Script e immettere i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce. È anche possibile immettere i comandi pre da eseguire prima di uscire in caso di errore.
   - Selezionare una delle opzioni di coerenza del backup:
     - Selezionare **File System Consistent** se si desidera garantire che i dati memorizzati nella cache del file system vengano svuotati prima di creare il backup e che non venga eseguita alcuna operazione sul file system durante la creazione del backup.
     - Selezionare **Crash Consistent** se si desidera garantire che i dati memorizzati nella cache dei file system vengano svuotati prima di creare il backup.
7. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.

      Puoi creare una policy cliccando .

      Nella sezione Configura pianificazioni per policy selezionate vengono elencate le policy selezionate.

   b. Clic nella colonna Configura pianificazioni per configurare una pianificazione per la policy desiderata.
   c. Nella finestra Aggiungi pianificazioni per il criterio *nome_criterio*, configura la pianificazione e quindi seleziona `OK` .

      *policy_name* è il nome della policy selezionata.

   Le pianificazioni configurate sono elencate nella colonna Pianificazioni applicate.

8. Nella pagina Notifica, seleziona gli scenari in cui desideri inviare le email dall'elenco a discesa **Preferenza email**.

   È necessario specificare gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. Se si desidera allegare il report dell'operazione di backup eseguita sulla risorsa, selezionare **Allega report attività**.

   Per la notifica via e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente o il comando PowerShell `Set-SmSmtpServer` .

9. Rivedi il riepilogo e poi clicca su **Fine**.

   Viene visualizzata la pagina della topologia.

10. Fare clic su **Esegui backup ora**.
11. Nella pagina Backup, procedere come segue:
    a. Se hai applicato più criteri alla risorsa, dall'elenco a discesa Criterio seleziona il criterio che desideri utilizzare per il backup.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Fare clic su **Backup**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Eseguire il backup dei gruppi di risorse dei file system Unix

È possibile eseguire il backup dei file system Unix definiti nel gruppo di risorse. È possibile eseguire il backup di un gruppo di risorse su richiesta dalla pagina Risorse. Se a un gruppo di risorse è associato un criterio e configurata una pianificazione, i backup vengono creati in base alla pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse** e il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Inserisci il nome del gruppo di risorse nella casella di ricerca oppure fai clic su e seleziona il tag.

   Clic per chiudere il riquadro del filtro.
4. Nella pagina Gruppo di risorse, seleziona il gruppo di risorse di cui eseguire il backup.
5. Nella pagina Backup, procedere come segue:
    a. Se al gruppo di risorse sono associati più criteri, selezionare il criterio di backup che si desidera utilizzare dall'elenco a discesa **Criterio**.

       Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

    b. Selezionare **Backup**.
6. Monitorare l'avanzamento selezionando **Monitoraggio > Lavori**.

## Monitorare il backup dei file system Unix

Scopri come monitorare l'avanzamento delle operazioni di backup e di protezione dei dati.

### Monitorare le operazioni di backup dei file system Unix

È possibile monitorare l'avanzamento delle diverse operazioni di backup utilizzando la pagina SnapCenterJobs. Potrebbe essere opportuno controllare lo stato di avanzamento per determinare quando il processo è completato o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato corrispondente delle operazioni:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Lavori**.
3. Nella pagina Lavori, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di backup.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, selezionare **Backup**.
   d. Dal menu a discesa **Stato**, seleziona lo stato del backup.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare un processo di backup, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.

   Sebbene lo stato del processo di backup venga visualizzato , quando fai clic sui dettagli del processo, potresti vedere che alcune delle attività secondarie dell'operazione di backup sono ancora in corso o contrassegnate con segnali di avviso.

5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

### Monitorare le operazioni di protezione dei dati nel riquadro Attività

Il riquadro Attività visualizza le cinque operazioni eseguite più di recente. Nel riquadro Attività viene inoltre visualizzato quando è stata avviata l'operazione e il suo stato.

Il riquadro Attività visualizza informazioni relative alle operazioni di backup, ripristino, clonazione e backup pianificato.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Clic nel riquadro Attività per visualizzare le cinque operazioni più recenti.

   Quando si fa clic su una delle operazioni, i dettagli dell'operazione vengono elencati nella pagina **Dettagli lavoro**.

## Visualizza i file system Unix protetti nella pagina Topologia

Quando ci si prepara a eseguire il backup, il ripristino o la clonazione di una risorsa, potrebbe essere utile visualizzare una rappresentazione grafica di tutti i backup, dei file system ripristinati e dei cloni nell'archiviazione primaria e secondaria.

### Informazioni su questo compito

Nella pagina Topologia è possibile visualizzare tutti i backup, i file system ripristinati e i cloni disponibili per la risorsa o il gruppo di risorse selezionato. È possibile visualizzare i dettagli di tali backup, file system ripristinati e cloni, quindi selezionarli per eseguire operazioni di protezione dei dati.

È possibile esaminare le seguenti icone nella vista Gestisci copie per determinare se i backup e i cloni sono disponibili nell'archivio primario o secondario (copie mirror o copie Vault).

- visualizza il numero di backup e cloni disponibili sullo storage primario.
- visualizza il numero di backup e cloni di cui è stato eseguito il mirroring sullo storage secondario mediante la tecnologia SnapMirror .
- visualizza il numero di backup e cloni replicati sullo storage secondario mediante la tecnologia SnapVault .

  Il numero di backup visualizzato include i backup eliminati dall'archivio secondario. Ad esempio, se hai creato 6 backup utilizzando un criterio per conservarne solo 4, il numero di backup visualizzato è 6.

I cloni di un backup di un mirror con versione flessibile su un volume di tipo mirror-vault vengono visualizzati nella vista topologia, ma il conteggio dei backup mirror nella vista topologia non include il backup con versione flessibile.

Se si dispone di una relazione secondaria come SnapMirror ActiveSync (inizialmente rilasciata come SnapMirror Business Continuity [SM-BC]), è possibile visualizzare le seguenti icone aggiuntive:

- Il sito replica è attivo.
- Il sito replica è inattivo.
- La relazione tra specchio secondario e volta non è stata ristabilita.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa dalla vista dei dettagli della risorsa o dalla vista dei dettagli del gruppo di risorse.

Se la risorsa è protetta, viene visualizzata la pagina Topologia della risorsa selezionata.

4. Esaminare la scheda Riepilogo per visualizzare un riepilogo del numero di backup e cloni disponibili sullo storage primario e secondario.

   Nella sezione Scheda riepilogativa viene visualizzato il numero totale di backup e cloni.

   Facendo clic sul pulsante **Aggiorna** viene avviata una query dello spazio di archiviazione per visualizzare un conteggio accurato.

   Se viene eseguito un backup abilitato per SnapLock , facendo clic sul pulsante **Aggiorna** vengono aggiornati i tempi di scadenza SnapLock primario e secondario recuperati da ONTAP. Una pianificazione settimanale aggiorna anche il tempo di scadenza primario e secondario SnapLock recuperato da ONTAP.

   Quando il file system è distribuito su più volumi, il tempo di scadenza SnapLock per il backup sarà il tempo di scadenza SnapLock più lungo impostato per uno Snapshot in un volume. Il tempo di scadenza SnapLock più lungo viene recuperato da ONTAP.

   Per la sincronizzazione attiva SnapMirror , facendo clic sul pulsante **Aggiorna** si aggiorna l'inventario di backup SnapCenter interrogando ONTAP sia per i siti primari che per quelli di replica. Una pianificazione settimanale esegue questa attività anche per tutti i database contenenti la relazione di sincronizzazione attiva SnapMirror .

   - Per SnapMirror ActiveSync e solo per ONTAP 9.14.1, le relazioni Async Mirror o Async MirrorVault con la nuova destinazione primaria devono essere configurate manualmente dopo il failover. Da ONTAP 9.15.1 in poi, Async Mirror o Async MirrorVault vengono configurati automaticamente sulla nuova destinazione primaria.
   - Dopo il failover, è necessario creare un backup affinché SnapCenter sia a conoscenza del failover. È possibile fare clic su **Aggiorna** solo dopo aver creato un backup.

5. Nella vista Gestisci copie, fare clic su **Backup** o **Cloni** dall'archivio primario o secondario per visualizzare i dettagli di un backup o di un clone.

   I dettagli dei backup e dei cloni vengono visualizzati in formato tabella.

6. Selezionare il backup dalla tabella, quindi fare clic sulle icone di protezione dei dati per eseguire operazioni di ripristino, clonazione ed eliminazione.

   Non è possibile rinominare o eliminare i backup presenti nell'archivio secondario.

7. Se si desidera eliminare un clone, selezionare il clone dalla tabella, quindi fare clic su .

**Esempio che mostra backup e cloni sullo storage primario**

# Ripristinare e recuperare i file system Unix

## Ripristinare i file system Unix

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i file system Unix.

### Informazioni su questo compito

- È necessario eseguire i seguenti comandi per stabilire la connessione con SnapCenter Server, elencare i backup e recuperarne le informazioni, quindi ripristinare il backup.

  Le informazioni riguardanti i parametri che possono essere utilizzati con il comando e le relative descrizioni possono essere ottenute eseguendo Get-Help *command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai comandi del software SnapCenter" .

- Per l'operazione di ripristino di SnapMirror ActiveSync, è necessario selezionare il backup dalla posizione principale.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** o **Gruppo di risorse** dall'elenco **Visualizza**.

3. Selezionare il file system dalla vista dettagli o dalla vista dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primario o secondario (con mirroring o replica).
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Ambito di ripristino:
   - Per i file system NFS, per impostazione predefinita è selezionato il ripristino **Connetti e copia**. Puoi anche selezionare **Ripristino volume** o **Ripristino rapido**.
   - Per i file system non NFS, l'ambito di ripristino viene selezionato in base al layout.

     A seconda del tipo e del layout del file system, i nuovi file creati dopo il backup potrebbero non essere disponibili dopo il ripristino.
7. Nella pagina PreOps, immettere i comandi di pre-ripristino da eseguire prima di eseguire un processo di ripristino.
8. Nella pagina PostOps, immettere i comandi di post-ripristino da eseguire dopo aver eseguito un processo di ripristino.

   Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in nella posizione _/opt/NetApp/snapcenter/scc/etc/allowed_commands.config_path.

9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le notifiche e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di ripristino eseguita, è necessario selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP utilizzando l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

10. Rivedi il riepilogo e poi clicca su **Fine**.

    Se l'operazione di ripristino fallisce, il rollback non è supportato.

    In caso di ripristino di un file system residente su un gruppo di volumi, il vecchio contenuto del file system non viene eliminato. Solo il contenuto del file system clonato verrà copiato nel file system di origine. Questa opzione è applicabile quando sono presenti più file system nel gruppo di volumi e vengono ripristinati i file system NFS predefiniti.

11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Monitorare le operazioni di ripristino dei file system Unix

È possibile monitorare l'avanzamento delle diverse operazioni di ripristino SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di

avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Gli stati post-ripristino descrivono le condizioni della risorsa dopo un'operazione di ripristino e qualsiasi ulteriore azione di ripristino che è possibile intraprendere.

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di ripristino.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Ripristina**.
   d. Dall'elenco a discesa **Stato**, selezionare lo stato di ripristino.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il processo di ripristino, quindi fare clic su **Dettagli** per visualizzare i dettagli del processo.
5. Nella pagina **Dettagli lavoro**, fare clic su **Visualizza registri**.

   Il pulsante **Visualizza registri** visualizza i registri dettagliati per l'operazione selezionata.

# Clonare i file system Unix

## Clona il backup del file system Unix

È possibile utilizzare SnapCenter per clonare il file system Unix utilizzando il backup del file system.

**Prima di iniziare**

- È possibile saltare l'aggiornamento del file fstab impostando il valore di *SKIP_FSTAB_UPDATE* su **true** nel file *agent.properties* che si trova in */opt/ NetApp/snapcenter/scc/etc*.
- È possibile avere un nome di volume clone statico e un percorso di giunzione impostando il valore di *USE_CUSTOM_CLONE_VOLUME_NAME_FORMAT* su **true** nel file *agent.properties* situato in */opt/ NetApp/snapcenter/scc/etc*. Dopo aver aggiornato il file, dovresti riavviare il servizio di creazione del plug-

in SnapCenter eseguendo il comando: `/opt/NetApp/snapcenter/scc/bin/scc restart`.

Esempio: senza questa proprietà il nome del volume clone e il percorso di giunzione saranno simili a <Source_volume_name>_Clone_<Timestamp> ma ora saranno <Source_volume_name>_Clone_<Clone_Name>

In questo modo il nome rimane costante, così puoi mantenere aggiornato manualmente il file fstab se non preferisci aggiornarlo tramite SnapCenter.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Percorso** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il file system dalla vista dettagli o dalla vista dettagli del gruppo di risorse.

   Viene visualizzata la pagina della topologia.

4. Dalla vista Gestisci copie, seleziona i backup tra Copie locali (primarie), Copie mirror (secondarie) o Copie vault (secondarie).
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Posizione, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Server clone | Per impostazione predefinita, l'host di origine è popolato. |
| Punto di montaggio clone | Specificare il percorso in cui verrà montato il file system. |

7. Nella pagina Script, procedere come segue:
   a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.

      Dovresti controllare se i comandi sono presenti nell'elenco dei comandi disponibile sull'host del plug-in dal percorso */opt/NetApp/snapcenter/scc/etc/allowed_commands.config*.

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. Se si desidera allegare il report dell'operazione di clonazione eseguita, selezionare **Allega report lavoro**.

   Per la notifica tramite e-mail, è necessario aver specificato i dettagli del server SMTP tramite l'interfaccia grafica utente (GUI) o il comando PowerShell Set-SmSmtpServer.

9. Rivedi il riepilogo e poi clicca su **Fine**.

10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Dividi un clone

È possibile utilizzare SnapCenter per dividere una risorsa clonata dalla risorsa padre. Il clone diviso diventa indipendente dalla risorsa padre.

**Informazioni su questo compito**

- Non è possibile eseguire l'operazione di divisione del clone su un clone intermedio.

  Ad esempio, dopo aver creato clone1 da un backup del database, è possibile creare un backup di clone1 e quindi clonare questo backup (clone2). Dopo aver creato clone2, clone1 è un clone intermedio e non è possibile eseguire l'operazione di divisione del clone su clone1. Tuttavia, è possibile eseguire l'operazione di divisione del clone su clone2.

  Dopo aver diviso clone2, è possibile eseguire l'operazione di divisione del clone su clone1 perché clone1 non è più il clone intermedio.

- Quando si divide un clone, le copie di backup e i processi di clonazione del clone vengono eliminati.
- Per informazioni sulle operazioni di suddivisione del volume FlexClone , vedere, "Dividere un volume FlexClone dal suo volume padre" .
- Assicurarsi che il volume o l'aggregato sul sistema di archiviazione sia online.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina **Risorse**, seleziona l'opzione appropriata dall'elenco Visualizza:

| Opzione | Descrizione |
|---|---|
| Per applicazioni di database | Selezionare **Database** dall'elenco Visualizza. |
| Per i file system | Selezionare **Percorso** dall'elenco Visualizza. |

3. Seleziona la risorsa appropriata dall'elenco.

   Viene visualizzata la pagina della topologia delle risorse.

4. Dalla vista **Gestisci copie**, seleziona la risorsa clonata (ad esempio, il database o il LUN), quindi fai clic su * *.
5. Verificare la dimensione stimata del clone da dividere e lo spazio disponibile richiesto sull'aggregato, quindi fare clic su **Avvia**.
6. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

   L'operazione di suddivisione del clone smette di rispondere se il servizio SMCore viene riavviato. È necessario eseguire il cmdlet Stop-SmJob per interrompere l'operazione di suddivisione del clone, quindi riprovare l'operazione.

   Se si desidera un tempo di polling più lungo o più breve per verificare se il clone è diviso o meno, è possibile modificare il valore del parametro *CloneSplitStatusCheckPollTime* nel file

*SMCoreServiceHost.exe.config* per impostare l'intervallo di tempo per SMCore per il polling dello stato dell'operazione di divisione del clone. Il valore è espresso in millisecondi e il valore predefinito è 5 minuti.

Per esempio:

```
<add key="CloneSplitStatusCheckPollTime" value="300000" />
```

L'operazione di avvio della suddivisione del clone fallisce se è in corso un backup, un ripristino o un'altra suddivisione del clone. È necessario riavviare l'operazione di suddivisione del clone solo dopo aver completato le operazioni in esecuzione.

**Informazioni correlate**

"La clonazione o la verifica SnapCenter non riesce perché l'aggregato non esiste"

## Monitorare le operazioni di clonazione dei file system Unix

È possibile monitorare l'avanzamento delle operazioni di clonazione SnapCenter utilizzando la pagina Lavori. Potrebbe essere opportuno controllare lo stato di avanzamento di un'operazione per stabilire quando è stata completata o se si è verificato un problema.

**Informazioni su questo compito**

Nella pagina Lavori vengono visualizzate le seguenti icone che indicano lo stato dell'operazione:

- In corso
- Completato con successo
- Fallito
- Completato con avvisi o non è stato possibile avviarlo a causa di avvisi
- In coda
- Annullato

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina **Monitor**, fare clic su **Lavori**.
3. Nella pagina **Lavori**, procedere come segue:
   a. Clic per filtrare l'elenco in modo che vengano elencate solo le operazioni di clonazione.
   b. Specificare le date di inizio e fine.
   c. Dall'elenco a discesa **Tipo**, seleziona **Clona**.
   d. Dall'elenco a discesa **Stato**, seleziona lo stato del clone.
   e. Fare clic su **Applica** per visualizzare le operazioni completate correttamente.
4. Selezionare il lavoro di clonazione, quindi fare clic su **Dettagli** per visualizzare i dettagli del lavoro.
5. Nella pagina Dettagli lavoro, fare clic su **Visualizza registri**.

# Proteggere le applicazioni in esecuzione su Azure NetApp Files

## Proteggere le applicazioni in esecuzione su Azure NetApp Files

SnapCenter supporta la protezione delle applicazioni quali Oracle, SQL e SAP HANA residenti su Azure NetApp Files. A partire dalla versione 6.0.1, SnapCenter supporta la funzionalità di backup Azure NetApp Files che amplia le capacità di protezione dei dati di Azure NetApp Files fornendo una soluzione di backup completamente gestita per il ripristino, l'archiviazione e la conformità a lungo termine.

Azure NetApp Files è una soluzione di archiviazione premium che può risultare costosa per la conservazione dei backup a lungo termine. Per ottimizzare i costi, è possibile spostare i backup dall'archiviazione di Azure NetApp Files a un archivio oggetti di Azure. A partire da SnapCenter 6.0.1, è possibile eseguire il backup e la clonazione delle applicazioni residenti in Azure NetApp Files in Azure Blob Storage (archivio oggetti). È possibile conservare due copie dei dati, copie snapshot del volume nell'archiviazione Azure NetApp Files per il ripristino a breve termine e un'altra copia nell'archiviazione BLOB di Azure per il ripristino a lungo termine.

Quando un criterio con backup Azure NetApp Files è abilitato e associato a una risorsa, SnapCenter gestisce la creazione di snapshot del volume e il relativo backup in Azure Blob Storage. SnapCenter crea il Backup Vault e abilita il backup per il volume. Se hai abilitato il backup per il volume, SnapCenter utilizza il vault esistente.

### Limitazioni

- Le funzionalità di archiviazione degli oggetti per i sistemi di archiviazione FAS, ASA o AFF ONTAP e Amazon FSx for NetApp ONTAP non sono supportate.
- I flussi di lavoro di montaggio e catalogazione di Oracle e SAP HANA non sono supportati per i backup di archiviazione di oggetti, ma sono supportati per gli snapshot.
- I cloni Oracle PDB non sono supportati per i backup di archiviazione di oggetti, ma sono supportati per gli snapshot.
- La verifica del backup dall'archiviazione di oggetti, il supporto dell'API REST, la gestione del ciclo di vita dei cloni dall'archiviazione di oggetti e le funzionalità di reporting per i backup dell'archiviazione di oggetti non sono supportati.
- Il ripristino dai backup su Azure Blob Storage ad Azure NetApp Files non è supportato. In alternativa, è possibile utilizzare l'opzione clone.
- La divisione dei cloni non è supportata.

# Installa SnapCenter e crea le credenziali

### Installa SnapCenter sulla macchina virtuale di Azure

È possibile scaricare il SnapCenter software dal sito di supporto NetApp e installarlo sulla macchina virtuale di Azure.

**Prima di iniziare**

- Assicurarsi che la macchina virtuale Windows di Azure soddisfi i requisiti per l'installazione di SnapCenter Server. Per informazioni, vedere"Requisiti per installare SnapCenter Server" .
- Se non hai familiarità con Azure NetApp Files e non hai un account NetApp esistente, assicurati di esserti registrato per poter accedere al software SnapCenter . Per informazioni, vedere"Registrati per accedere al SnapCenter software" .

**Passi**

1. Scarica il pacchetto di installazione di SnapCenter Server da "Sito di supporto NetApp" .
2. Avviare l'installazione di SnapCenter Server facendo doppio clic sul file .exe scaricato.

   Dopo aver avviato l'installazione, vengono eseguiti tutti i controlli preliminari e, se i requisiti minimi non vengono soddisfatti, vengono visualizzati i messaggi di errore o di avviso appropriati. È possibile ignorare i messaggi di avviso e procedere con l'installazione; tuttavia, gli errori dovrebbero essere corretti.

3. Rivedere i valori precompilati richiesti per l'installazione di SnapCenter Server e modificarli se necessario.

   Non è necessario specificare la password per il database del repository di MySQL Server. Durante l'installazione SnapCenter Server la password viene generata automaticamente.

   Il carattere speciale "%" non è supportato nel percorso personalizzato per il database del repository. Se si include "%" nel percorso, l'installazione fallisce.

4. Fare clic su **Installa ora**.

   Se sono stati specificati valori non validi, verranno visualizzati i messaggi di errore appropriati. Dovresti reinserire i valori e poi avviare l'installazione.

   Facendo clic sul pulsante **Annulla**, il passaggio in esecuzione verrà completato e verrà avviata l'operazione di rollback. Il server SnapCenter verrà completamente rimosso dall'host.

   Tuttavia, se si fa clic su **Annulla** quando sono in corso le operazioni "Riavvio del sito di SnapCenter Server" o "In attesa dell'avvio di SnapCenter Server", l'installazione procederà senza annullare l'operazione.

### Registra il prodotto per abilitare il supporto

Se sei un nuovo utente NetApp e non hai un account NetApp esistente, dovresti registrare il prodotto per abilitare il supporto.

**Passi**

1. Dopo aver installato SnapCenter, vai su **Aiuto > Informazioni**.
2. Nella finestra di dialogo *Informazioni su SnapCenter*, prendere nota dell'istanza SnapCenter , un numero di 20 cifre che inizia con 971.
3. Clic https://register.netapp.com .
4. Fare clic su **Non sono un cliente NetApp registrato**.
5. Specifica i tuoi dati per registrarti.
6. Lasciare vuoto il campo NetApp Reference SN.
7. Selezionare * SnapCenter* dal menu a discesa Linea di prodotti.

8. Selezionare il fornitore di fatturazione.
9. Immettere l'ID istanza SnapCenter di 20 cifre.
10. Fare clic su **Invia**.

## Creare le credenziali di Azure in SnapCenter

Per accedere all'account Azure NetApp , è necessario creare le credenziali di Azure in SnapCenter .

**Prima di iniziare**

- Assicurati di aver creato l'entità servizio in Azure.
- Assicurati di avere a disposizione l'ID tenant, l'ID client e la chiave segreta associati al servizio principale.
  - L'ID tenant è reperibile nel portale di Azure nella pagina Panoramica per l'ID Entra.
  - L'ID client è anche noto come ID applicazione per l'Enterprise App/Service Principal. Questa informazione è disponibile nel portale di Azure nella pagina Panoramica per l'applicazione aziendale creata per fungere da entità servizio per SnapCenter.
  - La chiave segreta del client è anche nota come valore segreto. È possibile creare questo segreto client nel portale di Azure accedendo a **Registrazioni app** in ID Entra. Dopo aver selezionato l'app aziendale creata, vai su **Certificati e segreti** e poi su **Nuovo segreto client**.

    È possibile accedere al valore segreto solo al momento della creazione. Non potrai accedervi in seguito.

  - È necessario concedere le autorizzazioni al Service Principal. Il ruolo di Collaboratore consentirà all'entità servizio di eseguire le azioni richieste in Azure. Questa operazione può essere eseguita tramite la pagina Controllo accessi (IAM) all'interno della pagina Abbonamento.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le seguenti informazioni necessarie per creare le credenziali.

| Per questo campo… | Fai questo… |
|---|---|
| Nome della credenziale | Inserisci un nome per la credenziale. |
| Modalità di autenticazione | Selezionare **Credenziali di Azure** dall'elenco a discesa. |
| ID inquilino | Inserisci l'ID del tenant. |
| ID cliente | Inserisci l'ID cliente. |
| Chiave segreta del cliente | Inserisci la chiave segreta del client. |

5. Fare clic su **OK**.

## Configurare l'account di archiviazione di Azure

Dovresti configurare l'account di archiviazione di Azure in SnapCenter.

L'account di archiviazione di Azure contiene dettagli sull'ID della sottoscrizione, sulle credenziali di Azure e sull'account Azure NetApp .

Per Azure NetApp Files non sono necessarie licenze standard e licenze basate sulla capacità.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, seleziona * Azure NetApp Files* e fai clic su **Nuovo**.
3. Selezionare le credenziali, l'ID di sottoscrizione e l'account NetApp dai rispettivi elenchi a discesa.
4. Fare clic su **Invia**.

## Crea le credenziali per aggiungere l'host del plug-in

SnapCenter utilizza le credenziali per autenticare gli utenti per le operazioni SnapCenter .

È necessario creare credenziali per l'installazione dei plug-in di SnapCenter e credenziali aggiuntive per l'esecuzione delle operazioni di protezione dei dati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Credenziali**.
3. Fare clic su **Nuovo**.
4. Nella pagina Credenziali, specificare le seguenti informazioni necessarie per creare le credenziali.

| **Per questo campo…** | **Fai questo…** |
|---|---|
| Nome della credenziale | Inserisci un nome per la credenziale. |
| Modalità di autenticazione | Selezionare la modalità di autenticazione dall'elenco a discesa. |
| Tipo di autenticazione | Selezionare **Basato su password** o **Basato su chiave SSH** (solo per host Linux). |
| Nome utente | Specificare il nome utente. |
| Password | Se hai selezionato Autenticazione basata su password, specifica la password. |
| Chiave privata SSH | Se hai selezionato l'autenticazione basata su chiave SSH, specifica la chiave privata. |

| Per questo campo… | Fai questo… |
| --- | --- |
| Utilizzare i privilegi sudo | Selezionare la casella di controllo Usa privilegi sudo se si stanno creando credenziali per un utente non root.<br>Questo vale solo per gli utenti Linux. |

5. Fare clic su **OK**.

# Proteggere i database SAP HANA

## Aggiungi host e installa il plug-in SnapCenter per il database SAP HANA

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare i pacchetti plug-in. I plug-in vengono installati automaticamente sugli host remoti.

**Prima di iniziare**

- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.
- Se si esegue l'installazione sull'host centralizzato, assicurarsi che il software client SAP HANA sia installato su tale host e aprire le porte necessarie sull'host del database SAP HANA per eseguire le query SQL HDB in remoto.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:
   a. Nel campo Tipo di host, selezionare il tipo di host.
   b. Nel campo Nome host, immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo Credenziali, inserisci le credenziali che hai creato.
5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.
6. (Facoltativo) Fare clic su **Altre opzioni** e specificare i dettagli.
7. Fare clic su **Invia**.
8. Se il tipo di host è Linux, verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

9. Monitorare l'avanzamento dell'installazione.

## Aggiungi il database SAP HANA

Dovresti aggiungere manualmente il database SAP HANA.

**Informazioni su questo compito**

Se il plug-in è installato su un server centralizzato, le risorse devono essere aggiunte manualmente. Se il plug-in SAP HANA è installato sull'host del database HANA, il sistema HANA viene rilevato automaticamente.

> La scoperta automatica non è supportata per la configurazione multi-host HANA; è necessario aggiungerla solo tramite plug-in centralizzato.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona il plug-in SnapCenter per il database SAP HANA dall'elenco a discesa, quindi fai clic su **Risorse**.
2. Nella pagina Risorse, fare clic su **Aggiungi database SAP HANA**.
3. Nella pagina Fornisci dettagli risorsa, esegui le seguenti azioni:
   a. Immettere il tipo di risorsa come Contenitore singolo, Contenitore di database multi-tenant o Volume non dati.
   b. Immettere il nome del sistema SAP HANA.
   c. Inserire l'ID del sistema (SID).
   d. Selezionare l'host del plug-in.
   e. Inserisci la chiave per connetterti al sistema SAP HANA.
   f. Immettere il nome utente per il quale è configurata la chiave HDB Secure User Store.
4. Nella pagina Fornisci impronta di archiviazione, seleziona * Azure NetApp Files* come tipo di archiviazione.
   a. Selezionare l'account Azure NetApp .
   b. Selezionare il pool di capacità e i volumi associati.
   c. Fare clic su **Salva**.
5. Rivedi il riepilogo e poi clicca su **Fine**.

## Creare policy di backup per i database SAP HANA

Prima di utilizzare SnapCenter per eseguire il backup delle risorse del database SAP HANA, è necessario creare una policy di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e la descrizione della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   a. Selezionare * Azure NetApp Files* come tipo di archiviazione.

b. Selezionare **Basato su file** se si desidera eseguire un controllo di integrità del database.

c. Selezionare **Basato su snapshot** se si desidera creare un backup utilizzando la tecnologia Snapshot.

6. Nella pagina Snapshot e backup, procedere come segue:

a. Selezionare la frequenza del backup pianificato.

b. Specificare le impostazioni di conservazione.

c. Se si desidera abilitare il backup Azure NetApp Files , selezionare **Abilita backup** e specificare le impostazioni di conservazione.

7. Rivedi il riepilogo e clicca su **Fine**.

## Crea gruppi di risorse e collega policy di backup SAP HANA

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Immettere un nome per il gruppo di risorse. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Criteri, procedere come segue:

a. Selezionare una o più policy dall'elenco a discesa.

b. Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.

c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
8. Rivedi il riepilogo e poi clicca su **Fine**.

## Eseguire il backup dei database SAP HANA in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.
3. Seleziona la risorsa di cui vuoi eseguire il backup.
4. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.
5. Nella pagina Impostazioni applicazione, procedere come segue:
   a. Selezionare la freccia **Backup** per impostare opzioni di backup aggiuntive.
   b. Selezionare la freccia **Script** per eseguire i comandi pre e post per le operazioni di quiesce, snapshot e unquiesce.
   c. Selezionare la freccia **Configurazioni personalizzate**, quindi immettere le coppie di valori personalizzati richieste per tutti i processi che utilizzano questa risorsa.
   d. Selezionare **Strumento Copia snapshot > SnapCenter senza coerenza del file system** per creare snapshot.

      L'opzione **Coerenza del file system** è applicabile solo alle applicazioni in esecuzione su host Windows.

6. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.
   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

7. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

   È necessario specificare anche gli indirizzi email del mittente e del destinatario, nonché l'oggetto dell'email. SMTP deve essere configurato anche in **Impostazioni** > **Impostazioni globali**.

8. Rivedi il riepilogo e seleziona **Fine**.
9. Seleziona **Esegui backup adesso**.
10. Nella pagina Backup, procedere come segue:

a. Se alla risorsa sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.

   Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

11. Selezionare **Backup**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Eseguire il backup dei gruppi di risorse SAP HANA

Un gruppo di risorse è una raccolta di risorse su un host. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se al gruppo di risorse sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.

      Se il criterio selezionato per il backup su richiesta è associato a una pianificazione di backup, i backup su richiesta verranno conservati in base alle impostazioni di conservazione specificate per il tipo di pianificazione.

   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Ripristinare e recuperare i database SAP HANA

È possibile ripristinare e recuperare i dati dai backup.

**Informazioni su questo compito**

Per i sistemi HANA rilevati automaticamente, se è selezionata l'opzione **Risorsa completa**, il ripristino viene eseguito utilizzando la tecnologia di ripristino snapshot di file singolo. Se è selezionata la casella di controllo **Ripristino rapido**, viene utilizzata la tecnologia Volume Revert.

Per le risorse aggiunte manualmente viene sempre utilizzata la tecnologia Volume Revert.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.
3. Selezionare la risorsa oppure selezionare un gruppo di risorse e quindi selezionare una risorsa in quel gruppo.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari o secondari (con mirroring o in vault).
5. Nella tabella Backup primari, seleziona il backup da cui desideri effettuare il ripristino, quindi fai clic su * *.
6. Nella pagina Ambito di ripristino, seleziona **Risorsa completa**.

   Vengono ripristinati tutti i volumi di dati configurati del database SAP HANA.
7. Per i sistemi HANA rilevati automaticamente, nella pagina Ambito di ripristino, eseguire le seguenti azioni:
   a. Seleziona **Recupera allo stato più recente** se desideri effettuare il recupero il più vicino possibile all'ora corrente.
   b. Selezionare **Recupera fino a un punto nel tempo** se si desidera ripristinare fino al punto nel tempo specificato.
   c. Selezionare **Ripristina su backup dati specificato** se si desidera ripristinare su un backup dati specifico.
   d. Seleziona **Nessun ripristino** se non desideri effettuare il ripristino ora.
   e. Specificare le posizioni di backup del registro.
   f. Specificare la posizione del catalogo di backup.
8. Nella pagina Pre ops, immettere i comandi pre restore e unmount da eseguire prima di eseguire un processo di ripristino.
9. Nella pagina Post ops, immettere i comandi mount e post restore da eseguire dopo aver eseguito un processo di ripristino.
10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.

    È necessario specificare anche gli indirizzi e-mail del mittente e del destinatario, nonché l'oggetto dell'e-mail. SMTP deve essere configurato anche nella pagina **Impostazioni** > **Impostazioni globali**.
11. Rivedi il riepilogo e poi clicca su **Fine**.
12. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Clona il backup del database SAP HANA

È possibile utilizzare SnapCenter per clonare un database SAP HANA utilizzando il backup del database. I cloni creati sono cloni spessi e vengono creati sul pool di capacità padre.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, filtra le risorse dall'elenco a discesa **Visualizza** in base al tipo di risorsa.
3. Selezionare la risorsa o il gruppo di risorse.
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione primario.
5. Selezionare il backup dei dati dalla tabella, quindi fare clic su .

6. Nella pagina Posizione, eseguire le seguenti azioni:

    a. Selezionare l'host su cui è installato il plug-in SAP HANA per la gestione del sistema HANA clonato.

    Può trattarsi di un host plug-in centralizzato o di un host di sistema HANA.

    > Se il plug-in HANA è installato su un host centralizzato che gestisce i database HANA su altri host, durante la creazione o l'eliminazione dei cloni, SnapCenter salta intenzionalmente le operazioni lato host (montaggio o smontaggio del file system) poiché il server di destinazione è un host centralizzato. Per eseguire le operazioni di montaggio e smontaggio, è necessario utilizzare script pre o post clone personalizzati.

    a. Immettere il SID SAP HANA da clonare dai backup esistenti.
    b. Immettere gli indirizzi IP o i nomi host su cui verranno esportati i volumi clonati.
    c. Se i volumi ANF del database SAP HANA sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

    Se non viene specificato il QOS per i volumi clonati, verrà utilizzato il QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

7. Nella pagina Script, procedere come segue:
    a. Immettere i comandi per il pre-clone o il post-clone che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
    b. Immettere il comando mount per montare un file system su un host.

    Se il sistema HANA di origine viene rilevato automaticamente e il plug-in dell'host di destinazione clone è installato sull'host SAP HANA, SnapCenter smonta automaticamente i volumi di dati HANA esistenti sull'host di destinazione clone e monta i nuovi volumi di dati HANA clonati.

8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
9. Rivedi il riepilogo e poi clicca su **Fine**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

> La suddivisione dei cloni è disabilitata per i cloni ANF perché il clone ANF è già un volume indipendente creato dallo snapshot selezionato.

# Proteggere i database di Microsoft SQL Server

## Aggiungi host e installa il plug-in SnapCenter per il database SQL Server

SnapCenter supporta la protezione dei dati delle istanze SQL sulle condivisioni SMB su Azure NetApp Files. Sono supportate le configurazioni standalone e del gruppo di disponibilità (AG).

È necessario utilizzare la pagina Aggiungi host SnapCenter per aggiungere host e quindi installare il pacchetto plug-in. I plug-in vengono installati automaticamente sugli host remoti.

**Prima di iniziare**

- Devi essere un utente a cui è assegnato un ruolo che dispone delle autorizzazioni di installazione e disinstallazione del plug-in, ad esempio il ruolo di amministratore SnapCenter .
- Quando si installa un plug-in su un host Windows, se si specifica una credenziale non integrata o se l'utente appartiene a un utente di un gruppo di lavoro locale, è necessario disabilitare UAC sull'host.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata in alto.
3. Selezionare **Aggiungi**.
4. Nella pagina Host procedi come segue:
   a. Nel campo Tipo di host, selezionare il tipo di host.
   b. Nel campo Nome host, immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo Credenziali, inserisci le credenziali che hai creato.
5. Nella sezione **Seleziona i plug-in da installare**, seleziona i plug-in da installare.
6. (Facoltativo) Fare clic su **Altre opzioni** e specificare i dettagli.
7. Seleziona **Invia**.
8. Selezionare **Configura directory registro** e nella pagina Configura directory registro host, immettere il percorso SMB della directory registro host e fare clic su **Salva**.
9. Fare clic su **Invia** e monitorare l'avanzamento dell'installazione.

## Creare criteri di backup per i database di SQL Server

È possibile creare un criterio di backup per la risorsa o il gruppo di risorse prima di utilizzare SnapCenter per eseguire il backup delle risorse di SQL Server oppure è possibile creare un criterio di backup al momento della creazione di un gruppo di risorse o del backup di una singola risorsa.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Fare clic su **Nuovo**.
4. Nella pagina Nome, immettere il nome e la descrizione della policy.
5. Nella pagina Tipo di policy, procedere come segue:
   a. Selezionare * Azure NetApp Files* come tipo di archiviazione.
   b. Selezionare il tipo di backup.
      i. Selezionare **Backup completo e backup del registro** se si desidera eseguire il backup dei file del database e dei registri delle transazioni.
      ii. Selezionare **Backup completo** se si desidera eseguire il backup solo dei file del database.
      iii. Selezionare **Backup del registro** se si desidera eseguire il backup solo dei registri delle transazioni.
      iv. Selezionare **Copia solo backup** se si desidera eseguire il backup delle risorse utilizzando un'altra applicazione.

c. Nella sezione Impostazioni gruppo di disponibilità, eseguire le seguenti azioni:
    i. Selezionare Backup sulla replica di backup preferita se si desidera eseguire il backup solo sulla replica.
    ii. Selezionare la replica AG primaria o la replica AG secondaria per il backup.
    iii. Selezionare la priorità del backup.
6. Nella pagina Snapshot e backup, procedere come segue:
    a. Selezionare la frequenza del backup pianificato.
    b. Specificare le impostazioni di conservazione in base al tipo di backup selezionato.
    c. Se si desidera abilitare il backup Azure NetApp Files , selezionare **Abilita backup** e specificare le impostazioni di conservazione.
7. Nella pagina Verifica, procedere come segue:
    a. Nella sezione Esegui verifica per le seguenti pianificazioni di backup, seleziona la frequenza della pianificazione.
    b. Nella sezione Opzioni di controllo della coerenza del database, eseguire le seguenti azioni:
        i. Selezionare **Limita la struttura di integrità alla struttura fisica del database (PHYSICAL_ONLY)** per limitare il controllo di integrità alla struttura fisica del database e per rilevare pagine danneggiate, errori di checksum e guasti hardware comuni che hanno un impatto sul database.
        ii. Selezionare **Sopprimi tutti i messaggi informativi (NO_INFOMSGS)** per sopprimere tutti i messaggi informativi.

            Selezionato per impostazione predefinita.

        iii. Selezionare **Visualizza tutti i messaggi di errore segnalati per oggetto (ALL_ERRORMSGS)** per visualizzare tutti gli errori segnalati per oggetto.
        iv. Selezionare **Non controllare gli indici non cluster (NOINDEX)** se non si desidera controllare gli indici non cluster.

            Il database di SQL Server utilizza Microsoft SQL Server Database Consistency Checker (DBCC) per verificare l'integrità logica e fisica degli oggetti nel database.

        v. Selezionare **Limita i controlli e ottieni i blocchi anziché utilizzare una copia Snapshot del database interno (TABLOCK)** per limitare i controlli e ottenere i blocchi anziché utilizzare una copia Snapshot del database interno.
    c. Nella sezione **Backup del registro**, seleziona **Verifica il backup del registro al completamento** per verificare il backup del registro al completamento.
    d. Nella sezione **Impostazioni script di verifica**, immettere il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di verifica.
8. Rivedi il riepilogo e clicca su **Fine**.

## Crea gruppi di risorse e collega criteri di backup SQL

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario

allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
| --- | --- |
| Nome | Immettere un nome per il gruppo di risorse. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.
   b. Nella colonna Configura pianificazioni, fare clic su * + * per la policy che vuoi configurare.
   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.
   d. Selezionare lo scheduler di Microsoft SQL Server.
7. Nella pagina Verifica, procedere come segue:
   a. Seleziona il server di verifica.
   b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi fai clic su * + *.
   c. Selezionare **Esegui verifica dopo backup** oppure **Esegui verifica pianificata**.
   d. Fare clic su **OK**.
8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
9. Rivedi il riepilogo e poi clicca su **Fine**.

## Eseguire il backup dei database di SQL Server in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Prima di iniziare**

È necessario creare un bilanciatore del carico se al cluster di failover Windows di Azure non è assegnato un IP del cluster o se non è raggiungibile da SnapCenter. L'IP del bilanciatore del carico deve essere configurato e raggiungibile dal server SnapCenter .

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, seleziona **Database**, **Istanza** o **Gruppo di disponibilità** dall'elenco a discesa Visualizza.
3. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.
4. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.
   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.

      *policy_name* è il nome della policy selezionata.

   d. Selezionare **Usa scheduler di Microsoft SQL Server**, quindi selezionare l'istanza dello scheduler dall'elenco a discesa **Istanza dello scheduler** associata al criterio di pianificazione.
5. Nella pagina Verifica, procedere come segue:
   a. Seleziona il server di verifica.
   b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi fai clic su * + *.
   c. Selezionare **Esegui verifica dopo backup** oppure **Esegui verifica pianificata**.
   d. Fare clic su OK.
6. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
7. Rivedi il riepilogo e poi clicca su **Fine**.
8. Seleziona **Esegui backup adesso**.
9. Nella pagina Backup, procedere come segue:
   a. Se alla risorsa sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.
   b. Selezionare **Verifica dopo il backup**.

c. Selezionare **Backup**.

10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Eseguire il backup dei gruppi di risorse di SQL Server

È possibile eseguire il backup dei gruppi di risorse costituiti da più risorse. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se al gruppo di risorse sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.
   b. Dopo il backup, seleziona **Verifica** per verificare il backup su richiesta.
   c. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Ripristinare e recuperare i database di SQL Server

È possibile utilizzare SnapCenter per ripristinare i database SQL Server sottoposti a backup. Il ripristino del database è un processo multifase che copia tutti i dati e le pagine di registro da un backup di SQL Server specificato a un database specificato.

**Informazioni su questo compito**

È necessario assicurarsi che l'istanza di destinazione per il ripristino sia configurata con un utente di Active Directory appartenente al dominio Active Directory SMB e che disponga delle autorizzazioni per impostare le autorizzazioni dei file in modo appropriato. È necessario configurare le credenziali in SnapCenter a livello di istanza.

L'autenticazione SQL per l'istanza di destinazione non sarà supportata per le configurazioni SMB. L'istanza di destinazione deve essere configurata in SnapCenter con l'utente di Active Directory dotato delle autorizzazioni richieste.

Se l'account del servizio SnapCenter Plug-in non è un utente di Active Directory, durante l'esecuzione del ripristino su un host alternativo, è necessario che l'utente abbia il controllo completo sui volumi di origine in modo che possa essere impersonato ed eseguire l'operazione richiesta.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database o il gruppo di risorse dall'elenco.

4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione.
5. Selezionare il backup dalla tabella, quindi fare clic su icona.
6. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:
   a. Selezionare **Ripristina il database sullo stesso host in cui è stato creato il backup** se si desidera ripristinare il database sullo stesso server SQL in cui vengono eseguiti i backup.
   b. Selezionare **Ripristina il database su un host alternativo** se si desidera che il database venga ripristinato su un server SQL diverso nello stesso host o in uno diverso in cui vengono eseguiti i backup.
7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:
   a. Selezionare **Nessuno** quando è necessario ripristinare solo il backup completo senza alcun registro.
   b. Selezionare l'operazione di ripristino del backup aggiornato **Tutti i backup del registro** per ripristinare tutti i backup del registro disponibili dopo il backup completo.
   c. Selezionare **Tramite backup del registro** per eseguire un'operazione di ripristino in un punto temporale specifico, che ripristina il database in base ai registri di backup fino al registro di backup con la data selezionata.
   d. Selezionare **In base a una data specifica fino a** per specificare la data e l'ora dopo le quali i registri delle transazioni non vengono applicati al database ripristinato.
   e. Se hai selezionato **Tutti i backup dei log**, **Per backup dei log** o **Per data specifica fino a** e i log si trovano in una posizione personalizzata, seleziona **Usa directory dei log personalizzata**, quindi specifica la posizione del log.
8. Nella pagina Pre-operatori e Post-operatori, specificare i dettagli richiesti.
9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

## Clona il backup del database SQL Server

È possibile utilizzare SnapCenter per clonare un database SQL utilizzando il backup del database. I cloni creati sono cloni spessi e vengono creati sul pool di capacità padre.

**Informazioni su questo compito**

È necessario assicurarsi che l'istanza di destinazione per il clone sia configurata con un utente di Active Directory appartenente al dominio Active Directory SMB e che disponga delle autorizzazioni per impostare le autorizzazioni dei file in modo appropriato. È necessario configurare le credenziali in SnapCenter a livello di istanza.

L'autenticazione SQL per l'istanza di destinazione non sarà supportata per le configurazioni SMB. L'istanza di destinazione deve essere configurata in SnapCenter con l'utente di Active Directory dotato delle autorizzazioni richieste.

Se l'account del servizio SnapCenter Plug-in non è un utente di Active Directory, durante l'esecuzione della clonazione è necessario che l'utente abbia il controllo completo sui volumi di origine, in modo che possa essere impersonato ed eseguire l'operazione richiesta.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database o il gruppo di risorse.
4. Dalla pagina di visualizzazione **Gestisci copie**, seleziona il backup dal sistema di archiviazione primario.
5. Seleziona il backup, quindi seleziona * *.
6. Nella pagina **Opzioni di clonazione**, fornisci tutti i dettagli richiesti.
7. Nella pagina Posizione, seleziona una posizione di archiviazione per creare un clone.

   Se i volumi ANF del database SQL Server sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificato il QOS per i volumi clonati, verrà utilizzato il QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

8. Nella pagina Registri, seleziona una delle seguenti opzioni:
   a. Selezionare **Nessuno** se si desidera clonare solo il backup completo senza alcun registro.
   b. Selezionare **Tutti i backup del registro** se si desidera clonare tutti i backup del registro disponibili con data successiva al backup completo.
   c. Selezionare **Per backup del registro fino a** se si desidera clonare il database in base ai registri di backup creati fino al registro di backup con la data selezionata.
   d. Selezionare **Entro una data specifica fino a** se non si desidera applicare i registri delle transazioni dopo la data e l'ora specificate.
9. Nella pagina **Script**, immettere il timeout dello script, il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
10. Nella pagina **Notifica**, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
11. Rivedi il riepilogo e seleziona **Fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

### Eseguire il ciclo di vita della clonazione

Utilizzando SnapCenter, è possibile creare cloni da un gruppo di risorse o da un database. È possibile eseguire la clonazione su richiesta oppure pianificare operazioni di clonazione ricorrenti di un gruppo di risorse o di un database. Se si clona periodicamente un backup, è possibile utilizzare il clone per sviluppare applicazioni, popolare dati o recuperare dati.

#### Passi

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il database o il gruppo di risorse.
4. Dalla pagina di visualizzazione **Gestisci copie**, seleziona il backup dal sistema di archiviazione primario.
5. Seleziona il backup, quindi seleziona * *.

6. Nella pagina **Opzioni di clonazione**, fornisci tutti i dettagli richiesti.
7. Nella pagina Posizione, seleziona una posizione di archiviazione per creare un clone.

   Se i volumi ANF del database SQL Server sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificato il QOS per i volumi clonati, verrà utilizzato il QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.
8. Nella pagina **Script**, immettere il timeout dello script, il percorso e gli argomenti del prescript o del postscript che devono essere eseguiti rispettivamente prima o dopo l'operazione di clonazione.
9. Nella pagina Pianificazione, eseguire una delle seguenti azioni:
   - Selezionare **Esegui ora** se si desidera eseguire immediatamente il processo di clonazione.
   - Selezionare **Configura pianificazione** quando si desidera determinare la frequenza con cui deve avvenire l'operazione di clonazione, quando deve iniziare la pianificazione della clonazione, in quale giorno deve avvenire l'operazione di clonazione, quando deve scadere la pianificazione e se i cloni devono essere eliminati dopo la scadenza della pianificazione.
10. Nella pagina **Notifica**, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
11. Rivedi il riepilogo e seleziona **Fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

# Proteggere i database Oracle

## Aggiungi host e installa il plug-in SnapCenter per il database Oracle

È possibile utilizzare la pagina Aggiungi host per aggiungere host e quindi installare il pacchetto di plug-in SnapCenter per Linux o il pacchetto di plug-in SnapCenter per AIX. I plug-in vengono installati automaticamente sugli host remoti.

È possibile aggiungere un host e installare pacchetti plug-in per un singolo host o per un cluster. Se si installa il plug-in su un cluster (Oracle RAC), il plug-in viene installato su tutti i nodi del cluster. Per Oracle RAC One Node, è necessario installare il plug-in sia sui nodi attivi che su quelli passivi.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che la scheda **Host gestiti** sia selezionata.
3. Fare clic su **Aggiungi**.
4. Nella pagina Host, eseguire le seguenti azioni:
   a. Nel campo Tipo di host, selezionare il tipo di host.
   b. Nel campo Nome host, immettere il nome di dominio completo (FQDN) o l'indirizzo IP dell'host.
   c. Nel campo Credenziali, inserisci le credenziali che hai creato.
5. Nella sezione Seleziona plug-in da installare, seleziona i plug-in da installare.
6. (Facoltativo) Fare clic su **Altre opzioni** e specificare i dettagli.
7. Fare clic su **Invia**.

8. Verificare l'impronta digitale, quindi fare clic su **Conferma e invia**.

   In una configurazione cluster, è necessario verificare l'impronta digitale di ciascun nodo del cluster.

9. Monitorare l'avanzamento dell'installazione.

## Creare policy di backup per i database Oracle

Prima di utilizzare SnapCenter per eseguire il backup delle risorse del database Oracle, è necessario creare un criterio di backup per la risorsa o il gruppo di risorse di cui si desidera eseguire il backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare Oracle Database dall'elenco a discesa.
4. Fare clic su **Nuovo**.
5. Nella pagina Nome, immettere il nome e la descrizione della policy.
6. Nella pagina Tipo di policy, procedere come segue:
   a. Selezionare * Azure NetApp Files* come tipo di archiviazione.
   b. Selezionare il tipo di backup, ovvero backup online o offline.
   c. Se si desidera catalogare il backup utilizzando Oracle Recovery Manager (RMAN), selezionare **Catalog backup with Oracle Recovery Manager (RMAN)**.
   d. Se si desidera eliminare i log di archivio dopo il backup, selezionare **Elimina log di archivio dopo il backup**.
   e. Specificare le impostazioni del registro di eliminazione dell'archivio.
7. Nella pagina Snapshot e backup, procedere come segue:
   a. Selezionare la frequenza del backup pianificato.
   b. Specificare le impostazioni di conservazione.
   c. Se si desidera abilitare il backup Azure NetApp Files , selezionare **Abilita backup** e specificare le impostazioni di conservazione.
8. Nella pagina Script, immettere il percorso e gli argomenti del prescript o del postscript che si desidera eseguire rispettivamente prima o dopo l'operazione di backup.
9. Nella pagina Verifica, seleziona la pianificazione del backup per cui desideri eseguire l'operazione di verifica e immetti il percorso e gli argomenti del prescript o del postscript che desideri eseguire rispettivamente prima o dopo l'operazione di verifica.
10. Rivedi il riepilogo e clicca su **Fine**.

## Crea gruppi di risorse e collega policy di backup Oracle

Un gruppo di risorse è il contenitore a cui è necessario aggiungere le risorse di cui si desidera eseguire il backup e la protezione.

Un gruppo di risorse consente di eseguire il backup simultaneo di tutti i dati associati a una determinata applicazione. Per qualsiasi attività di protezione dei dati è necessario un gruppo di risorse. È inoltre necessario

allegare una o più policy al gruppo di risorse per definire il tipo di processo di protezione dei dati che si desidera eseguire.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, fare clic su **Nuovo gruppo di risorse**.
3. Nella pagina Nome, eseguire le seguenti azioni:

| Per questo campo… | Fai questo… |
|---|---|
| Nome | Immettere un nome per il gruppo di risorse. |
| Etichette | Inserisci una o più etichette che ti aiuteranno a cercare in seguito il gruppo di risorse. |
| Utilizza il formato nome personalizzato per la copia Snapshot | Selezionare questa casella di controllo e immettere un formato di nome personalizzato che si desidera utilizzare per il nome dello snapshot. |
| Destinazione del file di registro dell'archivio | Specificare le destinazioni dei file di registro dell'archivio. |

4. Nella pagina Risorse, seleziona un nome host dall'elenco a discesa **Host** e il tipo di risorsa dall'elenco a discesa **Tipo di risorsa**.
5. Seleziona le risorse dalla sezione **Risorse disponibili**, quindi fai clic sulla freccia destra per spostarle nella sezione **Risorse selezionate**.
6. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.
   b. Nella colonna Configura pianificazioni, fare clic su * * per la policy che vuoi configurare.
   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi fare clic su **OK**.
7. Nella pagina Verifica, procedere come segue:
   a. Seleziona il server di verifica.
   b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi fai clic su * .
   c. Selezionare **Esegui verifica dopo backup** oppure **Esegui verifica pianificata**.
   d. Fare clic su **OK**.
8. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
9. Rivedi il riepilogo e poi clicca su **Fine**.

## Eseguire il backup dei database Oracle in esecuzione su Azure NetApp Files

Se una risorsa non fa ancora parte di alcun gruppo di risorse, è possibile eseguirne il backup dalla pagina Risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.
2. Nella pagina Risorsa, seleziona **Database** dall'elenco a discesa Visualizza.
3. Nella pagina Risorsa, seleziona **Usa formato nome personalizzato per copia Snapshot**, quindi immetti un formato nome personalizzato che desideri utilizzare per il nome Snapshot.
4. Nella pagina Criteri, procedere come segue:
   a. Selezionare una o più policy dall'elenco a discesa.
   b. Seleziona * + * nella colonna Configura pianificazioni per il criterio per il quale si desidera configurare una pianificazione.
   c. Nella finestra di dialogo Aggiungi pianificazioni per il criterio *nome_criterio*, configurare la pianificazione, quindi selezionare **OK**.
5. Nella pagina Verifica, procedere come segue:
   a. Seleziona il server di verifica.
   b. Seleziona la policy per la quale desideri configurare la pianificazione della verifica, quindi fai clic su * + *.
   c. Selezionare **Esegui verifica dopo backup** oppure **Esegui verifica pianificata**.
   d. Fare clic su OK.
6. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
7. Rivedi il riepilogo e poi clicca su **Fine**.
8. Seleziona **Esegui backup adesso**.
9. Nella pagina Backup, procedere come segue:
   a. Se alla risorsa sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.
   b. Fare clic su **Backup**.
10. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

## Eseguire il backup dei gruppi di risorse Oracle

È possibile eseguire il backup dei gruppi di risorse costituiti da più risorse. Un'operazione di backup sul gruppo di risorse viene eseguita su tutte le risorse definite nel gruppo di risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, seleziona **Risorse**, quindi seleziona il plug-in appropriato dall'elenco.

2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Nella pagina Gruppi di risorse, seleziona il gruppo di risorse di cui vuoi eseguire il backup, quindi seleziona **Esegui backup ora**.
4. Nella pagina Backup, procedere come segue:
   a. Se al gruppo di risorse sono associati più criteri, dall'elenco a discesa **Criterio** selezionare il criterio che si desidera utilizzare per il backup.
   b. Selezionare **Backup**.
5. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

## Ripristinare e recuperare i database Oracle

In caso di perdita di dati, è possibile utilizzare SnapCenter per ripristinare i dati da uno o più backup sul file system attivo e quindi recuperare il database.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database o il gruppo di risorse dall'elenco.
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione primario.
5. Seleziona il backup dalla tabella, quindi fai clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
   a. Selezionare RAC se è stato selezionato un backup di un database in ambiente RAC.
   b. Eseguire le seguenti azioni:
      i. Selezionare **Tutti i file di dati** se si desidera ripristinare solo i file del database.
      ii. Selezionare **Tablespace** se si desidera ripristinare solo i tablespace.
      iii. Selezionare **File di redo log** se si desidera ripristinare i file di redo log dei database Data Guard standby o Active Data Guard standby.
      iv. Selezionare **Database collegabili** e specificare i PDB che si desidera ripristinare.
      v. Selezionare **Spazi tabella del database collegabile (PDB)**, quindi specificare il PDB e gli spazi tabella di quel PDB che si desidera ripristinare.
      vi. Selezionare **Ripristina il database sullo stesso host in cui è stato creato il backup** se si desidera ripristinare il database sullo stesso server SQL in cui vengono eseguiti i backup.
      vii. Selezionare **Ripristina il database su un host alternativo** se si desidera che il database venga ripristinato su un server SQL diverso nello stesso host o in uno diverso in cui vengono eseguiti i backup.
      viii. Selezionare **Modifica stato del database se necessario per il ripristino e il recupero** per modificare lo stato del database nello stato richiesto per eseguire operazioni di ripristino e recupero.
      ix. Selezionare **Forza ripristino sul posto** se si desidera eseguire il ripristino sul posto negli scenari in cui vengono aggiunti nuovi file di dati dopo il backup o quando i LUN vengono aggiunti, eliminati o ricreati in un gruppo di dischi LVM.

7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:
    a. Selezionare **Tutti i registri** se si desidera ripristinare l'ultima transazione.
    b. Selezionare **Fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
    c. Seleziona **Data e ora** se desideri ripristinare una data e un'ora specifiche.
    d. Seleziona **Nessun ripristino** se non desideri effettuare il ripristino.
    e. Selezionare **Specifica posizioni registro archivio esterno** se si desidera specificare la posizione dei file registro archivio esterno.
8. Nella pagina Pre-operatori e Post-operatori, specificare i dettagli richiesti.
9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare l'avanzamento dell'operazione cliccando su **Monitoraggio** > **Lavori**.

### Ripristina e recupera gli spazi tabella utilizzando il ripristino point-in-time

È possibile ripristinare un sottoinsieme di tablespace danneggiati o eliminati senza influire sugli altri tablespace nel database. SnapCenter utilizza RMAN per eseguire il ripristino point-in-time (PITR) degli spazi tabella.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione.

    Se il backup non è catalogato, selezionarlo e fare clic su **Catalogo**.

5. Selezionare il backup catalogato, quindi fare clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
    a. Selezionare **RAC** se è stato selezionato un backup di un database in ambiente RAC.
    b. Selezionare **Tablespace** se si desidera ripristinare solo i tablespace.
    c. Selezionare **Modifica stato del database se necessario per il ripristino e il recupero** per modificare lo stato del database nello stato richiesto per eseguire operazioni di ripristino e recupero.
7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:
    a. Selezionare **Fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
    b. Seleziona **Data e ora** se desideri ripristinare una data e un'ora specifiche.
8. Nella pagina Pre-operatori e Post-operatori, specificare i dettagli richiesti.
9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

#### Ripristina e recupera il database collegabile utilizzando il ripristino point-in-time

È possibile ripristinare e recuperare un database collegabile (PDB) danneggiato o eliminato senza influire sugli altri PDB nel database contenitore (CDB). SnapCenter utilizza RMAN per eseguire il ripristino point-in-time (PITR) del PDB.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla vista Gestisci copie, seleziona **Backup** dal sistema di archiviazione.

   Se il backup non è catalogato, selezionarlo e fare clic su **Catalogo**.

5. Selezionare il backup catalogato, quindi fare clic su * *.
6. Nella pagina Ripristina ambito, eseguire le seguenti attività:
   a. Selezionare **RAC** se è stato selezionato un backup di un database in ambiente RAC.
   b. A seconda che si desideri ripristinare il PDB o gli spazi tabella in un PDB, eseguire una delle seguenti azioni:
      - Selezionare **Database collegabili (PDB)** se si desidera ripristinare un PDB.
      - Selezionare **Tablespace del database collegabile (PDB)** se si desidera ripristinare i tablespace in un PDB.
7. Nella pagina Ambito di ripristino, seleziona una delle seguenti opzioni:
   a. Selezionare **Fino a SCN (System Change Number)** se si desidera ripristinare un SCN specifico.
   b. Seleziona **Data e ora** se desideri ripristinare una data e un'ora specifiche.
8. Nella pagina Pre-operatori e Post-operatori, specificare i dettagli richiesti.
9. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
10. Rivedi il riepilogo e poi clicca su **Fine**.
11. Monitorare il processo di ripristino utilizzando la pagina **Monitor** > **Jobs**.

## Clona il backup del database Oracle

È possibile utilizzare SnapCenter per clonare un database Oracle utilizzando il backup del database. I cloni creati sono cloni spessi e vengono creati sul pool di capacità padre.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database.
4. Dalla pagina di visualizzazione Gestisci copie, seleziona il backup dal sistema di archiviazione primario.
5.

Seleziona Backup dati, quindi fai clic su * *.

6. Nella pagina Nome, seleziona se vuoi clonare un database (CDB o non CDB) o clonare un database collegabile (PDB).
7. Nella pagina Posizioni, specificare i dettagli richiesti.

   Se i volumi ANF del database Oracle sono configurati in un pool di capacità QOS manuale, specificare la QOS per i volumi clonati.

   Se non viene specificato il QOS per i volumi clonati, verrà utilizzato il QOS del volume di origine. Se viene utilizzato il pool di capacità QOS automatico, il valore QOS specificato verrà ignorato.

8. Nella pagina Credenziali, eseguire una delle seguenti operazioni:
   a. Per Nome credenziale per utente di sistema, selezionare la credenziale da utilizzare per definire la password dell'utente di sistema del database clone.
   b. Per il nome delle credenziali dell'istanza ASM, selezionare **Nessuno** se l'autenticazione del sistema operativo è abilitata per la connessione all'istanza ASM sull'host clone.

      In caso contrario, selezionare le credenziali Oracle ASM configurate con l'utente "sys" o un utente con privilegio "sysasm" applicabile all'host clone.

9. Nella pagina Pre-Ops specificare il percorso e gli argomenti delle prescrizioni e nella sezione Impostazioni parametri database modificare i valori dei parametri del database precompilati utilizzati per inizializzare il database.
10. Nella pagina Post-Ops, **Recupera database** e **Fino all'annullamento** sono selezionati per impostazione predefinita per eseguire il ripristino del database clonato.
    a. Se si seleziona **Fino all'annullamento**, SnapCenter esegue il ripristino montando l'ultimo backup del registro contenente la sequenza ininterrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione.
    b. Se si seleziona **Data e ora**, SnapCenter recupera il database fino a una data e un'ora specificate.
    c. Se si seleziona **Fino a SCN**, SnapCenter recupera il database fino a un SCN specificato.
    d. Se si seleziona **Specifica posizioni di log di archivio esterno**, SnapCenter identifica e monta il numero ottimale di backup di log in base all'SCN specificato o alla data e all'ora selezionate.
    e. Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** è selezionata per generare un numero univoco (DBID) per il database clonato, differenziandolo dal database di origine.

       Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui è già registrato il database di origine, l'operazione fallisce.

    f. Selezionare la casella di controllo **Crea file temporaneo per tablespace temporaneo** se si desidera creare un file temporaneo per lo spazio tabella temporaneo predefinito del database clonato.
    g. In **Immettere le voci SQL da applicare alla creazione del clone**, aggiungere le voci SQL che si desidera applicare alla creazione del clone.
    h. In **Inserisci gli script da eseguire dopo l'operazione di clonazione**, specifica il percorso e gli argomenti del PostScript che desideri eseguire dopo l'operazione di clonazione.
11. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
12. Rivedi il riepilogo e seleziona **Fine**.

13. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

### Clonare un database collegabile

È possibile clonare un database collegabile (PDB) su un CDB di destinazione diverso o uguale sullo stesso host o su un host alternativo. È anche possibile ripristinare il PDB clonato in un SCN o in una data e ora desiderati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Database** o **Gruppo di risorse** dall'elenco Visualizza.
3. Selezionare il database di tipo istanza singola (multitenant).
4. Dalla pagina di visualizzazione Gestisci copie, seleziona il backup dal sistema di archiviazione primario.
5. Seleziona il backup e poi clicca su * *.
6. Nella pagina Nome, seleziona **PDB Clone** e specifica gli altri dettagli.
7. Nella pagina Posizioni, specificare i dettagli richiesti.
8. Nella pagina Pre-Ops specificare il percorso e gli argomenti delle prescrizioni e nella sezione Impostazioni parametri database modificare i valori dei parametri del database precompilati utilizzati per inizializzare il database.
9. Nella pagina Post-Ops, **Fino all'annullamento** è selezionato per impostazione predefinita per eseguire il ripristino del database clonato.
   a. Se si seleziona **Fino all'annullamento**, SnapCenter esegue il ripristino montando l'ultimo backup del registro contenente la sequenza ininterrotta dei registri di archivio dopo il backup dei dati selezionato per la clonazione.
   b. Se si seleziona **Data e ora**, SnapCenter recupera il database fino a una data e un'ora specificate.
   c. Se si seleziona **Specifica posizioni di log di archivio esterno**, SnapCenter identifica e monta il numero ottimale di backup di log in base all'SCN specificato o alla data e all'ora selezionate.
   d. Per impostazione predefinita, la casella di controllo **Crea nuovo DBID** è selezionata per generare un numero univoco (DBID) per il database clonato, differenziandolo dal database di origine.

      Deselezionare la casella di controllo se si desidera assegnare il DBID del database di origine al database clonato. In questo scenario, se si desidera registrare il database clonato con il catalogo RMAN esterno in cui è già registrato il database di origine, l'operazione fallisce.

   e. Selezionare la casella di controllo **Crea file temporaneo per tablespace temporaneo** se si desidera creare un file temporaneo per lo spazio tabella temporaneo predefinito del database clonato.
   f. In **Immettere le voci SQL da applicare alla creazione del clone**, aggiungere le voci SQL che si desidera applicare alla creazione del clone.
   g. In **Inserisci gli script da eseguire dopo l'operazione di clonazione**, specifica il percorso e gli argomenti del PostScript che desideri eseguire dopo l'operazione di clonazione.
10. Nella pagina Notifica, dall'elenco a discesa **Preferenza e-mail**, seleziona gli scenari in cui desideri inviare le e-mail.
11. Rivedi il riepilogo e seleziona **Fine**.
12. Monitorare l'avanzamento dell'operazione selezionando **Monitoraggio** > **Lavori**.

# Gestisci SnapCenter Server e i plug-in

## Visualizza dashboard

### Panoramica della dashboard

Dal riquadro di navigazione sinistro SnapCenter , la Dashboard offre una prima panoramica sullo stato di salute del sistema, tra cui attività di lavoro recenti, avvisi, riepilogo della protezione, efficienza e utilizzo dello storage, stato dei processi SnapCenter (backup, clonazione, ripristino), stato della configurazione per host cluster Windows e autonomi, numero di Storage Virtual Machine (SVM) gestite da SnapCenter e capacità della licenza.

Le informazioni visualizzate nella vista Dashboard dipendono dal ruolo assegnato all'utente attualmente connesso a SnapCenter. Alcuni contenuti potrebbero non essere visualizzati se l'utente non dispone dell'autorizzazione per visualizzare tali informazioni.

In molti casi, è possibile visualizzare maggiori informazioni su un display passando il mouse su **i**. In alcuni casi, le informazioni visualizzate nella dashboard sono collegate a informazioni di origine dettagliate nelle pagine dell'interfaccia utente grafica SnapCenter , come Risorse, Monitor e Report.

#### Attività lavorative recenti

Il riquadro Attività recenti mostra le ultime attività di qualsiasi processo di backup, ripristino e clonazione a cui hai accesso. I lavori in questa visualizzazione hanno uno dei seguenti stati: Completato, Avviso, Non riuscito, In esecuzione, In coda e Annullato.

Passando il mouse sopra un lavoro si ottengono maggiori informazioni. È possibile visualizzare ulteriori informazioni sul lavoro cliccando sul numero di un lavoro specifico, che reindirizza alla pagina Monitor. Da lì è possibile ottenere dettagli sul lavoro o informazioni di registro e generare un report specifico per quel lavoro.

Fare clic su **Visualizza tutto** per visualizzare la cronologia di tutti i lavori SnapCenter .

#### Avvisi

Il riquadro Avvisi mostra gli ultimi avvisi critici e di avvertenza non risolti per gli host e SnapCenter Server.

Il conteggio totale degli avvisi di categoria Critica e Avvertenza viene visualizzato nella parte superiore del display. Facendo clic sui totali Critici o Avvertenza si viene reindirizzati alla pagina Avvisi con il filtro specifico applicato nella pagina Avvisi.

Facendo clic su un avviso specifico verrai reindirizzato alla pagina Avvisi per i dettagli relativi all'avviso in questione. Facendo clic su **Visualizza tutto** nella parte inferiore della visualizzazione si viene reindirizzati alla pagina Avvisi, dove è possibile visualizzare un elenco di tutti gli avvisi.

#### Riepilogo della protezione più recente

Il riquadro Riepilogo protezione più recente fornisce lo stato di protezione di tutte le entità a cui hai accesso. Per impostazione predefinita, la visualizzazione è impostata per fornire lo stato di tutti i plug-in. Le informazioni sullo stato vengono fornite per le risorse sottoposte a backup su storage primario come snapshot e su storage secondario tramite le tecnologie SnapMirror e SnapVault . La disponibilità delle informazioni sullo stato di protezione per l'archiviazione secondaria si basa sul tipo di plug-in selezionato.

Se si utilizza un criterio di protezione mirror-vault, i contatori per il riepilogo della protezione vengono visualizzati nel grafico di riepilogo SnapVault e non nel grafico SnapMirror .

Lo stato di protezione dei singoli plug-in è disponibile selezionando un plug-in dal menu a discesa. Un grafico a ciambella mostra la percentuale di risorse protette per il plug-in selezionato. Facendo clic su una fetta di ciambella si viene reindirizzati alla pagina **Report** > **Plug-in**, che fornisce un report dettagliato di tutte le attività di archiviazione primaria e secondaria per il plug-in specificato.

I report sullo storage secondario si applicano solo a SnapVault ; i report SnapMirror non sono supportati.

SAP HANA fornisce informazioni sullo stato di protezione per l'archiviazione primaria e secondaria per gli snapshot. Per i backup basati su file è disponibile solo lo stato di protezione dell'archiviazione primaria.

| Stato di protezione | Archiviazione primaria | Archiviazione secondaria |
|---|---|---|
| Fallito | Numero di entità che fanno parte di un gruppo di risorse, in cui il gruppo di risorse ha eseguito un backup, ma il backup non è riuscito. | Numero di entità con backup che non sono riusciti a trasferire a una destinazione secondaria. |
| Riuscito | Numero di entità in un gruppo di risorse, in cui il backup del gruppo di risorse è stato eseguito correttamente. | Numero di entità con backup trasferiti correttamente a una destinazione secondaria. |
| Non configurato | Conteggio delle entità che non fanno parte di alcun gruppo di risorse e di cui non è stato eseguito il backup. | Conteggio delle entità che fanno parte di uno o più gruppi di risorse non configurati per il trasferimento dei backup a una destinazione secondaria. |
| Non avviato | Conteggio delle entità che fanno parte di un gruppo di risorse, per le quali non è stato eseguito alcun backup. | Non applicabile. |

Se si utilizza SnapCenter Server 4.2 e una versione precedente del plug-in (precedente alla 4.2) per creare backup, il riquadro **Riepilogo protezione più recente** non visualizza lo stato di protezione SnapMirror di questi backup.

### Lavori

Il riquadro Lavori fornisce un riepilogo dei lavori di backup, ripristino e clonazione a cui hai accesso. È possibile personalizzare l'intervallo di tempo per qualsiasi report utilizzando il menu a discesa. Le opzioni relative all'intervallo di tempo sono fisse: ultime 24 ore, ultimi 7 giorni e ultimi 30 giorni. Il report predefinito mostra i processi di protezione dei dati eseguiti negli ultimi 7 giorni.

Le informazioni sui processi di backup, ripristino e clonazione vengono visualizzate in grafici a ciambella. Facendo clic su una fetta di ciambella si viene reindirizzati alla pagina Monitor con filtri di lavoro pre-applicati alla selezione.

| Stato del lavoro | Descrizione |
|---|---|
| Fallito | Numero di lavori falliti. |
| Avvertimento | Numero di lavori in cui si è verificato un errore. |
| Riuscito | Numero di lavori completati con successo. |
| Corsa | Numero di lavori attualmente in esecuzione. |

**Magazzinaggio**

Il riquadro Archiviazione mostra lo spazio di archiviazione primario e secondario consumato dai processi di protezione in un periodo di 90 giorni, illustra graficamente le tendenze di consumo e calcola i risparmi sullo spazio di archiviazione primario. Le informazioni di archiviazione vengono aggiornate ogni 24 ore alle 12:00

Il consumo totale giornaliero, che comprende il numero totale di backup disponibili in SnapCenter e la dimensione occupata da tali backup, verrà visualizzato nella parte superiore dello schermo. Un backup potrebbe avere più snapshot associati e il conteggio rifletterà lo stesso risultato. Ciò è applicabile sia agli snapshot primari che a quelli secondari. Ad esempio, hai creato 10 backup, di cui 2 sono stati eliminati a causa della conservazione dei backup basata su criteri e 1 backup è stato eliminato esplicitamente da te. Verrà quindi visualizzato il conteggio di 7 backup insieme alla dimensione occupata da questi 7 backup.

Il fattore di risparmio di storage per lo storage primario è il rapporto tra la capacità logica (risparmio di cloni e snapshot più storage consumato) e la capacità fisica dello storage primario. Un grafico a barre illustra il risparmio di spazio di archiviazione.

Il grafico a linee traccia separatamente il consumo di storage primario e secondario su base giornaliera per un periodo mobile di 90 giorni. Passando il mouse sui grafici si ottengono risultati dettagliati giorno per giorno.

Se si utilizza SnapCenter Server 4.2 e una versione precedente del plug-in (precedente alla 4.2) per creare backup, il riquadro **Archiviazione** non visualizza il numero di backup, lo spazio di archiviazione utilizzato da tali backup, i risparmi degli snapshot, i risparmi dei cloni e le dimensioni degli snapshot.

**Configurazione**

Il riquadro Configurazione fornisce informazioni consolidate sullo stato di tutti gli host cluster Windows e autonomi attivi gestiti SnapCenter e a cui hai accesso. Sono incluse le informazioni sullo stato dei plug-in associati a tali host.

Facendo clic sul numero accanto a Host si viene reindirizzati alla sezione Host gestiti nella pagina Host. Da lì è possibile ottenere informazioni dettagliate sull'host selezionato.

Inoltre, questa visualizzazione mostra la somma delle SVM ONTAP autonome e delle SVM ONTAP cluster gestite da SnapCenter e a cui hai accesso. Facendo clic sul numero accanto a SVM si viene reindirizzati alla pagina Sistemi di archiviazione. Da lì è possibile ottenere informazioni dettagliate per un SVM selezionato.

Lo stato di configurazione dell'host è rappresentato in rosso (critico), giallo (avviso) e verde (attivo), insieme al numero di host in ogni stato. Per ogni stato vengono forniti messaggi di stato.

| Stato di configurazione | Descrizione |
|---|---|
| Aggiornamento obbligatorio | Numero di host che eseguono plug-in non supportati e necessitano di un aggiornamento. Un plug-in non supportato non è compatibile con questa versione di SnapCenter. |
| Migrazione obbligatoria | Numero di host che eseguono plug-in non supportati e necessitano di migrazione. Un plug-in non supportato non è compatibile con questa versione di SnapCenter. |
| Nessun plug-in installato | Numero di host aggiunti correttamente ma in cui è necessario installare i plug-in oppure l'installazione dei plug-in non è riuscita. |
| Sospeso | Numero di host i cui programmi sono sospesi e in fase di manutenzione. |
| Fermato | Numero di host attivi, ma i servizi plug-in non sono in esecuzione. |
| Host inattivo | Numero di host inattivi o non raggiungibili. |
| Aggiornamento disponibile (facoltativo) | Numero di host in cui è disponibile una versione più recente del pacchetto plug-in per l'aggiornamento. |
| Migrazione disponibile (facoltativa) | Numero di host in cui è disponibile una versione più recente del plug-in per la migrazione. |
| Configurare la directory dei registri | Numero di host in cui è necessario configurare la directory dei log affinché SCSQL esegua il backup del log delle transazioni. |
| Configurare i plug-in VMware | Numero di host in cui è necessario aggiungere il SnapCenter Plug-in for VMware vSphere . |
| Sconosciuto | Numero di host registrati ma l'installazione non è ancora stata avviata. |
| Corsa | Numero di host attivi e plug-in in esecuzione. Nel caso dei plug-in SCSQL, vengono configurati la directory dei log e l'hypervisor. |
| Installazione/Disinstallazione dei plug-in | Numero di host in cui è in corso l'installazione o la disinstallazione del plug-in. |

## Come visualizzare le informazioni sulla dashboard

Dal riquadro di navigazione sinistro SnapCenter è possibile visualizzare vari riquadri o schermate della Dashboard, insieme ai dettagli di sistema associati. Il numero di display disponibili nella Dashboard è fisso e non può essere modificato. Il contenuto fornito in ogni visualizzazione dipende dal controllo degli accessi basato sui ruoli (RBAC).

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**.
2. Fare clic sulle aree attive su ogni display per ottenere informazioni aggiuntive.

   Ad esempio, cliccando su un grafico a ciambella in **Lavori**, verrai reindirizzato alla pagina Monitor per maggiori informazioni sulla tua selezione. Facendo clic su un grafico a ciambella in **Riepilogo protezione**, verrai reindirizzato alla pagina Rapporti, che può fornire maggiori informazioni sulla tua selezione.

## Richiedi report sullo stato dei lavori dalla dashboard

È possibile richiedere report sui processi di backup, ripristino e clonazione dalla pagina Dashboard. Questa funzione è utile se si desidera identificare il numero totale di processi riusciti o falliti nel proprio ambiente SnapCenter .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**
2. Individua il riquadro Lavori nella Dashboard, quindi seleziona **Backup**, **Ripristina** o **Clona**.
3. Utilizzando il menu a discesa, seleziona l'intervallo di tempo per il quale desideri ricevere informazioni sui lavori: 24 ore, 7 giorni o 30 giorni.

   I sistemi visualizzano un grafico a ciambella che copre i dati.

4. Fare clic sulla fetta di ciambella che rappresenta le informazioni sul lavoro per cui si desidera un report.

   Facendo clic sul grafico a ciambella, si viene reindirizzati dalla pagina Dashboard alla pagina Monitor. La pagina Monitor visualizza i lavori con lo stato selezionato dal grafico a ciambella.

5. Dall'elenco della pagina Monitor, fare clic su un lavoro specifico per selezionarlo.
6. Nella parte superiore della pagina Monitor, fare clic su **Report**.

**Risultato**

Il report visualizza solo le informazioni relative al lavoro selezionato. Puoi consultare il report o scaricarlo sul tuo sistema locale.

## Richiedi report sullo stato della protezione dalla dashboard

È possibile richiedere i dettagli sulla protezione per le risorse gestite da plug-in specifici tramite la Dashboard. Per il riepilogo della protezione dei dati vengono presi in considerazione solo i backup dei dati.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**.
2. Individua il riquadro Riepilogo protezione più recente nella Dashboard e utilizza il menu a discesa per selezionare un plug-in.

   La Dashboard visualizza un grafico a ciambella per le risorse sottoposte a backup nell'archiviazione primaria e, se applicabile al plug-in, un grafico a ciambella per le risorse sottoposte a backup nell'archiviazione secondaria.

   I report sulla protezione dei dati sono disponibili solo per specifici tipi di plug-in. La specifica di **Tutti i plug-in** non è supportata.

3. Fare clic sulla fetta di ciambella che rappresenta lo stato per il quale si desidera un report.

   Quando fai clic sul grafico a ciambella, verrai reindirizzato dalla pagina Dashboard ai Report e quindi alla pagina Plug-in. Il report visualizza solo lo stato del plug-in selezionato. Puoi consultare il report o scaricarlo sul tuo sistema locale.

   Il reindirizzamento alla pagina Report per il grafico a ciambella SnapMirror e il backup SAP HANA basato su file non è supportato.

# Gestisci RBAC

SnapCenter consente di modificare ruoli, utenti e gruppi.

## Modificare un ruolo

È possibile modificare un ruolo SnapCenter per rimuovere utenti o gruppi e modificare le autorizzazioni associate al ruolo. È particolarmente utile modificare i ruoli quando si desidera modificare o eliminare le autorizzazioni utilizzate da un intero ruolo.

**Prima di iniziare**

Devi aver effettuato l'accesso con il ruolo "SnapCenterAdmin".

Non è possibile modificare o rimuovere le autorizzazioni per il ruolo SnapCenterAdmin.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Ruoli**.
3. Nel campo Nome ruolo, fare clic sul ruolo che si desidera modificare.
4. Selezionare **Tutti i membri di questo ruolo possono vedere gli oggetti degli altri membri** per consentire agli altri membri del ruolo di vedere risorse quali volumi e host dopo aver aggiornato l'elenco delle risorse.

   Deseleziona questa opzione se non vuoi che i membri di questo ruolo vedano gli oggetti a cui sono assegnati altri membri.

Quando questa opzione è abilitata, non è necessario assegnare agli utenti l'accesso agli oggetti o alle risorse se gli utenti appartengono allo stesso ruolo dell'utente che ha creato gli oggetti o le risorse.

5. Nella pagina Dettagli ruolo, modificare le autorizzazioni o annullare l'assegnazione dei membri in base alle esigenze.
6. Fare clic su **Invia**.

### Modifica utenti e gruppi

È possibile modificare gli utenti o i gruppi SnapCenter per modificarne i ruoli e le risorse.

**Prima di iniziare**

Devi aver effettuato l'accesso come amministratore SnapCenter .

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Utenti e accesso**.
3. Dall'elenco Nome utente o gruppo, fare clic sull'utente o sul gruppo che si desidera modificare.
4. Nella pagina dei dettagli dell'utente o del gruppo, modifica ruoli e risorse.
5. Fare clic su **Invia**.

# Gestisci gli host

È possibile aggiungere host e installare pacchetti plug-in SnapCenter , aggiungere un server di verifica, rimuovere host, migrare processi di backup e aggiornare host per aggiornare pacchetti plug-in o aggiungere nuovi pacchetti plug-in. A seconda del plug-in utilizzato, è anche possibile effettuare il provisioning dei dischi, gestire le condivisioni SMB, gestire i gruppi di iniziatori (iGroup), gestire le sessioni iSCSI e migrare i dati.

| Puoi eseguire queste attività… | Per Microsoft Exchange Server | Per Microsoft SQL Server | Per Microsoft Windows | Per il database Oracle | Per il database SAP HANA | Per i plug-in supportati da NetApp | Per Db2 | Per PostgreSQL | Per MySQL |
|---|---|---|---|---|---|---|---|---|---|
| Aggiungi host e installa il pacchetto plug-in | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ |

| Puoi eseguire queste attività… | Per Microsoft Exchange Server | Per Microsoft SQL Server | Per Microsoft Windows | Per il database Oracle | Per il database SAP HANA | Per i plug-in supportati da NetApp | Per Db2 | Per PostgreSQL | Per MySQL |
|---|---|---|---|---|---|---|---|---|---|
| Aggiornare le informazioni ESXi per un host | NO | SÌ | NO | NO | NO | NO | NO | NO | NO |
| Sospendi le pianificazioni e metti gli host in modalità di manutenzione | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ |
| Modifica gli host aggiungendo, aggiornando o rimuovendo i plug-in | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ |
| Rimuovere gli host da SnapCenter | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ | SÌ |
| Avvia i servizi plug-in (applicabile solo per i plug-in in esecuzione su host Windows) | SÌ | SÌ | SÌ | NO | SÌ | SÌ | SÌ | SÌ | SÌ |

| Puoi eseguire queste attività… | Per Microsoft Exchange Server | Per Microsoft SQL Server | Per Microsoft Windows | Per il database Oracle | Per il database SAP HANA | Per i plug-in supportati da NetApp | Per Db2 | Per PostgreSQL | Per MySQL |
|---|---|---|---|---|---|---|---|---|---|
| Fornire dischi | NO | NO | SÌ | NO | NO | NO | NO | NO | NO |
| Gestire le condivisioni SMB | NO | NO | SÌ | NO | NO | NO | NO | NO | NO |
| Gestisci iGroups | NO | NO | SÌ | NO | NO | NO | NO | NO | NO |
| Gestire le sessioni iSCSI | NO | NO | SÌ | NO | NO | NO | NO | NO | NO |

## Aggiorna le informazioni della macchina virtuale

È necessario aggiornare le informazioni della macchina virtuale quando cambiano le credenziali di VMware vCenter o quando l'host del database o del file system viene riavviato. L'aggiornamento delle informazioni sulla macchina virtuale in SnapCenter avvia la comunicazione con VMware vSphere vCenter e ottiene le credenziali vCenter.

I dischi basati su RDM sono gestiti dal plug-in SnapCenter per Microsoft Windows, installato sull'host del database. Per gestire gli RDM, il plug-in SnapCenter per Microsoft Windows comunica con il server vCenter che gestisce l'host del database.

**Passi**

1. Nel riquadro di navigazione sinistro SnapCenter , fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Nella pagina Host gestiti, seleziona l'host che desideri aggiornare.
4. Fare clic su **Aggiorna VM**.

## Modifica gli host dei plug-in

Dopo aver installato un plug-in, se necessario è possibile modificarne i dettagli host. È possibile modificare le credenziali, il percorso di installazione, i plug-in, i dettagli della directory di registro per il plug-in SnapCenter per Microsoft SQL Server, l'account di servizio gestito del gruppo (gMSA) e la porta del plug-in.

Assicurarsi che la versione del plug-in sia la stessa della versione di SnapCenter Server.

**Informazioni su questo compito**

- È possibile modificare una porta plug-in solo dopo aver installato il plug-in.

Non è possibile modificare la porta del plug-in mentre sono in corso le operazioni di aggiornamento.

- Durante la modifica di una porta plug-in, è necessario tenere presente i seguenti scenari di rollback della porta:
  - In una configurazione autonoma, se SnapCenter non riesce a modificare la porta di uno dei componenti, l'operazione fallisce e la vecchia porta viene mantenuta per tutti i componenti.

    Se la porta è stata modificata per tutti i componenti ma uno di essi non riesce ad avviarsi con la nuova porta, la vecchia porta viene mantenuta per tutti i componenti. Ad esempio, se si desidera modificare la porta per due plug-in sull'host autonomo e SnapCenter non riesce ad applicare la nuova porta a uno dei plug-in, l'operazione fallisce (con un messaggio di errore appropriato) e la vecchia porta viene mantenuta per entrambi i plug-in.

  - In una configurazione in cluster, se SnapCenter non riesce a modificare la porta del plug-in installato su uno dei nodi, l'operazione fallisce e la vecchia porta viene mantenuta per tutti i nodi.

    Ad esempio, se il plug-in è installato su quattro nodi in una configurazione cluster e se la porta non viene modificata per uno dei nodi, la vecchia porta viene mantenuta per tutti i nodi.

Quando i plug-in vengono installati con gMSA, è possibile modificarli nella finestra **Altre opzioni**. Quando i plug-in vengono installati senza gMSA, è possibile specificare l'account gMSA per utilizzarlo come account del servizio plug-in.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Verificare che in alto sia selezionato **Host gestiti**.
3. Selezionare l'host per il quale si desidera modificare e modificare un campo qualsiasi.

   È possibile modificare solo un campo alla volta.
4. Fare clic su **Invia**.

**Risultato**

L'host viene convalidato e aggiunto a SnapCenter Server.

## Avvia o riavvia i servizi plug-in

L'avvio dei servizi plug-in SnapCenter consente di avviare i servizi se non sono in esecuzione o di riavviarli se sono in esecuzione. Potrebbe essere necessario riavviare i servizi dopo aver eseguito la manutenzione.

È necessario assicurarsi che non vi siano processi in esecuzione quando si riavviano i servizi.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Nella pagina Host gestiti, seleziona l'host che desideri avviare.
4. Clic icona e fare clic su **Avvia servizio** o **Riavvia servizio**.

È possibile avviare o riavviare il servizio di più host contemporaneamente.

### Sospendere le pianificazioni per la manutenzione dell'host

Se si desidera impedire all'host di eseguire attività pianificate di SnapCenter , è possibile impostare l'host in modalità di manutenzione. Dovresti farlo prima di aggiornare i plug-in o se stai eseguendo attività di manutenzione sugli host.

Non è possibile sospendere le pianificazioni su un host inattivo perché SnapCenter non riesce a comunicare con tale host.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Nella pagina Host gestiti, seleziona l'host che desideri sospendere.
4. Fare clic su sull'icona, quindi fare clic su **Sospendi pianificazione** per mettere l'host per questo plug-in in modalità di manutenzione.

   È possibile sospendere la pianificazione di più host contemporaneamente.

   Non è necessario interrompere prima il servizio plug-in. Il servizio plug-in può essere in esecuzione o arrestato.

**Risultato**

Dopo aver sospeso le pianificazioni sull'host, la pagina Host gestiti mostra **Sospeso** nel campo Stato generale per l'host.

Dopo aver completato la manutenzione dell'host, puoi uscire dalla modalità di manutenzione facendo clic su **Attiva pianificazione**. È possibile attivare la pianificazione di più host contemporaneamente.

# Operazioni supportate dalla pagina Risorse

È possibile scoprire risorse ed eseguire operazioni di protezione dei dati dalla pagina Risorse. Le operazioni che puoi eseguire variano in base al plug-in che stai utilizzando per gestire le tue risorse.

Dalla pagina Risorse è possibile eseguire le seguenti attività:

| Puoi eseguire queste attività… | Per Microsoft Exchange Server | Per Microsoft SQL Server | Per Microsoft Windows | Per il database Oracle | Per il database SAP HANA |
|---|---|---|---|---|---|
| Determinare se le risorse sono disponibili per il backup | SÌ | SÌ | SÌ | SÌ | SÌ |

| Puoi eseguire queste attività… | Per Microsoft Exchange Server | Per Microsoft SQL Server | Per Microsoft Windows | Per il database Oracle | Per il database SAP HANA |
|---|---|---|---|---|---|
| Eseguire il backup su richiesta di una risorsa | SÌ | SÌ | SÌ | SÌ | SÌ |
| Ripristina dai backup | SÌ | SÌ | SÌ | SÌ | SÌ |
| Backup clonati | NO | SÌ | SÌ | SÌ | SÌ |
| Gestire i backup | SÌ | SÌ | SÌ | SÌ | SÌ |
| Gestisci i cloni | NO | SÌ | SÌ | SÌ | SÌ |
| Gestire le politiche | SÌ | SÌ | SÌ | SÌ | SÌ |
| Gestisci le connessioni di archiviazione | SÌ | SÌ | SÌ | SÌ | SÌ |
| Montare i backup | NO | NO | NO | SÌ | NO |
| Smonta i backup | NO | NO | NO | SÌ | NO |
| Visualizza i dettagli | SÌ | SÌ | SÌ | SÌ | SÌ |

# Gestire le politiche

È possibile staccare i criteri da una risorsa o da un gruppo di risorse, modificarli, eliminarli, visualizzarli e copiarli.

## Modificare le politiche

È possibile modificare le opzioni di replica, le impostazioni di conservazione degli snapshot, il conteggio dei tentativi di errore o le informazioni sugli script mentre un criterio è associato a una risorsa o a un gruppo di risorse. È possibile modificare il tipo di pianificazione (frequenza) solo dopo aver scollegato un criterio.

### Informazioni su questo compito

La modifica del tipo di pianificazione in un criterio richiede passaggi aggiuntivi perché SnapCenter Server registra il tipo di pianificazione solo nel momento in cui il criterio viene associato a una risorsa o a un gruppo di risorse.

| Se lo desidera… | Poi… |
| --- | --- |
| Aggiungi un tipo di pianificazione aggiuntivo | Crea una nuova policy e associala alle risorse o ai gruppi di risorse necessari.<br><br>Ad esempio, se un criterio di gruppo di risorse specifica solo backup orari e si desidera aggiungere anche backup giornalieri, è possibile creare un criterio con un tipo di pianificazione giornaliera e aggiungerlo al gruppo di risorse. Il gruppo di risorse avrebbe quindi due criteri: orario e giornaliero. |
| Rimuovere o modificare un tipo di pianificazione | Eseguire le seguenti operazioni:<br><br>1. Scollegare il criterio da ogni risorsa e gruppo di risorse che utilizza tale criterio.<br>2. Modificare il tipo di pianificazione.<br>3. Associare nuovamente la policy a tutte le risorse e ai gruppi di risorse.<br><br>Ad esempio, se una policy specifica backup orari e si desidera modificarli in backup giornalieri, è necessario prima scollegare la policy. |

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare la policy, quindi fare clic su **Modifica**.
4. Modificare le informazioni, quindi fare clic su **Fine**.

## Distacca le politiche

È possibile scollegare i criteri da una risorsa o da un gruppo di risorse in qualsiasi momento, se non si desidera più che tali criteri governino la protezione dei dati per le risorse. È necessario scollegare un criterio prima di poterlo eliminare o prima di modificarne il tipo di pianificazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il gruppo di risorse, quindi fare clic su **Modifica gruppo di risorse**.
4. Nella pagina Criteri della procedura guidata Modifica gruppo di risorse, dall'elenco a discesa, deselezionare il segno di spunta accanto ai criteri che si desidera scollegare.
5. Apportare eventuali modifiche aggiuntive al gruppo di risorse nel resto della procedura guidata, quindi fare clic su **Fine**.

## Elimina le policy

Se non hai più bisogno di alcune policy, potresti volerle eliminare.

**Prima di iniziare**

Se il criterio è associato a una risorsa o a un gruppo di risorse, è necessario scollegarlo.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Criteri**.
3. Selezionare il criterio, quindi fare clic su **Elimina**.
4. Fare clic su **Sì**.

# Gestire gruppi di risorse

## È possibile eseguire varie operazioni sui gruppi di risorse.

È possibile eseguire le seguenti attività relative ai gruppi di risorse:

- Modifica un gruppo di risorse selezionandolo e cliccando su **Modifica gruppo di risorse** per modificare le informazioni fornite durante la creazione del gruppo di risorse.

  È possibile modificare la pianificazione modificando il gruppo di risorse. Tuttavia, per modificare il tipo di pianificazione è necessario modificare la policy.

  Se si rimuovono risorse da un gruppo di risorse, le impostazioni di conservazione dei backup definite nei criteri attualmente associati al gruppo di risorse continueranno a essere applicate alle risorse rimosse.

- Creare un backup di un gruppo di risorse.
- Crea un clone di un backup.

  È possibile clonare dai backup esistenti di file system SQL, Oracle, Windows, applicazioni personalizzate e risorse o gruppi di risorse del database SAP HANA.

- Crea un clone di un gruppo di risorse.

  Questa operazione è supportata solo per i gruppi di risorse SQL (che contengono solo database). È possibile configurare una pianificazione per la clonazione di un gruppo di risorse (ciclo di vita della clonazione).

- Impedisce l'avvio delle operazioni pianificate sui gruppi di risorse.
- Elimina un gruppo di risorse.

## Interrompere e riprendere le operazioni sui gruppi di risorse

È possibile disabilitare temporaneamente l'avvio delle operazioni pianificate su un gruppo di risorse. Successivamente, quando vorrai, potrai abilitare tali operazioni.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il gruppo di risorse e fare clic su **Manutenzione**.
4. Fare clic su **OK**.

Se si desidera riprendere le operazioni sul gruppo di risorse che era stato messo in modalità di manutenzione, selezionare il gruppo di risorse e fare clic su **Produzione**.

## Elimina gruppi di risorse

È possibile eliminare un gruppo di risorse se non è più necessario proteggere le risorse in esso contenute. Prima di rimuovere i plug-in da SnapCenter, è necessario assicurarsi che i gruppi di risorse siano stati eliminati.

**Informazioni su questo compito**

Dovresti eliminare manualmente tutti i cloni creati per una qualsiasi delle risorse nel gruppo di risorse. Facoltativamente, è possibile forzare l'eliminazione di tutti i backup, metadati, policy e snapshot associati al gruppo di risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona **Gruppo di risorse** dall'elenco **Visualizza**.
3. Selezionare il gruppo di risorse, quindi fare clic su **Elimina**.
4. Facoltativo: selezionare la casella di controllo **Elimina backup e scollega policy associate a questo gruppo di risorse** per rimuovere tutti i backup, i metadati, le policy e gli snapshot associati al gruppo di risorse.
5. Fare clic su **OK**.

# Gestire i backup

È possibile rinominare ed eliminare i backup. È anche possibile eliminare più backup contemporaneamente.

## Rinomina i backup

È possibile rinominare i backup se si desidera fornire un nome migliore per migliorarne la ricercabilità.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse. Se la risorsa o il gruppo di risorse non è configurato per la protezione dei dati, al posto della pagina della topologia viene visualizzata la procedura guidata di protezione.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari.

   Non è possibile rinominare i backup presenti sul sistema di archiviazione secondario.

   Se hai catalogato i backup dei database Oracle utilizzando Oracle Recovery Manager (RMAN), non puoi rinominare i backup catalogati.

5. Selezionare il backup, quindi fare clic su .
6. Nel campo **Rinomina backup come**, inserisci un nuovo nome e fai clic su **OK**.

## Elimina i backup

È possibile eliminare i backup se non sono più necessari per altre operazioni di protezione dei dati.

**Prima di iniziare**

Prima di eliminare un backup, è necessario eliminare i cloni associati.

Se un backup è associato a una risorsa clonata, non è possibile eliminare il backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Backup** dai sistemi di archiviazione primari.

   Non è possibile eliminare i backup presenti sul sistema di archiviazione secondario.

5. Selezionare il backup, quindi fare clic su .

   Se si elimina un backup del database SAP HANA, vengono eliminati anche i cataloghi SAP HANA associati al backup.

   Se viene eliminato l'ultimo backup rimanente, le voci del catalogo HANA associate non potranno essere eliminate.

6. Fare clic su **OK**.

   Se in SnapCenter sono presenti alcuni backup di database obsoleti che non hanno backup corrispondenti sul sistema di archiviazione, è necessario utilizzare il comando remove-smbackup per ripulire queste voci di backup obsolete. Se i backup obsoleti sono stati catalogati, verranno rimossi dal database del catalogo di ripristino.

### Rimuovi protezione

La rimozione della protezione elimina tutti i backup e scollega tutti i criteri. Prima di rimuovere la protezione, è necessario assicurarsi che i backup non siano montati e che non vi siano cloni associati al backup.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Selezionare il backup e fare clic su **Rimuovi protezione**.

# Elimina i cloni

Puoi eliminare i cloni se ritieni che non siano più necessari.

**Informazioni su questo compito**

Non è possibile eliminare i cloni che fungono da origine per altri cloni.

Ad esempio, se il database di produzione è db1, il database clone1 viene clonato dal backup di db1 e successivamente clone1 viene protetto. Il database clone2 viene clonato dal backup di clone1. Se decidi di eliminare clone1, devi prima eliminare clone2 e poi eliminare clone1.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Nella pagina Risorse, seleziona la risorsa o il gruppo di risorse dall'elenco a discesa **Visualizza**.
3. Selezionare la risorsa o il gruppo di risorse dall'elenco.

   Viene visualizzata la pagina della topologia della risorsa o del gruppo di risorse.

4. Dalla vista Gestisci copie, seleziona **Cloni** dai sistemi di archiviazione primari o secondari (con mirroring o replica).
5. Seleziona il clone e poi clicca .

   Se si eliminano cloni del database SAP HANA, nella pagina Elimina clone, eseguire le seguenti azioni:

   a. Nel campo **Eliminazione pre-clone**, immettere i comandi da eseguire prima di eliminare il clone.
   b. Nel campo **Smonta**, immettere il comando per smontare il clone prima di eliminarlo.
6. Fare clic su **OK**.

**Dopo aver finito**

A volte i file system non vengono eliminati. È necessario aumentare il valore del parametro CLONE_DELETE_DELAY eseguendo il seguente comando: `./sccli Set-SmConfigSettings`

Il parametro CLONE_DELETE_DELAY specifica il numero di secondi da attendere dopo aver completato l'eliminazione del clone dell'applicazione e prima di avviare l'eliminazione del file system.

Dopo aver modificato il valore del parametro, riavviare il servizio SnapCenter Plug-in Loader (SPL).

# Monitora lavori, pianificazioni, eventi e registri

Dalla pagina Monitor puoi monitorare l'avanzamento dei tuoi lavori, ottenere informazioni sui lavori programmati e rivedere eventi e registri.

## Monitorare i lavori

È possibile visualizzare informazioni sui processi di backup, clonazione, ripristino e verifica SnapCenter . È possibile filtrare questa visualizzazione in base alla data di inizio e fine, al tipo di processo, al gruppo di risorse, alla policy o al plug-in SnapCenter . È inoltre possibile ottenere dettagli aggiuntivi e file di registro per processi specifici.

È anche possibile monitorare i lavori correlati alle operazioni SnapMirror e SnapVault .

Puoi monitorare solo i lavori che hai creato e che sono rilevanti per te, a meno che non ti sia stato assegnato il ruolo di amministratore SnapCenter o un altro ruolo di superutente.

È possibile eseguire le seguenti attività relative al monitoraggio dei lavori:

- Monitorare le operazioni di backup, clonazione, ripristino e verifica.
- Visualizza i dettagli e i report del lavoro.
- Interrompere un lavoro pianificato.

### Gestire i processi di backup pianificati

A partire dalla versione 6.0.1 SnapCenter , è stato introdotto un nuovo parametro **JobConcurrencyThreshold** che imposta una soglia per il numero di processi pianificati che possono essere eseguiti in un dato momento. Ciò consente di controllare il numero di backup che si desidera eseguire in base alla configurazione hardware dei sistemi.

Il valore predefinito assegnato a **JobConcurrencyThreshold** è 0 ed è disabilitato. È possibile abilitare l'opzione assegnando un valore se si osserva un calo delle prestazioni durante la finestra di backup pianificata.

Se si abilita **JobConcurrencyThreshold** per gestire i processi simultanei, SnapCenter non consentirà di controllare l'ordine dei backup e i backup potrebbero non essere attivati contemporaneamente all'ora specificata nella pianificazione.

**Passi**

1. Impostare il valore del parametro *JobConcurrencyThreshold* situato in *C:\Program Files\ NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config*.
2. Riciclare il pool di applicazioni SnapCenter facendo clic su IIS > Pool di applicazioni > SnapCenter > Riavvia.
3. Riavviare il servizio Web SnapCenter facendo clic su IIS > Siti > SnapCenter > Riavvia.

### Gestisci i lavori obsoleti

I lavori obsoleti vengono creati da interruzioni in SnapCenter o da aggiornamenti di lavoro non corretti. A partire dalla versione 6.0.1 SnapCenter , è stata introdotta una pianificazione predefinita per ripulire i processi obsoleti bloccati per più di 72 ore. È possibile modificare la frequenza di pianificazione modificando il parametro configurabile **CleanUpStaleJobsIntervalHours**.

È possibile attivare la pulizia su richiesta eseguendo la pianificazione da **Monitor** > **Pianificazioni** > **SnapCenter_StaleJobCleanUp**.

#### Passi

1. Impostare il valore del parametro *CleanUpStaleJobsIntervalHours* situato in *C:\Program Files\ NetApp\ SnapCenter WebApp\ SnapManager.Web.UI.dll.config*.
2. Riciclare il pool di applicazioni SnapCenter facendo clic su IIS > Pool di applicazioni > SnapCenter > Riavvia.
3. Riavviare il servizio Web SnapCenter facendo clic su IIS > Siti > SnapCenter > Riavvia.

## Monitorare gli orari

Potrebbe essere utile visualizzare le pianificazioni correnti per determinare quando inizia l'operazione, quando è stata eseguita l'ultima volta e quando verrà eseguita la prossima. È anche possibile determinare l'host su cui viene eseguita l'operazione, insieme al gruppo di risorse dell'operazione e alle informazioni sui criteri.

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Pianificazioni**.
3. Selezionare il gruppo di risorse e il tipo di pianificazione.
4. Visualizza l'elenco delle operazioni programmate.

## Monitorare gli eventi

È possibile visualizzare un elenco di eventi SnapCenter nel sistema, ad esempio quando un utente crea un gruppo di risorse o quando il sistema avvia attività, come la creazione di un backup pianificato. Potrebbe essere necessario visualizzare gli eventi per determinare se è in corso un'operazione, ad esempio un backup o un ripristino.

#### Informazioni su questo compito

Tutte le informazioni sul lavoro vengono visualizzate nella pagina Eventi. Ad esempio, quando viene avviato un processo di backup, viene visualizzato l'evento "avvio backup". Al termine del backup, viene visualizzato l'evento "backup completato".

#### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Monitor, fare clic su **Eventi**.
3. (Facoltativo) Nella casella Filtro, immettere la data di inizio o di fine, la categoria dell'evento (ad esempio backup, gruppo di risorse o criterio) e il livello di gravità, quindi fare clic su **Applica**. In alternativa, inserisci i caratteri nella casella di ricerca.

4. Visualizza l'elenco degli eventi.

## Monitorare i registri

È possibile visualizzare e scaricare i registri di SnapCenter Server, i registri dell'agente host SnapCenter e i registri dei plug-in. Potrebbe essere utile visualizzare i registri per facilitare la risoluzione dei problemi.

**Informazioni su questo compito**

È possibile filtrare i log per visualizzare solo un livello di gravità specifico:

- Debug
- Informazioni
- Avvisare
- Errore
- Fatale

È anche possibile ottenere registri a livello di processo, ad esempio registri che aiutano a risolvere i problemi relativi al motivo dell'errore di un processo di backup. Per i registri a livello di lavoro, utilizzare l'opzione **Monitor** > **Lavori**.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
2. Nella pagina Lavori, seleziona un lavoro e fai clic su Scarica registri.

   La cartella compressa scaricata contiene i registri dei lavori e i registri comuni. Il nome della cartella compressa contiene l'ID del lavoro e il tipo di lavoro selezionato.

3. Nella pagina Monitor, fare clic su **Registri**.
4. Selezionare il tipo di registro, l'host e l'istanza.

   Se selezioni il tipo di registro come **plugin**, puoi selezionare un host o un plug-in SnapCenter . Non puoi farlo se il tipo di registro è **server**.

5. Per filtrare i log in base a una specifica origine, messaggio o livello di log, fare clic sull'icona del filtro nella parte superiore dell'intestazione della colonna.

   Per visualizzare tutti i registri, seleziona **Maggiore o uguale a** come `Debug` livello.

6. Fare clic su **Aggiorna**.
7. Visualizza l'elenco dei registri.
8. Fare clic su **Scarica** per scaricare i registri.

   La cartella compressa scaricata contiene i registri dei lavori e i registri comuni. Il nome della cartella compressa contiene l'ID del lavoro e il tipo di lavoro selezionato.

Nelle configurazioni di grandi dimensioni, per ottenere prestazioni ottimali, è consigliabile impostare le impostazioni di registro per SnapCenter al livello minimo utilizzando il cmdlet di PowerShell.

```
Set-SmLogSettings -LogLevel All -MaxFileSize 10MB -MaxSizeRollBackups 10
```

```
-JobLogsMaxFileSize 10MB -Server
```

Per accedere alle informazioni sullo stato o sulla configurazione al termine di un processo di failover, eseguire il cmdlet `Get-SmRepositoryConfig` .

## Rimuovere lavori e registri da SnapCenter

È possibile rimuovere i processi e i registri di backup, ripristino, clonazione e verifica da SnapCenter. SnapCenter memorizza i registri dei lavori riusciti e non riusciti in modo indefinito, a meno che non vengano rimossi. Potresti volerli rimuovere per ripristinare lo spazio di archiviazione.

### Informazioni su questo compito

Non devono esserci posti di lavoro attualmente in corso. È possibile rimuovere un lavoro specifico fornendo un ID lavoro oppure è possibile rimuovere i lavori entro un periodo di tempo specificato.

Non è necessario mettere l'host in modalità di manutenzione per rimuovere i processi.

### Passi

1. Avvia PowerShell.
2. Dal prompt dei comandi, immettere: `Open-SMConnection`
3. Dal prompt dei comandi, immettere: `Remove-SmJobs`
4. Nel riquadro di navigazione a sinistra, fare clic su **Monitor**.
5. Nella pagina Monitor, fare clic su **Lavori**.
6. Nella pagina Lavori, controlla lo stato del lavoro.

### Informazioni correlate

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

# Panoramica delle funzionalità di reporting SnapCenter

SnapCenter offre una varietà di opzioni di reporting che consentono di monitorare e gestire lo stato del sistema e il successo delle operazioni.

| Tipo di rapporto | Descrizione |
| --- | --- |
| Rapporto di backup | Il report di backup fornisce dati complessivi sulle tendenze di backup per l'ambiente SnapCenter , sulla percentuale di successo dei backup e alcune informazioni su ciascun backup eseguito durante il periodo di tempo specificato. Se un backup viene eliminato, il report non visualizza alcuna informazione sullo stato del backup eliminato. Il rapporto dettagliato sul backup fornisce informazioni dettagliate su un processo di backup specificato ed elenca le risorse il cui backup è stato eseguito correttamente e quelle il cui backup non è riuscito. |
| Rapporto di clonazione | Il report di clonazione fornisce dati generali sulle tendenze di clonazione per l'ambiente SnapCenter , il tasso di successo della clonazione e alcune informazioni su ciascun processo di clonazione eseguito durante il periodo di tempo specificato. Se un clone viene eliminato, il report non visualizza alcuna informazione sullo stato del clone eliminato. Il report dettagliato del clone fornisce informazioni dettagliate sul clone specificato, sull'host del clone e sullo stato dell'attività del processo di clone. Se un'attività fallisce, il report dettagliato sulla clonazione visualizza informazioni sull'errore. |
| Ripristina rapporto | Il rapporto di ripristino fornisce informazioni generali sui processi di ripristino. Il rapporto dettagliato sul ripristino fornisce informazioni dettagliate su un processo di ripristino specificato, tra cui il nome host, il nome del backup, l'inizio e la durata del processo e lo stato delle singole attività del processo. Se un'attività non riesce, il rapporto dettagliato sul ripristino visualizza informazioni sull'errore. |
| Rapporto di protezione | Questi report forniscono dettagli sulla protezione per le risorse gestite da tutte le istanze del plug-in SnapCenter . Questo report fornisce dettagli sulla protezione per le risorse gestite da tutte le istanze del plug-in. È possibile visualizzare una panoramica, i dettagli delle risorse non protette, le risorse di cui non è stato eseguito il backup al momento della generazione del report, le risorse di un gruppo di risorse per cui le operazioni di backup non sono riuscite e lo stato SnapVault . |

| Tipo di rapporto | Descrizione |
| --- | --- |
| Rapporto programmato | Questi report sono programmati per essere eseguiti periodicamente, ad esempio quotidianamente, settimanalmente o mensilmente. I report vengono generati automaticamente nella data e nell'ora specificate e inviati alle persone interessate tramite e-mail. È possibile abilitare, disabilitare, modificare o eliminare le pianificazioni. La pianificazione abilitata può essere eseguita su richiesta cliccando sul pulsante **Esegui ora**. L'amministratore può eseguire qualsiasi pianificazione, ma il report generato conterrà dati basati sull'autorizzazione fornita dall'utente che ha creato la pianificazione.<br><br>Qualsiasi altro utente diverso dall'amministratore potrà visualizzare o modificare la pianificazione in base alla propria autorizzazione. Se nella pagina Aggiungi ruolo è selezionata l'opzione Tutti i membri di questo ruolo possono vedere gli oggetti degli altri membri, gli altri membri del ruolo potranno visualizzare e modificare. |

## Rapporti di accesso

Puoi utilizzare la dashboard SnapCenter per ottenere una rapida panoramica dello stato di salute del tuo sistema. Dalla Dashboard è possibile approfondire i dettagli. In alternativa, è possibile accedere direttamente ai report dettagliati.

È possibile accedere ai report tramite uno dei seguenti metodi:

- Nel riquadro di navigazione a sinistra, fare clic su **Dashboard**, quindi sul grafico a torta **Riepilogo ultima protezione** per visualizzare maggiori dettagli nella pagina Report.
- Nel riquadro di navigazione a sinistra, fare clic su **Report**.

## Filtra il tuo report

Potresti voler filtrare i dati del tuo report in base a una serie di parametri, a seconda del livello di dettaglio e dell'intervallo di tempo delle informazioni richieste.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Report**.
2. Se la vista Parametri non è visualizzata, fare clic sull'icona **Attiva/disattiva area parametri** nella barra degli strumenti del report.
3. Specificare l'intervallo di tempo per il quale si desidera eseguire il report. + Se si omette la data di fine, si recuperano tutte le informazioni disponibili.
4. Filtra le informazioni del tuo report in base a uno qualsiasi dei seguenti criteri:
    - Gruppo di risorse
    - Ospite

- Politica
- Risorsa
- Stato
- Nome del plug-in

5. Fare clic su **Applica**.

## Esportare o stampare report

L'esportazione dei report SnapCenter consente di visualizzare il report in vari formati alternativi. È anche possibile stampare i report.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Report**.
2. Dalla barra degli strumenti dei report, eseguire una delle seguenti operazioni:
   - Fare clic sull'icona **Attiva/disattiva anteprima di stampa** per visualizzare l'anteprima di un report stampabile.
   - Selezionare un formato dall'elenco a discesa dell'icona **Esporta** per esportare un report in un formato alternativo.
3. Per stampare un report, fare clic sull'icona **Stampa**.
4. Per visualizzare il riepilogo di un report specifico, scorrere fino alla sezione appropriata del report.

## Imposta il server SMTP per le notifiche e-mail

È possibile specificare il server SMTP da utilizzare per inviare report sui processi di protezione dei dati a se stessi o ad altri. Puoi anche inviare un'e-mail di prova per verificare la configurazione. Le impostazioni vengono applicate globalmente a qualsiasi processo SnapCenter per il quale si configura la notifica e-mail.

Questa opzione configura il server SMTP per l'invio di tutti i report sui processi di protezione dei dati. Tuttavia, se si desidera ricevere regolarmente gli aggiornamenti dei processi di protezione dei dati SnapCenter per una determinata risorsa, in modo da poter monitorare lo stato di tali aggiornamenti, è possibile configurare l'opzione per inviare tramite e-mail i report SnapCenter quando si crea un gruppo di risorse.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Inserisci il server SMTP e fai clic su **Salva**.
4. Per inviare un'e-mail di prova, inserisci l'indirizzo e-mail da e a cui vuoi inviare l'e-mail, inserisci l'oggetto e fai clic su **Invia**.

## Configurare l'opzione per inviare i report via e-mail

Se desideri ricevere regolarmente aggiornamenti sui processi di protezione dei dati SnapCenter , a te stesso o ad altri, in modo da poter monitorare lo stato di tali aggiornamenti, puoi configurare l'opzione per inviare tramite e-mail i report SnapCenter quando crei un gruppo di risorse.

**Prima di iniziare**

Devi aver configurato il tuo server SMTP nella pagina Impostazioni globali in Impostazioni.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Risorse**, quindi selezionare il plug-in appropriato dall'elenco.
2. Seleziona il tipo di risorsa che desideri visualizzare e fai clic su **Nuovo gruppo di risorse**, oppure seleziona un gruppo di risorse esistente e fai clic su **Modifica** per configurare i report via e-mail per un gruppo di risorse esistente.
3. Nel pannello Notifiche della procedura guidata Nuovo gruppo di risorse, seleziona dal menu a discesa se desideri ricevere i report sempre, in caso di errore, in caso di errore o avviso.
4. Inserisci l'indirizzo da cui viene inviata l'e-mail, l'indirizzo a cui viene inviata l'e-mail e l'oggetto dell'e-mail.

# Gestire il repository di SnapCenter Server

Le informazioni relative alle varie operazioni eseguite da SnapCenter vengono archiviate nel repository del database di SnapCenter Server. È necessario creare backup del repository per proteggere SnapCenter Server dalla perdita di dati.

Il repository di SnapCenter Server è talvolta denominato database NSM.

## Prerequisiti per la protezione del repository SnapCenter

Per proteggere il repository SnapCenter , l'ambiente deve soddisfare determinati prerequisiti.

- Gestione delle connessioni della macchina virtuale di archiviazione (SVM)

  Dovresti configurare le credenziali di archiviazione.

- Provisioning degli host

  Almeno un disco di archiviazione NetApp deve essere presente sull'host del repository SnapCenter . Se un disco NetApp non è presente sull'host del repository SnapCenter , è necessario crearne uno.

  Per informazioni dettagliate sull'aggiunta di host, sulla configurazione delle connessioni SVM e sul provisioning degli host, consultare le istruzioni di installazione.

- Provisioning di iSCSI LUN o VMDK

  Per una configurazione ad alta disponibilità (HA), è possibile predisporre un LUN iSCSI o un VMDK in uno dei server SnapCenter .

## Eseguire il backup del repository SnapCenter

Il backup del repository di SnapCenter Server aiuta a proteggerlo dalla perdita di dati. È possibile eseguire il backup del repository eseguendo il cmdlet *Protect-SmRepository*.

**Informazioni su questo compito**

Il cmdlet *Protect-SmRepository* esegue le seguenti attività:

- Crea un gruppo di risorse e una policy
- Crea una pianificazione di backup per il repository SnapCenter

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , stabilire una sessione utilizzando il cmdlet *Open-SmConnection*, quindi immettere le credenziali.
3. Eseguire il backup del repository utilizzando il cmdlet *Protect-SmRepository* e i parametri richiesti.

## Visualizza i backup del repository SnapCenter

È possibile visualizzare un elenco dei backup del repository del database di SnapCenter Server eseguendo il cmdlet *Get-SmRepositoryBackups*.

I backup del repository vengono creati in base alla pianificazione specificata nel cmdlet *Protect-SmRepository*.

**Passi**

1. Avvia PowerShell.
2. Dal prompt dei comandi, immettere il seguente cmdlet e quindi fornire le credenziali per connettersi al server SnapCenter : *Open-SMConnection*
3. Elenca tutti i backup del database SnapCenter disponibili utilizzando il cmdlet *Get-SmRepositoryBackups*.

## Ripristinare il repository del database SnapCenter

È possibile ripristinare il repository SnapCenter eseguendo il cmdlet *Restore-SmRepositoryBackup*.

Quando si ripristina il repository SnapCenter , altre operazioni SnapCenter in esecuzione saranno interessate perché durante l'operazione di ripristino il database del repository non è accessibile.

**Passi**

1. Avvia PowerShell.
2. Dal prompt dei comandi, immettere il seguente cmdlet e quindi fornire le credenziali per connettersi al server SnapCenter : *Open-SMConnection*
3. Ripristinare il backup del repository utilizzando il cmdlet *Restore-SmRepositoryBackup*.

   Il seguente cmdlet ripristina il repository del database MySQL di SnapCenter dai backup esistenti su iSCSI LUN o VMDK:

   ```
   C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-x3550-s09_09-15-2016_10.32.00.4445
   ```

   Il seguente cmdlet ripristina il database MySQL di SnapCenter quando i file di backup vengono eliminati accidentalmente nella LUN iSCSI. Per VMDK ripristinare manualmente il backup dagli snapshot ONTAP .

```
C:\PS>Restore-SmRepositoryBackup -BackupName MYSQL_DS_SC_Repository_mva-
x3550-s09_09-15-2016_10.32.00.4445 -RestoreFileSystem
```

Il backup utilizzato per eseguire l'operazione di ripristino del repository non verrà elencato quando i backup del repository verranno recuperati dopo aver eseguito l'operazione di ripristino.

## Migrare il repository SnapCenter

È possibile migrare il repository del database di SnapCenter Server dalla posizione predefinita a un altro disco. È possibile migrare il repository quando si desidera spostarlo su un disco con più spazio.

**Passi**

1. Arrestare il servizio MYSQL57 in Windows.
2. Individuare la directory dei dati MySQL.

   Di solito la directory dei dati si trova in C:\ProgramData\MySQL\MySQL Server 5.7\Data.
3. Copiare la directory dei dati MySQL nella nuova posizione, ad esempio E:\Data\nsm.
4. Fare clic con il pulsante destro del mouse sulla nuova directory, quindi selezionare **Proprietà** > **Sicurezza** per aggiungere l'account del server locale del servizio di rete alla nuova directory, quindi assegnare all'account il controllo completo.
5. Rinominare la directory del database originale, ad esempio nsm_copy.
6. Da un prompt dei comandi di Windows, creare un collegamento simbolico alla directory utilizzando il comando *mklink*.

   ```
   "mklink /d "C:\ProgramData\MySQL\MySQL Server 5.7\Data\nsm" "E:\Data\nsm" "
   ```
7. Avviare il servizio MYSQL57 in Windows.
8. Verificare che la modifica della posizione del database sia avvenuta correttamente accedendo a SnapCenter e controllando le voci del repository oppure accedendo all'utilità MySQL e connettendosi al nuovo repository.
9. Eliminare la directory originale del repository del database rinominata (nsm_copy).

## Reimposta la password del repository SnapCenter

La password del database del repository di MySQL Server viene generata automaticamente durante l'installazione di SnapCenter Server da SnapCenter 4.2. Questa password generata automaticamente non è mai nota all'utente SnapCenter . Se si desidera accedere al database del repository, è necessario reimpostare la password.

**Prima di iniziare**

Per reimpostare la password è necessario disporre dei privilegi di amministratore SnapCenter .

**Passi**

1. Avvia PowerShell.
2. Dal prompt dei comandi, immettere il comando seguente e quindi fornire le credenziali per connettersi al

server SnapCenter : *Open-SMConnection*

3. Reimposta la password del repository: *Set-SmRepositoryPassword*

   Il seguente comando reimposta la password del repository:

```
Set-SmRepositoryPassword at command pipeline position 1
Supply values for the following parameters:
NewPassword: ********
ConfirmPassword: ********
Successfully updated the MySQL server password.
```

**Informazioni correlate**

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

# Gestire le risorse dei domini non attendibili

Oltre a gestire gli host nei domini attendibili di Active Directory (AD), SnapCenter gestisce anche gli host in più domini non attendibili di AD. I domini AD non attendibili devono essere registrati con SnapCenter Server. SnapCenter supporta utenti e gruppi di più domini AD non attendibili.

È possibile installare SnapCenter Server su una macchina appartenente a un dominio o a un gruppo di lavoro. Per installare SnapCenter Server, è necessario specificare le credenziali di dominio se la macchina si trova in un dominio oppure le credenziali di amministratore locale se la macchina si trova in un gruppo di lavoro.

I gruppi di Active Directory (AD) che appartengono a domini non registrati con SnapCenter Server non sono supportati. Sebbene sia possibile creare ruoli SnapCenter con questi gruppi AD, l'accesso a SnapCenter Server non riesce e viene visualizzato il seguente messaggio di errore: L'utente a cui si sta tentando di accedere non appartiene ad alcun ruolo. Contatta l'amministratore.

## Modificare i domini non attendibili

È possibile modificare un dominio non attendibile quando si desidera aggiornare gli indirizzi IP del controller di dominio o il nome di dominio completo (FQDN).

**Informazioni su questo compito**

Dopo aver modificato l'FQDN, le risorse associate (host, utenti e gruppi) potrebbero non funzionare come previsto.

Per modificare un dominio non attendibile, è possibile utilizzare l'interfaccia utente SnapCenter o i cmdlet di PowerShell.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.

3. Nella pagina Impostazioni globali, fare clic su **Impostazioni dominio**.
4. Clic e quindi fornire i seguenti dettagli:

| Per questo campo… | Fai questo… |
| --- | --- |
| FQDN del dominio | Specificare il nome di dominio completo (FQDN) e fare clic su **Risolvi**. |
| Indirizzi IP del controller di dominio | Se il nome di dominio completo (FQDN) non è risolvibile, specificare uno o più indirizzi IP del controller di dominio. |

5. Fare clic su **OK**.

## Annullare la registrazione dei domini Active Directory non attendibili

È possibile annullare la registrazione di un dominio Active Directory non attendibile se non si desidera utilizzare le risorse associate a tale dominio.

**Prima di iniziare**

Avresti dovuto rimuovere gli host, gli utenti, i gruppi e le credenziali associati al dominio non attendibile.

**Informazioni su questo compito**

- Dopo aver annullato la registrazione del dominio da SnapCenter Server, gli utenti di quel dominio non potranno più accedere a SnapCenter Server.
- Se sono presenti risorse associate (host, utenti e gruppi), dopo aver annullato la registrazione del dominio, le risorse non saranno operative.
- Per annullare la registrazione di un dominio non attendibile, è possibile utilizzare l'interfaccia utente SnapCenter o i cmdlet di PowerShell.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina Impostazioni, fare clic su **Impostazioni globali**.
3. Nella pagina Impostazioni globali, fare clic su **Impostazioni dominio**.
4. Dall'elenco dei domini, seleziona il dominio che desideri annullare la registrazione.
5. Clic e quindi fare clic su **OK**.

# Gestire il sistema di archiviazione

Dopo aver aggiunto il sistema di archiviazione, è possibile modificarne la configurazione e le connessioni oppure eliminarlo.

## Modificare la configurazione del sistema di archiviazione

È possibile utilizzare SnapCenter per modificare la configurazione del sistema di archiviazione se si desidera

cambiare il nome utente, la password, la piattaforma, la porta, il protocollo, il periodo di timeout, l'indirizzo IP preferito o le opzioni di messaggistica.

**Informazioni su questo compito**

È possibile modificare le connessioni di archiviazione per un singolo utente o per un gruppo. Se si appartiene a uno o più gruppi con autorizzazione per lo stesso sistema di archiviazione, il nome della connessione di archiviazione viene visualizzato più volte nell'elenco delle connessioni di archiviazione, una volta per ciascun gruppo con autorizzazione per il sistema di archiviazione.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, eseguire una delle seguenti azioni:

| Selezionare… | Passi… |
| --- | --- |
| SVM ONTAP | Per visualizzare tutte le macchine virtuali di archiviazione (SVM) aggiunte e per modificare la configurazione SVM richiesta.<br><br>a. Nella pagina Connessioni di archiviazione, fare clic sul nome SVM appropriato.<br>b. Eseguire una delle seguenti azioni:<br><br>◦ Se l'SVM non fa parte di alcun cluster, nella pagina Modifica sistema di archiviazione, modificare le configurazioni quali nome utente, password, impostazioni EMS e AutoSupport , piattaforma, protocollo, porta, timeout e IP preferito.<br>◦ Se l'SVM fa parte di un cluster, nella pagina Modifica sistema di archiviazione, seleziona **Gestisci SVM in modo indipendente** e modifica le configurazioni quali nome utente, password, impostazioni EMS e AutoSupport , piattaforma, protocollo, porta, timeout e IP preferito.<br><br>Dopo aver modificato l'SVM in modo che venga gestito in modo indipendente, se si decide di gestirlo tramite cluster, è necessario eliminare l'SVM e quindi fare clic su **Riscopri**. L'SVM verrà aggiunto al cluster ONTAP .<br><br>Quando la password di un sistema di archiviazione viene aggiornata nell'interfaccia utente grafica SnapCenter , è necessario riavviare i servizi SMCore del rispettivo plug-in o dell'host del server, poiché la password aggiornata non viene visualizzata in SMCore e i processi di backup non riusciranno con un errore di credenziale errata. |

| Selezionare… | Passi… |
| --- | --- |
| Cluster ONTAP | Per visualizzare tutti i cluster aggiunti e modificare la configurazione del cluster richiesta.<br>a. Nella pagina Connessioni di archiviazione, fare clic sul nome del cluster.<br>b. Nella pagina Modifica sistema di archiviazione, fare clic sull'icona di modifica accanto a Nome utente e modificare il nome utente e la password.<br>c. Selezionare o deselezionare le impostazioni EMS e AutoSupport .<br>d. Fare clic su **Altre opzioni** e modificare altre configurazioni quali piattaforma, protocollo, porta, timeout e IP preferito. |

3. Fare clic su **Invia**.

## Elimina il sistema di archiviazione

È possibile utilizzare SnapCenter per eliminare qualsiasi sistema di archiviazione inutilizzato.

### Informazioni su questo compito

È possibile eliminare le connessioni di archiviazione per un singolo utente o per un gruppo. Se si appartiene a uno o più gruppi con autorizzazione per lo stesso sistema di archiviazione, il nome del sistema di archiviazione viene visualizzato più volte nell'elenco delle connessioni di archiviazione, una volta per ciascun gruppo con autorizzazione per il sistema di archiviazione.

Quando si elimina un sistema di archiviazione, tutte le operazioni eseguite su tale sistema di archiviazione falliranno.

### Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Sistemi di archiviazione**.
2. Nella pagina Sistemi di archiviazione, dal menu a discesa **Tipo**, selezionare * ONTAP SVM* o * ONTAP Cluster*.
3. Nella pagina Connessioni di archiviazione, seleziona la casella di controllo accanto all'SVM o al cluster che desideri eliminare.

   Non è possibile selezionare l'SVM che fa parte di un cluster.

4. Fare clic su **Elimina**.
5. Nella pagina Elimina impostazioni di connessione al sistema di archiviazione, fare clic su **OK**.

   Se un SVM viene eliminato dal cluster ONTAP tramite l'interfaccia utente grafica ONTAP , nell'interfaccia utente grafica SnapCenter fare clic su **Riscopri** per aggiornare l'elenco SVM.

## Supporto API REST

Per impostazione predefinita, tutte le connessioni dei sistemi ASA, AFF o FAS a ONTAP passeranno tramite ZAPI. L'API REST può essere abilitata per versioni specifiche ONTAP .

SnapCenter sfrutta le API REST per eseguire tutte le operazioni sui sistemi ASA r2, che non supportano le ZAPI.

È possibile modificare le chiavi di configurazione nei seguenti file di configurazione:

- IsRestEnabledForStorageConnection

  Il valore predefinito è falso.

- MinOntapVersionToUseREST

  Il valore predefinito è 9.13.1.

#### Abilita la connessione tramite REST API

1. Impostare IsRestEnabledForStorageConnection su true.
2. Aggiungere la chiave in SMCoreServiceHost.dll.config e SnapDriveService.dll.config sia sul server che sugli host plug-in di Windows.

   *<aggiungi chiave="IsRestEnabledForStorageConnection" valore="true" />*

#### Limita la connessione tramite REST API a una versione specifica di ONTAP

1. Impostare il parametro di configurazione MinOntapVersionToUseREST su true.
2. Aggiungere la chiave in SMCoreServiceHost.dll.config e SnapDriveService.dll.config sia sul server che sugli host plug-in di Windows.

   *<aggiungi chiave="MinOntapVersionToUseREST" valore="9.13.1" />*

3. Riavviare il servizio per SmCore sul server e il servizio plug-in e SnapDrive sulla macchina plug-in.

# Gestire la raccolta dati EMS

È possibile pianificare e gestire la raccolta dati dell'Event Management System (EMS) utilizzando i cmdlet di PowerShell. La raccolta dati EMS comporta la raccolta di dettagli su SnapCenter Server, sui pacchetti plug-in SnapCenter installati, sugli host e informazioni simili, per poi inviarli a una macchina virtuale di archiviazione ONTAP (SVM) specificata.

L'utilizzo della CPU del sistema è elevato quando è in corso un'attività di raccolta dati. L'utilizzo della CPU rimane elevato finché l'operazione è in corso, indipendentemente dalle dimensioni dei dati.

## Interrompere la raccolta dati EMS

La raccolta dati EMS è abilitata per impostazione predefinita e viene eseguita ogni sette giorni dopo la data di installazione. È possibile disabilitare la raccolta dati in qualsiasi momento utilizzando il cmdlet di PowerShell

*Disable-SmDataCollectionEMS*.

**Passi**

1. Da una riga di comando di PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Disattivare la raccolta dati EMS immettendo *Disable-SmDataCollectionEms*.

## Avvia la raccolta dati EMS

La raccolta dati EMS è abilitata per impostazione predefinita e l'esecuzione è programmata ogni sette giorni a partire dalla data di installazione. Se lo hai disabilitato, puoi riavviare la raccolta dati EMS utilizzando il cmdlet *Enable-SmDataCollectionEMS*.

All'utente della macchina virtuale di archiviazione (SVM) è stata concessa l'autorizzazione generate-autosupport-log per l'evento NetApp ONTAP .

**Passi**

1. Da una riga di comando di PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Abilita la raccolta dati EMS immettendo *Enable-SmDataCollectionEMS*.

## Modificare il programma di raccolta dati EMS e l'SVM di destinazione

È possibile utilizzare i cmdlet di PowerShell per modificare la pianificazione della raccolta dati EMS o la macchina virtuale di archiviazione di destinazione (SVM).

**Passi**

1. Da una riga di comando di PowerShell, per stabilire una sessione con SnapCenter, immettere il cmdlet *Open-SmConnection*.
2. Per modificare la destinazione della raccolta dati EMS, immettere il cmdlet *Set-SmDataCollectionEmsTarget*.
3. Per modificare la pianificazione della raccolta dati EMS, immettere il cmdlet *Set-SmDataCollectionEmsSchedule*.

## Monitorare lo stato della raccolta dati EMS

È possibile monitorare lo stato della raccolta dati EMS utilizzando diversi cmdlet di PowerShell. È possibile ottenere informazioni sulla pianificazione, sulla destinazione della macchina virtuale di archiviazione (SVM) e sullo stato.

**Passi**

1. Da una riga di comando di PowerShell, stabilire una sessione con SnapCenter immettendo *Open-SmConnection*.
2. Recuperare informazioni sulla pianificazione della raccolta dati EMS immettendo *Get-SmDataCollectionEmsSchedule*.
3. Recupera informazioni sullo stato della raccolta dati EMS immettendo *Get-SmDataCollectionEmsStatus*.
4. Recuperare informazioni sulla destinazione della raccolta dati EMS immettendo *Get-SmDataCollectionEmsTarget*.

**Informazioni correlate**

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

# Aggiorna SnapCenter Server e i plug-in

## Configura SnapCenter per verificare la disponibilità di aggiornamenti

SnapCenter comunica periodicamente con il sito di supporto NetApp per informarti sulla disponibilità di aggiornamenti software. È anche possibile creare una pianificazione per specificare l'intervallo in cui si desidera ricevere informazioni sugli aggiornamenti disponibili.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Impostazioni**.
2. Nella pagina **Impostazioni**, fare clic su **Software**.

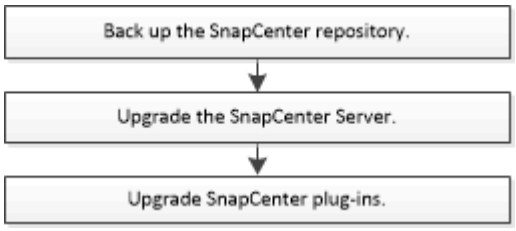
   La pagina Software disponibile mostra i pacchetti plug-in disponibili, le versioni disponibili e il loro stato di installazione.

3. Fare clic su **Controlla aggiornamenti** per verificare se sono disponibili versioni più recenti dei pacchetti plug-in.
4. Fare clic su **Pianifica aggiornamenti** per creare una pianificazione e specificare l'intervallo in cui si desidera ricevere informazioni sugli aggiornamenti disponibili:
   a. Selezionare l'intervallo in **Verifica aggiornamenti**.
   b. Selezionare le credenziali Windows di SnapCenter Server Admin e fare clic su **OK**.

# Flusso di lavoro di aggiornamento

Ogni versione di SnapCenter contiene un server SnapCenter aggiornato e un pacchetto plug-in. Gli aggiornamenti dei pacchetti plug-in vengono distribuiti con il programma di installazione SnapCenter . È possibile configurare SnapCenter per verificare la disponibilità di aggiornamenti.

Il flusso di lavoro mostra le diverse attività necessarie per aggiornare SnapCenter Server e i pacchetti Plug-in.




### Percorsi di aggiornamento supportati

Il percorso di aggiornamento ti aiuta a capire da quali versioni precedenti di SnapCenter puoi effettuare l'aggiornamento alle versioni più recenti di SnapCenter e quali versioni dei plug-in sono supportate.

| Se utilizzi la versione SnapCenter Server… | È possibile aggiornare direttamente SnapCenter Server a… | Versioni di plug-in supportate |
|---|---|---|
| 5,0 | 6,0 | • 5,0<br>• 6,0 |
| | 6.0.1 | • 6.0.1 |
| | 6,1 | • 6,1 |
| 6,0 | 6.0.1 | • 6,0<br>• 6.0.1 |
| | 6,1 | • 6,1 |
| 6.0.1 | 6,1 | • 6.0.1<br>• 6,1 |

Per informazioni sull'aggiornamento del SnapCenter Plug-in for VMware vSphere, vedere "Aggiorna il SnapCenter Plug-in for VMware vSphere" .

# Aggiornare il server SnapCenter sull'host Windows

È necessario aggiornare SnapCenter Server per accedere alle funzionalità e ai miglioramenti più recenti forniti nella versione più recente.

**Prima di iniziare**

- Aggiornare l'host del server SnapCenter con gli ultimi aggiornamenti di Windows e assicurarsi che non vi siano riavvii del sistema in sospeso.
- Prima di avviare l'aggiornamento, assicurarsi che non siano in esecuzione altre operazioni.
- Installare ASP.NET Core Runtime 8.0.12 (e tutte le patch 8.0.x successive) Hosting Bundle e PowerShell 7.4.2 o versione successiva.
- Eseguire il backup del database del repository SnapCenter (MySQL) dopo essersi assicurati che non vi siano processi in esecuzione. Si consiglia di effettuare questa operazione prima di aggiornare SnapCenter Server e il plug-in di Exchange.

  Per informazioni, vedere"Eseguire il backup del repository SnapCenter" .

- Eseguire il backup di tutti i file di configurazione SnapCenter modificati sull'host del server SnapCenter o sull'host del plug-in.

  Esempi di file di configurazione SnapCenter : SnapDriveService.exe.config, SMCoreServiceHost.exe.config e così via.

- Se hai installato più versioni del plug-in personalizzato in SnapCenter 5.0, prima di eseguire l'aggiornamento alla versione 6.0 o successiva, dovresti eseguire i cmdlet di PowerShell per rimuovere tutte le versioni precedenti del plug-in personalizzato (tranne quella più recente) dal repository SnapCenter

(database NSM).

- Correre `Open-SmConnection` e accedi utilizzando le credenziali del ruolo SnapCenterAdmin
- Correre `Remove-SmPluginPackage -PluginName M<plug-in name> -PluginVersion <version number>`

  Per ulteriori informazioni, consulta "L'aggiornamento a SnapCenter 6.0 o versione successiva non riesce" .

**Informazioni su questo compito**

- Durante l'aggiornamento, SnapCenter esegue uno script SQL per aggiornare i dati di Exchange nel database NSM, convertendo il DAG e il nome abbreviato dell'host in FQDN. Ciò si applica solo se si utilizza SnapCenter Server con il plug-in Exchange.
- Se hai messo manualmente l'host del server in modalità di manutenzione, dopo l'aggiornamento seleziona **Host** > **Attiva pianificazione** per far uscire l'host del server dalla modalità di manutenzione.
- Per le pianificazioni di backup e verifica esistenti con prescript e postscript abilitati nella policy, le operazioni di backup continueranno a funzionare dopo l'aggiornamento.

  Nella pagina **Dettagli lavoro**, un messaggio di avviso consiglia al cliente di copiare gli script in SCRIPTS_PATH e di modificare la policy per fornire un percorso relativo a SCRIPTS_PATH. Per il processo del ciclo di vita del clone, il messaggio di avviso viene visualizzato a livello di sottoprocesso.

**Passi**

1. Scaricare il pacchetto di installazione di SnapCenter Server dal sito di supporto NetApp .

   https://mysupport.netapp.com/site/products/all/details/snapcenter/downloads-tab

2. Creare una copia del file web.config che si trova in C:\Programmi\ NetApp\ SnapCenter WebApp.
3. Esportare le pianificazioni host del plug-in SnapCenter dall'Utilità di pianificazione di Windows per ripristinarle se l'aggiornamento non riesce.

   ```
   md d:\\SCBackup``schtasks /query /xml /TN taskname >>
   "D:\SCBackup\taskname.xml"
   ```

4. Creare il dump del database MySQL di SnapCenter se il backup del repository non è configurato.

   ```
   md d:\\SCBackup``mysqldump --all-databases --single-transaction --add-drop
   -database --triggers --routines --events -u root -p >
   D:\SCBackup\SCRepoBackup.dmp
   ```

   Quando richiesto, inserisci la password.

5. Fare doppio clic sul file .exe scaricato per avviare l'aggiornamento di SnapCenter Server.

   Dopo aver avviato l'aggiornamento, SnapCenter esegue dei controlli preliminari. Se il sistema non soddisfa i requisiti minimi, SnapCenter mostra messaggi di errore o di avviso. È possibile ignorare gli avvisi e continuare con l'installazione, ma è necessario correggere eventuali errori.

   SnapCenter continua a utilizzare la password del database del repository MySQL Server esistente fornita durante l'installazione della versione precedente di SnapCenter Server.

6. Seleziona **Aggiorna**.

   Se in qualsiasi momento selezioni **Annulla**, SnapCenter interrompe l'aggiornamento. Non ripristinerà lo stato precedente di SnapCenter Server.

   **Procedura consigliata:** disconnettersi e riconnettersi oppure aprire un nuovo browser per accedere all'interfaccia utente SnapCenter .

**Dopo aver finito**

- Se il plug-in viene installato tramite un utente sudo, è necessario copiare le chiavi sha224 disponibili in *C:\ProgramData\ NetApp\ SnapCenter\Package Repository\sc_unix_plugins_checksum.txt* per aggiornare il file */etc/sudoers*.
- Dovresti eseguire una nuova individuazione delle risorse sull'host del server.

  Se SnapCenter visualizza lo stato dell'host del server come arrestato, attendere qualche istante ed eseguire una nuova individuazione. È anche possibile modificare il valore del parametro **HostRefreshInterval** (il valore predefinito è 3600 secondi) impostandolo su un valore superiore a 10 minuti.

- Se l'aggiornamento non riesce, pulire l'installazione non riuscita, reinstallare la versione precedente di SnapCenter e ripristinare il database NSM allo stato in cui si trovava prima.
- Dopo aver aggiornato l'host del server, è necessario aggiornare anche i plug-in prima di aggiungere qualsiasi sistema di archiviazione.

# Aggiornare il server SnapCenter sull'host Linux

È possibile utilizzare il file di installazione di SnapCenter Server per aggiornare SnapCenter Server.

**Passi**

1. Eseguire una delle azioni per aggiornare SnapCenter Server.

| Se vuoi esibirti… | Fai questo… |
| --- | --- |
| Aggiornamento non interattivo | `sudo ./snapcenter-linux-server-(el8/el9/sles15).bin -i silent -DUPGRADE=<value> -DINSTALL_LOG_NAME=<filename>`<br><br>Esempio: sudo ./snapcenter_linux_server.bin -i silent -DUPGRADE=1 -DINSTALL_LOG_NAME=InstallerLog.log<br><br>I registri verranno archiviati in */var/opt/snapcenter/logs*.<br><br>Parametri da passare per l'aggiornamento:<br><br>• DINSTALL_LOG_NAME: Nome del file di registro in cui verranno archiviati i registri di installazione.<br>• DUPGRADE: Il valore predefinito è 0. Specificare questo parametro e il suo valore come un numero intero diverso da 0 per aggiornare SnapCenter Server. |
| Installazione interattiva | `./snapcenter-linux-server-(el8/el9/sles15).bin`<br><br>Ti verrà chiesto di confermare l'aggiornamento. Immettere un valore diverso da 0 per confermare l'aggiornamento di SnapCenter Server. |

Dovresti disconnetterti e poi accedere a SnapCenter oppure chiudere e poi aprire un nuovo browser per accedere all'interfaccia utente grafica SnapCenter .

# Aggiorna i tuoi pacchetti plug-in

I pacchetti plug-in vengono distribuiti come parte dell'aggiornamento SnapCenter .

Non è necessario mettere manualmente in modalità di manutenzione ogni host plug-in che si desidera aggiornare, perché la procedura di aggiornamento mette in modalità di manutenzione gli host plug-in Windows, Linux o AIX. La modalità di manutenzione impedisce l'esecuzione di attività pianificate sull'host del plug-in durante l'aggiornamento.

**Prima di iniziare**

- Se sei un utente non root con accesso alle macchine Linux, dovresti aggiornare il file */etc/sudoers* con i valori di checksum più recenti prima di eseguire l'operazione di aggiornamento.
- Per impostazione predefinita, SnapCenter rileva JAVA_HOME dall'ambiente. Se si desidera utilizzare un JAVA_HOME fisso e si stanno aggiornando i plug-in su un host Linux, è necessario aggiungere manualmente il parametro SKIP_JAVAHOME_UPDATE nel file *spl.properties* che si trova in */var/opt/snapcenter/spl/etc/* e impostare il valore su TRUE.

Il valore di JAVA_HOME viene aggiornato quando il plug-in viene aggiornato o quando il servizio SnapCenter Plug-in Loader (SPL) viene riavviato. Prima di aggiornare o riavviare l'SPL, se si aggiunge il parametro SKIP_JAVAHOME_UPDATE e si imposta il valore su TRUE, il valore di JAVA_HOME non viene aggiornato.

- Dovresti aver eseguito il backup di tutti i file di configurazione SnapCenter che hai modificato sull'host del server SnapCenter o sull'host del plug-in.

  Esempi di file di configurazione SnapCenter : SnapDriveService.exe.config, SMCoreServiceHost.exe.config e così via.

**Informazioni su questo compito**

- Per SnapCenter Plug-in per Microsoft SQL Server, SnapCenter Plug-in per Microsoft Exchange Server e SnapCenter Plug-in per Microsoft Windows, si consiglia di aggiornare sia il server che gli host del plug-in alla versione più recente affinché SCRIPTS_PATH possa essere eseguito.

  Per le pianificazioni di backup e verifica esistenti con prescript e postscript abilitati nella policy, le operazioni di backup continueranno a funzionare dopo l'aggiornamento.

  Nella pagina **Dettagli lavoro**, un messaggio di avviso consiglia al cliente di copiare gli script in SCRIPTS_PATH e di modificare la policy per fornire un percorso relativo a SCRIPTS_PATH. Per il processo del ciclo di vita del clone, il messaggio di avviso viene visualizzato a livello di sottoprocesso.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host** > **Host gestiti**.
2. Aggiornare gli host eseguendo una delle seguenti attività:
   - Se nella colonna Stato generale viene visualizzato "Aggiornamento disponibile" per uno degli host del plug-in, fare clic sul nome dell'host del plug-in ed eseguire le seguenti operazioni:
     i. Fare clic su **Altre opzioni**.
     ii. Selezionare **Salta controlli preliminari** se non si desidera verificare se l'host del plug-in soddisfa i requisiti per aggiornare il plug-in.
     iii. Fare clic su **Aggiorna**.
   - Se si desidera aggiornare più host, selezionare tutti gli host, fare clic su , quindi fare clic su **Aggiorna** > **OK**.

     Durante l'aggiornamento del plug-in, tutti i servizi correlati vengono riavviati.

     Vengono selezionati tutti i plug-in nel pacchetto, ma vengono aggiornati solo i plug-in installati con la versione precedente di SnapCenter , mentre i plug-in rimanenti non vengono installati. Per installare un nuovo plug-in è necessario utilizzare l'opzione **Aggiungi plug-in**.

     Se non hai selezionato la casella di controllo **Salta controlli preliminari**, l'host del plug-in viene convalidato per verificare se soddisfa i requisiti per l'installazione del plug-in. Se i requisiti minimi non vengono soddisfatti, vengono visualizzati messaggi di errore o di avviso appropriati. Dopo aver risolto il problema, fare clic su **Aggiorna**.

Se l’errore è correlato allo spazio su disco o alla RAM, è possibile aggiornare il file web.config situato in C:\Programmi\ NetApp\ SnapCenter WebApp oppure i file di configurazione di PowerShell situati in C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ SnapCenter\ per modificare i valori predefiniti. Se l’errore è correlato ai parametri rimanenti, è necessario risolvere il problema e quindi convalidare nuovamente i requisiti.

# Aggiornamento tecnologico

## Aggiornamento tecnologico dell'host del server SnapCenter

Quando è necessario aggiornare l'host di SnapCenter Server, è possibile installare la stessa versione di SnapCenter Server sul nuovo host e quindi eseguire le API per eseguire il backup di SnapCenter dal vecchio server e ripristinarlo sul nuovo server.

**Passi**

1. Distribuisci il nuovo host ed esegui le seguenti attività:
   a. Installare la stessa versione di SnapCenter Server.
   b. (Facoltativo) Configurare i certificati CA e abilitare SSL bidirezionale. Per maggiori informazioni, fare riferimento a "Configurare il certificato CA" E "Configurare e abilitare SSL bidirezionale" .
   c. (Facoltativo) Configurare l'autenticazione a più fattori. Per ulteriori informazioni, consulta "Abilita l'autenticazione a più fattori" .
2. Accedi come utente amministratore SnapCenter .
3. Creare un backup del server SnapCenter sul vecchio host utilizzando l'API: `/<snapcenter_version>/server/backup` oppure il cmdlet: *New-SmServerBackup*.

   Prima di eseguire il backup, sospendere tutti i processi pianificati e assicurarsi che non vi siano processi in esecuzione.

   Se si desidera ripristinare il backup sul server SnapCenter in esecuzione su un nuovo dominio, prima di eseguire un backup è necessario aggiungere il nuovo utente del dominio nel vecchio host SnapCenter e assegnare il ruolo di amministratore SnapCenter .
4. Copia il backup dal vecchio host al nuovo host.
5. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: `/<snapcenter_version>/server/restore` oppure il cmdlet: *Restore-SmServerBackup*.

   Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera saltare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server eseguendo l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

   Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <Nuovo IP> SC_Server_Name.

   Le voci *etc/host* del server non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

   Se il backup viene ripristinato sul server SnpCenter in esecuzione su un nuovo dominio e si desidera continuare a utilizzare gli utenti del vecchio dominio, è necessario registrare il vecchio dominio nel nuovo server SnapCenter .

Se hai aggiornato manualmente il file web.config nel vecchio host SnapCenter , gli aggiornamenti non verranno copiati nel nuovo host. Dovresti apportare manualmente le stesse modifiche nel file web.config del nuovo host.

6. Se hai saltato l'aggiornamento dell'URL del server SnapCenter o uno degli host era inattivo durante il processo di ripristino, aggiorna il nuovo nome del server in tutti gli host o negli host specificati gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.
7. Attivare i lavori pianificati su tutti gli host dal nuovo SnapCenter Server.

## Aggiornamento tecnico di un nodo nel cluster F5

È possibile effettuare l'aggiornamento tecnico di qualsiasi nodo nel cluster F5 rimuovendo il nodo e aggiungendone uno nuovo. Se il nodo che deve essere aggiornato è attivo, rendere attivo un altro nodo del cluster e quindi rimuovere il nodo.

Per informazioni su come aggiungere un nodo al cluster F5, fare riferimento a "Configurare i server SnapCenter per l'alta disponibilità utilizzando F5" .

Se l'URL del cluster F5 cambia, l'URL può essere aggiornato in tutti gli host utilizzando l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

## Dismissione del vecchio host del server SnapCenter

È possibile rimuovere il vecchio host di SnapCenter Server dopo aver verificato che il nuovo SnapCenter Server sia attivo e funzionante e che tutti gli host plug-in siano in grado di comunicare con il nuovo host di SnapCenter Server.

## Ripristina il vecchio host del server SnapCenter

In caso di problemi, è possibile ripristinare il vecchio host del server SnapCenter aggiornando l'URL del server SnapCenter in tutti gli host tramite l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

## Ripristino dopo un disastro

### Ripristino di emergenza dell'host SnapCenter autonomo

È possibile eseguire il ripristino di emergenza ripristinando il backup del server sul nuovo host.

#### Prima di iniziare

Assicurati di avere un backup del vecchio SnapCenter Server.

#### Passi

1. Distribuisci il nuovo host ed esegui le seguenti attività:
   a. Installare la stessa versione di SnapCenter Server.
   b. Configurare i certificati CA e abilitare SSL bidirezionale. Per maggiori informazioni, fare riferimento a "Configurare il certificato CA" E "Configurare e abilitare SSL bidirezionale" .
2. Copiare il vecchio backup del server SnapCenter sul nuovo host.

3. Accedi come utente amministratore SnapCenter .
4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: `/<snapcenter_version>/server/restore` oppure il cmdlet: *Restore-SmServerBackup*.

   Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera saltare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server tramite l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

   Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <Nuovo IP> SC_Server_Name.

   Le voci *etc/host* del server non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se hai saltato l'aggiornamento dell'URL o uno degli host era inattivo durante il processo di ripristino, aggiorna il nuovo nome del server in tutti gli host o negli host specificati gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

### Ripristino di emergenza del cluster SnapCenter F5

È possibile eseguire il ripristino di emergenza ripristinando il backup del server sul nuovo host e quindi convertendo l'host autonomo in un cluster.

#### Prima di iniziare

Assicurati di avere un backup del vecchio SnapCenter Server.

#### Passi

1. Distribuisci il nuovo host ed esegui le seguenti attività:
   a. Installare la stessa versione di SnapCenter Server.
   b. Configurare i certificati CA e abilitare SSL bidirezionale. Per maggiori informazioni, fare riferimento a "Configurare il certificato CA" E "Configurare e abilitare SSL bidirezionale" .
2. Copiare il vecchio backup del server SnapCenter sul nuovo host.
3. Accedi come utente amministratore SnapCenter .
4. Ripristinare il backup del server SnapCenter sul nuovo host utilizzando l'API: `/<snapcenter_version>/server/restore` oppure il cmdlet: *Restore-SmServerBackup*.

   Per impostazione predefinita, Restore aggiornerà il nuovo URL del server SnapCenter in tutti gli host. Se si desidera saltare l'aggiornamento, utilizzare l'attributo *-SkipSMSURLInHosts* e aggiornare separatamente l'URL del server tramite l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.

   Se l'host del plug-in non è in grado di risolvere il nome host del server, accedere a ciascun host del plug-in e aggiungere la voce *etc/host* per il nuovo IP nel formato <Nuovo IP> SC_Server_Name.

   Le voci *etc/host* del server non verranno ripristinate. È possibile ripristinarlo manualmente dal vecchio server.

5. Se hai saltato l'aggiornamento dell'URL o uno degli host era inattivo durante il processo di ripristino, aggiorna il nuovo nome del server in tutti gli host o negli host specificati gestiti da SnapCenter utilizzando l'API: `/<snapcenter_version>/server/configureurl` oppure il cmdlet: *Set-SmServerConfig*.
6. Convertire l'host autonomo in cluster F5.

   Per informazioni su come configurare F5, fare riferimento a "Configurare i server SnapCenter per l'alta disponibilità utilizzando F5" .

**Informazioni correlate**

Per informazioni sulle API, è necessario accedere alla pagina Swagger. vedere"Come accedere alle API REST utilizzando la pagina web dell'API Swagger" .

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento al "Guida di riferimento ai cmdlet del software SnapCenter" .

# Aggiornamento tecnologico degli host dei plug-in SnapCenter

Quando è necessario aggiornare gli host del plug-in SnapCenter , è necessario spostare le risorse dal vecchio host al nuovo host. Quando il nuovo host viene aggiunto a SnapCenter, rileverà tutte le risorse, ma verranno trattate come nuove risorse.

**Informazioni su questo compito**

Dovresti eseguire l'API o il cmdlet che accetterà come input il vecchio e il nuovo nome host, confronterà le risorse in base al nome e ricollegherà gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host. Le risorse corrispondenti verranno contrassegnate come protette.

- Per impostazione predefinita, il parametro *IsDryRun* è impostato su True e identifica le risorse corrispondenti del vecchio e del nuovo host.

  Dopo aver verificato le risorse corrispondenti, è necessario impostare il parametro *IsDryRun* su False per ricollegare gli oggetti delle risorse corrispondenti dal vecchio host al nuovo host.

- Per impostazione predefinita, il parametro *AutoMigrateManuallyAddedResources* è impostato su True e copia automaticamente le risorse aggiunte manualmente dal vecchio host al nuovo host.

  Il parametro *AutoMigrateManuallyAddedResources* è applicabile solo per le risorse Oracle e SAP HANA.

- Il parametro *SQLInstanceMapping* deve essere utilizzato se il nome dell'istanza è diverso tra il vecchio e il nuovo host. Se si tratta di un'istanza predefinita, utilizzare *default_instance* come nome dell'istanza.

L'aggiornamento tecnologico è supportato per i seguenti plug-in SnapCenter :

- Plug-in SnapCenter per Microsoft SQL Server
  - Se i database SQL sono protetti a livello di istanza e, come parte dell'aggiornamento tecnologico dell'host, solo risorse parziali vengono spostate sul nuovo host, la protezione a livello di istanza esistente verrà convertita in protezione del gruppo di risorse e le istanze di entrambi gli host verranno aggiunte al gruppo di risorse.
  - Se un host SQL (ad esempio host1) viene utilizzato come scheduler o server di verifica per le risorse di un altro host (ad esempio host2), durante l'esecuzione dell'aggiornamento tecnico su host1, la

pianificazione o i dettagli di verifica non verranno migrati e continueranno a essere eseguiti su host1. Se è necessario apportare modifiche, è necessario farlo manualmente nei rispettivi host.

    - Se si utilizza la configurazione SQL Failover Cluster Instances (FCI), è possibile eseguire l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster FCI e aggiornando l'host del plug-in in SnapCenter.
    - Se si utilizza la configurazione SQL Availability Group (AG), non è necessario un aggiornamento tecnico. È possibile aggiungere il nuovo nodo ad AG e aggiornare l'host in SnapCenter.

- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per Oracle Database

  Se si utilizza la configurazione Oracle Real Application Cluster (RAC), è possibile eseguire l'aggiornamento tecnico aggiungendo il nuovo nodo al cluster RAC e aggiornando l'host del plug-in in SnapCenter.

- Plug-in SnapCenter per database SAP HANA

I casi d'uso supportati sono:

- Migrazione delle risorse da un host a un altro.
- Migrazione di risorse da più host a uno o meno host.
- Migrazione delle risorse da un host a più host.

Gli scenari supportati sono:

- Il nuovo host ha un nome diverso dal vecchio host
- L'host esistente è stato rinominato

**Prima di iniziare**

Poiché questo flusso di lavoro modifica i dati nel repository SnapCenter , si consiglia di eseguire il backup del repository SnapCenter . In caso di problemi con i dati, è possibile ripristinare il repository SnapCenter allo stato precedente utilizzando il backup.

Per ulteriori informazioni, consulta "Eseguire il backup del repository SnapCenter" .

**Passi**

1. Distribuisci il nuovo host e installa l'applicazione.
2. Sospendi gli orari del vecchio host.
3. Spostare le risorse necessarie dal vecchio host al nuovo host.
    a. Caricare i database richiesti nel nuovo host dallo stesso archivio.
        - Assicurarsi che l'archiviazione sia mappata sulla stessa unità o sullo stesso percorso di montaggio del vecchio host. Se l'archiviazione non è mappata correttamente, i backup creati nel vecchio host non possono essere utilizzati per il ripristino.

          Per impostazione predefinita, Windows assegna automaticamente la successiva unità disponibile.

        - Se è abilitato il ripristino di emergenza dell'archiviazione, l'archiviazione corrispondente deve essere montata nel nuovo host.

    b. Verificare la compatibilità in caso di modifica della versione dell'applicazione.

c. Solo per l'host del plug-in Oracle, assicurarsi che gli UID e i GID di Oracle e dei suoi utenti di gruppo siano gli stessi del vecchio host.

   Per informazioni, fare riferimento a:

   - "Come migrare il database SQL dal vecchio host al nuovo host"
   - "Come migrare il database Oracle dal vecchio host al nuovo host"
   - "Come portare il database SAP HANA su un nuovo host"

4. Aggiungere il nuovo host a SnapCenter.
5. Verificare se tutte le risorse sono state rilevate.
6. Eseguire l'API di aggiornamento dell'host: `/<snapcenter_version>/techrefresh/host` oppure il cmdlet: *Invoke-SmTechRefreshHost*.

   Per impostazione predefinita, la prova di prova è abilitata e vengono identificate le risorse corrispondenti da ricollegare. È possibile verificare le risorse eseguendo l'API: '/jobs/{jobid}' o il cmdlet *Get-SmJobSummaryReport*.

   Se hai migrato le risorse da più host, dovresti eseguire l'API o il cmdlet per tutti gli host. Se l'unità o il percorso di montaggio nel nuovo host non sono gli stessi del vecchio host, le seguenti operazioni di ripristino non riusciranno:

   - Il ripristino SQL sul posto non riuscirà. Tuttavia, è possibile sfruttare la funzionalità RTAL.
   - Il ripristino dei database Oracle e SAP HANA non riuscirà.

     Se si desidera migrare su più host, è necessario eseguire tutti i passaggi dal passaggio 1 per tutti gli host.

   È possibile eseguire l'API o il cmdlet sullo stesso host più volte; il collegamento verrà effettuato solo se viene identificata una nuova risorsa.

7. (Facoltativo) Rimuovere il vecchio host o i vecchi host da SnapCenter.

**Informazioni correlate**

Per informazioni sulle API, è necessario accedere alla pagina Swagger. vedere"Come accedere alle API REST utilizzando la pagina web dell'API Swagger" .

Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento al "Guida di riferimento ai cmdlet del software SnapCenter" .

# Aggiornamento tecnologico del sistema di archiviazione

Quando lo storage viene aggiornato tecnologicamente, i dati vengono migrati su un nuovo storage e gli host dell'applicazione vengono montati con il nuovo storage. Il flusso di lavoro di backup SnapCenter identifica il nuovo archivio e crea lo snapshot se il nuovo archivio è registrato in SnapCenter.

È possibile eseguire il ripristino, il montaggio e la clonazione sui nuovi backup creati dopo l'aggiornamento dell'archiviazione. Tuttavia, queste operazioni non riusciranno se eseguite sui backup creati prima

dell'aggiornamento dell'archiviazione, perché i backup contengono i vecchi dettagli di archiviazione. Dovresti eseguire l'API o il cmdlet di aggiornamento della tecnologia di archiviazione per aggiornare i vecchi backup in SnapCenter con i nuovi dettagli di archiviazione.

L'aggiornamento tecnologico è supportato per i seguenti plug-in SnapCenter :

- Plug-in SnapCenter per Microsoft SQL Server
- Plug-in SnapCenter per Windows
- Plug-in SnapCenter per Oracle Database
- Plug-in SnapCenter per database SAP HANA
- Plug-in SnapCenter per Microsoft Exchange Server

I casi d'uso supportati sono:

- Aggiornamento dello storage primario

  L'aggiornamento della tecnologia di archiviazione è supportato per sostituire l'archiviazione primaria con una nuova. Non è possibile convertire l'archiviazione secondaria esistente in un'archiviazione primaria.

- Aggiornamento dell'archiviazione secondaria

## Aggiorna i backup dello storage primario

Quando la tecnologia di archiviazione viene aggiornata, è necessario eseguire l'API o il cmdlet di aggiornamento della tecnologia di archiviazione per aggiornare i vecchi backup in SnapCenter con i nuovi dettagli di archiviazione.

**Prima di iniziare**

Poiché questo flusso di lavoro modifica i dati nel repository SnapCenter , si consiglia di eseguire il backup del repository SnapCenter . In caso di problemi con i dati, è possibile ripristinare il repository SnapCenter allo stato precedente utilizzando il backup.

Per ulteriori informazioni, consulta "Eseguire il backup del repository SnapCenter" .

**Passi**

1. Migrare i dati dal vecchio storage al nuovo storage.

   Per informazioni su come effettuare la migrazione, fare riferimento a:

   - "Come migrare i dati su un nuovo storage"
   - "Come posso copiare un volume e conservare tutte le copie Snapshot?"
2. Mettere l'host in modalità di manutenzione.
3. Montare il nuovo storage nei rispettivi host e richiamare i database.

   Il nuovo storage deve essere connesso all'host nello stesso modo di prima. Ad esempio, se è stato connesso come SAN, deve essere connesso come SAN.

   Il nuovo storage deve essere montato sulla stessa unità o percorso del vecchio storage.

4. Verificare che tutte le risorse siano attive e funzionanti.
5. Aggiungere il nuovo spazio di archiviazione in SnapCenter.

Assicurati di avere un nome SVM univoco in tutti i cluster in SnapCenter. Se si utilizza lo stesso nome SVM nel nuovo archivio e se tutti i volumi dell'SVM possono essere migrati prima di eseguire l'aggiornamento dell'archivio, si consiglia di eliminare l'SVM nel vecchio cluster e di riscoprire il vecchio cluster in SnapCenter , il che rimuoverà l'SVM dalla cache.

6. Mettere l'host in modalità di produzione.
7. In SnapCenter, creare un backup delle risorse il cui storage viene migrato. È necessario un nuovo backup affinché SnapCenter identifichi l'ultimo spazio di archiviazione e verrà utilizzato per aggiornare i metadati dei vecchi backup esistenti.

> Ogni volta che un nuovo LUN viene collegato all'host, avrà un nuovo numero di serie. Durante l'individuazione del file system di Windows, SnapCenter tratterà ogni numero di serie univoco come una nuova risorsa. Durante l'aggiornamento della tecnologia di archiviazione, quando il LUN del nuovo archivio viene collegato all'host con la stessa lettera di unità o percorso, la scoperta del file system di Windows in SnapCenter contrassegnerà la risorsa esistente come eliminata anche se è montata con la stessa lettera di unità o percorso e visualizzerà il nuovo LUN come nuova risorsa. Poiché la risorsa è contrassegnata come eliminata, non verrà presa in considerazione per l'aggiornamento della tecnologia di archiviazione in SnapCenter e tutti i backup della vecchia risorsa andranno persi. Ogni volta che si verifica un aggiornamento dell'archiviazione, per le risorse del file system di Windows, l'individuazione delle risorse non deve essere eseguita prima di eseguire l'API o il cmdlet di aggiornamento dell'archiviazione.

8. Eseguire l'API di aggiornamento dello storage: `/<snapcenter_version>/techrefresh/primarystorage` oppure il cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

> Se la risorsa è configurata con un criterio di replicazione abilitato, l'ultimo backup dopo l'aggiornamento dell'archiviazione dovrebbe contenere i dettagli dell'archiviazione secondaria.

   a. Se si utilizza la configurazione SQL Failover Cluster Instances (FCI), i backup vengono mantenuti a livello di cluster. È necessario fornire il nome del cluster come input per l'aggiornamento della tecnologia di archiviazione.
   b. Se si utilizza la configurazione SQL Availability Group (AG), i backup vengono mantenuti a livello di nodo. Dovresti fornire il nome del nodo come input per l'aggiornamento della tecnologia di archiviazione.
   c. Se si utilizza la configurazione Oracle Real Application Clusters (RAC), è possibile eseguire l'aggiornamento della tecnologia di archiviazione su qualsiasi nodo.

      Per impostazione predefinita, l'attributo *IsDryRun* è impostato su True. Identificherà le risorse per cui viene aggiornato lo storage. È possibile visualizzare la risorsa e i dettagli di archiviazione modificati eseguendo l'API: '<snapcenter_version>/jobs/{jobid}' o il cmdlet *Get-SmJobSummaryReport*.

9. Dopo aver verificato i dettagli di archiviazione, impostare l'attributo *IsDryRun* su False ed eseguire l'API di aggiornamento dell'archiviazione: `/<snapcenter_version>/techrefresh/primarystorage` oppure il cmdlet: *Invoke-SmTechRefreshPrimaryStorage*.

   In questo modo verranno aggiornati i dettagli di archiviazione nei backup più vecchi.

   È possibile eseguire l'API o il cmdlet sullo stesso host più volte; i dettagli di archiviazione nei backup precedenti verranno aggiornati solo se l'archiviazione viene aggiornata.

La gerarchia dei cloni non può essere migrata in ONTAP. Se lo storage in fase di migrazione contiene metadati di clonazione in SnapCenter, la risorsa clonata verrà contrassegnata come risorsa indipendente. I cloni dei metadati dei cloni verranno rimossi in modo ricorsivo.

10. (Facoltativo) Se tutti gli snapshot non vengono spostati dal vecchio storage primario al nuovo storage primario, eseguire la seguente API: `/<snapcenter_version>/hosts/primarybackupsexistencecheck` oppure il cmdlet *Invoke-SmPrimaryBackupsExistenceCheck*.

    Verrà eseguito il controllo dell'esistenza dello snapshot sul nuovo archivio primario e i rispettivi backup verranno contrassegnati come non disponibili per alcuna operazione in SnapCenter.

## Aggiorna i backup dello storage secondario

Quando la tecnologia di archiviazione viene aggiornata, è necessario eseguire l'API o il cmdlet di aggiornamento della tecnologia di archiviazione per aggiornare i vecchi backup in SnapCenter con i nuovi dettagli di archiviazione.

**Prima di iniziare**

Poiché questo flusso di lavoro modifica i dati nel repository SnapCenter , si consiglia di eseguire il backup del repository SnapCenter . In caso di problemi con i dati, è possibile ripristinare il repository SnapCenter allo stato precedente utilizzando il backup.

Per ulteriori informazioni, consulta "Eseguire il backup del repository SnapCenter" .

**Passi**

1. Migrare i dati dal vecchio storage al nuovo storage.

    Per informazioni su come effettuare la migrazione, fare riferimento a:

    - "Come migrare i dati su un nuovo storage"
    - "Come posso copiare un volume e conservare tutte le copie Snapshot?"
2. Stabilisci la relazione SnapMirror tra l'archiviazione primaria e la nuova archiviazione secondaria e assicurati che lo stato della relazione sia corretto.
3. In SnapCenter, creare un backup delle risorse il cui storage viene migrato.

    È necessario un nuovo backup affinché SnapCenter identifichi l'ultimo spazio di archiviazione e verrà utilizzato per aggiornare i metadati dei vecchi backup esistenti.

    Dovresti attendere il completamento di questa operazione. Se si procede al passaggio successivo prima del completamento, SnapCenter perderà completamente i vecchi metadati dello snapshot secondario.

4. Dopo aver creato correttamente il backup di tutte le risorse in un host, eseguire l'API di aggiornamento dell'archiviazione secondaria: `/<snapcenter_version>/techrefresh/secondarystorage` oppure il cmdlet: *Invoke-SmTechRefreshSecondaryStorage*.

    In questo modo verranno aggiornati i dettagli dell'archiviazione secondaria dei backup più vecchi nell'host specificato.

    Se si desidera eseguire questa operazione a livello di risorsa, fare clic su **Aggiorna** per ogni risorsa per

aggiornare i metadati dell’archiviazione secondaria.

5. Dopo aver aggiornato correttamente i backup più vecchi, è possibile interrompere la vecchia relazione di archiviazione secondaria con quella primaria.

# Disinstallare SnapCenter Server e i plug-in

## Disinstallare i pacchetti plug-in SnapCenter

### Prerequisiti per la rimozione di un host

È possibile rimuovere gli host e disinstallare singoli plug-in o pacchetti di plug-in utilizzando l'interfaccia utente grafica SnapCenter . È anche possibile disinstallare singoli plug-in o pacchetti di plug-in su host remoti utilizzando l'interfaccia della riga di comando (CLI) sull'host SnapCenter Server oppure utilizzando l'opzione **Disinstalla un programma** di Windows localmente su qualsiasi host.

Prima di rimuovere un host da SnapCenter Server, è necessario completare i prerequisiti.

- Dovresti effettuare l'accesso come amministratore.
- È necessario assicurarsi che i processi di individuazione non siano in esecuzione sull'host.
- Dovresti ricevere un ruolo con le autorizzazioni necessarie per rimuovere tutti gli oggetti associati all'host. In caso contrario, l'operazione di rimozione fallisce.
- È necessario confermare l'impronta digitale se la chiave SSH è stata modificata dopo aver aggiunto l'host a SnapCenter.
- È necessario confermare l'impronta digitale se l'host SnapCenter è stato aggiornato a una versione successiva di SnapCenter ma l'host del plug-in esegue ancora una versione precedente del plug-in.

#### Prerequisiti per rimuovere un host utilizzando il controllo degli accessi basato sui ruoli

- Dovresti aver effettuato l'accesso utilizzando un ruolo RBAC che dispone delle autorizzazioni di lettura, eliminazione host, installazione, disinstallazione di plug-in ed eliminazione oggetti.

  Gli oggetti possono essere cloni, backup, gruppi di risorse, sistemi di archiviazione e così via.

- Avresti dovuto aggiungere l'utente RBAC al ruolo RBAC.
- È necessario assegnare l'utente RBAC all'host, al plug-in, alle credenziali, ai gruppi di risorse e al sistema di archiviazione (per i cloni) che si desidera eliminare.
- Dovresti aver effettuato l'accesso a SnapCenter come utente RBAC.

#### Prerequisiti per rimuovere un host con cloni creati dall'operazione del ciclo di vita del clone

- Avresti dovuto creare processi di clonazione utilizzando la gestione del ciclo di vita dei cloni per i database SQL.
- Dovresti aver creato un ruolo RBAC con autorizzazioni di lettura ed eliminazione clone, lettura ed eliminazione risorse, lettura ed eliminazione gruppi risorse, lettura ed eliminazione storage, lettura ed eliminazione provisioning, montaggio, smontaggio, installazione e disinstallazione plug-in, lettura ed eliminazione host.
- Avresti dovuto assegnare all'utente RBAC il ruolo RBAC.
- Dovresti aver assegnato l'utente RBAC all'host, al plug-in SnapCenter per Microsoft SQL Server, alle credenziali, al gruppo di risorse del ciclo di vita del clone e al sistema di archiviazione.
- Dovresti aver effettuato l'accesso a SnapCenter come utente RBAC.

Per informazioni sulla disinstallazione del SnapCenter Plug-in for VMware vSphere, vedere "Rimuovere il SnapCenter Plug-in for VMware vSphere" .

## Rimuovere un host

Quando SnapCenter Server rimuove un host, rimuove innanzitutto il backup, i cloni, i processi di clonazione, i gruppi di risorse e le risorse elencate per quell'host nella pagina Risorse SnapCenter , quindi disinstalla i pacchetti plug-in sull'host.

**Informazioni su questo compito**

- Se si elimina un host, vengono eliminati anche i backup, i cloni e i gruppi di risorse associati all'host.
- Quando si rimuovono i gruppi di risorse, vengono rimosse anche tutte le pianificazioni associate.
- Se l'host ha un gruppo di risorse condiviso con un altro host e si elimina l'host, verrà eliminato anche il gruppo di risorse.
- Per rimuovere gli host dei plug-in dismessi o non raggiungibili, è necessario utilizzare il cmdlet *Remove-SmHost*.

  Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter"

- Il tempo necessario per rimuovere un host dipende dal numero di backup e dalle impostazioni di conservazione. Ciò avviene perché gli snapshot vengono eliminati da ciascuno dei controller e i metadati vengono ripuliti.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina **Host**, fare clic su **Host gestiti**.
3. Seleziona l'host che vuoi rimuovere, quindi fai clic su **Rimuovi**.
4. Per i cluster Oracle RAC, per rimuovere il SnapCenter software da tutti gli host nel cluster, selezionare **Includi tutti gli host del cluster**.

   È anche possibile rimuovere un nodo di un cluster e in questo modo rimuovere tutti i nodi uno alla volta.

5. Fare clic su **OK**.

> Quando si disinstallano e si reinstallano i plug-in host su un cluster, le risorse del cluster non vengono rilevate automaticamente. Selezionare il nome host del cluster, quindi fare clic su **Aggiorna risorse** per rilevare automaticamente le risorse del cluster.

## Disinstallare i plug-in utilizzando l'interfaccia grafica utente SnapCenter

Quando decidi che un singolo plug-in o un pacchetto di plug-in non ti serve più, puoi disinstallarlo tramite l'interfaccia SnapCenter .

**Prima di iniziare**

- Dovresti aver rimosso i gruppi di risorse per il pacchetto plug-in che stai disinstallando.
- Dovresti aver scollegato i criteri associati ai gruppi di risorse per il pacchetto plug-in che stai disinstallando.

**Informazioni su questo compito**

È possibile disinstallare un singolo plug-in. Ad esempio, potrebbe essere necessario disinstallare il plug-in SnapCenter per Microsoft SQL Server perché un host sta esaurendo le risorse e si desidera spostare il plug-in su un host più potente. È anche possibile disinstallare un intero pacchetto plug-in. Ad esempio, potrebbe essere necessario disinstallare il pacchetto di plug-in SnapCenter per Linux, che include il plug-in SnapCenter per Oracle Database e il plug-in SnapCenter per UNIX.

- La rimozione di un host comporta la disinstallazione di tutti i plug-in.

  Quando si rimuove un host da SnapCenter, SnapCenter disinstalla tutti i pacchetti plug-in sull'host prima di rimuoverlo.

- L'interfaccia grafica utente SnapCenter rimuove i plug-in da un host alla volta.

  Quando si utilizza l'interfaccia utente grafica SnapCenter , è possibile disinstallare i plug-in su un solo host alla volta. Tuttavia, è possibile eseguire più operazioni di disinstallazione contemporaneamente.

  È anche possibile disinstallare un plug-in da più host utilizzando il cmdlet *Uninstall-SmHostPackage* e i parametri richiesti. Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento a "Guida di riferimento ai cmdlet del software SnapCenter" .

> La disinstallazione del pacchetto plug-in SnapCenter per Windows da un host su cui è installato SnapCenter Server danneggerà l'installazione SnapCenter Server. Non disinstallare il pacchetto di plug-in SnapCenter per Windows a meno che non si sia certi di non aver più bisogno di SnapCenter Server.

**Passi**

1. Nel riquadro di navigazione a sinistra, fare clic su **Host**.
2. Nella pagina Host, fare clic su **Host gestiti**.
3. Nella pagina Host gestiti, seleziona l'host da cui desideri disinstallare il plug-in o il pacchetto plug-in.
4. Accanto al plug-in che vuoi rimuovere, fai clic su **Rimuovi** > **Invia**.

**Dopo aver finito**

Dovresti attendere 5 minuti prima di reinstallare il plug-in su quell'host. Questo intervallo di tempo è sufficiente affinché l'interfaccia utente grafica SnapCenter aggiorni lo stato dell'host gestito. L'installazione fallisce se si reinstalla immediatamente il plug-in.

Se si sta disinstallando il pacchetto plug-in SnapCenter per Linux, i file di registro specifici della disinstallazione sono disponibili in: */custom_location/snapcenter/log*.

## Disinstallare i plug-in di Windows utilizzando il cmdlet PowerShell

È possibile disinstallare singoli plug-in o disinstallare pacchetti di plug-in da uno o più host utilizzando il cmdlet *Uninstall-SmHostPackage* nell'interfaccia della riga di comando dell'host SnapCenter Server.

Dovresti aver effettuato l'accesso a SnapCenter come utente di dominio con diritti di amministratore locale su ciascun host su cui desideri disinstallare i plug-in.

**Passi**

1. Avvia PowerShell.
2. Sull'host del server SnapCenter , immettere il comando: *Open-SMConnection -SMSbaseUrl https://SNAPCENTER_SERVER_NAME/DOMAIN_NAME*, quindi immettere le credenziali.
3. Disinstallare i plug-in di Windows utilizzando il cmdlet *Uninstall-SmHostPackage* e i parametri richiesti.

   Le informazioni relative ai parametri che possono essere utilizzati con il cmdlet e le relative descrizioni possono essere ottenute eseguendo *Get-Help command_name*. In alternativa, puoi anche fare riferimento al "Guida di riferimento ai cmdlet del software SnapCenter" .

## Disinstallare i plug-in localmente su un host

È possibile disinstallare i plug-in SnapCenter localmente su un host se non è possibile raggiungere l'host dal server SnapCenter .

**Informazioni su questo compito**

La procedura consigliata per disinstallare singoli plug-in o pacchetti di plug-in è quella di utilizzare l'interfaccia utente grafica SnapCenter oppure il cmdlet Uninstall-SmHostPackage sull'interfaccia della riga di comando dell'host di SnapCenter Server. Queste procedure aiutano il server SnapCenter a rimanere aggiornato su eventuali modifiche.

Tuttavia, in rari casi, potrebbe essere necessario disinstallare i plug-in localmente. Ad esempio, potresti aver eseguito un processo di disinstallazione da SnapCenter Server ma il processo non è riuscito oppure potresti aver disinstallato SnapCenter Server e i plug-in orfani rimangono su un host.

La disinstallazione di un pacchetto plug-in localmente su un host non elimina i dati associati all'host, ad esempio i processi pianificati e i metadati di backup.

Non tentare di disinstallare localmente il pacchetto plug-in SnapCenter per Windows dal Pannello di controllo. È necessario utilizzare l'interfaccia utente grafica SnapCenter per assicurarsi che il plug-in SnapCenter per Microsoft Windows sia stato disinstallato correttamente.

**Passi**

1. Sul sistema host, vai al Pannello di controllo e clicca su **Disinstalla un programma**.
2. Nell'elenco dei programmi, seleziona il plug-in o il pacchetto plug-in SnapCenter che desideri disinstallare e fai clic su **Disinstalla**.

   Windows disinstalla tutti i plug-in nel pacchetto selezionato.

## Disinstallare il pacchetto plug-in per Linux o AIX tramite CLI

È possibile disinstallare SnapCenter Plug-ins Package per Linux o SnapCenter Plug-ins Package per AIX utilizzando l'interfaccia della riga di comando.

**Prima di iniziare**

- Assicurati di aver eliminato i lavori pianificati
- Assicurarsi che tutti i lavori in esecuzione siano completati.

**Fare un passo**

Eseguire */custom_location/ NetApp/snapcenter/spl/installation/plugins/uninstall* per disinstallare.

# Disinstallare SnapCenter Server sull'host Windows

Se non si desidera più utilizzare SnapCenter Server per gestire i processi di protezione dei dati, è possibile disinstallare SnapCenter Server tramite il Pannello di controllo Programmi e funzionalità sull'host di SnapCenter Server. La disinstallazione di SnapCenter Server rimuove tutti i suoi componenti.

**Prima di iniziare**

- Assicurarsi di avere almeno 2 GB di spazio libero sull'unità in cui è installato SnapCenter Server.
- Assicurarsi che il dominio in cui è installato SnapCenter Server non venga rimosso.

  Se si rimuove il dominio in cui è stato installato SnapCenter Server e poi si tenta di disinstallarlo, l'operazione non riesce.

- Dovresti aver eseguito il backup del database del repository perché verrà ripulito e disinstallato.

**Passi**

1. Sull'host del server SnapCenter , accedere al Pannello di controllo.
2. Assicurati di essere nella visualizzazione **Categoria**.
3. In Programmi, fare clic su **Disinstalla un programma**.

   Si apre la finestra Programmi e funzionalità.

4. Selezionare NetApp SnapCenter Server, quindi fare clic su **Disinstalla**.

   A partire da SnapCenter 4.2, quando si disinstalla SnapCenter Server, tutti i suoi componenti, incluso il database del repository MySQL Server, vengono disinstallati.

   - Per rimuovere il nodo NLB da un cluster NLB è necessario riavviare l'host del server SnapCenter . Se non si riavvia l'host, potrebbe verificarsi un errore se si tenta di reinstallare SnapCenter Server.
   - Dovresti disinstallare manualmente .NET Framework che non viene rimosso durante la disinstallazione.

# Disinstallare SnapCenter Server sull'host Linux

Se non si desidera più utilizzare SnapCenter Server per gestire i processi di protezione dei dati, è possibile disinstallare SnapCenter Server. La disinstallazione di SnapCenter Server rimuove tutti i suoi componenti.

**Passi**

1. Eseguire una delle azioni per disinstallare SnapCenter Server.

| Se vuoi esibirti… | Fai questo… |
| --- | --- |
| Disinstallazione non interattiva | `$ sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall -i silent -DCONFIRM=1`<br><br>Esempio: sudo /opt/NetApp/snapcenter/SnapManagerWeb/installation/uninstall |
| Disinstallazione interattiva | `$ sudo <USER_INSTALL_DIR>/NetApp/snapcenter/SnapManagerWeb/installation/uninstall`<br><br>Immettere un valore diverso da 0 nel campo di conferma per confermare la disinstallazione. |

# Automatizzare utilizzando le API REST

## Automazione SnapCenter tramite API REST

È possibile utilizzare le API REST per eseguire diverse operazioni di gestione SnapCenter . Le API REST sono accessibili tramite la pagina web Swagger. È possibile accedere alla pagina Web di Swagger disponibile all'indirizzo *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/* per visualizzare la documentazione dell'API REST e per emettere manualmente una chiamata API.

I plug-in che supportano le API REST sono:

- Plug-in per Microsoft SQL Server
- Plug-in per il database SAP HANA
- Plug-in per Oracle Database

Per informazioni sul SnapCenter Plug-in for VMware vSphere , vedere "SnapCenter Plug-in for VMware vSphere"

## Come accedere in modo nativo all'API REST di SnapCenter

È possibile accedere direttamente all'API REST SnapCenter utilizzando qualsiasi linguaggio di programmazione che supporti un client REST. I linguaggi più diffusi sono Python, PowerShell e Java.

## Fondazione dei servizi web REST

Il Representational State Transfer (REST) è uno stile per la creazione di applicazioni web distribuite. Applicato alla progettazione di un'API di servizi web, stabilisce un insieme di tecnologie e best practice per l'esposizione delle risorse basate su server e la gestione dei loro stati. Utilizza protocolli e standard tradizionali per fornire una base flessibile per la gestione SnapCenter.

### Risorse e rappresentanza statale

Le risorse sono i componenti di base di un sistema basato sul web. Quando si crea un'applicazione di servizi web REST, le prime attività di progettazione includono:

#### Identificazione delle risorse basate sul sistema o sul server

Ogni sistema utilizza e gestisce risorse. Una risorsa può essere un file, una transazione aziendale, un processo o un'entità amministrativa. Uno dei primi compiti nella progettazione di un'applicazione basata su servizi web REST è l'identificazione delle risorse.

**Definizione degli stati delle risorse e delle operazioni di stato associate**

Le risorse si trovano sempre in uno di un numero finito di stati. Gli stati, così come le operazioni associate utilizzate per influenzare i cambiamenti di stato, devono essere chiaramente definiti.

### Endpoint URI

Ogni risorsa REST deve essere definita e resa disponibile utilizzando uno schema di indirizzamento ben definito. Gli endpoint in cui le risorse sono localizzate e identificate utilizzano un Uniform Resource Identifier (URI).

L'URI fornisce un framework generale per la creazione di un nome univoco per ciascuna risorsa nella rete. L'Uniform Resource Locator (URL) è un tipo di URI utilizzato con i servizi web per identificare e accedere alle risorse. Le risorse sono in genere esposte in una struttura gerarchica simile a una directory di file.

### Messaggi HTTP

Il protocollo HTTP (Hypertext Transfer Protocol) è il protocollo utilizzato dal client e dal server dei servizi web per scambiare messaggi di richiesta e risposta relativi alle risorse.

Nell'ambito della progettazione di un'applicazione di servizi Web, i metodi HTTP vengono mappati alle risorse e alle corrispondenti azioni di gestione dello stato. HTTP è un protocollo stateless. Pertanto, per associare un insieme di richieste e risposte correlate come parte di una transazione, è necessario includere informazioni aggiuntive nelle intestazioni HTTP trasportate con i flussi di dati di richiesta e risposta.

### Formattazione JSON

Sebbene le informazioni possano essere strutturate e trasferite tra un client e un server di servizi Web in diversi modi, l'opzione più diffusa è JavaScript Object Notation (JSON).

JSON è uno standard industriale per la rappresentazione di strutture dati semplici in testo normale e viene utilizzato per trasferire informazioni sullo stato che descrivono le risorse. L'API REST SnapCenter utilizza JSON per formattare i dati contenuti nel corpo di ogni richiesta e risposta HTTP.

# Caratteristiche operative di base

Sebbene REST stabilisca un insieme comune di tecnologie e best practice, i dettagli di ciascuna API possono variare in base alle scelte progettuali.

### Transazione API di richiesta e risposta

Ogni chiamata API REST viene eseguita come una richiesta HTTP al sistema SnapCenter Server, che genera una risposta associata al client. Questa coppia di richiesta e risposta è considerata una transazione API.

Prima di utilizzare l'API, è necessario acquisire familiarità con le variabili di input disponibili per controllare una richiesta e il contenuto dell'output della risposta.

### Supporto per le operazioni CRUD

Ciascuna delle risorse disponibili tramite l'API REST SnapCenter è accessibile in base al modello CRUD:

- Creare

- Leggere
- Aggiornamento
- Eliminare

Per alcune risorse è supportato solo un sottoinsieme delle operazioni.

## Identificatori di oggetti

A ogni istanza o oggetto di risorsa viene assegnato un identificatore univoco al momento della creazione. Nella maggior parte dei casi, l'identificatore è un UUID a 128 bit. Questi identificatori sono univoci a livello globale all'interno di uno specifico SnapCenter Server.

Dopo aver emesso una chiamata API che crea una nuova istanza di oggetto, un URL con l'ID associato viene restituito al chiamante nell'intestazione della posizione della risposta HTTP. È possibile estrarre l'identificatore e utilizzarlo nelle chiamate successive quando si fa riferimento all'istanza della risorsa.

Il contenuto e la struttura interna degli identificatori degli oggetti possono cambiare in qualsiasi momento. Si consiglia di utilizzare gli identificatori solo nelle chiamate API applicabili, quando necessario, quando si fa riferimento agli oggetti associati.

## Istanze e raccolte di oggetti

A seconda del percorso della risorsa e del metodo HTTP, una chiamata API può essere applicata a un'istanza di oggetto specifica o a una raccolta di oggetti.

## Operazioni sincrone e asincrone

SnapCenter esegue una richiesta HTTP ricevuta da un client in modo sincrono o asincrono.

### Elaborazione sincrona

SnapCenter esegue la richiesta immediatamente e risponde con un codice di stato HTTP pari a 200 o 201 se l'operazione ha esito positivo.

Ogni richiesta che utilizza il metodo GET viene sempre eseguita in modo sincrono. Inoltre, le richieste che utilizzano POST sono progettate per essere eseguite in modo sincrono se si prevede che vengano completate in meno di due secondi.

### Elaborazione asincrona

Se una richiesta asincrona è valida, SnapCenter crea un'attività in background per elaborare la richiesta e un oggetto processo per ancorare l'attività. Il codice di stato HTTP 202 viene restituito al chiamante insieme all'oggetto del processo. Per determinare se l'operazione è riuscita o meno, è necessario recuperare lo stato del lavoro.

Le richieste che utilizzano i metodi POST e DELETE sono progettate per essere eseguite in modo asincrono se si prevede che impiegheranno più di due secondi per essere completate.

## Sicurezza

La sicurezza fornita dall'API REST si basa principalmente sulle funzionalità di sicurezza esistenti disponibili con SnapCenter. L'API utilizza la seguente sicurezza:

#### Sicurezza del livello di trasporto

Tutto il traffico inviato sulla rete tra il server SnapCenter e il client viene in genere crittografato tramite TLS, in base alle impostazioni di configurazione SnapCenter .

#### Autenticazione HTTP

A livello HTTP, per le transazioni API viene utilizzata l'autenticazione di base. A ogni richiesta viene aggiunta un'intestazione HTTP con il nome utente e la password in una stringa base64.

# Variabili di input che controllano una richiesta API

È possibile controllare il modo in cui una chiamata API viene elaborata tramite parametri e variabili impostati nella richiesta HTTP.

## Metodi HTTP

I metodi HTTP supportati dall'API REST SnapCenter sono mostrati nella tabella seguente.

Non tutti i metodi HTTP sono disponibili in ciascuno degli endpoint REST.

| Metodo HTTP | Descrizione |
|---|---|
| OTTENERE | Recupera le proprietà degli oggetti su un'istanza o una raccolta di risorse. |
| INVIARE | Crea una nuova istanza di risorsa in base all'input fornito. |
| ELIMINARE | Elimina un'istanza di risorsa esistente. |
| METTERE | Modifica un'istanza di risorsa esistente. |

## Intestazioni di richiesta

Dovresti includere diverse intestazioni nella richiesta HTTP.

#### Tipo di contenuto

Se il corpo della richiesta include JSON, questa intestazione deve essere impostata su *application/json*.

#### Accettare

Questa intestazione dovrebbe essere impostata su *application/json*.

#### Autorizzazione

L'autenticazione di base deve essere impostata con il nome utente e la password codificati come stringa base64.

## Corpo della richiesta

Il contenuto del corpo della richiesta varia a seconda della chiamata specifica. Il corpo della richiesta HTTP è

costituito da uno dei seguenti elementi:

- Oggetto JSON con variabili di input
- Vuoto

## Filtraggio degli oggetti

Quando si esegue una chiamata API che utilizza GET, è possibile limitare o filtrare gli oggetti restituiti in base a qualsiasi attributo. Ad esempio, è possibile specificare un valore esatto da ricercare:

```
<field>=<query value>
```

Oltre alla corrispondenza esatta, sono disponibili altri operatori per restituire un set di oggetti su un intervallo di valori. L'API REST SnapCenter supporta gli operatori di filtraggio mostrati nella tabella seguente.

| Operatore | Descrizione |
|---|---|
| = | Uguale a |
| < | Meno di |
| > | Maggiore di |
| ⇐ | Minore o uguale a |
| >= | Maggiore o uguale a |
| AGGIORNAMENTO | O |
| ! | Non uguale a |
| * | Jolly avido |

È anche possibile restituire una raccolta di oggetti in base al fatto che un campo specifico sia impostato o meno utilizzando la parola chiave **null** o la sua negazione **!null** come parte della query.

In genere, tutti i campi non impostati vengono esclusi dalle query corrispondenti.

## Richiesta di campi di oggetti specifici

Per impostazione predefinita, l'emissione di una chiamata API tramite GET restituisce solo gli attributi che identificano in modo univoco l'oggetto o gli oggetti. Questo set minimo di campi funge da chiave per ciascun oggetto e varia in base al tipo di oggetto. È possibile selezionare proprietà aggiuntive dell'oggetto utilizzando `fields` parametro di query nei seguenti modi:

#### Campi comuni o standard

Specificare **fields=*** per recuperare i campi oggetto utilizzati più comunemente. Questi campi vengono solitamente mantenuti nella memoria del server locale o richiedono poca elaborazione per accedervi. Si tratta delle stesse proprietà restituite per un oggetto dopo aver utilizzato GET con una chiave del percorso URL (UUID).

#### Tutti i campi

Specificare **fields=**** per recuperare tutti i campi dell'oggetto, compresi quelli che richiedono un'ulteriore elaborazione del server per l'accesso.

#### Selezione di campi personalizzati

Utilizzare **fields=<nome_campo>** per specificare il campo esatto desiderato. Quando si richiedono più campi, i valori devono essere separati da virgole senza spazi.

> Come buona pratica, dovresti sempre identificare i campi specifici che desideri. Dovresti recuperare solo il set di campi comuni o tutti i campi quando necessario. NetApp determina quali campi vengono classificati come comuni e restituiti utilizzando *fields=** in base all'analisi interna delle prestazioni. La classificazione di un campo potrebbe cambiare nelle versioni future.

## Ordinamento degli oggetti nel set di output

I record in una raccolta di risorse vengono restituiti nell'ordine predefinito definito dall'oggetto. È possibile modificare l'ordine utilizzando il `order_by` parametro di query con il nome del campo e la direzione di ordinamento come segue:

```
order_by=<field name> asc|desc
```

Ad esempio, è possibile ordinare il campo tipo in ordine decrescente seguito da id in ordine crescente:

```
order_by=type desc, id asc
```

- Se si specifica un campo di ordinamento ma non si fornisce una direzione, i valori vengono ordinati in ordine crescente.
- Quando si includono più parametri, è necessario separare i campi con una virgola.

## Paginazione durante il recupero di oggetti in una raccolta

Quando si invia una chiamata API tramite GET per accedere a una raccolta di oggetti dello stesso tipo, SnapCenter tenta di restituire quanti più oggetti possibile in base a due vincoli. È possibile controllare ciascuno di questi vincoli utilizzando parametri di query aggiuntivi nella richiesta. Il primo vincolo raggiunto per una richiesta GET specifica termina la richiesta e quindi limita il numero di record restituiti.

> Se una richiesta termina prima di aver eseguito l'iterazione su tutti gli oggetti, la risposta contiene il collegamento necessario per recuperare il batch successivo di record.

#### Limitare il numero di oggetti

Per impostazione predefinita, SnapCenter restituisce un massimo di 10.000 oggetti per una richiesta GET. È possibile modificare questo limite utilizzando il parametro di query *max_records*. Per esempio:

```
max_records=20
```

Il numero di oggetti effettivamente restituiti può essere inferiore al massimo effettivo, in base al vincolo di tempo correlato e al numero totale di oggetti nel sistema.

#### Limitare il tempo impiegato per recuperare gli oggetti

Per impostazione predefinita, SnapCenter restituisce quanti più oggetti possibile entro il tempo consentito per la richiesta GET. Il timeout predefinito è 15 secondi. È possibile modificare questo limite utilizzando il parametro di query *return_timeout*. Per esempio:

```
return_timeout=5
```

Il numero di oggetti effettivamente restituiti può essere inferiore al massimo effettivo, in base al vincolo correlato al numero di oggetti e al numero totale di oggetti nel sistema.

#### Restringimento del set di risultati

Se necessario, è possibile combinare questi due parametri con parametri di query aggiuntivi per restringere il set di risultati. Ad esempio, quanto segue restituisce fino a 10 eventi EMS generati dopo il tempo specificato:

```
time⇒ 2018-04-04T15:41:29.140265Z&max_records=10
```

È possibile inviare più richieste per sfogliare gli oggetti. Ogni successiva chiamata API dovrebbe utilizzare un nuovo valore temporale basato sull'evento più recente nell'ultimo set di risultati.

### Proprietà dimensionali

I valori di input utilizzati con alcune chiamate API e determinati parametri di query sono numerici. Invece di fornire un numero intero in byte, è possibile utilizzare facoltativamente un suffisso come mostrato nella tabella seguente.

| Suffisso | Descrizione |
|---|---|
| KB | KB Kilobyte (1024 byte) o kibibyte |
| MB | MB Megabyte (KB x 1024 byte) o mebibyte |
| GB | GB Gigabyte (MB x 1024 byte) o gibibyte |
| tubercolosi | TB Terabyte (GB x 1024 byte) o tebibyte |
| PB | PB Petabyte (TB x 1024 byte) o pebibyte |

# Interpretazione di una risposta API

Ogni richiesta API genera una risposta al client. Dovresti esaminare la risposta per determinare se ha avuto successo e recuperare dati aggiuntivi se necessario.

### Codice di stato HTTP

Di seguito sono descritti i codici di stato HTTP utilizzati dall'API REST SnapCenter .

| Codice | Descrizione |
|---|---|
| 200 | OK Indica il successo delle chiamate che non creano un nuovo oggetto. |
| 201 | Creato Un oggetto è stato creato correttamente. L'intestazione della posizione nella risposta include l'identificatore univoco dell'oggetto. |
| 202 | Accettato È stato avviato un processo in background per eseguire la richiesta, ma non è ancora stato completato. |

| Codice | Descrizione |
| --- | --- |
| 400 | Richiesta non valida La richiesta di input non è stata riconosciuta o è inappropriata. |
| 401 | L'autenticazione dell'utente non autorizzato non è riuscita. |
| 403 | L'accesso proibito è stato negato a causa di un errore di autorizzazione (RBAC). |
| 404 | Non trovato La risorsa a cui si fa riferimento nella richiesta non esiste. |
| 405 | Metodo non consentito Il metodo HTTP nella richiesta non è supportato per la risorsa. |
| 409 | Conflitto Un tentativo di creare un oggetto non è riuscito perché è necessario creare prima un oggetto diverso oppure l'oggetto richiesto esiste già. |
| 500 | Errore interno Si è verificato un errore interno generale sul server. |

## Intestazioni di risposta

Nella risposta HTTP generata da SnapCenter sono incluse diverse intestazioni.

### Posizione

Quando viene creato un oggetto, l'intestazione della posizione include l'URL completo del nuovo oggetto, incluso l'identificatore univoco assegnato all'oggetto.

### Tipo di contenuto

Questo sarà normalmente `application/json` .

## Corpo della risposta

Il contenuto del corpo della risposta risultante da una richiesta API varia in base all'oggetto, al tipo di elaborazione e all'esito positivo o negativo della richiesta. La risposta viene sempre renderizzata in JSON.

### Oggetto singolo

In base alla richiesta, è possibile restituire un singolo oggetto con un set di campi. Ad esempio, è possibile utilizzare GET per recuperare proprietà selezionate di un cluster utilizzando l'identificatore univoco.

### Oggetti multipli

È possibile restituire più oggetti da una raccolta di risorse. In tutti i casi, viene utilizzato un formato coerente, con `num_records` Indica il numero di record e record contenenti un array delle istanze dell'oggetto. Ad esempio, è possibile recuperare i nodi definiti in un cluster specifico.

### Oggetto di lavoro

Se una chiamata API viene elaborata in modo asincrono, viene restituito un oggetto Job che ancora l'attività in background. Ad esempio, la richiesta PATCH utilizzata per aggiornare la configurazione del cluster viene elaborata in modo asincrono e restituisce un oggetto Job.

### Oggetto di errore

Se si verifica un errore, viene sempre restituito un oggetto Error. Ad esempio, verrà visualizzato un errore quando si tenta di modificare un campo non definito per un cluster.

### Vuoto

In alcuni casi non vengono restituiti dati e il corpo della risposta include un oggetto JSON vuoto.

## Errori

Se si verifica un errore, nel corpo della risposta viene restituito un oggetto errore.

### Formato

Un oggetto errore ha il seguente formato:

```
"error": {
"message": "<string>",
"code": <integer>[,
"target": "<string>"]
}
```

È possibile utilizzare il valore del codice per determinare il tipo o la categoria generale dell'errore e il messaggio per determinare l'errore specifico. Se disponibile, il campo di destinazione include l'input utente specifico associato all'errore.

### Codici di errore comuni

I codici di errore più comuni sono descritti nella tabella seguente. Le chiamate API specifiche possono includere codici di errore aggiuntivi.

| Codice | Descrizione |
|---|---|
| 409 | Esiste già un oggetto con lo stesso identificatore. |
| 400 | Il valore di un campo non è valido o è mancante, oppure è stato fornito un campo aggiuntivo. |
| 400 | L'operazione non è supportata. |
| 405 | Impossibile trovare un oggetto con l'identificatore specificato. |
| 403 | L'autorizzazione a eseguire la richiesta è negata. |
| 409 | La risorsa è in uso. |

# API REST supportate per SnapCenter Server e plug-in

Le risorse disponibili tramite l'API REST SnapCenter sono organizzate in categorie, come mostrato nella pagina della documentazione dell'API SnapCenter . Di seguito viene presentata una breve descrizione di ciascuna risorsa con i relativi percorsi di base, insieme ad ulteriori considerazioni sull'utilizzo, ove opportuno.

## Autenticazione

È possibile utilizzare questa API per accedere al server SnapCenter . Questa API restituisce un token di autorizzazione utente che viene utilizzato per autenticare le richieste successive.

## Domini

È possibile utilizzare le API per eseguire diverse operazioni.

- recupera tutti i domini in SnapCenter
- recuperare i dettagli di un dominio specifico
- registrare o annullare la registrazione di un dominio
- modificare un dominio

## Lavori

È possibile utilizzare le API per eseguire diverse operazioni.

- recupera tutti i lavori in SnapCenter
- recuperare lo stato di un lavoro
- annullare o interrompere un lavoro

## Impostazioni

È possibile utilizzare le API per eseguire diverse operazioni.

- registrare, modificare o rimuovere una credenziale
- visualizza le informazioni sulle credenziali registrate nel server SnapCenter
- configurare le impostazioni di notifica
- recupera informazioni sul server SMTP attualmente configurato per inviare notifiche e-mail e visualizza il nome del server SMTP, il nome dei destinatari e il nome del mittente
- visualizza la configurazione dell'autenticazione a più fattori (MFA) dell'accesso al server SnapCenter
- abilitare o disabilitare e configurare MFA per l'accesso a SnapCenter Server
- creare il file di configurazione necessario per impostare MFA

## Ospiti

È possibile utilizzare le API per eseguire diverse operazioni.

- interroga tutti gli host SnapCenter

- rimuovere uno o più host da SnapCenter
- recuperare un host per nome
- recuperare tutte le risorse su un host
- recuperare una risorsa utilizzando l'ID della risorsa
- recuperare i dettagli di configurazione del plug-in
- configurare l'host del plug-in
- recupera tutte le risorse del plug-in per l'host Microsoft SQL Server
- recupera tutte le risorse del plug-in per l'host del database Oracle
- recupera tutte le risorse del plug-in per l'host dell'applicazione personalizzata
- recupera tutte le risorse del plug-in per l'host SAP HANA
- recuperare i plug-in installati
- installare i plug-in su un host esistente
- aggiorna il pacchetto host
- rimuovere i plug-in da un host esistente
- aggiungere plug-in su un host
- aggiungi o modifica l'host
- ottenere la firma dell'host Linux
- registrare la firma dell'host Linux
- mettere l'host in modalità di manutenzione o produzione
- avviare o riavviare i servizi plug-in sull'host
- rinominare un host

## Risorse

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutte le risorse
- recuperare una risorsa utilizzando l'ID della risorsa
- recupera tutte le risorse del plug-in per l'host Microsoft SQL Server
- recupera tutte le risorse del plug-in per l'host del database Oracle
- recupera tutte le risorse del plug-in per l'host dell'applicazione personalizzata
- recupera tutte le risorse del plug-in per l'host SAP HANA
- recuperare una risorsa di Microsoft SQL Server utilizzando una chiave
- recuperare una risorsa personalizzata utilizzando una chiave
- modificare una risorsa del plug-in per l'host dell'applicazione personalizzata
- rimuovere una risorsa del plug-in per l'host dell'applicazione personalizzata utilizzando una chiave
- recuperare una risorsa SAP HANA utilizzando una chiave
- modificare una risorsa del plug-in per l'host SAP HANA
- rimuovere una risorsa del plug-in per l'host SAP HANA utilizzando una chiave

- recuperare una risorsa Oracle utilizzando una chiave
- creare una risorsa di volume dell'applicazione Oracle
- modificare una risorsa del volume dell'applicazione Oracle
- rimuovere una risorsa del volume dell'applicazione Oracle utilizzando una chiave
- recuperare i dettagli secondari della risorsa Oracle
- eseguire il backup della risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- eseguire il backup della risorsa Oracle utilizzando il plug-in per il database Oracle
- eseguire il backup della risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- configurare il database SAP HANA
- configurare il database Oracle
- ripristinare un backup del database SQL
- ripristinare un backup del database Oracle
- ripristinare un backup di un'applicazione personalizzata
- creare una risorsa SAP HANA
- proteggere una risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- proteggere una risorsa di Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- modificare una risorsa protetta di Microsoft SQL Server
- rimuovere la protezione per la risorsa Microsoft SQL Server
- proteggere una risorsa Oracle utilizzando il plug-in per il database Oracle
- modificare una risorsa Oracle protetta
- rimuovere la protezione dalla risorsa Oracle
- clonare una risorsa dal backup utilizzando il plug-in per l'applicazione personalizzata
- clonare un volume di un'applicazione Oracle dal backup utilizzando il plug-in per il database Oracle
- clonare una risorsa di Microsoft SQL Server dal backup utilizzando il plug-in per Microsoft SQL Server
- creare un ciclo di vita clone di una risorsa Microsoft SQL Server
- modificare il ciclo di vita del clone di una risorsa di Microsoft SQL Server
- elimina il ciclo di vita del clone di una risorsa di Microsoft SQL Server
- spostare un database Microsoft SQL Server esistente da un disco locale a una LUN NetApp
- creare un file di specifiche clone per un database Oracle
- avviare un processo di aggiornamento del clone su richiesta di una risorsa Oracle
- creare una risorsa Oracle dal backup utilizzando il file di specifica del clone
- ripristina il database nella replica secondaria e lo unisce nuovamente al gruppo di disponibilità
- creare una risorsa di volume dell'applicazione Oracle

## Backup

È possibile utilizzare le API per eseguire diverse operazioni.

- recupera i dettagli del backup in base al nome del backup, al tipo, al plug-in, alla risorsa o alla data

- recuperare tutti i backup
- recuperare i dettagli del backup
- rinominare o eliminare i backup
- montare un backup Oracle
- smontare un backup Oracle
- catalogare un backup di Oracle
- decatalogare un backup Oracle
- ottenere tutti i backup necessari per essere montati per eseguire il ripristino point-in-time

## Cloni

È possibile utilizzare le API per eseguire diverse operazioni.

- creare, visualizzare, modificare ed eliminare il file di specifica del clone del database Oracle
- visualizza la gerarchia dei cloni del database Oracle
- recuperare i dettagli del clone
- recuperare tutti i cloni
- eliminare i cloni
- recupera i dettagli del clone tramite ID
- avviare un processo di aggiornamento del clone su richiesta di una risorsa Oracle
- clonare una risorsa Oracle dal backup utilizzando il file di specifica del clone

## Clone diviso

È possibile utilizzare le API per eseguire diverse operazioni.

- stimare l'operazione di divisione del clone della risorsa clonata
- recuperare lo stato di un'operazione di divisione del clone
- avviare o interrompere un'operazione di divisione del clone

## Gruppi di risorse

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di tutti i gruppi di risorse
- recupera il gruppo di risorse per nome
- creare un gruppo di risorse per il plug-in per l'applicazione personalizzata
- creare un gruppo di risorse per il plug-in per Microsoft SQL Server
- creare un gruppo di risorse per il plug-in per il database Oracle
- modificare un gruppo di risorse per il plug-in per l'applicazione personalizzata
- modificare un gruppo di risorse per il plug-in per Microsoft SQL Server
- modificare un gruppo di risorse per il plug-in per il database Oracle

- creare, modificare o eliminare il ciclo di vita del clone di un gruppo di risorse per il plug-in per Microsoft SQL Server
- eseguire il backup di un gruppo di risorse
- mettere il gruppo di risorse in modalità di manutenzione o produzione
- rimuovere un gruppo di risorse

## Politiche

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli della polizza
- recupera i dettagli della polizza per nome
- eliminare una policy
- creare una copia di una policy esistente
- creare o modificare la policy per il plug-in per l'applicazione personalizzata
- creare o modificare i criteri per il plug-in per Microsoft SQL Server
- creare o modificare la policy per il plug-in per il database Oracle
- creare o modificare la policy per il plug-in per il database SAP HANA

## Magazzinaggio

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutte le azioni
- recuperare una condivisione per nome
- creare o eliminare una condivisione
- recuperare i dettagli di archiviazione
- recupera i dettagli di archiviazione per nome
- creare, modificare o eliminare un archivio
- scoprire le risorse su un cluster di archiviazione
- recuperare risorse su un cluster di archiviazione

## Condividere

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di una quota
- recuperare i dettagli di tutte le azioni
- creare o eliminare una condivisione sullo storage
- recuperare una condivisione per nome

## Plugin

È possibile utilizzare le API per eseguire diverse operazioni.

- elenca tutti i plug-in per un host
- recuperare una risorsa di Microsoft SQL Server utilizzando una chiave
- modificare una risorsa personalizzata utilizzando una chiave
- rimuovere una risorsa personalizzata utilizzando una chiave
- recuperare una risorsa SAP HANA utilizzando una chiave
- modificare una risorsa SAP HANA utilizzando una chiave
- rimuovere una risorsa SAP HANA utilizzando una chiave
- recuperare una risorsa Oracle utilizzando una chiave
- modificare una risorsa del volume dell'applicazione Oracle utilizzando una chiave
- rimuovere una risorsa del volume dell'applicazione Oracle utilizzando una chiave
- eseguire il backup della risorsa Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server e una chiave
- eseguire il backup della risorsa Oracle utilizzando il plug-in per il database Oracle e una chiave
- eseguire il backup della risorsa dell'applicazione personalizzata utilizzando il plug-in per l'applicazione personalizzata e una chiave
- configurare il database SAP HANA utilizzando una chiave
- configurare il database Oracle utilizzando una chiave
- ripristinare un backup di un'applicazione personalizzata utilizzando una chiave
- creare una risorsa SAP HANA
- creare una risorsa di volume dell'applicazione Oracle
- proteggere una risorsa personalizzata utilizzando il plug-in per l'applicazione personalizzata
- proteggere una risorsa di Microsoft SQL Server utilizzando il plug-in per Microsoft SQL Server
- modificare una risorsa protetta di Microsoft SQL Server
- rimuovere la protezione per la risorsa Microsoft SQL Server
- proteggere una risorsa Oracle utilizzando il plug-in per il database Oracle
- modificare una risorsa Oracle protetta
- rimuovere la protezione dalla risorsa Oracle
- clonare una risorsa dal backup utilizzando il plug-in per l'applicazione personalizzata
- clonare un volume di un'applicazione Oracle dal backup utilizzando il plug-in per il database Oracle
- clonare una risorsa di Microsoft SQL Server dal backup utilizzando il plug-in per Microsoft SQL Server
- creare un ciclo di vita clone di una risorsa Microsoft SQL Server
- modificare il ciclo di vita del clone di una risorsa di Microsoft SQL Server
- elimina il ciclo di vita del clone di una risorsa di Microsoft SQL Server
- creare un file di specifiche clone per un database Oracle
- avviare un ciclo di vita di clonazione su richiesta di una risorsa Oracle
- clonare una risorsa Oracle dal backup utilizzando il file di specifica del clone

## Rapporti

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare report di operazioni di backup, ripristino e clonazione per i rispettivi plug-in
- aggiungere, eseguire, eliminare o modificare le pianificazioni
- recuperare i dati per i report pianificati

## Avvisi

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare tutti gli avvisi
- recuperare gli avvisi tramite ID
- elimina più avvisi o elimina un avviso per ID

## Rbac

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i dettagli di utenti, gruppi e ruoli
- aggiungere o eliminare utenti
- assegnare l'utente al ruolo
- rimuovere l'assegnazione dell'utente dal ruolo
- creare, modificare o eliminare ruoli
- assegnare un gruppo a un ruolo
- annullare l'assegnazione di un gruppo a un ruolo
- aggiungere o eliminare gruppi
- creare una copia di un ruolo esistente
- assegnare o annullare l'assegnazione di risorse all'utente o al gruppo

## Configurazione

È possibile utilizzare le API per eseguire diverse operazioni.

- visualizzare le impostazioni di configurazione
- modificare le impostazioni di configurazione

## Impostazioni del certificato

È possibile utilizzare le API per eseguire diverse operazioni.

- visualizzare lo stato del certificato per SnapCenter Server o per l'host del plug-in
- modificare le impostazioni del certificato per SnapCenter Server o l'host del plug-in

### Deposito

È possibile utilizzare le API per eseguire diverse operazioni.

- recuperare i backup del repository
- visualizzare le informazioni di configurazione sul repository
- proteggere e ripristinare il repository SnapCenter
- rimuovere la protezione dal repository SnapCenter
- ricostruire ed eseguire il failover del repository

### Versione

È possibile utilizzare questa API per visualizzare la versione SnapCenter .

# Come accedere alle API REST utilizzando la pagina web dell'API Swagger

Le API REST sono accessibili tramite la pagina web Swagger. È possibile accedere alla pagina web di Swagger per visualizzare le API REST di SnapCenter Server, nonché per emettere manualmente una chiamata API. È possibile utilizzare le API REST per gestire SnapCenter Server o per eseguire operazioni di protezione dei dati.

È necessario conoscere l'indirizzo IP di gestione o il nome di dominio del server SnapCenter su cui si desidera eseguire le API REST.

Non sono necessarie autorizzazioni speciali per eseguire il client REST API. Qualsiasi utente può accedere alla pagina web di Swagger. Le rispettive autorizzazioni sugli oggetti a cui si accede tramite l'API REST si basano sull'utente che genera il token per accedere all'API REST.

**Passi**

1. Da un browser, immettere l'URL per accedere alla pagina Web di Swagger nel formato *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/swagger/*.

   Assicurarsi che l'URL dell'API REST non contenga i seguenti caratteri: +, ., % e &.

2. Nel campo **Swagger Explore**, se la documentazione dell'API Swagger non viene visualizzata automaticamente, digitare: *https://<SnapCenter_IP_address_or_name>:<SnapCenter_port>/Content/swagger/ SnapCenter.yaml*
3. Fare clic su **Esplora**.

   Viene visualizzato un elenco di tipi o categorie di risorse API.

4. Fare clic su un tipo di risorsa API per visualizzare le API in quel tipo di risorsa.

Se si verifica un comportamento imprevisto durante l'esecuzione delle API REST SnapCenter , è possibile utilizzare i file di registro per identificare la causa e risolvere il problema. È possibile scaricare i file di registro dall'interfaccia utente di SnapCenter facendo clic su **Monitor** > **Registri** > **Scarica**.

# Inizia con l'API REST

Puoi iniziare subito a utilizzare l'API REST SnapCenter . L'accesso all'API fornisce una prospettiva prima di iniziare a utilizzarla con i processi di flusso di lavoro più complessi su una configurazione live.

## Ciao mondo

Puoi eseguire un semplice comando sul tuo sistema per iniziare a utilizzare l'API REST SnapCenter e verificarne la disponibilità.

**Prima di iniziare**

- Assicurati che l'utilità Curl sia disponibile sul tuo sistema.
- Indirizzo IP o nome host del server SnapCenter
- Nome utente e password per un account autorizzato ad accedere all'API REST SnapCenter .

> Se le tue credenziali includono caratteri speciali, devi formattarli in un modo che sia accettabile per Curl in base alla shell che stai utilizzando. Ad esempio, è possibile inserire una barra rovesciata prima di ogni carattere speciale o racchiudere l'intero `username:password` stringa tra virgolette singole.

**Fare un passo**

Nell'interfaccia della riga di comando, eseguire quanto segue per recuperare le informazioni sul plug-in:

```
curl -X GET -u username:password -k
"https://<ip_address>/api/hosts?fields=IncludePluginInfo"
```

Esempio:

```
curl -X GET -u admin:password -k
"'https://10.225.87.97/api/hosts?fields=IncludePluginInfo"
```

# Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

## Copyright

"https://www.netapp.com/company/legal/copyright/"

## Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

"https://www.netapp.com/company/legal/trademarks/"

## Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Politica sulla riservatezza

"https://www.netapp.com/company/legal/privacy-policy/"

## Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

"Avviso per SnapCenter 6.1"

**Informazioni sul copyright**

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

**Informazioni sul marchio commerciale**

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.