Documentazione software SolidFire ed Element

Element Software

NetApp
March 05, 2025

This PDF was generated from https://docs.netapp.com/it-it/element-software-123/index.html on March 05, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione software SolidFire ed Element . . . 1
Informazioni sulla release corrente e precedente . . . 2
- Software NetApp Element . . . 2
- Servizi di gestione . . . 2
- Plug-in NetApp Element per server vCenter . . . 2
- Firmware dello storage . . . 3
- Trova ulteriori informazioni . . . 3
- Novità . . . 3
  - NetApp Bugs Online contiene problemi noti e risolti . . . 3
  - Elemento 12.3.2 . . . 4
  - Elemento 12.3.1 . . . 4
  - Supporto per la valutazione dinamica dei nodi della CPU per le piattaforme host SolidFire eSDS . . . 5
  - Elemento 12.3 . . . 5

Concetti . . . 8
- Trova ulteriori informazioni . . . 8
- Panoramica del prodotto . . . 8
  - Funzionalità di SolidFire . . . 8
  - Implementazione di SolidFire . . . 8
  - Trova ulteriori informazioni . . . 9
- Panoramica dell’architettura di SolidFire . . . 9
  - URL comuni . . . 10
  - Trova ulteriori informazioni . . . 11
  - Interfacce software SolidFire . . . 11
  - SolidFire Active IQ . . . 13
  - Nodo di gestione per software Element . . . 13
  - Servizi di gestione per lo storage all-flash SolidFire . . . 14
- Nodi . . . 14
  - Nodo di gestione . . . 14
  - Nodo storage . . . 14
  - Nodo Fibre Channel . . . 15
  - stato operativo del nodo . . . 15
  - Trova ulteriori informazioni . . . 16
- Cluster . . . 16
  - Cluster di storage autorevoli . . . 16
  - Regola dei terzi . . . 17
  - Capacità inutilizzata . . . 17
  - Efficienza dello storage . . . 17
  - Quorum del cluster di storage . . . 18
- Sicurezza . . . 18
  - Crittografia a riposo (hardware) . . . 18
  - Crittografia a riposo (software) . . . 18
  - Gestione esterna delle chiavi . . . 18
  - Autenticazione a più fattori . . . 19

FIPS 140-2 per HTTPS e crittografia dei dati a riposo 19
Per ulteriori informazioni 19
Account e permessi 19
Account amministratore del cluster di storage 20
Account utente 20
Account utente del cluster autorevoli 20
Account di volume 21
Storage 21
Volumi 21
Volumi virtuali (vVol) 22
Gruppi di accesso ai volumi 23
Iniziatori 24
Protezione dei dati 24
Tipi di replica remota 24
Snapshot dei volumi per la protezione dei dati 26
Cloni di volume 26
Panoramica del processo di backup e ripristino per lo storage Element 27
Domini di protezione 27
Domini di protezione personalizzati 27
Doppia Helix ad alta disponibilità 28
Performance e qualità del servizio 28
Parametri della qualità del servizio 28
Limiti del valore QoS 29
Performance QoS 30
Policy di QoS 31
Trova ulteriori informazioni 31
Requisiti 32
Trova ulteriori informazioni 32
Networking 32
Per ulteriori informazioni 32
Configurazione dello switch per i cluster che eseguono il software Element 32
Per ulteriori informazioni 34
Requisiti delle porte di rete 34
Per ulteriori informazioni 37
Provalo 38
Trova ulteriori informazioni 38
Prova le funzionalità di storage utilizzando Element Demo Node 38
Funzionalità supportate: 38
Requisiti delle macchine virtuali 39
Requisiti dell'host 39
Nodo demo elemento di download 39
Installare Element Demo Node su VMware ESXi 39
Come ottenere supporto 40
Trova ulteriori informazioni 40
Installazione e manutenzione dell'hardware 41

Trova ulteriori informazioni . . . 41
Informazioni sull'hardware H410S e H610S . . . 41
Trova ulteriori informazioni . . . 41
Installare nodi storage H-Series . . . 41
Sostituire un nodo H410S . . . 51
Sostituire un nodo H610S . . . 55
Sostituire i dischi . . . 57
Sostituire un alimentatore . . . 61
Informazioni sull'hardware della serie SF . . . 63
Trova ulteriori informazioni . . . 64
Sostituire uno chassis . . . 64
Sostituire le unità per i nodi di storage della serie SF . . . 66
Sostituire un alimentatore . . . 70
Tornare alle informazioni immagine di fabbrica . . . 71
Configurare RTFI . . . 71
Il processo RTFI . . . 72
Menu delle opzioni RTFI . . . 75
Panoramica dell'installazione . . . 78
Trova ulteriori informazioni . . . 78
Configurazione di un cluster con nodi storage Element . . . 78
Trova ulteriori informazioni . . . 79
Configurare un nodo di storage . . . 79
Creare un cluster di storage . . . 81
Accedere all'interfaccia utente del software Element . . . 83
Aggiungere dischi a un cluster . . . 83
Configurare un cluster con nodi Fibre Channel . . . 84
Configurare un nodo Fibre Channel . . . 84
Creare un nuovo cluster con nodi Fibre Channel . . . 85
Aggiunta di nodi Fibre Channel a un cluster . . . 86
Impostare le zone per i nodi Fibre Channel . . . 86
Creare un gruppo di accesso al volume per i client Fibre Channel . . . 87
Determinare quali componenti di SolidFire installare . . . 87
Per ulteriori informazioni . . . 88
Configurare un nodo di gestione . . . 88
Trova ulteriori informazioni . . . 88
Configurare l'accesso completo all'interfaccia utente Web Domain Name . . . 88
Configurare l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control . . . 89
Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST . . . 90
Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control . . . 91
Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST . . . 91
Risoluzione dei problemi . . . 92
Trova ulteriori informazioni . . . 93
Cosa succederà . . . 93
Trova ulteriori informazioni . . . 93
Gestire lo storage con il software Element . . . 94

Trova ulteriori informazioni . . . 94
Accedere all'interfaccia utente del software Element . . . 94
Trova ulteriori informazioni . . . 95
Configurare le opzioni del sistema SolidFire dopo l'implementazione . . . 95
Trova ulteriori informazioni . . . 95
Modificare le credenziali in NetApp HCI e NetApp SolidFire . . . 95
Modificare il certificato SSL predefinito del software Element . . . 99
Modificare la password IPMI predefinita per i nodi . . . 100
Utilizzare le opzioni di base nell'interfaccia utente del software Element . . . 102
Per ulteriori informazioni . . . 102
Visualizzare l'attività API . . . 102
Icone nell'interfaccia degli elementi . . . 103
Fornire un feedback . . . 104
Gestire gli account . . . 104
Per ulteriori informazioni . . . 105
Utilizzare gli account con CHAP . . . 105
Gestire gli account utente degli amministratori del cluster . . . 107
Gestire il sistema . . . 118
Per ulteriori informazioni . . . 119
Abilitare l'autenticazione a più fattori . . . 119
Configurare le impostazioni del cluster . . . 120
Creare un cluster che supporti i dischi FIPS . . . 136
Abilitare FIPS 140-2 per HTTPS sul cluster . . . 139
Inizia a utilizzare la gestione esterna delle chiavi . . . 141
Gestire volumi e volumi virtuali . . . 146
Per ulteriori informazioni . . . 146
Lavorare con i volumi . . . 147
Lavorare con volumi virtuali . . . 156
Lavorare con gli iniziatori e i gruppi di accesso ai volumi . . . 165
Proteggi i tuoi dati . . . 173
Per ulteriori informazioni . . . 174
Utilizzare le snapshot dei volumi per la protezione dei dati . . . 174
Eseguire la replica remota tra cluster che eseguono il software NetApp Element . . . 187
Utilizzare la replica SnapMirror tra cluster Element e ONTAP . . . 202
Backup e ripristino dei volumi . . . 214
Risolvere i problemi del sistema . . . 218
Per ulteriori informazioni . . . 219
Visualizza informazioni sugli eventi di sistema . . . 219
Visualizzare lo stato delle attività in esecuzione . . . 222
Visualizzare gli avvisi di sistema . . . 223
Visualizzare l'attività delle performance dei nodi . . . 240
Visualizza le performance dei volumi . . . 240
Visualizzare le sessioni iSCSI . . . 242
Visualizzare le sessioni Fibre Channel . . . 244
Risolvere i problemi relativi ai dischi . . . 245

Risolvere i problemi dei nodi . . . 248
Utilizzo di utility per nodo per nodi di storage . . . 249
Comprendere i livelli di completezza del cluster . . . 256
Gestione e monitoraggio dello storage con NetApp Hybrid Cloud Control . . . 259
Aggiungi e gestisci cluster di storage utilizzando NetApp Hybrid Cloud Control . . . 259
Aggiungere un cluster di storage . . . 260
Confermare lo stato del cluster di storage . . . 260
Modificare le credenziali del cluster di storage . . . 260
Rimuovere un cluster di storage . . . 261
Attiva e disattiva la modalità di manutenzione . . . 261
Creare e gestire gli account utente utilizzando NetApp Hybrid Cloud Control . . . 263
Attivare LDAP . . . 263
Gestire gli account cluster autorevoli . . . 264
Gestire gli account dei volumi . . . 265
Crea e gestisci i volumi utilizzando NetApp Hybrid Cloud Control . . . 267
Creare un volume . . . 267
Applicare un criterio QoS a un volume . . . 269
Modificare un volume . . . 269
Clonare i volumi . . . 270
Aggiungere volumi a un gruppo di accesso al volume . . . 272
Eliminare un volume . . . 272
Ripristinare un volume cancellato . . . 273
Eliminare un volume cancellato . . . 273
Creare e gestire i gruppi di accesso ai volumi . . . 274
Aggiungere un gruppo di accesso al volume . . . 274
Modificare un gruppo di accesso al volume . . . 274
Eliminare un gruppo di accesso al volume . . . 275
Creare e gestire gli iniziatori . . . 275
Creare un iniziatore . . . 276
Aggiungere gli iniziatori a un gruppo di accesso al volume . . . 277
Modificare un alias iniziatore . . . 277
Eliminare gli iniziatori . . . 278
Creare e gestire policy di QoS per volumi . . . 278
Creare una policy QoS . . . 279
Applicare un criterio QoS a un volume . . . 279
Modificare l’assegnazione del criterio QoS di un volume . . . 280
Modificare un criterio QoS . . . 280
Eliminare una policy QoS . . . 281
Monitorate il vostro sistema SolidFire con il controllo del cloud ibrido NetApp . . . 281
Monitorare le risorse di storage sul pannello di controllo del cloud ibrido . . . 281
Visualizzare l’inventario nella pagina nodi . . . 286
Monitorare i volumi nel cluster di storage . . . 288
Raccogliere i registri per la risoluzione dei problemi . . . 289
Gestire lo storage con Element API . . . 294
Trova ulteriori informazioni . . . 294

Informazioni sull'API del software Element . . . 295
Trova ulteriori informazioni . . . 295
Richiedi membri dell'oggetto . . . 295
Membri dell'oggetto di risposta . . . 296
Endpoint della richiesta . . . 297
Autenticazione API . . . 297
Metodi asincroni . . . 298
Attributi . . . 298
Oggetti comuni . . . 299
Trova ulteriori informazioni . . . 302
account . . . 302
AuthSessionInfo . . . 303
BulkVolumeJob . . . 305
binding (volumi virtuali) . . . 306
CertificateDettagli . . . 307
cluster . . . 307
ClusterAdmin . . . 309
Capacità del clusterCapacity . . . 310
Clusterconfig . . . 313
ClusterInfo . . . 314
ClusterPair . . . 316
ClusterStats . . . 317
Struttura del clusterStructure . . . 319
disco . . . 320
DriveStats . . . 323
errore . . . 325
evento . . . 325
guasto . . . 327
FiberChannelPort . . . 329
FipsErrorNodeReport . . . 331
FipsNodeReport . . . 331
FipsReport . . . 332
GroupSnapshot . . . 332
HardwareInfo . . . 334
host (volumi virtuali) . . . 336
IdpConfigInfo . . . 336
iniziatore . . . 337
KeyProviderKmip . . . 338
KeyServerKmip . . . 339
LdapConfiguration . . . 341
Server di loggingServer . . . 342
rete (interfacce collegate) . . . 343
rete (tutte le interfacce) . . . 347
Rete (interfacce Ethernet) . . . 348
rete (interfacce locali) . . . 350

Rete (SNMP) . . . 352
NetworkInterface . . . 353
NetworkInterfaceStats . . . 353
nodo . . . 355
NodeProtectionDomini . . . 357
NodeStats . . . 357
OntapVersionInfo . . . 359
PendingActiveNode . . . 360
PendingNode . . . 361
Protection Domain (dominio di protezione) . . . 363
ProtectionDomainLevel . . . 364
ProtectionDomainResiliency . . . 365
ProtectionDomainTolerance . . . 365
ProtectionSchemeResiliency . . . 366
ProtectionSchemeTolerance . . . 367
ProtocolEndpoint . . . 367
QoS . . . 368
QoSPolicy . . . 369
RemoteClusterSnapshotStatus . . . 370
pianificazione . . . 371
Sessione (Fibre Channel) . . . 374
Sessione (iSCSI) . . . 375
SnapMirrorAggregate . . . 378
SnapMirrorClusterIdentity . . . 378
SnapMirrorEndpoint . . . 379
SnapMirrorJobScheduleCronInfo . . . 380
SnapMirrorLunInfo . . . 380
SnapMirrorNetworkInterface . . . 381
SnapMirrorNode . . . 382
SnapMirrorPolicy . . . 383
SnapMirrorPolicyRule . . . 384
SnapMirrorRelationship . . . 385
SnapMirrorVolume . . . 388
SnapMirrorVolumeInfo . . . 389
SnapMirrorVserver . . . 389
SnapMirrorVserverAggregateInfo . . . 391
snapshot . . . 391
SnmpTrapRecipient . . . 394
StorageContainer . . . 395
SyncJob . . . 396
task (volumi virtuali) . . . 398
UsmUser . . . 401
VirtualNetwork . . . 401
VirtualVolume . . . 403
volume . . . 404

VolumeAccessGroup . . . 408
VolumePair . . . 409
VolumeStats . . . 410
Metodi comuni . . . 416
Trova ulteriori informazioni . . . 417
GetAPI . . . 417
GetAsyncResult . . . 425
GetCompleteStats . . . 429
GetLimits . . . 429
GetOrigin . . . 432
GetRawStats . . . 433
ListAsyncResults . . . 433
Metodi API dell'account . . . 436
Trova ulteriori informazioni . . . 436
AddAccount . . . 436
GetAccountByID . . . 439
GetAccountByName . . . 440
GetAccountEfficiency . . . 442
ListAccounts . . . 443
ModifyAccount . . . 446
RemoveAccount . . . 448
Metodi API dell'amministratore . . . 449
Trova ulteriori informazioni . . . 450
AddClusterAdmin . . . 450
GetCurrentClusterAdmin . . . 452
GetLoginBanner . . . 453
ListClusterAdmins . . . 455
ModifyClusterAdmin . . . 458
RemoveClusterAdmin . . . 459
SetLoginBanner . . . 460
Metodi API del cluster . . . 463
Trova ulteriori informazioni . . . 464
AddNode . . . 464
ClearClusterFaults . . . 467
CreateClusterInterfacePreference . . . 469
DeleteClusterInterfacePreference . . . 470
EnableFeature . . . 471
GetClusterCapacity . . . 473
GetClusterFullThreshold . . . 475
GetClusterHardwareInfo . . . 481
GetClusterInfo . . . 483
GetClusterInterfacePreference . . . 485
GetClusterMasterNodeID . . . 486
GetClusterStats . . . 487
GetClusterVersionInfo . . . 488

GetFeatureStatus . . . 492
GetLoginSessionInfo . . . 494
GetNodeHardwareInfo . . . 495
GetNodeStats . . . 497
ListActiveNode . . . 498
ListAllNode . . . 499
ListClusterFaults . . . 501
ListClusterInterfacePreferences . . . 505
ListEvents . . . 506
ListNodeStats . . . 509
ListISCSISessions . . . 510
ListServices . . . 512
ListPendingNode . . . 515
ListPendingActiveNode . . . 517
ModifyClusterFullThreshold . . . 518
ModifyClusterInterfacePreference . . . 525
RemoveNode . . . 526
SetLoginSessionInfo . . . 528
Spegnere . . . 530
Metodi API per la creazione di cluster . . . 531
Trova ulteriori informazioni . . . 531
CheckProposedCluster . . . 531
CreateCluster . . . 533
GetBootstrapConfig . . . 536
Metodi API del disco . . . 540
Trova ulteriori informazioni . . . 540
AddDrive . . . 540
GetDriveHardwareInfo . . . 542
GetDriveStats . . . 544
ListDrive . . . 547
ListDriveStats . . . 549
RemoveDrives . . . 551
SecureEraseDrive . . . 553
Metodi API Fibre Channel . . . 554
Trova ulteriori informazioni . . . 555
GetVolumeAccessGroupLunAssignments . . . 555
ListFiberChannelPortInfo . . . 556
ListFiberChannelSessions . . . 560
ListNodeFibreChannelPortInfo . . . 561
ModifyVolumeAccessGroupLunAssignments . . . 563
Metodi API initiator . . . 565
Trova ulteriori informazioni . . . 566
CreateInitiator . . . 566
DeleteInitiator . . . 570
ListInitiator . . . 571

ModifyInitiator . . . 573
Metodi API LDAP . . . 577
Trova ulteriori informazioni . . . 578
AddLdapClusterAdmin . . . 578
EnableLdapAuthentication . . . 579
DisableLdapAuthentication . . . 584
GetLdapConfiguration . . . 585
TestLdapAuthentication . . . 587
Metodi API di autenticazione a più fattori . . . 589
Trova ulteriori informazioni . . . 589
AddIdpClusterAdmin . . . 589
CreateIdpConfiguration . . . 592
DeleteAuthSession . . . 594
DeleteAuthSessionsByClusterAdmin . . . 595
DeleteAuthSessionsByNomeUtente . . . 597
DeleteIdpConfiguration (Configurazione DeleteIdp) . . . 599
DisableIdpAuthentication . . . 601
EnableIdpAuthentication . . . 601
GetIdpAuthenticationState . . . 603
ListActiveAuthSessions . . . 603
ListIdpconfigurazioni . . . 605
UpdateIdpConfiguration . . . 606
Metodi API per l'autenticazione della sessione . . . 609
Trova ulteriori informazioni . . . 609
ListAuthSessionsByClusterAdmin . . . 609
ListAuthSessionsByNomeUtente . . . 611
Metodi API del nodo . . . 613
Trova ulteriori informazioni . . . 615
CheckPingOnVlan . . . 615
CheckProposedNodeAdditions . . . 618
CreateClusterSupportBundle . . . 621
CreateSupportBundle . . . 624
DeleteAllSupportBundles . . . 627
DisableMaintenanceMode . . . 627
DisableSsh . . . 630
EnableMaintenanceMode . . . 631
EnableSsh . . . 634
GetClusterConfig . . . 635
GetClusterState . . . 636
GetConfig . . . 638
GetDriveConfig . . . 639
GetHardwareConfig . . . 641
GetHardwareInfo . . . 643
GetIpmiConfig . . . 645
GetIpmiInfo . . . 650

GetNetworkConfig . . . 653
Interfaccia GetNetworkInterface . . . 654
GetNodeActiveTlsCiphers . . . 658
GetNodeFipsDrivesReport . . . 659
GetNodeSSLCertificate . . . 660
GetNodeSupportedTlsCiphers . . . 662
GetPatchInfo . . . 664
GetPendingOperation . . . 666
GetSshInfo . . . 667
ListDrivehardware . . . 668
ListNetworkInterfaces . . . 671
ListNetworkInterfaceStats . . . 673
ListTest . . . 675
ListUtilities . . . 676
RemoveNodeSSLCertificate . . . 677
ResetDrive . . . 678
ResetNode . . . 680
ResetNodeSupplementalTlsCiphers . . . 683
Restart Networking (Ripristino rete) . . . 683
RestartServices . . . 684
SetClusterConfig . . . 686
SetConfig . . . 688
SetNetworkConfig . . . 690
SetNodeSSLCertificate . . . 692
SetNodeSupplementalTlsCiphers . . . 695
Spegnere . . . 696
TestConnectEnsemble . . . 698
TestConnectMvip . . . 699
TestConnectSvip . . . 704
TestDrive . . . 709
TestHardwareConfig . . . 710
TestLocateCluster . . . 712
TestLocalConnectivity . . . 713
TestNetworkConfig . . . 716
Test Ping . . . 718
TestRemoteConnectivity . . . 722
Metodi API di replica . . . 724
Trova ulteriori informazioni . . . 725
Ordine delle operazioni di abbinamento dei cluster . . . 725
Ordine delle operazioni di abbinamento dei volumi . . . 726
Modalità di replica supportate per i cluster accoppiati . . . 726
CompleteClusterPairing . . . 726
CompleteVolumePairing . . . 728
ListClusterPairs . . . 729
ListActivePairedVolumes . . . 731

ModifyVolumePair . . . 734
RemoveClusterPair . . . 736
RemoveVolumePair . . . 737
StartClusterPairing . . . 738
StartVolumePairing . . . 739
Metodi API di sicurezza . . . 743
Trova ulteriori informazioni . . . 743
AddKeyServerToProviderKmip . . . 743
CreateKeyProviderKmip . . . 745
CreateKeyServerKmip . . . 746
CreatePublicPrivateKeyPair . . . 749
DeleteKeyProviderKmip . . . 751
DeleteKeyServerKmip . . . 752
DisableEncryptionAtRest . . . 753
EnableEncryptionAtRest . . . 754
GetClientCertificateSignRequest . . . 756
GetKeyProviderKmip . . . 757
GetKeyServerKmip . . . 759
GetSoftwareEncryptionAtRestInfo . . . 760
ListKeyProvidersKmip . . . 762
ListKeyServerKmip . . . 765
ModifyKeyServerKmip . . . 768
RekeySoftwareEncryptionAtRestMasterKey . . . 771
RemoveKeyServerFromProviderKmip . . . 773
TestKeyProviderKmip . . . 774
TestKeyServerKmip . . . 775
Metodi API di SnapMirror . . . 776
Trova ulteriori informazioni . . . 777
AbortSnapMirrorRelationship . . . 777
BreakSnapMirrorRelationship . . . 778
BreakSnapMirrorVolume . . . 779
CreateSnapMirrorEndpoint . . . 781
CreateSnapMirrorEndpointUnmanaged . . . 782
CreateSnapMirrorRelationship . . . 782
CreateSnapMirrorVolume . . . 784
DeleteSnapMirrorEndpoint . . . 786
DeleteSnapMirrorRelationships . . . 786
GetOntapVersionInfo . . . 787
GetSnapMirrorClusterIdentity . . . 788
InitializeSnapMirrorRelationship . . . 788
ListSnapMirrorAggregates . . . 789
ListSnapMirrorEndpoint . . . 790
ListSnapMirrorLun . . . 791
ListSnapMirrorNetworkInterfaces . . . 792
ListSnapMirrorNode . . . 792

ListSnapMirrorPolicies . . . 793
ListSnapMirrorSchedules . . . 794
ListSnapMirrorRelationships . . . 794
ListSnapMirrorVolumes . . . 796
ListSnapMirrorVservers . . . 797
ModifySnapMirrorEndpoint . . . 798
ModifySnapMirrorEndpoint (non gestito) . . . 799
ModifySnapMirrorRelationship . . . 799
UpdateSnapMirrorRelationship . . . 801
QuiesceSnapMirrorRelationship . . . 802
ResumeSnapMirrorRelationship . . . 803
ResyncSnapMirrorRelationship . . . 803
Metodi API di configurazione del sistema . . . 805
Trova ulteriori informazioni . . . 806
DisableBmcColdReset . . . 806
DisableClusterSsh . . . 807
DisableSnmp . . . 808
EnableBmcColdReset . . . 809
EnableClusterSsh . . . 810
EnableSnmp . . . 812
Proprietà GetBinAssignment . . . 813
GetClusterSshInfo . . . 816
GetClusterStructure . . . 817
GetFipsReport . . . 818
GetLldpConfig . . . 820
GetLldpInfo . . . 821
GetNodeFipsDrivesReport . . . 822
GetNtpInfo . . . 823
GetNvramInfo . . . 825
GetProtectionDomainLayout . . . 826
GetRemoteLoggingHost . . . 828
GetSnmpACL . . . 829
GetSnmpInfo . . . 830
GetSnmpState . . . 832
GetSnmpTrapInfo . . . 833
GetSSLCertificate . . . 835
ListProtectionDomainLevels . . . 837
RemoveSSLCertificate . . . 839
ResetNetworkConfig . . . 840
ResetSupplementalTlsCipher . . . 841
SetClusterStructure . . . 842
SetLldpConfig . . . 843
SetNtpInfo . . . 844
SetProtectionDomainLayout . . . 846
SetRemoteLoggingHost . . . 849

SetSnmpACL . . . 850
SetSnmpInfo . . . 852
SetSnmpTrapInfo . . . 855
SetSSLCertificate . . . 857
SnmpSendTestTrap . . . 859
TestAddressAvailability . . . 860
Metodi API di rete multi-tenant . . . 862
Prerequisiti per la configurazione di una rete virtuale multi-tenant . . . 862
Ordine delle operazioni di rete virtuale . . . 862
Trova ulteriori informazioni . . . 862
Convenzioni di naming della rete virtuale . . . 862
AddVirtualNetwork . . . 863
ModifyVirtualNetwork . . . 866
ListVirtualNetworks . . . 869
RemoveVirtualNetwork . . . 872
Metodi API del volume . . . 873
Trova ulteriori informazioni . . . 874
CancelClone . . . 875
CancelGroupClone . . . 876
CloneMultipleVolumes . . . 877
CloneVolume . . . 880
CopyVolume . . . 885
CreateQoSPolicy . . . 887
CreateVolume . . . 888
CreateBackupTarget . . . 895
Policy DeleteQoS . . . 896
DeleteVolume . . . 897
DeleteVolumes . . . 900
GetBackupTarget . . . 902
GetVolumeStats . . . 904
GetDefaultQoS . . . 907
Policy GetQoS . . . 908
GetVolumeCount . . . 910
GetVolumeEfficiency . . . 911
ListActiveVolumes . . . 912
ListBackupTargets . . . 914
ListBulkVolumeJobs . . . 915
ListDeletedVolumes . . . 917
ListQoSPolicies . . . 920
ListSyncJobs . . . 922
ListVolumeQoSIstogrammi . . . 924
ListVolumes . . . 926
ListVolumeStats . . . 930
ListVolumesForAccount . . . 932
ListVolumeStatsByAccount . . . 935

ListVolumeStatsByVirtualVolume . . . 936
ListVolumeStatsByVolume . . . 939
ListVolumeStatsByVolumeAccessGroup . . . 941
ModifyBackupTarget . . . 943
ModifyQoSPolicy . . . 944
ModifyVolume . . . 946
ModifyVolumes . . . 955
PurgeDeletedVolume . . . 964
PurgeDeletedVolumes . . . 965
RemoveBackupTarget . . . 966
RestoreDeletedVolume . . . 967
SetDefaultQoS . . . 968
StartBulkVolumeRead . . . 970
StartBulkVolumeWrite . . . 973
UpdateBulkVolumeStatus . . . 976
Metodi API del gruppo di accesso al volume . . . 978
Trova ulteriori informazioni . . . 978
AddInitiatorsToVolumeAccessGroup . . . 978
AddVolumesToVolumeAccessGroup . . . 981
CreateVolumeAccessGroup . . . 983
DeleteVolumeAccessGroup . . . 986
ListVolumeAccessGroups . . . 988
RemoveVolumesFromVolumeAccessGroup . . . 990
RemoveInitialisFromVolumeAccessGroup . . . 992
ModifyVolumeAccessGroup . . . 994
GetVolumeAccessGroupEfficiency . . . 998
Metodi API di Volume Snapshot . . . 1000
Trova ulteriori informazioni . . . 1000
Panoramica delle istantanee . . . 1000
CreateGroupSnapshot . . . 1001
CreateSchedule . . . 1007
CreateSnapshot . . . 1020
DeleteGroupSnapshot . . . 1026
DeleteSnapshot . . . 1028
GetSchedule . . . 1029
ListGroupSnapshot . . . 1031
Elenchi . . . 1034
ListSnapshot . . . 1036
ModifyGroupSnapshot . . . 1038
ModifySchedule . . . 1042
ModifySnapshot . . . 1049
RollbackToGroupSnapshot . . . 1053
RollbackToSnapshot . . . 1058
Metodi API dei volumi virtuali . . . 1061
Trova ulteriori informazioni . . . 1061

CreateStorageContainer 1061
DeleteStorageContainers 1063
GetStorageContainerEfficiency 1064
GetVirtualVolumeCount 1066
ListProtocolEndpoint 1067
ListStorageContainers 1070
ListVirtualVolumeBindings 1071
ListVirtualVolumeHost 1073
ListVirtualVolumes 1074
ListVirtualVolumeTasks 1078
ModifyStorageContainer 1079
Controllo degli accessi 1081
account 1081
amministratore 1081
ClusterAdmin 1082
dischi 1085
nodi 1085
leggi 1086
creazione di report 1087
repository 1088
volumi 1088
di scrittura 1090
Esempi di risposte 1091
Trova ulteriori informazioni 1091
GetConfig 1092
GetClusterHardwareInfo 1094
GetLldpInfo 1108
GetNetworkConfig 1137
GetNodeHardwareInfo (output per iSCSI) 1142
GetNodeHardwareInfo (output per nodi Fibre Channel) 1143
GetNvramInfo 1151
ListActiveNode 1160
ListActiveVolumes 1163
TestHardwareConfig 1172
Plug-in NetApp Element per server vCenter 1178
Per ulteriori informazioni 1178
Monitorare lo storage con SolidFire Active IQ 1179
Per ulteriori informazioni 1179
Lavorare con il nodo di gestione 1180
Panoramica del nodo di gestione 1180
Installare o ripristinare un nodo di gestione 1181
Installare un nodo di gestione 1181
Configurazione di un NIC (Network Interface Controller) per lo storage 1187
Ripristinare un nodo di gestione 1189
Accedere al nodo di gestione 1194

Accedere all'interfaccia utente del nodo di gestione per nodo . . . 1194
Accedere all'interfaccia utente REST API del nodo di gestione . . . 1195
Utilizzare l'interfaccia utente del nodo di gestione . . . 1196
Panoramica dell'interfaccia utente del nodo di gestione . . . 1196
Configurare il monitoraggio degli avvisi . . . 1197
Modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione . . . 1197
Eseguire le utility di sistema dal nodo di gestione . . . 1199
Utilizzare l'API REST del nodo di gestione . . . 1200
Panoramica dell'interfaccia utente REST API del nodo di gestione . . . 1200
Ottenere l'autorizzazione per utilizzare le API REST . . . 1201
Abilita il monitoraggio Active IQ e NetApp . . . 1202
Configurare NetApp Hybrid Cloud Control per più vCenter . . . 1205
Aggiungere una risorsa controller al nodo di gestione . . . 1206
Creare e gestire le risorse del cluster di storage . . . 1208
Visualizzare o modificare le risorse dei controller esistenti . . . 1213
Configurare un server proxy . . . 1214
Verificare le versioni dei sistemi operativi e dei servizi del nodo di gestione . . . 1216
Recupero dei log dai servizi di gestione . . . 1217
Gestire le connessioni di supporto . . . 1218
Avviare una sessione remota di NetApp Support . . . 1218
Gestire la funzionalità SSH sul nodo di gestione . . . 1219
Aggiorna la versione del tuo sistema storage all-flash NetApp SolidFire Element 12,3.x . . . 1223
Panoramica della sequenza di aggiornamento . . . 1223
sequenza di aggiornamento del sistema . . . 1223
Procedure di aggiornamento del sistema . . . 1224
Servizi di gestione degli aggiornamenti . . . 1224
Effettua l'aggiornamento alla versione più recente di HealthTools . . . 1227
Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage . . . 1229
Aggiornare il software Element . . . 1237
Aggiornare il firmware dello storage . . . 1254
Aggiornare un nodo di gestione . . . 1263
Aggiornare il plug-in Element per vCenter Server . . . 1278
Aggiorna i componenti vSphere per un sistema storage NetApp SolidFire con il plug-in Element per vCenter Server . . . 1284
Trova ulteriori informazioni . . . 1284
Versioni precedenti della documentazione software SolidFire e NetApp Element . . . 1285
Per ulteriori informazioni . . . 1285
Note legali . . . 1286
Copyright . . . 1286
Marchi . . . 1286
Brevetti . . . 1286
Direttiva sulla privacy . . . 1286
Open source . . . 1286

Documentazione software SolidFire ed Element

Informazioni sulla release corrente e precedente

Sono disponibili collegamenti alle note di rilascio più recenti e precedenti per i vari componenti dell'ambiente storage Element.

Ti verrà richiesto di effettuare l'accesso utilizzando le credenziali del supporto NetApp.

Software NetApp Element

- "Note sulla versione del software NetApp Element 12.3.2"
- "Note sulla versione del software NetApp Element 12.3.1"
- "Note sulla versione del software NetApp Element 12.3"
- "Note sulla versione del software NetApp Element 12.2.1"
- "Note sulla versione del software NetApp Element 12.2"
- "Note sulla versione del software NetApp Element 12.0.1"
- "Note sulla versione del software NetApp Element 12.0"
- "Note sulla versione del software NetApp Element 11.8.2"
- "Note sulla versione del software NetApp Element 11.8.1"
- "Note sulla versione del software NetApp Element 11.8"
- "Note sulla versione del software NetApp Element 11.7"
- "Note sulla versione del software NetApp Element 11.5.1"
- "Note sulla versione del software NetApp Element 11.3P1"

Servizi di gestione

- "Note sulla versione di Management Services"

Plug-in NetApp Element per server vCenter

- "VCenter Plug-in 5,3 - Note sulla versione" *NUOVO*
- "VCenter Plug-in 5,2 - Note sulla versione"
- "Note sulla versione di vCenter Plug-in 5.1"
- "Note sulla versione di vCenter Plug-in 5.0"
- "Note sulla versione di vCenter Plug-in 4.10"
- "Note sulla versione di vCenter Plug-in 4.9"
- "Note sulla versione di vCenter Plug-in 4.8"
- "Note sulla versione di vCenter Plug-in 4.7"
- "Note sulla versione di vCenter Plug-in 4.6"
- "Note sulla versione di vCenter Plug-in 4.5"
- "Note sulla versione di vCenter Plug-in 4.4"

- "Note sulla versione di vCenter Plug-in 4.3"

Firmware dello storage

- "Note sulla versione di Storage firmware Bundle 2.146 (più recenti)"
- "Note sulla versione di Storage firmware Bundle 2.99.2"
- "Note sulla versione di Storage firmware Bundle 2.76"
- "Note sulla versione di Storage firmware Bundle 2.27"
- "H610S BMC 3.84.07 Release Notes"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"
- "Panoramica dello storage all-flash SolidFire"

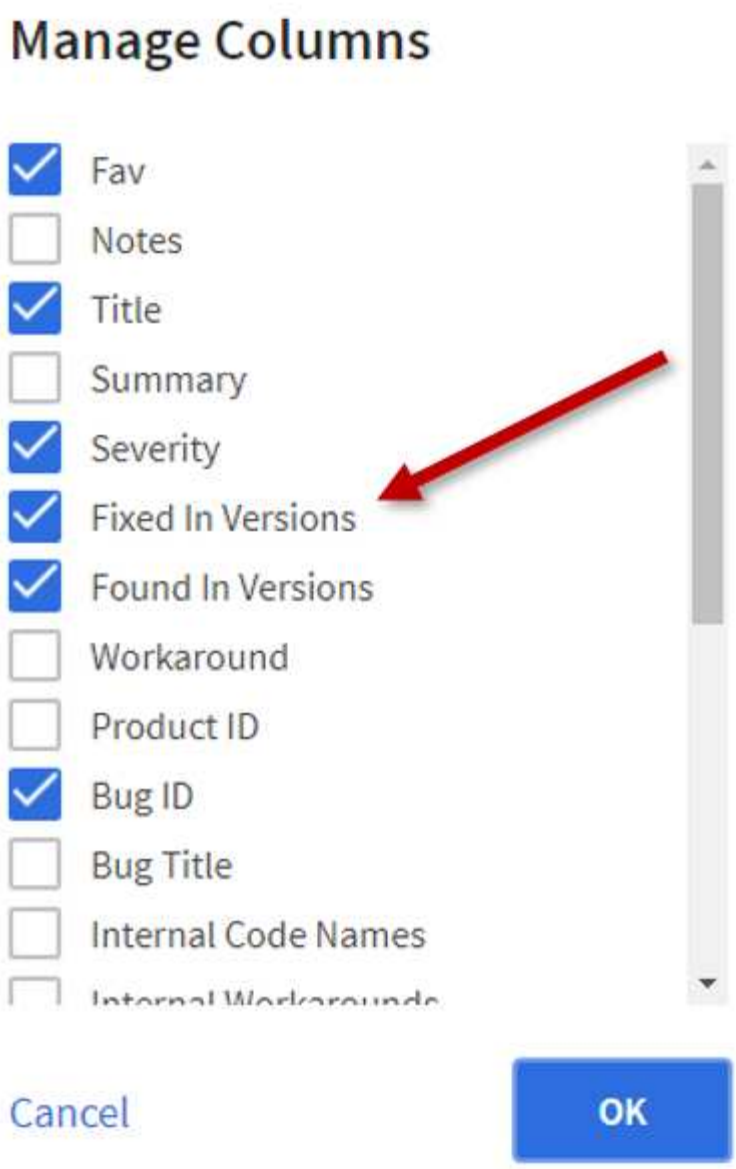
Novità

NetApp aggiorna periodicamente SolidFire e il software Element per offrire nuove funzionalità, miglioramenti e correzioni di bug. Element 12.3 introduce miglioramenti alla crittografia software a riposo, miglioramenti alla sicurezza, aggiornamenti del firmware dello storage, funzionalità snapshot avanzate e comportamento migliorato per i dischi guasti.

NetApp Bugs Online contiene problemi noti e risolti

I problemi noti e risolti sono ora elencati nel tool NetApp Bugs Online. È possibile esaminare questi problemi per Element e altri prodotti.

1. Passare a. "NetApp Bugs Online".
2. Digitare il nome del prodotto, ad esempio "Element", nel campo **Cerca per parola chiave**.
3. Selezionare Selezionare **Fixed in Versions** e selezionare **OK**.



4. Per filtrare in base alla release, digitare la versione della release nel campo **fixed in Versions**.

Elemento 12.3.2

Scopri di più sulle novità di Element 12.3.2.

La versione 12.3.2 del software Element contiene la mitigazione che chiude l'esposizione del software Element alla vulnerabilità di Apache Log4j. I cluster di storage NetApp SolidFire con la funzione volumi virtuali (VVol) attivata sono esposti a questa vulnerabilità.

Elemento 12.3.1

Scopri di più sulle novità di Element 12.3.1.

Bundle firmware per lo storage 2.99.2

La release Element 12.3.1 include la versione 2.99.2 del bundle firmware di storage. Se il cluster di storage è già in Element 12.3, è possibile installare semplicemente il nuovo bundle firmware 2.99.2.

Supporto per la valutazione dinamica dei nodi della CPU per le piattaforme host SolidFire eSDS

SolidFire eSDS ora supporta la gamma completa di CPU di generazione Gold e Silver Cascade Lake, una gamma di 24 modelli. La funzione Dynamic Node Rating assegna al server host una classificazione QoS IOPS compresa tra 50.000 e 100.000 in base alla CPU.

Numero di core della CPU	Valutazione IOPS nodo ESDS
8	50.000
10	60.000
12	75 K.
16+	100.000

Supporto per configurazione di rete single bond per SolidFire eSDS

Ora puoi utilizzare una configurazione di rete single bond per il tuo host con SolidFire eSDS.

Nuovo supporto server in SolidFire SDS Enterprise

SolidFire eSDS è ora disponibile sui server HPE DL380. Vedere "Tool di matrice di interoperabilità NetApp (IMT)" per ulteriori informazioni sulla configurazione supportata.

Elemento 12.3

Scopri di più sulle novità di Element 12.3.

Supporto della coda di snapshot FIFO

Element 12.3 consente di creare una coda FIFO (first-in-first-out) per gli snapshot dei volumi. Utilizzando l'API Element, è possibile specificare il numero minimo e massimo di slot di snapshot FIFO da riservare quando si crea un volume. Quando la coda di snapshot FIFO per un volume è piena, lo snapshot successivo creato per quel volume rimuove lo snapshot meno recente di quel volume dal sistema. Le snapshot FIFO e non FIFO utilizzano lo stesso pool di slot di snapshot disponibili su un volume.

I seguenti metodi API Element sono correlati alle snapshot FIFO (vedere la "Documentazione API Element" Per informazioni dettagliate su ciascun metodo API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- CreateVolume
- ModifyGroupSnapshot
- ModifySchedule
- ModifySnapshot
- ModifyVolume

- ModifyVolumes

Supporto per la serializzazione di Snapshot

Element 12.3 supporta la creazione di snapshot serializzati. Quando si crea un nuovo snapshot utilizzando l'API Element, è possibile specificare che lo snapshot non debba essere creato se è ancora in corso una replica precedente.

I seguenti metodi API Element sono correlati alla serializzazione delle snapshot (vedere la "Documentazione API Element" Per informazioni dettagliate su ciascun metodo API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- ModifySchedule

Supporto per la conservazione di Snapshot

Element 12.3 consente di specificare un tempo di conservazione per gli snapshot. Se non si specifica un tempo di conservazione o una scadenza per uno snapshot, questo viene conservato per sempre.

I seguenti metodi API Element sono correlati alla conservazione degli snapshot (vedere la "Documentazione API Element" Per informazioni dettagliate su ciascun metodo API):

- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- ModifyGroupSnapshot
- ModifySchedule
- ModifySnapshot

Miglioramenti della crittografia software a riposo

Per la funzione di crittografia software a riposo, Element 12.3 introduce la gestione delle chiavi esterne (EKM) e la possibilità di reimmettere la chiave master di crittografia software. È possibile attivare la crittografia software a riposo quando si crea un cluster di storage. Quando si crea un cluster di storage SDS aziendale SolidFire, la crittografia software a riposo viene attivata per impostazione predefinita. Questa funzione crittografa tutti i dati memorizzati sugli SSD nei nodi di storage e causa solo un impatto molto ridotto (~2%) sulle performance sull'io del client.

I seguenti metodi API Element sono correlati alla crittografia software a riposo (vedere la "Documentazione API Element" Per informazioni dettagliate su ciascun metodo API):

- CreateCluster
- DisableEncryptionAtRest
- EnableEncryptionAtRest
- GetSoftwareEncryptionAtRestInfo
- RekeySoftwareEncryptionAtRestMasterKey

Aggiornamenti del firmware del nodo di storage

Element 12.3 include aggiornamenti del firmware per i nodi di storage. "Scopri di più".

Miglioramenti della sicurezza

L'elemento 12.3 risolve le vulnerabilità di sicurezza per i nodi di storage e il nodo di gestione. "Scopri di più" informazioni su questi miglioramenti della sicurezza.

Miglioramento del comportamento dei dischi guasti

Element 12.3 esegue controlli periodici dello stato di salute sui dischi dell'appliance SolidFire utilizzando i dati di stato SMART dei dischi. Un disco che non supera IL controllo dello stato DI salute INTELLIGENTE potrebbe essere prossimo al guasto. Se un disco non supera il controllo DELLO stato SMART, il disco passa allo stato **Failed** (guasto) e viene visualizzato un errore del cluster di severità critica: `Drive with serial: <serial number> in slot: <node slot><drive slot> has failed the SMART overall health check. To resolve this fault, replace the drive.`

Nuovo supporto server in SolidFire SDS Enterprise

SolidFire eSDS è ora disponibile sui server Dell R640. Vedere "Tool di matrice di interoperabilità NetApp (IMT)" per ulteriori informazioni sulla configurazione supportata.

Nuova posizione per i problemi noti di SolidFire eSDS

È ora possibile cercare i problemi noti su "Tool bugs Online (accesso richiesto)".

Trova ulteriori informazioni

- "Note sulla versione di NetApp Hybrid Cloud Control and Management Services"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"
- "Documentazione software SolidFire ed Element"
- "Centro di documentazione software SolidFire ed Element per le versioni precedenti"
- "Pagina delle risorse NetApp HCI"
- "Versioni del firmware dello storage supportate per i nodi di storage SolidFire" *NUOVO*

Concetti

Scopri i concetti di base relativi al software Element.

- "Panoramica del prodotto"
- Panoramica dell'architettura di SolidFire
- Nodi
- Cluster
- "Sicurezza"
- Account e permessi
- "Volumi"
- Protezione dei dati
- Performance e qualità del servizio

Trova ulteriori informazioni

- "Panoramica dello storage all-flash SolidFire"
- "Documentazione software SolidFire ed Element"

Panoramica del prodotto

Un sistema storage all-flash SolidFire è composto da componenti hardware discreti (dischi e nodi) che vengono combinati in un singolo pool di risorse di storage. Questo cluster unificato si presenta come un singolo sistema storage per l'utilizzo da parte di client esterni ed è gestito con il software NetApp Element.

Utilizzando l'interfaccia Element, l'API o altri strumenti di gestione, è possibile monitorare la capacità e le performance dello storage del cluster SolidFire e gestire l'attività dello storage in un'infrastruttura multi-tenant.

Funzionalità di SolidFire

Un sistema SolidFire offre le seguenti funzionalità:

- Offre uno storage dalle performance elevate per la tua infrastruttura di cloud privato su larga scala
- Offre una scalabilità flessibile che consente di soddisfare le mutevoli esigenze di storage
- Utilizza un'interfaccia software per elementi di gestione dello storage basata su API
- Garantisce le performance utilizzando le policy di qualità del servizio
- Include il bilanciamento automatico del carico su tutti i nodi del cluster
- Ribilanciare automaticamente i cluster quando i nodi vengono aggiunti o sottratti

Implementazione di SolidFire

Utilizzare i nodi di storage forniti da NetApp e integrati con il software NetApp Element.

"Panoramica dell’architettura dello storage all-flash SolidFire"

Trova ulteriori informazioni

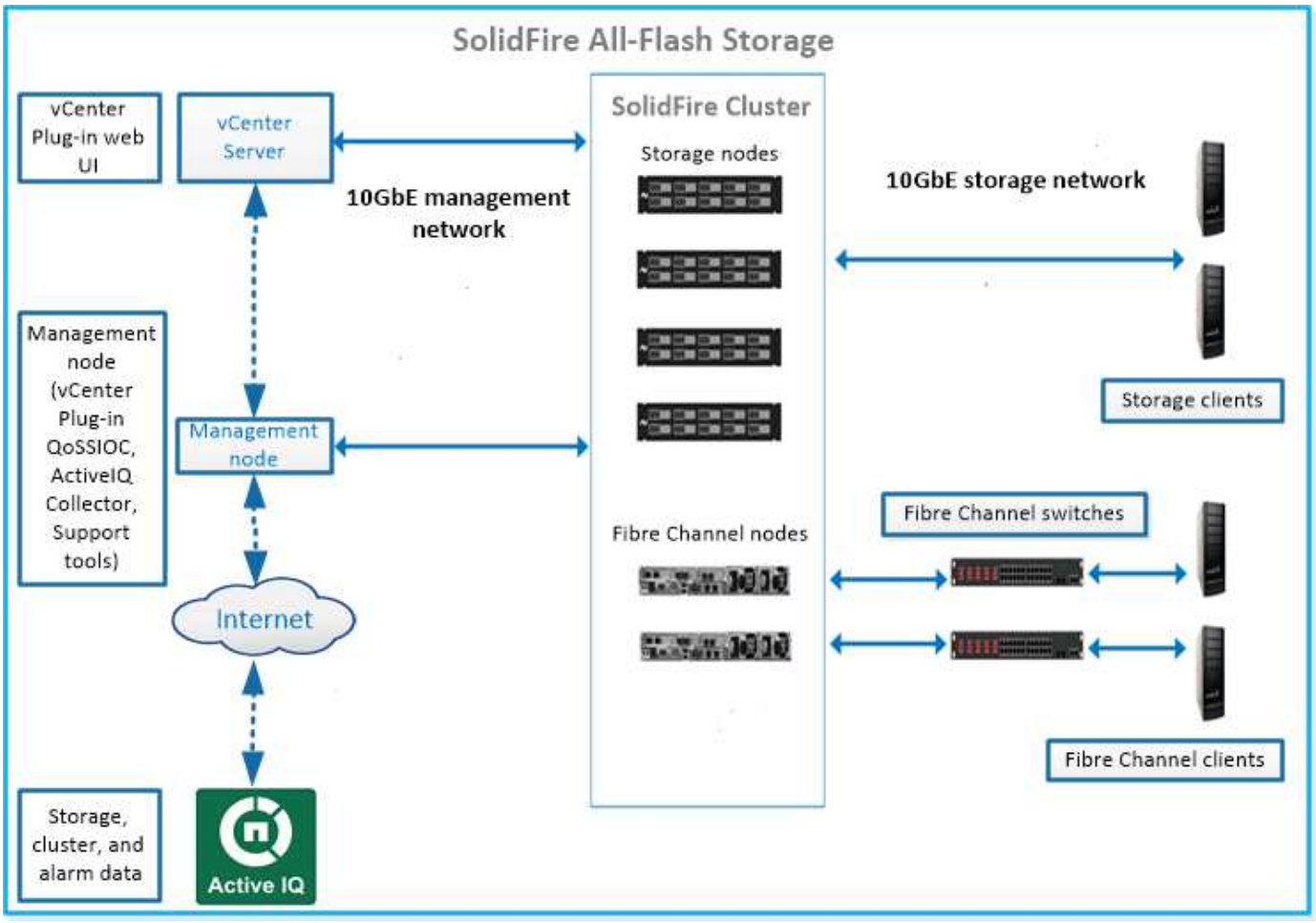
- "Panoramica dello storage all-flash SolidFire"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Panoramica dell’architettura di SolidFire

Un sistema storage all-flash SolidFire è composto da componenti hardware discreti (dischi e nodi) che vengono combinati in un pool di risorse storage con il software NetApp Element in esecuzione indipendente su ciascun nodo. Questo singolo sistema storage viene gestito come singola entità utilizzando l’interfaccia utente del software Element, l’API e altri strumenti di gestione.

Un sistema storage SolidFire include i seguenti componenti hardware:

- **Cluster**: L’hub del sistema storage SolidFire che è un insieme di nodi.
- **Nodi**: I componenti hardware raggruppati in un cluster. Esistono due tipi di nodi:
  - Nodi di storage, ovvero server che contengono una raccolta di dischi
  - Nodi Fibre Channel (FC), utilizzati per la connessione ai client FC
- **Drives**: Utilizzato nei nodi di storage per memorizzare i dati per il cluster. Un nodo di storage contiene due tipi di dischi:
  - I dischi di metadati dei volumi memorizzano informazioni che definiscono i volumi e altri oggetti all’interno di un cluster.
  - I dischi a blocchi memorizzano i blocchi di dati per i volumi.



È possibile gestire, monitorare e aggiornare il sistema utilizzando l'interfaccia utente Web Element e altri strumenti compatibili:

- "Interfacce software SolidFire"
- "SolidFire Active IQ"
- "Nodo di gestione per software Element"
- "Servizi di gestione"

URL comuni

Di seguito sono riportati gli URL comuni utilizzati con un sistema di storage all-flash SolidFire:

URL	Descrizione
`https://[storage cluster MVIP address]`	Accedere all'interfaccia utente del software NetApp Element.
`https://activeiq.solidfire.com`	Monitorare i dati e ricevere avvisi in caso di colli di bottiglia delle performance o potenziali problemi del sistema.
`https://[management node IP address]`	Accedi a NetApp Hybrid Cloud Control per aggiornare l'installazione dello storage e i servizi di gestione degli aggiornamenti.

URL	Descrizione
`https://[IP address]:442`	Dall'interfaccia utente per nodo, accedere alle impostazioni di rete e cluster e utilizzare le utility e i test di sistema. "Scopri di più."
`https://[management node IP address]/mnode`	Utilizzare i servizi di gestione REST API e altre funzionalità dal nodo di gestione."Scopri di più."
`https://[management node IP address]:9443`	Registrare il pacchetto vCenter Plug-in in vSphere Web Client."Scopri di più."

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Interfacce software SolidFire

È possibile gestire un sistema storage SolidFire utilizzando diverse interfacce software e utility di integrazione NetApp Element.

Opzioni

- Interfaccia utente del software NetApp Element
- API del software NetApp Element
- Plug-in NetApp Element per server vCenter
- NetApp Hybrid Cloud Control
- UI del nodo di gestione
- Utility e tool di integrazione aggiuntivi

Interfaccia utente del software NetApp Element

Consente di configurare lo storage Element, monitorare la capacità e le performance del cluster e gestire l'attività dello storage in un'infrastruttura multi-tenant. Element è il sistema operativo per lo storage al centro di un cluster SolidFire. Il software Element viene eseguito in modo indipendente su tutti i nodi del cluster e consente ai nodi del cluster di combinare le risorse presentate come un singolo sistema storage ai client esterni. Il software Element è responsabile di tutto il coordinamento, la scalabilità e la gestione del cluster nel suo complesso. L'interfaccia software si basa sull'API Element.

"Gestire lo storage con il software Element"

API del software NetApp Element

Consente di utilizzare un set di oggetti, metodi e routine per gestire lo storage degli elementi. L'API Element si basa sul protocollo JSON-RPC su HTTPS. È possibile monitorare le operazioni API nell'interfaccia utente Element attivando il log API; in questo modo è possibile visualizzare i metodi che vengono emessi al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi che vengono emessi.

"Gestire lo storage con l'API Element"

Plug-in NetApp Element per server vCenter

Consente di configurare e gestire cluster di storage che eseguono software Element utilizzando un'interfaccia alternativa per l'interfaccia utente Element di VMware vSphere.

"Plug-in NetApp Element per server vCenter"

NetApp Hybrid Cloud Control

Consente di aggiornare i servizi di storage e gestione degli elementi e di gestire le risorse di storage utilizzando l'interfaccia NetApp Hybrid Cloud Control.

"Gestione e monitoraggio dello storage con la panoramica di NetApp Hybrid Cloud Control"

UI del nodo di gestione

Il nodo di gestione contiene due interfacce utente: Un'interfaccia utente per la gestione dei servizi basati SU REST e un'interfaccia utente per nodo per la gestione delle impostazioni di rete e cluster, nonché test e utility del sistema operativo. Dall'interfaccia utente dell'API REST, è possibile accedere a un menu di API correlate al servizio che controllano la funzionalità del sistema basata sul servizio dal nodo di gestione.

Utility e tool di integrazione aggiuntivi

Anche se in genere si gestisce lo storage con NetApp Element, API NetApp Element e plug-in NetApp Element per vCenter Server, è possibile utilizzare utility e strumenti di integrazione aggiuntivi per accedere allo storage.

Elemento CLI

"Elemento CLI" Consente di controllare un sistema storage SolidFire utilizzando un'interfaccia a riga di comando senza dover utilizzare l'API Element.

Tool PowerShell Element

"Tool PowerShell Element" Consente di utilizzare una raccolta di funzioni di Microsoft Windows PowerShell che utilizzano l'API Element per gestire un sistema storage SolidFire.

SDK elemento

"SDK elemento" Consente di gestire il cluster SolidFire utilizzando i seguenti strumenti:

- Element Java SDK: Consente ai programmatori di integrare l'API Element con il linguaggio di programmazione Java.
- Element .NET SDK: Consente ai programmatori di integrare l'API Element con la piattaforma di programmazione .NET.
- Element Python SDK: Consente ai programmatori di integrare l'API Element con il linguaggio di programmazione Python.

Suite di test API Postman di SolidFire

Consente ai programmatori di utilizzare una raccolta di "Postino" Funzioni che testano le chiamate API degli elementi.

Adattatore per la replica dello storage SolidFire

"Adattatore per la replica dello storage SolidFire" Si integra con VMware Site Recovery Manager (SRM) per consentire la comunicazione con cluster di storage SolidFire replicati ed eseguire flussi di lavoro supportati.

SolidFire Vro

"SolidFire Vro" Offre un metodo pratico per utilizzare l'API Element per amministrare il sistema di storage SolidFire con VMware vRealize Orchestrator.

Provider VSS di SolidFire

"Provider VSS di SolidFire" Integra le copie shadow VSS con snapshot e cloni degli elementi.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

SolidFire Active IQ

"SolidFire Active IQ" è uno strumento basato sul web che offre viste storiche costantemente aggiornate dei dati a livello di cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le performance e la capacità del sistema, oltre a essere sempre informato sullo stato dei cluster.

In SolidFire Active IQ sono disponibili le seguenti informazioni relative al sistema in uso:

- Numero di nodi e stato dei nodi: Integro, offline o guasto
- Rappresentazione grafica della CPU, dell'utilizzo della memoria e della limitazione dei nodi
- Dettagli sul nodo, come il numero di serie, la posizione dello slot nello chassis, il modello e la versione del software NetApp Element in esecuzione sul nodo di storage
- Informazioni relative a CPU e storage sulle macchine virtuali

Per ulteriori informazioni su SolidFire Active IQ, consultare "Documentazione SolidFire Active IQ".

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"
- **Sito di supporto NetApp › Tool per Active IQ**

Nodo di gestione per software Element

Il "Nodo di gestione (mNode)" È una macchina virtuale che viene eseguita in parallelo con uno o più cluster di storage basati su software Element. Viene utilizzato per aggiornare e fornire servizi di sistema, tra cui monitoraggio e telemetria, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema e abilitare l'accesso al

supporto NetApp per la risoluzione dei problemi.

Il nodo di gestione interagisce con un cluster di storage per eseguire azioni di gestione, ma non è membro del cluster di storage. I nodi di gestione raccolgono periodicamente informazioni sul cluster tramite chiamate API e inviano tali informazioni a Active IQ per il monitoraggio remoto (se abilitato). I nodi di gestione sono inoltre responsabili del coordinamento degli aggiornamenti software dei nodi del cluster.

A partire dalla release Element 11.3, il nodo di gestione funziona come un host microservice, consentendo aggiornamenti più rapidi di servizi software selezionati al di fuori delle release principali. Questi microservizi o. "servizi di gestione" vengono aggiornati frequentemente come bundle di servizi.

Servizi di gestione per lo storage all-flash SolidFire

A partire dalla release Element 11.3, i **servizi di gestione** sono ospitati su "nodo di gestione", consentendo aggiornamenti più rapidi di servizi software selezionati al di fuori delle release principali.

I servizi di gestione forniscono funzionalità di gestione estese e centrali per lo storage all-flash SolidFire. Questi servizi includono "NetApp Hybrid Cloud Control", Telemetria del sistema Active IQ, registrazione e aggiornamenti del servizio, nonché il servizio QoSSIOC per il plug-in Element per vCenter.

Scopri di più "release di servizi di gestione".

Nodi

I nodi sono risorse hardware o virtuali raggruppate in un cluster per fornire funzionalità di calcolo e storage a blocchi.

Il software NetApp Element definisce diversi ruoli di nodo per un cluster. I tipi di ruoli dei nodi sono i seguenti:

- Nodo di gestione
- Nodo storage
- Nodo Fibre Channel

stati dei nodi varia in base all'associazione del cluster.

Nodo di gestione

Un nodo di gestione è una macchina virtuale utilizzata per aggiornare e fornire servizi di sistema tra cui monitoraggio e telemetria, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi."Scopri di più"

Nodo storage

Un nodo di storage SolidFire è un server che contiene una raccolta di dischi che comunicano tra loro attraverso l'interfaccia di rete Bond10G. I dischi nel nodo contengono spazio di blocchi e metadati per lo storage e la gestione dei dati. Ogni nodo contiene un'immagine di fabbrica del software NetApp Element.

I nodi di storage hanno le seguenti caratteristiche:

- Ogni nodo ha un nome univoco. Se il nome di un nodo non viene specificato da un amministratore, per

impostazione predefinita è SF-XXXX, dove XXXX è costituito da quattro caratteri casuali generati dal sistema.

- Ogni nodo dispone di una propria cache di scrittura NVRAM (non-volatile Random Access Memory) dalle performance elevate per migliorare le prestazioni generali del sistema e ridurre la latenza di scrittura.
- Ogni nodo è collegato a due reti, storage e gestione, ciascuna con due collegamenti indipendenti per ridondanza e performance. Ciascun nodo richiede un indirizzo IP su ciascuna rete.
- È possibile creare un cluster con nuovi nodi di storage o aggiungere nodi di storage a un cluster esistente per aumentare la capacità e le performance dello storage.
- È possibile aggiungere o rimuovere nodi dal cluster in qualsiasi momento senza interrompere il servizio.

Nodo Fibre Channel

I nodi Fibre Channel SolidFire forniscono connettività a uno switch Fibre Channel, che è possibile collegare ai client Fibre Channel. I nodi Fibre Channel fungono da convertitore di protocollo tra i protocolli Fibre Channel e iSCSI, consentendo di aggiungere connettività Fibre Channel a qualsiasi cluster SolidFire nuovo o esistente.

I nodi Fibre Channel hanno le seguenti caratteristiche:

- Gli switch Fibre Channel gestiscono lo stato del fabric, fornendo interconnessioni ottimizzate.
- Il traffico tra due porte passa solo attraverso gli switch e non viene trasmesso ad altre porte.
- Il guasto di una porta è isolato e non influisce sul funzionamento di altre porte.
- Più coppie di porte possono comunicare contemporaneamente in un fabric.

stato operativo del nodo

Un nodo può trovarsi in uno dei diversi stati a seconda del livello di configurazione.

- **Disponibile**

  Il nodo non ha un nome di cluster associato e non fa ancora parte di un cluster.

- **In sospeso**

  Il nodo è configurato e può essere aggiunto a un cluster designato.

  Per accedere al nodo non è richiesta l'autenticazione.

- **Attivo in sospeso**

  Il sistema sta installando un software compatibile sul nodo. Al termine, il nodo passa allo stato attivo.

- **Attivo**

  Il nodo partecipa a un cluster.

  L'autenticazione è necessaria per modificare il nodo.

In ciascuno di questi stati, alcuni campi sono di sola lettura.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Cluster

Un cluster è l'hub di un sistema storage SolidFire ed è costituito da un insieme di nodi. È necessario disporre di almeno quattro nodi in un cluster per ottenere l'efficienza dello storage SolidFire. Un cluster viene visualizzato sulla rete come singolo gruppo logico ed è quindi possibile accedervi come storage a blocchi.

La creazione di un nuovo cluster inizializza un nodo come proprietario delle comunicazioni per un cluster e stabilisce le comunicazioni di rete per ciascun nodo del cluster. Questo processo viene eseguito una sola volta per ogni nuovo cluster. È possibile creare un cluster utilizzando l'interfaccia utente Element o l'API.

È possibile scalare un cluster aggiungendo nodi aggiuntivi. Quando si aggiunge un nuovo nodo, non si verifica alcuna interruzione del servizio e il cluster utilizza automaticamente le prestazioni e la capacità del nuovo nodo.

Gli amministratori e gli host possono accedere al cluster utilizzando indirizzi IP virtuali. Qualsiasi nodo del cluster può ospitare gli indirizzi IP virtuali. L'IP virtuale di gestione (MVIP) consente la gestione del cluster tramite una connessione 1GbE, mentre l'IP virtuale dello storage (SVIP) consente l'accesso dell'host allo storage tramite una connessione 10GbE. Questi indirizzi IP virtuali consentono connessioni coerenti indipendentemente dalle dimensioni o dalla composizione di un cluster SolidFire. Se un nodo che ospita un indirizzo IP virtuale non riesce, un altro nodo del cluster inizia a ospitare l'indirizzo IP virtuale.

> A partire dalla versione 11.0 di Element, i nodi possono essere configurati con indirizzi IPv4, IPv6 o entrambi per la propria rete di gestione. Questo vale sia per i nodi di storage che per i nodi di gestione, ad eccezione del nodo di gestione 11.3 e successivo che non supporta IPv6. Quando si crea un cluster, è possibile utilizzare solo un indirizzo IPv4 o IPv6 singolo per MVIP e il tipo di indirizzo corrispondente deve essere configurato su tutti i nodi.

Ulteriori informazioni sui cluster

- Cluster di storage autorevoli
- Regola dei terzi
- Capacità inutilizzata
- Efficienza dello storage
- Quorum del cluster di storage

Cluster di storage autorevoli

Il cluster di storage autorevole è il cluster di storage utilizzato da NetApp Hybrid Cloud Control per autenticare gli utenti.

Se il nodo di gestione dispone di un solo cluster di storage, si tratta del cluster autorevole. Se il nodo di gestione dispone di due o più cluster di storage, uno di questi viene assegnato come cluster autorevole e solo gli utenti di quel cluster possono accedere a NetApp Hybrid Cloud Control. Per scoprire quale cluster è il cluster autorevole, è possibile utilizzare `GET /mnode/about` API. Nella risposta, l'indirizzo IP in `token_url` Il campo è l'indirizzo IP virtuale di gestione (MVIP) del cluster di storage autorevole. Se si tenta di accedere a

NetApp Hybrid Cloud Control come utente che non si trova nel cluster autorevole, il tentativo di accesso non avrà esito positivo.

Molte funzionalità di NetApp Hybrid Cloud Control sono progettate per funzionare con più cluster di storage, ma l'autenticazione e l'autorizzazione hanno dei limiti. Il limite dell'autenticazione e dell'autorizzazione è che l'utente del cluster autorevole può eseguire azioni su altri cluster legati a NetApp Hybrid Cloud Control anche se non è un utente degli altri cluster di storage.

Prima di procedere con la gestione di più cluster di storage, è necessario assicurarsi che gli utenti definiti nei cluster autorevoli siano definiti in tutti gli altri cluster di storage con le stesse autorizzazioni. È possibile gestire gli utenti da "Interfaccia utente del software Element".

Vedere "creare e gestire le risorse del cluster di storage" per ulteriori informazioni sull'utilizzo delle risorse cluster di storage dei nodi di gestione.

Regola dei terzi

Quando si mischiano tipi di nodi di storage in un cluster di storage NetApp SolidFire, nessun singolo nodo di storage può contenere oltre il 33% della capacità totale del cluster di storage.

Capacità inutilizzata

Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunta una maggiore capacità di storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato un guasto appropriato del cluster.

Efficienza dello storage

I cluster di storage NetApp SolidFire utilizzano deduplica, compressione e thin provisioning per ridurre la quantità di storage fisico necessaria per l'archiviazione di un volume.

- **Compressione**

  La compressione riduce la quantità di storage fisico richiesta per un volume combinando i blocchi di dati in gruppi di compressione, ciascuno dei quali viene memorizzato come blocco singolo.

- **Deduplica**

  La deduplica riduce la quantità di storage fisico richiesta per un volume eliminando i blocchi di dati duplicati.

- **Thin provisioning**

  Un volume con thin provisioning o LUN è un volume per il quale lo storage non è riservato in anticipo. Invece, lo storage viene allocato in modo dinamico, in base alle esigenze. Lo spazio libero viene nuovamente rilasciato nel sistema di storage quando i dati nel volume o nel LUN vengono cancellati

Quorum del cluster di storage

Element Software crea un cluster di storage da nodi selezionati, che mantiene un database replicato della configurazione del cluster. Per poter mantenere il quorum per la resilienza del cluster, sono necessari almeno tre nodi per partecipare all'ensemble del cluster.

Sicurezza

Quando si utilizza il sistema di storage all-flash SolidFire, i dati vengono protetti da protocolli di sicurezza standard di settore.

Crittografia a riposo (hardware)

Tutti i dischi nei nodi di storage sono in grado di utilizzare la crittografia AES a 256 bit a livello di unità. Ogni disco dispone di una propria chiave di crittografia, che viene creata al momento della prima inizializzazione del disco. Quando si attiva la funzione di crittografia, viene creata una password a livello di cluster e i frammenti di password vengono quindi distribuiti a tutti i nodi del cluster. Nessun nodo singolo memorizza l'intera password. La password viene quindi utilizzata per proteggere con password tutti gli accessi ai dischi. La password è necessaria per sbloccare l'unità e non è necessaria a meno che l'alimentazione non venga rimossa dall'unità o l'unità non sia bloccata.

"Attivazione della funzione di crittografia hardware a riposo" non influisce sulle prestazioni o sull'efficienza del cluster. Se un disco o nodo abilitato alla crittografia viene rimosso dalla configurazione del cluster con l'API Element o l'interfaccia utente Element, la crittografia a riposo viene disattivata sui dischi. Una volta rimosso il disco, è possibile cancellarlo in modo sicuro utilizzando `SecureEraseDrives` Metodo API. Se un disco o nodo fisico viene rimosso forzatamente, i dati rimangono protetti dalla password a livello di cluster e dalle singole chiavi di crittografia dell'unità.

Crittografia a riposo (software)

Un altro tipo di crittografia a riposo e a riposo del software consente di crittografare tutti i dati scritti su SSD in un cluster di storage. "Se attivato", crittografa tutti i dati scritti e decrta tutti i dati letti automaticamente nel software. La crittografia software a riposo esegue il mirroring dell'implementazione dell'unità con crittografia automatica (SED) nell'hardware per garantire la sicurezza dei dati in assenza di SED.

> Per i cluster di storage all-flash SolidFire, la crittografia software a riposo deve essere attivata durante la creazione del cluster e non può essere disattivata dopo la creazione del cluster.

La crittografia a riposo basata su software e hardware può essere utilizzata in modo indipendente o in combinazione tra loro.

Gestione esterna delle chiavi

È possibile configurare Element Software in modo che utilizzi un servizio di gestione delle chiavi (KMS) conforme a KMIP di terze parti per gestire le chiavi di crittografia del cluster di storage. Quando si attiva questa funzione, la chiave di crittografia della password di accesso al disco a livello di cluster dello storage viene gestita da un KMS specificato dall'utente.

Element può utilizzare i seguenti servizi di gestione delle chiavi:

- Gemalto SafeNet KeySecure
- SafeNet IN KeySecure

- KeyControl HyTrust
- Vormetric Data Security Manager
- IBM Security Key Lifecycle Manager

Per ulteriori informazioni sulla configurazione della gestione esterna delle chiavi, vedere "introduzione alla gestione esterna delle chiavi" documentazione.

Autenticazione a più fattori

L'autenticazione a più fattori (MFA) consente di richiedere agli utenti di presentare diversi tipi di prove per l'autenticazione con l'interfaccia utente Web o l'interfaccia utente del nodo di storage di NetApp Element al momento dell'accesso. È possibile configurare Element in modo che accetti solo l'autenticazione a più fattori per gli accessi che si integrano con il sistema di gestione degli utenti e il provider di identità esistenti. È possibile configurare Element per l'integrazione con un provider di identità SAML 2.0 esistente, in grado di applicare più schemi di autenticazione, ad esempio password e SMS, password e messaggi di posta elettronica o altri metodi.

È possibile associare l'autenticazione a più fattori con i comuni provider di identità compatibili con SAML 2.0 (IDP), come Microsoft Active Directory Federation Services (ADFS) e Shibboleth.

Per configurare MFA, vedere "attiva l'autenticazione a più fattori" documentazione.

FIPS 140-2 per HTTPS e crittografia dei dati a riposo

I cluster di storage NetApp SolidFire supportano la crittografia conforme ai requisiti FIPS (Federal Information Processing Standard) 140-2 per i moduli crittografici. È possibile abilitare la conformità FIPS 140-2 sul cluster SolidFire per le comunicazioni HTTPS e la crittografia del disco.

Quando si attiva la modalità operativa FIPS 140-2 sul cluster, il cluster attiva il modulo di sicurezza crittografica NetApp (NCSM) e sfrutta la crittografia certificata FIPS 140-2 livello 1 per tutte le comunicazioni via HTTPS all'interfaccia utente e all'API NetApp Element. Si utilizza `EnableFeature` API Element con `fips` Parametro per attivare la crittografia HTTPS FIPS 140-2. Nei cluster di storage con hardware compatibile con FIPS, è anche possibile attivare la crittografia del disco FIPS per i dati inattivi utilizzando `EnableFeature` API Element con `FipsDrives` parametro.

Per ulteriori informazioni sulla preparazione di un nuovo cluster di storage per la crittografia FIPS 140-2, vedere "Creare un cluster che supporti i dischi FIPS".

Per ulteriori informazioni sull'attivazione di FIPS 140-2 su un cluster già esistente, vedere "API dell'elemento EnableFeature".

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Account e permessi

Per amministrare e fornire l'accesso alle risorse di storage del sistema, è necessario configurare account per le risorse di sistema.

Utilizzando lo storage Element, è possibile creare e gestire i seguenti tipi di account:

- Account utente amministratore per il cluster di storage
- Account utente per l'accesso al volume di storage
- Account utente cluster autorevoli per NetApp Hybrid Cloud Control

Account amministratore del cluster di storage

Esistono due tipi di account amministratore in un cluster di storage che esegue il software NetApp Element:

- **Primary cluster Administrator account**: Questo account amministratore viene creato al momento della creazione del cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo a un utente root in un sistema Linux. È possibile modificare la password per questo account amministratore.
- **Account amministratore cluster**: È possibile assegnare a un account amministratore cluster un intervallo limitato di accesso amministrativo per eseguire attività specifiche all'interno di un cluster. Le credenziali assegnate a ciascun account amministratore del cluster vengono utilizzate per autenticare le richieste API ed Element UI all'interno del sistema di storage.

Per accedere ai nodi attivi di un cluster tramite l'interfaccia utente per nodo, è necessario un account amministratore locale (non LDAP). Le credenziali dell'account non sono richieste per accedere a un nodo che non fa ancora parte di un cluster.

È possibile "gestire gli account degli amministratori del cluster" Creando, eliminando e modificando gli account amministratore del cluster, modificando la password dell'amministratore del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

Account utente

Gli account utente vengono utilizzati per controllare l'accesso alle risorse di storage su una rete basata su software NetApp Element. È necessario almeno un account utente prima di poter creare un volume.

Quando si crea un volume, questo viene assegnato a un account. Se è stato creato un volume virtuale, l'account è il container di storage.

Di seguito sono riportate alcune considerazioni aggiuntive:

- L'account contiene l'autenticazione CHAP richiesta per accedere ai volumi ad esso assegnati.
- A un account possono essere assegnati fino a 2000 volumi, ma un volume può appartenere a un solo account.
- Gli account utente possono essere gestiti dal punto di estensione Gestione NetApp Element.

Account utente del cluster autorevoli

Gli account utente del cluster autorevoli possono eseguire l'autenticazione con qualsiasi risorsa di storage associata all'istanza di NetApp Hybrid Cloud Control di nodi e cluster. Con questo account, puoi gestire volumi, account, gruppi di accesso e molto altro in tutti i cluster.

Gli account utente autorevoli vengono gestiti dal menu in alto a destra dell'opzione User Management (Gestione utente) in NetApp Hybrid Cloud Control.

Il "cluster di storage autorevole" È il cluster di storage utilizzato da NetApp Hybrid Cloud Control per

autenticare gli utenti.

Tutti gli utenti creati sul cluster di storage autorevole possono accedere al NetApp Hybrid Cloud Control. Gli utenti creati su altri cluster di storage *non possono* accedere a Hybrid Cloud Control.

- Se il nodo di gestione dispone di un solo cluster di storage, si tratta del cluster autorevole.
- Se il nodo di gestione dispone di due o più cluster di storage, uno di questi viene assegnato come cluster autorevole e solo gli utenti di quel cluster possono accedere a NetApp Hybrid Cloud Control.

Sebbene molte funzionalità di NetApp Hybrid Cloud Control funzionino con più cluster di storage, l'autenticazione e l'autorizzazione hanno limitazioni necessarie. Il limite dell'autenticazione e dell'autorizzazione è che gli utenti del cluster autorevole possono eseguire azioni su altri cluster legati a NetApp Hybrid Cloud Control anche se non sono utenti degli altri cluster di storage. Prima di procedere con la gestione di più cluster di storage, è necessario assicurarsi che gli utenti definiti nei cluster autorevoli siano definiti in tutti gli altri cluster di storage con le stesse autorizzazioni. Puoi gestire gli utenti da NetApp Hybrid Cloud Control.

Account di volume

Gli account specifici del volume sono specifici solo per il cluster di storage in cui sono stati creati. Questi account consentono di impostare autorizzazioni su volumi specifici della rete, ma non hanno alcun effetto al di fuori di tali volumi.

Gli account dei volumi vengono gestiti all'interno della tabella NetApp Hybrid Cloud Control Volumes.

Storage

Volumi

Il sistema storage NetApp Element esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel.

Lo storage degli elementi consente di creare, visualizzare, modificare, eliminare, clonare, backup o ripristino dei volumi per gli account utente. È inoltre possibile gestire ciascun volume di un cluster e aggiungere o rimuovere volumi in gruppi di accesso ai volumi.

Volumi persistenti

I volumi persistenti consentono ai dati di configurazione dei nodi di gestione di essere memorizzati in un cluster di storage specifico, piuttosto che localmente con una macchina virtuale, in modo che i dati possano essere conservati in caso di perdita o rimozione dei nodi di gestione. I volumi persistenti sono una configurazione del nodo di gestione opzionale ma consigliata.

Un'opzione per abilitare i volumi persistenti è inclusa negli script di installazione e aggiornamento quando "implementazione di un nuovo nodo di gestione". I volumi persistenti sono volumi su un cluster di storage basato su software Element che contengono informazioni di configurazione del nodo di gestione per la VM del nodo di gestione host che persistono oltre la vita della macchina virtuale. In caso di perdita del nodo di gestione, una macchina virtuale del nodo di gestione sostitutivo può riconnettersi e ripristinare i dati di configurazione per la macchina virtuale persa.

La funzionalità dei volumi persistenti, se attivata durante l'installazione o l'aggiornamento, crea automaticamente più volumi. Questi volumi, come qualsiasi volume basato su software Element, possono

essere visualizzati utilizzando l'interfaccia utente Web del software Element, il plug-in NetApp Element per vCenter Server o l'API, a seconda delle preferenze e dell'installazione. I volumi persistenti devono essere attivi e in esecuzione con una connessione iSCSI al nodo di gestione per mantenere i dati di configurazione correnti che possono essere utilizzati per il ripristino.

> I volumi persistenti associati ai servizi di gestione vengono creati e assegnati a un nuovo account durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare i volumi o l'account associato

Volumi virtuali (vVol)

VSphere Virtual Volumes è un paradigma di storage per VMware che sposta gran parte della gestione dello storage per vSphere dal sistema di storage a VMware vCenter. Con i volumi virtuali (vVol), è possibile allocare lo storage in base ai requisiti delle singole macchine virtuali.

Associazioni

Il cluster NetApp Element sceglie un endpoint del protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint del protocollo e restituisce il binding all'host ESXi. Una volta eseguito il bound, l'host ESXi può eseguire operazioni di i/o con il volume virtuale associato.

Endpoint del protocollo

Gli host VMware ESXi utilizzano proxy i/o logici noti come endpoint del protocollo per comunicare con i volumi virtuali. Gli host ESXi collegano i volumi virtuali agli endpoint del protocollo per eseguire operazioni di i/O. Quando una macchina virtuale sull'host esegue un'operazione di i/o, l'endpoint del protocollo associato indirizza l'i/o al volume virtuale con cui è associato.

Gli endpoint del protocollo in un cluster NetApp Element funzionano come unità logiche amministrative SCSI. Ogni endpoint del protocollo viene creato automaticamente dal cluster. Per ogni nodo di un cluster, viene creato un endpoint del protocollo corrispondente. Ad esempio, un cluster a quattro nodi avrà quattro endpoint di protocollo.

ISCSI è l'unico protocollo supportato per il software NetApp Element. Il protocollo Fibre Channel non è supportato. Gli endpoint del protocollo non possono essere cancellati o modificati da un utente, non sono associati a un account e non possono essere aggiunti a un gruppo di accesso al volume.

Container di storage

I container di storage sono costrutti logici che vengono mappati agli account NetApp Element e utilizzati per la creazione di report e l'allocazione delle risorse. Raggruppano capacità di storage raw o capacità di storage aggregate che il sistema di storage può fornire ai volumi virtuali. Un datastore VVol creato in vSphere viene mappato a un singolo container di storage. Per impostazione predefinita, un singolo container di storage dispone di tutte le risorse disponibili dal cluster NetApp Element. Se è necessaria una governance più granulare per il multi-tenancy, è possibile creare più container di storage.

I container di storage funzionano come gli account tradizionali e possono contenere volumi virtuali e volumi tradizionali. È supportato un massimo di quattro container di storage per cluster. Per utilizzare la funzionalità VVol, è necessario almeno un container di storage. È possibile rilevare i container di storage in vCenter durante la creazione di VVol.

Provider VASA

Per rendere vSphere consapevole della funzionalità vVol sul cluster NetApp Element, l'amministratore di vSphere deve registrare il provider VASA NetApp Element con vCenter. Il provider VASA è il percorso di controllo out-of-band tra vSphere e il cluster di elementi. È responsabile dell'esecuzione delle richieste sul cluster Element per conto di vSphere, come la creazione di macchine virtuali, la messa a disposizione di vSphere delle macchine virtuali e la pubblicità delle funzionalità di storage su vSphere.

Il provider VASA viene eseguito come parte del cluster master nel software Element. Il cluster master è un servizio altamente disponibile che esegue il failover su qualsiasi nodo del cluster in base alle necessità. In caso di failover del cluster master, il provider VASA si sposta con esso, garantendo un'elevata disponibilità per il provider VASA. Tutte le attività di provisioning e gestione dello storage utilizzano il provider VASA, che gestisce le modifiche necessarie al cluster di elementi.

Non registrare più di un provider VASA NetApp Element in una singola istanza di vCenter. Quando viene aggiunto un secondo provider VASA NetApp Element, questo rende inaccessibili tutti i datastore VVOL.

Il supporto DI VASA per un massimo di 10 vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con vCenter. Per eseguire l'installazione, seguire le istruzioni nel manifest VASA39 e scaricare il file .tar.gz da "Download di software NetApp" sito. Il provider VASA di NetApp Element utilizza un certificato NetApp. Con questa patch, il certificato viene utilizzato senza modifiche da vCenter per supportare più vCenter per l'utilizzo di VASA e VVol. Non modificare il certificato. I certificati SSL personalizzati non sono supportati da VASA.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gruppi di accesso ai volumi

Creando e utilizzando i gruppi di accesso ai volumi, è possibile controllare l'accesso a un set di volumi. Quando si associano un set di volumi e un set di iniziatori a un gruppo di accesso al volume, il gruppo di accesso concede agli iniziatori l'accesso a tale set di volumi.

I gruppi di accesso ai volumi nello storage NetApp SolidFire consentono agli IQN iSCSI Initiator o alle WWPN Fibre Channel di accedere a una raccolta di volumi. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza utilizzare l'autenticazione CHAP. Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso di rete Fibre Channel ai volumi del gruppo di accesso.

I gruppi di accesso ai volumi hanno i seguenti limiti:

- Un massimo di 128 iniziatori per gruppo di accesso al volume.
- Un massimo di 64 gruppi di accesso per volume.
- Un gruppo di accesso può essere costituito da un massimo di 2000 volumi.
- Un IQN o WWPN può appartenere a un solo gruppo di accesso al volume.
- Per i cluster Fibre Channel, un singolo volume può appartenere a un massimo di quattro gruppi di accesso.

Iniziatori

Gli iniziatori consentono ai client esterni di accedere ai volumi di un cluster, fungendo da punto di ingresso per la comunicazione tra client e volumi. È possibile utilizzare gli iniziatori per l'accesso ai volumi di storage basato su CHAP piuttosto che su account. Un singolo iniziatore, quando aggiunto a un gruppo di accesso al volume, consente ai membri del gruppo di accesso al volume di accedere a tutti i volumi di storage aggiunti al gruppo senza richiedere l'autenticazione. Un iniziatore può appartenere a un solo gruppo di accesso.

Protezione dei dati

Le funzionalità di protezione dei dati includono replica remota, snapshot dei volumi, cloning dei volumi, domini di protezione e alta disponibilità con la tecnologia Double Helix.

La protezione dei dati dello storage Element include i seguenti concetti:

- Tipi di replica remota
- Snapshot dei volumi per la protezione dei dati
- Cloni di volume
- Panoramica del processo di backup e ripristino per lo storage Element
- Domini di protezione
- Domini di protezione personalizzati
- Doppia Helix ad alta disponibilità

Tipi di replica remota

La replica remota dei dati può assumere le seguenti forme:

- Replica sincrona e asincrona tra cluster
- Replica solo Snapshot
- Replica tra cluster Element e ONTAP utilizzando SnapMirror

Per ulteriori informazioni, vedere "TR-4741: Replica remota del software NetApp Element".

Replica sincrona e asincrona tra cluster

Per i cluster che eseguono il software NetApp Element, la replica in tempo reale consente la creazione rapida di copie remote dei dati dei volumi.

È possibile associare un cluster di storage a un massimo di quattro altri cluster di storage. È possibile replicare i dati del volume in modo sincrono o asincrono da uno dei cluster di una coppia di cluster per scenari di failover e failback.

Replica sincrona

La replica sincrona replica continuamente i dati dal cluster di origine al cluster di destinazione ed è influenzata da latenza, perdita di pacchetti, jitter e larghezza di banda.

La replica sincrona è appropriata per le seguenti situazioni:

- Replica di diversi sistemi su una breve distanza
- Un sito di disaster recovery geograficamente locale rispetto all'origine
- Applicazioni sensibili al tempo e protezione dei database
- Applicazioni di business continuity che richiedono che il sito secondario agisca come sito primario quando il sito primario è inattivo

Replica asincrona

La replica asincrona replica continuamente i dati da un cluster di origine a un cluster di destinazione senza attendere i riconoscimenti dal cluster di destinazione. Durante la replica asincrona, le scritture vengono riconosciute al client (applicazione) dopo che sono state assegnate al cluster di origine.

La replica asincrona è appropriata per le seguenti situazioni:

- Il sito di disaster recovery è lontano dall'origine e l'applicazione non tollera le latenze indotte dalla rete.
- La rete che collega i cluster di origine e di destinazione presenta limitazioni di larghezza di banda.

Replica solo Snapshot

La protezione dei dati solo Snapshot replica i dati modificati in specifici punti di tempo in un cluster remoto. Vengono replicati solo gli snapshot creati nel cluster di origine. Le scritture attive dal volume di origine non lo sono.

È possibile impostare la frequenza delle repliche degli snapshot.

La replica di Snapshot non influisce sulla replica asincrona o sincrona.

Replica tra cluster Element e ONTAP utilizzando SnapMirror

Con la tecnologia NetApp SnapMirror, è possibile replicare le snapshot acquisite con il software NetApp Element su ONTAP per scopi di disaster recovery. In una relazione SnapMirror, Element è un endpoint e ONTAP è l'altro.

SnapMirror è una tecnologia di replica Snapshot di NetApp che facilita il disaster recovery, progettata per il failover dallo storage primario allo storage secondario in un sito geograficamente remoto. La tecnologia SnapMirror crea una replica, o mirroring, dei dati di lavoro nello storage secondario da cui è possibile continuare a servire i dati in caso di interruzione nel sito primario. I dati vengono mirrorati a livello di volume.

La relazione tra il volume di origine nello storage primario e il volume di destinazione nello storage secondario viene definita relazione di protezione dei dati. I cluster sono definiti endpoint in cui risiedono i volumi e i volumi che contengono i dati replicati devono essere trasmessi in peering. Una relazione peer consente a cluster e volumi di scambiare dati in modo sicuro.

SnapMirror viene eseguito in modo nativo sui controller NetApp ONTAP ed è integrato in Element, che viene eseguito sui cluster NetApp HCI e SolidFire. La logica di controllo di SnapMirror risiede nel software ONTAP; pertanto, tutte le relazioni di SnapMirror devono coinvolgere almeno un sistema ONTAP per eseguire il lavoro di coordinamento. Gli utenti gestiscono le relazioni tra i cluster Element e ONTAP principalmente attraverso

l'interfaccia utente Element; tuttavia, alcune attività di gestione risiedono in Gestione di sistema NetApp ONTAP. Gli utenti possono inoltre gestire SnapMirror tramite l'interfaccia CLI e l'API, entrambe disponibili in ONTAP ed Element.

Vedere "TR-4651: Architettura e configurazione di NetApp SolidFire SnapMirror" (accesso richiesto)

È necessario attivare manualmente la funzionalità SnapMirror a livello di cluster utilizzando il software Element. La funzionalità SnapMirror è disattivata per impostazione predefinita e non viene attivata automaticamente durante una nuova installazione o un aggiornamento.

Dopo aver attivato SnapMirror, è possibile creare relazioni SnapMirror dalla scheda Data Protection (protezione dati) del software Element.

Il software NetApp Element 10.1 e versioni successive supporta la funzionalità SnapMirror per copiare e ripristinare le snapshot con i sistemi ONTAP.

I sistemi che eseguono Element 10.1 e versioni successive includono codice in grado di comunicare direttamente con SnapMirror su sistemi ONTAP con versione 9.3 o superiore. L'API Element fornisce metodi per abilitare la funzionalità SnapMirror su cluster, volumi e snapshot. Inoltre, l'interfaccia utente di Element include funzionalità per gestire le relazioni di SnapMirror tra il software Element e i sistemi ONTAP.

A partire dai sistemi Element 10.3 e ONTAP 9.4, è possibile replicare i volumi originati da ONTAP in volumi di elementi in casi di utilizzo specifici con funzionalità limitate.

Per ulteriori informazioni, consultare la documentazione di ONTAP.

Snapshot dei volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume che può essere utilizzata in seguito per ripristinare un volume all'ora specifica.

Sebbene le snapshot siano simili ai cloni dei volumi, le snapshot sono semplicemente repliche dei metadati dei volumi, pertanto non è possibile montarle o scriverle. La creazione di uno snapshot di volume richiede anche solo una piccola quantità di risorse e spazio di sistema, rendendo la creazione dello snapshot più rapida rispetto alla clonazione.

È possibile replicare gli snapshot in un cluster remoto e utilizzarli come copia di backup del volume. In questo modo è possibile eseguire il rollback di un volume a un punto specifico utilizzando lo snapshot replicato; è inoltre possibile creare un clone di un volume da uno snapshot replicato.

È possibile eseguire il backup delle snapshot da un cluster di elementi a un archivio di oggetti esterno o a un altro cluster di elementi. Quando si esegue il backup di uno snapshot in un archivio di oggetti esterno, è necessario disporre di una connessione all'archivio di oggetti che consenta le operazioni di lettura/scrittura.

È possibile creare un'istantanea di uno o più volumi per la protezione dei dati.

Cloni di volume

Un clone di uno o più volumi è una copia point-in-time dei dati. Quando si clonano un volume, il sistema crea uno snapshot del volume e quindi una copia dei dati a cui fa riferimento lo snapshot.

Si tratta di un processo asincrono e la quantità di tempo richiesta dal processo dipende dalla dimensione del volume che si sta clonando e dal carico corrente del cluster.

Il cluster supporta fino a due richieste di cloni in esecuzione per volume alla volta e fino a otto operazioni di

cloni dei volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per l'elaborazione successiva.

Panoramica del processo di backup e ripristino per lo storage Element

È possibile eseguire il backup e il ripristino dei volumi su altri storage SolidFire, nonché su archivi di oggetti secondari compatibili con Amazon S3 o OpenStack Swift.

È possibile eseguire il backup di un volume nei seguenti modi:

- Un cluster di storage SolidFire
- Un archivio di oggetti Amazon S3
- Un archivio di oggetti OpenStack Swift

Quando ripristini i volumi da OpenStack Swift o Amazon S3, hai bisogno di informazioni manifeste dal processo di backup originale. Se si sta ripristinando un volume di cui è stato eseguito il backup su un sistema di storage SolidFire, non sono necessarie informazioni sul manifesto.

Domini di protezione

Un dominio di protezione è un nodo o un insieme di nodi raggruppati in modo che qualsiasi parte o anche tutto l'IT possa guastarsi, mantenendo al contempo la disponibilità dei dati. I domini di protezione consentono a un cluster di storage di riparare automaticamente in caso di perdita di uno chassis (affinità dello chassis) o di un intero dominio (gruppo di chassis).

È possibile attivare manualmente il monitoraggio del dominio di protezione utilizzando il punto di estensione Configurazione NetApp Element nel plug-in NetApp Element per vCenter Server. È possibile selezionare una soglia del dominio di protezione in base ai domini del nodo o dello chassis. È inoltre possibile attivare il monitoraggio del dominio di protezione utilizzando l'API Element o l'interfaccia utente Web.

Un layout del dominio di protezione assegna ogni nodo a un dominio di protezione specifico.

Sono supportati due diversi layout del dominio di protezione, denominati livelli di dominio di protezione.

- A livello di nodo, ciascun nodo si trova nel proprio dominio di protezione.
- A livello di chassis, solo i nodi che condividono uno chassis si trovano nello stesso dominio di protezione.
  - Il layout a livello di chassis viene determinato automaticamente dall'hardware quando il nodo viene aggiunto al cluster.
  - In un cluster in cui ciascun nodo si trova in uno chassis separato, questi due livelli sono funzionalmente identici.

Quando si crea un nuovo cluster, se si utilizzano nodi di storage che risiedono in uno chassis condiviso, si consiglia di progettare la protezione dai guasti a livello di chassis utilizzando la funzione Protection Domains.

Domini di protezione personalizzati

È possibile definire un layout personalizzato del dominio di protezione che corrisponda al layout di chassis e nodi specifico e in cui ciascun nodo è associato a un solo dominio di protezione personalizzato. Per impostazione predefinita, ogni nodo viene assegnato allo stesso dominio di protezione personalizzato predefinito.

Se non sono assegnati domini di protezione personalizzati:

- Il funzionamento del cluster non viene influenzato.
- Il livello personalizzato non è tollerante né resiliente.

Quando si configurano i domini di protezione personalizzati per un cluster, sono disponibili tre livelli di protezione, visibili dalla dashboard dell'interfaccia utente Web Element:

- Non protetto: Il cluster di storage non è protetto dal guasto di uno dei suoi domini di protezione personalizzati. Per risolvere questo problema, aggiungere ulteriore capacità di storage al cluster o riconfigurare i domini di protezione personalizzati del cluster per proteggere il cluster da eventuali perdite di dati.
- Tolleranza agli errori: Il cluster di storage dispone di capacità libera sufficiente per evitare la perdita di dati dopo il guasto di uno dei suoi domini di protezione personalizzati.
- Fault Resilient (resiliente agli errori): Il cluster di storage dispone di capacità libera sufficiente per eseguire la riparazione automatica dopo il guasto di uno dei domini di protezione personalizzati. Una volta completato il processo di riparazione, il cluster sarà protetto dalla perdita di dati in caso di guasto di altri domini.

Se viene assegnato più di un dominio di protezione personalizzato, ciascun sottosistema assegna i duplicati a domini di protezione personalizzati separati. Se ciò non è possibile, viene ripristinata l'assegnazione di duplicati a nodi separati. Ogni sottosistema (ad esempio, bin, slice, provider di endpoint del protocollo e gruppo) esegue questa operazione in modo indipendente.

È possibile configurare domini di protezione personalizzati utilizzando i seguenti metodi API:

- "GetProtectionDomainLayout" - Indica lo chassis e il dominio di protezione personalizzato in cui si trova ciascun nodo.
- "SetProtectionDomainLayout" Consente di assegnare un dominio di protezione personalizzato a ciascun nodo.

Doppia Helix ad alta disponibilità

La protezione dei dati Double Helix è un metodo di replica che distribuisce almeno due copie ridondanti dei dati su tutti i dischi all'interno di un sistema. L'approccio "RAID-less" consente a un sistema di assorbire più guasti simultanei in tutti i livelli del sistema storage e di ripararli rapidamente.

Performance e qualità del servizio

Un cluster di storage SolidFire è in grado di fornire parametri di qualità del servizio (QoS) per volume. È possibile garantire le prestazioni del cluster misurate in input e output al secondo (IOPS) utilizzando tre parametri configurabili che definiscono QoS: IOPS min, IOPS max e IOPS burst.

SolidFire Active IQ dispone di una pagina di consigli sulla qualità del servizio che fornisce consigli sulla configurazione ottimale e sull'impostazione delle impostazioni di qualità del servizio.

Parametri della qualità del servizio

I parametri IOPS sono definiti nei seguenti modi:

- **IOPS minimo** - il numero minimo di IOPS (Inputs and Outputs per Second) sostenuti che il cluster di storage fornisce a un volume. Il livello minimo di IOPS configurato per un volume è il livello garantito di performance per un volume. Le performance non scendono al di sotto di questo livello.
- **Massimo IOPS** - il numero massimo di IOPS sostenuti che il cluster di storage fornisce a un volume. Quando i livelli di IOPS del cluster sono estremamente elevati, questo livello di performance IOPS non viene superato.
- **Burst IOPS** - numero massimo di IOPS consentiti in uno scenario a burst breve. Se un volume è stato eseguito al di sotto del massimo IOPS, i crediti burst vengono accumulati. Quando i livelli di performance diventano molto elevati e vengono trasferiti ai livelli massimi, sono consentiti brevi burst di IOPS sul volume.

  Il software Element utilizza gli IOPS Burst quando un cluster viene eseguito in uno stato di basso utilizzo degli IOPS del cluster.

  Un singolo volume può accumulare IOPS burst e utilizzare i crediti per ottenere un burst oltre i massimi IOPS fino al livello di IOPS burst per un "periodo di burst" impostato. Un volume può esplodere fino a 60 secondi se il cluster ha la capacità di ospitare il burst. Un volume aumenta di un secondo di credito burst (fino a un massimo di 60 secondi) per ogni secondo in cui il volume scende al di sotto del limite massimo di IOPS.

  Gli IOPS burst sono limitati in due modi:

  - Un volume può raggiungere un picco superiore al massimo IOPS per un numero di secondi pari al numero di crediti burst accumulati dal volume.
  - Quando un volume supera l'impostazione di massimo IOPS, è limitato dall'impostazione di burst IOPS. Pertanto, gli IOPS burst non superano mai l'impostazione di IOPS burst per il volume.
- **Larghezza di banda massima effettiva** - la larghezza di banda massima viene calcolata moltiplicando il numero di IOPS (in base alla curva QoS) per la dimensione di io.

  Esempio: Le impostazioni dei parametri QoS di 100 IOPS min, 1000 IOPS max e 1500 IOPS burst hanno i seguenti effetti sulla qualità delle performance:

  - I carichi di lavoro sono in grado di raggiungere e sostenere un massimo di 1000 IOPS fino a quando la condizione di conflitto del carico di lavoro per gli IOPS non diventa evidente nel cluster. Gli IOPS vengono quindi ridotti in modo incrementale fino a quando gli IOPS su tutti i volumi non rientrano negli intervalli di QoS designati e il conflitto per le performance viene ridotto.
  - Le performance su tutti i volumi vengono trasferite al minimo IOPS di 100. I livelli non scendono al di sotto dell'impostazione min IOPS, ma potrebbero rimanere superiori a 100 IOPS quando il conflitto del carico di lavoro viene sollevato.
  - Le performance non sono mai superiori a 1000 IOPS o inferiori a 100 IOPS per un periodo prolungato. Sono consentite performance di 1500 IOPS (burst IOPS), ma solo per quei volumi che hanno accumulato crediti burst con un'esecuzione inferiore al massimo di IOPS e sono consentiti solo per brevi periodi di tempo. I livelli di burst non sono mai sostenuti.

Limiti del valore QoS

Ecco i possibili valori minimi e massimi per QoS.

Parametri	Valore minimo	Predefinito	4 KB	5 8 KB	6 16KB	262 KB
IOPS minimi	50	50	15,000	9,375*	5556*	385*

Parametri	Valore minimo	Predefinito	4 KB	5 8 KB	6 16KB	262 KB
IOPS max	100	15,000	200,000**	125,000	74,074	5128
IOPS burst	100	15,000	200,000**	125,000	74.074	5128

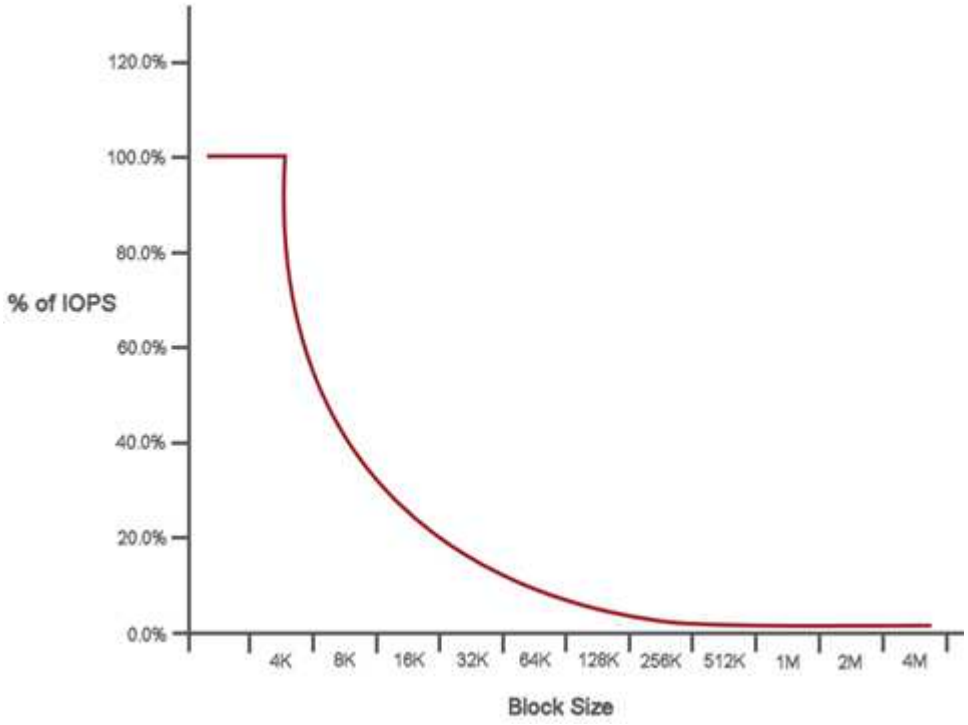
*Queste stime sono approssimative. **È possibile impostare IOPS massimi e IOPS burst fino a 200,000; tuttavia, questa impostazione consente solo di rimuovere efficacemente le prestazioni di un volume. Le performance massime reali di un volume sono limitate dall'utilizzo del cluster e dalle performance per nodo.

Performance QoS

La curva delle performance QoS mostra la relazione tra la dimensione del blocco e la percentuale di IOPS.

Le dimensioni dei blocchi e la larghezza di banda hanno un impatto diretto sul numero di IOPS che un'applicazione può ottenere. Il software Element tiene conto delle dimensioni dei blocchi ricevuti normalizzando le dimensioni dei blocchi a 4k. In base al carico di lavoro, il sistema potrebbe aumentare le dimensioni dei blocchi. Con l'aumentare delle dimensioni dei blocchi, il sistema aumenta la larghezza di banda fino a raggiungere un livello necessario per elaborare blocchi di dimensioni maggiori. Man mano che la larghezza di banda aumenta il numero di IOPS, il sistema è in grado di raggiungere una diminuzione.

La curva delle performance di QoS mostra la relazione tra l'aumento delle dimensioni dei blocchi e la diminuzione della percentuale di IOPS:



Ad esempio, se le dimensioni dei blocchi sono 4k e la larghezza di banda è 4000 kbps, gli IOPS sono 1000. Se le dimensioni dei blocchi aumentano fino a 8k, la larghezza di banda aumenta fino a 5000 kbps e gli IOPS diminuiscono fino a 625. Tenendo conto delle dimensioni dei blocchi, il sistema garantisce che i carichi di lavoro con priorità più bassa che utilizzano blocchi di dimensioni più elevate, come backup e attività dell'hypervisor, non richiedano una quantità eccessiva delle performance richieste dal traffico con priorità più alta utilizzando blocchi di dimensioni più piccole.

Policy di QoS

Una policy di QoS consente di creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi.

Le policy di QoS sono le migliori per gli ambienti di servizio, ad esempio con database, applicazioni o server di infrastruttura che raramente si riavviano e necessitano di un accesso costante e uguale allo storage. La qualità del servizio dei singoli volumi è la soluzione migliore per le macchine virtuali di uso leggero, come desktop virtuali o macchine virtuali specializzate di tipo Kiosk, che possono essere riavviate, accese o spente ogni giorno o più volte al giorno.

Le policy QoS e QoS non devono essere utilizzate insieme. Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascrive e regola i valori dei criteri QoS per le impostazioni QoS del volume.

Il cluster selezionato deve essere l'elemento 10.0 o successivo per utilizzare i criteri QoS; in caso contrario, le funzioni dei criteri QoS non sono disponibili.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

Requisiti

Prima di iniziare, è necessario esaminare i prerequisiti per l'implementazione del software NetApp Element, inclusi i requisiti di rete e di porta.

- "Requisiti di rete"
- "Configurazione dello switch"
- "Requisiti delle porte di rete"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

Networking

La configurazione di rete per un sistema SolidFire comprende i requisiti di switch e porte. L'implementazione di questi elementi dipende dal sistema in uso.

Per ulteriori informazioni

- "Configurazione dello switch per i cluster che eseguono il software Element"
- "Requisiti delle porte di rete"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurazione dello switch per i cluster che eseguono il software Element

Il sistema software NetApp Element dispone di determinati requisiti e Best practice relativi allo switch per ottenere performance di storage ottimali.

I nodi di storage richiedono switch Ethernet da 10 o 25 GbE, a seconda dell'hardware del nodo specifico, per i servizi di storage iSCSI e la comunicazione dei servizi intra-cluster del nodo. Gli switch 1GbE possono essere utilizzati per questi tipi di traffico:

- Gestione del cluster e dei nodi
- Traffico di gestione intra-cluster tra i nodi
- Traffico tra i nodi del cluster e la macchina virtuale del nodo di gestione

Best practice: quando si configurano gli switch Ethernet per il traffico cluster, è necessario implementare le seguenti Best practice:

- Per il traffico non storage nel cluster, implementare una coppia di switch 1GbE per fornire alta disponibilità e condivisione del carico.
- Sugli switch della rete di storage, implementare gli switch a coppie e configurare e utilizzare i frame jumbo (una dimensione MTU di 9216 byte). In questo modo si garantisce una corretta installazione ed elimina gli errori di rete dovuti a pacchetti frammentati.

L'implementazione degli elementi richiede almeno due segmenti di rete, uno per ciascuno dei seguenti tipi di traffico:

- Gestione
- Storage/dati

A seconda dei modelli di nodo storage NetApp H-Series e della configurazione di cablaggio pianificata, è possibile separare fisicamente queste reti utilizzando switch separati o separarle logicamente utilizzando VLAN. Per la maggior parte delle implementazioni, tuttavia, è necessario separare logicamente queste reti utilizzando VLAN.

I nodi storage devono essere in grado di comunicare prima, durante e dopo l'implementazione.

Se si stanno implementando reti di gestione separate per i nodi di storage, assicurarsi che tali reti di gestione dispongano di percorsi di rete tra di esse. A queste reti devono essere assegnati gateway e deve essere presente un percorso tra i gateway. Assicurarsi che ogni nuovo nodo disponga di un gateway assegnato per facilitare la comunicazione tra i nodi e le reti di gestione.

NetApp Element richiede quanto segue:

- Tutte le porte switch collegate ai nodi storage NetApp H-Series devono essere configurate come porte edge spanning tree.
  - Sugli switch Cisco, a seconda del modello dello switch, della versione del software e del tipo di porta, è possibile eseguire questa operazione con uno dei seguenti comandi:
    - `spanning-tree port type edge`
    - `spanning-tree port type edge trunk`
    - `spanning-tree portfast`
    - `spanning-tree portfast trunk`
  - Sui centralini Mellanox, è possibile eseguire questa operazione con `spanning-tree port type edge` comando.
- Gli switch che gestiscono il traffico di storage devono supportare velocità di almeno 10 GbE per porta (sono supportati fino a 25 GbE per porta).
- Gli switch che gestiscono il traffico di gestione devono supportare velocità di almeno 1 GbE per porta.
- È necessario configurare i frame jumbo sulle porte dello switch che gestiscono il traffico di storage. Gli host devono essere in grado di inviare pacchetti da 9000 byte end-to-end per una corretta installazione.
- La latenza di rete di andata e ritorno tra tutti i nodi di storage non deve superare i 2 ms.

Alcuni nodi offrono funzionalità di gestione out-of-band aggiuntive tramite una porta di gestione dedicata. I nodi

NetApp H300S, H500S e H700S consentono anche l'accesso IPMI tramite la porta A. Come Best practice, dovresti semplificare la gestione remota configurando la gestione fuori banda per tutti i nodi del tuo ambiente.

Per ulteriori informazioni

- "Requisiti di rete e switch NetApp HCI"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Requisiti delle porte di rete

Potrebbe essere necessario abilitare le seguenti porte TCP e UDP attraverso il firewall perimetrale del data center, in modo da poter gestire il sistema in remoto e consentire ai client esterni al data center di connettersi alle risorse. Alcune di queste porte potrebbero non essere necessarie, a seconda delle modalità di utilizzo del sistema.

Tutte le porte sono TCP, se non diversamente specificato, e tutte le porte TCP devono supportare la comunicazione handshake a tre vie tra il server di supporto NetApp, il nodo di gestione e i nodi che eseguono il software Element. Ad esempio, l'host su un'origine del nodo di gestione comunica con l'host su una destinazione MVIP del cluster di storage attraverso la porta TCP 443, e l'host di destinazione comunica nuovamente con l'host di origine attraverso qualsiasi porta.

Abilitare ICMP tra il nodo di gestione, i nodi che eseguono il software Element e il cluster MVIP.

Nella tabella vengono utilizzate le seguenti abbreviazioni:

- MIP: Indirizzo IP di gestione, un indirizzo per nodo
- SIP: Indirizzo IP dello storage, un indirizzo per nodo
- MVIP: Indirizzo IP virtuale di gestione
- SVIP: Indirizzo IP virtuale dello storage

Origine	Destinazione	Porta	Descrizione
Client iSCSI	Cluster di storage MVIP	443	(Facoltativo) accesso all'interfaccia utente e alle API
Client iSCSI	Cluster di storage SVIP	3260	Comunicazioni iSCSI del client
Client iSCSI	SIP. Nodo storage	3260	Comunicazioni iSCSI del client
Nodo di gestione	`sfsupport.solidfire.com`	22	Tunnel SSH inverso per l'accesso al supporto
Nodo di gestione	MIP nodo storage	22	Accesso SSH per il supporto
Nodo di gestione	Server DNS	53 TCP/UDP	Ricerca DNS

Origine	Destinazione	Porta	Descrizione
Nodo di gestione	MIP nodo storage	442	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	Cluster di storage MVIP	442	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	`monitoring.solidfire.com`	443	Report del cluster di storage a Active IQ
Nodo di gestione	Cluster di storage MVIP	443	Accesso API e UI agli aggiornamenti del software Element e del nodo di storage
Nodo di gestione	repo.netapp.com	443	Fornisce l'accesso ai componenti necessari per installare/aggiornare l'implementazione on-premise.
Nodo di gestione	Nodo di storage BMC/IPMI	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
Nodo di gestione	Nodo di controllo	9442	Servizio API di configurazione per nodo
Nodo di gestione	Server vCenter	9443	Registrazione del plug-in vCenter. La porta può essere chiusa al termine della registrazione.
Server SNMP	Cluster di storage MVIP	161 UDP	Polling SNMP
Server SNMP	MIP nodo storage	161 UDP	Polling SNMP
Nodo di storage BMC/IPMI	Nodo di gestione	623 UDP	Porta RMCP. Questo è necessario per gestire i sistemi abilitati IPMI.
MIP nodo storage	Server DNS	53 TCP/UDP	Ricerca DNS
MIP nodo storage	Nodo di gestione	80	Aggiornamenti del software Element
MIP nodo storage	Endpoint S3/Swift	80	(Opzionale) comunicazione HTTP con l'endpoint S3/Swift per backup e ripristino
MIP nodo storage	Server NTP	123 UDP	NTP
MIP nodo storage	Nodo di gestione	162 UDP	(Facoltativo) trap SNMP

Origine	Destinazione	Porta	Descrizione
MIP nodo storage	Server SNMP	162 UDP	(Facoltativo) trap SNMP
MIP nodo storage	Server LDAP	389 TCP/UDP	(Facoltativo) Ricerca LDAP
MIP nodo storage	Nodo di gestione	443	Aggiornamenti del firmware dello storage Element
MIP nodo storage	Cluster di storage remoto MVIP	443	Comunicazione di accoppiamento del cluster di replica remota
MIP nodo storage	MIP nodo storage remoto	443	Comunicazione di accoppiamento del cluster di replica remota
MIP nodo storage	Endpoint S3/Swift	443	(Opzionale) comunicazione HTTPS con l'endpoint S3/Swift per backup e ripristino
MIP nodo storage	Nodo di gestione	514 TCP/UDP 10514 TCP/UDP	Inoltro syslog
MIP nodo storage	Server syslog	514 TCP/UDP 10514 TCP/UDP	Inoltro syslog
MIP nodo storage	Server LDAPS	636 TCP/UDP	Ricerca LDAPS
MIP nodo storage	MIP nodo storage remoto	2181	Comunicazione tra cluster per la replica remota
SIP. Nodo storage	SIP. Nodo storage remoto	2181	Comunicazione tra cluster per la replica remota
SIP. Nodo storage	SIP. Nodo storage	3260	ISCSI internodo
SIP. Nodo storage	SIP. Nodo storage remoto	da 4000 a 4020	Trasferimento dei dati da nodo a nodo per la replica remota
PC dell'amministratore di sistema	Nodo di gestione	442	Accesso dell'interfaccia utente HTTPS al nodo di gestione
PC dell'amministratore di sistema	MIP nodo storage	442	Accesso API e interfaccia utente HTTPS al nodo di storage

Origine	Destinazione	Porta	Descrizione
PC dell'amministratore di sistema	Nodo di gestione	443	Accesso API e interfaccia utente HTTPS al nodo di gestione
PC dell'amministratore di sistema	Cluster di storage MVIP	443	Accesso API e interfaccia utente HTTPS al cluster di storage
PC dell'amministratore di sistema	Serie BMC (Baseboard Management Controller)/IPMI (Intelligent Platform Management Interface) H410 e H600 del nodo storage	443	Accesso API e interfaccia utente HTTPS al controllo remoto del nodo
PC dell'amministratore di sistema	MIP nodo storage	443	Creazione di cluster di storage HTTPS, accesso UI post-implementazione al cluster di storage
PC dell'amministratore di sistema	Nodo storage serie BMC/IPMI H410 e H600	623 UDP	Porta Remote Management Control Protocol. Questo è necessario per gestire i sistemi abilitati IPMI.
PC dell'amministratore di sistema	Nodo di controllo	8080	Interfaccia utente Web nodo di controllo per nodo
Server vCenter	Cluster di storage MVIP	443	Accesso all'API del plug-in vCenter
Server vCenter	Plug-in remoto	8333	Servizio Remote vCenter Plug-in
Server vCenter	Nodo di gestione	8443	(Facoltativo) servizio QoSSIOC vCenter Plug-in.
Server vCenter	Cluster di storage MVIP	8444	Accesso al provider vCenter VASA (solo VVol)
Server vCenter	Nodo di gestione	9443	Registrazione del plug-in vCenter. La porta può essere chiusa al termine della registrazione.

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Provalo

Scopri le risorse e gli strumenti per iniziare a utilizzare il software Element.

- "Lab on Demand per la flessibilità dello storage nel cloud privato con Element (accesso richiesto)": Questo laboratorio presenta i concetti di scale-out senza limitazioni, performance garantite dei carichi di lavoro e automazione dell'infrastruttura storage che si applicano ai sistemi storage che eseguono il software Element.
- "Prova le funzionalità di storage utilizzando Element Demo Node": Element Demo Node è una versione della macchina virtuale VMware del software Element, che offre un modo semplice per dimostrare molte delle principali funzionalità di storage dei prodotti NetApp HCI e SolidFire.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

Prova le funzionalità di storage utilizzando Element Demo Node

"Nodo demo elemento" È una versione di macchine virtuali VMware del software Element, che offre un modo semplice per dimostrare molte delle principali funzionalità di storage dei prodotti NetApp HCI e SolidFire. Il nodo demo consente agli sviluppatori di codificare in base all'API Element senza la necessità di hardware fisico. È confezionato come file OVA per una facile implementazione VMware.

Funzionalità supportate:

Element Demo Node deve essere utilizzato solo come strumento di dimostrazione e sviluppo. Prima di utilizzare il nodo dimostrativo, tenere presenti le seguenti limitazioni funzionali:

- Element Demo Node non supporta il clustering. Funziona solo come cluster a nodo singolo.
- Non supporta gli aggiornamenti degli elementi. Per eseguire una dimostrazione di una versione più recente di Element, è necessario installare una nuova VM del nodo demo.
- Non è destinato a dimostrare le performance dello storage. Le performance osservate sul nodo demo non sono in alcun modo indicative delle performance sui cluster fisici.
- Non è possibile aggiungere nodi demo ai cluster NetApp HCI o SolidFire.
- Le VLAN VRF non sono supportate (sono supportate le VLAN con tag standard).
- Il servizio multi-drive slice (MDSS) non è supportato.
- Element Demo Node è supportato solo con datastore VMFS. I VVol non sono supportati.
- Le funzionalità di configurazione e monitoraggio basate su hardware non funzionano con il nodo demo.
- Supporta un massimo di 10 snapshot per volume.
- Supporta un massimo di 20 account per nodo/cluster.
- Supporta un massimo di 100 volumi per account.
- Supporta un massimo di 200 vVol per account.

- Supporta una dimensione massima del volume di 100 GiB.
- Supporta un limite di cluster sostenuto di 3000 IOPS.

> Si applicano tutte le altre limitazioni del software Element. Per ulteriori informazioni, consulta le ultime note di rilascio del software Element.

Requisiti delle macchine virtuali

- Capacità totale di 240 GB (le dimensioni e il numero dei dischi virtuali per la macchina virtuale non possono essere modificati. Qualsiasi storage aggiuntivo presentato tramite l'hypervisor viene ignorato dal sistema operativo guest).
- Disco root da 60 GB
- Thick provisioning/ansioso azzerato (un'unità di metadati da 30 GB o tre unità a blocchi da 50 GB) o thin provisioning/ansioso azzerato (**consigliato**) (un'unità di metadati da 30 GB o tre unità a blocchi da 50 GB)
- Due vCPU (completamente riservate)
- 16 GB di RAM (completamente riservata)
- HBA singolo per tutti i dischi, LSI Logic Parallel
- Due vNIC, entrambe vmxnet3 (una gestione, uno storage)

Requisiti dell'host

- ESXI 6.0 o 6.5 per Element Demo Node 11.7 VM
- ESXi 6.5 per Element Demo Node 12.0 e 12.2 VM
- ESXi 6.7 e 7.0 per Element Demo Node 12.3 VM
- Architettura Intel® multi-core a 64 bit

Nodo demo elemento di download

Il software Element Demo Node è un insieme di file VMware che sono stati confezionati in un file .ova.

Installare Element Demo Node su VMware ESXi

L'installazione di Element Demo Node su VMware ESXi comporta le seguenti attività:

- Configurare le interfacce di rete
- Registrare il nodo demo su un server ESXi
- Avviare il nodo demo su un server ESXi

Configurare le interfacce di rete

L'elemento Demo Node richiede due reti di macchine virtuali separate. Uno per il traffico di storage e l'altro per il traffico di gestione. È necessario configurare la rete di storage in modo che supporti i frame jumbo.

Registrare il nodo demo su un server ESXi

Per registrare Element Demo Node su un server ESXi, è necessario implementare il file .ova del nodo demo utilizzando il client vSphere.

Fasi

1. Accedere a vSphere Client e selezionare l'host ESXi dal pannello di inventario.
2. Selezionare **file** > **Deploy OVF Template**.

   Viene avviata la procedura guidata Deploy OVF Template Wizard.

3. Nella pagina **Select template** (Seleziona modello), individuare il file OVA scaricato e selezionare **Open** (Apri).
4. Selezionare **Avanti**.
5. Nella pagina **Nome e posizione**, specificare un nome e una posizione per il modello distribuito, quindi selezionare **Avanti**.
6. Nella pagina **Seleziona una risorsa**, individuare la posizione in cui si desidera eseguire il modello e selezionare **Avanti**.
7. Verificare i dettagli e selezionare **Avanti**.
8. Nella pagina Select storage (Seleziona storage), selezionare la posizione in cui si desidera memorizzare i file della macchina virtuale, quindi selezionare **Next** (Avanti).
9. Nella pagina **Select networks** (Seleziona reti), mappare la rete utilizzata nel file OVA sulle due reti di macchine virtuali separate presenti nell'inventario e selezionare **Next** (Avanti).
10. Nella pagina **Pronto per il completamento**, verificare i dettagli sulla macchina virtuale che si sta creando, quindi selezionare **fine**.

   Il completamento dell'implementazione del nodo demo potrebbe richiedere alcuni minuti.

Avviare il nodo demo su un server ESXi

Avviare la VM del nodo demo per accedere a Element tramite la console VMware ESXi.

Fasi

1. In vSphere Client, selezionare il nodo demo VM creato.
2. Selezionare la scheda **Riepilogo** per visualizzare i dettagli relativi a questa macchina virtuale.
3. Selezionare **Power on** (accensione) per avviare la macchina virtuale.
4. Selezionare **Avvia console Web**.
5. Utilizzare l'interfaccia telefonica utente per configurare il nodo demo. Per ulteriori informazioni, vedere "Configurare un nodo di storage".

Come ottenere supporto

Element Demo Node è disponibile su base volontaria Best-effort. Per assistenza, inviare le domande al "Forum nodo demo elemento".

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Pagina di download di Element Demo Node (accesso obbligatorio)"

Installazione e manutenzione dell’hardware

Scopri di più sull’installazione e la manutenzione dell’hardware serie H e SF.

- Informazioni sull’hardware H410S e H610S
- Informazioni sull’hardware della serie SF
- Tornare alle informazioni immagine di fabbrica

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Informazioni sull’hardware H410S e H610S

Sono disponibili informazioni sull’installazione e la manutenzione dei nodi di storage H-Series.

Di seguito sono riportati i collegamenti ai contenuti relativi all’installazione e alla manutenzione:

- "Installare nodi storage H-Series"
- "Sostituire un nodo H410S"
- "Sostituire un nodo H610S"
- "Sostituire i dischi"
- "Sostituire un alimentatore"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Installare nodi storage H-Series

Prima di iniziare a utilizzare il sistema storage all-flash, è necessario installare e configurare correttamente i nodi di storage.

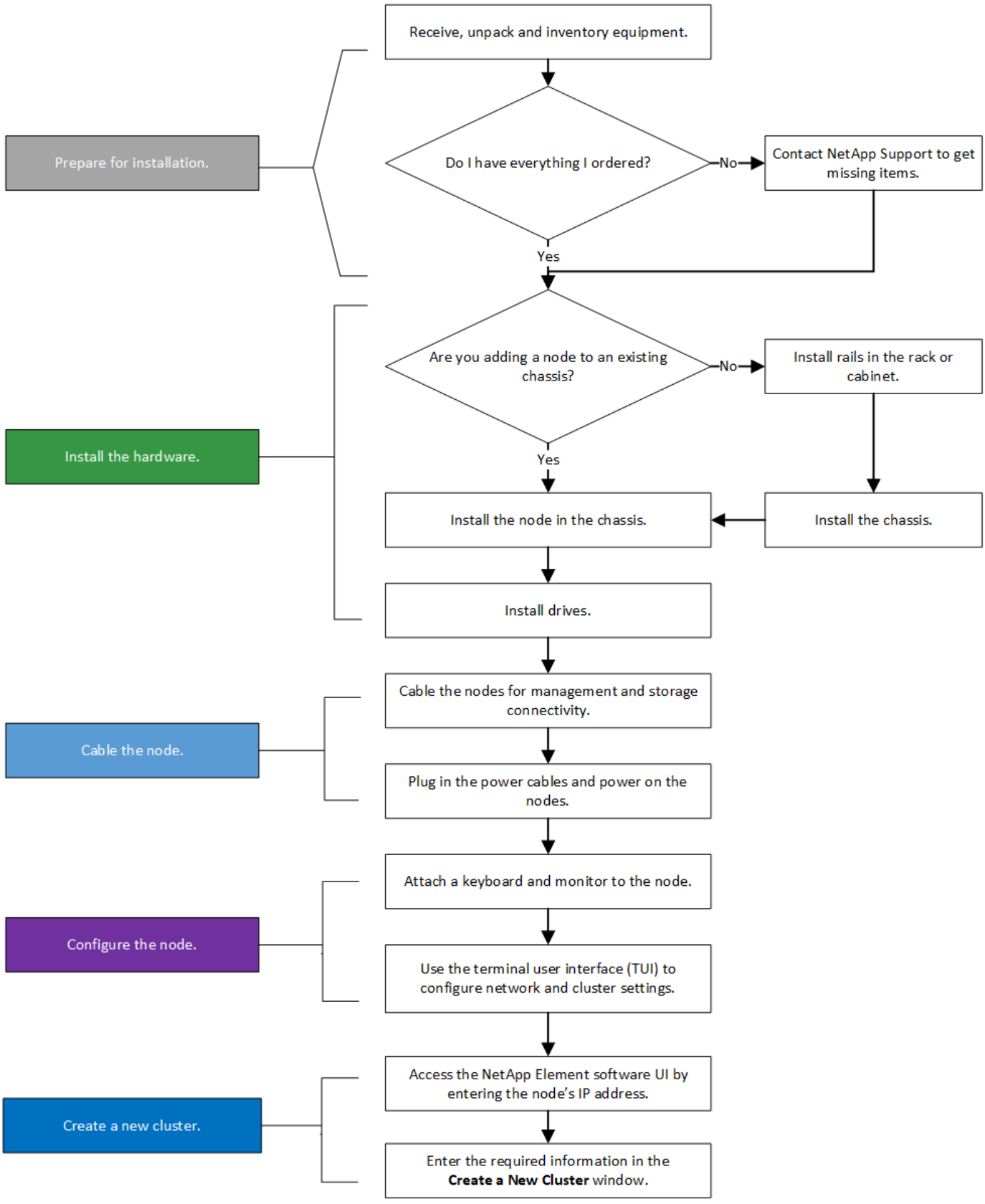
Vedere "poster" per una rappresentazione visiva delle istruzioni.

- Diagrammi del flusso di lavoro
- Preparazione per l’installazione
- Montare le guide
- Installare e cablare i nodi
- Configurare i nodi
- Creare un cluster

Diagrammi del flusso di lavoro

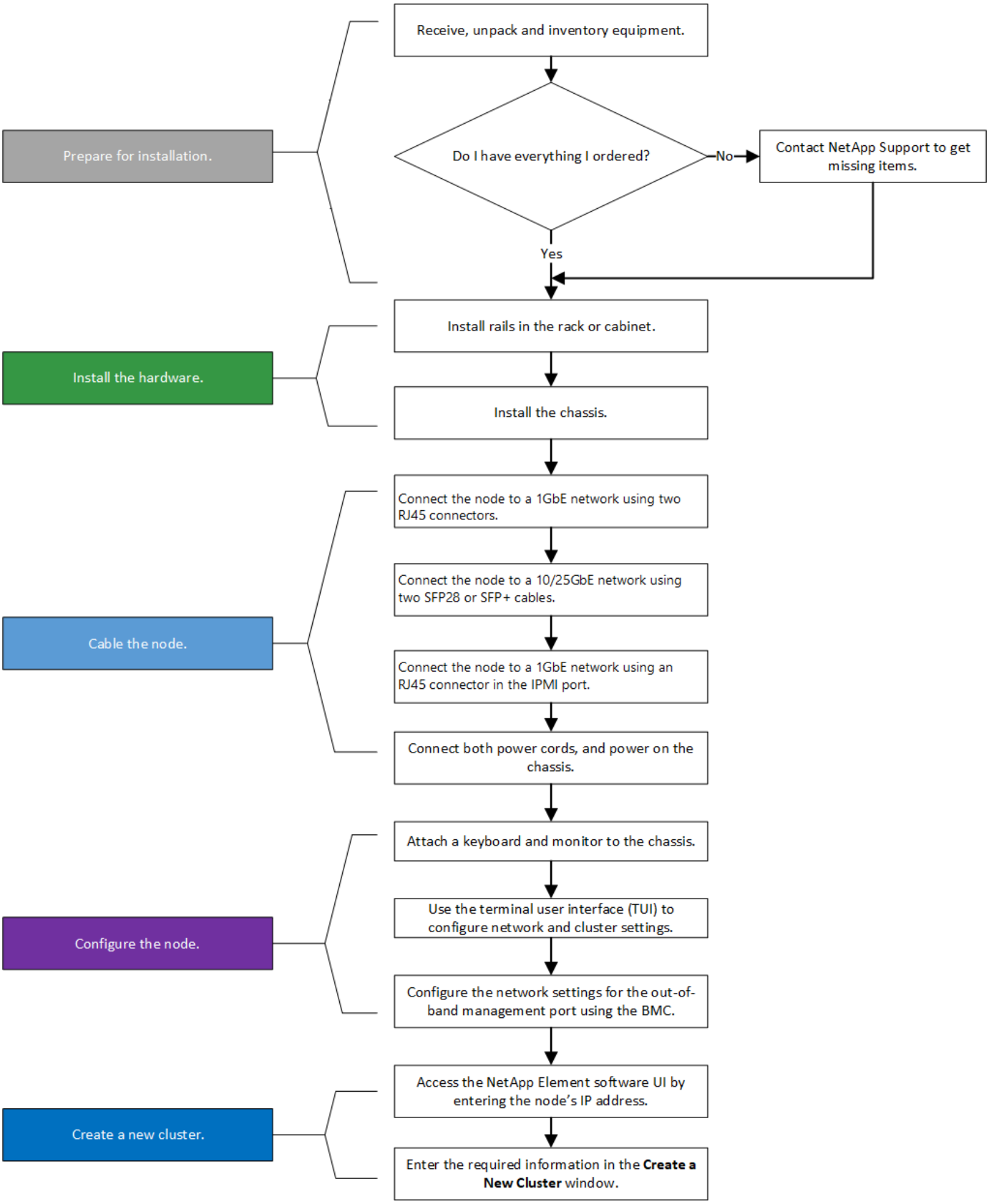
I diagrammi del flusso di lavoro forniscono una panoramica generale delle fasi di installazione. Le fasi variano leggermente a seconda del modello della serie H.

H410S


Prepare for installation.
Receive, unpack and inventory equipment.
Do I have everything I ordered?
No
Contact NetApp Support to get missing items.
Yes
Install the hardware.
Are you adding a node to an existing chassis?
No
Install rails in the rack or cabinet.
Yes
Install the node in the chassis.
Install the chassis.
Install drives.
Cable the node.
Cable the nodes for management and storage connectivity.
Plug in the power cables and power on the nodes.
Configure the node.
Attach a keyboard and monitor to the node.
Use the terminal user interface (TUI) to configure network and cluster settings.
Create a new cluster.
Access the NetApp Element software UI by entering the node's IP address.
Enter the required information in the **Create a New Cluster** window.

H610S

I termini "nodo" e "chassis" sono utilizzati in modo intercambiabile nel caso di H610S, perché nodo e chassis non sono componenti separati, a differenza del caso di uno chassis 2U a quattro nodi.



Preparazione per l'installazione

In preparazione dell'installazione, inventariare l'hardware spedito e contattare il supporto NetApp se alcuni degli elementi sono mancanti.

Assicurarsi di disporre dei seguenti elementi nella posizione di installazione:

- Spazio rack per il sistema.

Tipo di nodo	Spazio rack
Nodi H410S	Due unità rack (2U)
Nodi H610S	Un'unità rack (1U)

- Cavi o ricetrasmettitori a collegamento diretto SFP28/SFP+
- Cavi Cat5e o superiori con connettore RJ45
- Uno switch KVM (Keyboard, Video, mouse) per configurare il sistema
- Chiavetta USB (opzionale)

L'hardware spedito dipende da quello che si ordina. Un nuovo ordine 2U a quattro nodi include chassis, pannello, kit guide di scorrimento, dischi, nodi di storage, e cavi di alimentazione (due per chassis). Se si ordinano nodi di storage H610S, le unità vengono installate nello chassis.

Durante l'installazione dell'hardware, assicurarsi di rimuovere tutto il materiale di imballaggio e l'imballaggio dall'unità. In questo modo si eviteranno il surriscaldamento e lo spegnimento dei nodi.

Montare le guide

L'ordine hardware fornito include un set di guide di scorrimento. Per completare l'installazione della guida, è necessario un cacciavite. Le fasi di installazione variano leggermente per ciascun modello di nodo.

Installare l'hardware dalla parte inferiore del rack fino alla parte superiore per evitare che l'apparecchiatura si rovescii. Se il rack include dispositivi di stabilizzazione, installarli prima di installare l'hardware.

- H410S
- H610S

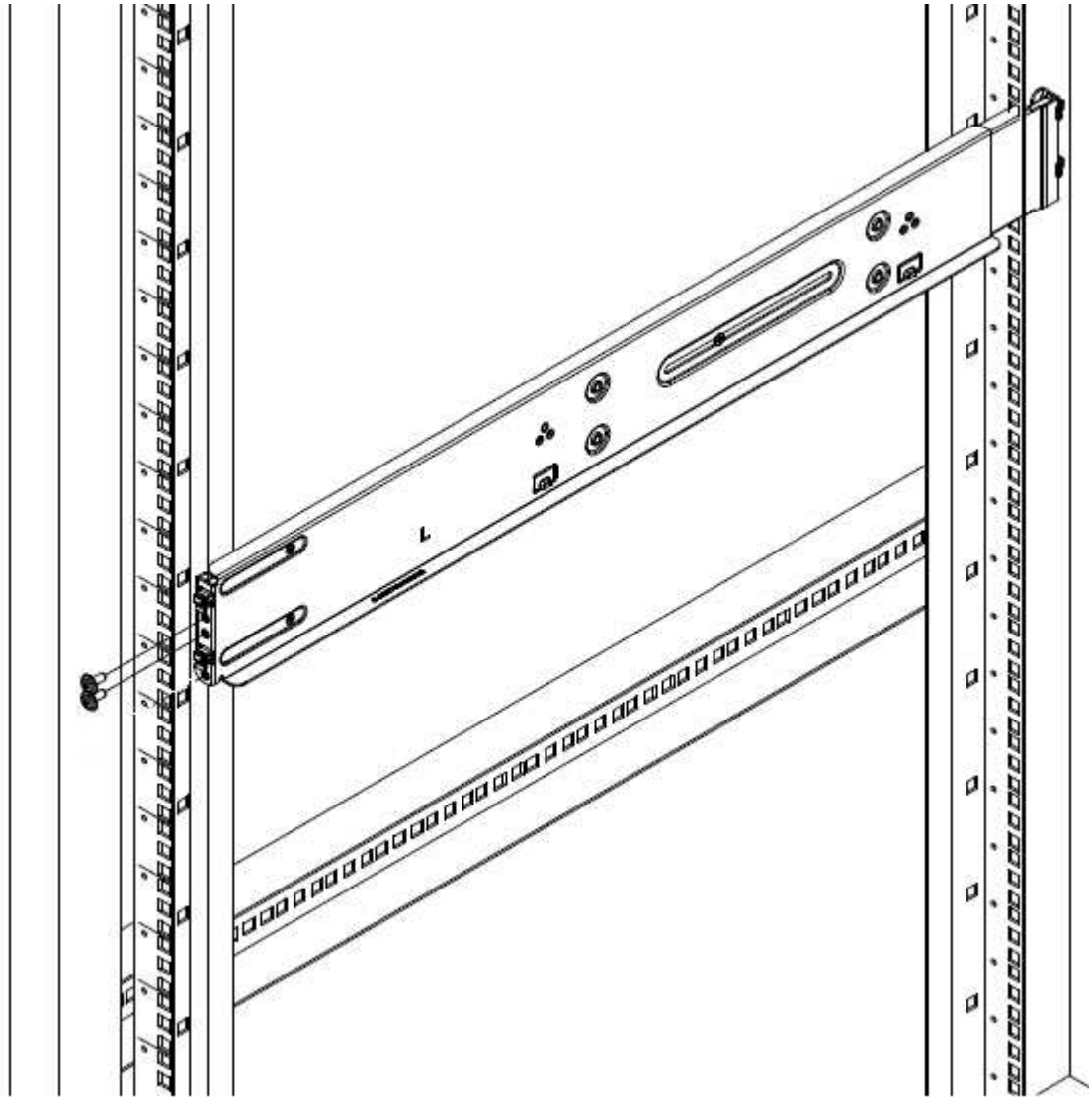
H410S

I nodi H410S sono installati in chassis 2U a quattro nodi serie H, fornito con due set di adattatori. Se si desidera installare lo chassis in un rack con fori rotondi, utilizzare gli adattatori appropriati per un rack con fori rotondi. Le guide per i nodi H410S si adattano a un rack con una profondità compresa tra 29 e 33.5 pollici. Quando la guida è completamente contratta, è lunga 28 pollici e le sezioni anteriore e posteriore della guida sono tenute insieme da una sola vite.

Se si installa il telaio su una guida completamente contratta, le sezioni anteriore e posteriore della guida potrebbero separarsi.

Fasi

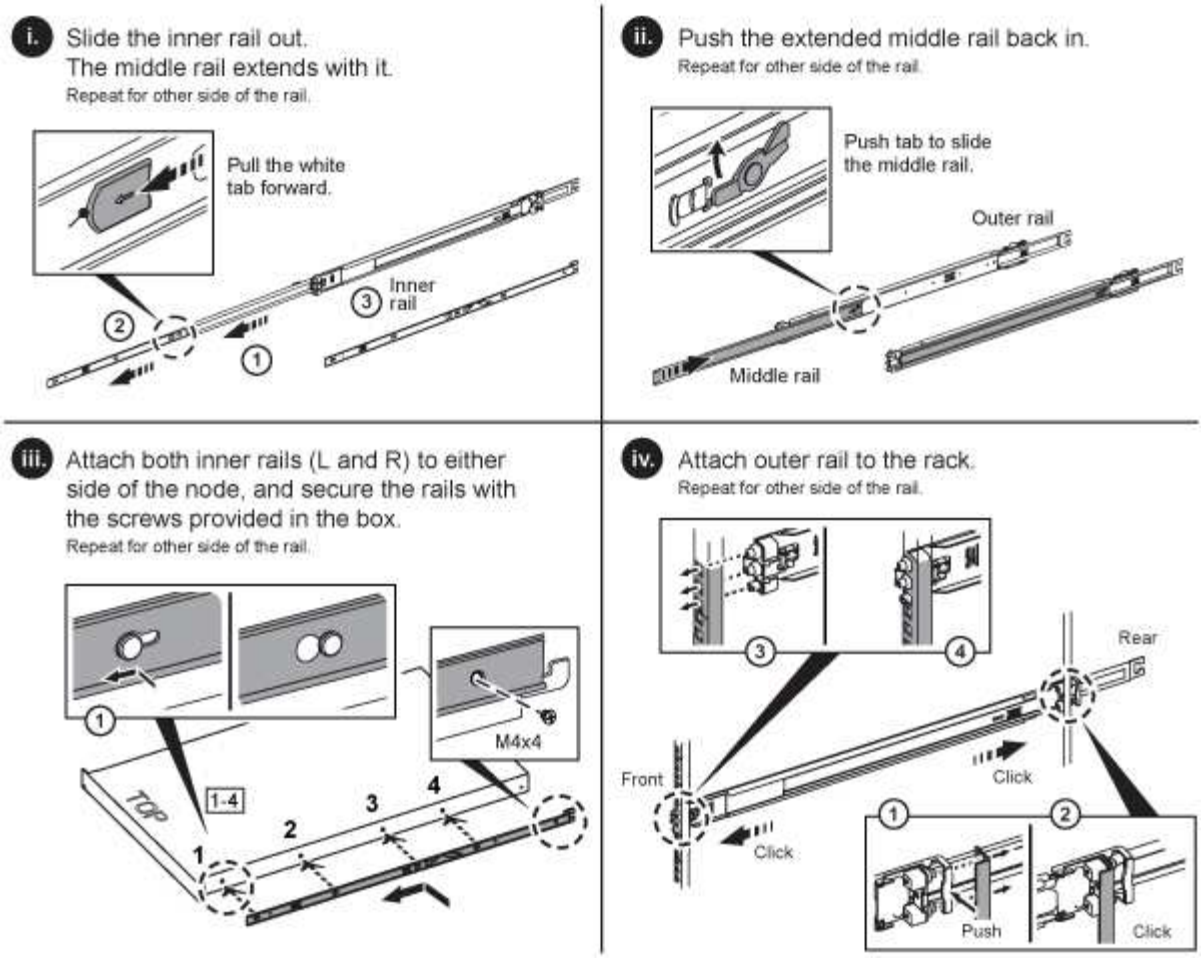
1. Allineare la parte anteriore della guida con i fori sul montante anteriore del rack.
2. Spingere i ganci sulla parte anteriore della guida nei fori sul montante anteriore del rack, quindi abbassarli fino a quando i perni caricati a molla non scattano nei fori del rack.
3. Fissare la guida al rack con le viti. Di seguito viene illustrata la guida sinistra collegata alla parte anteriore del rack:



4. Estendere la sezione posteriore della guida fino al montante posteriore del rack.
5. Allineare i ganci sul retro della guida con i fori appropriati sul montante posteriore, assicurandosi che la parte anteriore e posteriore della guida siano allo stesso livello.
6. Montare la parte posteriore della guida sul rack e fissarla con le viti.
7. Eseguire tutte le operazioni descritte sopra per l'altro lato del rack.

H610S

Di seguito viene illustrata l'installazione delle guide per un nodo di storage H610S:



Sul modello H610S sono presenti guide di destra e di sinistra. Posizionare il foro della vite verso il basso in modo che la vite a testa zigrinata H610S possa fissare il telaio alla guida.

Installare e cablare i nodi

Il nodo di storage H410S viene installato in uno chassis 2U a quattro nodi. Per H610S, installare lo chassis/nodo direttamente sulle guide nel rack.

Rimuovere tutto il materiale di imballaggio e l'imballaggio dall'unità. In questo modo si evitano il surriscaldamento e lo spegnimento dei nodi.

- H410S
- H610S

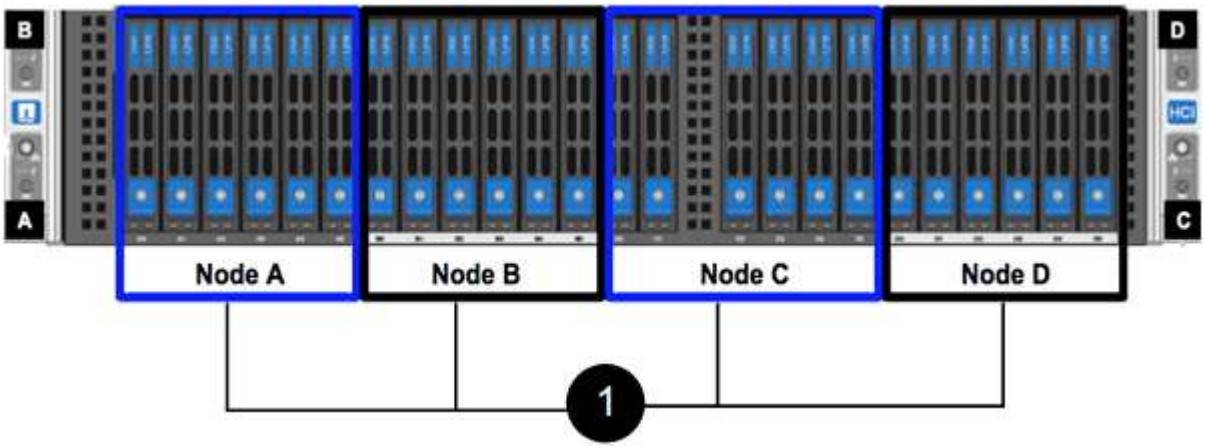
H410S

Fasi

1. Installare i nodi H410S nello chassis. Ecco un esempio di vista posteriore di uno chassis con quattro nodi installati:

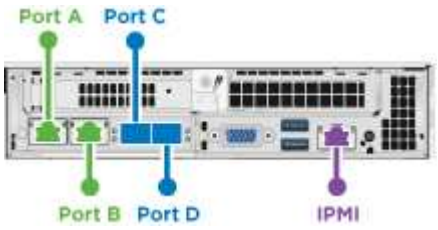
Prestare attenzione durante il sollevamento e l'installazione dell'hardware nel rack. Uno chassis vuoto a due rack (2U) e quattro nodi pesa 24.7 kg (54.45 lb) e un nodo pesa 3.6 kg (8.0 lb).

2. Installare i dischi.



3. Collegare i nodi.

Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento.



- Collegare due cavi CAT5e o superiori nelle porte A e B per la connettività di gestione.
- Collegare due cavi o ricetrasmettitori SFP28/SFP+ nelle porte C e D per la connettività dello storage.
- (Opzionale, consigliato) collegare un cavo CAT5e alla porta IPMI per la connettività di gestione out-of-band.

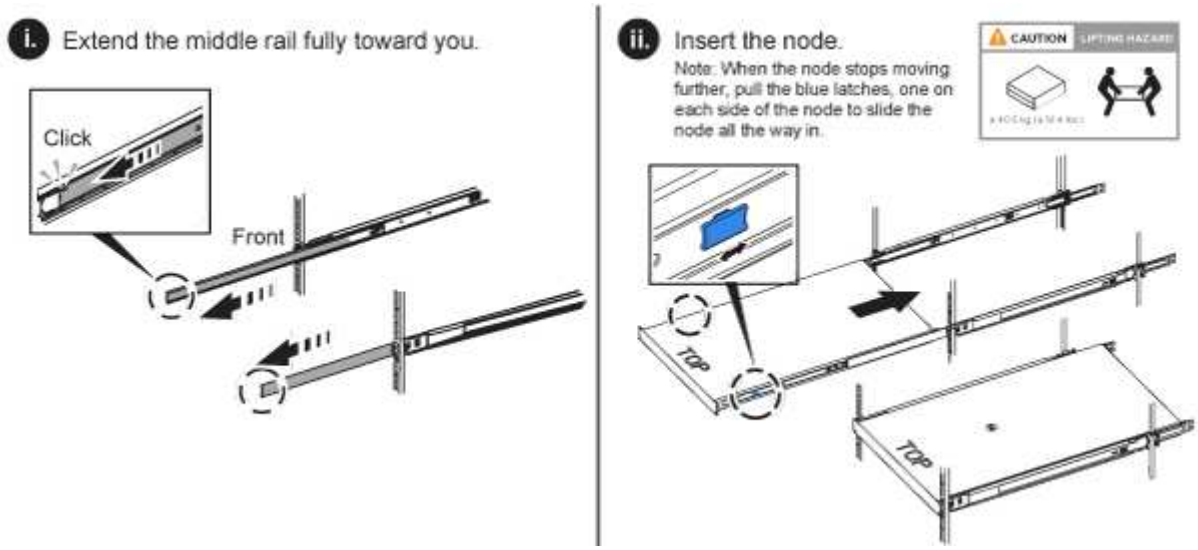
4. Collegare i cavi di alimentazione alle due unità di alimentazione per chassis e collegarle alla PDU da 240 V o alla presa di corrente.
5. Accendere i nodi.

L'avvio del nodo richiede circa sei minuti.

H610S

Fasi

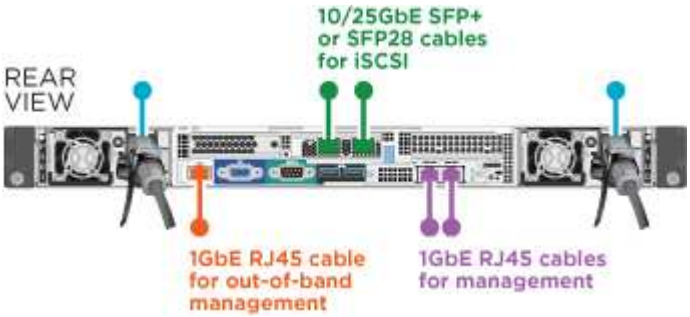
1. Installare il telaio H610S. Di seguito viene riportata un'illustrazione per l'installazione del nodo/chassis nel rack:



Prestare attenzione durante il sollevamento e l'installazione dell'hardware nel rack. Uno chassis H610S pesa 18.4 kg (40.5 lb).

2. Collegare i nodi.

Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento.



- Collegare il nodo a una rete 10/25GbE utilizzando due cavi SFP28 o SFP+.
- Collegare il nodo a una rete 1GbE utilizzando due connettori RJ45.

- Collegare il nodo a una rete 1GbE utilizzando un connettore RJ-45 nella porta IPMI.
- Collegare entrambi i cavi di alimentazione al nodo.

3. Accendere i nodi.

> L'avvio del nodo richiede circa cinque minuti e 30 secondi.

Configurare i nodi

Dopo aver montato in rack e collegato l'hardware, è possibile configurare la nuova risorsa di storage.

Fasi

1. Collegare una tastiera e un monitor al nodo.
2. Nell'interfaccia utente del terminale (TUI) visualizzata, configurare le impostazioni di rete e del cluster per il nodo utilizzando la navigazione a schermo.

> L'indirizzo IP del nodo deve essere ottenuto dall'interfaccia telefonica utente (TUI). Ciò è necessario quando si aggiunge il nodo a un cluster. Dopo aver salvato le impostazioni, il nodo si trova in uno stato di attesa e può essere aggiunto a un cluster. Vedere <insert link to Setup section>.

3. Configurare la gestione out-of-band utilizzando Baseboard Management Controller (BMC). Questi passaggi si applicano **solo ai nodi H610S**.
   a. Utilizzare un browser Web e accedere all'indirizzo IP BMC predefinito: 192.168.0.120
   b. Accedere utilizzando **root** come nome utente e **calvin** come password.
   c. Dalla schermata di gestione dei nodi, accedere a **Impostazioni** > **Impostazioni di rete** e configurare i parametri di rete per la porta di gestione fuori banda.

> Vedere "Questo articolo della Knowledge base (è necessario effettuare l'accesso)".

Creare un cluster

Dopo aver aggiunto il nodo di storage all'installazione e aver configurato la nuova risorsa di storage, è possibile creare un nuovo cluster di storage

Fasi

1. Da un client sulla stessa rete del nodo appena configurato, accedere all'interfaccia utente del software NetApp Element immettendo l'indirizzo IP del nodo.
2. Inserire le informazioni richieste nella finestra **Crea nuovo cluster**. Vedere "panoramica dell'installazione" per ulteriori informazioni.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

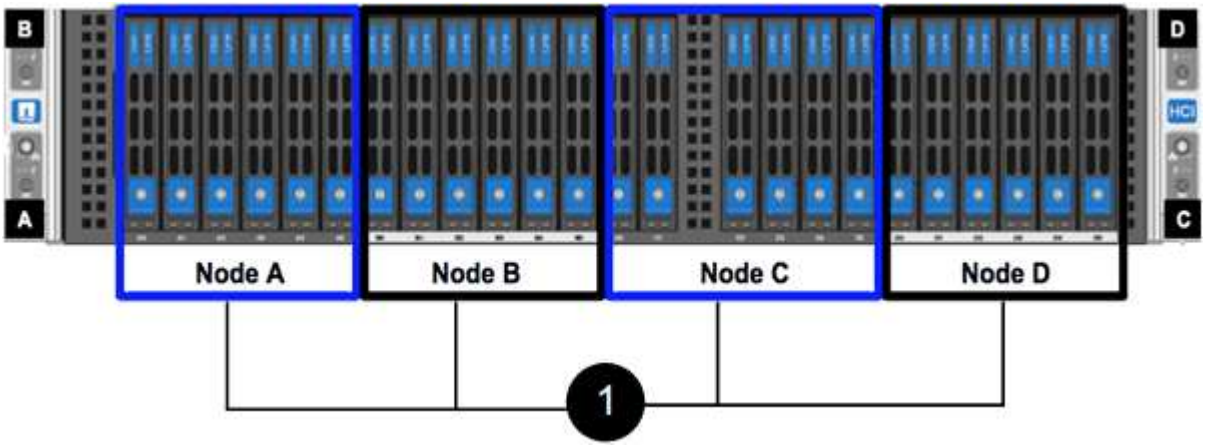
Sostituire un nodo H410S

Sostituire un nodo di storage in caso di guasto della CPU, problemi della scheda Radian, altri problemi della scheda madre o in caso di mancata accensione. Le istruzioni si applicano ai nodi di storage H410S.

Gli allarmi nell'interfaccia utente del software NetApp Element avvisano l'utente in caso di guasto di un nodo di storage. Utilizzare l'interfaccia utente Element per ottenere il numero di serie (codice di matricola) del nodo guasto. Queste informazioni sono necessarie per individuare il nodo guasto nel cluster.

Ecco il retro di uno chassis a quattro nodi con due unità rack (2U) e quattro nodi con quattro nodi di storage:

Di seguito viene mostrata la vista frontale di uno chassis a quattro nodi con nodi H410S, che mostra gli alloggiamenti corrispondenti a ciascun nodo:



Di cosa hai bisogno

- Hai verificato che il nodo di storage è guasto e deve essere sostituito.
- È stato ottenuto un nodo storage sostitutivo.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Ciascun cavo collegato al nodo di storage è etichettato.

Ecco una panoramica di alto livello dei passaggi:

- Prepararsi a sostituire il nodo
- Sostituire il nodo nel telaio
- Aggiungere il nodo al cluster

Prepararsi a sostituire il nodo

Prima di installare il nodo sostitutivo, è necessario rimuovere correttamente il nodo di storage guasto dal cluster nell'interfaccia utente del software NetApp Element. È possibile eseguire questa operazione senza causare alcuna interruzione del servizio. Il numero di serie del nodo di storage guasto deve essere ottenuto dall'interfaccia utente dell'elemento e deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Fasi

1. Nell'interfaccia utente di Element, selezionare **Cluster** > **Drives**.
2. Rimuovere le unità dal nodo utilizzando uno dei seguenti metodi:

Opzione	Fasi
Per rimuovere singoli dischi	a. Fare clic su **azioni** per l'unità che si desidera rimuovere. b. Fare clic su **Rimuovi**.
Per rimuovere più dischi	a. Selezionare tutte le unità che si desidera rimuovere e fare clic su **azioni in blocco**. b. Fare clic su **Rimuovi**.

3. Selezionare **Cluster** > **Nodes**.
4. Annotare il numero di serie (codice di matricola) del nodo difettoso. Deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.
5. Dopo aver preso nota del numero di serie, rimuovere il nodo dal cluster come segue:
   a. Selezionare il pulsante **azioni** del nodo che si desidera rimuovere.
   b. Selezionare **Rimuovi**.

Sostituire il nodo nel telaio

Dopo aver rimosso il nodo difettoso dal cluster utilizzando l'interfaccia utente del software NetApp Element, è possibile rimuovere fisicamente il nodo dallo chassis. Installare il nodo sostitutivo nello stesso slot dello chassis da cui è stato rimosso il nodo guasto.

Fasi

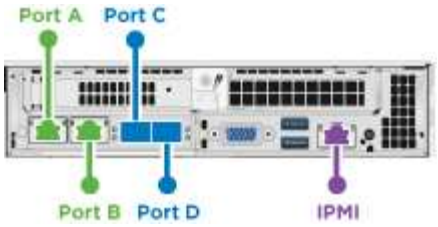
1. Indossare una protezione antistatica prima di procedere.
2. Disimballare il nuovo nodo storage e impostarlo su una superficie piana vicino allo chassis.

   Conservare il materiale di imballaggio per quando si restituisce il nodo difettoso a NetApp.

3. Etichettare ciascun cavo inserito nella parte posteriore del nodo di storage che si desidera rimuovere.

   Dopo aver installato il nuovo nodo di storage, inserire i cavi nelle porte originali.

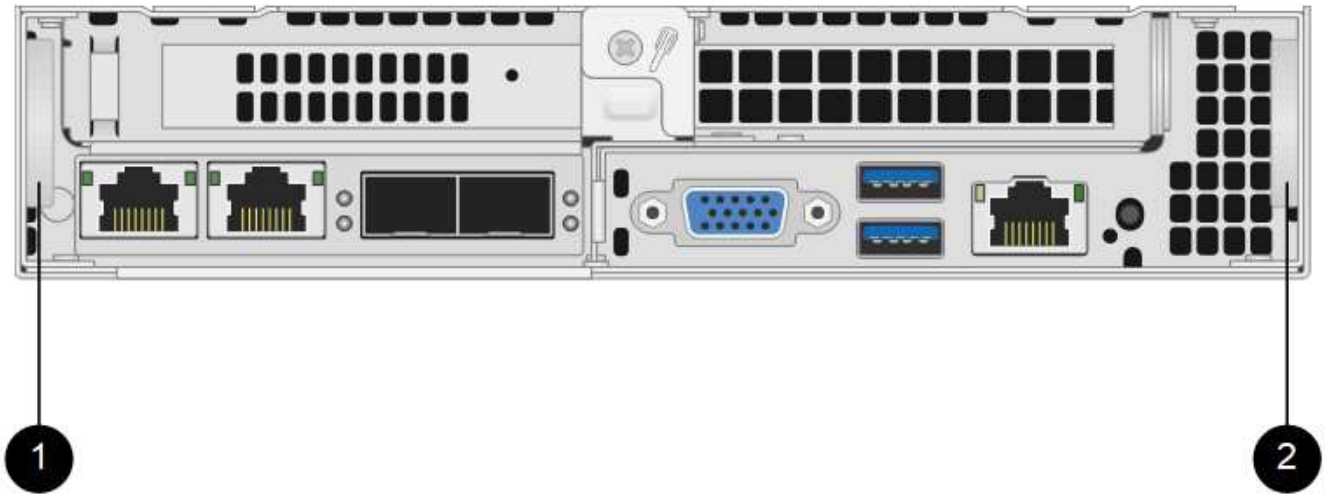
   Di seguito viene mostrata un'immagine che mostra il retro di un nodo di storage:



Porta	Dettagli
Porta A.	Porta RJ45 1/10 GbE
Porta B	Porta RJ45 1/10 GbE
Porta C	Porta 10/25GbE SFP+ o SFP28
Porta D	Porta 10/25GbE SFP+ o SFP28
IPMI	Porta RJ45 1/10 GbE

4. Scollegare tutti i cavi dal nodo di storage.
5. Tirare verso il basso la maniglia della camma sul lato destro del nodo ed estrarre il nodo utilizzando entrambe le maniglie della camma.

   La maniglia della camma che si trascina verso il basso presenta una freccia che indica la direzione in cui si sposta. L'altra maniglia CAM non si sposta ed è lì per aiutare a estrarre il nodo.



Elemento	Descrizione
1	Maniglia CAM per estrarre il nodo.
2	Maniglia CAM che si tira verso il basso prima di estrarre il nodo.

Supportare il nodo con entrambe le mani quando lo si tira fuori dallo chassis.

6. Posizionare il nodo su una superficie piana.

   È necessario imballare il nodo e restituirlo a NetApp.

7. Installare il nodo sostitutivo nello stesso slot del telaio.

   Assicurarsi di non esercitare una forza eccessiva quando si fa scorrere il nodo nel telaio.

8. Spostare le unità dal nodo rimosso e inserirle nel nuovo nodo.
9. Ricollegare i cavi alle porte da cui sono stati precedentemente scollegati.

   Le etichette presenti sui cavi al momento della disconnessione sono utili come guida.

   a. Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, possono verificarsi guasti prematuri dei componenti dovuti al surriscaldamento.
   b. Non forzare i cavi nelle porte, poiché si potrebbero danneggiare i cavi, le porte o entrambe.

   Assicurarsi che il nodo sostitutivo sia cablato nello stesso modo degli altri nodi nello chassis.

10. Premere il pulsante nella parte anteriore del nodo per accenderlo.

Aggiungere il nodo al cluster

Quando si aggiunge un nodo al cluster o si installano nuove unità in un nodo esistente, le unità vengono automaticamente registrate come disponibili. È necessario aggiungere le unità al cluster utilizzando l'interfaccia utente Element o l'API prima che possano partecipare al cluster.

La versione software di ciascun nodo di un cluster deve essere compatibile. Quando si aggiunge un nodo a un cluster, il cluster installa la versione cluster del software Element sul nuovo nodo in base alle necessità.

Fasi

1. Selezionare **Cluster** > **Nodes**.
2. Selezionare **Pending** per visualizzare l'elenco dei nodi in sospeso.
3. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli nodi, selezionare l'icona **azioni** del nodo che si desidera aggiungere.
   - Per aggiungere più nodi, selezionare la casella di controllo dei nodi da aggiungere, quindi **azioni in blocco**.

   Se il nodo che si sta aggiungendo ha una versione del software Element diversa da quella in esecuzione sul cluster, il cluster aggiorna il nodo in modo asincrono alla versione del software Element in esecuzione sul master del cluster. Una volta aggiornato, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo si trova in una `pendingActive` stato.

4. Selezionare **Aggiungi**.

   Il nodo viene visualizzato nell'elenco dei nodi attivi.

5. Dall'interfaccia utente di Element, selezionare **Cluster** > **Drives**.
6. Selezionare **Available** per visualizzare l'elenco dei dischi disponibili.
7. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli dischi, selezionare l'icona **azioni** del disco che si desidera aggiungere, quindi selezionare **Aggiungi**.
   - Per aggiungere più dischi, selezionare le caselle di controllo delle unità da aggiungere, selezionare **azioni in blocco**, quindi **Aggiungi**.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire un nodo H610S

Potrebbe essere necessario sostituire lo chassis se la ventola, l'unità di elaborazione centrale (CPU) o il modulo DIMM (Dual Inline Memory Module) si guasta o se si verificano problemi di surriscaldamento o problemi durante il processo di avvio. Il LED ambra lampeggiante nella parte anteriore dello chassis indica la possibile necessità di sostituire lo chassis. Prima di procedere, contatta il supporto NetApp.

Vedere "Articolo della Knowledge base" Per informazioni sui requisiti di installazione per i nodi H610S. I nodi storage H610S nuovi e spare potrebbero avere requisiti di installazione aggiuntivi in base alla versione software Element esistente del cluster di storage. Per ulteriori informazioni, contatta il supporto NetApp.

I termini "nodo" e "chassis" sono utilizzati in modo intercambiabile nel caso di H610S, che è uno chassis a un'unità rack (1U).

Best practice per l'aggiunta e la rimozione di dischi

Attenersi alle seguenti Best practice per aggiungere dischi al cluster:

- Aggiungi tutti i dischi a blocchi e assicurati che la sincronizzazione dei blocchi sia completa prima di aggiungere i dischi slice.
- Per il software Element 10.x e versioni successive, aggiungere tutti i dischi a blocchi contemporaneamente. Assicurarsi di non eseguire questa operazione per più di tre nodi alla volta.
- Per il software Element 9.x e versioni precedenti, aggiungere tre dischi alla volta per sincronizzarli completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere il disco slice e assicurarsi che la sincronizzazione slice sia completa prima di rimuovere i dischi a blocchi.
- Rimuovere tutti i dischi a blocchi da un singolo nodo alla volta. Assicurarsi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

Di cosa hai bisogno

- Hai contattato il supporto NetApp. Se stai ordinando un prodotto sostitutivo, dovresti avere un caso aperto con il supporto NetApp.

- Il nodo sostitutivo è stato ottenuto.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Se è necessario eseguire la procedura di ripristino dell'immagine di fabbrica (RTFI), è stata ottenuta la chiave USB. Il supporto NetApp può aiutarti a decidere se eseguire il processo RTFI.
- Si dispone di una tastiera e di un monitor.
- Il nodo guasto è stato rimosso correttamente dal cluster.
- In caso di guasto di un DIMM, sono state rimosse le unità prima di rimuovere il nodo dal cluster.

A proposito di questa attività

Gli allarmi nell'interfaccia utente Element avvisano l'utente quando un host non funziona. Il numero di serie dell'host guasto di VMware vSphere Web Client deve corrispondere al numero di serie riportato sull'etichetta sul retro del nodo.

Fasi

1. Individuare il codice di matricola nella parte anteriore dello chassis guasto.

2. Verificare che il numero di serie sul codice di matricola corrisponda al numero del caso NetApp Support al momento dell'ordine dello chassis sostitutivo.
3. Collegare la tastiera e il monitor al retro dello chassis guasto.
4. Verificare il numero di serie del nodo guasto con il supporto NetApp.
5. Spegnere lo chassis.
6. Etichettare le unità nella parte anteriore e i cavi nella parte posteriore con le rispettive posizioni, in modo da poterle riposizionare nelle stesse posizioni dopo la sostituzione. Vedere la seguente immagine per il posizionamento delle unità nello chassis:

7. Rimuovere i cavi.
8. Rimuovere il telaio svitando le viti a testa zigrinata sulle linguette di montaggio. È necessario imballare e restituire lo chassis guasto a NetApp.
9. Installare il telaio sostitutivo.
10. Rimuovere con cautela le unità dallo chassis guasto e inserirle nello chassis sostitutivo.

    Inserire le unità negli stessi slot in cui si trovavano prima di rimuoverle.

11. Rimuovere le unità di alimentazione dallo chassis guasto e inserirle nello chassis sostitutivo.
12. Inserire i cavi di alimentazione e di rete nelle porte originali.
13. I ricetrasmettitori SFP (Small Form-factor Pluggable) potrebbero essere inseriti nelle porte 10 GbE del nodo sostitutivo. Rimuoverli prima di collegare via cavo le porte 10GbE.

    Se lo switch non riconosce i cavi, consultare la documentazione del fornitore dello switch.

14. Accendere lo chassis premendo il pulsante di accensione sulla parte anteriore. L'avvio del nodo richiede circa cinque minuti e 30 secondi.
15. Eseguire la procedura di configurazione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire i dischi

Se un disco è difettoso o se il livello di usura del disco scende al di sotto di una soglia, sostituirlo. Gli allarmi nell'interfaccia utente del software Element avvisano l'utente in caso di guasto o guasto di un disco. È possibile sostituire a caldo un disco guasto.

A proposito di questa attività

Questa procedura serve per sostituire i dischi nei nodi di storage H410S e H610S. La rimozione di un disco porta il disco offline. Tutti i dati presenti sul disco vengono rimossi e migrati su altri dischi del cluster. La migrazione dei dati ad altri dischi attivi nel sistema può richiedere da alcuni minuti a un'ora, a seconda dell'utilizzo della capacità e dell'i/o attivo nel cluster. Attenersi alle seguenti procedure consigliate per la gestione delle unità durante la rimozione e la sostituzione:

- Tenere l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
- Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.
- Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis.
- Utilizzare sempre entrambe le mani durante la rimozione, l'installazione o il trasporto di un disco.
- Non forzare mai un disco nello chassis.
- Utilizzare sempre imballaggi approvati per la spedizione delle unità.
- Non impilare i dischi l'uno sull'altro.

Best practice per l'aggiunta e la rimozione di dischi

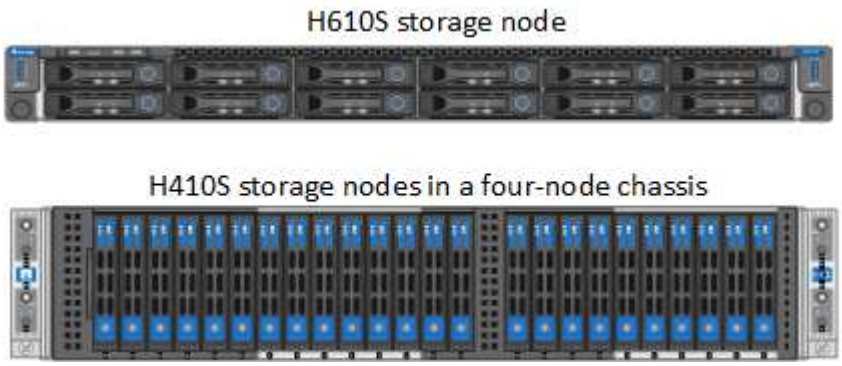
- Aggiungi tutti i dischi a blocchi e assicurati che la sincronizzazione dei blocchi sia completa prima di aggiungere i dischi slice.
- Per il software Element 10.x e versioni successive, aggiungere tutti i dischi a blocchi contemporaneamente. Assicurarsi di non eseguire questa operazione per più di tre nodi contemporaneamente.
- Per il software Element 9.x e versioni precedenti, aggiungere tre dischi alla volta per sincronizzarli completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere il disco slice e assicurarsi che la sincronizzazione slice sia completa prima di rimuovere i dischi a blocchi.
- Rimuovere tutti i dischi a blocchi da un singolo nodo alla volta. Assicurarsi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

Fasi

1. Rimuovere l'unità dal cluster utilizzando l'interfaccia utente del software NetApp Element:
   a. Dall'interfaccia utente di Element, selezionare **Cluster > Drives**.
   b. Selezionare **Failed** per visualizzare l'elenco dei dischi guasti.
   c. Annotare il numero di slot del disco guasto. Queste informazioni sono necessarie per individuare il disco guasto nello chassis.
   d. Selezionare **azioni** per l'unità che si desidera rimuovere.
   e. Selezionare **Rimuovi**.

   Se la capacità non è sufficiente per rimuovere i dischi attivi prima di rimuovere un nodo, viene visualizzato un messaggio di errore quando si conferma la rimozione del disco. Dopo aver risolto l'errore, è possibile rimuovere fisicamente il disco dal telaio.

2. Sostituire l'unità dal telaio:
   a. Disimballare l'unità sostitutiva e posizionarla su una superficie piana e priva di scariche elettrostatiche vicino al rack. Conservare il materiale di imballaggio per quando si restituisce il disco guasto a NetApp. Di seguito è riportato il punto di vista frontale dei nodi di storage H610S e H410S con i dischi:

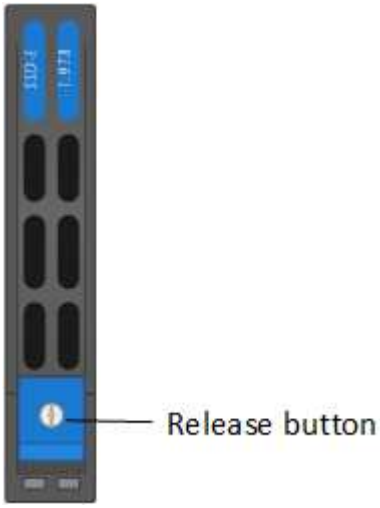


   b. (**solo H410S**) effettuare le seguenti operazioni:
      i. Identificare il nodo facendo corrispondere il numero di serie (codice di matricola) con il numero annotato dall'interfaccia utente dell'elemento. Il numero di serie è riportato su un adesivo sul retro di ciascun nodo. Una volta identificato il nodo, è possibile utilizzare le informazioni relative agli slot

per identificare lo slot in cui si trova l'unità guasta. I dischi sono disposti in ordine alfabetico da A a D e da 0 a 5.

ii. Rimuovere il pannello.

iii. Premere il pulsante di rilascio sul disco guasto:



Quando si preme il pulsante di rilascio, la maniglia della camma sulle molle dell'unità si apre parzialmente e l'unità si rilascia dalla scheda intermedia.

i. Aprire la maniglia della camma ed estrarre con cautela l'unità con entrambe le mani.

ii. Posizionare l'unità su una superficie piana antistatica.

iii. Inserire l'unità sostitutiva nello slot completamente nello chassis con entrambe le mani.

iv. Premere la maniglia della camma fino a farla scattare in posizione.

v. Reinstallare il pannello.

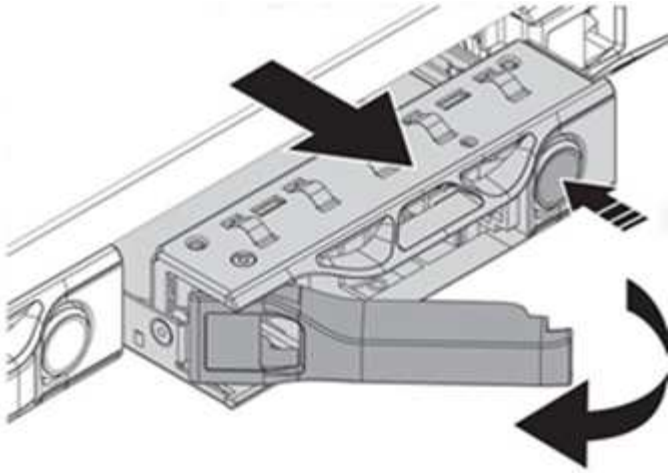
vi. Informare il supporto NetApp in merito alla sostituzione del disco. Il supporto NetApp fornirà istruzioni per la restituzione del disco guasto.

c. (**solo H610S**) effettuare le seguenti operazioni:

i. Far corrispondere il numero di slot del disco guasto dell'interfaccia utente Element con il numero sullo chassis. Il LED sul disco guasto è acceso in ambra.

ii. Rimuovere il pannello.

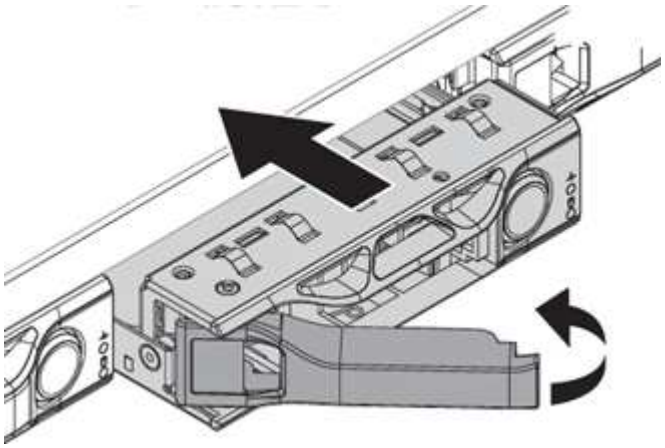
iii. Premere il pulsante di rilascio e rimuovere il disco guasto come mostrato nell'illustrazione seguente:



Assicurarsi che la maniglia del vassoio sia completamente aperta prima di provare a far scorrere l'unità fuori dal telaio.

i. Estrarre l'unità e posizionarla su una superficie piana e priva di elettricità statica.

ii. Premere il pulsante di rilascio sull'unità sostitutiva prima di inserirla nell'alloggiamento. Le molle della maniglia del vassoio dell'unità si aprono.



iii. Inserire l'unità sostitutiva senza esercitare una forza eccessiva. Quando l'unità è inserita completamente, si sente uno scatto.

iv. Chiudere con cautela la maniglia del vassoio dell'unità.

v. Reinstallare il pannello.

vi. Informare il supporto NetApp in merito alla sostituzione del disco. Il supporto NetApp fornirà istruzioni per la restituzione del disco guasto.

3. Aggiungere nuovamente il disco al cluster utilizzando l'interfaccia utente Element.

Quando si installa un nuovo disco in un nodo esistente, il disco viene automaticamente registrato come **Available** nell'interfaccia utente Element. È necessario aggiungere l'unità al cluster prima che possa partecipare al cluster.

a. Dall'interfaccia utente di Element, selezionare **Cluster > Drives**.

b. Selezionare **Available** per visualizzare l'elenco dei dischi disponibili.

c. Selezionare l'icona Actions (azioni) per l'unità che si desidera aggiungere e selezionare **Add**

(Aggiungi).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire un alimentatore

Ogni chassis include due alimentatori per la ridondanza dell'alimentazione. Se un alimentatore è difettoso, sostituirlo il prima possibile per assicurarsi che lo chassis disponga di una fonte di alimentazione ridondante.

Di cosa hai bisogno

- L'alimentatore è guasto.
- Si dispone di un alimentatore sostitutivo.
- Hai verificato che il secondo alimentatore funziona.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.

A proposito di questa attività

La procedura di sostituzione si applica ai seguenti modelli di nodi:

- Due unità rack (2U), chassis NetApp HCI a quattro nodi
- Uno chassis storage H610S con unità rack (1U)

> Nel caso di H610S, i termini "nodo" e "chassis" vengono utilizzati in modo intercambiabile perché nodo e chassis non sono componenti separati, a differenza del caso dello chassis 2U a quattro nodi.

Gli allarmi nell'interfaccia utente Element forniscono informazioni sull'alimentatore guasto, riferendosi a PS1 o PS2. In uno chassis NetApp HCI 2U a quattro nodi, PS1 si riferisce all'unità nella riga superiore dello chassis e PS2 all'unità nella riga inferiore dello chassis. È possibile sostituire l'unità di alimentazione difettosa mentre lo chassis è acceso e funzionante, purché l'unità di alimentazione ridondante funzioni.

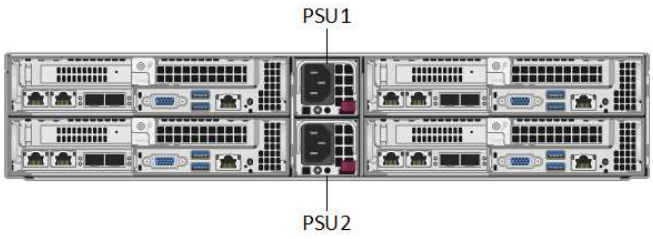
> Se si stanno sostituendo entrambe le PSU in un nodo, le PSU devono avere lo stesso numero di parte e lo stesso wattaggio. PSU non corrispondenti possono danneggiare il sistema.

Fasi

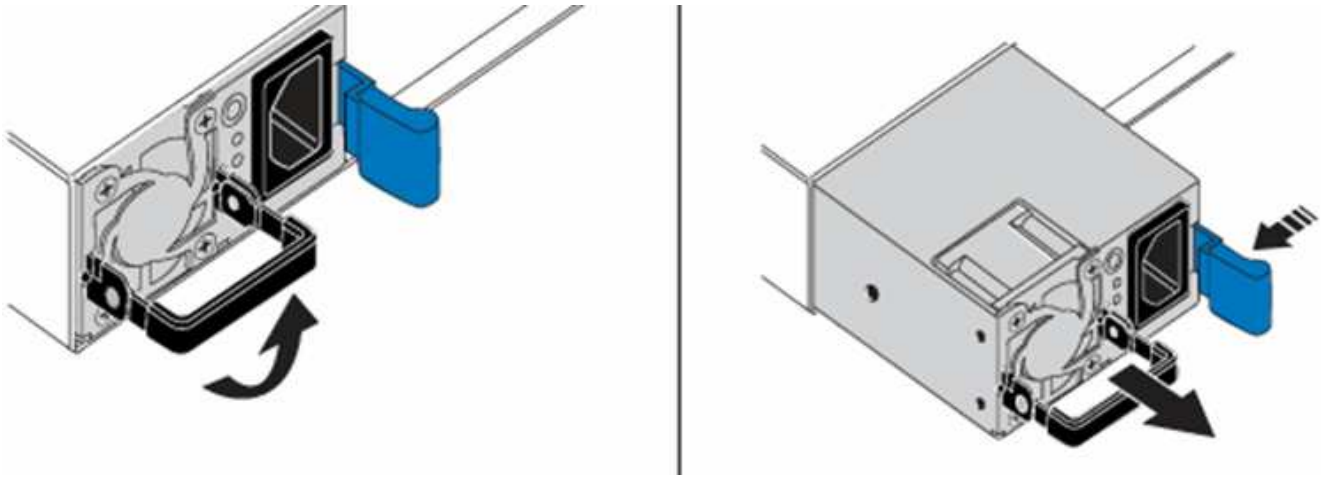
1. Individuare l'unità di alimentazione difettosa nel telaio. Il LED sull'unità guasta è di colore ambra.

   > Le unità di alimentazione si trovano in modo diverso a seconda del tipo di chassis.

   Vedere le immagini riportate di seguito per le posizioni degli alimentatori:

Modello	Ubicazione delle unità di alimentazione
Chassis storage NetApp HCI 2U a quattro nodi	 I nodi nello chassis potrebbero essere diversi a seconda del tipo di nodi (storage o calcolo) in uso.
Chassis H610S	

2. Identificare il nodo corretto utilizzando il tag blu o il numero di serie. Il tag blu pull-out elenca il numero di serie (S/N) e il layout del disco. Confermare il numero di serie del nodo da sottoporre a manutenzione.
   - Se si stanno sostituendo entrambi gli alimentatori, passare alla fase 3.
   - Se si sta sostituendo un solo alimentatore, passare alla fase 4.
3. Verificare che il nodo sia stato spento o sia pronto per essere spento per l'assistenza. Tenere presente quanto segue:
   - Un nodo che è stato spento non visualizza alcun LED di alimentazione blu sulle unità o sul pulsante di alimentazione.
   - Un nodo che non è stato ancora spento visualizza i LED blu sui dischi e il pulsante di alimentazione.
   - Un nodo che è stato spento e pronto per l'assistenza visualizza un LED PSU lampeggiante che lampeggia (verde) e si spegne (nessun colore).
   - Un nodo che non è stato ancora spento visualizza LED verdi sugli alimentatori.
4. Scollegare il cavo di alimentazione dall'alimentatore o da entrambi i cavi di alimentazione, se si sostituiscono entrambe le unità.
5. Sollevare la maniglia della camma e premere il fermo blu per estrarre l'alimentatore.



L'illustrazione è un esempio. La posizione o le posizioni delle unità di alimentazione nello chassis e il colore del pulsante di rilascio variano a seconda del tipo di chassis in uso.

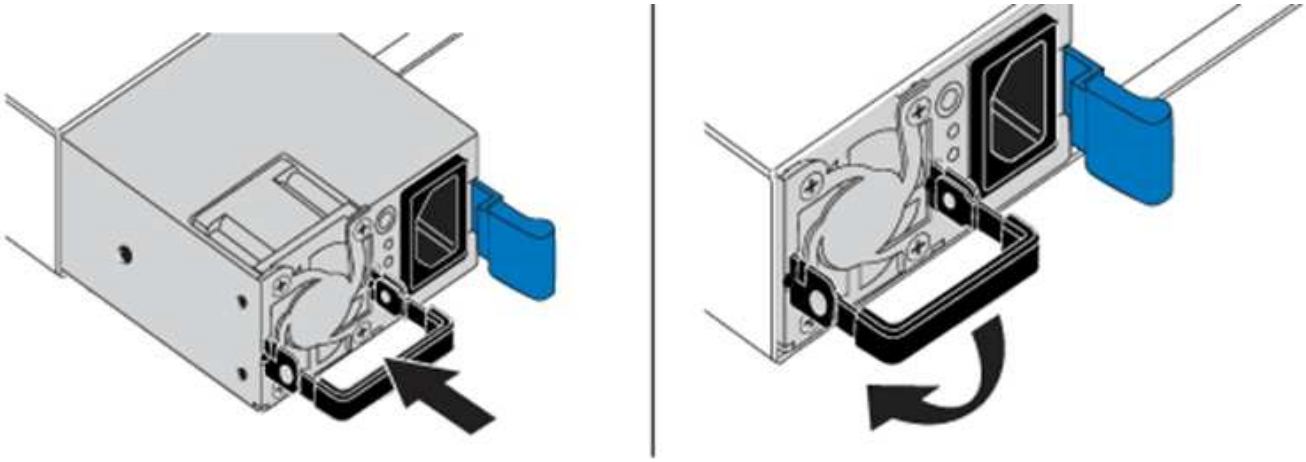
Assicurarsi di utilizzare entrambe le mani per sostenere il peso dell'alimentatore.

Ripetere i passi 3, 4 e 5 se si sostituisce un secondo alimentatore.

6. Individuare l'etichetta sull'unità di alimentazione rimossa dal telaio. L'etichetta contiene i dettagli del produttore e del wattaggio di uscita.

Non sostituire l'alimentatore se il wattaggio dell'alimentatore RMA non corrisponde al wattaggio dell'alimentatore rimosso. Contatta il supporto NetApp per le fasi successive.

7. Allineare con entrambe le mani i bordi dell'alimentatore con l'apertura del telaio, spingere delicatamente l'unità nel telaio utilizzando la maniglia della camma fino a bloccarla in posizione e riportare la maniglia della camma in posizione verticale.



8. Collegare uno o entrambi i cavi di alimentazione.
9. Se sono state sostituite entrambe le unità di alimentazione, andare nella parte anteriore del nodo e premere il pulsante di alimentazione per accendere i nodi. Dopo l'accensione, il LED del pulsante di alimentazione si illumina di blu fisso. I LED blu delle unità e il pulsante di identificazione iniziano a lampeggiare.
10. Restituire l'unità difettosa a NetApp seguendo le istruzioni riportate nella confezione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Informazioni sull'hardware della serie SF

Sono disponibili informazioni sull'installazione e la manutenzione dei nodi di storage della serie SF.

Di seguito sono riportati i collegamenti ai contenuti relativi all'installazione e alla manutenzione:

- "Installare e configurare i nodi SolidFire C-Series"
- "Installare e configurare i nodi Fibre Channel"
- "Installare e configurare nodi storage serie SF"
- "Sostituire uno chassis"
- "Sostituire i dischi"
- "Sostituire un alimentatore"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire uno chassis

Potrebbe essere necessario sostituire lo chassis se la ventola, l'unità di elaborazione centrale (CPU) o il modulo DIMM (Dual Inline Memory Module) si guasta o se si verificano problemi di surriscaldamento o problemi durante il processo di avvio. I guasti del cluster nell'interfaccia utente del software NetApp Element e la spia ambra lampeggiante nella parte anteriore dello chassis indicano una possibile necessità di sostituzione dello chassis. Prima di procedere, contatta il supporto NetApp.

Di cosa hai bisogno

- Hai contattato il supporto NetApp.

  Se si sta ordinando un prodotto sostitutivo, è necessario aprire un caso con il supporto NetApp.

- Hai ottenuto lo chassis sostitutivo.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o di un'altra protezione antistatica.
- Se è necessario eseguire la procedura di ripristino dell'immagine di fabbrica (RTFI), è stata ottenuta la chiave USB.

  Il supporto NetApp ti aiuterà a decidere se RTFI è necessario. Vedere "Questo articolo della Knowledge base (accesso richiesto)".

- Si dispone di una tastiera e di un monitor.

A proposito di questa attività

Le istruzioni contenute in questo documento si applicano se si dispone di uno chassis con un'unità rack (1U) con uno dei seguenti nodi:

- SF2405
- SF3010
- SF4805
- SF6010
- SF9605
- SF9608

- SF9010
- SF19210
- SF38410
- SF-FCN-01
- FC0025

Fasi

1. Individuare il codice di matricola dello chassis guasto e verificare che il numero di serie corrisponda al numero riportato sul caso aperto presso il supporto NetApp al momento dell'ordine del prodotto sostitutivo.

   È possibile individuare il codice di matricola dalla parte anteriore dello chassis.

   La figura seguente è un esempio del codice di matricola:

   La figura precedente è un esempio. La posizione esatta del codice di matricola può variare a seconda del modello di hardware in uso.

2. Collegare la tastiera e il monitor al retro dello chassis guasto.
3. Verificare le informazioni sullo chassis con il supporto NetApp.
4. Spegnere lo chassis.
5. Etichettare le unità nella parte anteriore dello chassis e i cavi nella parte posteriore.

   I nodi Fibre Channel non dispongono di unità nella parte anteriore.

6. Rimuovere i cavi e le unità di alimentazione.
7. Rimuovere le unità con cautela e posizionarle su una superficie piana e antistatica.

   Se si dispone di un nodo Fibre Channel, è possibile saltare questo passaggio.

8. Rimuovere lo chassis premendo il fermo o svitando la vite a testa zigrinata, a seconda del modello di hardware in uso.

È necessario imballare e restituire lo chassis guasto a NetApp.

9. **Opzionale**: Rimuovere le guide e installare le nuove guide fornite con il telaio sostitutivo.

   È possibile scegliere di riutilizzare le guide esistenti. Se si stanno riutilizzando le guide esistenti, è possibile saltare questo passaggio.

10. Far scorrere il telaio sostitutivo sulle guide.
11. Per i nodi di storage, inserire le unità dallo chassis guasto allo chassis sostitutivo.

    Inserire le unità negli stessi slot dello chassis guasto.

12. Installare le unità di alimentazione.
13. Inserire i cavi dell'alimentatore e i cavi da 1 GbE e 10 GbE nelle porte originali.

    I ricetrasmettitori SFP (Small Form-factor Pluggable) potrebbero essere inseriti nelle porte 10 GbE dello chassis sostitutivo. Rimuoverli prima di collegare via cavo le porte 10GbE.

14. Se si è stabilito che non è necessario eseguire il processo RTFI sul nodo, avviare il nodo e attendere la visualizzazione dell'interfaccia utente del terminale (TUI). Passare al punto 16 e consentire al cluster di ricreare l'immagine del nodo automaticamente quando viene aggiunto utilizzando l'interfaccia utente.
15. **Opzionale**: Se il supporto NetApp consiglia di ricreare l'imaging del nodo con una chiave USB, eseguire i seguenti passaggi secondari:
    a. Accendere lo chassis. Viene avviato con l'immagine chiave RTFI.
    b. Al primo prompt, digitare **Y** per visualizzare l'immagine del nodo di storage.
    c. Al secondo prompt, digitare **N** per i controlli dello stato dell'hardware.

       Se lo script RTFI rileva un problema con un componente hardware, viene visualizzato un errore nella console. Se viene visualizzato un errore, contattare il supporto NetApp. Al termine del processo RTFI, il nodo si spegne.

    d. Rimuovere la chiave USB dallo slot USB.
    e. Avviare il nodo appena sottoposto a imaging e attendere la visualizzazione dell'interfaccia telefonica utente (TUI).
16. Configurare le informazioni di rete e del cluster dall'interfaccia telefonica utente (TUI).

    Puoi contattare il supporto NetApp per assistenza.

17. Aggiungere il nuovo nodo al cluster utilizzando la TUI del cluster.
18. Imballare e restituire lo chassis guasto.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire le unità per i nodi di storage della serie SF

È possibile sostituire a caldo un disco a stato solido guasto con un disco sostitutivo.

Di cosa hai bisogno

- Si dispone di un disco sostitutivo.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.
- Hai contattato il supporto NetApp per verificare che l'SSD debba essere sostituito e per ricevere assistenza con la procedura di risoluzione corretta.

  Quando si contatta il supporto NetApp, è necessario il codice di matricola o il numero di serie. Il supporto collaborerà con te per ottenere un disco sostitutivo in base al tuo Service Level Agreement.

A proposito di questa attività

Le istruzioni si applicano ai seguenti modelli di nodi di storage SolidFire:

- SF2405
- SF3010
- SF4805
- SF6010
- SF9605
- SF9608
- SF9010
- SF19210
- SF38410

La seguente figura mostra la posizione delle unità in uno chassis SF9605:

La figura precedente è un esempio. SF9608 ha un diverso layout dei dischi che include solo otto dischi numerati da uno a otto, da sinistra a destra.

Lo slot 0 contiene il disco di metadati per il nodo. Se si sta sostituendo l'unità nello slot 0, è necessario applicare l'adesivo incluso nella scatola di spedizione sull'unità sostitutiva, in modo da poterla identificare separatamente dal resto. SF3010 è un'eccezione, in quanto i metadati vengono conservati nel modulo di memoria DIMM (Dual Inline Memory Module) interno Serial Advanced Technology Attachment (SATA).

Seguire queste Best practice durante la gestione dei dischi:

- Evitare le scariche elettrostatiche (ESD) mantenendo l'unità nella busta ESD fino a quando non si è pronti per l'installazione.
- Non inserire utensili metallici o coltelli nel sacchetto ESD.
- Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.
- Conservare il sacchetto ESD e il materiale di imballaggio nel caso in cui sia necessario restituire un'unità in un secondo momento.
- Indossare sempre un braccialetto antistatico collegato a terra su una superficie non verniciata dello chassis.
- Utilizzare sempre entrambe le mani durante la rimozione, l'installazione o il trasporto di un disco.
- Non forzare mai un disco nello chassis.
- Non impilare i dischi l'uno sull'altro.
- Utilizzare sempre imballaggi approvati per la spedizione delle unità.

Ecco una panoramica di alto livello dei passaggi:

- Rimuovere l'unità dal cluster
- Sostituire l'unità dal telaio
- Aggiungere l'unità al cluster

Rimuovere l'unità dal cluster

Il sistema SolidFire mette un disco in uno stato di errore se l'autodiagnosi del disco indica al nodo che si è verificato un errore o se la comunicazione con il disco si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco dei dischi guasti. Rimuovere un disco guasto dall'elenco dei dischi guasti nel software NetApp Element.

Fasi

1. Nell'interfaccia utente di Element, selezionare **Cluster** > **Drives**.
2. Selezionare **Failed** per visualizzare l'elenco dei dischi guasti.
3. Annotare il numero di slot del disco guasto.

   Queste informazioni sono necessarie per individuare il disco guasto nello chassis.

4. Rimuovere il disco guasto utilizzando uno dei seguenti metodi:

Opzione	Fasi
Per rimuovere singoli dischi	a. Selezionare **azioni** per l'unità che si desidera rimuovere. b. Selezionare **Rimuovi**.

Opzione	Fasi
Per rimuovere più dischi	a. Selezionare tutte le unità che si desidera rimuovere e selezionare **azioni in blocco**. b. Selezionare **Rimuovi**.

Sostituire l'unità dal telaio

Dopo aver rimosso un disco guasto dall'elenco dei dischi guasti nell'interfaccia utente di Element, è possibile sostituire fisicamente il disco guasto dallo chassis.

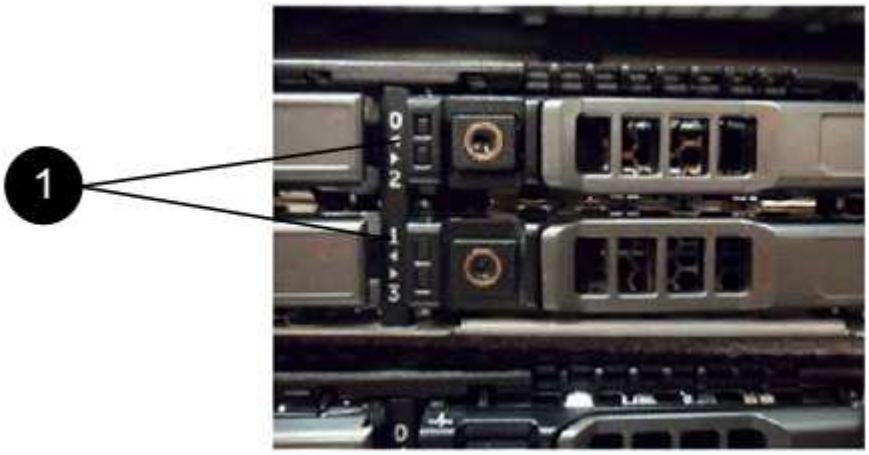
Fasi

1. Disimballare l'unità sostitutiva e posizionarla su una superficie piana e priva di scariche elettrostatiche vicino al rack.

   Conservare il materiale di imballaggio per quando si restituisce il disco guasto a NetApp.

2. Far corrispondere il numero di slot del disco guasto dell'interfaccia utente Element con il numero sullo chassis.

   La seguente figura mostra un esempio di numerazione degli slot delle unità:



Elemento	Descrizione
1	Numeri degli slot delle unità

3. Premere il cerchio rosso sull'unità che si desidera rimuovere per rilasciare l'unità.

   La chiusura a scatto si apre.

4. Estrarre l'unità dallo chassis e posizionarla su una superficie piana e priva di elettricità statica.
5. Premere il cerchio rosso sull'unità sostitutiva prima di inserirla nello slot.
6. Inserire l'unità sostitutiva e premere il cerchio rosso per chiudere il fermo.
7. Informare il supporto NetApp in merito alla sostituzione del disco.

   Il supporto NetApp fornirà istruzioni per la restituzione del disco guasto.

Aggiungere l'unità al cluster

Dopo aver installato un nuovo disco nello chassis, viene registrato come disponibile. È necessario aggiungere il disco al cluster utilizzando l'interfaccia utente Element prima che possa partecipare al cluster.

Fasi

1. Nell'interfaccia utente di Element, fare clic su **Cluster** > **Drives**.
2. Fare clic su **Available** (disponibile) per visualizzare l'elenco dei dischi disponibili.
3. Scegliere una delle seguenti opzioni per aggiungere dischi:

Opzione	Fasi
Per aggiungere singoli dischi	a. Selezionare il pulsante **azioni** dell'unità che si desidera aggiungere. b. Selezionare **Aggiungi**.
Per aggiungere più dischi	a. Selezionare le caselle di controllo delle unità da aggiungere, quindi selezionare **azioni in blocco**. b. Selezionare **Aggiungi**.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Sostituire un alimentatore

Ogni chassis SolidFire include due alimentatori per la ridondanza dell'alimentazione. In caso di guasto di un alimentatore, sostituirlo il prima possibile per assicurarsi che lo chassis disponga di una fonte di alimentazione ridondante.

Di cosa hai bisogno

- Hai determinato che l'alimentatore deve essere sostituito.
- Si dispone di un alimentatore sostitutivo.
- Hai verificato che il secondo alimentatore funziona.
- Si dispone di un braccialetto per le scariche elettrostatiche (ESD) o si sono prese altre precauzioni antistatiche.

A proposito di questa attività

Le istruzioni si applicano se si dispone di uno chassis a un rack (1U) con uno dei seguenti nodi:

- SF2405
- SF3010
- SF4805
- SF6010

- SF9605
- SF9608
- SF9010
- SF19210
- SF38410
- SF-FCN-01
- FC0025

Fasi

1. Scollegare il cavo di alimentazione dall'unità di alimentazione da sostituire.
2. Premere il pulsante di rilascio per estrarre l'alimentatore dal telaio.

   Assicurarsi di utilizzare entrambe le mani per sostenere il peso dell'alimentatore.

3. Allineare con entrambe le mani i bordi dell'alimentatore sostitutivo con l'apertura del telaio e spingere delicatamente l'unità nel telaio.

   Non esercitare una forza eccessiva quando si fa scorrere l'alimentatore nel telaio per evitare di danneggiare l'hardware.

4. Collegare il cavo di alimentazione.
5. Restituire l'unità guasta a NetApp seguendo le istruzioni riportate nella confezione.

   Puoi contattare il supporto NetApp per assistenza nella procedura di sostituzione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Tornare alle informazioni immagine di fabbrica

Configurare RTFI

I sistemi storage NetApp SolidFire utilizzano il processo di ripristino dell'immagine di fabbrica (RTFI) per scrivere un'immagine software su un nuovo nodo o ripristinare un nodo allo stato di fabbrica originale. Il processo RTFI cancella in modo sicuro tutti i dati e le configurazioni esistenti (se presenti) e installa un'immagine software NetApp Element non configurata. Il processo RTFI è disponibile per tutti i nodi SolidFire.

I sistemi SolidFire utilizzano un unico processo RTFI per tutte le installazioni di software Element. Ciò include installazioni manuali interne eseguite da sviluppatori, installazioni automatiche mediante test di framework automatizzati, installazioni sul campo da parte di tecnici dell'assistenza e clienti e installazioni eseguite da vari integratori e partner. Lo stesso processo RTFI viene utilizzato su tutti i nodi SolidFire, indipendentemente dal tipo di chassis o nodo in uso, per risolvere automaticamente eventuali problemi.

I destinatari di questa guida sono gli integratori che installano, configurano, utilizzano o risolvono i problemi

relativi allo storage.

- Linux: Hai un po' di background con i sistemi Linux.
- Networking: Hai familiarità con la rete dei server e lo storage di rete, inclusi indirizzi IP, netmask e gateway.

> Il processo RTFI è distruttivo per i dati e cancella in modo sicuro tutti i dati e i dettagli di configurazione dal nodo e installa un nuovo sistema operativo. Verificare che il nodo utilizzato per il processo RTFI non sia attivo come parte di un cluster.

Implementare e installare l'immagine RTFI International Organization for Standardization (ISO) ed eseguire il processo RTFI:

- Opzioni di installazione e implementazione RTFI
- Eseguire il processo RTFI
- Menu delle opzioni RTFI

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Il processo RTFI

È possibile iniziare il processo di ritorno all'immagine di fabbrica (RTFI) interagendo con il nodo attraverso messaggi di testo della console che appaiono prima dell'avvio del sistema.

> Il processo RTFI è distruttivo per i dati e cancella in modo sicuro tutti i dati e i dettagli di configurazione dal nodo e installa un nuovo sistema operativo. Verificare che il nodo utilizzato per il processo RTFI non sia attivo come parte di un cluster.

Il processo RTFI esegue le seguenti operazioni di alto livello:

1. Avvia l'installazione dopo la conferma dell'utente e convalida l'immagine.
2. Sblocca tutti i dischi su un nodo.
3. Convalida e aggiornamento del firmware.
4. Verifica l'hardware.
5. Verifica l'hardware.
6. Secure cancella tutti i dischi selezionati.
7. Partizione del disco root e creazione di file system.
8. Consente di montare e disimballare l'immagine.
9. Consente di configurare il nome host, la rete (Dynamic host Configuration Protocol), la configurazione predefinita del cluster e il boot loader GRUB.
10. Arresta tutti i servizi, raccoglie i registri e si riavvia.

Per configurare il nodo al termine del processo RTFI, consultare la "Documentazione relativa alla versione del software Element". Una volta completato correttamente il processo RTFI, un nodo passa allo stato *Available* (non configurato) per impostazione predefinita.

Eseguire il processo RTFI

Per ripristinare il software Element sul nodo SolidFire, attenersi alla procedura riportata di seguito.

Per informazioni sulla creazione di una chiave USB o sull'utilizzo di BMC per eseguire il processo RTFI, vedere Opzioni di installazione e implementazione RTFI.

Prima di iniziare

Verificare di soddisfare i seguenti requisiti:

- È possibile accedere a una console per il nodo SolidFire.
- Il nodo su cui si sta eseguendo il processo RTFI viene acceso e connesso a una rete.
- Il nodo su cui si sta eseguendo il processo RTFI non fa parte di un cluster attivo.
- Si dispone dell'accesso a un supporto di installazione avviabile che contiene l'immagine della versione del software Element pertinente per la configurazione.

In caso di dubbi, contattare il supporto NetApp prima di eseguire il processo RTFI.

Fasi

1. Collegare un monitor e una tastiera alla parte posteriore del nodo oppure connettersi all'interfaccia utente IP BMC e visualizzare la console **iKVM/HTML5** dalla scheda **Remote Control** dell'interfaccia utente.
2. Inserire una chiave USB con un'immagine appropriata in uno dei due slot USB sul retro del nodo.
3. Accendere o spegnere e riaccendere il nodo. Durante l'avvio, selezionare Boot Device (periferica di avvio) selezionando **F11**:

   È necessario selezionare **F11** più volte in rapida successione perché la schermata Boot Device (dispositivo di avvio) passa rapidamente.

4. Nel menu di selezione Boot Device (periferica di avvio), evidenziare l'opzione USB (USB).

   Le opzioni visualizzate dipendono dalla marca USB utilizzata.

   Se non sono presenti dispositivi USB nell'elenco, accedere al BIOS, verificare che l'unità USB sia elencata nell'ordine di avvio, riavviare e riprovare.

   Se il problema persiste, accedere al BIOS, accedere alla scheda **Save and Exit** (Salva ed esci), selezionare **Restore to Optimized Defaults** (Ripristina impostazioni predefinite ottimizzate), accettare e salvare le impostazioni e riavviare.

5. Viene visualizzato un elenco delle immagini presenti sul dispositivo USB evidenziato. Selezionare la versione desiderata e selezionare invio per avviare il processo RTFI.

   Vengono visualizzati il nome software dell'elemento immagine RTFI e il numero di versione.

6. Al prompt iniziale, viene visualizzato un messaggio che informa che il processo rimuoverà tutti i dati dal nodo e che i dati non possono essere ripristinati dopo l'inizio del processo. Immettere **Sì** per iniziare.

   Tutti i dati e i dettagli di configurazione vengono cancellati in modo permanente dal nodo dopo l'avvio del processo. Se si sceglie di non procedere, si viene indirizzati a. Menu delle opzioni RTFI.

   Se si desidera guardare la console durante il processo RTFI, è possibile premere i tasti **ALT+F8** per passare alla console in modalità dettagliata. Premere **ALT+F7** per tornare alla GUI principale.

7. Inserire **No** quando viene richiesto di eseguire test hardware approfonditi, a meno che non si abbia motivo di sospettare un guasto hardware o non si venga indirizzati all'esecuzione dei test da parte del supporto NetApp.

   Un messaggio indica che il processo RTFI è terminato e che il sistema si spegne.

8. Se necessario, rimuovere tutti i supporti di installazione avviabili dopo lo spegnimento del nodo.

   Il nodo è pronto per essere acceso e configurato. Vedere "Documentazione sullo storage per la configurazione del software Element" per configurare il nodo di storage.

   Se durante il processo RTFI viene visualizzato un messaggio di errore, vedere Menu delle opzioni RTFI.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Menu delle opzioni RTFI

Il seguente menu di opzioni viene visualizzato se il processo RTFI non riesce o se si sceglie di non procedere al prompt iniziale del processo RTFI.

Contattare il supporto NetApp prima di utilizzare una delle seguenti opzioni di comando.

Opzione	Descrizione
Riavviare	Chiude il processo RTFI e riavvia il nodo nello stato corrente. Non viene eseguita alcuna pulizia.
Spegnimento	Spegne correttamente il nodo nello stato corrente. Non viene eseguita alcuna pulizia.
Esci	Chiude il processo RTFI e apre un prompt dei comandi.
UploadLogs	Raccoglie tutti i log del sistema e carica un singolo archivio di log consolidato in un URL specificato.

Caricare i registri

Raccogliere tutti i registri sul sistema e caricarli su un URL specificato in base alla procedura seguente.

Fasi

1. Al prompt del menu delle opzioni RTFI, immettere **UploadLogs**.
2. Inserire le informazioni della directory remota:

   a. Digitare un URL che includa il protocollo. Ad esempio: `ftp://,scp://,http://,orhttps://`.

   b. (Facoltativo) aggiungere un nome utente e una password incorporati. Ad esempio: `scp://user:password@URLaddress.com`.

   > Per una gamma completa di opzioni di sintassi, vedere "Arricciatura" manuale dell'utente.

   Il file di log viene caricato e salvato nella directory specificata come `.tbz2` archiviare.

Utilizzare il tunnel di supporto

Se hai bisogno di supporto tecnico per il tuo sistema NetApp HCI o per il sistema storage all-flash SolidFire, il supporto NetApp può connetterti in remoto con il tuo sistema. Per avviare una sessione e ottenere l'accesso remoto, il supporto NetApp può aprire una connessione Secure Shell (SSH) inversa al proprio ambiente.

Con il supporto NetApp è possibile aprire una porta TCP per una connessione a tunnel inverso SSH. Questa connessione consente al supporto NetApp di accedere al nodo di gestione.

Prima di iniziare

- Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disattivata per impostazione predefinita nel nodo di gestione. Per attivare la funzionalità di accesso remoto, vedere "Gestire la funzionalità SSH sul nodo di gestione".
- Se il nodo di gestione si trova dietro un server proxy, nel file sshd.config sono necessarie le seguenti porte TCP:

Porta TCP	Descrizione	Direzione di connessione
443	Chiamate API/HTTPS per l'inoltro inverso delle porte all'interfaccia utente Web tramite tunnel di supporto aperto	Nodo di gestione ai nodi di storage
22	Accesso SSH	Nodo di gestione per nodi di storage o da nodi di storage a nodi di gestione

Fasi

- Accedere al nodo di gestione e aprire una sessione terminale.
- Quando richiesto, immettere quanto segue:

  ```
  rst -r sfsupport.solidfire.com -u element -p <port_number>
  ```

- Per chiudere il tunnel di supporto remoto, immettere quanto segue:

  ```
  rst --killall
  ```

- (Facoltativo) Disattiva "funzionalità di accesso remoto" di nuovo.

SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

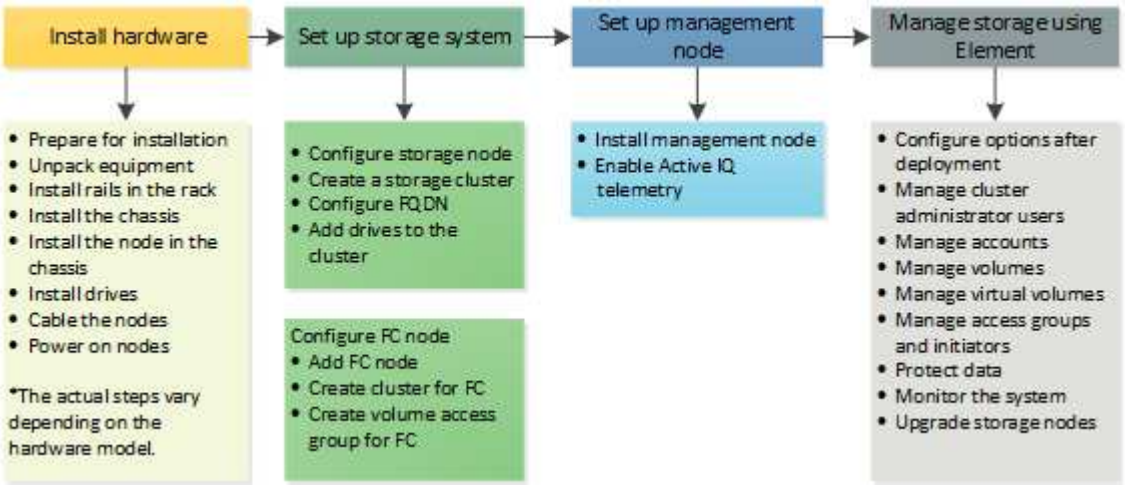
Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Panoramica dell'installazione

A questo punto, l'hardware dovrebbe essere installato. L'hardware include anche software Element.

Successivamente, è necessario configurare il sistema di storage per il proprio ambiente. È possibile configurare un cluster con nodi di storage o Fibre Channel e gestirlo utilizzando il software Element dopo l'installazione e l'accensione dei nodi in un'unità rack.



Procedura per la configurazione dello storage

1. Selezionare una delle seguenti opzioni:
   - "Configurare il cluster con nodi di storage"
   - "Configurare il cluster con nodi Fibre Channel"
2. "Determinare quali componenti di SolidFire installare"
3. "Configurare un nodo di gestione e abilitare la telemetria Active IQ"

Trova ulteriori informazioni

- "Scopri i passaggi successivi per l'utilizzo dello storage"
- "Documentazione software SolidFire ed Element"

Configurazione di un cluster con nodi storage Element

È possibile configurare un cluster con nodi di storage e gestirlo utilizzando il software Element dopo aver installato e collegato i nodi in un'unità rack e averli accesi. È quindi possibile installare e configurare componenti aggiuntivi nel sistema di storage.

Fasi

1. "Configurare un nodo di storage"
2. "Creare un cluster di storage"
3. "Accedere all'interfaccia utente del software Element"
4. "Aggiungere dischi al cluster"

5. "Determinare quali componenti di SolidFire installare"
6. "Configurare un nodo di gestione"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

Configurare un nodo di storage

È necessario configurare singoli nodi prima di aggiungerli a un cluster. Dopo aver installato e collegato un nodo in un'unità rack e averlo acceso, è possibile configurare le impostazioni di rete del nodo utilizzando l'interfaccia utente per nodo o l'interfaccia utente del terminale del nodo (TUI). Prima di procedere, assicurarsi di disporre delle informazioni di configurazione di rete necessarie per il nodo.

Sono disponibili due opzioni per la configurazione dei nodi di storage:

- UI per nodo: Utilizzare l'interfaccia utente per nodo (https://<node_management_IP>:442) per configurare le impostazioni di rete del nodo.
- TUI: Utilizzare l'interfaccia utente del terminale del nodo (TUI) per configurare il nodo.

Non è possibile aggiungere un nodo con indirizzi IP assegnati da DHCP a un cluster. È possibile utilizzare l'indirizzo IP DHCP per configurare inizialmente il nodo nell'interfaccia utente, nell'interfaccia telefonica utente o nell'API per nodo. Durante questa configurazione iniziale, è possibile aggiungere informazioni sull'indirizzo IP statico in modo da poter aggiungere il nodo a un cluster.

Dopo la configurazione iniziale, è possibile accedere al nodo utilizzando l'indirizzo IP di gestione del nodo. È quindi possibile modificare le impostazioni del nodo, aggiungerle a un cluster o utilizzare il nodo per creare un cluster. È inoltre possibile configurare un nuovo nodo utilizzando i metodi API del software Element.

> A partire dalla versione 11.0 di Element, i nodi possono essere configurati con indirizzi IPv4, IPv6 o entrambi per la propria rete di gestione. Questo vale sia per i nodi di storage che per i nodi di gestione, ad eccezione del nodo di gestione 11.3 e successivo che non supporta IPv6. Quando si crea un cluster, è possibile utilizzare un solo indirizzo IPv4 o IPv6 per MVIP e il tipo di indirizzo corrispondente deve essere configurato su tutti i nodi.

Configurare un nodo di storage utilizzando l'interfaccia utente per nodo

È possibile configurare i nodi utilizzando l'interfaccia utente per nodo.

A proposito di questa attività

- È possibile configurare il nodo in modo che disponga di un indirizzo IPv4 o IPv6.
- Per accedere a un nodo, è necessario l'indirizzo DHCP visualizzato nell'interfaccia telefonica utente. Non è possibile utilizzare gli indirizzi DHCP per aggiungere un nodo a un cluster.

È necessario configurare le interfacce di gestione (Bond1G) e storage (Bond10G) per sottoreti separate. Le interfacce Bond1G e Bond10G configurate per la stessa subnet causano problemi di routing quando il traffico di storage viene inviato tramite l'interfaccia Bond1G. Se è necessario utilizzare la stessa subnet per il traffico di gestione e storage, configurare manualmente il traffico di gestione per utilizzare l'interfaccia Bond10G. È possibile eseguire questa operazione per ciascun nodo utilizzando la pagina **Cluster Settings** dell'interfaccia utente per nodo.

Fasi

1. In una finestra del browser, inserire l'indirizzo IP DHCP di un nodo.

   È necessario aggiungere l'interno `:442` per accedere al nodo, ad esempio https://172.25.103.6:442.

   Viene visualizzata la scheda **Network Settings** (Impostazioni di rete) con la sezione **Bond1G**.

2. Inserire le impostazioni di rete di gestione 1G.
3. Fare clic su **Applica modifiche**.
4. Fare clic su **Bond10G** per visualizzare le impostazioni della rete di storage 10G.
5. Inserire le impostazioni della rete di storage 10G.
6. Fare clic su **Applica modifiche**.
7. Fare clic su **Cluster Settings** (Impostazioni cluster).
8. Immettere il nome host per la rete 10G.
9. Inserire il nome del cluster.

   Questo nome deve essere aggiunto alla configurazione per tutti i nodi prima di poter creare un cluster. Tutti i nodi di un cluster devono avere nomi di cluster identici. I nomi dei cluster sono sensibili al maiuscolo/minuscolo.

10. Fare clic su **Applica modifiche**.

Configurare un nodo di storage utilizzando l'interfaccia telefonica utente (TUI)

È possibile utilizzare l'interfaccia utente del terminale (TUI) per eseguire la configurazione iniziale per i nuovi nodi.

Configurare le interfacce Bond1G (Management) e Bond10G (Storage) per sottoreti separate. Le interfacce Bond1G e Bond10G configurate per la stessa sottorete causano problemi di routing quando il traffico di storage viene inviato tramite l'interfaccia Bond1G. Se è necessario utilizzare la stessa subnet per il traffico di gestione e storage, configurare manualmente il traffico di gestione per utilizzare l'interfaccia Bond10G. È possibile eseguire questa operazione per ciascun nodo utilizzando la pagina **Cluster** > **Nodes** dell'interfaccia utente Element.

Fasi

1. Collegare una tastiera e un monitor al nodo, quindi accendere il nodo.

   Il menu principale dello storage NetApp dell'interfaccia telefonica utente viene visualizzato sul terminale tty1.

Se il nodo non riesce a raggiungere il server di configurazione, l'interfaccia telefonica utente visualizza un messaggio di errore. Verificare la connessione al server di configurazione o alla rete per risolvere l'errore.

2. Selezionare **Network** > **Network Config**.

Per spostarsi all'interno del menu, premere i tasti freccia su o giù. Per passare a un altro pulsante o ai campi dei pulsanti, premere **Tab**. Per spostarsi tra i campi, utilizzare i tasti freccia su o giù.

3. Selezionare **Bond1G (Management)** o **Bond10G (Storage)** per configurare le impostazioni di rete 1G e 10G per il nodo.
4. Per i campi modalità Bond e Stato, premere **Tab** per selezionare il pulsante Help (Guida) e identificare le opzioni disponibili.

   Tutti i nodi di un cluster devono avere nomi di cluster identici. I nomi dei cluster sono sensibili al maiuscolo/minuscolo. Se sulla rete è in esecuzione un server DHCP con indirizzi IP disponibili, l'indirizzo 1GbE viene visualizzato nel campo Address (Indirizzo).

5. Premere **Tab** per selezionare il pulsante **OK** e salvare le modifiche.

   Il nodo viene messo in uno stato in sospeso e può essere aggiunto a un cluster esistente o a un nuovo cluster.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Creare un cluster di storage

È possibile creare un cluster di storage dopo aver configurato tutti i singoli nodi. Quando si crea un cluster, viene creato automaticamente un account utente amministratore del cluster. L'amministratore del cluster dispone dell'autorizzazione per gestire tutti gli attributi del cluster e può creare altri account amministratore del cluster.

Di cosa hai bisogno

- Il nodo di gestione è stato installato.
- Sono stati configurati tutti i singoli nodi.

A proposito di questa attività

Durante la configurazione del nuovo nodo, gli indirizzi IP di gestione (MIP) 1G o 10G vengono assegnati a ciascun nodo. Per aprire la pagina Create a New Cluster (Crea nuovo cluster), è necessario utilizzare uno degli indirizzi IP del nodo creati durante la configurazione. L'indirizzo IP utilizzato dipende dalla rete scelta per la gestione del cluster.

Se si desidera attivare l'intero cluster "crittografia software a riposo", è necessario creare il cluster utilizzando "CreateCluster" Metodo API e impostare il parametro enableSoftwareEncryptionAtRest su `true`. Una volta attivata, la crittografia software a riposo non può essere disattivata nel cluster. La crittografia basata su hardware a riposo può essere "attivato e disattivato" dopo la creazione del cluster.

Quando si crea un nuovo cluster, considerare quanto segue:

- Se si utilizzano nodi di storage che risiedono in uno chassis condiviso, è consigliabile progettare la protezione dai guasti a livello di chassis utilizzando la funzione dei domini di protezione.
- Se uno chassis condiviso non viene utilizzato, è possibile definire un layout personalizzato del dominio di protezione.

Fasi

1. In una finestra del browser, immettere `https://MIP:443`, Dove MIP è l'indirizzo IP del nodo di gestione.
2. In Create a New Cluster (Crea nuovo cluster), immettere le seguenti informazioni:
   - VIP di gestione: IP virtuale instradabile sulla rete 1GbE o 10GbE per le attività di gestione della rete.

     È possibile creare un nuovo cluster utilizzando l'indirizzamento IPv4 o IPv6.

   - VIP iSCSI (storage): IP virtuale sulla rete 10GbE per lo storage e il rilevamento iSCSI.

     Dopo aver creato il cluster, non è possibile modificare il nome MVIP, SVIP o del cluster.

   - User name (Nome utente): Il nome utente principale dell'amministratore del cluster per l'accesso autenticato al cluster. Salvare il nome utente per riferimenti futuri.

     È possibile utilizzare lettere maiuscole e minuscole, caratteri speciali e numeri per il nome utente e la password.

   - Password: Password per l'accesso autenticato al cluster. È necessario salvare la password per riferimenti futuri. La protezione dei dati bidirezionale è attivata per impostazione predefinita. Non è possibile modificare questa impostazione.
3. Leggere il Contratto di licenza con l'utente finale e selezionare **Accetto**.
4. **Opzionale**: Nell'elenco nodi, assicurarsi che le caselle di controllo per i nodi che non devono essere inclusi nel cluster non siano selezionate.
5. Selezionare **Create Cluster** (Crea cluster).

   Il sistema potrebbe impiegare diversi minuti per creare il cluster a seconda del numero di nodi nel cluster. Su una rete correttamente configurata, un piccolo cluster di cinque nodi dovrebbe richiedere meno di un minuto. Una volta creato il cluster, la finestra Create a New Cluster (Crea nuovo cluster) viene reindirizzata all'indirizzo URL MVIP del cluster e viene visualizzata l'interfaccia utente elemento.

Per ulteriori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione software SolidFire ed Element"

- "Plug-in NetApp Element per server vCenter"

Accedere all'interfaccia utente del software Element

È possibile accedere all'interfaccia utente Element utilizzando l'indirizzo IP virtuale di gestione (MVIP) del nodo principale del cluster.

Assicurarsi che i blocchi dei popup e le impostazioni NoScript siano disattivati nel browser.

È possibile accedere all'interfaccia utente utilizzando l'indirizzamento IPv4 o IPv6, a seconda della configurazione durante la creazione del cluster.

Fasi

1. Scegliere una delle seguenti opzioni:
   - IPv6: Invio `https://[IPv6_MVIP_address]`. Ad esempio:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

   - IPv4: Immettere `https://[IPv4 MVIP address]`. Ad esempio:

     ```
     https://10.123.456.789/
     ```

2. Per DNS, immettere il nome host.
3. Fare clic sui messaggi dei certificati di autenticazione.

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiungere dischi a un cluster

Quando si aggiunge un nodo al cluster o si installano nuove unità in un nodo esistente, le unità vengono automaticamente registrate come disponibili. È necessario aggiungere le unità al cluster utilizzando l'interfaccia utente Element o l'API prima che possano partecipare al cluster.

Le unità non vengono visualizzate nell'elenco Available Drives (unità disponibili) quando sussistono le seguenti condizioni:

- Le unità sono in stato attivo, Rimozione, cancellazione o guasto.
- Il nodo di cui fa parte l'unità è in stato Pending.

Fasi

1. Dall'interfaccia utente di Element, selezionare **Cluster** > **Drives**.
2. Fare clic su **Available** (disponibile) per visualizzare l'elenco dei dischi disponibili.

3. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli dischi, fare clic sull'icona **azioni** del disco che si desidera aggiungere e fare clic su **Aggiungi**.
   - Per aggiungere più dischi, selezionare le caselle di controllo delle unità da aggiungere, fare clic su **azioni in blocco** e fare clic su **Aggiungi**.

```
== Find more information
* https://docs.netapp.com/us-en/element-software/index.html[SolidFire
and Element Software Documentation]
* https://docs.netapp.com/us-en/vcp/index.html[NetApp Element Plug-in
for vCenter Server^]
```

Configurare un cluster con nodi Fibre Channel

Configurare un nodo Fibre Channel

I nodi Fibre Channel consentono di collegare il cluster a un fabric di rete Fibre Channel. I nodi Fibre Channel vengono aggiunti a coppie e funzionano in modalità Active-Active (tutti i nodi elaborano attivamente il traffico per il cluster). I cluster che eseguono Element Software versione 9.0 e successive supportano fino a quattro nodi; i cluster che eseguono versioni precedenti supportano un massimo di due nodi.

Prima di configurare un nodo Fibre Channel, assicurarsi che siano soddisfatte le seguenti condizioni:

- Almeno due nodi Fibre Channel sono collegati agli switch Fibre Channel.
- Tutte le porte Fibre Channel SolidFire devono essere collegate al fabric Fibre Channel. Le quattro connessioni di rete SolidFire Bond10G devono essere collegate in un unico gruppo di bond LACP a livello di switch. In questo modo si otterranno le migliori prestazioni complessive dei sistemi Fibre Channel.
- Esaminare e convalidare tutte le Best practice per i cluster Fibre Channel incluse in questo articolo della Knowledge base di NetApp.

  "Best practice per il cluster SolidFire FC"

Le fasi di configurazione della rete e del cluster sono le stesse per i nodi Fibre Channel e i nodi di storage.

Quando si crea un nuovo cluster con nodi Fibre Channel e nodi di storage SolidFire, gli indirizzi WWPN (Worldwide Port Name) per i nodi sono disponibili nell'interfaccia utente di Element. È possibile utilizzare gli indirizzi WWPN per mettere in zona lo switch Fibre Channel.

Le WWPN vengono registrate nel sistema quando si crea un nuovo cluster con nodi. Nell'interfaccia utente Element, è possibile trovare gli indirizzi WWPN dalla colonna WWPN della scheda FC Ports (Porte FC), a cui si accede dalla scheda Cluster.

Trova ulteriori informazioni

Aggiunta di nodi Fibre Channel a un cluster

Creare un nuovo cluster con nodi Fibre Channel

È possibile creare un nuovo cluster dopo aver configurato i singoli nodi Fibre Channel. Quando si crea un cluster, viene creato automaticamente un account utente amministratore del cluster. L'amministratore del cluster dispone dell'autorizzazione per gestire tutti gli attributi del cluster e può creare altri account amministratore del cluster.

Durante la configurazione del nuovo nodo, gli indirizzi IP di gestione (MIP) 1G o 10G vengono assegnati a ciascun nodo. Per aprire la pagina Create a New Cluster (Crea nuovo cluster), è necessario utilizzare uno degli indirizzi IP del nodo creati durante la configurazione. L'indirizzo IP utilizzato dipende dalla rete scelta per la gestione del cluster.

Di cosa hai bisogno

I singoli nodi Fibre Channel sono stati configurati.

Fasi

1. In una finestra del browser, inserire un indirizzo MIP del nodo.
2. In Create a New Cluster (Crea nuovo cluster), immettere le seguenti informazioni:
   - VIP di gestione: IP virtuale instradabile sulla rete 1GbE o 10GbE per le attività di gestione della rete.
   - VIP iSCSI (storage): IP virtuale sulla rete 10GbE per lo storage e il rilevamento iSCSI.

     Non è possibile modificare l'SVIP dopo aver creato il cluster.

   - User name (Nome utente): Il nome utente principale di Cluster Admin per l'accesso autenticato al cluster. Salvare il nome utente per riferimenti futuri.

     È possibile utilizzare lettere maiuscole e minuscole, caratteri speciali e numeri per il nome utente.

   - Password: Password per l'accesso autenticato al cluster. Salvare il nome utente per riferimenti futuri. La protezione dei dati bidirezionale è attivata per impostazione predefinita. Non è possibile modificare questa impostazione.
3. Leggere il Contratto di licenza con l'utente finale e fare clic su **Accetto**.
4. **Opzionale**: Nell'elenco nodi, assicurarsi che le caselle di controllo per i nodi che non devono essere inclusi nel cluster non siano selezionate.
5. Fare clic su **Create Cluster** (Crea cluster).

   Il sistema potrebbe impiegare diversi minuti per creare il cluster a seconda del numero di nodi nel cluster. Su una rete correttamente configurata, un piccolo cluster di cinque nodi dovrebbe richiedere meno di un minuto. Una volta creato il cluster, la finestra Create a New Cluster (Crea nuovo cluster) viene reindirizzata all'indirizzo URL MVIP del cluster e viene visualizzata l'interfaccia utente Web.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiunta di nodi Fibre Channel a un cluster

È possibile aggiungere nodi Fibre Channel a un cluster quando è necessario più storage o durante la creazione del cluster. I nodi Fibre Channel richiedono la configurazione iniziale quando vengono accesi per la prima volta. Una volta configurato, il nodo viene visualizzato nell'elenco dei nodi in sospeso ed è possibile aggiungerlo a un cluster.

La versione software di ciascun nodo Fibre Channel di un cluster deve essere compatibile. Quando si aggiunge un nodo Fibre Channel a un cluster, il cluster installa la versione cluster di Element sul nuovo nodo in base alle necessità.

Fasi

1. Selezionare **Cluster** > **Nodes**.
2. Fare clic su **Pending** (in sospeso) per visualizzare l'elenco dei nodi in sospeso.
3. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli nodi, fare clic sull'icona **azioni** del nodo che si desidera aggiungere.
   - Per aggiungere più nodi, selezionare la casella di controllo dei nodi da aggiungere, quindi **azioni in blocco**.

   > Se il nodo che si sta aggiungendo ha una versione di Element diversa dalla versione in esecuzione sul cluster, il cluster aggiorna il nodo in modo asincrono alla versione di Element in esecuzione sul cluster master. Una volta aggiornato, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo si trova in uno stato Active pendingActive.

4. Fare clic su **Aggiungi**.

   Il nodo viene visualizzato nell'elenco dei nodi attivi.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Impostare le zone per i nodi Fibre Channel

Quando si crea un nuovo cluster con nodi Fibre Channel e nodi di storage SolidFire, gli indirizzi WWPN (Worldwide Port Name) per i nodi sono disponibili nell'interfaccia utente Web. È possibile utilizzare gli indirizzi WWPN per mettere in zona lo switch Fibre Channel.

Le WWPN vengono registrate nel sistema quando si crea un nuovo cluster con nodi. Nell'interfaccia utente Element, è possibile trovare gli indirizzi WWPN dalla colonna WWPN della scheda FC Ports (Porte FC), a cui si accede dalla scheda Cluster.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"

- "Plug-in NetApp Element per server vCenter"

Creare un gruppo di accesso al volume per i client Fibre Channel

I gruppi di accesso ai volumi consentono la comunicazione tra i client Fibre Channel e i volumi su un sistema storage SolidFire. Il mapping degli iniziatori client Fibre Channel (WWPN) ai volumi di un gruppo di accesso volume consente l'i/o sicuro dei dati tra una rete Fibre Channel e un volume SolidFire.

È inoltre possibile aggiungere gli iniziatori iSCSI a un gruppo di accesso al volume, in modo che gli iniziatori possano accedere agli stessi volumi nel gruppo di accesso al volume.

Fasi

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic su **Create Access Group** (Crea gruppo di accesso).
3. Inserire un nome per il gruppo di accesso al volume nel campo **Nome**.
4. Selezionare e aggiungere gli iniziatori Fibre Channel dall'elenco **Initiator Fibre Channel non associati**.

   È possibile aggiungere o eliminare gli iniziatori in un secondo momento.

5. **Opzionale:** selezionare e aggiungere un iSCSI Initiator dall'elenco **Initiator**.
6. Per collegare i volumi al gruppo di accesso, attenersi alla seguente procedura:
   a. Selezionare un volume dall'elenco **volumi**.
   b. Fare clic su **Allega volume**.
7. Fare clic su **Create Access Group** (Crea gruppo di accesso).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Determinare quali componenti di SolidFire installare

A seconda delle opzioni di configurazione e implementazione, è possibile verificare quali componenti di SolidFire, come il nodo di gestione, Active IQ e l'agente di monitoraggio NetApp (NMA), devono essere installati.

La seguente tabella elenca i componenti aggiuntivi e indica se è necessario installarli.

Componente	Cluster di storage SolidFire standalone	Cluster NetApp HCI
Nodo di gestione	Consigliato	Installato per impostazione predefinita, obbligatorio
Active IQ	Consigliato*	Consigliato*

Componente	Cluster di storage SolidFire standalone	Cluster NetApp HCI
Agente di monitoraggio NetApp	Non supportato	Consigliato

*Active IQ è richiesto per i cluster di storage SolidFire con licenza di capacità.

Fasi

1. Determinare i componenti da installare.
2. Completare l'installazione seguendo le istruzioni della "installare il nodo di gestione" procedura.

> Per configurare Active IQ, utilizzare `--telemetry_active` Nello script di setup per abilitare la raccolta di dati per l'analisi da parte di Active IQ.

3. Per informazioni su NetApp Monitoring Agent, consulta questa sezione "procedura".

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare un nodo di gestione

È possibile installare il nodo di gestione del software NetApp Element (mNode) per aggiornare e fornire servizi di sistema, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

1. Vedere "installare il nodo di gestione" documentazione.

> Per configurare Active IQ, utilizzare `--telemetry_active` Nello script di setup per abilitare la raccolta di dati per l'analisi da parte di Active IQ.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare l'accesso completo all'interfaccia utente Web Domain Name

Lo storage all-flash SolidFire con il software NetApp Element 12.2 o versione successiva consente di accedere alle interfacce Web del cluster di storage utilizzando il nome di dominio completo (FQDN). Se si desidera utilizzare l'FQDN per accedere alle interfacce utente Web, ad esempio l'interfaccia utente Web Element, l'interfaccia utente per nodo o l'interfaccia utente del nodo di gestione, è necessario prima aggiungere un'impostazione

del cluster di storage per identificare l'FQDN utilizzato dal cluster.

Questo processo consente al cluster di reindirizzare correttamente una sessione di accesso e migliora l'integrazione con servizi esterni come i key manager e i provider di identità per l'autenticazione a più fattori.

Di cosa hai bisogno

- Questa funzione richiede Element 12.2 o versione successiva.
- La configurazione di questa funzionalità utilizzando le API REST di NetApp Hybrid Cloud Control richiede servizi di gestione 2.15 o successivi.
- La configurazione di questa funzione mediante l'interfaccia utente di NetApp Hybrid Cloud Control richiede servizi di gestione 2.19 o successivi.
- Per utilizzare le API REST, è necessario aver implementato un nodo di gestione con versione 11.5 o successiva.
- Sono necessari nomi di dominio completi per il nodo di gestione e ciascun cluster di storage che si risolvono correttamente nell'indirizzo IP del nodo di gestione e in ciascun indirizzo IP del cluster di storage.

È possibile configurare o rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control e l'API REST. È inoltre possibile risolvere i problemi relativi a FQDN configurati in modo errato.

- Configurare l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control
- Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST
- Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control
- Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST
- Risoluzione dei problemi

Configurare l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare l'icona del menu nella parte superiore destra della pagina.
4. Selezionare **Configura**.
5. Nel riquadro **Fully Qualified Domain Names**, selezionare **Set Up**.
6. Nella finestra visualizzata, immettere gli FQDN per il nodo di gestione e ciascun cluster di storage.
7. Selezionare **Salva**.

   Il riquadro **Fully Qualified Domain Names** elenca ciascun cluster di storage con i relativi MVIP e FQDN associati.

   Solo i cluster di storage connessi con il set FQDN sono elencati nel riquadro **Fully Qualified Domain Names**.

Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST

Fasi

1. Assicurarsi che i nodi di storage Element e mNode abbiano il DNS configurato correttamente per l'ambiente di rete in modo che gli FQDN nell'ambiente possano essere risolti. Per impostare il DNS, accedere all'interfaccia utente per nodo per i nodi di storage e al nodo di gestione, quindi selezionare **Impostazioni di rete** > **rete di gestione**.
   a. Interfaccia utente per nodo per nodi di storage: `https://<storage_node_management_IP>:442`
   b. Interfaccia utente per nodo per il nodo di gestione: `https://<management_node_IP>:442`
2. Modificare le impostazioni del cluster di storage utilizzando l'API Element.
   a. Accedere all'API Element e creare la seguente preferenza di interfaccia cluster utilizzando "CreateClusterInterfacePreference" Metodo API, inserendo il FQDN MVIP del cluster come valore di preferenza:
      - Nome: `mvip_fqdn`
      - Valore: `Fully Qualified Domain Name for the Cluster MVIP`

        In questo esempio, FQDN=storagecluster.my.org:

```
https://<Cluster_MVIP>/json-rpc/12.2?
method=CreateClusterInterfacePreference&name=mvip_fqdn&value=storageclus
ter.my.org
```

3. Modificare le impostazioni del nodo di gestione utilizzando l'API REST sul nodo di gestione:
   a. Accedere all'interfaccia utente API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`

      Ad esempio:

`https://<management_node_IP>/mnode/2/`

   a. Fare clic su **autorizzare** o su un'icona a forma di lucchetto e immettere il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Fare clic su **autorizzare** per avviare la sessione e chiudere la finestra.
   d. Dall'elenco dei server, selezionare `mnode2`.
   e. Fare clic su **GET /settings**.
   f. Fare clic su **Provalo**.
   g. Fare clic su **Execute** (Esegui).
   h. Registrare eventuali impostazioni proxy riportate nel corpo della risposta.
   i. Fare clic su **PUT/settings**.
   j. Fare clic su **Provalo**.
   k. Nell'area del corpo della richiesta, inserire il nodo di gestione FQDN come valore per `mnode_fqdn`

parametro.

l. Inserire i valori di impostazione del proxy registrati in precedenza nei parametri rimanenti nel corpo della richiesta. Se si lasciano vuoti i parametri proxy o non li si includono nel corpo della richiesta, le impostazioni proxy esistenti verranno rimosse.

m. Fare clic su **Execute** (Esegui).

Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando NetApp Hybrid Cloud Control

È possibile utilizzare questa procedura per rimuovere l'accesso Web FQDN per il nodo di gestione e i cluster di storage.

Fasi

1. Nel riquadro **Fully Qualified Domain Names**, selezionare **Edit** (Modifica).
2. Nella finestra visualizzata, eliminare il contenuto del campo di testo **FQDN**.
3. Selezionare **Salva**.

   La finestra si chiude e l'FQDN non è più elencato nel riquadro **Fully Qualified Domain Names**.

Rimuovere l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST

Fasi

1. Modificare le impostazioni del cluster di storage utilizzando l'API Element.

   a. Accedere all'API Element ed eliminare la seguente preferenza di interfaccia cluster utilizzando `DeleteClusterInterfacePreference` Metodo API:

      - Nome: `mvip_fqdn`

        Ad esempio:

```
https://<Cluster_MVIP>/json-
rpc/12.2?method=DeleteClusterInterfacePreference&name=mvip_fqdn
```

2. Modificare le impostazioni del nodo di gestione utilizzando l'API REST sul nodo di gestione:

   a. Accedere all'interfaccia utente API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`. Ad esempio:

```
https://<management_node_IP>/mnode/2/
```

   b. Selezionare **autorizzare** o un'icona a forma di lucchetto e inserire il nome utente e la password del cluster di elementi.

   c. Immettere l'ID client come `mnode-client`.

   d. Selezionare **autorizzare** per avviare una sessione.

   e. Chiudere la finestra.

f. Selezionare **PUT /settings**.

g. Selezionare **Provalo**.

h. Nell'area del corpo della richiesta, non inserire un valore per `mnode_fqdn` parametro. Specificare inoltre se utilizzare il proxy (`true` oppure `false`) per `use_proxy` parametro.

```
{
 "mnode_fqdn": "",
 "use_proxy": false
}
```

i. Selezionare **Esegui**.

Risoluzione dei problemi

Se gli FQDN non sono configurati correttamente, potrebbero verificarsi problemi di accesso al nodo di gestione, a un cluster di storage o a entrambi. Utilizzare le seguenti informazioni per risolvere il problema.

Problema	Causa	Risoluzione
• Viene visualizzato un errore del browser quando si tenta di accedere al nodo di gestione o al cluster di storage utilizzando l'FQDN. • Non è possibile accedere al nodo di gestione o al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione e l'FQDN del cluster di storage non sono configurati correttamente.	Utilizzare le istruzioni REST API riportate in questa pagina per rimuovere le impostazioni FQDN del nodo di gestione e del cluster di storage e configurarle di nuovo.
• Viene visualizzato un errore del browser quando si tenta di accedere al FQDN del cluster di storage. • Non è possibile accedere al nodo di gestione o al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione è configurato correttamente, ma l'FQDN del cluster di storage non è configurato correttamente.	Utilizzare le istruzioni REST API riportate in questa pagina per rimuovere le impostazioni FQDN del cluster di storage e configurarle di nuovo
• Si verifica un errore del browser quando si tenta di accedere al nodo di gestione FQDN. • È possibile accedere al nodo di gestione e al cluster di storage utilizzando un indirizzo IP.	L'FQDN del nodo di gestione non è configurato correttamente, ma l'FQDN del cluster di storage è configurato correttamente.	Accedere a NetApp Hybrid Cloud Control per correggere le impostazioni FQDN del nodo di gestione nell'interfaccia utente oppure utilizzare le istruzioni API REST in questa pagina per correggere le impostazioni.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Cosa succederà

Dopo aver configurato il software Element, è possibile gestire lo storage completando alcune delle seguenti opzioni:

- "Accedere all'interfaccia utente del software Element"
- "Configurare le opzioni del sistema SolidFire dopo l'implementazione"
- "Gestire gli account"
- "Gestire il sistema"
- "Gestire volumi e volumi virtuali"
- "Proteggi i tuoi dati"
- "Risolvere i problemi del sistema"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"
- "Plug-in NetApp Element per server vCenter"

Gestire lo storage con il software Element

Utilizza il software Element per configurare lo storage SolidFire, monitorare la capacità e le performance del cluster e gestire l'attività dello storage in un'infrastruttura multi-tenant.

Element è il sistema operativo per lo storage al centro di un cluster SolidFire. Il software Element viene eseguito in modo indipendente su tutti i nodi del cluster e consente ai nodi del cluster di combinare le risorse e di presentarsi come un singolo sistema storage ai client esterni. Il software Element è responsabile di tutto il coordinamento, la scalabilità e la gestione del cluster nel suo complesso.

L'interfaccia software si basa sull'API Element.

- "Accedere all'interfaccia utente del software Element"
- "Configurare le opzioni del sistema SolidFire dopo l'implementazione"
- "Aggiornare i componenti del sistema storage"
- "Utilizzare le opzioni di base nell'interfaccia utente del software Element"
- "Gestire gli account"
- "Gestire il sistema"
- "Gestire volumi e volumi virtuali"
- "Proteggi i tuoi dati"
- "Risolvere i problemi del sistema"

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Accedere all'interfaccia utente del software Element

È possibile accedere all'interfaccia utente Element utilizzando l'indirizzo IP virtuale di gestione (MVIP) del nodo principale del cluster.

Assicurarsi che i blocchi dei popup e le impostazioni NoScript siano disattivati nel browser.

È possibile accedere all'interfaccia utente utilizzando l'indirizzamento IPv4 o IPv6, a seconda della configurazione durante la creazione del cluster.

1. Scegliere una delle seguenti opzioni:
   - IPv6: Inserire https://[IPv6 MVIP address] ad esempio:

     ```
     https://[fd20:8b1e:b256:45a::1234]/
     ```

   - IPv4: Inserire https://[IPv4 MVIP address] ad esempio:

```
https://10.123.456.789/
```

2. Per DNS, immettere il nome host.
3. Fare clic sui messaggi dei certificati di autenticazione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare le opzioni del sistema SolidFire dopo l'implementazione

Dopo aver configurato il sistema SolidFire, è possibile eseguire alcune attività facoltative.

Se si modificano le credenziali nel sistema, potrebbe essere necessario conoscere l'impatto su altri componenti.

Inoltre, è possibile configurare le impostazioni per l'autenticazione a più fattori, la gestione delle chiavi esterne e la protezione FIPS (Federal Information Processing Standards). Inoltre, è consigliabile aggiornare le password quando necessario.

Trova ulteriori informazioni

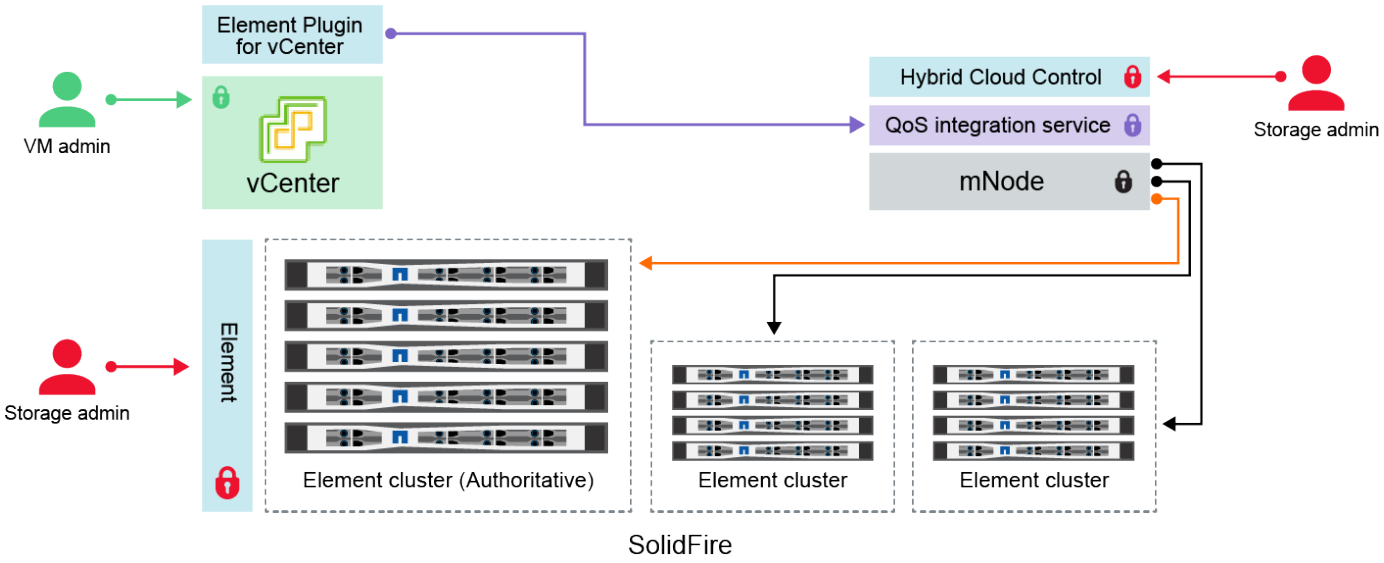
- "Modificare le credenziali in NetApp HCI e NetApp SolidFire"
- "Modificare il certificato SSL predefinito del software Element"
- "Modificare la password IPMI per i nodi"
- "Abilitare l'autenticazione a più fattori"
- "Inizia a utilizzare la gestione esterna delle chiavi"
- "Creare un cluster che supporti i dischi FIPS"

Modificare le credenziali in NetApp HCI e NetApp SolidFire

A seconda delle policy di sicurezza dell'organizzazione che ha implementato NetApp HCI o NetApp SolidFire, la modifica delle credenziali o delle password è generalmente parte delle procedure di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nell'implementazione.

Se si modificano le credenziali per un componente di un'implementazione di NetApp HCI o NetApp SolidFire, la seguente tabella fornisce indicazioni sull'impatto sugli altri componenti.

Interazioni dei componenti NetApp SolidFire:



Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali dell'elemento	**Applicabile a**: NetApp HCI e SolidFire Gli amministratori utilizzano queste credenziali per accedere a: • Interfaccia utente Element sul cluster di storage Element • Controllo del cloud ibrido sul nodo di gestione (mnode) Quando Hybrid Cloud Control gestisce più cluster di storage, accetta solo le credenziali di amministratore per i cluster di storage, noto come *cluster autorevole* per cui è stato inizialmente configurato mnode. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se le credenziali per i cluster di storage aggiunti successivamente vengono modificate, le credenziali devono essere aggiornate anche in mnode utilizzando l'API mnode.	• "Aggiornare le password di amministrazione del cluster di storage." • Aggiornare le credenziali di amministratore del cluster di storage in mnode utilizzando "API modifyclusteradmin".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali vSphere Single Sign-on	**Applicabile a**: Solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere a VMware vSphere Client. Quando vCenter fa parte dell'installazione di NetApp HCI, le credenziali vengono configurate nel motore di implementazione NetApp come segue: • username@vsphere.local con la password specificata, e. • administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per implementare NetApp HCI, le credenziali di accesso singolo vSphere vengono gestite dagli amministratori IT VMware.	"Aggiornare le credenziali vCenter ed ESXi".
Credenziali BMC (Baseboard Management Controller)	**Applicabile a**: Solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di calcolo NetApp in un'implementazione NetApp HCI. BMC offre funzioni di base per il monitoraggio dell'hardware e la console virtuale. Le credenziali BMC (a volte denominate *IPMI*) per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con BMC nei nodi di calcolo durante gli aggiornamenti del firmware del nodo di calcolo. Quando le credenziali BMC vengono modificate, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate anche su mnode per mantenere tutte le funzionalità di controllo del cloud ibrido.	• "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C, "Modificare la password IPMI predefinita". • Per i nodi H410S e H610S, "Modificare la password IPM predefinita". • "Modificare le credenziali BMC sul nodo di gestione".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali ESXi	**Applicabile a**: Solo NetApp HCI Gli amministratori possono accedere agli host ESXi utilizzando SSH o DCUI locale con un account root locale. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. Le credenziali radice ESXi per ciascun nodo di calcolo NetApp vengono memorizzate in modo sicuro sull'mnode nelle implementazioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali in una capacità di account di servizio per comunicare direttamente con gli host ESXi durante gli aggiornamenti del firmware del nodo di calcolo e i controlli dello stato. Quando le credenziali root di ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di calcolo devono essere aggiornate su mnode per mantenere la funzionalità di controllo del cloud ibrido.	"Aggiorna le credenziali per gli host vCenter e ESXi".
Password di integrazione QoS	**Applicabile a**: NetApp HCI e opzionale in SolidFire Non utilizzato dagli amministratori per gli accessi interattivi. L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite: • Plug-in Element per vCenter Server e. • Servizio QoS su mnode. Per l'autenticazione, il servizio QoS utilizza una password utilizzata esclusivamente in questo contesto. La password QoS viene specificata durante l'installazione iniziale del plug-in Element per vCenter Server o generata automaticamente durante l'implementazione di NetApp HCI. Nessun impatto su altri componenti.	"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server". Il plug-in NetApp Element per la password SIOC del server vCenter è noto anche come *password QoSSIOC*. Consulta l'articolo Element Plug-in for vCenter Server KB article.

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Consultare queste istruzioni
Credenziali di vCenter Service Appliance	**Applicabile a**: NetApp HCI solo se configurato dal motore di implementazione NetApp Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle implementazioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale del nodo di calcolo nel motore di implementazione NetApp. A seconda della versione di VMware vSphere implementata, alcuni amministratori del dominio di Single Sign-on di vSphere possono anche accedere all'appliance. Nessun impatto su altri componenti.	Non sono necessarie modifiche.
Credenziali amministratore di NetApp Management Node	**Applicabile a**: NetApp HCI e opzionale in SolidFire Gli amministratori possono accedere alle macchine virtuali del nodo di gestione NetApp per la configurazione avanzata e la risoluzione dei problemi. A seconda della versione del nodo di gestione implementata, l'accesso tramite SSH non è attivato per impostazione predefinita. Nelle implementazioni NetApp HCI, il nome utente e la password sono stati specificati dall'utente durante l'installazione iniziale di tale nodo di calcolo nel motore di implementazione NetApp. Nessun impatto su altri componenti.	Non sono necessarie modifiche.

Trova ulteriori informazioni

- "Modificare il certificato SSL predefinito del software Element"
- "Modificare la password IPMI per i nodi"
- "Abilitare l'autenticazione a più fattori"
- "Inizia a utilizzare la gestione esterna delle chiavi"
- "Creare un cluster che supporti i dischi FIPS"

Modificare il certificato SSL predefinito del software Element

È possibile modificare il certificato SSL predefinito e la chiave privata del nodo di storage nel cluster utilizzando l'API NetApp Element.

Quando viene creato un cluster software NetApp Element, il cluster crea un certificato SSL (Secure Sockets Layer) con firma automatica e una chiave privata univoci che vengono utilizzati per tutte le comunicazioni HTTPS tramite l'interfaccia utente Element, l'interfaccia utente per nodo o le API. Il software Element supporta i certificati autofirmati e quelli emessi e verificati da un'autorità di certificazione (CA) attendibile.

È possibile utilizzare i seguenti metodi API per ottenere ulteriori informazioni sul certificato SSL predefinito e apportare modifiche.

- **GetSSLCertificate**

  È possibile utilizzare "Metodo GetSSLCertificate" Per recuperare informazioni sul certificato SSL attualmente installato, inclusi tutti i dettagli del certificato.

- **SetSSLCertificate**

  È possibile utilizzare "Metodo SetSSLCertificate" Per impostare i certificati SSL del cluster e per nodo in base al certificato e alla chiave privata fornita. Il sistema convalida il certificato e la chiave privata per impedire l'applicazione di un certificato non valido.

- **RemoveSSLCertificate**

  Il "Metodo RemoveSSLCertificate" Rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una nuova chiave privata.

> Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Tutti i nodi rimossi dal cluster tornano a un certificato autofirmato e tutte le informazioni di certificato e chiave definite dall'utente vengono rimosse dal nodo.

Trova ulteriori informazioni

- "Modificare il certificato SSL predefinito del nodo di gestione"
- "Quali sono i requisiti relativi all'impostazione di certificati SSL personalizzati in Element Software?"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Modificare la password IPMI predefinita per i nodi

È possibile modificare la password di amministratore predefinita di Intelligent Platform Management Interface (IPMI) non appena si dispone dell'accesso remoto IPMI al nodo. Questa operazione potrebbe essere utile se sono stati rilevati aggiornamenti per l'installazione.

Per ulteriori informazioni sulla configurazione dell'accesso IPM per i nodi, vedere "Configurare IPMI per ciascun nodo".

È possibile modificare la password IPM per questi nodi:

- Nodi H410S
- Nodi H610S

Modificare la password IPMI predefinita per i nodi H410S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di storage non appena si configura la porta di rete IPMI.

Di cosa hai bisogno

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Immettere il nome utente `ADMIN` e password `ADMIN` al prompt di login.
3. Una volta effettuato l'accesso, fare clic sulla scheda **Configuration** (Configurazione).
4. Fare clic su **utenti**.
5. Selezionare `ADMIN` E fare clic su **Modify User** (Modifica utente).
6. Selezionare la casella di controllo **Change Password** (Modifica password).
7. Immettere una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modify**, quindi su **OK**.
9. Ripetere questa procedura per tutti gli altri nodi H410S con password IPMI predefinite.

Modificare la password IPMI predefinita per i nodi H610S

È necessario modificare la password predefinita per l'account amministratore IPMI su ciascun nodo di storage non appena si configura la porta di rete IPMI.

Di cosa hai bisogno

L'indirizzo IP IPMI dovrebbe essere stato configurato per ciascun nodo di storage.

Fasi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e individuare l'indirizzo IP IPMI del nodo.
2. Immettere il nome utente `root` e password `calvin` al prompt di login.
3. Una volta effettuato l'accesso, fare clic sull'icona di navigazione del menu in alto a sinistra della pagina per aprire il cassetto della barra laterale.
4. Fare clic su **Impostazioni**.
5. Fare clic su **Gestione utenti**.
6. Selezionare l'utente **Administrator** dall'elenco.
7. Attivare la casella di controllo **Change Password** (Modifica password).
8. Immettere una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Save** (Salva) nella parte inferiore della pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Utilizzare le opzioni di base nell'interfaccia utente del software Element

L'interfaccia utente Web del software NetApp Element (Element UI) consente di monitorare ed eseguire attività comuni sul sistema SolidFire.

Le opzioni di base includono la visualizzazione dei comandi API attivati dall'attività dell'interfaccia utente e il feedback.

- "Visualizzare l'attività API"
- "Icone nell'interfaccia degli elementi"
- "Fornire un feedback"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Visualizzare l'attività API

Il sistema Element utilizza l'API NetApp Element come base per le sue funzionalità e funzionalità. L'interfaccia utente di Element consente di visualizzare vari tipi di attività API in tempo reale sul sistema durante l'utilizzo dell'interfaccia. Con il log API, è possibile visualizzare l'attività API di sistema avviata dall'utente e in background, nonché le chiamate API effettuate nella pagina visualizzata.

È possibile utilizzare il log API per identificare i metodi API utilizzati per determinate attività e vedere come utilizzare i metodi e gli oggetti API per creare applicazioni personalizzate.

Per informazioni su ciascun metodo, vedere "Riferimento API di Element Software".

1. Dalla barra di navigazione dell'interfaccia utente di Element, fare clic su **API Log**.
2. Per modificare il tipo di attività API visualizzata nella finestra API Log (Registro API), attenersi alla seguente procedura:
   a. Selezionare **Requests** per visualizzare il traffico delle richieste API.
   b. Selezionare **Responses** per visualizzare il traffico di risposta API.
   c. Filtrare i tipi di traffico API selezionando una delle seguenti opzioni:
      - **Avviato dall'utente**: Traffico API dalle attività durante questa sessione dell'interfaccia utente Web.
      - **Background polling**: Traffico API generato dall'attività di sistema in background.
      - **Pagina corrente**: Traffico API generato dalle attività sulla pagina che si sta visualizzando.

Trova ulteriori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Frequenza di refresh dell'interfaccia influenzata dal carico del cluster

A seconda dei tempi di risposta delle API, il cluster potrebbe regolare automaticamente l'intervallo di aggiornamento dei dati per alcune parti della pagina del software NetApp Element che si sta visualizzando.

L'intervallo di refresh viene ripristinato ai valori predefiniti quando si ricarica la pagina nel browser. Per visualizzare l'intervallo di aggiornamento corrente, fare clic sul nome del cluster nell'angolo superiore destro della pagina. Si noti che l'intervallo controlla la frequenza con cui vengono effettuate le richieste API, non la velocità con cui i dati vengono ripristinati dal server.

Quando un cluster è sottoposto a un carico pesante, potrebbe mettere in coda le richieste API dall'interfaccia utente di Element. In rari casi, quando la risposta del sistema viene ritardata in modo significativo, ad esempio una connessione di rete lenta combinata con un cluster occupato, è possibile che l'utente venga disconnesso dall'interfaccia utente di Element se il sistema non risponde alle richieste API in coda in modo sufficientemente rapido. Se si viene reindirizzati alla schermata di disconnessione, è possibile effettuare nuovamente l'accesso dopo aver disperso qualsiasi richiesta iniziale di autenticazione del browser. Quando si torna alla pagina di panoramica, potrebbe essere richiesto di inserire le credenziali del cluster se non vengono salvate dal browser.

Icone nell'interfaccia degli elementi

L'interfaccia del software NetApp Element visualizza icone che rappresentano le azioni che è possibile intraprendere sulle risorse di sistema.

La seguente tabella fornisce un riferimento rapido:

Icona	Descrizione
	Azioni
	Backup in
	Clonare o copiare
	Eliminare o eliminare
	Modifica
	Filtro
	Abbinare

	Aggiornare
	Ripristinare
	Ripristina da
	Eseguire il rollback
	Snapshot

Fornire un feedback

È possibile migliorare l'interfaccia utente Web del software Element e risolvere eventuali problemi dell'interfaccia utente utilizzando il modulo di feedback accessibile dall'interfaccia utente.

1. Da qualsiasi pagina dell'interfaccia utente di Element, fare clic sul pulsante **Feedback**.
2. Inserire le informazioni pertinenti nei campi Summary (Riepilogo) e Description (Descrizione).
3. Allegare eventuali screenshot utili.
4. Immettere un nome e un indirizzo e-mail.
5. Selezionare la casella di controllo per includere i dati relativi all'ambiente corrente.
6. Fare clic su **Invia**.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire gli account

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi di un cluster. Quando si crea un volume, questo viene assegnato a un account specifico. È inoltre possibile gestire gli account amministratore del cluster per un sistema storage SolidFire.

- "Utilizzare gli account con CHAP"
- "Gestire gli account utente degli amministratori del cluster"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Utilizzare gli account con CHAP

Nei sistemi storage SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi di un cluster. Un account contiene l'autenticazione CHAP (Challenge-Handshake Authentication Protocol) richiesta per accedere ai volumi assegnati. Quando si crea un volume, questo viene assegnato a un account specifico.

A un account possono essere assegnati fino a duemila volumi, ma un volume può appartenere a un solo account.

Creare un account

È possibile creare un account per consentire l'accesso ai volumi.

Ogni nome account nel sistema deve essere univoco.

1. Selezionare **Gestione** > **account**.
2. Fare clic su **Create account** (Crea account).
3. Immettere un **Nome utente**.
4. Nella sezione **Impostazioni CHAP**, immettere le seguenti informazioni:

   Lasciare vuoti i campi delle credenziali per generare automaticamente una delle due password.

   - **Initiator Secret** per l'autenticazione della sessione del nodo CHAP.
   - **Target Secret** per l'autenticazione della sessione del nodo CHAP.
5. Fare clic su **Create account** (Crea account).

Visualizza i dettagli dell'account

È possibile visualizzare l'attività delle performance per i singoli account in un formato grafico.

Le informazioni del grafico forniscono informazioni di i/o e throughput per l'account. I livelli di attività medi e di picco sono indicati in incrementi di periodi di reporting di 10 secondi. Queste statistiche includono l'attività per tutti i volumi assegnati all'account.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni di un account.
3. Fare clic su **View Details** (Visualizza dettagli).

Di seguito sono riportati alcuni dettagli:

- **Status**: Lo stato dell'account. Valori possibili:
  - Attivo: Un account attivo.

    - Locked (bloccato): Un account bloccato.
    - Rimosso: Un account che è stato eliminato e rimosso.
- **Active Volumes** (volumi attivi): Il numero di volumi attivi assegnati all'account.
- **Compressione**: Il punteggio di efficienza della compressione per i volumi assegnati all'account.
- **Deduplica**: Il punteggio di efficienza della deduplica per i volumi assegnati all'account.
- **Thin Provisioning**: Il punteggio di efficienza del thin provisioning per i volumi assegnati all'account.
- **Efficienza complessiva**: Il punteggio di efficienza globale per i volumi assegnati all'account.

Modificare un account

È possibile modificare un account per modificare lo stato, i segreti CHAP o il nome dell'account.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettersi sempre dalle sessioni iSCSI che saranno interessate dalla modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato modifiche alle impostazioni dell'iniziatore e del cluster.

> I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni di un account.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. **Opzionale:** modificare il **Nome utente**.
5. **Opzionale:** fare clic sull'elenco a discesa **Stato** e selezionare un altro stato.

> Se si modifica lo stato su **Locked**, tutte le connessioni iSCSI all'account vengono terminate e l'account non è più accessibile. I volumi associati all'account vengono mantenuti; tuttavia, i volumi non sono rilevabili tramite iSCSI.

6. **Opzionale:** in **Impostazioni CHAP**, modificare le credenziali **Segreto iniziatore** e **Segreto di destinazione** utilizzate per l'autenticazione della sessione del nodo.

> Se non si modificano le credenziali **CHAP Settings**, queste rimangono invariate. Se i campi delle credenziali vengono vuoti, il sistema genera nuove password.

7. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un account

È possibile eliminare un account quando non è più necessario.

Eliminare e rimuovere tutti i volumi associati all'account prima di eliminarlo.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account creato durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare l'account associato.

1. Selezionare **Gestione** > **account**.
2. Fare clic sull'icona azioni dell'account che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire gli account utente degli amministratori del cluster

È possibile gestire gli account amministratore del cluster per un sistema storage SolidFire creando, eliminando e modificando gli account amministratore del cluster, modificando la password amministratore del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

Tipi di account amministratore del cluster di storage

Esistono due tipi di account amministratore in un cluster di storage che esegue il software NetApp Element: L'account primario dell'amministratore del cluster e un account dell'amministratore del cluster.

- **Account primario amministratore del cluster**

  Questo account amministratore viene creato al momento della creazione del cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo a un utente root in un sistema Linux. È possibile modificare la password per questo account amministratore.

- **Account amministratore del cluster**

  È possibile assegnare a un account amministratore del cluster un intervallo limitato di accesso amministrativo per eseguire attività specifiche all'interno di un cluster. Le credenziali assegnate a ciascun account amministratore del cluster vengono utilizzate per autenticare le richieste API ed Element UI all'interno del sistema di storage.

Per accedere ai nodi attivi di un cluster tramite l'interfaccia utente per nodo, è necessario un account amministratore locale (non LDAP). Le credenziali dell'account non sono richieste per accedere a un nodo che non fa ancora parte di un cluster.

Visualizzare i dettagli dell'amministratore del cluster

1. Per creare un account di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **utenti** > **amministratori cluster**.

2. Nella pagina Cluster Admins della scheda Users (utenti), è possibile visualizzare le seguenti informazioni.
   - **ID**: Numero sequenziale assegnato all'account dell'amministratore del cluster.
   - **Username**: Il nome assegnato all'account dell'amministratore del cluster al momento della creazione.
   - **Access**: Le autorizzazioni utente assegnate all'account utente. Valori possibili:
     - leggi
     - creazione di report
     - nodi
     - dischi
     - volumi
     - account
     - ClusterAdmins
     - amministratore

     Tutte le autorizzazioni sono disponibili per il tipo di accesso amministratore.
   - **Type**: Il tipo di amministratore del cluster. Valori possibili:
     - Cluster
     - LDAP
   - **Attributes**: Se l'account amministratore del cluster è stato creato utilizzando l'API Element, questa colonna mostra tutte le coppie nome-valore impostate utilizzando tale metodo.

     Vedere "Riferimento API software NetApp Element".

Creare un account amministratore del cluster

È possibile creare nuovi account amministratore del cluster con autorizzazioni per consentire o limitare l'accesso a specifiche aree del sistema di storage. Quando si impostano le autorizzazioni dell'account amministratore del cluster, il sistema concede i diritti di sola lettura per le autorizzazioni non assegnate all'amministratore del cluster.

Se si desidera creare un account amministratore del cluster LDAP, assicurarsi che LDAP sia configurato sul cluster prima di iniziare.

"Abilitare l'autenticazione LDAP con l'interfaccia utente Element"

In seguito, è possibile modificare i privilegi degli account amministratore del cluster per report, nodi, dischi, volumi, account, e a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

È inoltre possibile rimuovere in seguito qualsiasi account utente amministratore del cluster creato da un amministratore di sistema. Non è possibile rimuovere l'account amministratore del cluster primario creato al momento della creazione del cluster.

1. Per creare un account di amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
   a. Fare clic su **utenti** > **amministratori cluster**.

b. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
c. Selezionare il tipo di utente **Cluster**.
d. Immettere un nome utente e una password per l'account e confermare la password.
e. Selezionare le autorizzazioni utente da applicare all'account.
f. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.
g. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

2. Per creare un account amministratore del cluster nella directory LDAP, eseguire le seguenti operazioni:

a. Fare clic su **Cluster** > **LDAP**.
b. Assicurarsi che l'autenticazione LDAP sia attivata.
c. Fare clic su **Test User Authentication** (verifica autenticazione utente) e copiare il nome distinto visualizzato per l'utente o per uno dei gruppi di cui l'utente è membro in modo da poterlo incollare in un secondo momento.
d. Fare clic su **utenti** > **amministratori cluster**.
e. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).
f. Selezionare il tipo di utente LDAP.
g. Nel campo Distinguished Name (Nome distinto), seguire l'esempio nella casella di testo per immettere un nome distinto completo per l'utente o il gruppo. In alternativa, incollarlo dal nome distinto precedentemente copiato.

   Se il nome distinto fa parte di un gruppo, tutti gli utenti che fanno parte di tale gruppo sul server LDAP disporranno delle autorizzazioni per questo account admin.

Per aggiungere utenti o gruppi amministratori cluster LDAP, il formato generale del nome utente è "LDAP:<Full Distinguished Name>".

a. Selezionare le autorizzazioni utente da applicare all'account.
b. Selezionare la casella di controllo per accettare il Contratto di licenza con l'utente finale.
c. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

Modificare le autorizzazioni di amministratore del cluster

È possibile modificare i privilegi dell'account amministratore del cluster per report, nodi, dischi, volumi, account, e a livello di cluster. Quando si abilita un'autorizzazione, il sistema assegna l'accesso in scrittura per quel livello. Il sistema concede all'utente amministratore l'accesso in sola lettura per i livelli non selezionati.

1. Fare clic su **utenti** > **amministratori cluster**.
2. Fare clic sull'icona Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Selezionare le autorizzazioni utente da applicare all'account.
5. Fare clic su **Save Changes** (Salva modifiche).

Modificare le password per gli account amministratore del cluster

È possibile utilizzare l'interfaccia utente Element per modificare le password dell'amministratore del cluster.

1. Fare clic su **utenti** > **amministratori cluster**.
2. Fare clic sull'icona Actions (azioni) dell'amministratore del cluster che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Nel campo Change Password (Modifica password), immettere una nuova password e confermarla.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- "Abilitare l'autenticazione LDAP con l'interfaccia utente Element"
- "Disattiva LDAP"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire LDAP

È possibile impostare il protocollo LDAP (Lightweight Directory Access Protocol) per abilitare la funzionalità di accesso sicura e basata su directory allo storage SolidFire. È possibile configurare LDAP a livello di cluster e autorizzare utenti e gruppi LDAP.

La gestione di LDAP implica la configurazione dell'autenticazione LDAP su un cluster SolidFire utilizzando un ambiente Microsoft Active Directory esistente e il test della configurazione.

È possibile utilizzare indirizzi IPv4 e IPv6.

L'abilitazione di LDAP prevede le seguenti procedure di alto livello, descritte in dettaglio:

1. **Completare la procedura di preconfigurazione per il supporto LDAP**. Verificare di disporre di tutti i dettagli necessari per configurare l'autenticazione LDAP.
2. **Attiva autenticazione LDAP**. Utilizzare l'interfaccia utente Element o l'API Element.
3. **Convalidare la configurazione LDAP**. Facoltativamente, verificare che il cluster sia configurato con i valori corretti eseguendo il metodo GetLdapConfiguration API o controllando la configurazione LCAP utilizzando l'interfaccia utente Element.
4. **Verificare l'autenticazione LDAP** (con il `readonly` utente). Verificare che la configurazione LDAP sia corretta eseguendo il metodo TestLdapAuthentication API o utilizzando l'interfaccia utente Element. Per questo test iniziale, utilizzare il nome utente "sAMAccountName" di `readonly` utente. In questo modo, il cluster viene convalidato per verificare che sia configurato correttamente per l'autenticazione LDAP `readonly` le credenziali e l'accesso sono corretti. Se questo passaggio non riesce, ripetere i passi da 1 a 3.
5. **Verificare l'autenticazione LDAP** (con un account utente che si desidera aggiungere). Ripetere il setp 4 con un account utente che si desidera aggiungere come amministratore del cluster di elementi. Copiare il `distinguished` Nome (DN) o l'utente (o il gruppo). Questo DN verrà utilizzato nella fase 6.
6. **Aggiungere l'amministratore del cluster LDAP** (copiare e incollare il DN dalla fase di autenticazione LDAP di prova). Utilizzando l'interfaccia utente Element o il metodo API AddLdapClusterAdmin, creare un nuovo utente amministratore del cluster con il livello di accesso appropriato. Per il nome utente, incollare il DN completo copiato al punto 5. In questo modo si garantisce che il DN sia formattato correttamente.
7. **Verificare l'accesso dell'amministratore del cluster**. Accedere al cluster utilizzando l'utente amministratore del cluster LDAP appena creato. Se è stato aggiunto un gruppo LDAP, è possibile

effettuare l'accesso come qualsiasi utente del gruppo.

Completare la procedura di preconfigurazione per il supporto LDAP

Prima di attivare il supporto LDAP in Element, è necessario configurare un server Windows Active Directory ed eseguire altre attività di preconfigurazione.

Fasi

1. Configurare un server Windows Active Directory.
2. **Opzionale:** attiva il supporto LDAPS.
3. Creare utenti e gruppi.
4. Creare un account di servizio di sola lettura (ad esempio "sfreadonly") da utilizzare per la ricerca nella directory LDAP.

Abilitare l'autenticazione LDAP con l'interfaccia utente Element

È possibile configurare l'integrazione del sistema di storage con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso al sistema storage per gli utenti.

È possibile configurare LDAP con l'interfaccia utente Element o l'API Element. Questa procedura descrive come configurare LDAP utilizzando l'interfaccia utente Element.

Questo esempio mostra come configurare l'autenticazione LDAP su SolidFire e in uso `SearchAndBind` come tipo di autenticazione. Nell'esempio viene utilizzato un singolo Windows Server 2012 R2 Active Directory Server.

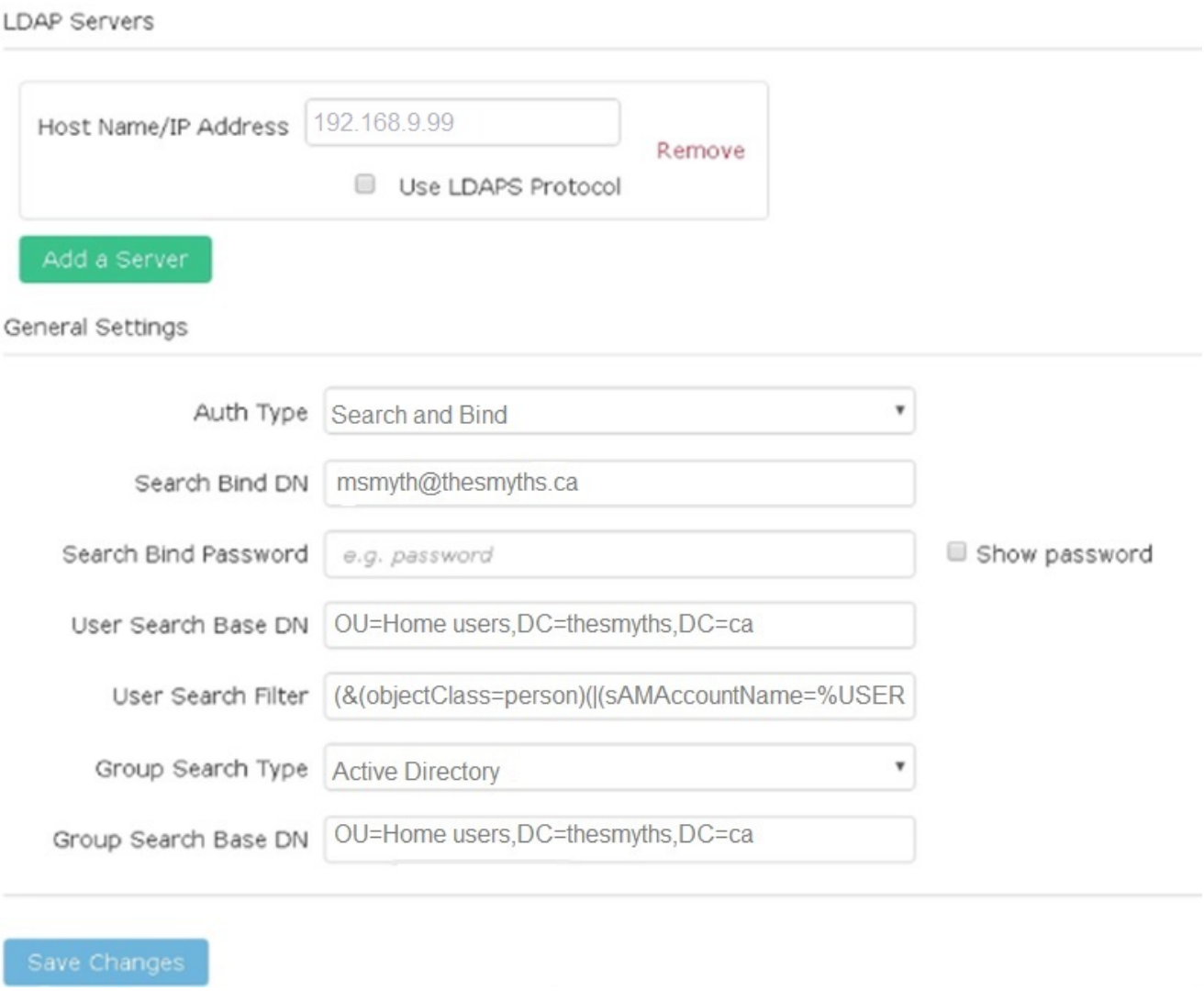
Fasi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **Sì** per attivare l'autenticazione LDAP.
3. Fare clic su **Aggiungi un server**.
4. Inserire il campo **host Name/IP Address** (Nome host/Indirizzo IP).

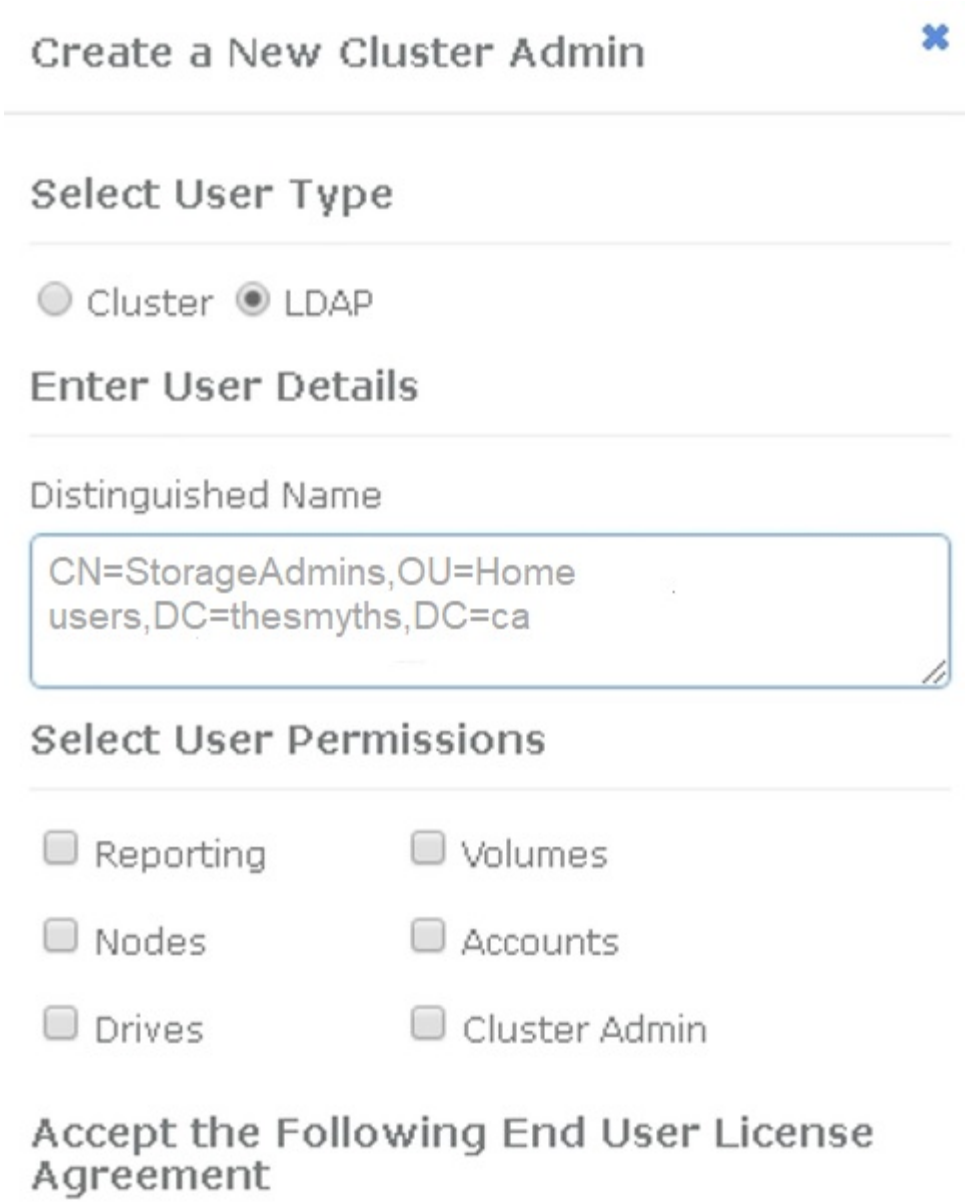
   È inoltre possibile inserire un numero di porta personalizzato opzionale.

   Ad esempio, per aggiungere un numero di porta personalizzato, immettere <host name or ip address>:<port number>

5. **Opzionale:** selezionare **Usa protocollo LDAPS**.
6. Inserire le informazioni richieste in **Impostazioni generali**.



7. Fare clic su **Enable LDAP** (attiva LDAP).
8. Fare clic su **Test User Authentication** (verifica autenticazione utente) per verificare l'accesso al server per un utente.
9. Copiare il nome distinto e le informazioni del gruppo di utenti che verranno visualizzate in seguito per la creazione degli amministratori del cluster.
10. Fare clic su **Save Changes** (Salva modifiche) per salvare le nuove impostazioni.
11. Per creare un utente in questo gruppo in modo che chiunque possa effettuare l'accesso, attenersi alla seguente procedura:
    a. Fare clic su **utente** > **Visualizza**.



b. Per il nuovo utente, fare clic su **LDAP** per tipo utente e incollare il gruppo copiato nel campo Nome distinto.
c. Selezionare le autorizzazioni, in genere tutte le autorizzazioni.
d. Scorrere verso il basso fino al Contratto di licenza con l'utente finale e fare clic su **Accetto**.
e. Fare clic su **Create Cluster Admin** (Crea amministratore cluster).

   Ora si dispone di un utente con il valore di un gruppo Active Directory.

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Abilitare l'autenticazione LDAP con l'API Element

È possibile configurare l'integrazione del sistema di storage con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso al sistema storage per gli utenti.

È possibile configurare LDAP con l'interfaccia utente Element o l'API Element. Questa procedura descrive

come configurare LDAP utilizzando l'API Element.

Per sfruttare l'autenticazione LDAP su un cluster SolidFire, attivare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.

Fasi

1. Attivare prima l'autenticazione LDAP sul cluster utilizzando `EnableLdapAuthentication` Metodo API.
2. Inserire le informazioni richieste.

```
{
     "method":"EnableLdapAuthentication",
     "params":{
          "authType": "SearchAndBind",
          "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
          "groupSearchType": "ActiveDirectory",
          "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
          "searchBindPassword": "ReadOnlyPW",
          "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net ",
          "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
          "serverURIs": [
               "ldap://172.27.1.189",
          [
     },
  "id":"1"
}
```

3. Modificare i valori dei seguenti parametri:

Parametri utilizzati	Descrizione
AuthType: SearchAndBind	Indica che il cluster utilizzerà l'account di servizio di sola lettura per cercare prima l'utente autenticato e successivamente associare tale utente, se trovato e autenticato.
GroupSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca dei gruppi. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.

Parametri utilizzati	Descrizione
UserSearchBaseDN: dc=prodtest,DC=solidfire,DC=net	Specifica la posizione nella struttura LDAP per avviare la ricerca degli utenti. Per questo esempio, abbiamo utilizzato la radice del nostro albero. Se la struttura LDAP è molto grande, potrebbe essere necessario impostarla su un sottostruttura più granulare per ridurre i tempi di ricerca.
GroupSearchType: ActiveDirectory	Utilizza il server Windows Active Directory come server LDAP.

`userSearchFilter: "(&(objectClass=person)(sAMAccountName=%USERNAME%))"`
 	
Per utilizzare userPrincipalName (indirizzo e-mail per l'accesso), è possibile modificare userSearchFilter in:
 	
`"(&(objectClass=person)(userPrincipalName=%USERNAME%))"`
 	
In alternativa, per eseguire ricerche in userPrincipalName e sAMAccountName, è possibile utilizzare il seguente userSearchFilter:
 	
`"(&(objectClass=person)(`
	(SAMAccountName=%NOME UTENTE%)(userPrincipalName=%NOME UTENTE%))" ----

Utilizza sAMAccountName come nome utente per accedere al cluster SolidFire. Queste impostazioni indicano a LDAP di cercare il nome utente specificato durante l'accesso nell'attributo sAMAccountName e di limitare la ricerca alle voci che hanno "Person" come valore nell'attributo objectClass.	SearchBindDN
Si tratta del nome distinto dell'utente di sola lettura che verrà utilizzato per cercare nella directory LDAP. Per Active directory è generalmente più semplice utilizzare userPrincipalName (formato indirizzo email) per l'utente.	SearchBindPassword

Per verificare questo, disconnettersi dall'interfaccia utente di Element e accedere nuovamente come utente di quel gruppo.

Visualizza i dettagli LDAP

Visualizzare le informazioni LDAP nella pagina LDAP della scheda Cluster.

Per visualizzare queste impostazioni di configurazione LDAP, è necessario attivare LDAP.

1. Per visualizzare i dettagli LDAP con l'interfaccia utente Element, fare clic su **Cluster** > **LDAP**.
   - **Host Name/IP Address** (Nome host/Indirizzo IP): Indirizzo di un server di directory LDAP o LDAPS.
   - **Auth Type**: Il metodo di autenticazione dell'utente. Valori possibili:
     - Binding diretto
     - Ricerca e binding
   - **Search Bind DN**: DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP dell'utente (richiede l'accesso a livello di bind alla directory LDAP).
   - **Search Bind Password**: Password utilizzata per autenticare l'accesso al server LDAP.
   - **User Search base DN** (DN base ricerca utente): Il DN di base della struttura utilizzata per avviare la ricerca dell'utente. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
   - **User Search Filter** (filtro di ricerca utente): Immettere quanto segue utilizzando il nome di dominio:

     ```
     (&(objectClass=person)(|(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%)))
     ```

   - **Group Search Type** (tipo ricerca gruppo): Tipo di ricerca che controlla il filtro di ricerca gruppo predefinito utilizzato. Valori possibili:
     - Active Directory: Appartenenza nidificata a tutti i gruppi LDAP di un utente.
     - No Groups (Nessun gruppo): Nessun supporto di gruppo.
     - DN membro: Gruppi di membri in stile DN (livello singolo).
   - **Group Search base DN**: Il DN di base della struttura utilizzata per avviare la ricerca di gruppo. Il sistema esegue la ricerca nella sottostruttura dalla posizione specificata.
   - **Test User Authentication** (verifica autenticazione utente): Una volta configurato LDAP, utilizzare questa opzione per verificare l'autenticazione del nome utente e della password per il server LDAP. Immettere un account già esistente per eseguire il test. Vengono visualizzate le informazioni distinte relative al nome e al gruppo di utenti, che è possibile copiare per l'utilizzo successivo durante la creazione degli amministratori del cluster.

Verificare la configurazione LDAP

Dopo aver configurato LDAP, è necessario testarlo utilizzando l'interfaccia utente Element o l'API Element `TestLdapAuthentication` metodo.

Fasi

1. Per verificare la configurazione LDAP con l'interfaccia utente Element, procedere come segue:
   a. Fare clic su **Cluster** > **LDAP**.
   b. Fare clic su **Test autenticazione LDAP**.
   c. Risolvere eventuali problemi utilizzando le informazioni riportate nella tabella seguente:

Messaggio di errore	Descrizione
`xLDAPUserNotFound`	• L'utente sottoposto a test non è stato trovato nella configurazione `userSearchBaseDN` sottostruttura. • Il `userSearchFilter` non è configurato correttamente.
`xLDAPBindFailed (Error: Invalid credentials)`	• Il nome utente sottoposto a test è un utente LDAP valido, ma la password fornita non è corretta. • Il nome utente sottoposto a test è un utente LDAP valido, ma l'account è attualmente disattivato.
`xLDAPSearchBindFailed (Error: Can't contact LDAP server)`	L'URI del server LDAP non è corretto.
`xLDAPSearchBindFailed (Error: Invalid credentials)`	Il nome utente o la password di sola lettura non sono configurati correttamente.
`xLDAPSearchFailed (Error: No such object)`	Il `userSearchBaseDN` Non è una posizione valida all'interno della struttura LDAP.
`xLDAPSearchFailed (Error: Referral)`	• Il `userSearchBaseDN` Non è una posizione valida all'interno della struttura LDAP. • Il `userSearchBaseDN` e. `groupSearchBaseDN` Si trovano in un'unità organizzativa nidificata. Ciò può causare problemi di autorizzazione. La soluzione è includere l'unità organizzativa nelle voci DN di base dell'utente e del gruppo, ad esempio: `ou=storage, cn=company, cn=com`)

2. Per verificare la configurazione LDAP con l'API Element, procedere come indicato di seguito:
   a. Chiamare il metodo TestLdapAuthentication.

```
{
  "method":"TestLdapAuthentication",
     "params":{
        "username":"admin1",
        "password":"admin1PASS
      },
      "id": 1
}
```

b. Esaminare i risultati. Se la chiamata API ha esito positivo, i risultati includono il nome distinto dell'utente specificato e un elenco di gruppi a cui l'utente è membro.

```
{
"id": 1
     "result": {
         "groups": [

"CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
         ],
         "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
     }
}
```

Disattiva LDAP

È possibile disattivare l'integrazione LDAP utilizzando l'interfaccia utente Element.

Prima di iniziare, prendere nota di tutte le impostazioni di configurazione, poiché la disattivazione di LDAP cancella tutte le impostazioni.

Fasi

1. Fare clic su **Cluster** > **LDAP**.
2. Fare clic su **No**.
3. Fare clic su **Disable LDAP** (Disattiva LDAP).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire il sistema

È possibile gestire il sistema nell'interfaccia utente di Element. Ciò include l'abilitazione dell'autenticazione a più fattori, la gestione delle impostazioni del cluster, il supporto degli

standard FIPS (Federal Information Processing Standards) e l'utilizzo della gestione esterna delle chiavi.

- "Abilitare l'autenticazione a più fattori"
- "Configurare le impostazioni del cluster"
- "Creare un cluster che supporti i dischi FIPS"
- "Inizia a utilizzare la gestione esterna delle chiavi"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Abilitare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) utilizza un provider di identità (IdP) di terze parti tramite il linguaggio SAML (Security Assertion Markup Language) per gestire le sessioni utente. MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, come password e SMS, password e messaggi di posta elettronica.

Impostare l'autenticazione a più fattori

È possibile utilizzare questi passaggi di base tramite l'API Element per configurare il cluster in modo che utilizzi l'autenticazione a più fattori.

I dettagli di ciascun metodo API sono disponibili nella "Riferimento API dell'elemento".

1. Creare una nuova configurazione IdP (Identity Provider) di terze parti per il cluster chiamando il seguente metodo API e passando i metadati IdP in formato JSON: `CreateIdpConfiguration`

   I metadati IDP, in formato testo normale, vengono recuperati da IdP di terze parti. Questi metadati devono essere validati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni del formatter JSON, ad esempio:https://freeformatter.com/json-escape.html.

2. Recuperare i metadati del cluster, tramite spMetadataUrl, da copiare nell'IdP di terze parti chiamando il seguente metodo API: `ListIdpConfigurations`

   SpMetadataUrl è un URL utilizzato per recuperare i metadati del provider di servizi dal cluster per IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull'IdP di terze parti in modo che includa l'attributo "NameID" per identificare in modo univoco un utente per la registrazione dell'audit e per il corretto funzionamento della disconnessione singola.
4. Creare uno o più account utente amministratore del cluster autenticati da un IdP di terze parti per l'autorizzazione chiamando il seguente metodo API:`AddIdpClusterAdmin`

   Il nome utente per l'amministratore del cluster IdP deve corrispondere alla mappatura nome/valore attributo SAML per l'effetto desiderato, come mostrato negli esempi seguenti:

- Email=bob@company.com — dove IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
- Group=cluster-Administrator - dove IdP è configurato per rilasciare una proprietà di gruppo in cui tutti gli utenti devono avere accesso. Tenere presente che l'associazione nome attributo/valore SAML è sensibile alla distinzione tra maiuscole e minuscole per motivi di sicurezza.

5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Ulteriori informazioni per l'autenticazione a più fattori

È necessario conoscere le seguenti avvertenze relative all'autenticazione a più fattori.

- Per aggiornare i certificati IdP non più validi, è necessario utilizzare un utente amministratore non IdP per chiamare il seguente metodo API: `UpdateIdpConfiguration`
- MFA non è compatibile con i certificati di lunghezza inferiore a 2048 bit. Per impostazione predefinita, nel cluster viene creato un certificato SSL a 2048 bit. Evitare di impostare un certificato di dimensioni inferiori quando si chiama il metodo API: `SetSSLCertificate`

> Se il cluster utilizza un certificato precedente all'aggiornamento a meno di 2048 bit, il certificato del cluster deve essere aggiornato con un certificato a 2048 bit o superiore dopo l'aggiornamento all'elemento 12.0 o successivo.

- Gli utenti amministratori IDP non possono essere utilizzati per effettuare chiamate API direttamente (ad esempio, tramite SDK o Postman) o per altre integrazioni (ad esempio, OpenStack Cinder o vCenter Plug-in). Aggiungere utenti amministratori cluster LDAP o utenti amministratori cluster locali se si desidera creare utenti con queste funzionalità.

Trova ulteriori informazioni

- "Gestione dello storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare le impostazioni del cluster

È possibile visualizzare e modificare le impostazioni a livello di cluster ed eseguire attività specifiche del cluster dalla scheda Cluster dell'interfaccia utente di Element.

È possibile configurare impostazioni come la soglia di fullness del cluster, l'accesso al supporto, la crittografia a riposo, i volumi virtuali, SnapMirror, E NTP broadcast client.

Opzioni

- Lavorare con volumi virtuali
- Utilizzare la replica SnapMirror tra cluster Element e ONTAP
- Impostare la soglia completa del cluster

- Abilitare e disabilitare l'accesso al supporto
- "Come vengono calcolate le soglie blockSpace per l'elemento"
- Attivare e disattivare la crittografia per un cluster
- Gestire il banner Termini di utilizzo
- Configurare i server Network Time Protocol per il cluster da interrogare
- Gestire SNMP
- Gestire i dischi
- Gestire i nodi
- Gestire le reti virtuali
- Visualizza i dettagli delle porte Fibre Channel

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Attivare e disattivare la crittografia a riposo per un cluster

Con i cluster SolidFire, è possibile crittografare tutti i dati inattivi memorizzati sui dischi del cluster. È possibile abilitare la protezione a livello di cluster dei dischi con crittografia automatica (SED) utilizzando entrambi "crittografia basata su hardware o software a riposo".

È possibile attivare la crittografia hardware a riposo utilizzando l'interfaccia utente o l'API Element. L'attivazione della funzione di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile attivare la crittografia software a riposo utilizzando solo l'API Element.

La crittografia basata su hardware a riposo non è attivata per impostazione predefinita durante la creazione del cluster e può essere attivata e disattivata dall'interfaccia utente di Element.

> Per i cluster di storage all-flash SolidFire, la crittografia software a riposo deve essere attivata durante la creazione del cluster e non può essere disattivata dopo la creazione del cluster.

Di cosa hai bisogno

- Si dispone dei privilegi di amministratore del cluster per attivare o modificare le impostazioni di crittografia.
- Per la crittografia basata su hardware a riposo, è stato garantito che il cluster sia in buono stato prima di modificare le impostazioni di crittografia.
- Se si disattiva la crittografia, due nodi devono partecipare a un cluster per accedere alla chiave e disattivare la crittografia su un disco.

Controllare la crittografia nello stato di riposo

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare "GetClusterInfo" metodo. È possibile utilizzare "GetSoftwareEncryptionAtRestInfo" metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi.

La dashboard dell'interfaccia utente del software Element all'indirizzo `https://<MVIP>/` attualmente mostra solo la crittografia in stato di riposo per la crittografia basata su hardware.

Opzioni

- Abilitare la crittografia basata su hardware a riposo
- Abilitare la crittografia basata su software a riposo
- Disattiva la crittografia basata su hardware a riposo

Abilitare la crittografia basata su hardware a riposo

Per attivare la crittografia a riposo utilizzando una configurazione di gestione delle chiavi esterna, è necessario attivare la crittografia a riposo tramite "API". L'abilitazione mediante il pulsante Element UI esistente tornerà a utilizzare chiavi generate internamente.

1. Dall'interfaccia utente di Element, selezionare **Cluster** > **Settings**.
2. Selezionare **Enable Encryption at REST (attiva crittografia a riposo)**.

Abilitare la crittografia basata su software a riposo

La crittografia software a riposo non può essere disattivata dopo che è stata attivata sul cluster.

1. Durante la creazione del cluster, eseguire "creare il metodo del cluster" con `enableSoftwareEncryptionAtRest` impostare su `true`.

Disattiva la crittografia basata su hardware a riposo

1. Dall'interfaccia utente di Element, selezionare **Cluster** > **Settings**.
2. Selezionare **Disattiva crittografia a riposo**.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Impostare la soglia completa del cluster

È possibile modificare il livello con cui il sistema genera un avviso di riempimento del cluster a blocchi seguendo la procedura riportata di seguito. Inoltre, è possibile utilizzare il metodo dell'API ModifyClusterFullThreshold per modificare il livello con cui il sistema genera un avviso di blocco o metadati.

Di cosa hai bisogno

È necessario disporre dei privilegi di amministratore del cluster.

Fasi

1. Fare clic su **Cluster** > **Settings**.
2. Nella sezione Cluster Full Settings (Impostazioni cluster complete), inserire una percentuale in **Raise a warning alert when _% Capacity remains before Helix not recovery from a node failure** (Invia un avviso quando la capacità del _% rimane prima che Helix non possa

3. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

"Come vengono calcolate le soglie blockSpace per l'elemento"

Abilitare e disabilitare l'accesso al supporto

È possibile abilitare l'accesso al supporto per consentire temporaneamente al personale di supporto NetApp di accedere ai nodi di storage tramite SSH per la risoluzione dei problemi.

Per modificare l'accesso al supporto, è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **Cluster** > **Settings**.
2. Nella sezione Enable / Disable Support Access (attiva/Disattiva accesso al supporto), immettere la durata (in ore) per la quale si desidera consentire l'accesso al supporto.
3. Fare clic su **Enable Support Access** (attiva accesso supporto).
4. **Opzionale:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestire il banner Termini di utilizzo

È possibile attivare, modificare o configurare un banner contenente un messaggio per l'utente.

Opzioni

Attivare il banner Termini di utilizzo
Modificare il banner Termini di utilizzo
Disattiva il banner Termini di utilizzo

Attivare il banner Termini di utilizzo

È possibile attivare un banner Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente fa clic sul banner, viene visualizzata una finestra di dialogo contenente il messaggio configurato per il cluster. Il banner può essere ignorato in qualsiasi momento.

Per attivare la funzionalità Termini di utilizzo, è necessario disporre dei privilegi di amministratore del cluster.

1. Fare clic su **utenti** > **Termini di utilizzo**.
2. Nel modulo **Termini di utilizzo**, inserire il testo da visualizzare nella finestra di dialogo Termini di utilizzo.

   Non superare i 4096 caratteri.

3. Fare clic su **Enable** (attiva).

Modificare il banner Termini di utilizzo

Puoi modificare il testo visualizzato dall'utente quando seleziona il banner di accesso Termini di utilizzo.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.

- Assicurarsi che la funzione Termini di utilizzo sia attivata.

Fasi

1. Fare clic su **utenti** > **Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modificare il testo che si desidera visualizzare.

   Non superare i 4096 caratteri.

3. Fare clic su **Save Changes** (Salva modifiche).

Disattiva il banner Termini di utilizzo

È possibile disattivare il banner Termini di utilizzo. Con il banner disattivato, non viene più richiesto all'utente di accettare i termini di utilizzo quando si utilizza l'interfaccia utente di Element.

Di cosa hai bisogno

- Per configurare le Condizioni d'uso, è necessario disporre dei privilegi di amministratore del cluster.
- Assicurarsi che le condizioni d'uso siano attivate.

Fasi

1. Fare clic su **utenti** > **Termini di utilizzo**.
2. Fare clic su **Disable** (Disattiva).

Impostare Network Time Protocol

L'impostazione del protocollo NTP (Network Time Protocol) può essere eseguita in due modi: Istruire ciascun nodo di un cluster a rimanere in attesa delle trasmissioni o richiedere a ciascun nodo di eseguire una query su un server NTP per gli aggiornamenti.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno deve far parte della configurazione iniziale del cluster.

Configurare i server Network Time Protocol per il cluster da interrogare

È possibile richiedere a ciascun nodo di un cluster di eseguire query su un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede informazioni NTP.

Configurare NTP sul cluster in modo che punti a un server NTP locale. È possibile utilizzare l'indirizzo IP o il nome host FQDN. Il server NTP predefinito al momento della creazione del cluster è impostato su us.pool.ntp.org; tuttavia, non è sempre possibile stabilire una connessione a questo sito a seconda della posizione fisica del cluster SolidFire.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di storage siano state configurate e operative. A tale scopo, configurare i server DNS su ogni nodo di storage e assicurarsi che le porte siano aperte consultando la pagina requisiti della porta di rete.

È possibile inserire fino a cinque server NTP diversi.

È possibile utilizzare indirizzi IPv4 e IPv6.

Di cosa hai bisogno

Per configurare questa impostazione, è necessario disporre dei privilegi di amministratore del cluster.

Fasi

1. Configurare un elenco di IP e/o FQDN nelle impostazioni del server.
2. Assicurarsi che il DNS sia impostato correttamente sui nodi.
3. Fare clic su **Cluster** > **Settings**.
4. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **No**, che utilizza la configurazione NTP standard.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Configurare il cluster in modo che sia in attesa di trasmissioni NTP

Utilizzando la modalità di trasmissione, è possibile impostare ciascun nodo di un cluster in modo che ascolti sulla rete i messaggi di trasmissione NTP (Network Time Protocol) provenienti da un determinato server.

Di cosa hai bisogno

- Per configurare questa impostazione, è necessario disporre dei privilegi di amministratore del cluster.
- È necessario configurare un server NTP sulla rete come server di trasmissione.

Fasi

1. Fare clic su **Cluster** > **Settings**.
2. Inserire il server NTP o i server che utilizzano la modalità di trasmissione nell'elenco dei server.
3. In Network Time Protocol Settings (Impostazioni protocollo ora di rete), selezionare **Yes** (Sì) per utilizzare un client di trasmissione.
4. Per impostare il client di trasmissione, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire SNMP

È possibile configurare il protocollo SNMP (Simple Network Management Protocol) nel cluster.

È possibile selezionare un richiedente SNMP, selezionare la versione di SNMP da utilizzare, identificare l'utente del modello di protezione basato sull'utente SNMP e configurare i trap per monitorare il cluster

SolidFire. È inoltre possibile visualizzare e accedere ai file della base di informazioni di gestione.

È possibile utilizzare indirizzi IPv4 e IPv6.

Dettagli SNMP

Nella pagina SNMP della scheda Cluster, è possibile visualizzare le seguenti informazioni.

- **MIB SNMP**

  I file MIB disponibili per la visualizzazione o il download.

- **Impostazioni SNMP generali**

  È possibile attivare o disattivare SNMP. Dopo aver attivato SNMP, è possibile scegliere la versione da utilizzare. Se si utilizza la versione 2, è possibile aggiungere i requestori e, se si utilizza la versione 3, è possibile configurare gli utenti USM.

- **SNMP Trap Settings** (Impostazioni trap SNMP)

  È possibile identificare le trap che si desidera acquisire. È possibile impostare l'host, la porta e la stringa di comunità per ciascun destinatario del trap.

Configurare un richiedente SNMP

Quando SNMP versione 2 è attivato, è possibile attivare o disattivare un richiedente e configurare i requestori per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster › SNMP**.
2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 2** (versione 2).
4. Nella sezione **Requestori**, inserire le informazioni **stringa di comunità** e **rete**.

   Per impostazione predefinita, la stringa di comunità è pubblica e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Opzionale:** per aggiungere un altro richiedente, fare clic su **Aggiungi richiedente** e immettere le informazioni **stringa di comunità** e **rete**.
6. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- Configurare i trap SNMP
- Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

Configurare un utente SNMP USM

Quando si attiva SNMP versione 3, è necessario configurare un utente USM per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster** > **SNMP**.
2. In **General SNMP Settings** (Impostazioni SNMP generali), fare clic su **Yes** (Sì) per attivare SNMP.
3. Dall'elenco **Version** (versione), selezionare **Version 3** (versione 3).
4. Nella sezione **utenti USM**, immettere il nome, la password e la passphrase.
5. **Opzionale:** per aggiungere un altro utente USM, fare clic su **Aggiungi utente USM** e inserire il nome, la password e la passphrase.
6. Fare clic su **Save Changes** (Salva modifiche).

Configurare i trap SNMP

Gli amministratori di sistema possono utilizzare i trap SNMP, definiti anche notifiche, per monitorare lo stato del cluster SolidFire.

Quando i trap SNMP sono attivati, il cluster SolidFire genera trap associati alle voci del registro eventi e agli avvisi di sistema. Per ricevere notifiche SNMP, è necessario scegliere i trap da generare e identificare i destinatari delle informazioni trap. Per impostazione predefinita, non viene generato alcun trap.

1. Fare clic su **Cluster** > **SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
   - Trap di guasti del cluster
   - Trap di guasti risolti nel cluster
   - Trap di eventi del cluster
3. Nella sezione **destinatari trap**, immettere le informazioni relative a host, porta e community string per un destinatario.
4. **Opzionale**: Per aggiungere un altro destinatario trap, fare clic su **Aggiungi destinatario trap** e immettere le informazioni relative a host, porta e stringa di comunità.
5. Fare clic su **Save Changes** (Salva modifiche).

Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione

È possibile visualizzare e scaricare i file MIB (Management Information base) utilizzati per definire ciascuno degli oggetti gestiti. La funzionalità SNMP supporta l'accesso in sola lettura agli oggetti definiti in SolidFire-StorageCluster-MIB.

I dati statistici forniti nel MIB mostrano l'attività del sistema per quanto segue:

- Statistiche del cluster
- Statistiche dei volumi
- Volumi per statistiche account
- Statistiche dei nodi
- Altri dati, ad esempio report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente gli access point di livello superiore (OID) per i prodotti SF-Series.

Fasi

1. Fare clic su **Cluster** > **SNMP**.
2. In **MIB SNMP**, fare clic sul file MIB che si desidera scaricare.
3. Nella finestra di download risultante, aprire o salvare il file MIB.

Gestire i dischi

Ogni nodo contiene uno o più dischi fisici utilizzati per memorizzare una parte dei dati per il cluster. Il cluster utilizza la capacità e le prestazioni del disco dopo che il disco è stato aggiunto correttamente a un cluster. È possibile utilizzare l'interfaccia utente Element per gestire i dischi.

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Dettagli sui dischi

La pagina Drives (unità) della scheda Cluster (cluster) fornisce un elenco dei dischi attivi nel cluster. È possibile filtrare la pagina selezionando dalle schede attivo, disponibile, Rimozione, cancellazione e non riuscito.

Quando si inizializza per la prima volta un cluster, l'elenco delle unità attive è vuoto. È possibile aggiungere dischi non assegnati a un cluster ed elencati nella scheda Available (disponibili) dopo la creazione di un nuovo cluster SolidFire.

I seguenti elementi vengono visualizzati nell'elenco dei dischi attivi.

- **ID unità**

  Il numero sequenziale assegnato al disco.

- **ID nodo**

  Il numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

  Il nome del nodo che ospita l'unità.

- **Slot**

  Il numero dello slot in cui si trova fisicamente l'unità.

- **Capacità**

  Le dimensioni del disco, in GB.

- **Seriale**

  Il numero di serie del disco.

- **Usura residua**

  L'indicatore del livello di usura.

  Il sistema storage indica la quantità approssimativa di usura disponibile su ogni disco a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un disco che ha consumato il 5% dei cicli di scrittura e cancellazione progettati riporta il 95% di usura rimanente. Il sistema non aggiorna automaticamente le informazioni sull'usura del disco; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

  Il tipo di disco. Il tipo può essere blocco o metadati.

Gestire i nodi

È possibile gestire lo storage SolidFire e i nodi Fibre Channel dalla pagina nodi della scheda cluster.

Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato un guasto appropriato del cluster.

Trova ulteriori informazioni

Aggiungere un nodo a un cluster

Aggiungere un nodo a un cluster

È possibile aggiungere nodi a un cluster quando è necessario più storage o dopo la creazione del cluster. I nodi richiedono la configurazione iniziale quando vengono accesi per la prima volta. Una volta configurato, il nodo viene visualizzato nell'elenco dei nodi in sospeso ed è possibile aggiungerlo a un cluster.

La versione software di ciascun nodo di un cluster deve essere compatibile. Quando si aggiunge un nodo a un cluster, il cluster installa la versione del software NetApp Element sul nuovo nodo in base alle necessità.

È possibile aggiungere nodi di capacità inferiore o superiore a un cluster esistente. È possibile aggiungere capacità di nodi maggiori a un cluster per consentire la crescita della capacità. I nodi più grandi aggiunti a un cluster con nodi più piccoli devono essere aggiunti a coppie. Ciò consente a Double Helix di spostare i dati in modo da lasciare spazio sufficiente in caso di guasto di uno dei nodi più grandi. È possibile aggiungere capacità di nodo inferiori a un cluster di nodi più grande per migliorare le performance.

> Se un nodo aggiunto di recente rappresenta oltre il 50% della capacità totale del cluster, una parte della capacità di questo nodo viene resa inutilizzabile ("bloccato"), in modo che sia conforme alla regola di capacità. Questo rimane il caso fino a quando non viene aggiunto ulteriore storage. Se viene aggiunto un nodo molto grande che disobbedisce anche alla regola di capacità, il nodo precedentemente bloccato non verrà più bloccato, mentre il nodo appena aggiunto viene bloccato. La capacità deve essere sempre aggiunta in coppie per evitare che ciò accada. Quando un nodo viene bloccato, viene generato l'errore del cluster strandedCapacity.

"Video di NetApp: Scalabilità in base ai termini: Espansione di un cluster SolidFire"

È possibile aggiungere nodi alle appliance NetApp HCI.

Fasi

1. Selezionare **Cluster** > **Nodes**.
2. Fare clic su **Pending** (in sospeso) per visualizzare l'elenco dei nodi in sospeso.

   Una volta completato il processo di aggiunta dei nodi, questi vengono visualizzati nell'elenco nodi attivi. Fino ad allora, i nodi in sospeso vengono visualizzati nell'elenco Pending Active (attivo in sospeso).

   SolidFire installa la versione software Element del cluster sui nodi in sospeso quando vengono aggiunti a un cluster. L'operazione potrebbe richiedere alcuni minuti.

3. Effettuare una delle seguenti operazioni:
   - Per aggiungere singoli nodi, fare clic sull'icona **azioni** del nodo che si desidera aggiungere.
   - Per aggiungere più nodi, selezionare la casella di controllo dei nodi da aggiungere, quindi **azioni in blocco**. **Nota:** se il nodo che si sta aggiungendo ha una versione del software Element diversa da quella in esecuzione sul cluster, il cluster aggiorna in modo asincrono il nodo alla versione del software Element in esecuzione sul master del cluster. Una volta aggiornato, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo si trova in uno stato Active pendingActive.
4. Fare clic su **Aggiungi**.

   Il nodo viene visualizzato nell'elenco dei nodi attivi.

Trova ulteriori informazioni

Versione e compatibilità dei nodi

Versione e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione software di Element installata su un nodo. I cluster di storage basati su software Element imbasano automaticamente un'immagine di un nodo alla versione software Element sul cluster se il nodo e il cluster non sono compatibili.

Il seguente elenco descrive i livelli di importanza delle release software che compongono il numero di versione del software Element:

- **Maggiore**

  Il primo numero indica una versione software. Un nodo con un numero di componente principale non può essere aggiunto a un cluster contenente nodi con un numero di patch principale diverso, né può essere creato un cluster con nodi con versioni principali miste.

- **Minore**

  Il secondo numero indica funzionalità software più piccole o miglioramenti alle funzionalità software esistenti che sono state aggiunte a una release principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa release incrementale non è compatibile con altre release incrementali di software elemento con un componente minore diverso. Ad

esempio, 11.0 non è compatibile con 11.1 e 11.1 non è compatibile con 11.2.

- **Micro**

  Il terzo numero indica una patch compatibile (release incrementale) con la versione software dell'elemento rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0 e 11.0.2 con 11.0.3.

I numeri di versione principali e secondari devono corrispondere per la compatibilità. I micro numeri non devono corrispondere per la compatibilità.

Capacità del cluster in un ambiente a nodi misti

È possibile combinare diversi tipi di nodi in un cluster. La serie SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 e H-Series possono coesistere in un cluster.

La serie H è composta da nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi sono entrambi compatibili con 10 GbE e 25 GbE.

Si consiglia di non mischiare nodi non crittografati e crittografati. In un cluster a nodi misti, nessun nodo può superare il 33% della capacità totale del cluster. Ad esempio, in un cluster con quattro nodi SF-Series 4805, il nodo più grande che può essere aggiunto da solo è SF-Series 9605. La soglia di capacità del cluster viene calcolata in base alla potenziale perdita del nodo più grande in questa situazione.

A partire da Element 12.0, i seguenti nodi storage della serie SF non sono supportati:

- SF3010
- SF6010
- SF9010

Se si aggiorna uno di questi nodi di storage all'elemento 12.0, viene visualizzato un errore che indica che questo nodo non è supportato dall'elemento 12.0.

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio i tag di servizio, i dettagli dei dischi e la grafica per l'utilizzo e le statistiche dei dischi. La pagina nodi della scheda Cluster fornisce la colonna Version (versione) in cui è possibile visualizzare la versione software di ciascun nodo.

Fasi

1. Fare clic su **Cluster** > **Nodes**.
2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **azioni** di un nodo.
3. Fare clic su **View Details** (Visualizza dettagli).
4. Esaminare i dettagli del nodo:
   - **Node ID**: L'ID generato dal sistema per il nodo.
   - **Node Name** (Nome nodo): Il nome host del nodo.
   - **IOPS 4k disponibili**: Gli IOPS configurati per il nodo.
   - **Node role**: Ruolo del nodo nel cluster. Valori possibili:

        - Cluster Master: Nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
        - Ensemble Node: Nodo che partecipa al cluster. Esistono 3 o 5 nodi di ensemble a seconda delle dimensioni del cluster.
        - Fibre Channel: Un nodo nel cluster.
    - **Node Type**: Il tipo di modello del nodo.
    - **Active Drives**: Il numero di dischi attivi nel nodo.
    - **IP di gestione**: L'indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione della rete da 1 GbE o 10 GbE.
    - **Cluster IP**: L'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi dello stesso cluster.
    - **Storage IP**: L'indirizzo IP (SIP) dello storage assegnato al nodo utilizzato per il rilevamento della rete iSCSI e per tutto il traffico della rete dati.
    - **Management VLAN ID** (ID VLAN di gestione): L'ID virtuale per la rete locale di gestione.
    - **Storage VLAN ID**: L'ID virtuale per la rete locale di storage.
    - **Version**: La versione del software in esecuzione su ciascun nodo.
    - **Replication Port** (porta di replica): La porta utilizzata sui nodi per la replica remota.
    - **Service Tag**: Numero di service tag univoco assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

È possibile visualizzare i dettagli delle porte Fibre Channel, ad esempio lo stato, il nome e l'indirizzo della porta, dalla pagina Porte FC.

Consente di visualizzare informazioni sulle porte Fibre Channel collegate al cluster.

Fasi

1. Fare clic su **Cluster** > **FC Ports**.
2. Per filtrare le informazioni in questa pagina, fare clic su **Filter** (filtro).
3. Leggi i dettagli:
    - **Node ID**: Il nodo che ospita la sessione per la connessione.
    - **Node Name**: Nome del nodo generato dal sistema.
    - **Slot**: Numero dello slot in cui si trova la porta Fibre Channel.
    - **HBA Port**: Porta fisica sull'HBA (host bus adapter) Fibre Channel.
    - **WWNN**: Il nome del nodo mondiale.
    - **WWPN**: Il nome della porta universale di destinazione.
    - **Switch WWN**: Nome mondiale dello switch Fibre Channel.
    - **Port state** (Stato porta): Stato corrente della porta.
    - **NID porta**: L'ID della porta del nodo sul fabric Fibre Channel.
    - **Speed**: La velocità negoziata di Fibre Channel. I valori possibili sono i seguenti:
        - 4 Gbps
        - 8 Gbps

- 16 Gbps

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire le reti virtuali

Il networking virtuale nello storage SolidFire consente di connettere il traffico tra più client su reti logiche separate a un cluster. Le connessioni al cluster vengono separate nello stack di rete attraverso l'utilizzo del tagging VLAN.

Trova ulteriori informazioni

- Aggiungere una rete virtuale
- Abilitare il routing e l'inoltro virtuale
- Modificare una rete virtuale
- Modificare le VLAN VRF
- Eliminare una rete virtuale

Aggiungere una rete virtuale

È possibile aggiungere una nuova rete virtuale a una configurazione del cluster per abilitare una connessione di ambiente multi-tenant a un cluster che esegue il software Element.

Di cosa hai bisogno

- Identificare il blocco di indirizzi IP che verranno assegnati alle reti virtuali sui nodi del cluster.
- Identificare un indirizzo IP della rete di storage (SVIP) che verrà utilizzato come endpoint per tutto il traffico dello storage NetApp Element.

Per questa configurazione, è necessario prendere in considerazione i seguenti criteri:

- Le VLAN non abilitate per VRF richiedono che gli iniziatori si trovino nella stessa sottorete dell'SVIP.
- Le VLAN abilitate per VRF non richiedono che gli iniziatori si trovino nella stessa sottorete di SVIP e che il routing sia supportato.
- L'SVIP predefinito non richiede che gli iniziatori si trovano nella stessa subnet dell'SVIP e il routing è supportato.

Quando viene aggiunta una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascun nodo richiede un indirizzo IP della rete virtuale. Il numero di indirizzi IP specificati durante la creazione di una nuova rete virtuale deve essere uguale o superiore al numero di nodi nel cluster. Gli indirizzi delle reti virtuali vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi nel cluster.

Fasi

1. Fare clic su **Cluster** > **Network**.

2. Fare clic su **Create VLAN** (Crea VLAN).
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:
   - **Nome VLAN**
   - **Tag VLAN**
   - **SVIP**
   - **Netmask**
   - (Facoltativo) **Descrizione**
4. Inserire l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **blocchi di indirizzi IP**.
5. Inserire **Size** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
6. Fare clic su **Add a block** (Aggiungi un blocco) per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
7. Fare clic su **Create VLAN** (Crea VLAN).

Visualizza i dettagli della rete virtuale

Fasi

1. Fare clic su **Cluster** > **Network**.
2. Esaminare i dettagli.
   - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
   - **Name**: Nome univoco assegnato dall'utente per la rete VLAN.
   - **VLAN Tag**: Tag VLAN assegnato al momento della creazione della rete virtuale.
   - **SVIP**: Indirizzo IP virtuale dello storage assegnato alla rete virtuale.
   - **Netmask**: Netmask per questa rete virtuale.
   - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere attivato.
   - **VRF Enabled**: Indicazione dell'attivazione o meno del routing e dell'inoltro virtuale.
   - **IP utilizzati**: Intervallo di indirizzi IP della rete virtuale utilizzati per la rete virtuale.

Abilitare il routing e l'inoltro virtuale

È possibile attivare il routing e l'inoltro virtuale (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di lavorare contemporaneamente. Questa funzionalità è disponibile solo per le reti di storage.

È possibile attivare VRF solo al momento della creazione di una VLAN. Se si desidera tornare a non VRF, è necessario eliminare e ricreare la VLAN.

1. Fare clic su **Cluster** > **Network**.
2. Per attivare VRF su una nuova VLAN, selezionare **Create VLAN** (Crea VLAN).
   a. Inserire le informazioni pertinenti per la nuova VRF/VLAN. Vedere aggiunta di una rete virtuale.
   b. Selezionare la casella di controllo **Enable VRF** (attiva VRF*).
   c. **Opzionale**: Inserire un gateway.
3. Fare clic su **Create VLAN** (Crea VLAN).

Trova ulteriori informazioni

Aggiungere una rete virtuale

Modificare una rete virtuale

È possibile modificare gli attributi della VLAN, ad esempio il nome della VLAN, la netmask e la dimensione dei blocchi di indirizzi IP. Il tag VLAN e SVIP non possono essere modificati per una VLAN. L'attributo gateway non è un parametro valido per le VLAN non VRF.

Se sono presenti iSCSI, replica remota o altre sessioni di rete, la modifica potrebbe non riuscire.

Quando si gestiscono le dimensioni degli intervalli di indirizzi IP della VLAN, tenere presenti le seguenti limitazioni:

- È possibile rimuovere gli indirizzi IP solo dall'intervallo di indirizzi IP iniziale assegnato al momento della creazione della VLAN.
- È possibile rimuovere un blocco di indirizzi IP aggiunto dopo l'intervallo di indirizzi IP iniziale, ma non è possibile ridimensionare un blocco IP rimuovendo gli indirizzi IP.
- Quando si tenta di rimuovere gli indirizzi IP, dall'intervallo di indirizzi IP iniziale o in un blocco IP, utilizzati dai nodi nel cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare indirizzi IP in uso specifici ad altri nodi nel cluster.

È possibile aggiungere un blocco di indirizzi IP seguendo la procedura riportata di seguito:

1. Selezionare **Cluster** > **Network**.
2. Selezionare l'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **Edit VLAN** (Modifica VLAN), immettere i nuovi attributi per la VLAN.
5. Selezionare **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per la rete virtuale.
6. Selezionare **Save Changes** (Salva modifiche).

Collegamento agli articoli della Knowledge base per la risoluzione dei problemi

Collegamento agli articoli della Knowledge base per assistenza nella risoluzione dei problemi relativi alla gestione degli intervalli di indirizzi IP della VLAN.

- "Avviso IP duplicato dopo l'aggiunta di un nodo di storage nella VLAN sul cluster di elementi"
- "Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati in Element"

Modificare le VLAN VRF

È possibile modificare gli attributi della VLAN VRF, ad esempio nome VLAN, netmask, gateway e blocchi di indirizzi IP.

1. Fare clic su **Cluster** > **Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera modificare.
3. Fare clic su **Edit** (Modifica).

4. Inserire i nuovi attributi per la VLAN VRF nella finestra di dialogo **Edit VLAN** (Modifica VLAN).
5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare una rete virtuale

È possibile rimuovere un oggetto di rete virtuale. È necessario aggiungere i blocchi di indirizzi a un'altra rete virtuale prima di rimuovere una rete virtuale.

1. Fare clic su **Cluster** > **Network**.
2. Fare clic sull'icona Actions (azioni) per la VLAN che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Trova ulteriori informazioni

Modificare una rete virtuale

Creare un cluster che supporti i dischi FIPS

La sicurezza sta diventando sempre più critica per l'implementazione di soluzioni in molti ambienti dei clienti. Gli standard FIPS (Federal Information Processing Standards) sono standard per la sicurezza e l'interoperabilità dei computer. La crittografia certificata FIPS 140-2 per i dati inattivi è un componente della soluzione di sicurezza globale.

- "Evitare la combinazione di nodi per i dischi FIPS"
- "Abilitare la crittografia a riposo"
- "Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS"
- "Attivare la funzione dischi FIPS"
- "Controllare lo stato del disco FIPS"
- "Risolvere i problemi relativi alla funzione del disco FIPS"

Evitare la combinazione di nodi per i dischi FIPS

Per prepararsi all'attivazione della funzione dischi FIPS, evitare di combinare nodi in cui alcuni sono in grado di supportare dischi FIPS e altri no.

Un cluster è considerato conforme ai dischi FIPS in base alle seguenti condizioni:

- Tutti i dischi sono certificati come dischi FIPS.
- Tutti i nodi sono nodi di dischi FIPS.
- La crittografia a riposo (EAR) è attivata.
- La funzione dischi FIPS è attivata. Tutti i dischi e i nodi devono essere compatibili con FIPS e la crittografia a riposo deve essere attivata per abilitare la funzione disco FIPS.

Abilitare la crittografia a riposo

È possibile attivare e disattivare la crittografia a livello di cluster a riposo. Questa funzione

non è attivata per impostazione predefinita. Per supportare le unità FIPS, è necessario attivare la crittografia a riposo.

1. Nell'interfaccia utente del software NetApp Element, fare clic su **cluster** > **Impostazioni**.
2. Fare clic su *Enable Encryption at REST (attiva crittografia a riposo)

Trova ulteriori informazioni

- Attivare e disattivare la crittografia per un cluster
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Identificare se i nodi sono pronti per la funzionalità dei dischi FIPS

Verificare se tutti i nodi del cluster di storage sono pronti a supportare le unità FIPS utilizzando il metodo API GetFipsReport del software NetApp Element.

Il report risultante mostra uno dei seguenti stati:

- None (Nessuna): Il nodo non è in grado di supportare la funzione dei dischi FIPS.
- Parziale: Il nodo è compatibile con FIPS, ma non tutti i dischi sono dischi FIPS.
- Pronto: Il nodo è compatibile con FIPS e tutti i dischi sono dischi FIPS o non sono presenti dischi.

Fasi

1. Utilizzando l'API Element, verificare se i nodi e i dischi nel cluster di storage sono in grado di utilizzare dischi FIPS immettendo:

   ```
   GetFipsReport
   ```

2. Esaminare i risultati, prendendo nota di eventuali nodi che non hanno visualizzato lo stato Ready (Pronto).
3. Per i nodi che non hanno visualizzato lo stato Ready, verificare se il disco è in grado di supportare la funzione dei dischi FIPS:
   - Utilizzando l'API Element, immettere: `GetHardwareList`
   - Annotare il valore di **DriveEncryptionCapabilityType**. Se si tratta di "fips", l'hardware può supportare la funzione dei dischi FIPS.

     Vedere i dettagli su `GetFipsReport` oppure `ListDriveHardware` in "Riferimento API dell'elemento".
4. Se il disco non supporta la funzione dischi FIPS, sostituire l'hardware con hardware FIPS (nodo o dischi).

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Attivare la funzione dischi FIPS

È possibile attivare la funzione dischi FIPS utilizzando il software NetApp Element

`EnableFeature` Metodo API.

La crittografia a riposo deve essere attivata sul cluster e tutti i nodi e le unità devono essere compatibili con FIPS, come indicato quando GetFipsReport visualizza uno stato Ready per tutti i nodi.

Fase

1. Utilizzando l'API Element, abilitare FIPS su tutti i dischi immettendo:

   ```
   EnableFeature params: FipsDrives
   ```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Controllare lo stato del disco FIPS

È possibile verificare se la funzione delle unità FIPS è attivata sul cluster utilizzando il software NetApp Element `GetFeatureStatus` Metodo API, che indica se lo stato FIPS Drives Enabled (dischi FIPS abilitati) è true (vero) o false.

1. Utilizzando l'API Element, verificare la funzione dei dischi FIPS nel cluster immettendo:

   ```
   GetFeatureStatus
   ```

2. Esaminare i risultati di `GetFeatureStatus` Chiamata API. Se il valore FIPS Drives Enabled (dischi FIPS attivati) è True (vero), la funzione FIPS Drives (dischi FIPS) è attivata.

   ```
   {"enabled": true,
   "feature": "FipsDrives"
   }
   ```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Risolvere i problemi relativi alla funzione del disco FIPS

Utilizzando l'interfaccia utente del software NetApp Element, è possibile visualizzare avvisi per informazioni su errori o guasti del cluster nel sistema correlati alla funzione dischi FIPS.

1. Utilizzando l'interfaccia utente di Element, selezionare **Reporting** > **Alerts**.
2. Individuare eventuali guasti del cluster, tra cui:

- Dischi FIPS non corrispondenti
- FIPS non rispetta la conformità

3. Per suggerimenti sulla risoluzione, vedere informazioni sul codice di errore del cluster.

Trova ulteriori informazioni

- Codici di guasto del cluster
- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Abilitare FIPS 140-2 per HTTPS sul cluster

È possibile utilizzare il metodo API EnableFeature per attivare la modalità operativa FIPS 140-2 per le comunicazioni HTTPS.

Con il software NetApp Element, è possibile attivare la modalità operativa FIPS (Federal Information Processing Standards) 140-2 sul cluster. L'attivazione di questa modalità attiva il modulo di sicurezza crittografica NetApp (NCSM) e sfrutta la crittografia certificata FIPS 140-2 livello 1 per tutte le comunicazioni via HTTPS all'interfaccia utente e all'API NetApp Element.

> Una volta attivata la modalità FIPS 140-2, non è possibile disattivarla. Quando la modalità FIPS 140-2 è attivata, ciascun nodo del cluster si riavvia ed esegue un autotest che garantisce che NCSM sia abilitato e funzioni correttamente nella modalità certificata FIPS 140-2. Ciò causa un'interruzione delle connessioni di gestione e di storage sul cluster. È necessario pianificare attentamente e attivare questa modalità solo se l'ambiente richiede il meccanismo di crittografia che offre.

Per ulteriori informazioni, vedere le informazioni sull'API Element.

Di seguito viene riportato un esempio della richiesta API per attivare FIPS:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "fips"
    },
    "id": 1
}
```

Una volta attivata questa modalità operativa, tutte le comunicazioni HTTPS utilizzano le crittografia approvate da FIPS 140-2.

Trova ulteriori informazioni

- Crittografie SSL
- "Gestire lo storage con l'API Element"

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Crittografie SSL

Le crittografie SSL sono algoritmi di crittografia utilizzati dagli host per stabilire una comunicazione sicura. Esistono cifrari standard supportati dal software Element e non standard quando è attivata la modalità FIPS 140-2.

I seguenti elenchi forniscono le crittografie standard SSL (Secure Socket Layer) supportate dal software Element e le crittografie SSL supportate quando la modalità FIPS 140-2 è attivata:

- **FIPS 140-2 disattivato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C.

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

  TLS_RSA_WITH_CAMELLIA_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_CAMELLIA_256_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_IDEA_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_RC4_128_MD5 (RSA 2048) - C

  TLS_RSA_WITH_RC4_128_SHA (RSA 2048) - C.

  TLS_RSA_WITH_SEED_CBC_SHA (RSA 2048) - A.

- **FIPS 140-2 abilitato**

  TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 (DH 2048) - A.

  TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 (DH 2048) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECT571R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECP256R1) - A.

  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (SECT571R1) - A.

  TLS_RSA_WITH_3DES_EDE_CBC_SHA (RSA 2048) - C.

  TLS_RSA_WITH_AES_128_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_CBC_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_128_GCM_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_CBC_SHA256 (RSA 2048) - A.

  TLS_RSA_WITH_AES_256_GCM_SHA384 (RSA 2048) - A.

Trova ulteriori informazioni

Abilitare FIPS 140-2 per HTTPS sul cluster

Inizia a utilizzare la gestione esterna delle chiavi

EKM (External Key Management) offre una gestione sicura delle chiavi di autenticazione (AK) insieme a un server esterno delle chiavi (EKS) off-cluster. Gli AKS vengono utilizzati per bloccare e sbloccare i dischi con crittografia automatica (SED) quando "crittografia a riposo" è attivato sul cluster. EKS fornisce generazione e storage sicuri di AKS. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito DA OASIS, per comunicare con EKS.

- "Configurare la gestione esterna"
- "Ridigita la chiave master di crittografia software a riposo"
- "Ripristino di chiavi di autenticazione inaccessibili o non valide"
- "Comandi API esterni per la gestione delle chiavi"

Trova ulteriori informazioni

- "API CreateCluster che può essere utilizzata per attivare la crittografia software a riposo"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Impostare la gestione esterna delle chiavi

È possibile seguire questi passaggi e utilizzare i metodi API Element elencati per configurare la funzione di gestione delle chiavi esterna.

Di cosa hai bisogno

- Se si imposta la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, è stata attivata la crittografia software a riposo utilizzando "CreateCluster" metodo su un nuovo cluster che non contiene volumi.

Fasi

1. Stabilire una relazione di trust con EKS (External Key Server).
   a. Creare una coppia di chiavi pubbliche/private per il cluster di elementi che viene utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API: "CreatePublicPrivateKeyPair"
   b. Ottenere la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. La CSR consente al server delle chiavi di verificare che il cluster di elementi che accederà alle chiavi sia autenticato come cluster di elementi. Chiamare il seguente metodo API: "GetClientCertificateSignRequest"
   c. Utilizzare EKS/Certificate Authority per firmare la CSR recuperata. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un provider di chiavi definisce dove ottenere una chiave e un server definisce gli attributi specifici di EKS con cui verrà comunicata.
   a. Creare un provider di chiavi in cui risiedono i dettagli del server di chiavi chiamando il seguente metodo API: "CreateKeyProviderKmip"
   b. Creare un server chiavi che fornisce il certificato firmato e il certificato della chiave pubblica dell'autorità di certificazione chiamando i seguenti metodi API: "CreateKeyServerKmip" "TestKeyServerKmip"

      Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.
   c. Aggiungere il server delle chiavi nel contenitore del provider di chiavi chiamando i seguenti metodi API:"AddKeyServerToProviderKmip" "TestKeyProviderKmip"

      Se il test non riesce, verificare la connettività e la configurazione del server. Quindi ripetere il test.

3. Eseguire una delle seguenti operazioni come fase successiva per la crittografia a riposo:
   a. (Per la crittografia hardware a riposo) Enable (attiva) "crittografia hardware a riposo" Fornendo l'ID del provider di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il "EnableEncryptionAtRest" Metodo API.

      È necessario attivare la crittografia a riposo tramite "API". Attivando la crittografia a riposo utilizzando il pulsante dell'interfaccia utente Element esistente, la funzione torna a utilizzare le chiavi generate internamente.

   b. (Per la crittografia software a riposo) per "crittografia software a riposo" Per utilizzare il provider di chiavi appena creato, passare l'ID del provider di chiavi a "RekeySoftwareEncryptionAtRestMasterKey" Metodo API.

Trova ulteriori informazioni

- "Attivare e disattivare la crittografia per un cluster"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ridigita la chiave master di crittografia software a riposo

È possibile utilizzare l'API Element per reimmettere una chiave esistente. Questo processo crea una nuova chiave master sostitutiva per il server di gestione delle chiavi esterno. Le chiavi master vengono sempre sostituite da nuove chiavi master e non vengono mai duplicate o sovrascritte.

Potrebbe essere necessario eseguire una nuova chiave nell'ambito di una delle seguenti procedure:

- Creare una nuova chiave come parte di un cambiamento dalla gestione interna delle chiavi alla gestione esterna delle chiavi.
- Creare una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.

Questo processo è asincrono e restituisce una risposta prima del completamento dell'operazione di rekey. È possibile utilizzare "GetAsyncResult" metodo per eseguire il polling del sistema per verificare il completamento del processo.

Di cosa hai bisogno

- È stata attivata la crittografia software a riposo utilizzando "CreateCluster" Metodo su un nuovo cluster che non contiene volumi e non dispone di i/O. Utilizzare il `GetSoftwareEncryptionatRestInfo` per confermare che lo stato è `enabled` prima di procedere.
- Lo hai fatto "instaurazione di una relazione di fiducia" Tra il cluster SolidFire e un server di chiavi esterne (EKS). Eseguire "TestKeyProviderKmip" metodo per verificare che sia stabilita una connessione con il provider di chiavi.

Fasi

1. Eseguire "ListKeyProvidersKmip" Comando e copia dell'ID del provider di chiavi (`keyProviderID`).
2. Eseguire "RekeySoftwareEncryptionAtRestMasterKey" con `keyManagementType` parametro as `external` e. `keyProviderID` Come numero ID del provider di chiavi del passaggio precedente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

3. Copiare il `asyncHandle` valore di `RekeySoftwareEncryptionAtRestMasterKey` risposta del comando.
4. Eseguire "GetAsyncResult" con il `asyncHandle` valore del passaggio precedente per confermare la modifica della configurazione. Dalla risposta del comando, dovresti vedere che la configurazione della vecchia chiave master è stata aggiornata con le nuove informazioni sulla chiave. Copiare il nuovo ID del provider di chiavi per utilizzarlo in un passaggio successivo.

```
{
   "id": null,
   "result": {
     "createTime": "2021-01-01T22:29:18Z",
     "lastUpdateTime": "2021-01-01T22:45:51Z",
     "result": {
       "keyToDecommission": {
         "keyID": "<value>",
         "keyManagementType": "internal"
     },
     "newKey": {
       "keyID": "<value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "operation": "Rekeying Master Key. Master Key management being
transferred from Internal Key Management to External Key Management with
keyProviderID=<value>",
     "state": "Ready"
   },
   "resultType": "RekeySoftwareEncryptionAtRestMasterKey",
   "status": "complete"
}
```

5. Eseguire `GetSoftwareEncryptionatRestInfo` per confermare i dettagli della nuova chiave, incluso il `keyProviderID`, sono stati aggiornati.

```
{
   "id": null,
   "result": {
     "masterKeyInfo": {
       "keyCreatedTime": "2021-01-01T22:29:18Z",
       "keyID": "<updated value>",
       "keyManagementType": "external",
       "keyProviderID": <value>
     },
     "rekeyMasterKeyAsyncResultID": <value>
     "status": "enabled",
     "version": 1
   },
}
```

Trova ulteriori informazioni

- "Gestire lo storage con l'API Element"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ripristino di chiavi di autenticazione inaccessibili o non valide

Occasionalmente, può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, viene generato un guasto del cluster (indicato come codice di guasto del cluster). I due casi più probabili sono descritti qui.

Il cluster non è in grado di sbloccare i dischi a causa di un errore del cluster KmipServerFault.

Questo può verificarsi quando il cluster si avvia per la prima volta e il server delle chiavi non è accessibile o la chiave richiesta non è disponibile.

1. Seguire le fasi di ripristino riportate nei codici di guasto del cluster (se presenti).

Un errore sliceServiceUnhealthy potrebbe essere impostato perché i dischi metadati sono stati contrassegnati come guasti e posizionati nello stato "Available" (disponibile).

Procedura per la cancellazione:

1. Aggiungere di nuovo i dischi.
2. Dopo 3-4 minuti, controllare che il `sliceServiceUnhealthy` il guasto è stato cancellato.

Vedere "codici di guasto del cluster" per ulteriori informazioni.

Comandi API esterni per la gestione delle chiavi

Elenco di tutte le API disponibili per la gestione e la configurazione di EKM.

Utilizzato per stabilire una relazione di trust tra il cluster e i server esterni di proprietà del cliente:

- CreatePublicPrivateKeyPair
- GetClientCertificateSignRequest

Utilizzato per definire i dettagli specifici dei server esterni di proprietà del cliente:

- CreateKeyServerKmip
- ModifyKeyServerKmip
- DeleteKeyServerKmip
- GetKeyServerKmip
- ListKeyServerKmip
- TestKeyServerKmip

Utilizzato per la creazione e la manutenzione di provider di chiavi che gestiscono server di chiavi esterni:

- CreateKeyProviderKmip
- DeleteKeyProviderKmip
- AddKeyServerToProviderKmip
- RemoveKeyServerFromProviderKmip
- GetKeyProviderKmip
- ListKeyProvidersKmip
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmip

Per informazioni sui metodi API, vedere "Informazioni di riferimento API".

Gestire volumi e volumi virtuali

È possibile gestire i dati in un cluster che esegue il software Element dalla scheda Management (Gestione) dell'interfaccia utente Element. Le funzioni di gestione dei cluster disponibili includono la creazione e la gestione di volumi di dati, gruppi di accesso ai volumi, iniziatori e policy di qualità del servizio (QoS).

- "Lavorare con i volumi"
- "Lavorare con volumi virtuali"
- "Lavorare con gli iniziatori e i gruppi di accesso ai volumi"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Lavorare con i volumi

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel. Dalla pagina Volumes (volumi) della scheda Management (Gestione), è possibile creare, modificare, clonare ed eliminare volumi su un nodo. È inoltre possibile visualizzare le statistiche relative alla larghezza di banda del volume e all'utilizzo di i/O.

Trova ulteriori informazioni

- "Gestire le policy di qualità del servizio"
- "Creare un volume"
- "Visualizza i dettagli delle performance dei singoli volumi"
- "Modificare i volumi attivi"
- "Eliminare un volume"
- "Ripristinare un volume cancellato"
- "Eliminare un volume"
- "Clonare un volume"
- "Assegnare LUN a volumi Fibre Channel"
- "Applicare una policy di QoS ai volumi"
- "Rimuovere l'associazione dei criteri QoS di un volume"

Gestire le policy di qualità del servizio

Una policy di qualità del servizio (QoS) consente di creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi. È possibile creare, modificare ed eliminare i criteri QoS dalla pagina QoS Policies (Criteri QoS) nella scheda Management (Gestione).

> Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascrive e regola i valori dei criteri QoS per le impostazioni QoS del volume.

"Video NetApp: Policy di qualità del servizio SolidFire"

Vedere "Performance e qualità del servizio".

- Creare una policy QoS
- Modificare un criterio QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare policy QoS e applicarle durante la creazione di volumi.

1. Selezionare **Management** > **QoS Policies**.
2. Fare clic su **Crea policy QoS**.

3. Inserire il nome * Policy Name*.
4. Inserire i valori**min IOPS**, **Max IOPS** e **Burst IOPS**.
5. Fare clic su **Crea policy QoS**.

Modificare un criterio QoS

È possibile modificare il nome di un criterio QoS esistente o i valori associati al criterio. La modifica di un criterio QoS influisce su tutti i volumi associati al criterio.

1. Selezionare **Management** > **QoS Policies**.
2. Fare clic sull'icona Actions (azioni) per il criterio QoS che si desidera modificare.
3. Nel menu visualizzato, selezionare**Edit** (Modifica).
4. Nella finestra di dialogo **Edit QoS Policy** (Modifica policy QoS), modificare le seguenti proprietà come richiesto:
   - Nome policy
   - IOPS minimi
   - IOPS max
   - IOPS burst
5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare una policy QoS

È possibile eliminare una policy QoS se non è più necessaria. Quando si elimina un criterio QoS, tutti i volumi associati al criterio mantengono le impostazioni QoS ma non vengono associati a un criterio.

> Se invece si tenta di disassociare un volume da un criterio QoS, è possibile modificare le impostazioni QoS per quel volume su customizzato.

1. Selezionare **Management** > **QoS Policies**.
2. Fare clic sull'icona Actions (azioni) per il criterio QoS che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Trova ulteriori informazioni

- "Rimuovere l'associazione dei criteri QoS di un volume"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Gestire i volumi

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel.

Dalla pagina Volumes (volumi) della scheda Management (Gestione), è possibile creare, modificare, clonare ed eliminare volumi su un nodo.

Creare un volume

È possibile creare un volume e associarlo a un determinato account. Ogni volume deve essere associato a un account. Questa associazione consente all'account di accedere al volume tramite gli iniziatori iSCSI utilizzando le credenziali CHAP.

È possibile specificare le impostazioni QoS per un volume durante la creazione.

1. Selezionare **Management** > **Volumes**.
2. Fare clic su **Create Volume** (Crea volume).
3. Nella finestra di dialogo **Create a New Volume** (Crea un nuovo volume), immettere il nome del volume.
4. Inserire le dimensioni totali del volume.

   La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

   - 1 GB = 000 000 000 byte
   - 1GiB = 1 073 741 824 byte
5. Selezionare **Block Size** (dimensione blocco) per il volume.
6. Fare clic sull'elenco a discesa **account** e selezionare l'account che deve avere accesso al volume.

   Se non esiste un account, fare clic sul collegamento **Create account** (Crea account), immettere un nuovo nome account e fare clic su **Create** (Crea). L'account viene creato e associato al nuovo volume.

   Se sono presenti più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.
7. Per impostare la **qualità del servizio**, effettuare una delle seguenti operazioni:
   a. In **Policy**, è possibile selezionare un criterio QoS esistente, se disponibile.
   b. In **Custom Settings** (Impostazioni personalizzate), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.

      I volumi con un valore massimo o burst IOPS superiore a 20,000 IOPS potrebbero richiedere una profondità di coda elevata o più sessioni per ottenere questo livello di IOPS su un singolo volume.
8. Fare clic su **Create Volume** (Crea volume).

Visualizzare i dettagli del volume

1. Selezionare **Management** > **Volumes**.
2. Esaminare i dettagli.
   - **ID**: L'ID generato dal sistema per il volume.
   - **Name** (Nome): Il nome assegnato al volume al momento della creazione.
   - **Account**: Il nome dell'account assegnato al volume.
   - **Gruppi di accesso**: Il nome del gruppo o dei gruppi di accesso al volume a cui appartiene il volume.
   - **Access**: Il tipo di accesso assegnato al volume al momento della creazione. Valori possibili:
     - Lettura/scrittura: Tutte le letture e le scritture sono accettate.

        - Sola lettura: Tutte le attività di lettura sono consentite; non sono consentite scritture.
        - Bloccato: È consentito solo l'accesso come amministratore.
        - ReplicationTarget: Designato come volume di destinazione in una coppia di volumi replicati.
    - **Utilizzato**: La percentuale di spazio utilizzato nel volume.
    - **Size**: Dimensione totale (in GB) del volume.
    - **Snapshot**: Il numero di snapshot creati per il volume.
    - **QoS Policy**: Il nome e il collegamento alla policy QoS definita dall'utente.
    - **IOPS min**: Il numero minimo di IOPS garantito per il volume.
    - **IOPS max**: Il numero massimo di IOPS consentito per il volume.
    - **Burst IOPS**: Il numero massimo di IOPS consentito per un breve periodo di tempo per il volume. Impostazione predefinita = 15,000.
    - **Attributes**: Attributi assegnati al volume come coppia chiave/valore tramite un metodo API.
    - **512e**: Indicazione dell'attivazione di 512e su un volume. Valori possibili:
        - Sì
        - No
    - **Creato il**: La data e l'ora in cui è stato creato il volume.

Visualizzare i dettagli dei singoli volumi

È possibile visualizzare le statistiche delle performance per i singoli volumi.

1. Selezionare **Reporting** > **Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Actions (azioni) per un volume.
3. Fare clic su **View Details** (Visualizza dettagli).

   Nella parte inferiore della pagina viene visualizzato un vassoio contenente informazioni generali sul volume.

4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi ulteriori dettagli**.

   Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Modificare i volumi attivi

È possibile modificare gli attributi del volume, ad esempio i valori di QoS, le dimensioni del volume e l'unità di misura in cui vengono calcolati i valori di byte. È inoltre possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

È possibile ridimensionare un volume quando lo spazio disponibile sul cluster è sufficiente nelle seguenti condizioni:

- Condizioni di funzionamento normali.
- Vengono segnalati errori o errori del volume.
- Il volume è in fase di clonaggio.
- Il volume è in fase di risyncing.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Nella finestra **Active**, fare clic sull'icona Actions (azioni) del volume che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. **Opzionale:** consente di modificare le dimensioni totali del volume.
   - È possibile aumentare, ma non diminuire, le dimensioni del volume. È possibile ridimensionare un solo volume in una singola operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.
   - Se si stanno regolando le dimensioni del volume per la replica, è necessario innanzitutto aumentare le dimensioni del volume assegnato come destinazione della replica. Quindi, è possibile ridimensionare il volume di origine. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

     La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

   - 1 GB = 000 000 000 byte
   - 1GiB = 1 073 741 824 byte
5. **Opzionale:** selezionare un livello di accesso diverso per uno dei seguenti account:
   - Di sola lettura
   - Lettura/scrittura
   - Bloccato
   - Destinazione della replica
6. **Opzionale:** selezionare l'account che deve avere accesso al volume.

   Se l'account non esiste, fare clic sul collegamento **Create account** (Crea account), immettere un nuovo nome account e fare clic su **Create** (Crea). L'account viene creato e associato al volume.

   Se sono presenti più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.

7. **Opzionale:** per modificare la selezione in **qualità del servizio**, effettuare una delle seguenti operazioni:

   a. In **Policy**, è possibile selezionare un criterio QoS esistente, se disponibile.
   b. In **Custom Settings** (Impostazioni personalizzate), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.

   Se si utilizzano policy QoS su un volume, è possibile impostare una QoS personalizzata per rimuovere l'affiliazione della policy QoS con il volume. La QoS personalizzata sovrascrive e regola i valori dei criteri QoS per le impostazioni QoS del volume.

   Quando si modificano i valori IOPS, è necessario aumentare in decine o centinaia. I valori di input richiedono numeri interi validi.

Configurare volumi con un valore burst estremamente elevato. Ciò consente al sistema di elaborare più rapidamente carichi di lavoro sequenziali occasionali a blocchi di grandi dimensioni, limitando al contempo gli IOPS sostenuti per un volume.

8. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un volume

È possibile eliminare uno o più volumi da un cluster di storage Element.

Il sistema non elimina immediatamente un volume cancellato; il volume rimane disponibile per circa otto ore. Se si ripristina un volume prima che venga spurgato dal sistema, il volume torna online e le connessioni iSCSI vengono ripristinate.

Se un volume utilizzato per creare uno snapshot viene cancellato, le relative snapshot associate diventano inattive. Quando i volumi di origine cancellati vengono rimossi, anche le snapshot inattive associate vengono rimosse dal sistema.

I volumi persistenti associati ai servizi di gestione vengono creati e assegnati a un nuovo account durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare i volumi o l'account associato.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Per eliminare un singolo volume, attenersi alla seguente procedura:
   a. Fare clic sull'icona Actions (azioni) per il volume che si desidera eliminare.
   b. Nel menu visualizzato, fare clic su **Delete** (Elimina).
   c. Confermare l'azione.

   Il sistema sposta il volume nell'area **Deleted** della pagina **Volumes**.
3. Per eliminare più volumi, attenersi alla seguente procedura:
   a. Nell'elenco dei volumi, selezionare la casella accanto ai volumi che si desidera eliminare.
   b. Fare clic su **azioni in blocco**.
   c. Nel menu visualizzato, fare clic su **Delete** (Elimina).
   d. Confermare l'azione.

   Il sistema sposta i volumi nell'area **Deleted** della pagina **Volumes**.

Ripristinare un volume cancellato

È possibile ripristinare un volume nel sistema se è stato eliminato ma non ancora eliminato. Il sistema elimina automaticamente un volume circa otto ore dopo l'eliminazione. Se il sistema ha disinstallato il volume, non è possibile ripristinarlo.

1. Selezionare **Management** > **Volumes**.
2. Fare clic sulla scheda **Deleted** per visualizzare l'elenco dei volumi eliminati.
3. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.

4. Nel menu visualizzato, fare clic su **Restore** (Ripristina).
5. Confermare l'azione.

   Il volume viene inserito nell'elenco dei volumi **attivi** e le connessioni iSCSI al volume vengono ripristinate.

Eliminare un volume

Quando un volume viene eliminato, viene rimosso in modo permanente dal sistema. Tutti i dati nel volume vengono persi.

Il sistema elimina automaticamente i volumi cancellati otto ore dopo l'eliminazione. Tuttavia, se si desidera eliminare un volume prima dell'ora pianificata, è possibile farlo.

1. Selezionare **Management** > **Volumes**.
2. Fare clic sul pulsante **Deleted**.
3. Eseguire la procedura per eliminare uno o più volumi.

Opzione	Fasi
Eliminare un singolo volume	a. Fare clic sull'icona Actions (azioni) per il volume che si desidera eliminare. b. Fare clic su **Rimuovi**. c. Confermare l'azione.
Eliminare più volumi	a. Selezionare i volumi che si desidera eliminare. b. Fare clic su **azioni in blocco**. c. Nel menu visualizzato, selezionare **Rimuovi**. d. Confermare l'azione.

Clonare un volume

È possibile creare un clone di uno o più volumi per creare una copia point-in-time dei dati. Quando si clonano un volume, il sistema crea uno snapshot del volume e quindi una copia dei dati a cui fa riferimento lo snapshot. Si tratta di un processo asincrono e la quantità di tempo richiesta dal processo dipende dalla dimensione del volume che si sta clonando e dal carico corrente del cluster.

Il cluster supporta fino a due richieste di cloni in esecuzione per volume alla volta e fino a otto operazioni di cloni dei volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per l'elaborazione successiva.

I sistemi operativi differiscono per il trattamento dei volumi clonati. VMware ESXi tratterà un volume clonato come una copia di volume o un volume di snapshot. Il volume sarà un dispositivo disponibile da utilizzare per creare un nuovo datastore. Per ulteriori informazioni sul montaggio di volumi cloni e sulla gestione delle LUN snapshot, consultare la documentazione VMware all'indirizzo "Montaggio di una copia del datastore VMFS" e. "Gestione di datastore VMFS duplicati".

Prima di troncare un volume clonato clonando su una dimensione inferiore, assicurarsi di preparare le partizioni in modo che si adattino al volume più piccolo.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Per clonare un singolo volume, attenersi alla seguente procedura:
   a. Nell'elenco dei volumi nella pagina **Active**, fare clic sull'icona Actions (azioni) del volume che si desidera clonare.
   b. Nel menu visualizzato, fare clic su **Clone**.
   c. Nella finestra **Clone Volume**, immettere un nome di volume per il volume appena clonato.
   d. Selezionare una dimensione e una misurazione per il volume utilizzando la casella di selezione **Volume Size** (dimensione volume) e l'elenco.

      La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB:

      - 1 GB = 000 000 000 byte
      - 1GiB = 1 073 741 824 byte

   e. Selezionare il tipo di accesso per il volume appena clonato.
   f. Selezionare un account da associare al volume appena clonato dall'elenco **account**.

      Durante questa fase, è possibile creare un account facendo clic sul collegamento **Create account** (Crea account), immettendo un nome account e facendo clic su **Create** (Crea account). Il sistema aggiunge automaticamente l'account all'elenco **account** dopo averlo creato.

3. Per clonare più volumi, attenersi alla seguente procedura:
   a. Nell'elenco dei volumi nella pagina **Active**, selezionare la casella accanto ai volumi che si desidera clonare.
   b. Fare clic su **azioni in blocco**.
   c. Nel menu visualizzato, selezionare **Clone**.
   d. Nella finestra di dialogo **Clone Multiple Volumes** (Copia volumi multipli), inserire un prefisso per i volumi clonati nel campo **New Volume Name Prefix** (nuovo prefisso nome volume).
   e. Selezionare un account da associare ai volumi clonati dall'elenco **account**.
   f. Selezionare il tipo di accesso per i volumi clonati.
4. Fare clic su **Avvia clonazione**.

   L'aumento delle dimensioni del volume di un clone comporta la creazione di un nuovo volume con ulteriore spazio libero alla fine del volume. A seconda dell'utilizzo del volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per utilizzarlo.

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Assegnare LUN a volumi Fibre Channel

È possibile modificare l'assegnazione del LUN per un volume Fibre Channel in un gruppo di accesso al volume. È inoltre possibile assegnare i LUN dei volumi Fibre Channel quando si crea un gruppo di accesso ai volumi.

L'assegnazione di nuovi LUN Fibre Channel è una funzione avanzata e potrebbe avere conseguenze sconosciute sull'host connesso. Ad esempio, il nuovo ID LUN potrebbe non essere rilevato automaticamente sull'host e l'host potrebbe richiedere una nuova scansione per rilevare il nuovo ID LUN.

1. Selezionare **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso che si desidera modificare.
3. Nel menu visualizzato, selezionare**Edit** (Modifica).
4. In **Assign LUN ID** (Assegna ID LUN) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **LUN Assignments** (assegnazioni LUN).
5. Per ciascun volume dell'elenco a cui si desidera assegnare un LUN, immettere un nuovo valore nel campo **LUN** corrispondente.
6. Fare clic su **Save Changes** (Salva modifiche).

Applicare una policy di QoS ai volumi

È possibile applicare in blocco una policy QoS esistente a uno o più volumi.

Il criterio QoS che si desidera applicare in blocco deve esistere.

1. Selezionare **Management** > **Volumes**.
2. Nell'elenco dei volumi, selezionare la casella accanto ai volumi a cui si desidera applicare il criterio QoS.
3. Fare clic su **azioni in blocco**.
4. Nel menu visualizzato, fare clic su **Apply QoS Policy** (Applica policy QoS).
5. Selezionare il criterio QoS dall'elenco a discesa.
6. Fare clic su **Apply** (Applica).

Trova ulteriori informazioni

Policy sulla qualità del servizio

Rimuovere l'associazione dei criteri QoS di un volume

È possibile rimuovere un'associazione di policy QoS da un volume selezionando impostazioni QoS personalizzate.

Il volume che si desidera modificare deve essere associato a un criterio QoS.

1. Selezionare **Management** > **Volumes**.
2. Fare clic sull'icona Actions (azioni) per un volume che contiene un criterio QoS che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Nel menu visualizzato sotto **qualità del servizio**, fare clic su **Impostazioni personalizzate**.

5. Modificare **min IOPS**, **Max IOPS** e **Burst IOPS** oppure mantenere le impostazioni predefinite.
6. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

Eliminare una policy QoS

Lavorare con volumi virtuali

È possibile visualizzare informazioni ed eseguire attività per volumi virtuali e relativi container di storage, endpoint di protocollo, associazioni e host associati utilizzando l'interfaccia utente di Element.

Il sistema di storage software NetApp Element viene fornito con la funzione volumi virtuali (VVol) disattivata. È necessario eseguire un'attività singola per attivare manualmente la funzionalità vSphere Vol tramite l'interfaccia utente di Element.

Dopo aver attivato la funzionalità Vol, nell'interfaccia utente viene visualizzata una scheda Vols che offre opzioni di monitoraggio correlate a Vols e di gestione limitate. Inoltre, un componente software lato storage noto come provider VASA funge da servizio di consapevolezza dello storage per vSphere. La maggior parte dei comandi VVol, come creazione, cloning e modifica di VVol, vengono avviati da un host vCenter Server o ESXi e tradotti dal provider VASA in API Element per il sistema storage software Element. I comandi per creare, eliminare e gestire i container di storage e eliminare i volumi virtuali possono essere avviati utilizzando l'interfaccia utente di Element.

La maggior parte delle configurazioni necessarie per l'utilizzo della funzionalità Virtual Volumes con i sistemi storage software Element è realizzata in vSphere. Consultare la *Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire* per registrare il provider VASA in vCenter, creare e gestire i datastore VVol e gestire lo storage in base alle policy.

> Non registrare più di un provider VASA NetApp Element in una singola istanza di vCenter. Quando viene aggiunto un secondo provider VASA NetApp Element, questo rende inaccessibili tutti i datastore VVOL.

> Il supporto DI VASA per più vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con vCenter. Per eseguire l'installazione, scaricare il file VASA39 .tar.gz dal "Download di software NetApp" e seguire le indicazioni nel manifesto. Il provider VASA di NetApp Element utilizza un certificato NetApp. Con questa patch, il certificato viene utilizzato senza modifiche da vCenter per supportare più vCenter per l'utilizzo di VASA e VVol. Non modificare il certificato. I certificati SSL personalizzati non sono supportati da VASA.

Trova ulteriori informazioni

- Abilitare i volumi virtuali
- Visualizzare i dettagli del volume virtuale
- Eliminare un volume virtuale
- Creare un container di storage
- Modificare un container di storage
- Eliminare un contenitore di storage

- Endpoint del protocollo
- Associazioni
- Dettagli host

Abilitare i volumi virtuali

È necessario attivare manualmente la funzionalità vVol (vSphere Virtual Volumes) tramite il software NetApp Element. Il sistema software Element viene fornito con la funzionalità VVol disattivata per impostazione predefinita e non viene automaticamente attivata durante una nuova installazione o un aggiornamento. L'attivazione della funzione VVol è un'attività di configurazione unica.

Di cosa hai bisogno

- Il cluster deve eseguire Element 9.0 o versione successiva.
- Il cluster deve essere connesso a un ambiente ESXi 6.0 o successivo compatibile con VVol.
- Se si utilizza Element 11.3 o versione successiva, il cluster deve essere connesso a un ambiente ESXi 6.0 update 3 o versione successiva.

> L'attivazione della funzionalità vSphere Virtual Volumes modifica in modo permanente la configurazione del software Element. La funzionalità VVol deve essere attivata solo se il cluster è connesso a un ambiente compatibile con VMware ESXi VVols. È possibile disattivare la funzione VVol e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster, che elimina tutti i dati presenti nel sistema.

Fasi

1. Selezionare **Clusters** > **Settings**.
2. Individuare le impostazioni specifiche del cluster per i volumi virtuali.
3. Fare clic su **Enable Virtual Volumes** (Abilita volumi virtuali
4. Fare clic su **Sì** per confermare la modifica della configurazione dei volumi virtuali.

   La scheda **VVol** viene visualizzata nell'interfaccia utente di Element.

   > Quando la funzionalità VVol è attivata, il cluster SolidFire avvia il provider VASA, apre la porta 8444 per il traffico VASA e crea endpoint di protocollo che possono essere rilevati da vCenter e da tutti gli host ESXi.

5. Copiare l'URL del provider VASA dalle impostazioni dei volumi virtuali (VVol) in **Clusters** > **Settings**. Questo URL verrà utilizzato per registrare il provider VASA in vCenter.
6. Creare un contenitore di storage in **VVol** > **Storage Containers**.

   > È necessario creare almeno un container di storage in modo che le VM possano essere fornite a un datastore Vol.

7. Selezionare **VVol** > **Protocol Endpoint**.
8. Verificare che sia stato creato un endpoint del protocollo per ciascun nodo del cluster.

VSphere richiede ulteriori attività di configurazione. Consultare la *Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire* per registrare il provider VASA in vCenter, creare e gestire i datastore VVol e gestire lo storage in base alle policy.

Trova ulteriori informazioni

"Guida alla configurazione dello storage VMware vSphere Virtual Volumes per SolidFire"

Visualizzare i dettagli del volume virtuale

È possibile rivedere le informazioni sui volumi virtuali per tutti i volumi virtuali attivi nel cluster nell'interfaccia utente di Element. È inoltre possibile visualizzare l'attività delle performance per ogni volume virtuale, inclusi input, output, throughput, latenza, profondità della coda e informazioni sul volume.

Di cosa hai bisogno

- La funzionalità VVol dovrebbe essere stata attivata nell'interfaccia utente Element per il cluster.
- È necessario aver creato un container di storage associato.
- Il cluster vSphere dovrebbe essere stato configurato per utilizzare la funzionalità VVol del software Element.
- È necessario aver creato almeno una macchina virtuale in vSphere.

Fasi

1. Fare clic su **VVol** > **volumi virtuali**.

   Vengono visualizzate le informazioni relative a tutti i volumi virtuali attivi.

2. Fare clic sull'icona **Actions** del volume virtuale che si desidera esaminare.
3. Nel menu visualizzato, selezionare **Visualizza dettagli**.

Dettagli

La pagina Virtual Volumes (volumi virtuali) della scheda VVols (volumi virtuali) fornisce informazioni su ciascun volume virtuale attivo nel cluster, ad esempio l'ID del volume, lo snapshot ID, l'ID del volume virtuale padre e l'ID del volume virtuale.

- **Volume ID**: L'ID del volume sottostante.
- **Snapshot ID**: L'ID dello snapshot del volume sottostante. Il valore è 0 se il volume virtuale non rappresenta uno snapshot SolidFire.
- **Parent Virtual Volume ID**: L'ID del volume virtuale del volume virtuale padre. Se l'ID è pari a zero, il volume virtuale è indipendente senza alcun collegamento a un elemento padre.
- **Virtual Volume ID**: UUID del volume virtuale.
- **Name** (Nome): Il nome assegnato al volume virtuale.
- **Storage Container**: Il container di storage proprietario del volume virtuale.
- **Guest OS Type**: Sistema operativo associato al volume virtuale.
- **Virtual Volume Type**: Il tipo di volume virtuale: Config, Data, Memory, Swap o Other.

- **Access**: Le autorizzazioni di lettura/scrittura assegnate al volume virtuale.
- **Size**: Dimensione del volume virtuale in GB o GiB.
- **Snapshot**: Il numero di snapshot associati. Fare clic sul numero per il collegamento ai dettagli dell'istantanea.
- **Min IOPS**: Impostazione minima di QoS IOPS del volume virtuale.
- **Massimo IOPS**: Impostazione massima di QoS IOPS del volume virtuale.
- **Burst IOPS**: Impostazione massima di qualità del burst del volume virtuale.
- **VMW_VMID**: Le informazioni nei campi che precedono "VMW_" sono definite da VMware.
- **Create Time** (ora di creazione): L'ora in cui è stata completata l'attività di creazione del volume virtuale.

Dettagli dei singoli volumi virtuali

La pagina Virtual Volumes (volumi virtuali) della scheda Vols (volumi virtuali) fornisce le seguenti informazioni sul volume virtuale quando si seleziona un singolo volume virtuale e ne visualizza i dettagli.

- **VMW_XXX**: Le informazioni nei campi con la dicitura "VMW_" sono definite da VMware.
- **Parent Virtual Volume ID**: L'ID del volume virtuale del volume virtuale padre. Se l'ID è pari a zero, il volume virtuale è indipendente senza alcun collegamento a un elemento padre.
- **Virtual Volume ID**: UUID del volume virtuale.
- **Virtual Volume Type**: Il tipo di volume virtuale: Config, Data, Memory, Swap o Other.
- **Volume ID**: L'ID del volume sottostante.
- **Access**: Le autorizzazioni di lettura/scrittura assegnate al volume virtuale.
- **Nome account**: Nome dell'account contenente il volume.
- **Gruppi di accesso**: Gruppi di accesso al volume associati.
- **Total Volume Size**: Capacità totale fornita in byte.
- **Blocchi diversi da zero**: Numero totale di blocchi da 4 KiB con dati dopo il completamento dell'ultima operazione di garbage collection.
- **Zero Blocks**: Numero totale di blocchi da 4 KiB senza dati dopo il completamento dell'ultimo round dell'operazione di garbage collection.
- **Snapshot**: Il numero di snapshot associati. Fare clic sul numero per il collegamento ai dettagli dell'istantanea.
- **Min IOPS**: Impostazione minima di QoS IOPS del volume virtuale.
- **Massimo IOPS**: Impostazione massima di QoS IOPS del volume virtuale.
- **Burst IOPS**: Impostazione massima di qualità del burst del volume virtuale.
- **Enable 512**: Poiché i volumi virtuali utilizzano sempre l'emulazione delle dimensioni dei blocchi da 512 byte, il valore è sempre sì.
- **Volumes paired** (volumi associati): Indica se un volume è associato.
- **Create Time** (ora di creazione): L'ora in cui è stata completata l'attività di creazione del volume virtuale.
- **Dimensione blocchi**: Dimensione dei blocchi sul volume.
- **Unaligned Scritture**: Per i volumi 512e, il numero di operazioni di scrittura che non si trovavano su un confine di settore 4k. Un numero elevato di scritture non allineate potrebbe indicare un allineamento errato delle partizioni.

- **Letture non allineate**: Per i volumi 512e, il numero di operazioni di lettura che non si trovavano su un confine di settore 4k. Un numero elevato di letture non allineate potrebbe indicare un allineamento errato delle partizioni.
- **ScsiEUIDeviceID**: Identificatore univoco globale del dispositivo SCSI per il volume nel formato a 16 byte basato su EUI-64.
- **ScsiNAADeviceID**: Identificatore univoco globale del dispositivo SCSI per il volume in formato NAA IEEE Registered Extended.
- **Attributes**: Elenco delle coppie nome-valore nel formato oggetto JSON.

Eliminare un volume virtuale

Sebbene i volumi virtuali debbano essere sempre cancellati dal VMware Management Layer, la funzionalità di eliminazione dei volumi virtuali è attivata dall'interfaccia utente di Element. Eliminare un volume virtuale dall'interfaccia utente di Element solo quando è assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire.

1. Selezionare **VVol** > **volumi virtuali**.
2. Fare clic sull'icona Actions (azioni) per il volume virtuale che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).

> È necessario eliminare un volume virtuale dal livello di gestione VMware per assicurarsi che il volume virtuale sia correttamente slegato prima dell'eliminazione. Eliminare un volume virtuale dall'interfaccia utente di Element solo quando è assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire. Se si elimina un volume virtuale dall'interfaccia utente di Element, il volume viene eliminato immediatamente.

4. Confermare l'azione.
5. Aggiornare l'elenco dei volumi virtuali per confermare che il volume virtuale è stato rimosso.
6. **Opzionale**: Selezionare **Reporting** > **Event Log** per confermare che l'eliminazione è stata eseguita correttamente.

Gestire i container di storage

Un container di storage è una rappresentazione del datastore vSphere creata su un cluster che esegue il software Element.

I container di storage vengono creati e legati agli account NetApp Element. Un container di storage creato sullo storage Element viene visualizzato come datastore vSphere in vCenter ed ESXi. I container di storage non allocano spazio nello storage degli elementi. Vengono semplicemente utilizzati per associare logicamente i volumi virtuali.

È supportato un massimo di quattro container di storage per cluster. Per abilitare la funzionalità VVol, è necessario almeno un container di storage.

Creare un container di storage

È possibile creare contenitori di storage nell'interfaccia utente di Element e rilevarli in vCenter. È necessario

creare almeno un container di storage per iniziare il provisioning delle macchine virtuali con supporto Vol.

Prima di iniziare, attivare la funzionalità VVol nell'interfaccia utente Element per il cluster.

Fasi

1. Selezionare **VVol** > **Storage Containers**.
2. Fare clic sul pulsante **Create Storage Containers** (Crea container di storage).
3. Inserire le informazioni sul contenitore di storage nella finestra di dialogo **Crea un nuovo contenitore di storage**:
   a. Immettere un nome per il contenitore di storage.
   b. Configurare i segreti di initiator e target per CHAP.

      Lasciare vuoti i campi CHAP Settings (Impostazioni CHAP) per generare automaticamente i segreti.

   c. Fare clic sul pulsante **Create Storage Container** (Crea contenitore di storage).
4. Verificare che il nuovo contenitore di storage venga visualizzato nell'elenco nella sottoscheda **Storage Containers**.

   Poiché un ID account NetApp Element viene creato automaticamente e assegnato al container di storage, non è necessario creare manualmente un account.

Visualizzare i dettagli del container di storage

Nella pagina Storage Containers della scheda VVol, è possibile visualizzare le informazioni relative a tutti i container di storage attivi nel cluster.

- **Account ID**: L'ID dell'account NetApp Element associato al container di storage.
- **Name**: Il nome del contenitore di storage.
- **Status**: Lo stato del contenitore di storage. Valori possibili:
  - Attivo: Il contenitore di storage è in uso.
  - Bloccato: Il contenitore di storage è bloccato.
- **PE Type**: Il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile per il software Element).
- **Storage Container ID**: UUID del container di storage del volume virtuale.
- **Active Virtual Volumes** (volumi virtuali attivi): Il numero di volumi virtuali attivi associati al container di storage.

Visualizzare i dettagli dei singoli container di storage

È possibile visualizzare le informazioni sul contenitore di storage per un singolo contenitore selezionandole dalla pagina Storage Containers nella scheda VVols.

- **Account ID**: L'ID dell'account NetApp Element associato al container di storage.
- **Name**: Il nome del contenitore di storage.
- **Status**: Lo stato del contenitore di storage. Valori possibili:
  - Attivo: Il contenitore di storage è in uso.

◦ Bloccato: Il contenitore di storage è bloccato.

- **CHAP Initiator Secret**: Il segreto CHAP unico per l'iniziatore.
- **CHAP Target Secret**: Il segreto CHAP unico per il target.
- **Storage Container ID**: UUID del container di storage del volume virtuale.
- **Protocol Endpoint Type** (tipo endpoint protocollo): Indica il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile).

Modificare un container di storage

È possibile modificare l'autenticazione CHAP del container di storage nell'interfaccia utente di Element.

1. Selezionare **VVol** > **Storage Containers**.
2. Fare clic sull'icona **azioni** del contenitore di storage che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. In Impostazioni CHAP, modificare le credenziali Initiator Secret e Target Secret utilizzate per l'autenticazione.

   Se non si modificano le credenziali CHAP Settings, queste rimangono invariate. Se i campi delle credenziali vengono vuoti, il sistema genera automaticamente nuovi segreti.

5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un contenitore di storage

È possibile eliminare i contenitori di storage dall'interfaccia utente di Element.

Di cosa hai bisogno

Assicurarsi che tutte le macchine virtuali siano state rimosse dal datastore Vol.

Fasi

1. Selezionare **VVol** > **Storage Containers**.
2. Fare clic sull'icona **azioni** del contenitore di storage che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.
5. Aggiornare l'elenco dei contenitori di storage nella sottoscheda **Storage Containers** per confermare che il contenitore di storage è stato rimosso.

Endpoint del protocollo

Gli endpoint del protocollo sono access point utilizzati da un host per gestire lo storage in un cluster che esegue il software NetApp Element. Gli endpoint del protocollo non possono essere cancellati o modificati da un utente, non sono associati a un account e non possono essere aggiunti a un gruppo di accesso al volume.

Un cluster con software Element crea automaticamente un endpoint di protocollo per nodo di storage nel cluster. Ad esempio, un cluster di storage a sei nodi dispone di sei endpoint di protocollo mappati a ciascun host ESXi. Gli endpoint del protocollo sono gestiti dinamicamente dal software Element e vengono creati, spostati o rimossi in base alle necessità senza alcun intervento. Gli endpoint del protocollo sono la

destinazione per il multi-pathing e fungono da proxy i/o per le LUN sussidiarie. Ogni endpoint del protocollo utilizza un indirizzo SCSI disponibile, proprio come un target iSCSI standard. Gli endpoint del protocollo appaiono come un dispositivo di storage a blocco singolo (512 byte) nel client vSphere, ma questo dispositivo di storage non è disponibile per la formattazione o l'utilizzo come storage.

ISCSI è l'unico protocollo supportato. Il protocollo Fibre Channel non è supportato.

Dettagli degli endpoint del protocollo

La pagina Protocol Endpoints (endpoint del protocollo) nella scheda VVols (VVols) fornisce informazioni sull'endpoint del protocollo.

- **ID provider primario**

  L'ID del provider dell'endpoint del protocollo primario.

- **ID provider secondario**

  L'ID del provider dell'endpoint del protocollo secondario.

- **ID endpoint del protocollo**

  UUID dell'endpoint del protocollo.

- **Protocol Endpoint state (Stato endpoint protocollo)**

  Lo stato dell'endpoint del protocollo. I valori possibili sono i seguenti:

  - Attivo: L'endpoint del protocollo è in uso.
  - Start: L'endpoint del protocollo è in fase di avvio.
  - Failover: Si è verificato un failover dell'endpoint del protocollo.
  - Riservato: L'endpoint del protocollo è riservato.

- **Tipo di provider**

  Il tipo di provider dell'endpoint del protocollo. I valori possibili sono i seguenti:

  - Primario
  - Secondario

- **SCSI NAA DEVICE ID** (ID DISPOSITIVO NAA SCSI)

  Identificatore univoco globale del dispositivo SCSI per l'endpoint del protocollo in NAA IEEE Registered Extended Format.

Associazioni

Per eseguire operazioni di i/o con un volume virtuale, un host ESXi deve prima associare il volume virtuale.

Il cluster SolidFire sceglie un endpoint del protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint del protocollo e restituisce il binding all'host ESXi. Una volta eseguito il bound, l'host ESXi può eseguire operazioni di i/o con il volume virtuale associato.

Dettagli sui binding

La pagina binding della scheda VVol fornisce informazioni di binding su ciascun volume virtuale.

Vengono visualizzate le seguenti informazioni:

- **ID host**

  UUID dell'host ESXi che ospita volumi virtuali ed è noto al cluster.

- **ID endpoint del protocollo**

  ID endpoint del protocollo corrispondenti a ciascun nodo del cluster SolidFire.

- **Protocol Endpoint in Band ID**

  L'ID del dispositivo NAA SCSI dell'endpoint del protocollo.

- **Protocol Endpoint Type** (tipo di endpoint del protocollo)

  Il tipo di endpoint del protocollo.

- **VVol Binding ID**

  UUID di binding del volume virtuale.

- **ID volume**

  UUID (Universally Unique Identifier) del volume virtuale.

- **VVol ID secondario**

  L'ID secondario del volume virtuale che è un ID LUN di secondo livello SCSI.

Dettagli host

La pagina host della scheda VVols fornisce informazioni sugli host VMware ESXi che ospitano volumi virtuali.

Vengono visualizzate le seguenti informazioni:

- **ID host**

  UUID dell'host ESXi che ospita volumi virtuali ed è noto al cluster.

- **Indirizzo host**

  L'indirizzo IP o il nome DNS dell'host ESXi.

- * Binding*

  ID di binding per tutti i volumi virtuali associati all'host ESXi.

- **ID cluster ESX**

L'ID del cluster host vSphere o il GUID vCenter.

- **IQN iniziatore**

  IQN iniziatore per l'host del volume virtuale.

- **ID endpoint del protocollo SolidFire**

  Endpoint del protocollo attualmente visibili all'host ESXi.

Lavorare con gli iniziatori e i gruppi di accesso ai volumi

È possibile utilizzare gli iniziatori iSCSI o gli iniziatori Fibre Channel per accedere ai volumi definiti all'interno dei gruppi di accesso ai volumi.

È possibile creare gruppi di accesso mappando gli IQN degli iniziatori iSCSI o le WWPN Fibre Channel in un insieme di volumi. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza richiedere l'autenticazione CHAP.

Esistono due tipi di metodi di autenticazione CHAP:

- Autenticazione CHAP a livello di account: È possibile assegnare l'autenticazione CHAP per l'account.
- Autenticazione CHAP a livello di iniziatore: È possibile assegnare una destinazione CHAP univoca e segreti per iniziatori specifici senza essere associati a un singolo CHAP in un singolo account. Questa autenticazione CHAP a livello di iniziatore sostituisce le credenziali a livello di account.

Facoltativamente, con il CHAP per-initiator, è possibile applicare l'autorizzazione per initiator e l'autenticazione CHAP per-initiator. Queste opzioni possono essere definite in base all'iniziatore e un gruppo di accesso può contenere una combinazione di iniziatori con diverse opzioni.

Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso di rete Fibre Channel ai volumi del gruppo di accesso.

I gruppi di accesso ai volumi hanno i seguenti limiti:

- In un gruppo di accesso è consentito un massimo di 64 IQN o WWPN.
- Un gruppo di accesso può essere costituito da un massimo di 2000 volumi.
- Un IQN o WWPN può appartenere a un solo gruppo di accesso.
- Un singolo volume può appartenere a un massimo di quattro gruppi di accesso.

Trova ulteriori informazioni

- Creare un gruppo di accesso al volume
- Aggiungere volumi a un gruppo di accesso
- Rimuovere i volumi da un gruppo di accesso
- Creare un iniziatore
- Modificare un iniziatore
- Aggiungere un singolo iniziatore a un gruppo di accesso al volume

- Aggiungere più iniziatori a un gruppo di accesso al volume
- Rimuovere gli iniziatori da un gruppo di accesso
- Eliminare un gruppo di accesso
- Eliminare un iniziatore

Creare un gruppo di accesso al volume

È possibile creare gruppi di accesso ai volumi associando gli iniziatori a un insieme di volumi per un accesso protetto. È quindi possibile concedere l'accesso ai volumi del gruppo con un account CHAP Initiator secret e un account CHAP Secret.

Se si utilizza CHAP basato su iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso a volume, fornendo una maggiore sicurezza. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

Fasi

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic su **Create Access Group** (Crea gruppo di accesso).
3. Inserire un nome per il gruppo di accesso al volume nel campo **Nome**.
4. Aggiungere un iniziatore al gruppo di accesso al volume in uno dei seguenti modi:

Opzione	Descrizione
Aggiunta di un iniziatore Fibre Channel	a. Nella sezione Add Initiator (Aggiungi iniziatori), selezionare un iniziatore Fibre Channel esistente dall'elenco Unbound Fibre Channel Initiator (iniziatori Fibre Channel non associati). b. Fare clic su **Aggiungi iniziatore FC**. È possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo un nome iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco degli iniziatori dopo averlo creato. Un esempio del formato è il seguente: `5f:47:ac:c0:5c:74:d4:02`

Opzione	Descrizione
Aggiunta di un iniziatore iSCSI	Nella sezione Add Initiator (Aggiungi iniziatori), selezionare un iniziatore esistente dall'elenco Initiator (iniziatori). **Nota:** è possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo il nome di un iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco degli iniziatori dopo averlo creato. Un esempio del formato è il seguente: `iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b` È possibile trovare l'IQN iniziatore per ciascun volume selezionando **View Details** (Visualizza dettagli) nel menu Actions (azioni) del volume nell'elenco **Management** > **Volumes** > **Active** (Gestione* > **volumi** > **attivo**). Quando si modifica un iniziatore, è possibile impostare l'attributo requiredCHAP su True, che consente di impostare il segreto dell'iniziatore di destinazione. Per ulteriori informazioni, vedere informazioni API sul metodo ModifyInitator API. "Gestire lo storage con l'API Element"

5. **Opzionale:** aggiungere altri iniziatori secondo necessità.
6. In Add Volumes (Aggiungi volumi), selezionare un volume dall'elenco **Volumes** (volumi).

   Il volume viene visualizzato nell'elenco **Attached Volumes** (volumi collegati).
7. **Opzionale:** aggiungere altri volumi in base alle esigenze.
8. Fare clic su **Create Access Group** (Crea gruppo di accesso).

Trova ulteriori informazioni

Aggiungere volumi a un gruppo di accesso

Visualizzare i dettagli dei singoli gruppi di accesso

È possibile visualizzare i dettagli di un singolo gruppo di accesso, ad esempio i volumi collegati e gli iniziatori, in un formato grafico.

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per un gruppo di accesso.
3. Fare clic su **View Details** (Visualizza dettagli).

Dettagli del gruppo di accesso al volume

La pagina gruppi di accesso nella scheda Gestione fornisce informazioni sui gruppi di accesso ai volumi.

Vengono visualizzate le seguenti informazioni:

- **ID**: L'ID generato dal sistema per il gruppo di accesso.
- **Name** (Nome): Il nome assegnato al gruppo di accesso al momento della creazione.
- **Active Volumes** (volumi attivi): Il numero di volumi attivi nel gruppo di accesso.
- **Compressione**: Il punteggio di efficienza della compressione per il gruppo di accesso.
- **Deduplica**: Il punteggio di efficienza della deduplica per il gruppo di accesso.
- **Thin Provisioning**: Il punteggio di efficienza del thin provisioning per il gruppo di accesso.
- **Efficienza complessiva**: Il punteggio di efficienza globale per il gruppo di accesso.
- **Initiator**: Numero di iniziatori connessi al gruppo di accesso.

Aggiungere volumi a un gruppo di accesso

È possibile aggiungere volumi a un gruppo di accesso al volume. Ciascun volume può appartenere a più di un gruppo di accesso al volume; è possibile visualizzare i gruppi a cui appartiene ciascun volume nella pagina **Active** Volumes.

È inoltre possibile utilizzare questa procedura per aggiungere volumi a un gruppo di accesso ai volumi Fibre Channel.

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso a cui si desidera aggiungere volumi.
3. Fare clic sul pulsante **Edit** (Modifica).
4. In Add Volumes (Aggiungi volumi), selezionare un volume dall'elenco **Volumes** (volumi).

   È possibile aggiungere altri volumi ripetendo questo passaggio.

5. Fare clic su **Save Changes** (Salva modifiche).

Rimuovere i volumi da un gruppo di accesso

Quando si rimuove un volume da un gruppo di accesso, il gruppo non ha più accesso a tale volume.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato qualsiasi modifica alle impostazioni dell'iniziatore e del cluster.

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona Actions (azioni) per il gruppo di accesso da cui si desidera rimuovere i volumi.
3. Fare clic su **Edit** (Modifica).
4. In Add Volumes (Aggiungi volumi) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **Attached Volumes** (volumi collegati).
5. Selezionare il volume che si desidera rimuovere dall'elenco e fare clic sull'icona **x** per rimuoverlo dall'elenco.

È possibile rimuovere più volumi ripetendo questo passaggio.

6. Fare clic su **Save Changes** (Salva modifiche).

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnarli alias.

È inoltre possibile assegnare attributi CHAP basati su initator utilizzando una chiamata API. Per aggiungere un nome account CHAP e le credenziali per ogni iniziatore, è necessario utilizzare `CreateInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP. L'accesso initiator può essere limitato a una o più VLAN specificando uno o più virtualNetworkID tramite `CreateInitiators` e. `ModifyInitiators` Chiamate API. Se non viene specificata alcuna rete virtuale, l'iniziatore può accedere a tutte le reti.

Per ulteriori informazioni, vedere le informazioni di riferimento API."Gestire lo storage con l'API Element"

Fasi

1. Fare clic su **Gestione** > **iniziatori**.
2. Fare clic su **Crea iniziatore**.
3. Eseguire la procedura per creare un singolo iniziatore o più iniziatori:

Opzione	Fasi
Creare un singolo iniziatore	a. Fare clic su **Crea un singolo iniziatore**. b. Immettere l'IQN o il WWPN dell'iniziatore nel campo **IQN/WWPN**. c. Immettere un nome descrittivo per l'iniziatore nel campo **Alias**. d. Fare clic su **Crea iniziatore**.
Creare più iniziatori	a. Fare clic su **creazione di iniziatori in blocco**. b. Inserire un elenco di IQN o WWPN nella casella di testo. c. Fare clic su **Aggiungi iniziatori**. d. Scegliere un iniziatore dall'elenco risultante e fare clic sull'icona Aggiungi corrispondente nella colonna **Alias** per aggiungere un alias per l'iniziatore. e. Fare clic sul segno di spunta per confermare il nuovo alias. f. Fare clic su **Create initiator** (Crea iniziatori).

Modificare un iniziatore

È possibile modificare l'alias di un iniziatore esistente o aggiungere un alias se non ne esiste già uno.

Per aggiungere un nome account CHAP e le credenziali per ogni iniziatore, è necessario utilizzare `ModifyInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP.

Vedere "Gestire lo storage con l'API Element".

Fasi

1. Fare clic su **Gestione** > **iniziatori**.
2. Fare clic sull'icona Actions (azioni) per l'iniziatore che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Inserire un nuovo alias per l'iniziatore nel campo **Alias**.
5. Fare clic su **Save Changes** (Salva modifiche).

Aggiungere un singolo iniziatore a un gruppo di accesso al volume

È possibile aggiungere un iniziatore a un gruppo di accesso a un volume esistente.

Quando si aggiunge un iniziatore a un gruppo di accesso al volume, l'iniziatore ha accesso a tutti i volumi in quel gruppo di accesso al volume.

È possibile trovare l'iniziatore per ciascun volume facendo clic sull'icona Actions (azioni) e selezionando **View Details** (Visualizza dettagli) per il volume nell'elenco Active Volumes (volumi attivi).

Se si utilizza CHAP basato su iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso a volume, fornendo una maggiore sicurezza. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

Fasi

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera modificare.
3. Fare clic su **Edit** (Modifica).
4. Per aggiungere un iniziatore Fibre Channel al gruppo di accesso al volume, attenersi alla seguente procedura:

   a. In Add Initiator (Aggiungi iniziatori), selezionare un iniziatore Fibre Channel esistente dall'elenco **Unbound Fibre Channel Initiator** (iniziatori Fibre Channel non associati).

   b. Fare clic su **Aggiungi iniziatore FC**.

   È possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo un nome iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco **initiator** dopo averlo creato.

   Un esempio del formato è il seguente:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Per aggiungere un iSCSI Initiator al gruppo di accesso al volume, in Add Initiator (Aggiungi iniziatori), selezionare un iniziatore esistente dall'elenco **Initiator** (iniziatori).

   È possibile creare un iniziatore durante questa fase facendo clic sul collegamento **Create Initiator** (Crea iniziatore), immettendo un nome iniziatore e facendo clic su **Create** (Crea). Il sistema aggiunge automaticamente l'iniziatore all'elenco **initiator** dopo averlo creato.

Il formato accettato di un IQN iniziatore è il seguente: iqn.yyyy-mm, in cui y e m sono cifre, seguito da testo che deve contenere solo cifre, caratteri alfabetici minuscoli, un punto (.), due punti (:) o trattino (-).

Un esempio del formato è il seguente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

È possibile trovare l'IQN iniziatore per ciascun volume dalla pagina **Management** > **Volumes** Active Volumes facendo clic sull'icona Actions (azioni) e selezionando **View Details** (Visualizza dettagli) per il volume.

6. Fare clic su **Save Changes** (Salva modifiche).

Aggiungere più iniziatori a un gruppo di accesso al volume

È possibile aggiungere più iniziatori a un gruppo di accesso a un volume esistente per consentire l'accesso ai volumi nel gruppo di accesso a un volume con o senza richiedere l'autenticazione CHAP.

Quando si aggiungono gli iniziatori a un gruppo di accesso al volume, gli iniziatori hanno accesso a tutti i volumi in quel gruppo di accesso al volume.

È possibile trovare l'iniziatore per ciascun volume facendo clic sull'icona Actions (azioni), quindi su **View Details** (Visualizza dettagli) per il volume nell'elenco Active Volumes (volumi attivi).

È possibile aggiungere più iniziatori a un gruppo di accesso a un volume esistente per consentire l'accesso ai volumi e assegnare credenziali CHAP univoche per ciascun iniziatore all'interno di tale gruppo di accesso a un volume. Questa opzione consente di applicare questa opzione ai gruppi di accesso ai volumi già esistenti.

È possibile assegnare attributi CHAP basati su initator utilizzando una chiamata API. Per aggiungere un nome account CHAP e le credenziali per ogni iniziatore, è necessario utilizzare la chiamata API ModifyInitator per rimuovere e aggiungere gli attributi e l'accesso CHAP.

Per ulteriori informazioni, vedere "Gestire lo storage con l'API Element".

Fasi

1. Fare clic su **Gestione** > **iniziatori**.
2. Selezionare gli iniziatori che si desidera aggiungere a un gruppo di accesso.
3. Fare clic sul pulsante **azioni in blocco**.
4. Fare clic su **Add to Volume Access Group** (Aggiungi a gruppo di accesso volume).
5. Nella finestra di dialogo Add to Volume Access Group (Aggiungi a gruppo di accesso al volume), selezionare un gruppo di accesso dall'elenco **Volume Access Group** (Gruppo di accesso al volume).
6. Fare clic su **Aggiungi**.

Rimuovere gli iniziatori da un gruppo di accesso

Quando si rimuove un iniziatore da un gruppo di accesso, non sarà più possibile accedere ai volumi di tale gruppo di accesso al volume. Il normale accesso dell'account

al volume non viene interrotto.

La modifica delle impostazioni CHAP in un account o la rimozione di iniziatori o volumi da un gruppo di accesso può causare la perdita improvvisa dell'accesso ai volumi da parte degli iniziatori. Per verificare che l'accesso al volume non venga perso in modo imprevisto, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica di un account o di un gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver apportato qualsiasi modifica alle impostazioni dell'iniziatore e del cluster.

Fasi

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera rimuovere.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. In Add Initiator (Aggiungi iniziatori) nella finestra di dialogo **Edit Volume Access Group** (Modifica gruppo di accesso volume), fare clic sulla freccia nell'elenco **Initiators** (iniziatori).
5. Selezionare l'icona x per ciascun iniziatore che si desidera rimuovere dal gruppo di accesso.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminare un gruppo di accesso

È possibile eliminare un gruppo di accesso quando non è più necessario. Non è necessario eliminare gli ID iniziatore e gli ID volume dal gruppo di accesso al volume prima di eliminare il gruppo. Una volta eliminato il gruppo di accesso, l'accesso di gruppo ai volumi viene interrotto.

1. Fare clic su **Gestione** > **gruppi di accesso**.
2. Fare clic sull'icona **azioni** del gruppo di accesso che si desidera eliminare.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Per eliminare anche gli iniziatori associati a questo gruppo di accesso, selezionare la casella di controllo **Delete initiator in this access group** (Elimina iniziatori in questo gruppo di accesso).
5. Confermare l'azione.

Eliminare un iniziatore

È possibile eliminare un iniziatore una volta che non è più necessario. Quando si elimina un iniziatore, il sistema lo rimuove da qualsiasi gruppo di accesso al volume associato. Tutte le connessioni che utilizzano l'iniziatore rimangono valide fino al ripristino della connessione.

Fasi

1. Fare clic su **Gestione** > **iniziatori**.
2. Eseguire la procedura per eliminare un singolo iniziatore o più iniziatori:

Opzione	Fasi
Eliminare un singolo iniziatore	a. Fare clic sull'icona **azioni** dell'iniziatore che si desidera eliminare. b. Fare clic su **Delete** (Elimina). c. Confermare l'azione.
Eliminare più iniziatori	a. Selezionare le caselle di controllo accanto agli iniziatori che si desidera eliminare. b. Fare clic sul pulsante **azioni in blocco**. c. Nel menu visualizzato, selezionare **Delete** (Elimina). d. Confermare l'azione.

Proteggi i tuoi dati

Il software NetApp Element consente di proteggere i dati in diversi modi grazie a funzionalità come snapshot per singoli volumi o gruppi di volumi, replica tra cluster e volumi eseguiti su Element e replica sui sistemi ONTAP.

- **Istantanee**

  La protezione dei dati solo Snapshot replica i dati modificati in specifici punti di tempo in un cluster remoto. Vengono replicati solo gli snapshot creati nel cluster di origine. Le scritture attive dal volume di origine non lo sono.

  Utilizzare le snapshot dei volumi per la protezione dei dati

- **Replica remota tra cluster e volumi eseguiti su Element**

  È possibile replicare i dati del volume in modo sincrono o asincrono da uno dei cluster di una coppia di cluster, entrambi in esecuzione su Element per scenari di failover e failback.

  Eseguire la replica remota tra cluster che eseguono il software NetApp Element

- **Replica tra cluster Element e ONTAP con tecnologia SnapMirror**

  Con la tecnologia NetApp SnapMirror, è possibile replicare le snapshot acquisite utilizzando Element to ONTAP per scopi di disaster recovery. In una relazione SnapMirror, Element è un endpoint e ONTAP è l'altro.

  Utilizzare la replica SnapMirror tra cluster Element e ONTAP

- **Eseguire il backup e il ripristino dei volumi dagli archivi di oggetti SolidFire, S3 o Swift**

  È possibile eseguire il backup e il ripristino dei volumi su altri storage SolidFire, nonché su archivi di oggetti secondari compatibili con Amazon S3 o OpenStack Swift.

  Eseguire il backup e il ripristino dei volumi in archivi a oggetti SolidFire, S3 o Swift

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Utilizzare le snapshot dei volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume. È possibile creare un'istantanea di un volume e utilizzarla in un secondo momento se è necessario riportare un volume nello stato in cui si trovava al momento della creazione dell'istantanea.

Gli snapshot sono simili ai cloni dei volumi. Tuttavia, le snapshot sono semplicemente repliche dei metadati del volume, pertanto non è possibile montarle o scriverle. La creazione di uno snapshot di volume richiede anche solo una piccola quantità di risorse e spazio di sistema, rendendo la creazione dello snapshot più rapida rispetto alla clonazione.

È possibile creare un'istantanea di un singolo volume o di un set di volumi.

Facoltativamente, replicare gli snapshot in un cluster remoto e utilizzarli come copia di backup del volume. In questo modo, è possibile eseguire il rollback di un volume a un punto specifico utilizzando lo snapshot replicato. In alternativa, è possibile creare un clone di un volume da uno snapshot replicato.

Trova ulteriori informazioni

- Utilizzare snapshot di singoli volumi per la protezione dei dati
- Utilizzo di snapshot di gruppo per attività di protezione dei dati
- Pianificazione di uno snapshot

Utilizzare snapshot di singoli volumi per la protezione dei dati

Uno snapshot di un volume è una copia point-in-time di un volume. È possibile utilizzare un singolo volume anziché un gruppo di volumi per lo snapshot.

Trova ulteriori informazioni

- Creare un'istantanea del volume
- Modifica la conservazione delle snapshot
- Eliminazione di uno snapshot
- Clonare un volume da uno snapshot
- Eseguire il rollback di un volume in uno snapshot
- Backup di uno snapshot di volume in un archivio di oggetti Amazon S3
- Backup di uno snapshot di volume in un archivio di oggetti OpenStack Swift
- Backup di uno snapshot di volume in un cluster SolidFire

Creare un'istantanea del volume

È possibile creare uno snapshot di un volume attivo per conservare l'immagine del volume in qualsiasi momento. È possibile creare fino a 32 snapshot per un singolo

volume.

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona **Actions** del volume che si desidera utilizzare per lo snapshot.
3. Nel menu visualizzato, selezionare **Snapshot**.
4. Nella finestra di dialogo **Create Snapshot of Volume** (Crea snapshot del volume), inserire il nuovo nome dello snapshot.
5. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per assicurarsi che lo snapshot venga acquisito in replica quando il volume padre viene associato.
6. Per impostare la conservazione dello snapshot, selezionare una delle seguenti opzioni:
   - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
   - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
7. Per eseguire una singola istantanea, attenersi alla seguente procedura:
   a. Fare clic su **scatta istantanea ora**.
   b. Fare clic su**Create Snapshot** (Crea istantanea).
8. Per pianificare l'esecuzione dello snapshot in un momento successivo, attenersi alla seguente procedura:
   a. Fare clic su **Crea pianificazione snapshot**.
   b. Immettere un **nuovo nome pianificazione**.
   c. Scegliere un **tipo di pianificazione** dall'elenco.
   d. **Opzionale:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
   e. Fare clic su **Crea pianificazione**.

Trova ulteriori informazioni

Pianifica un'istantanea

Modifica la conservazione delle snapshot

È possibile modificare il periodo di conservazione di uno snapshot per controllare quando o se il sistema elimina gli snapshot. Il periodo di conservazione specificato inizia quando si inserisce il nuovo intervallo. Quando si imposta un periodo di conservazione, è possibile selezionare un periodo che inizia all'ora corrente (la conservazione non viene calcolata dall'ora di creazione dello snapshot). È possibile specificare intervalli in minuti, ore e giorni.

Fasi

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea che si desidera modificare.
3. Nel menu visualizzato, fare clic su **Edit** (Modifica).
4. **Opzionale:** selezionare la casella di controllo**Includi snapshot nella replica quando accoppiato** per assicurarsi che lo snapshot venga acquisito nella replica quando il volume padre viene associato.

5. **Opzionale:** selezionare un'opzione di conservazione per lo snapshot:
   - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
   - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per selezionare il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminare uno snapshot

È possibile eliminare uno snapshot di volume da un cluster di storage che esegue il software Element. Quando si elimina uno snapshot, il sistema lo rimuove immediatamente.

È possibile eliminare gli snapshot replicati dal cluster di origine. Se uno snapshot viene sincronizzato con il cluster di destinazione quando lo si elimina, la replica di sincronizzazione viene completata e lo snapshot viene cancellato dal cluster di origine. Lo snapshot non viene cancellato dal cluster di destinazione.

È inoltre possibile eliminare dal cluster di destinazione le snapshot replicate nella destinazione. Lo snapshot cancellato viene conservato in un elenco di snapshot cancellati sulla destinazione fino a quando il sistema non rileva l'eliminazione dello snapshot sul cluster di origine. Quando la destinazione rileva l'eliminazione dello snapshot di origine, la destinazione interrompe la replica dello snapshot.

Quando si elimina uno snapshot dal cluster di origine, lo snapshot del cluster di destinazione non viene influenzato (anche il contrario è vero).

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sull'icona **azioni** per lo snapshot che si desidera eliminare.
3. Nel menu visualizzato, selezionare **Delete** (Elimina).
4. Confermare l'azione.

Clonare un volume da uno snapshot

È possibile creare un nuovo volume da uno snapshot di un volume. In questo modo, il sistema utilizza le informazioni di snapshot per clonare un nuovo volume utilizzando i dati contenuti nel volume al momento della creazione dello snapshot. Questo processo memorizza le informazioni relative ad altri snapshot del volume nel volume appena creato.

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot che si desidera utilizzare per il clone del volume.
3. Nel menu visualizzato, fare clic su **Clone Volume from Snapshot** (Clona volume da snapshot).
4. Inserire un **Nome volume** nella finestra di dialogo **Clone Volume from Snapshot** (Copia volume da snapshot).
5. Selezionare **Total Size** (dimensione totale) e le unità di misura per il nuovo volume.
6. Selezionare un tipo **Access** per il volume.
7. Selezionare un **account** dall'elenco da associare al nuovo volume.
8. Fare clic su **Avvia clonazione**.

Eseguire il rollback di un volume in uno snapshot

È possibile eseguire il rollback di un volume a uno snapshot precedente in qualsiasi momento. In questo modo vengono ripristinate le modifiche apportate al volume dalla creazione dello snapshot.

Fasi

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, selezionare **Rollback Volume to Snapshot** (Ripristina volume in snapshot).
4. **Opzionale:** per salvare lo stato corrente del volume prima di eseguire il rollback allo snapshot:
   a. Nella finestra di dialogo **Rollback to Snapshot**, selezionare **Save the current state as a snapshot** (Salva stato corrente del volume come snapshot).
   b. Immettere un nome per il nuovo snapshot.
5. Fare clic su **Rollback Snapshot**.

Eseguire il backup di uno snapshot di un volume

È possibile utilizzare la funzione di backup integrata per eseguire il backup di uno snapshot di un volume. È possibile eseguire il backup delle snapshot da un cluster SolidFire a un archivio di oggetti esterno o a un altro cluster SolidFire. Quando si esegue il backup di uno snapshot in un archivio di oggetti esterno, è necessario disporre di una connessione all'archivio di oggetti che consenta le operazioni di lettura/scrittura.

- "Eseguire il backup di uno snapshot di volume in un archivio di oggetti Amazon S3"
- "Eseguire il backup di uno snapshot di volume in un archivio di oggetti OpenStack Swift"
- "Eseguire il backup di uno snapshot di volume in un cluster SolidFire"

Eseguire il backup di uno snapshot di volume in un archivio di oggetti Amazon S3

Puoi eseguire il backup delle istantanee di SolidFire in archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su**Data Protection** > **Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Integrated Backup** sotto **Backup in**, selezionare **S3**.
5. Selezionare un'opzione in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
7. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
8. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).

9. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
10. **Opzionale**: Inserire un nametag da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di uno snapshot di volume in un archivio di oggetti OpenStack Swift

È possibile eseguire il backup degli snapshot SolidFire in archivi di oggetti secondari compatibili con OpenStack Swift.

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sull'icona **Actions** per l'istantanea di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup in**, selezionare **Swift**.
5. Selezionare un'opzione in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un **URL** da utilizzare per accedere all'archivio di oggetti.
7. Inserire un **Nome utente** per l'account.
8. Inserire la **Authentication Key** dell'account.
9. Inserire il **container** in cui memorizzare il backup.
10. **Opzionale**: Inserire un **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di uno snapshot di volume in un cluster SolidFire

È possibile eseguire il backup delle snapshot dei volumi che risiedono su un cluster SolidFire in un cluster SolidFire remoto.

Assicurarsi che i cluster di origine e di destinazione siano associati.

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona **Actions** del volume di destinazione.
3. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
4. Nella finestra di dialogo **Ripristino integrato** sotto **Ripristina da**, selezionare **SolidFire**.
5. Selezionare un formato dati in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).

7. Copiare la chiave dalla casella **Bulk Volume Write Key** negli Appunti.
8. Nel cluster di origine, fare clic su **Data Protection** > **Snapshot**.
9. Fare clic sull'icona Actions (azioni) per lo snapshot che si desidera utilizzare per il backup.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo**Backup integrato** sotto **Backup in**, selezionare **SolidFire**.
12. Selezionare lo stesso formato di dati selezionato in precedenza nel campo **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Nel campo **Bulk Volume Write Key** (chiave di scrittura volume in blocco), incollare la chiave generata in precedenza nel cluster di destinazione.
17. Fare clic su **Avvia lettura**.

Utilizzo di snapshot di gruppo per attività di protezione dei dati

È possibile creare un'istantanea di gruppo di un set correlato di volumi per conservare una copia point-in-time dei metadati per ciascun volume. È possibile utilizzare lo snapshot di gruppo in futuro come backup o rollback per ripristinare lo stato del gruppo di volumi a uno stato precedente.

Trova ulteriori informazioni

- Creare un'istantanea di gruppo
- Modificare le snapshot di gruppo
- Modificare i membri dell'istantanea del gruppo
- Eliminare uno snapshot di gruppo
- Eseguire il rollback dei volumi in uno snapshot di gruppo
- Clonare più volumi
- Clonare più volumi da uno snapshot di gruppo

Dettagli snapshot di gruppo

La pagina Group Snapshots (istantanee gruppo) della scheda Data Protection (protezione dati) fornisce informazioni sulle istantanee del gruppo.

- **ID**

  L'ID generato dal sistema per lo snapshot di gruppo.

- **UUID**

  L'ID univoco dello snapshot di gruppo.

- **Nome**

Nome definito dall'utente per lo snapshot di gruppo.

- **Ora di creazione**

  L'ora in cui è stata creata l'istantanea del gruppo.

- **Stato**

  Lo stato corrente dello snapshot. Valori possibili:

  - Preparazione: Lo snapshot è in fase di preparazione e non è ancora scrivibile.
  - Fatto: Questo snapshot ha terminato la preparazione ed è ora utilizzabile.
  - Attivo: Lo snapshot è il ramo attivo.

- * N. volumi*

  Il numero di volumi nel gruppo.

- **Conservare fino al**

  Il giorno e l'ora in cui lo snapshot viene cancellato.

- **Replica remota**

  Indicazione dell'attivazione o meno dello snapshot per la replica su un cluster SolidFire remoto. Valori possibili:

  - Enabled (attivato): Lo snapshot è abilitato per la replica remota.
  - Disabled (Disattivato): Lo snapshot non è abilitato per la replica remota.

Creazione di uno snapshot di gruppo

È possibile creare un'istantanea di un gruppo di volumi e una pianificazione snapshot di gruppo per automatizzare le snapshot di gruppo. Un singolo snapshot di gruppo può creare costantemente snapshot di fino a 32 volumi alla volta.

Fasi

1. Fare clic su **Management** > **Volumes**.
2. Utilizzare le caselle di controllo per selezionare più volumi per un gruppo di volumi.
3. Fare clic su **azioni in blocco**.
4. Fare clic su **Group Snapshot** (istantanea gruppo).
5. Inserire un nuovo nome di snapshot di gruppo nella finestra di dialogo Crea snapshot di gruppo dei volumi.
6. **Opzionale:** selezionare la casella di controllo **Includi ogni membro Snapshot di gruppo nella replica quando accoppiato** per assicurarsi che ogni snapshot venga acquisito nella replica quando il volume padre viene associato.
7. Selezionare un'opzione di conservazione per lo snapshot di gruppo:
   - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
   - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.

8. Per eseguire una singola istantanea, attenersi alla seguente procedura:
    a. Fare clic su **scatta snapshot di gruppo ora**.
    b. Fare clic su **Create Group Snapshot** (Crea istantanea gruppo).
9. Per pianificare l'esecuzione dello snapshot in un momento successivo, attenersi alla seguente procedura:
    a. Fare clic su **Crea pianificazione snapshot di gruppo**.
    b. Immettere un **nuovo nome pianificazione**.
    c. Selezionare un **tipo di pianificazione** dall'elenco.
    d. **Opzionale:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
    e. Fare clic su **Crea pianificazione**.

Modifica delle snapshot di gruppo

È possibile modificare le impostazioni di replica e conservazione per gli snapshot di gruppo esistenti.

1. Fare clic su **Data Protection** > **Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera modificare.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. **Opzionale:** per modificare l'impostazione di replica per lo snapshot di gruppo:
    a. Fare clic su **Edit** (Modifica) accanto a **Current Replication** (replica corrente).
    b. Selezionare la casella di controllo **include each Group Snapshot Member in Replication when paired** (Includi ogni membro Snapshot di gruppo nella replica quando viene associato) per assicurarsi che ogni snapshot venga acquisito in replica quando viene associato il volume padre.
5. **Opzionale:** per modificare l'impostazione di conservazione per lo snapshot di gruppo, selezionare una delle seguenti opzioni:
    a. Fare clic su **Edit** (Modifica) accanto a **Current retention** (conservazione corrente).
    b. Selezionare un'opzione di conservazione per lo snapshot di gruppo:
        - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
        - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Eliminazione di uno snapshot di gruppo

È possibile eliminare un'istantanea di gruppo dal sistema. Quando si elimina lo snapshot di gruppo, è possibile scegliere se tutte le snapshot associate al gruppo vengono eliminate o conservate come singole istantanee.

Se si elimina un volume o uno snapshot membro di uno snapshot di gruppo, non è più possibile eseguire il rollback allo snapshot di gruppo. Tuttavia, è possibile eseguire il rollback di ciascun volume singolarmente.

1. Fare clic su **Data Protection** > **Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot che si desidera eliminare.

3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Selezionare una delle seguenti opzioni nella finestra di dialogo di conferma:
   - Fare clic su **Delete group snapshot AND all group snapshot members** (Elimina snapshot di gruppo E tutti i membri dello snapshot di gruppo) per eliminare lo snapshot di gruppo e tutti gli snapshot dei membri.
   - Fare clic su **Mantieni membri snapshot di gruppo come singole snapshot** per eliminare lo snapshot di gruppo ma conservare tutti gli snapshot dei membri.
5. Confermare l'azione.

Eseguire il rollback dei volumi in uno snapshot di gruppo

È possibile eseguire il rollback di un gruppo di volumi in qualsiasi momento in uno snapshot di gruppo.

Quando si esegue il rollback di un gruppo di volumi, tutti i volumi del gruppo vengono ripristinati allo stato in cui si trovavano al momento della creazione dello snapshot di gruppo. Il rollback ripristina anche le dimensioni del volume alle dimensioni registrate nello snapshot originale. Se il sistema ha eliminato un volume, anche tutte le snapshot di quel volume sono state eliminate al momento della rimozione; il sistema non ripristina le snapshot del volume eliminate.

1. Fare clic su **Data Protection** > **Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera utilizzare per il rollback del volume.
3. Nel menu risultante, selezionare **Rollback Volumes to Group Snapshot** (Esegui il rollback dei volumi in Group Snapshot).
4. **Opzionale**: Per salvare lo stato corrente dei volumi prima di eseguire il rollback allo snapshot:
   a. Nella finestra di dialogo **Rollback to Snapshot**, selezionare **Save Volumes' Current state as a group snapshot** (Salva stato corrente dei volumi come snapshot di gruppo).
   b. Immettere un nome per il nuovo snapshot.
5. Fare clic su **Rollback Group Snapshot**.

Modifica dei membri dello snapshot di gruppo

È possibile modificare le impostazioni di conservazione per i membri di uno snapshot di gruppo esistente.

1. Fare clic su **Data Protection** > **Snapshot**.
2. Fare clic sulla scheda **membri**.
3. Fare clic sull'icona Actions (azioni) per il membro dello snapshot di gruppo che si desidera modificare.
4. Nel menu visualizzato, selezionare **Edit** (Modifica).
5. Per modificare l'impostazione di replica per lo snapshot, selezionare una delle seguenti opzioni:
   - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
   - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
6. Fare clic su **Save Changes** (Salva modifiche).

Clonare più volumi

È possibile creare più cloni di volume in una singola operazione per creare una copia point-in-time dei dati su un gruppo di volumi.

Quando si clonano un volume, il sistema crea uno snapshot del volume e crea un nuovo volume dai dati nello snapshot. È possibile montare e scrivere sul nuovo clone del volume. La clonazione di più volumi è un processo asincrono e richiede un tempo variabile in base alle dimensioni e al numero dei volumi clonati.

Le dimensioni del volume e il carico corrente del cluster influiscono sul tempo necessario per completare un'operazione di cloning.

Fasi

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sulla scheda **Active**.
3. Utilizzare le caselle di controllo per selezionare più volumi, creando un gruppo di volumi.
4. Fare clic su **azioni in blocco**.
5. Fare clic su **Clone** nel menu visualizzato.
6. Inserire un **nuovo prefisso nome volume** nella finestra di dialogo **Clone multiple Volumes** (Copia volumi multipli).

   Il prefisso viene applicato a tutti i volumi del gruppo.

7. **Opzionale:** selezionare un account diverso a cui appartiene il clone.

   Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

8. **Opzionale:** selezionare un metodo di accesso diverso per i volumi nel clone.

   Se non si seleziona un metodo di accesso, il sistema utilizza l'accesso al volume corrente.

9. Fare clic su **Avvia clonazione**.

Clonazione di più volumi da uno snapshot di gruppo

È possibile clonare un gruppo di volumi da uno snapshot di gruppo point-in-time. Questa operazione richiede che esista già uno snapshot di gruppo dei volumi, poiché lo snapshot di gruppo viene utilizzato come base per creare i volumi. Dopo aver creato i volumi, è possibile utilizzarli come qualsiasi altro volume del sistema.

Le dimensioni del volume e il carico corrente del cluster influiscono sul tempo necessario per completare un'operazione di cloning.

1. Fare clic su **Data Protection** > **Group Snapshot**.
2. Fare clic sull'icona Actions (azioni) per lo snapshot di gruppo che si desidera utilizzare per i cloni del volume.
3. Nel menu risultante, selezionare **Clone Volumes from Group Snapshot** (Clona volumi da snapshot di gruppo).
4. Inserire un **nuovo prefisso nome volume** nella finestra di dialogo **Clone Volumes from Group Snapshot** (Copia volumi da snapshot gruppo).

Il prefisso viene applicato a tutti i volumi creati dallo snapshot di gruppo.

5. **Opzionale:** selezionare un account diverso a cui appartiene il clone.

   Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

6. **Opzionale:** selezionare un metodo di accesso diverso per i volumi nel clone.

   Se non si seleziona un metodo di accesso, il sistema utilizza l'accesso al volume corrente.

7. Fare clic su **Avvia clonazione**.

Pianifica un'istantanea

È possibile proteggere i dati di un volume o di un gruppo di volumi programmando che le snapshot dei volumi vengano eseguite a intervalli specificati. È possibile pianificare l'esecuzione automatica di snapshot di singoli volumi o di gruppi.

Quando si configura una pianificazione snapshot, è possibile scegliere tra intervalli di tempo in base ai giorni della settimana o dei giorni del mese. È inoltre possibile specificare i giorni, le ore e i minuti prima che si verifichi l'istantanea successiva. Se il volume viene replicato, è possibile memorizzare le snapshot risultanti su un sistema di storage remoto.

Trova ulteriori informazioni

- Creare una pianificazione di snapshot
- Modificare una pianificazione di snapshot
- Eliminare una pianificazione di snapshot
- Copiare una pianificazione di snapshot

Dettagli della pianificazione di Snapshot

Nella pagina Data Protection > Schedules (protezione dati > programmi), è possibile visualizzare le seguenti informazioni nell'elenco delle pianificazioni di snapshot.

- **ID**

  L'ID generato dal sistema per lo snapshot.

- **Tipo**

  Il tipo di pianificazione. Snapshot è attualmente l'unico tipo supportato.

- **Nome**

  Il nome assegnato alla pianificazione al momento della sua creazione. I nomi delle pianificazioni di Snapshot possono contenere fino a 223 caratteri e contengono caratteri a-z, 0-9 e trattino (-).

- **Frequenza**

  La frequenza con cui viene eseguita la pianificazione. La frequenza può essere impostata in ore e minuti, settimane o mesi.

- **Ricorrente**

  Indicazione se il programma deve essere eseguito una sola volta o a intervalli regolari.

- **Pausa manuale**

  Indicazione se la pianificazione è stata messa in pausa manualmente.

- **ID volume**

  L'ID del volume utilizzato dalla pianificazione quando viene eseguita la pianificazione.

- **Ultima esecuzione**

  L'ultima volta in cui è stato eseguito il programma.

- **Stato ultima esecuzione**

  Il risultato dell'ultima esecuzione del programma. Valori possibili:

  - Successo
  - Guasto

Creare una pianificazione di snapshot

È possibile pianificare un'istantanea di uno o più volumi in modo che venga eseguita automaticamente a intervalli specificati.

Quando si configura una pianificazione snapshot, è possibile scegliere tra intervalli di tempo in base ai giorni della settimana o dei giorni del mese. È inoltre possibile creare una pianificazione ricorrente e specificare i giorni, le ore e i minuti prima che si verifichi l'istantanea successiva.

Se si pianifica l'esecuzione di uno snapshot in un periodo di tempo non divisibile di 5 minuti, lo snapshot verrà eseguito nel periodo di tempo successivo, divisibile di 5 minuti. Ad esempio, se si pianifica l'esecuzione di uno snapshot alle 12:42:00 UTC, questo verrà eseguito alle 12:45:00 UTC. Non è possibile pianificare l'esecuzione di uno snapshot a intervalli inferiori a 5 minuti.

Fasi

1. Fare clic su **Data Protection** > **Schedules**.
2. Fare clic su **Crea pianificazione**.
3. Nel campo **Volume IDS CSV**, immettere un singolo ID volume o un elenco separato da virgole di ID volume da includere nell'operazione di snapshot.
4. Immettere un nuovo nome per la pianificazione.
5. Selezionare un tipo di pianificazione e impostarla dalle opzioni fornite.
6. **Opzionale:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione dello snapshot a tempo indeterminato.
7. **Opzionale:** inserire un nome per la nuova istantanea nel campo **New Snapshot Name** (Nome nuova istantanea).

   Se si lascia il campo vuoto, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.

8. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiate** per assicurarsi che le snapshot vengano acquisite nella replica quando il volume padre viene associato.
9. Per impostare la conservazione dello snapshot, selezionare una delle seguenti opzioni:
   - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
   - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per scegliere il periodo di tempo in cui il sistema conserva lo snapshot.
10. Fare clic su **Crea pianificazione**.

Modificare una pianificazione di snapshot

È possibile modificare le pianificazioni di snapshot esistenti. Dopo la modifica, la prossima volta che la pianificazione viene eseguita, utilizza gli attributi aggiornati. Tutte le snapshot create dalla pianificazione originale rimangono nel sistema di storage.

Fasi

1. Fare clic su **Data Protection** > **Schedules**.
2. Fare clic sull'icona **azioni** relativa alla pianificazione che si desidera modificare.
3. Nel menu visualizzato, fare clic su **Edit** (Modifica).
4. Nel campo **Volume IDS CSV**, modificare l'ID di un singolo volume o l'elenco separato da virgole degli ID di volume attualmente inclusi nell'operazione di snapshot.
5. Per sospendere o riprendere la pianificazione, selezionare una delle seguenti opzioni:
   - Per mettere in pausa un programma attivo, selezionare **Sì** dall'elenco **Pausa manualmente programma**.
   - Per riprendere un programma in pausa, selezionare **No** dall'elenco **Manually Pause Schedule** (programma di pausa manuale).
6. Immettere un nome diverso per la pianificazione nel campo **New Schedule Name** (Nome nuova pianificazione), se si desidera.
7. Per modificare la pianificazione in modo che venga eseguita in giorni diversi della settimana o del mese, selezionare **tipo di pianificazione** e modificare la pianificazione dalle opzioni fornite.
8. **Opzionale:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione dello snapshot a tempo indeterminato.
9. **Opzionale:** inserire o modificare il nome del nuovo snapshot nel campo **New Snapshot Name** (Nome nuovo snapshot).

   Se si lascia il campo vuoto, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.

10. **Opzionale:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiate** per assicurarsi che le snapshot vengano acquisite nella replica quando il volume padre viene associato.
11. Per modificare l'impostazione di conservazione, selezionare una delle seguenti opzioni:
    - Fare clic su **Keep Forever** per conservare l'istantanea sul sistema a tempo indeterminato.
    - Fare clic su **Set retention period** (Imposta periodo di conservazione) e utilizzare le caselle di selezione della data per selezionare il periodo di tempo in cui il sistema conserva lo snapshot.
12. Fare clic su **Save Changes** (Salva modifiche).

Copiare una pianificazione di snapshot

È possibile copiare una pianificazione e mantenerne gli attributi correnti.

1. Fare clic su **Data Protection** > **Schedules**.
2. Fare clic sull'icona Actions (azioni) per il programma che si desidera copiare.
3. Nel menu visualizzato, fare clic su **Crea copia**.

   Viene visualizzata la finestra di dialogo **Create Schedule** (Crea pianificazione), contenente gli attributi correnti della pianificazione.

4. **Opzionale:** inserire un nome e gli attributi aggiornati per la nuova pianificazione.
5. Fare clic su **Crea pianificazione**.

Eliminare una pianificazione di snapshot

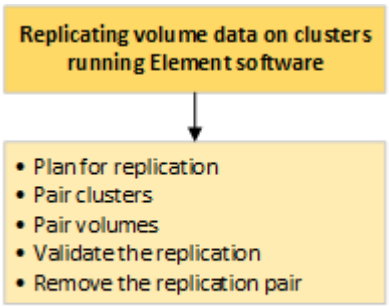
È possibile eliminare una pianificazione di snapshot. Una volta eliminata la pianificazione, non vengono eseguite snapshot pianificate in futuro. Tutte le snapshot create dalla pianificazione rimangono nel sistema di storage.

1. Fare clic su **Data Protection** > **Schedules**.
2. Fare clic sull'icona **azioni** del programma che si desidera eliminare.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Confermare l'azione.

Eseguire la replica remota tra cluster che eseguono il software NetApp Element

Per i cluster che eseguono il software Element, la replica in tempo reale consente la creazione rapida di copie remote dei dati dei volumi. È possibile associare un cluster di storage a un massimo di quattro altri cluster di storage. È possibile replicare i dati del volume in modo sincrono o asincrono da uno dei cluster di una coppia di cluster per scenari di failover e failback.

Il processo di replica include i seguenti passaggi:



- "Pianificare l'associazione di cluster e volumi per la replica in tempo reale"
- "Associare i cluster per la replica"

- "Associare i volumi"
- "Convalidare la replica del volume"
- "Eliminare una relazione di volume dopo la replica"
- "Gestire le relazioni dei volumi"

Pianificare l'associazione di cluster e volumi per la replica in tempo reale

La replica remota in tempo reale richiede l'associazione di due cluster di storage che eseguono il software Element, l'associazione di volumi su ciascun cluster e la convalida della replica. Una volta completata la replica, è necessario eliminare la relazione del volume.

Di cosa hai bisogno

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.
- Tutti gli indirizzi IP dei nodi delle reti di gestione e storage per i cluster accoppiati vengono instradati l'uno all'altro.
- La MTU di tutti i nodi accoppiati deve essere la stessa e deve essere supportata end-to-end tra i cluster.
- Entrambi i cluster di storage devono avere nomi di cluster univoci, MVIP, SVIP e tutti gli indirizzi IP dei nodi.
- La differenza tra le versioni software degli elementi sui cluster non è superiore a una versione principale. Se la differenza è maggiore, uno dei cluster deve essere aggiornato per eseguire la replica dei dati.

> Le appliance WAN Accelerator non sono state qualificate da NetApp per l'utilizzo durante la replica dei dati. Queste appliance possono interferire con la compressione e la deduplica se implementate tra due cluster che stanno replicando i dati. Assicurarsi di qualificare completamente gli effetti di qualsiasi appliance WAN Accelerator prima di implementarla in un ambiente di produzione.

Trova ulteriori informazioni

- Associare i cluster per la replica
- Associare i volumi
- Assegnare un'origine e una destinazione di replica ai volumi accoppiati

Associare i cluster per la replica

Per utilizzare la funzionalità di replica in tempo reale, è necessario associare due cluster come primo passo. Dopo aver associato e connesso due cluster, è possibile configurare i volumi attivi su un cluster per la replica continua su un secondo cluster, fornendo una protezione continua dei dati (CDP).

Di cosa hai bisogno

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.
- Tutti i MIPS e i SIPS dei nodi vengono instradati l'uno verso l'altro.
- Meno di 2000 ms di latenza di andata e ritorno tra i cluster.
- Entrambi i cluster di storage devono avere nomi di cluster univoci, MVIP, SVIP e tutti gli indirizzi IP dei

nodi.

- La differenza tra le versioni software degli elementi sui cluster non è superiore a una versione principale. Se la differenza è maggiore, uno dei cluster deve essere aggiornato per eseguire la replica dei dati.

> L'associazione dei cluster richiede una connettività completa tra i nodi della rete di gestione. La replica richiede la connettività tra i singoli nodi sulla rete del cluster di storage.

È possibile associare un cluster a un massimo di quattro altri cluster per la replica dei volumi. È inoltre possibile associare tra loro i cluster all'interno del gruppo di cluster.

Trova ulteriori informazioni

Requisiti delle porte di rete

Associare i cluster utilizzando MVIP o una chiave di accoppiamento

È possibile associare un cluster di origine e di destinazione utilizzando l'MVIP del cluster di destinazione se è disponibile l'accesso dell'amministratore del cluster a entrambi i cluster. Se l'accesso dell'amministratore del cluster è disponibile solo su un cluster di una coppia di cluster, è possibile utilizzare una chiave di accoppiamento sul cluster di destinazione per completare l'associazione del cluster.

1. Selezionare uno dei seguenti metodi per associare i cluster:
   - Accoppia cluster utilizzando MVIP: Utilizzare questo metodo se esiste l'accesso dell'amministratore del cluster a entrambi i cluster. Questo metodo utilizza l'MVIP del cluster remoto per associare due cluster.
   - Accoppia cluster utilizzando una chiave di accoppiamento: Utilizzare questo metodo se l'amministratore del cluster ha accesso a uno solo dei cluster. Questo metodo genera una chiave di accoppiamento che può essere utilizzata sul cluster di destinazione per completare l'associazione del cluster.

Trova ulteriori informazioni

- Associare i cluster utilizzando MVIP
- Associare i cluster utilizzando una chiave di accoppiamento

Associare i cluster utilizzando MVIP

È possibile associare due cluster per la replica in tempo reale utilizzando l'MVIP di un cluster per stabilire una connessione con l'altro cluster. Per utilizzare questo metodo, è necessario disporre dell'accesso dell'amministratore del cluster su entrambi i cluster. Il nome utente e la password dell'amministratore del cluster vengono utilizzati per autenticare l'accesso al cluster prima di poter associare i cluster.

1. Nel cluster locale, selezionare **Data Protection** > **Cluster Pairs**.
2. Fare clic su **Pair Cluster**.
3. Fare clic su **Start Pairing** (Avvia associazione) e fare clic su **Yes** (Sì) per indicare che si dispone dell'accesso al cluster remoto.
4. Inserire l'indirizzo MVIP del cluster remoto.

5. Fare clic su **complete pairing on remote cluster**.

   Nella finestra **Authentication Required** (autenticazione richiesta), immettere il nome utente e la password dell'amministratore del cluster remoto.

6. Sul cluster remoto, selezionare **Data Protection** > **Cluster Pairs**.
7. Fare clic su **Pair Cluster**.
8. Fare clic su **completa associazione**.
9. Fare clic sul pulsante **complete Pairing** (completa associazione).

Trova ulteriori informazioni

- Associare i cluster utilizzando una chiave di accoppiamento
- "Associazione di cluster mediante MVIP (video)"

Associare i cluster utilizzando una chiave di accoppiamento

Se si dispone dell'accesso di un amministratore del cluster a un cluster locale ma non a un cluster remoto, è possibile associare i cluster utilizzando una chiave di accoppiamento. Una chiave di accoppiamento viene generata su un cluster locale e quindi inviata in modo sicuro a un amministratore del cluster presso un sito remoto per stabilire una connessione e completare l'accoppiamento del cluster per la replica in tempo reale.

1. Nel cluster locale, selezionare **Data Protection** > **Cluster Pairs**.
2. Fare clic su **Pair Cluster**.
3. Fare clic su **Start Pairing** (Avvia associazione) e fare clic su **No** per indicare che non si dispone dell'accesso al cluster remoto.
4. Fare clic su **generate Key** (genera chiave).

   Questa azione genera una chiave di testo per l'associazione e crea una coppia di cluster non configurata sul cluster locale. Se la procedura non viene completata, è necessario eliminare manualmente la coppia di cluster.

5. Copiare la chiave di accoppiamento del cluster negli Appunti.
6. Rendere la chiave di accoppiamento accessibile all'amministratore del cluster nel sito del cluster remoto.

   La chiave di accoppiamento del cluster contiene una versione di MVIP, nome utente, password e informazioni sul database per consentire le connessioni dei volumi per la replica remota. Questa chiave deve essere trattata in modo sicuro e non memorizzata in modo da consentire l'accesso accidentale o non sicuro al nome utente o alla password.

   Non modificare i caratteri della chiave di accoppiamento. La chiave diventa non valida se viene modificata.

7. Sul cluster remoto, selezionare **Data Protection** > **Cluster Pairs**.
8. Fare clic su **Pair Cluster**.

9. Fare clic su **complete Pairing** (completa associazione) e inserire la chiave di associazione nel campo **Pairing Key** (chiave di associazione) (il metodo consigliato è incollare).
10. Fare clic su **completa associazione**.

Trova ulteriori informazioni

- Associare i cluster utilizzando MVIP
- "Associazione dei cluster mediante una chiave di accoppiamento dei cluster (video)"

Convalidare la connessione della coppia di cluster

Una volta completata l'associazione del cluster, è possibile verificare la connessione della coppia di cluster per garantire la riuscita della replica.

1. Nel cluster locale, selezionare **Data Protection** > **Cluster Pairs**.
2. Nella finestra **Cluster Pairs**, verificare che la coppia di cluster sia connessa.
3. **Opzionale:** tornare al cluster locale e alla finestra **Cluster Pairs** e verificare che la coppia di cluster sia connessa.

Associare i volumi

Dopo aver stabilito una connessione tra i cluster di una coppia di cluster, è possibile associare un volume di un cluster a un volume dell'altro cluster della coppia. Quando viene stabilita una relazione di accoppiamento dei volumi, è necessario identificare quale volume è la destinazione della replica.

È possibile associare due volumi per la replica in tempo reale memorizzati in diversi cluster di storage in una coppia di cluster connessi. Dopo aver associato due cluster, è possibile configurare i volumi attivi su un cluster per la replica continua su un secondo cluster, fornendo una protezione continua dei dati (CDP). È inoltre possibile assegnare un volume come origine o destinazione della replica.

I volumi sono sempre uno a uno. Dopo che un volume fa parte di un'associazione con un volume su un altro cluster, non è possibile associarlo nuovamente con altri volumi.

Di cosa hai bisogno

- È stata stabilita una connessione tra i cluster di una coppia di cluster.
- Si dispone dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.

Fasi

1. Creare un volume di destinazione con accesso in lettura o scrittura
2. Associare i volumi utilizzando un ID volume o una chiave di associazione
3. Assegnare un'origine e una destinazione di replica ai volumi accoppiati

Creare un volume di destinazione con accesso in lettura o scrittura

Il processo di replica coinvolge due endpoint: Il volume di origine e quello di destinazione. Quando si crea il volume di destinazione, il volume viene automaticamente impostato sulla modalità di lettura/scrittura per accettare i dati durante la replica.

1. Selezionare **Management** > **Volumes**.
2. Fare clic su **Create Volume** (Crea volume).
3. Nella finestra di dialogo Create a New Volume (Crea un nuovo volume), immettere il nome del volume.
4. Inserire le dimensioni totali del volume, selezionare una dimensione di blocco per il volume e selezionare l'account che deve avere accesso al volume.
5. Fare clic su **Create Volume** (Crea volume).
6. Nella finestra Active (attivo), fare clic sull'icona Actions (azioni) per il volume.
7. Fare clic su **Edit** (Modifica).
8. Impostare il livello di accesso dell'account su destinazione della replica.
9. Fare clic su **Save Changes** (Salva modifiche).

Associare i volumi utilizzando un ID volume o una chiave di associazione

Il processo di associazione prevede l'associazione di due volumi utilizzando un ID volume o una chiave di associazione.

1. Associare i volumi selezionando uno dei seguenti metodi:
   - Utilizzo di un ID volume: Utilizzare questo metodo se si dispone dell'accesso dell'amministratore del cluster a entrambi i cluster sui quali devono essere associati i volumi. Questo metodo utilizza l'ID del volume sul cluster remoto per avviare una connessione.
   - Utilizzo di una chiave di accoppiamento: Utilizzare questo metodo se si dispone dell'accesso dell'amministratore del cluster solo al cluster di origine. Questo metodo genera una chiave di accoppiamento che può essere utilizzata sul cluster remoto per completare la coppia di volumi.

> La chiave di accoppiamento del volume contiene una versione crittografata delle informazioni del volume e potrebbe contenere informazioni riservate. Condividere questa chiave solo in modo sicuro.

Trova ulteriori informazioni

- Associare i volumi utilizzando un ID volume
- Associare i volumi utilizzando una chiave di accoppiamento

Associare i volumi utilizzando un ID volume

È possibile associare un volume a un altro volume su un cluster remoto se si dispone delle credenziali di amministratore del cluster per il cluster remoto.

Di cosa hai bisogno

- Assicurarsi che i cluster contenenti i volumi siano associati.
- Creare un nuovo volume sul cluster remoto.

È possibile assegnare un'origine e una destinazione di replica dopo il processo di associazione. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione delle dimensioni del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

- Conoscere l'ID del volume di destinazione.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Fare clic sull'icona **azioni** del volume che si desidera associare.
3. Fare clic su **Pair** (abbina).
4. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **Start Pairing** (Avvia associazione).
5. Selezionare **i do** per indicare che si dispone dell'accesso al cluster remoto.
6. Selezionare una **Replication Mode** dall'elenco:
   - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.
   - **Real-time (Synchronous)**: Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
   - **Solo istantanee**: Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Selezionare un cluster remoto dall'elenco.
8. Scegliere un ID volume remoto.
9. Fare clic su **Start Pairing** (Avvia associazione).

   Il sistema apre una scheda del browser Web che si connette all'interfaccia utente Element del cluster remoto. Potrebbe essere necessario accedere al cluster remoto con le credenziali di amministratore del cluster.

10. Nell'interfaccia utente Element del cluster remoto, selezionare **complete Pairing** (completa associazione).
11. Confermare i dettagli in **Confirm Volume Pairing** (Conferma associazione volume).
12. Fare clic su **completa associazione**.

    Dopo aver confermato l'associazione, i due cluster iniziano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Volume Status** (Stato volume) della finestra **Volume Pairs** (coppie di volumi). Viene visualizzata la coppia di volumi `PausedMisconfigured` fino a quando non vengono assegnate l'origine e la destinazione della coppia di volumi.

    Una volta completata l'associazione, aggiornare la tabella Volumes (volumi) per rimuovere l'opzione **Pair** dall'elenco **Actions** (azioni) per il volume associato. Se non si aggiorna la tabella, l'opzione **Pair** rimane disponibile per la selezione. Se si seleziona di nuovo l'opzione **Pair**, viene visualizzata una nuova scheda e, poiché il volume è già associato, il sistema riporta un `StartVolumePairing Failed: xVolumeAlreadyPaired` Messaggio di errore nella finestra **Pair Volume** della pagina dell'interfaccia utente dell'elemento.

Trova ulteriori informazioni

- Messaggi di associazione del volume
- Avvisi di associazione del volume
- Assegnare un'origine e una destinazione di replica ai volumi accoppiati

Associare i volumi utilizzando una chiave di accoppiamento

Se non si dispone delle credenziali di amministratore del cluster per un cluster remoto, è possibile associare un volume a un altro volume di un cluster remoto utilizzando una chiave di accoppiamento.

Di cosa hai bisogno

- Assicurarsi che i cluster contenenti i volumi siano associati.
- Assicurarsi che sul cluster remoto sia presente un volume da utilizzare per l'associazione.

> È possibile assegnare un'origine e una destinazione di replica dopo il processo di associazione. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione delle dimensioni del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

Fasi

1. Selezionare **Management** > **Volumes**.
2. Fare clic sull'icona **azioni** del volume che si desidera associare.
3. Fare clic su **Pair** (abbina).
4. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **Start Pairing** (Avvia associazione).
5. Selezionare **i do not** per indicare che non si dispone dell'accesso al cluster remoto.
6. Selezionare una **Replication Mode** dall'elenco:
   - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.
   - **Real-time (Synchronous)**: Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
   - **Solo istantanee**: Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Fare clic su **generate Key** (genera chiave).

> Questa azione genera una chiave di testo per l'associazione e crea una coppia di volumi non configurata sul cluster locale. Se la procedura non viene completata, è necessario eliminare manualmente la coppia di volumi.

8. Copiare la chiave di accoppiamento nella clipboard del computer.
9. Rendere la chiave di accoppiamento accessibile all'amministratore del cluster nel sito del cluster remoto.

La chiave di accoppiamento del volume deve essere trattata in modo sicuro e non deve essere utilizzata in modo da consentire un accesso accidentale o non protetto.

Non modificare i caratteri della chiave di accoppiamento. La chiave diventa non valida se viene modificata.

10. Nell'interfaccia utente degli elementi del cluster remoto, selezionare **Management** > **Volumes**.
11. Fare clic sull'icona Actions (azioni) per il volume che si desidera associare.
12. Fare clic su **Pair** (abbina).
13. Nella finestra di dialogo **Pair Volume** (Volume coppia), selezionare **complete Pairing** (completa associazione).
14. Incollare la chiave di accoppiamento dall'altro cluster nella casella **Pairing Key** (chiave di associazione).
15. Fare clic su **completa associazione**.

    Dopo aver confermato l'associazione, i due cluster iniziano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Volume Status** (Stato volume) della finestra **Volume Pairs** (coppie di volumi). Viene visualizzata la coppia di volumi `PausedMisconfigured` fino a quando non vengono assegnate l'origine e la destinazione della coppia di volumi.

    Una volta completata l'associazione, aggiornare la tabella Volumes (volumi) per rimuovere l'opzione **Pair** dall'elenco **Actions** (azioni) per il volume associato. Se non si aggiorna la tabella, l'opzione **Pair** rimane disponibile per la selezione. Se si seleziona di nuovo l'opzione **Pair**, viene visualizzata una nuova scheda e, poiché il volume è già associato, il sistema riporta un `StartVolumePairing Failed: xVolumeAlreadyPaired` Messaggio di errore nella finestra **Pair Volume** della pagina dell'interfaccia utente dell'elemento.

Trova ulteriori informazioni

- Messaggi di associazione del volume
- Avvisi di associazione del volume
- Assegnare un'origine e una destinazione di replica ai volumi accoppiati

Assegnare un'origine e una destinazione di replica ai volumi accoppiati

Una volta associati i volumi, è necessario assegnare un volume di origine e il relativo volume di destinazione della replica. Un'origine o una destinazione di replica può essere un volume in una coppia di volumi. È inoltre possibile utilizzare questa procedura per reindirizzare i dati inviati a un volume di origine a un volume di destinazione remoto nel caso in cui il volume di origine non fosse disponibile.

Di cosa hai bisogno

È possibile accedere ai cluster contenenti i volumi di origine e di destinazione.

Fasi

1. Preparare il volume di origine:

   a. Dal cluster che contiene il volume che si desidera assegnare come origine, selezionare **Management**

> **Volumes**.

b. Fare clic sull'icona **azioni** del volume che si desidera assegnare come origine e fare clic su **Modifica**.

c. Nell'elenco a discesa **Access**, selezionare **Read/Write** (lettura/scrittura).

> Se si sta annullando l'assegnazione di origine e destinazione, questa azione fa sì che la coppia di volumi visualizzi il seguente messaggio fino a quando non viene assegnata una nuova destinazione di replica: `PausedMisconfigured`

La modifica dell'accesso interrompe la replica del volume e interrompe la trasmissione dei dati. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

a. Fare clic su **Save Changes** (Salva modifiche).

2. Preparare il volume di destinazione:

a. Dal cluster che contiene il volume che si desidera assegnare come destinazione, selezionare **Management** > **Volumes**.

b. Fare clic sull'icona Actions (azioni) per il volume che si desidera assegnare come destinazione e fare clic su **Edit** (Modifica).

c. Nell'elenco a discesa **Access**, selezionare **Replication Target**.

> Se si assegna un volume esistente come destinazione della replica, i dati su quel volume verranno sovrascritti. È necessario utilizzare un nuovo volume di destinazione che non contenga dati e che abbia le caratteristiche esatte del volume di origine, ad esempio dimensioni, impostazione 512e e configurazione QoS. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

d. Fare clic su **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

- Associare i volumi utilizzando un ID volume
- Associare i volumi utilizzando una chiave di accoppiamento

Convalidare la replica del volume

Una volta replicato un volume, assicurarsi che i volumi di origine e di destinazione siano attivi. Quando si trova in uno stato attivo, i volumi vengono associati, i dati vengono inviati dall'origine al volume di destinazione e i dati sono sincronizzati.

1. Da entrambi i cluster, selezionare **Data Protection** > **Volume Pairs**.
2. Verificare che lo stato del volume sia attivo.

Trova ulteriori informazioni

Avvisi di associazione del volume

Eliminare una relazione di volume dopo la replica

Una volta completata la replica e non è più necessaria la relazione della coppia di volumi,

è possibile eliminare la relazione del volume.

1. Selezionare **Data Protection** > **Volume Pairs**.
2. Fare clic sull'icona **Actions** della coppia di volumi che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Gestire le relazioni dei volumi

È possibile gestire le relazioni dei volumi in molti modi, ad esempio mettendo in pausa la replica, invertendo l'accoppiamento dei volumi, modificando la modalità di replica, eliminando una coppia di volumi o eliminando una coppia di cluster.

Trova ulteriori informazioni

- Mettere in pausa la replica
- Modificare la modalità di replica
- Eliminare le coppie di volumi

Mettere in pausa la replica

È possibile sospendere manualmente la replica se è necessario interrompere l'elaborazione i/o per un breve periodo di tempo. È possibile sospendere la replica se si verifica un aumento nell'elaborazione i/o e si desidera ridurre il carico di elaborazione.

1. Selezionare **Data Protection** > **Volume Pairs**.
2. Fare clic sull'icona Actions (azioni) per la coppia di volumi.
3. Fare clic su **Edit** (Modifica).
4. Nel riquadro **Edit Volume Pair** (Modifica coppia di volumi), sospendere manualmente il processo di replica.

> La sospensione o la ripresa manuale della replica del volume causa la cessazione o la ripresa della trasmissione dei dati. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Save Changes** (Salva modifiche).

Modificare la modalità di replica

È possibile modificare le proprietà della coppia di volumi per modificare la modalità di replica della relazione della coppia di volumi.

1. Selezionare **Data Protection** > **Volume Pairs**.
2. Fare clic sull'icona Actions (azioni) per la coppia di volumi.
3. Fare clic su **Edit** (Modifica).
4. Nel riquadro **Edit Volume Pair** (Modifica coppia di volumi), selezionare una nuova modalità di replica:
    - **Real-time (asincrono)**: Le scritture vengono riconosciute al client dopo il commit sul cluster di origine.

- **Real-time (Synchronous)**: Le scritture vengono riconosciute al client dopo il commit sia sul cluster di origine che su quello di destinazione.
- **Solo istantanee**: Vengono replicate solo le istantanee create nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate. **Attenzione:** la modifica della modalità di replica modifica immediatamente la modalità. Assicurarsi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Save Changes** (Salva modifiche).

Eliminare le coppie di volumi

È possibile eliminare una coppia di volumi se si desidera rimuovere un'associazione di coppia tra due volumi.

1. Selezionare **Data Protection** > **Volume Pairs**.
2. Fare clic sull'icona Actions (azioni) per la coppia di volumi che si desidera eliminare.
3. Fare clic su **Delete** (Elimina).
4. Confermare il messaggio.

Eliminare una coppia di cluster

È possibile eliminare una coppia di cluster dall'interfaccia utente degli elementi di uno dei cluster della coppia.

1. Fare clic su **Data Protection** > **Cluster Pairs**.
2. Fare clic sull'icona Actions (azioni) per una coppia di cluster.
3. Nel menu visualizzato, fare clic su **Delete** (Elimina).
4. Confermare l'azione.
5. Eseguire nuovamente i passaggi dal secondo cluster nell'associazione del cluster.

Dettagli della coppia di cluster

La pagina Cluster Pairs della scheda Data Protection (protezione dati) fornisce informazioni sui cluster che sono stati associati o che sono in fase di associazione. Il sistema visualizza i messaggi di associazione e di avanzamento nella colonna Status (Stato).

- **ID**

  ID generato dal sistema assegnato a ciascuna coppia di cluster.

- **Nome cluster remoto**

  Il nome dell'altro cluster della coppia.

- **MVIP remoto**

  L'indirizzo IP virtuale di gestione dell'altro cluster della coppia.

- **Stato**

Stato della replica del cluster remoto

- **Replica dei volumi**

  Il numero di volumi contenuti nel cluster che sono accoppiati per la replica.

- **UUID**

  Un ID univoco assegnato a ciascun cluster della coppia.

Dettagli della coppia di volumi

La pagina Volume Pairs (coppie di volumi) nella scheda Data Protection (protezione dati) fornisce informazioni sui volumi che sono stati associati o che sono in fase di associazione. Il sistema visualizza i messaggi di associazione e di avanzamento nella colonna Volume Status (Stato volume).

- **ID**

  ID generato dal sistema per il volume.

- **Nome**

  Il nome assegnato al volume al momento della creazione. I nomi dei volumi possono contenere fino a 223 caratteri e contengono a-z, 0-9 e trattino (-).

- **Account**

  Nome dell'account assegnato al volume.

- **Volume Status** (Stato volume)

  Stato di replica del volume

- **Stato snapshot**

  Stato del volume di snapshot.

- **Modalità**

  Il metodo di replica in scrittura del client. I valori possibili sono i seguenti:

  - Asincrono
  - Solo Snapshot
  - Sincronizza

- **Direzione**

  La direzione dei dati del volume:

  - Icona del volume di origine (→) indica che i dati vengono scritti in una destinazione esterna al cluster.
  - Icona del volume di destinazione (←) indica che i dati vengono scritti nel volume locale da un'origine esterna.

- **Ritardo asincrono**

  Periodo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è associato, il valore è nullo.

- **Cluster remoto**

  Nome del cluster remoto su cui risiede il volume.

- **ID volume remoto**

  ID volume del volume sul cluster remoto.

- **Nome volume remoto**

  Nome assegnato al volume remoto al momento della creazione.

Messaggi di associazione del volume

È possibile visualizzare i messaggi di associazione dei volumi durante il processo di associazione iniziale dalla pagina Volume Pairs (coppie di volumi) nella scheda Data Protection (protezione dati). Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia nella vista elenco Replica volumi.

- **PausedDisconnected**

  Replica di origine o sincronizzazione RPC scaduta. La connessione al cluster remoto è stata persa. Controllare le connessioni di rete al cluster.

- **RisumingConnected**

  La sincronizzazione della replica remota è ora attiva. Avvio del processo di sincronizzazione e attesa dei dati.

- **RisumingRRSync**

  Una singola copia helix dei metadati del volume viene eseguita sul cluster associato.

- **RisumingLocalSync**

  Viene eseguita una copia a doppia elica dei metadati del volume nel cluster associato.

- **RisumingDataTransfer**

  Il trasferimento dei dati è ripreso.

- **Attivo**

  I volumi vengono associati e i dati vengono inviati dall'origine al volume di destinazione e i dati sono sincronizzati.

- **Inattivo**

Nessuna attività di replica in corso.

Avvisi di associazione del volume

La pagina Thevolume Pairs della scheda Data Protection (protezione dati) fornisce questi messaggi dopo l'accoppiamento dei volumi. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia (se non diversamente indicato) nella vista elenco Replica volumi.

- **PausedClusterFull**

  Poiché il cluster di destinazione è pieno, la replica di origine e il trasferimento di dati in blocco non possono procedere. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedExceedMaxSnapshotCount**

  Il volume di destinazione dispone già del numero massimo di snapshot e non può replicare snapshot aggiuntivi.

- **PausedManual**

  Il volume locale è stato messo in pausa manualmente. Prima di riprendere la replica, è necessario che la replica sia sospesa.

- **PausedManualRemote**

  Il volume remoto è in modalità di pausa manuale. È richiesto l'intervento manuale per riattivare il volume remoto prima che la replica venga ripresa.

- **PausedMisconfigured**

  In attesa di un'origine e di una destinazione attive. È richiesto l'intervento manuale per riprendere la replica.

- **QoS Paused**

  QoS di destinazione non è riuscito a sostenere i/o in entrata. La replica riprende automaticamente. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedSlowLink**

  Collegamento lento rilevato e replica interrotta. La replica riprende automaticamente. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **PausedVolumeSizeMismatch**

  Il volume di destinazione non ha le stesse dimensioni del volume di origine.

- **PausedXCopy**

  Viene inviato un comando SCSI XCOPY a un volume di origine. Il comando deve essere completato prima che la replica possa riprendere. Il messaggio viene visualizzato solo sul lato di origine della coppia.

- **StoppedMisconfigured**

È stato rilevato un errore di configurazione permanente. Il volume remoto è stato disaccoppiato o disaccoppiato. Non è possibile eseguire alcuna azione correttiva; è necessario stabilire una nuova associazione.

Utilizzare la replica SnapMirror tra cluster Element e ONTAP

È possibile creare relazioni SnapMirror dalla scheda protezione dati dell'interfaccia utente di NetApp Element. La funzionalità di SnapMirror deve essere attivata per visualizzarla nell'interfaccia utente.

IPv6 non è supportato per la replica di SnapMirror tra il software NetApp Element e i cluster ONTAP.

"Video NetApp: SnapMirror per NetApp HCI ed Element Software"

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare le copie Snapshot con i sistemi NetApp ONTAP. Il motivo principale dell'utilizzo di questa tecnologia è il disaster recovery di NetApp HCI in ONTAP. Gli endpoint includono ONTAP, ONTAP Select e Cloud Volumes ONTAP. Consulta la protezione dei dati TR-4641 NetApp HCI.

"Report tecnico NetApp 4641: Protezione dei dati NetApp HCI"

Trova ulteriori informazioni

- "Creazione del data fabric con NetApp HCI, ONTAP e infrastruttura convergente"
- "Replica tra il software NetApp Element e ONTAP"

Panoramica di SnapMirror

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare le snapshot con i sistemi NetApp ONTAP.

I sistemi che eseguono Element possono comunicare direttamente con SnapMirror su sistemi ONTAP 9.3 o superiori. L'API di NetApp Element fornisce metodi per abilitare la funzionalità SnapMirror su cluster, volumi e snapshot. Inoltre, l'interfaccia utente di Element include tutte le funzionalità necessarie per gestire le relazioni di SnapMirror tra il software Element e i sistemi ONTAP.

È possibile replicare i volumi originati da ONTAP in volumi Element in casi di utilizzo specifici con funzionalità limitate. Per ulteriori informazioni, consultare la documentazione di ONTAP.

Trova ulteriori informazioni

"Replica tra software Element e ONTAP"

Attivare SnapMirror sul cluster

È necessario attivare manualmente la funzionalità SnapMirror a livello di cluster tramite l'interfaccia utente di NetApp Element. Il sistema viene fornito con la funzionalità SnapMirror disattivata per impostazione predefinita e non viene attivata automaticamente durante una nuova installazione o un aggiornamento. L'attivazione della funzione SnapMirror è un'attività di configurazione unica.

SnapMirror può essere abilitato solo per i cluster che eseguono il software Element utilizzato insieme ai volumi su un sistema NetApp ONTAP. È necessario attivare la funzionalità SnapMirror solo se il cluster è connesso per l'utilizzo con i volumi NetApp ONTAP.

Di cosa hai bisogno

Il cluster di storage deve eseguire il software NetApp Element.

Fasi

1. Fare clic su **Clusters** > **Impostazioni**.
2. Individuare le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Enable SnapMirror** (attiva SnapMirror

> L'attivazione della funzionalità SnapMirror modifica in modo permanente la configurazione del software Element. È possibile disattivare la funzione SnapMirror e ripristinare le impostazioni predefinite solo ripristinando l'immagine predefinita del cluster.

4. Fare clic su **Sì** per confermare la modifica della configurazione di SnapMirror.

Attivare SnapMirror sul volume

È necessario attivare SnapMirror sul volume nell'interfaccia utente di Element. Ciò consente la replica dei dati in volumi ONTAP specificati. Questa è l'autorizzazione dell'amministratore del cluster che esegue il software NetApp Element per SnapMirror per controllare un volume.

Di cosa hai bisogno

- SnapMirror è stato attivato nell'interfaccia utente Element per il cluster.
- È disponibile un endpoint SnapMirror.
- Il volume deve essere di dimensioni di blocco 512e.
- Il volume non partecipa alla replica remota.
- Il tipo di accesso al volume non è destinazione della replica.

> È inoltre possibile impostare questa proprietà durante la creazione o la clonazione di un volume.

Fasi

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona **Actions** del volume per il quale si desidera attivare SnapMirror.
3. Nel menu visualizzato, selezionare **Edit** (Modifica).
4. Nella finestra di dialogo **Edit Volume** (Modifica volume), selezionare la casella di controllo **Enable SnapMirror** (attiva SnapMirror).
5. Fare clic su **Save Changes** (Salva modifiche).

Creare un endpoint SnapMirror

Prima di creare una relazione, è necessario creare un endpoint SnapMirror nell'interfaccia utente di NetApp Element.

Un endpoint SnapMirror è un cluster ONTAP che funge da destinazione di replica per un cluster che esegue software Element. Prima di creare una relazione SnapMirror, creare un endpoint SnapMirror.

È possibile creare e gestire fino a quattro endpoint SnapMirror in un cluster di storage che esegue il software Element.

> Se un endpoint esistente è stato originariamente creato utilizzando l'API e le credenziali non sono state salvate, è possibile visualizzare l'endpoint nell'interfaccia utente dell'elemento e verificarne l'esistenza, ma non può essere gestito utilizzando l'interfaccia utente dell'elemento. Questo endpoint può quindi essere gestito solo utilizzando l'API Element.

Per ulteriori informazioni sui metodi API, vedere "Gestire lo storage con l'API Element".

Di cosa hai bisogno

- È necessario aver attivato SnapMirror nell'interfaccia utente Element per il cluster di storage.
- Conosci le credenziali ONTAP per l'endpoint.

Fasi

1. Fare clic su **Data Protection** > **SnapMirror Endpoints**.
2. Fare clic su **Create Endpoint** (Crea endpoint).
3. Nella finestra di dialogo **Crea nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster del sistema ONTAP.
4. Immettere le credenziali di amministratore di ONTAP associate all'endpoint.
5. Leggi ulteriori dettagli:
   - LIF: Elenca le interfacce logiche dell'intercluster ONTAP utilizzate per comunicare con Element.
   - Status (Stato): Mostra lo stato corrente dell'endpoint SnapMirror. I valori possibili sono: Connesso, disconnesso e non gestito.
6. Fare clic su **Create Endpoint** (Crea endpoint).

Creare una relazione SnapMirror

È necessario creare una relazione SnapMirror nell'interfaccia utente di NetApp Element.

> Quando un volume non è ancora abilitato per SnapMirror e si sceglie di creare una relazione dall'interfaccia utente di Element, SnapMirror viene attivato automaticamente su tale volume.

Di cosa hai bisogno

SnapMirror è attivato sul volume.

Fasi

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona **azioni** del volume che deve essere parte della relazione.
3. Fare clic su **Crea una relazione SnapMirror**.
4. Nella finestra di dialogo **Crea una relazione SnapMirror**, selezionare un endpoint dall'elenco **endpoint**.
5. Selezionare se la relazione verrà creata utilizzando un nuovo volume ONTAP o un volume ONTAP esistente.

6. Per creare un nuovo volume ONTAP nell'interfaccia utente di Element, fare clic su **Crea nuovo volume**.
   a. Selezionare **Storage Virtual Machine** per questa relazione.
   b. Selezionare **aggregato** dall'elenco a discesa.
   c. Nel campo **Volume Name Suffix** (suffisso nome volume), immettere un suffisso.

      Il sistema rileva il nome del volume di origine e lo copia nel campo **Volume Name** (Nome volume). Il suffisso inserito aggiunge il nome.

   d. Fare clic su **Crea volume di destinazione**.
7. Per utilizzare un volume ONTAP esistente, fare clic su **Use existing volume** (Usa volume esistente).
   a. Selezionare **Storage Virtual Machine** per questa relazione.
   b. Selezionare il volume di destinazione per questa nuova relazione.
8. Nella sezione **Dettagli relazione**, selezionare un criterio. Se il criterio selezionato dispone di regole di conservazione, nella tabella regole vengono visualizzate le regole e le etichette associate.
9. **Opzionale**: Selezionare un programma.

   In questo modo si determina la frequenza con cui la relazione crea le copie.

10. **Opzionale**: Nel campo **limita larghezza di banda a**, immettere la quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
11. Leggi ulteriori dettagli:
    - **State**: Stato di relazione corrente del volume di destinazione. I valori possibili sono:
      - uninitialized (non inizializzato): Il volume di destinazione non è stato inizializzato.
      - snapmirrored: Il volume di destinazione è stato inizializzato ed è pronto per ricevere gli aggiornamenti di SnapMirror.
      - Interrotto: Il volume di destinazione è in lettura/scrittura e sono presenti snapshot.
    - **Status**: Stato corrente della relazione. I valori possibili sono idle, trasferimento, controllo, sospensione, quiesced, in coda, preparazione, finalizzazione, interruzione e interruzione.
    - **Lag Time** (tempo di ritardo): La quantità di tempo in secondi che il sistema di destinazione rimane indietro rispetto al sistema di origine. Il tempo di ritardo non deve superare l'intervallo di pianificazione del trasferimento.
    - **Bandwidth limit** (limite larghezza di banda): La quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
    - **Ultimo trasferimento**: Data e ora dell'ultimo snapshot trasferito. Fare clic per ulteriori informazioni.
    - **Nome policy**: Il nome del criterio SnapMirror di ONTAP per la relazione.
    - **Tipo di policy**: Tipo di policy SnapMirror di ONTAP selezionata per la relazione. I valori possibili sono:
      - mirror_asincrono
      - vault_mirror
    - **Nome pianificazione**: Nome della pianificazione preesistente sul sistema ONTAP selezionato per questa relazione.
12. Per non eseguire l'inizializzazione in questo momento, assicurarsi che la casella di controllo **Inizializza** non sia selezionata.

L'inizializzazione può richiedere molto tempo. Potrebbe essere necessario eseguire questa operazione durante le ore di lavoro fuori dalle ore di punta. L'inizializzazione esegue un trasferimento baseline; crea una copia snapshot del volume di origine, quindi trasferisce la copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. È possibile eseguire l'inizializzazione manualmente o utilizzare un programma per avviare il processo di inizializzazione (e gli aggiornamenti successivi) in base alla pianificazione.

13. Fare clic su **Crea relazione**.
14. Fare clic su **Data Protection** > **SnapMirror Relationship** per visualizzare questa nuova relazione SnapMirror.

Azioni di relazione di SnapMirror

È possibile configurare una relazione dalla pagina delle relazioni di SnapMirror della scheda protezione dati. Di seguito sono descritte le opzioni dell'icona azioni.

- **Edit**: Modifica la policy utilizzata o la pianificazione della relazione.
- **Delete**: Elimina la relazione SnapMirror. Questa funzione non elimina il volume di destinazione.
- **Inizializza**: Esegue il primo trasferimento iniziale dei dati di riferimento per stabilire una nuova relazione.
- **Update**: Esegue un aggiornamento on-demand della relazione, replicando i nuovi dati e le copie Snapshot incluse dall'ultimo aggiornamento alla destinazione.
- **Quiesce**: Impedisce ulteriori aggiornamenti per una relazione.
- **Resume**: Riprende una relazione che è stata rinunciata.
- **Break**: Consente di eseguire la lettura/scrittura del volume di destinazione e di interrompere tutti i trasferimenti correnti e futuri. Determinare che i client non utilizzano il volume di origine originale, poiché l'operazione di risincronizzazione inversa rende il volume di origine di sola lettura.
- **Resync**: Stabilisce una relazione interrotta nella stessa direzione prima che si verificasse l'interruzione.
- **Reverse Resync**: Automatizza i passaggi necessari per creare e inizializzare una nuova relazione nella direzione opposta. Questa operazione può essere eseguita solo se la relazione esistente si trova in uno stato interrotto. Questa operazione non elimina la relazione corrente. Il volume di origine torna alla copia Snapshot più recente e viene risincronizzato con la destinazione. Tutte le modifiche apportate al volume di origine dall'ultimo aggiornamento di SnapMirror sono perse. Tutte le modifiche apportate o i nuovi dati scritti nel volume di destinazione corrente vengono inviati nuovamente al volume di origine originale.
- **Interrompi**: Annulla un trasferimento in corso. Se viene emesso un aggiornamento di SnapMirror per una relazione interrotta, la relazione continua con l'ultimo trasferimento dall'ultimo checkpoint di riavvio creato prima dell'interruzione.

Etichette SnapMirror

Un'etichetta SnapMirror funge da indicatore per il trasferimento di uno snapshot specificato in base alle regole di conservazione della relazione.

L'applicazione di un'etichetta a uno snapshot lo contrassegna come destinazione per la replica di SnapMirror. Il ruolo della relazione è quello di applicare le regole al momento del trasferimento dei dati selezionando lo snapshot etichettato corrispondente, copiandolo nel volume di destinazione e garantendo che venga conservato il numero corretto di copie. Si riferisce alla policy per determinare il numero di conservazione e il periodo di conservazione. Il criterio può avere un numero qualsiasi di regole e ogni regola ha un'etichetta univoca. Questa etichetta funge da collegamento tra lo snapshot e la regola di conservazione.

È l'etichetta SnapMirror che indica quale regola applicare per lo snapshot, lo snapshot di gruppo o la pianificazione selezionati.

Aggiungere le etichette SnapMirror alle snapshot

Le etichette SnapMirror specificano il criterio di conservazione delle snapshot sull'endpoint SnapMirror. È possibile aggiungere etichette alle istantanee e raggruppare le istantanee.

È possibile visualizzare le etichette disponibili da una finestra di dialogo relazione SnapMirror esistente o da Gestore di sistema NetApp ONTAP.

> Quando si aggiunge un'etichetta a uno snapshot di gruppo, le etichette esistenti alle singole istantanee vengono sovrascritte.

Di cosa hai bisogno

- SnapMirror è attivato sul cluster.
- L'etichetta che si desidera aggiungere esiste già in ONTAP.

Fasi

1. Fare clic su **Data Protection** > **Snapshot** o sulla pagina **Group Snapshot**.
2. Fare clic sull'icona **Actions** per lo snapshot o lo snapshot di gruppo a cui si desidera aggiungere un'etichetta SnapMirror.
3. Nella finestra di dialogo **Edit Snapshot** (Modifica snapshot), inserire il testo nel campo **SnapMirror Label** (etichetta SnapMirror). L'etichetta deve corrispondere all'etichetta di una regola nel criterio applicato alla relazione SnapMirror.
4. Fare clic su **Save Changes** (Salva modifiche).

Aggiunta di etichette SnapMirror alle pianificazioni di snapshot

È possibile aggiungere etichette SnapMirror alle pianificazioni di snapshot per garantire l'applicazione di un criterio SnapMirror. È possibile visualizzare le etichette disponibili da una finestra di dialogo relazione SnapMirror esistente o da NetAppONTAP System Manager.

Di cosa hai bisogno

- SnapMirror deve essere attivato a livello di cluster.
- L'etichetta che si desidera aggiungere esiste già in ONTAP.

Fasi

1. Fare clic su **Data Protection** > **Schedules**.
2. Aggiungere un'etichetta SnapMirror a una pianificazione in uno dei seguenti modi:

Opzione	Fasi
Creazione di una nuova pianificazione	a. Selezionare **Crea pianificazione**. b. Inserire tutti gli altri dettagli pertinenti. c. Selezionare **Crea pianificazione**.
Modifica della pianificazione esistente	a. Fare clic sull'icona **azioni** del programma a cui si desidera aggiungere un'etichetta e selezionare **Modifica**. b. Nella finestra di dialogo visualizzata, inserire il testo nel campo **etichetta SnapMirror**. c. Selezionare **Save Changes** (Salva modifiche).

Trova ulteriori informazioni

Creare una pianificazione di snapshot

Disaster recovery con SnapMirror

In caso di problemi con un volume o un cluster che esegue il software NetApp Element, utilizzare la funzionalità SnapMirror per interrompere la relazione e il failover verso il volume di destinazione.

Se il cluster originale è completamente guasto o non esiste, contattare il supporto NetApp per ulteriore assistenza.

Eseguire un failover da un cluster di elementi

È possibile eseguire un failover dal cluster di elementi per rendere il volume di destinazione di lettura/scrittura e accessibile agli host sul lato di destinazione. Prima di eseguire un failover dal cluster di elementi, è necessario interrompere la relazione SnapMirror.

Utilizzare l'interfaccia utente di NetApp Element per eseguire il failover. Se l'interfaccia utente di Element non è disponibile, è possibile utilizzare anche Gestore di sistema di ONTAP o l'interfaccia utente di ONTAP per eseguire il comando break relationship.

Di cosa hai bisogno

- Esiste una relazione SnapMirror che contiene almeno uno snapshot valido nel volume di destinazione.
- È necessario eseguire il failover sul volume di destinazione a causa di un'interruzione non pianificata o di un evento pianificato nel sito primario.

Fasi

1. Nell'interfaccia utente di Element, fare clic su **Data Protection** > **SnapMirror Relanes**.
2. Individuare la relazione con il volume di origine che si desidera eseguire il failover.
3. Fare clic sull'icona **azioni**.
4. Fare clic su **Interrompi**.

5. Confermare l'azione.

   Il volume sul cluster di destinazione dispone ora dell'accesso in lettura/scrittura e può essere montato sugli host delle applicazioni per riprendere i carichi di lavoro di produzione. Tutta la replica di SnapMirror viene interrotta in seguito a questa azione. La relazione mostra uno stato di interrotto.

Eseguire un failback a Element

Una volta mitigato il problema sul lato primario, è necessario risincronizzare il volume di origine originale e ripristinare il software NetApp Element. I passaggi da eseguire variano a seconda che il volume di origine sia ancora esistente o che sia necessario eseguire il failback a un volume appena creato.

Trova ulteriori informazioni

- Eseguire un failback quando il volume di origine esiste ancora
- Eseguire un failback quando il volume di origine non esiste più
- Scenari di failback di SnapMirror

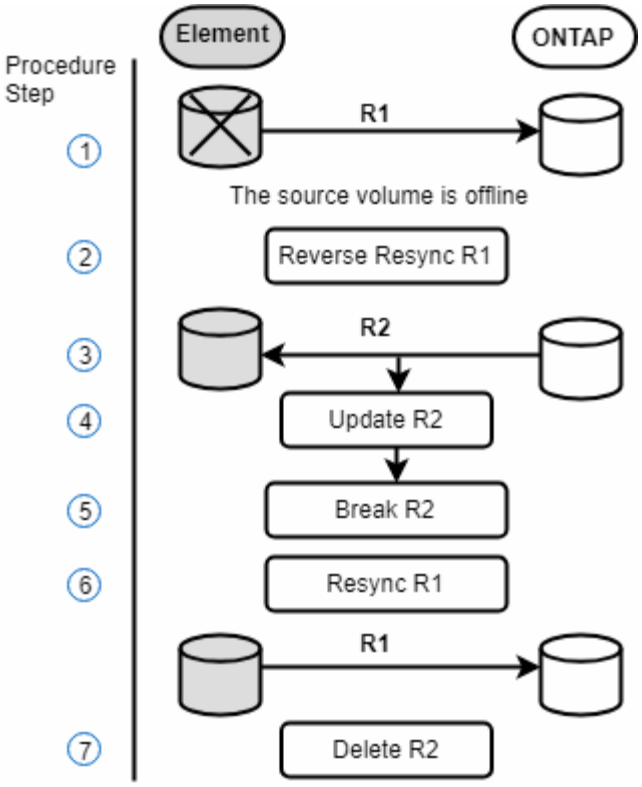
Scenari di failback di SnapMirror

La funzionalità di disaster recovery di SnapMirror è illustrata in due scenari di failback. Questi presuppongono che la relazione originale sia stata interrotta.

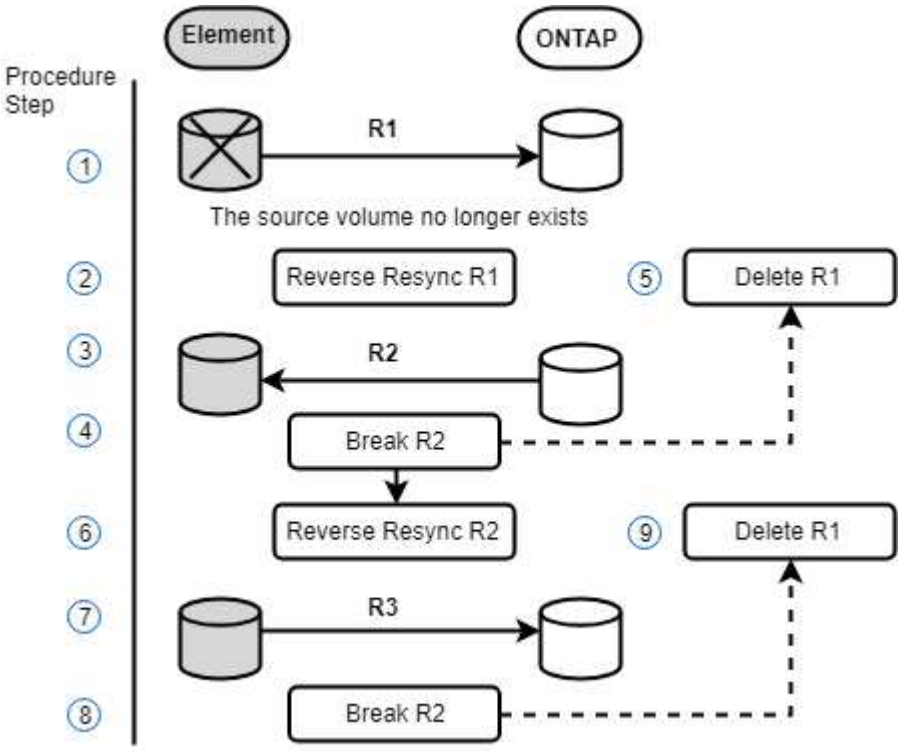
Le fasi delle procedure corrispondenti vengono aggiunte come riferimento.

> Negli esempi qui riportati, R1 = relazione originale in cui il cluster che esegue il software NetApp Element è il volume di origine (elemento) originale e ONTAP è il volume di destinazione originale (ONTAP). R2 e R3 rappresentano le relazioni inverse create attraverso l'operazione di risincronizzazione inversa.

La seguente immagine mostra lo scenario di failback quando il volume di origine è ancora presente:



L'immagine seguente mostra lo scenario di failback quando il volume di origine non esiste più:



Trova ulteriori informazioni

- Eseguire un failback quando il volume di origine esiste ancora
- Eseguire un failback quando il volume di origine non esiste più

Eseguire un failback quando il volume di origine esiste ancora

È possibile risincronizzare il volume di origine originale e eseguire un failback utilizzando l'interfaccia utente di NetApp Element. Questa procedura si applica agli scenari in cui il volume di origine originale esiste ancora.

1. Nell'interfaccia utente di Element, individuare la relazione che si è spezzata per eseguire il failover.
2. Fare clic sull'icona delle azioni e fare clic su **Reverse Resync** (risincronizzazione inversa).
3. Confermare l'azione.

> L'operazione Reverse Resync crea una nuova relazione in cui i ruoli dei volumi di origine e di destinazione originali vengono invertiti (questo comporta due relazioni quando la relazione originale persiste). Tutti i nuovi dati del volume di destinazione originale vengono trasferiti al volume di origine come parte dell'operazione di risincronizzazione inversa. È possibile continuare ad accedere e scrivere i dati nel volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host nel volume di origine ed eseguire un aggiornamento di SnapMirror prima di reindirizzare nuovamente al volume primario originale.

4. Fare clic sull'icona Actions (azioni) della relazione inversa appena creata e fare clic su **Update** (Aggiorna).

   Una volta completata la risincronizzazione inversa, assicurarsi che non vi siano sessioni attive connesse al volume sul lato di destinazione e che i dati più recenti si trovino sul volume primario originale, per completare il failback e riattivare il volume primario originale, procedere come segue:

5. Fare clic sull'icona Actions (azioni) della relazione inversa e fare clic su **Break** (Interrompi).
6. Fare clic sull'icona Actions (azioni) della relazione originale e fare clic su **Resync**.

> Il volume primario originale può ora essere montato per riprendere i carichi di lavoro di produzione sul volume primario originale. La replica di SnapMirror originale riprende in base al criterio e alla pianificazione configurati per la relazione.

7. Dopo aver confermato che lo stato della relazione originale è "snapmirrored", fare clic sull'icona Actions (azioni) della relazione inversa e fare clic su **Delete** (Elimina).

Trova ulteriori informazioni

Scenari di failback di SnapMirror

Eseguire un failback quando il volume di origine non esiste più

È possibile risincronizzare il volume di origine originale e eseguire un failback utilizzando l'interfaccia utente di NetApp Element. Questa sezione si applica agli scenari in cui il volume di origine originale è stato perso ma il cluster originale è ancora intatto. Per istruzioni su come eseguire il ripristino in un nuovo cluster, consultare la documentazione sul sito del supporto NetApp.

Di cosa hai bisogno

- Si dispone di una relazione di replica interrotta tra i volumi Element e ONTAP.
- Il volume dell'elemento viene irrimediabilmente perso.

- Il nome del volume originale viene visualizzato come NON TROVATO.

Fasi

1. Nell'interfaccia utente di Element, individuare la relazione che si è spezzata per eseguire il failover.

   Best practice: prendere nota della policy di SnapMirror e dei dettagli di pianificazione della relazione interrotta originale. Queste informazioni saranno necessarie quando si ricrea la relazione.

2. Fare clic sull'icona **azioni** e fare clic su **Reverse Resync** (risincronizzazione inversa).
3. Confermare l'azione.

   L'operazione Reverse Resync crea una nuova relazione in cui i ruoli del volume di origine originale e del volume di destinazione vengono invertiti (questo comporta due relazioni quando la relazione originale persiste). Poiché il volume originale non esiste più, il sistema crea un nuovo volume elemento con lo stesso nome e le stesse dimensioni del volume di origine. Al nuovo volume viene assegnata una policy QoS predefinita chiamata SM-recovery ed è associato a un account predefinito chiamato SM-recovery. Si desidera modificare manualmente l'account e la policy QoS per tutti i volumi creati da SnapMirror per sostituire i volumi di origine distrutti.

   I dati dell'ultimo snapshot vengono trasferiti al nuovo volume come parte dell'operazione di risincronizzazione inversa. È possibile continuare ad accedere e scrivere i dati nel volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host nel volume attivo ed eseguire un aggiornamento di SnapMirror prima di ripristinare la relazione primaria originale in un passaggio successivo. Dopo aver completato la risincronizzazione inversa e aver verificato che non vi siano sessioni attive connesse al volume sul lato di destinazione e che i dati più recenti si trovino sul volume primario originale, continuare con i seguenti passaggi per completare il failback e riattivare il volume primario originale:

4. Fare clic sull'icona **azioni** della relazione inversa creata durante l'operazione di risincronizzazione inversa e fare clic su **interruzione**.
5. Fare clic sull'icona **azioni** della relazione originale, in cui il volume di origine non esiste, quindi fare clic su **Elimina**.
6. Fare clic sull'icona **Actions** della relazione inversa, che si è spezzata al punto 4, quindi fare clic su **Reverse Resync** (risincronizzazione inversa).
7. In questo modo vengono invertiti l'origine e la destinazione e si ottiene una relazione con la stessa origine e destinazione del volume della relazione originale.
8. Fare clic sull'icona **azioni** e su **Modifica** per aggiornare questa relazione con le impostazioni di pianificazione e policy QoS originali di cui si è preso nota.
9. Ora è possibile eliminare in modo sicuro la relazione inversa risynced al punto 6.

Trova ulteriori informazioni

Scenari di failback di SnapMirror

Eseguire un trasferimento o una migrazione una tantum da ONTAP a Element

In genere, quando si utilizza SnapMirror per il disaster recovery da un cluster di storage SolidFire che esegue il software NetApp Element al software ONTAP, Element è l'origine e ONTAP la destinazione. Tuttavia, in alcuni casi il sistema di storage ONTAP può

fungere da origine ed elemento come destinazione.

- Esistono due scenari:
  - Nessuna relazione precedente di disaster recovery. Seguire tutte le fasi di questa procedura.
  - Esiste una relazione di disaster recovery precedente, ma non tra i volumi utilizzati per questa mitigazione. In questo caso, seguire solo i passaggi 3 e 4 riportati di seguito.

Di cosa hai bisogno

- Il nodo di destinazione dell'elemento deve essere stato reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica di SnapMirror.

Specificare il percorso di destinazione dell'elemento nel formato hostip:/lun/<id_number>, dove lun è la stringa corrente "lun" e id_number è l'ID del volume dell'elemento.

Fasi

1. Utilizzando ONTAP, creare la relazione con il cluster di elementi:

```
snapmirror create -source-path SVM:volume|cluster://SVM/volume
-destination-path hostip:/lun/name -type XDP -schedule schedule -policy
    policy
```

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy MirrorLatest
```

2. Verificare che la relazione SnapMirror sia stata creata utilizzando il comando show di ONTAP snapmirror.

   Vedere le informazioni sulla creazione di una relazione di replica nella documentazione di ONTAP e per la sintassi completa dei comandi, vedere la pagina man di ONTAP.

3. Utilizzando il `ElementCreateVolume` API, creare il volume di destinazione e impostare la modalità di accesso al volume di destinazione su SnapMirror:

   Creare un volume Element utilizzando l'API Element

```
{
   "method": "CreateVolume",
   "params": {
        "name": "SMTargetVolumeTest2",
        "accountID": 1,
        "totalSize": 100000000000,
        "enable512e": true,
        "attributes": {},
        "qosPolicyID": 1,
        "enableSnapMirrorReplication": true,
        "access": "snapMirrorTarget"
    },
    "id": 1
}
```

4. Inizializzare la relazione di replica utilizzando ONTAP `snapmirror initialize` comando:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Backup e ripristino dei volumi

È possibile eseguire il backup e il ripristino dei volumi su altri storage SolidFire, nonché su archivi di oggetti secondari compatibili con Amazon S3 o OpenStack Swift.

Quando ripristini i volumi da OpenStack Swift o Amazon S3, hai bisogno di informazioni manifeste dal processo di backup originale. Se si sta ripristinando un volume di cui è stato eseguito il backup su un sistema di storage SolidFire, non sono necessarie informazioni sul manifesto.

Trova ulteriori informazioni

- Eseguire il backup di un volume in un archivio di oggetti Amazon S3
- Eseguire il backup di un volume in un archivio di oggetti OpenStack Swift
- Eseguire il backup di un volume in un cluster di storage SolidFire
- Ripristinare un volume dal backup in un archivio di oggetti Amazon S3
- Ripristinare un volume dal backup in un archivio di oggetti OpenStack Swift
- Ripristinare un volume dal backup su un cluster di storage SolidFire

Eseguire il backup di un volume in un archivio di oggetti Amazon S3

Puoi eseguire il backup dei volumi in archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume di cui si desidera eseguire il backup.

3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Integrated Backup** sotto **Backup in**, selezionare **S3**.
5. Selezionare un'opzione in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
7. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
8. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).
9. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
10. Inserire un nametag da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di un volume in un archivio di oggetti OpenStack Swift

È possibile eseguire il backup dei volumi in archivi di oggetti esterni compatibili con OpenStack Swift.

1. Fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume di cui eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup in**.
4. Nella finestra di dialogo **Backup integrato** sotto **Backup in**, selezionare **Swift**.
5. Selezionare un formato dati in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Inserire un URL da utilizzare per accedere all'archivio di oggetti nel campo **URL**.
7. Immettere un nome utente per l'account nel campo **Nome utente**.
8. Inserire la chiave di autenticazione per l'account nel campo **Authentication Key** (chiave di autenticazione).
9. Inserire il contenitore in cui memorizzare il backup nel campo **container**.
10. **Opzionale**: Inserire un tag nome da aggiungere al prefisso nel campo **nametag**.
11. Fare clic su **Avvia lettura**.

Eseguire il backup di un volume in un cluster di storage SolidFire

È possibile eseguire il backup dei volumi che risiedono su un cluster remoto per i cluster di storage che eseguono il software Element.

Assicurarsi che i cluster di origine e di destinazione siano associati.

Vedere "Associare i cluster per la replica".

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come

autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, **Gestione** > **volumi**.
2. Fare clic sull'icona Actions (azioni) per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **SolidFire**.
5. Selezionare un'opzione in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).
7. Copiare la chiave dalla casella **Bulk Volume Write Key** negli Appunti.
8. Nel cluster di origine, andare a **Management** > **Volumes**.
9. Fare clic sull'icona Actions (azioni) per il volume di cui eseguire il backup.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo **Backup integrato** sotto **Backup in**, selezionare **SolidFire**.
12. Selezionare la stessa opzione selezionata in precedenza nel campo **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Nel campo **Bulk Volume Write Key** (chiave di scrittura volume in blocco), incollare la chiave generata in precedenza nel cluster di destinazione.
17. Fare clic su **Avvia lettura**.

Ripristinare un volume dal backup in un archivio di oggetti Amazon S3

Puoi ripristinare un volume da un backup su un archivio di oggetti Amazon S3.

1. Fare clic su **Reporting** > **Event Log**.
2. Individuare l'evento di backup che ha creato il backup da ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copiare le informazioni del manifesto negli Appunti.
5. Fare clic su **Management** > **Volumes**.
6. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
8. Nella finestra di dialogo **Integrated Restore** sotto **Restore from** (Ripristina da), selezionare **S3**.
9. Selezionare l'opzione corrispondente al backup in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.

- **Non compresso**: Un formato non compresso compatibile con altri sistemi.

10. Inserire un nome host da utilizzare per accedere all'archivio di oggetti nel campo **Nome host**.
11. Inserire un ID della chiave di accesso per l'account nel campo **Access Key ID** (ID chiave di accesso).
12. Inserire la chiave di accesso segreta per l'account nel campo **Secret Access Key** (chiave di accesso segreta).
13. Inserire il bucket S3 in cui memorizzare il backup nel campo **S3 bucket**.
14. Incollare le informazioni del manifesto nel campo **manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup in un archivio di oggetti OpenStack Swift

È possibile ripristinare un volume da un backup su un archivio di oggetti OpenStack Swift.

1. Fare clic su **Reporting** > **Event Log**.
2. Individuare l'evento di backup che ha creato il backup da ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copiare le informazioni del manifesto negli Appunti.
5. Fare clic su **Management** > **Volumes**.
6. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
8. Nella finestra di dialogo **Integrated Restore** sotto **Restore from**, selezionare **Swift**.
9. Selezionare l'opzione corrispondente al backup in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
10. Inserire un URL da utilizzare per accedere all'archivio di oggetti nel campo **URL**.
11. Immettere un nome utente per l'account nel campo **Nome utente**.
12. Inserire la chiave di autenticazione per l'account nel campo **Authentication Key** (chiave di autenticazione).
13. Inserire il nome del contenitore in cui è memorizzato il backup nel campo **container**.
14. Incollare le informazioni del manifesto nel campo **manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup su un cluster di storage SolidFire

È possibile ripristinare un volume da un backup su un cluster di storage SolidFire.

Quando si esegue il backup o il ripristino da un cluster all'altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume in blocco consente al cluster di origine di autenticarsi con il cluster di destinazione, fornendo un livello di sicurezza durante la scrittura nel volume di destinazione. Nell'ambito del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume in blocco dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Management** > **Volumes**.
2. Fare clic sull'icona Actions (azioni) per il volume che si desidera ripristinare.
3. Nel menu visualizzato, fare clic su **Restore from** (Ripristina da).
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **SolidFire**.
5. Selezionare l'opzione corrispondente al backup in **formato dati**:
   - **Nativo**: Formato compresso leggibile solo dai sistemi storage SolidFire.
   - **Non compresso**: Un formato non compresso compatibile con altri sistemi.
6. Fare clic su **generate Key** (genera chiave).
7. Copiare le informazioni **Volume Write Key** negli Appunti.
8. Nel cluster di origine, fare clic su **Management** > **Volumes**.
9. Fare clic sull'icona Actions (azioni) del volume che si desidera utilizzare per il ripristino.
10. Nel menu visualizzato, fare clic su **Backup in**.
11. Nella finestra di dialogo **Backup integrato**, selezionare **SolidFire** in **Backup su**.
12. Selezionare l'opzione corrispondente al backup in **formato dati**.
13. Inserire l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **Remote Cluster MVIP**.
14. Inserire il nome utente del cluster remoto nel campo **Remote Cluster Username** (Nome utente cluster remoto).
15. Inserire la password del cluster remoto nel campo **Remote Cluster Password**.
16. Incollare la chiave dagli appunti nel campo **Volume Write Key**.
17. Fare clic su **Avvia lettura**.

Risolvere i problemi del sistema

È necessario monitorare il sistema a scopo diagnostico e ottenere informazioni sulle tendenze delle performance e sugli stati delle varie operazioni del sistema. Potrebbe essere necessario sostituire nodi o SSD per scopi di manutenzione.

- "Visualizza informazioni sugli eventi di sistema"
- "Visualizzare lo stato delle attività in esecuzione"
- "Visualizzare gli avvisi di sistema"
- "Visualizzare l'attività delle performance dei nodi"
- "Visualizza le performance dei volumi"
- "Visualizzare le sessioni iSCSI"
- "Visualizzare le sessioni Fibre Channel"
- "Risolvere i problemi relativi ai dischi"
- "Risolvere i problemi dei nodi"
- "Utilizzo di utility per nodo per nodi di storage"
- "Lavorare con il nodo di gestione"

- "Comprendere i livelli di completezza del cluster"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Visualizza informazioni sugli eventi di sistema

È possibile visualizzare informazioni sui vari eventi rilevati nel sistema. Il sistema aggiorna i messaggi degli eventi ogni 30 secondi. Il registro eventi visualizza gli eventi chiave per il cluster.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **Event Log**.

   Per ogni evento, vengono visualizzate le seguenti informazioni:

Elemento	Descrizione
ID	ID univoco associato a ciascun evento.
Tipo di evento	Il tipo di evento registrato, ad esempio eventi API o eventi clone.
Messaggio	Messaggio associato all'evento.
Dettagli	Informazioni che aiutano a identificare il motivo per cui si è verificato l'evento.
ID servizio	Il servizio che ha segnalato l'evento (se applicabile).
Nodo	Il nodo che ha riportato l'evento (se applicabile).
ID disco	L'unità che ha segnalato l'evento (se applicabile).
Ora dell'evento	L'ora in cui si è verificato l'evento.

Trova ulteriori informazioni

Tipi di evento

Tipi di evento

Il sistema riporta diversi tipi di eventi; ogni evento è un'operazione che il sistema ha completato. Gli eventi possono essere di routine, eventi normali o eventi che richiedono l'attenzione dell'amministratore. La colonna tipi di evento nella pagina Registro eventi indica in quale parte del sistema si è verificato l'evento.

Il sistema non registra i comandi API di sola lettura nel registro eventi.

L'elenco seguente descrive i tipi di eventi che vengono visualizzati nel registro eventi:

- **ApiEvent**

  Eventi avviati da un utente attraverso un'API o un'interfaccia utente Web che modificano le impostazioni.

- **BinAssignmentsEvent**

  Eventi correlati all'assegnazione dei bin di dati. I bin sono essenzialmente container che contengono dati e sono mappati nel cluster.

- **BinSyncEvent**

  Eventi di sistema correlati a una riassegnazione di dati tra servizi a blocchi.

- **BsCheckEvent**

  Eventi di sistema correlati ai controlli del servizio a blocchi.

- **BsKillEvent**

  Eventi di sistema correlati alle interruzioni del servizio di blocco.

- **BulkOpEvent**

  Eventi correlati alle operazioni eseguite su un intero volume, ad esempio backup, ripristino, snapshot o clone.

- **CloneEvent**

  Eventi correlati alla clonazione del volume.

- **ClusterMasterEvent**

  Eventi visualizzati all'inizializzazione del cluster o in seguito a modifiche della configurazione del cluster, ad esempio l'aggiunta o la rimozione di nodi.

- **CsumEvent**

  Eventi relativi a checksum di dati non validi sul disco.

- **DataEvent**

  Eventi relativi alla lettura e alla scrittura dei dati.

- **DbEvent**

  Eventi correlati al database globale gestito dai nodi dell'ensemble nel cluster.

- **DriveEvent**

  Eventi relativi alle operazioni del disco.

- **EncryptionAtRestEvent**

  Eventi correlati al processo di crittografia su un cluster.

- **EnsembleEvent**

  Eventi correlati all'aumento o alla diminuzione del numero di nodi in un ensemble.

- **FiberChannelEvent**

  Eventi relativi alla configurazione e alle connessioni ai nodi.

- **GcEvent**

  Gli eventi relativi ai processi vengono eseguiti ogni 60 minuti per recuperare lo storage su dischi a blocchi. Questo processo è noto anche come garbage collection.

- **IeEvent**

  Errore di sistema interno.

- **InstallEvent**

  Eventi di installazione automatica del software. Il software viene installato automaticamente su un nodo in sospeso.

- **ISCSIEvent**

  Eventi relativi a problemi iSCSI nel sistema.

- **LimitEvent**

  Eventi correlati al numero di volumi o volumi virtuali in un account o nel cluster che si avvicina al numero massimo consentito.

- **MaintenanceModeEvent**

  Eventi correlati alla modalità di manutenzione del nodo, ad esempio la disattivazione del nodo.

- **NetworkEvent**

  Eventi relativi allo stato della rete virtuale.

- **PlatformHardwareEvent**

  Eventi relativi a problemi rilevati sui dispositivi hardware.

- **RemoteClusterEvent**

  Eventi relativi all'associazione remota del cluster.

- **SchedulerEvent**

  Eventi correlati agli snapshot pianificati.

- **ServiceEvent**

Eventi relativi allo stato del servizio di sistema.

- **SliceEvent**

  Eventi correlati al server Slice, come la rimozione di un disco o di un volume di metadati.

  Esistono tre tipi di eventi di riassegnazione delle sezioni, che includono informazioni sul servizio a cui viene assegnato un volume:

  - flipping: passaggio del servizio primario a un nuovo servizio primario

    ```
    sliceID oldPrimaryServiceID->newPrimaryServiceID
    ```

  - spostamento: passaggio del servizio secondario a un nuovo servizio secondario

    ```
    sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
    ```

  - eliminazione: rimozione di un volume da un set di servizi

    ```
    sliceID {oldSecondaryServiceID(s)}
    ```

- **SnmpTrapEvent**

  Eventi relativi ai trap SNMP.

- **StatEvent**

  Eventi relativi alle statistiche di sistema.

- **TsEvent**

  Eventi relativi al servizio di trasporto del sistema.

- *Exception *

  Eventi correlati a eccezioni di sistema impreviste.

- **UreEvent**

  Eventi correlati a errori di lettura non ripristinabili che si verificano durante la lettura dal dispositivo di storage.

- **VasaProviderEvent**

  Eventi relativi a un provider VASA (vSphere API for Storage Awareness).

Visualizzare lo stato delle attività in esecuzione

È possibile visualizzare lo stato di avanzamento e completamento delle attività in

esecuzione nell'interfaccia utente Web che vengono segnalate dai metodi API ListSyncJobs e ListBulkVolumeJobs. È possibile accedere alla pagina delle attività in esecuzione dalla scheda Reporting dell'interfaccia utente di Element.

Se sono presenti numerose attività, il sistema potrebbe metterle in coda ed eseguirle in batch. La pagina operazioni in esecuzione visualizza i servizi attualmente sincronizzati. Una volta completato, un'attività viene sostituita dalla successiva attività di sincronizzazione in coda. Le attività di sincronizzazione potrebbero continuare a essere visualizzate nella pagina delle attività in esecuzione fino a quando non sono più necessarie.

È possibile visualizzare i dati di sincronizzazione delle repliche per i volumi sottoposti a replica nella pagina delle attività in esecuzione del cluster contenente il volume di destinazione.

Visualizzare gli avvisi di sistema

È possibile visualizzare gli avvisi per informazioni sugli errori o sugli errori del cluster nel sistema. Gli avvisi possono essere informazioni, avvisi o errori e rappresentano un buon indicatore della corretta esecuzione del cluster. La maggior parte degli errori si risolve automaticamente.

È possibile utilizzare il metodo API ListClusterFaults per automatizzare il monitoraggio degli avvisi. Ciò consente di ricevere una notifica di tutti gli avvisi che si verificano.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **Alerts**.

   Il sistema aggiorna gli avvisi sulla pagina ogni 30 secondi.

   Per ogni evento, vengono visualizzate le seguenti informazioni:

Elemento	Descrizione
ID	ID univoco associato a un avviso del cluster.

Severità	Il grado di importanza dell'avviso. Valori possibili: • Attenzione: Un problema di lieve entità che potrebbe richiedere presto l'intervento dell'utente. Gli aggiornamenti del sistema sono ancora consentiti. • Errore: Un errore che potrebbe causare il peggioramento delle performance o la perdita di alta disponibilità (ha). Gli errori in genere non devono influire altrimenti sul servizio. • Critico: Un guasto grave che influisce sul servizio. Il sistema non è in grado di fornire richieste di i/o API o client. Il funzionamento in questo stato potrebbe causare la potenziale perdita di dati. • BestPractice: Non viene utilizzata una procedura consigliata per la configurazione del sistema.
Tipo	L'elemento interessato dal guasto. Può essere un nodo, un disco, un cluster, un servizio o un volume.
Nodo	ID nodo per il nodo a cui si riferisce questo guasto. Incluso per i guasti al nodo e al disco, altrimenti impostato su - (DASH).
ID disco	ID del disco a cui si riferisce questo guasto. Incluso per i guasti del disco, altrimenti impostato su - (DASH).
Codice di errore	Un codice descrittivo che indica la causa del guasto.
Dettagli	Una descrizione del guasto con ulteriori dettagli.
Data	La data e l'ora in cui è stato registrato il guasto.

2. Fare clic su **Show Details** (Mostra dettagli) per visualizzare le informazioni relative all'avviso.
3. Per visualizzare i dettagli di tutti gli avvisi nella pagina, fare clic sulla colonna Dettagli.

   Dopo che il sistema ha risolto un avviso, tutte le informazioni relative all'avviso, inclusa la data in cui è stato risolto, vengono spostate nell'area Resolved (risolto).

Trova ulteriori informazioni

- Codici di guasto del cluster
- "Gestire lo storage con l'API Element"

Codici di guasto del cluster

Il sistema segnala un errore o uno stato che potrebbe essere interessante generando un codice di errore, elencato nella pagina Avvisi. Questi codici consentono di determinare quale componente del sistema ha rilevato l'avviso e perché è stato generato.

L'elenco seguente descrive i diversi tipi di codici:

- **AuthenticationServiceFault**

  Il servizio di autenticazione su uno o più nodi del cluster non funziona come previsto.

  Contattare il supporto NetApp per assistenza.

- **AvailableVirtualNetworkIPAddressesLow**

  Il numero di indirizzi della rete virtuale nel blocco di indirizzi IP è basso.

  Per risolvere questo guasto, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuale.

- **BlockClusterFull**

  Lo spazio di storage a blocchi disponibile non è sufficiente per supportare una perdita di un singolo nodo. Per informazioni dettagliate sui livelli di completezza del cluster, vedere il metodo API GetClusterFullThreshold. Questo guasto del cluster indica una delle seguenti condizioni:

  - Stage3Low (Avvertenza): Soglia definita dall'utente superata. Regolare le impostazioni di Cluster Full o aggiungere altri nodi.
  - Stage4critical (errore): Spazio insufficiente per il ripristino in caso di guasto a 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
  - Stage5CompletelyConsumed (critico)1; non sono consentite operazioni di scrittura o nuove connessioni iSCSI. Verranno mantenute le attuali connessioni iSCSI. Le operazioni di scrittura non vengono eseguite fino a quando non viene aggiunta una maggiore capacità al cluster. Per risolvere questo errore, eliminare o eliminare volumi o aggiungere un altro nodo di storage al cluster di storage.

- **BlocksDegraded**

  I dati del blocco non vengono più replicati completamente a causa di un errore.

Severità	Descrizione
Attenzione	Sono accessibili solo due copie complete dei dati del blocco.
Errore	È possibile accedere a una sola copia completa dei dati del blocco.
Critico	Non è possibile accedere a copie complete dei dati del blocco.

  Nota: lo stato di avviso può verificarsi solo su un sistema Triple Helix.

  Per risolvere questo guasto, ripristinare i nodi offline o i servizi di blocco oppure contattare il supporto

NetApp per assistenza.

- **BlockServiceToFull**

  Un servizio a blocchi sta utilizzando troppo spazio.

  Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **BlockServiceUnhealthy**

  Un servizio a blocchi è stato rilevato come non integro:

  - Severità = Avvertenza: Non viene intrapresa alcuna azione. Questo periodo di avviso scade tra cTimeUntilBSIsKilledMsec=330000 millisecondi.
  - Severità = errore: Il sistema sta discommissionando automaticamente i dati e replicando i dati su altri dischi integri.
  - Severità = critico: Ci sono servizi di blocco guasti su diversi nodi maggiori o uguali al numero di repliche (2 per doppia elica). I dati non sono disponibili e la sincronizzazione bin non verrà completata. Verificare la presenza di problemi di connettività di rete ed errori hardware. In caso di guasto di componenti hardware specifici, si verificheranno altri guasti. Il guasto viene disattivato quando il servizio a blocchi è accessibile o quando il servizio è stato disattivato.

- **ClockSkewExceedsFaultThreshold**

  L'inclinazione temporale tra il master del cluster e il nodo che presenta un token supera la soglia consigliata. Il cluster di storage non è in grado di correggere automaticamente l'inclinazione temporale tra i nodi.

  Per risolvere questo errore, utilizzare server NTP interni alla rete, anziché i valori predefiniti per l'installazione. Se si utilizza un server NTP interno, contattare il supporto NetApp per assistenza.

- **ClusterCannotSync**

  Esiste una condizione di spazio insufficiente e i dati sulle unità di storage a blocchi offline non possono essere sincronizzati con le unità ancora attive.

  Per risolvere questo guasto, aggiungere ulteriore storage.

- **ClusterFull**

  Non c'è più spazio di storage libero nel cluster di storage.

  Per risolvere questo guasto, aggiungere ulteriore storage.

- **ClusterIOPSAreOverProvised**

  Il provisioning degli IOPS del cluster è eccessivo. La somma di tutti gli IOPS QoS minimi è maggiore degli IOPS previsti del cluster. La QoS minima non può essere mantenuta per tutti i volumi contemporaneamente.

  Per risolvere questo problema, ridurre le impostazioni minime di QoS IOPS per i volumi.

- **DisableDriveSecurityFailed**

  Il cluster non è configurato per abilitare la sicurezza del disco (crittografia a riposo), ma almeno un disco ha

attivato la sicurezza del disco, il che significa che la disattivazione della sicurezza del disco su tali dischi ha avuto esito negativo. Questo guasto viene registrato con la severità “Warning”.

Per risolvere questo guasto, controllare i dettagli del guasto per individuare il motivo per cui non è stato possibile disattivare la protezione del disco. I motivi possibili sono:

- Impossibile acquisire la chiave di crittografia. Esaminare il problema di accesso alla chiave o al server delle chiavi esterno.
- L’operazione di disattivazione non è riuscita sul disco, determinare se potrebbe essere stata acquisita la chiave errata. Se nessuna di queste è la causa del guasto, potrebbe essere necessario sostituire il disco.

È possibile tentare di ripristinare un disco che non disattiva correttamente la protezione anche se viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere i dischi dal sistema spostandoli su Available (disponibile), eseguire una cancellazione sicura sul disco e riportarli su Active (attivo).

- **DisconnectedClusterPair**

  Una coppia di cluster è disconnessa o configurata in modo errato. Controllare la connettività di rete tra i cluster.

- **DisconnectedRemoteNode**

  Un nodo remoto è disconnesso o configurato in modo non corretto. Verificare la connettività di rete tra i nodi.

- **DisconnettedSnapMirrorEndpoint**

  Un endpoint SnapMirror remoto è disconnesso o configurato in modo errato. Controllare la connettività di rete tra il cluster e SnapMirrorEndpoint remoto.

- **DriveAvailable**

  Uno o più dischi sono disponibili nel cluster. In generale, tutti i cluster devono avere tutti i dischi aggiunti e nessuno nello stato disponibile. Se il guasto si verifica in modo imprevisto, contattare il supporto NetApp.

  Per risolvere questo guasto, aggiungere eventuali dischi disponibili al cluster di storage.

- **DriveFailed**

  Il cluster restituisce questo errore quando uno o più dischi si sono guastati, indicando una delle seguenti condizioni:

  - Drive Manager non può accedere al disco.
  - Il servizio slice o block ha avuto un errore troppe volte, presumibilmente a causa di errori di lettura o scrittura del disco e non può essere riavviato.
  - Disco mancante.
  - Il servizio master per il nodo non è accessibile (tutti i dischi nel nodo sono considerati mancanti/guasti).
  - L’unità è bloccata e non è possibile acquisire la chiave di autenticazione dell’unità.
  - L’unità è bloccata e l’operazione di sblocco non riesce. Per risolvere questo problema:
  - Verificare la connettività di rete del nodo.

- Sostituire l’unità.
- Assicurarsi che la chiave di autenticazione sia disponibile.

- **DriveHealthFault**

  Un disco non ha superato il controllo dello stato DI salute SMART e di conseguenza le funzioni del disco sono ridotte. Per questo guasto è presente un livello di gravità critico:

  - Disco con seriale: <serial number> nello slot: <node slot> <drive slot> non ha superato IL controllo dello stato DI salute generale SMART. Per risolvere il problema, sostituire il disco.

- **DriveWearFault**

  La durata rimanente di un disco è scesa al di sotto delle soglie, ma è ancora in funzione.esistono due livelli di gravità possibili per questo guasto: Critico e Avviso:

  - Disco con seriale: <serial number> nello slot: <node slot> <drive slot> ha livelli di usura critici.
  - Disco con seriale: <serial number> nello slot: <node slot> <drive slot> ha basse riserve di usura. Per risolvere il problema, sostituire il disco al più presto.

- **DuplicateClusterMasterCandidate**

  È stato rilevato più di un candidato master del cluster di storage. Contattare il supporto NetApp per assistenza.

- **EnableDriveSecurityFailed**

  Il cluster è configurato per richiedere la protezione del disco (crittografia a riposo), ma non è stato possibile attivare la protezione del disco su almeno un disco. Questo guasto viene registrato con la severità “Warning”.

  Per risolvere questo guasto, controllare i dettagli del guasto per individuare il motivo per cui non è stato possibile attivare la protezione del disco. I motivi possibili sono:

  - Impossibile acquisire la chiave di crittografia. Esaminare il problema di accesso alla chiave o al server delle chiavi esterno.
  - L’operazione di abilitazione non è riuscita sul disco, determinare se potrebbe essere stata acquisita la chiave errata. Se nessuna di queste è la causa del guasto, potrebbe essere necessario sostituire il disco.

  È possibile tentare di ripristinare un disco che non abilita correttamente la protezione anche se viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere i dischi dal sistema spostandoli su Available (disponibile), eseguire una cancellazione sicura sul disco e riportarli su Active (attivo).

- **EnsembleDebraded**

  La connettività di rete o l’alimentazione di uno o più nodi dell’ensemble sono state perse.

  Per risolvere questo errore, ripristinare la connettività di rete o l’alimentazione.

- **eccezione**

  Un guasto segnalato che non è un guasto di routine. Questi guasti non vengono cancellati automaticamente dalla coda degli errori. Contattare il supporto NetApp per assistenza.

- **FailedSpaceTooFull**

  Un servizio a blocchi non risponde alle richieste di scrittura dei dati. In questo modo il servizio slice esaurisce lo spazio necessario per memorizzare le scritture non riuscite.

  Per risolvere questo errore, ripristinare la funzionalità dei servizi a blocchi per consentire la normale continuazione delle operazioni di scrittura e l'archiviazione dello spazio non riuscito dal servizio slice.

- **FanSensor**

  Un sensore della ventola è guasto o mancante.

  Per risolvere questo guasto, sostituire l'hardware guasto.

- **FiberChannelAccessDebraded**

  Un nodo Fibre Channel non risponde ad altri nodi nel cluster di storage sul proprio IP di storage per un certo periodo di tempo. In questo stato, il nodo viene quindi considerato non reattivo e genera un errore del cluster. Controllare la connettività di rete.

- **FiberChannelAccessUnavailable**

  Tutti i nodi Fibre Channel non rispondono. Vengono visualizzati gli ID del nodo. Controllare la connettività di rete.

- **FiberChannelActiveIxL**

  Il numero di Nexus IXL si sta avvicinando al limite supportato di 8000 sessioni attive per nodo Fibre Channel.

  - Il limite delle Best practice è 5500.
  - Il limite di avviso è 7500.
  - Il limite massimo (non applicato) è 8192. Per risolvere questo guasto, ridurre il numero di Nexus IXL al di sotto del limite di Best practice di 5500.

- **FiberChannelConfig**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - Sullo slot PCI è presente una porta Fibre Channel imprevista.
  - Esiste un modello HBA Fibre Channel imprevisto.
  - Si è verificato un problema con il firmware di un HBA Fibre Channel.
  - Una porta Fibre Channel non è in linea.
  - Si è verificato un problema persistente nella configurazione del pass-through Fibre Channel. Contattare il supporto NetApp per assistenza.

- **FiberChannelIOPS**

  Il numero totale di IOPS si sta avvicinando al limite di IOPS per i nodi Fibre Channel nel cluster. I limiti sono:

  - FC0025: Limite DI 450.000 IOPS con dimensione del blocco 4K per nodo Fibre Channel.
  - FCN001: Limite OPS di 625 K con dimensione del blocco 4K per nodo Fibre Channel. Per risolvere

questo guasto, bilanciare il carico su tutti i nodi Fibre Channel disponibili.

- **FiberChannelStaticIxL**

  Il numero di Nexus IXL si sta avvicinando al limite supportato di 16000 sessioni statiche per nodo Fibre Channel.

  - Il limite delle Best practice è 11000.
  - Il limite di avviso è 15000.
  - Il limite massimo (imposto) è 16384. Per risolvere questo guasto, ridurre il numero di Nexus IXL al di sotto del limite di Best practice di 11000.

- **FileSystemCapacityLow**

  Spazio insufficiente su uno dei filesystem.

  Per risolvere questo errore, aggiungere più capacità al file system.

- **FipsDrivesMismatch**

  Un'unità non FIPS è stata fisicamente inserita in un nodo di storage FIPS o un'unità FIPS è stata fisicamente inserita in un nodo di storage non FIPS. Viene generato un singolo guasto per nodo ed elenca tutti i dischi interessati.

  Per risolvere questo guasto, rimuovere o sostituire il disco o i dischi non corrispondenti in questione.

- **FipsDrivesOutOfCompliance**

  Il sistema ha rilevato che la crittografia a riposo è stata disattivata dopo l'attivazione della funzione dischi FIPS. Questo errore viene generato anche quando la funzione FIPS Drives (dischi FIPS) è attivata e nel cluster di storage è presente un disco o un nodo non FIPS.

  Per risolvere questo errore, attivare la crittografia a riposo o rimuovere l'hardware non FIPS dal cluster di storage.

- **FipsSelfTestFailure**

  Il sottosistema FIPS ha rilevato un errore durante l'autotest.

  Contattare il supporto NetApp per assistenza.

- **HardwareConfigMismatch**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - La configurazione non corrisponde alla definizione del nodo.
  - Le dimensioni del disco non sono corrette per questo tipo di nodo.
  - È stato rilevato un disco non supportato. Una possibile ragione è che la versione dell'elemento installata non riconosce questo disco. Si consiglia di aggiornare il software Element su questo nodo.
  - Il firmware del disco non corrisponde.
  - Lo stato che supporta la crittografia del disco non corrisponde al nodo. Contattare il supporto NetApp per assistenza.

- **IdPCertificateExpiration**

Il certificato SSL del provider di servizi del cluster da utilizzare con un provider di identità di terze parti (IdP) è in fase di scadenza o è già scaduto. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione
Attenzione	Il certificato scade entro 30 giorni.
Errore	Il certificato scade entro 7 giorni.
Critico	Il certificato scade entro 3 giorni o è già scaduto.

Per risolvere questo errore, aggiornare il certificato SSL prima della scadenza. Utilizzare il metodo UpdateIdpConfiguration API con `refreshCertificateExpirationTime=true` Per fornire il certificato SSL aggiornato.

- **InconsistentBondModes**

  Mancano le modalità bond sul dispositivo VLAN. Questo guasto visualizza la modalità bond prevista e la modalità bond attualmente in uso.

- **InconsistentInterfaceConfiguration**

  La configurazione dell'interfaccia non è coerente.

  Per risolvere questo errore, assicurarsi che le interfacce dei nodi nel cluster di storage siano configurate in modo coerente.

- **InconsistentMentus**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - Mancata corrispondenza Bond1G: MTU non coerenti rilevate sulle interfacce Bond1G.
  - Mancata corrispondenza Bond10G: MTU non coerenti rilevate sulle interfacce Bond10G. Questo errore visualizza il nodo o i nodi in questione insieme al valore MTU associato.

- **InconsistentRoutingRules**

  Le regole di routing per questa interfaccia non sono coerenti.

- **InconsistentSubnetMasks**

  La maschera di rete sul dispositivo VLAN non corrisponde alla maschera di rete registrata internamente per la VLAN. Questo errore visualizza la maschera di rete prevista e la maschera di rete attualmente in uso.

- **IncorrectBondPortCount**

  Il numero di porte bond non è corretto.

- **InvalidConfiguredFiberChannelNodeCount**

  Una delle due connessioni di nodo Fibre Channel previste è degradata. Questo errore viene visualizzato quando è collegato un solo nodo Fibre Channel.

Per risolvere questo guasto, controllare la connettività di rete del cluster e il cablaggio di rete e verificare la presenza di servizi non riusciti. Se non ci sono problemi di rete o di servizio, contattare il supporto NetApp per la sostituzione di un nodo Fibre Channel.

- **IrqBalanceFailed**

  Si è verificata un'eccezione durante il tentativo di bilanciare gli interrupt.

  Contattare il supporto NetApp per assistenza.

- **KmipCertificateFault**
  - Il certificato dell'autorità di certificazione principale (CA) sta per scadere.

    Per risolvere questo errore, acquisire un nuovo certificato dalla CA principale con una data di scadenza di almeno 30 giorni e utilizzare ModifyKeyServerKmip per fornire il certificato CA principale aggiornato.

  - Il certificato client è in scadenza.

    Per risolvere questo errore, creare una nuova CSR utilizzando GetClientCertificateSigningRequest, fare in modo che la nuova data di scadenza sia di almeno 30 giorni e utilizzare ModifyKeyServerKmip per sostituire il certificato del client KMIP in scadenza con il nuovo certificato.

  - Il certificato dell'autorità di certificazione principale (CA) è scaduto.

    Per risolvere questo errore, acquisire un nuovo certificato dalla CA principale con una data di scadenza di almeno 30 giorni e utilizzare ModifyKeyServerKmip per fornire il certificato CA principale aggiornato.

  - Certificato client scaduto.

    Per risolvere questo errore, creare una nuova CSR utilizzando GetClientCertificateSigningRequest, fare in modo che la nuova data di scadenza sia di almeno 30 giorni e utilizzare ModifyKeyServerKmip per sostituire il certificato client KMIP scaduto con il nuovo certificato.

  - Errore nel certificato dell'autorità di certificazione principale (CA).

    Per risolvere questo errore, verificare che sia stato fornito il certificato corretto e, se necessario, riacquisire il certificato dalla CA principale. Utilizzare ModifyKeyServerKmip per installare il certificato client KMIP corretto.

  - Errore nel certificato del client.

    Per risolvere questo errore, verificare che sia installato il certificato client KMIP corretto. La CA principale del certificato client deve essere installata su EKS. Utilizzare ModifyKeyServerKmip per installare il certificato client KMIP corretto.

- **KmipServerFault**
  - Errore di connessione

    Per risolvere questo guasto, verificare che il server delle chiavi esterne sia attivo e raggiungibile tramite la rete. Utilizzare TestKeyServerKimp e TestKeyProviderKmip per verificare la connessione.

  - Errore di autenticazione

    Per risolvere questo errore, verificare che vengano utilizzati i certificati CA root e client KMIP corretti e che la chiave privata e il certificato del client KMIP corrispondano.

◦ Errore del server

Per risolvere questo guasto, controllare i dettagli dell'errore. In base all'errore restituito, potrebbe essere necessario eseguire la risoluzione dei problemi sul server chiavi esterno.

- **MemoriaEccThreshold**

Sono stati rilevati numerosi errori ECC correggibili o non correggibili. Questo guasto utilizza le seguenti severità in base all'urgenza:

Evento	Severità	Descrizione
Un singolo cErrorCount DIMM raggiunge cDimmCorrectableErrWarrThreshold.	Attenzione	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM Slot>
Un singolo cErrorCount DIMM rimane al di sopra di cDimmCorrectableErrWarrThreshold fino alla scadenza di cErrorFaultTimer per il DIMM.	Errore	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM>
Un controller di memoria riporta cErrorCount al di sopra di cMemCtlrCorrectableErrWarrThreshold e cMemCtlrCorrectableErrWarrWarrDuration è specificato.	Attenzione	Errori di memoria ECC correggibili superiori alla soglia sul controller di memoria: <Processor> <Memory Controller>
Un controller di memoria segnala cErrorCount al di sopra di cMemCtlrCorrectableErrWarnThreshold fino alla scadenza di cErrorFaultTimer per il controller di memoria.	Errore	Errori di memoria ECC correggibili superiori alla soglia su DIMM: <Processor> <DIMM>
Un singolo DIMM riporta un uErrorCount superiore a zero, ma inferiore a cDimmUncorrectableErrFaultThreshold.	Attenzione	Errori di memoria ECC non correggibili rilevati su DIMM: <Processor> <DIMM Slot>
Un singolo DIMM riporta un uErrorCount di almeno cDimmUncorrectableErrFaultThreshold.	Errore	Errori di memoria ECC non correggibili rilevati su DIMM: <Processor> <DIMM Slot>

Un controller di memoria segnala un valore uErrorCount superiore a zero, ma inferiore a cMemCtlrUncorrectableErrFaultThreshold.	Attenzione	Errori di memoria ECC non correggibili rilevati sul controller di memoria: <Processor> <Memory Controller>
Un controller di memoria segnala un uErrorCount di almeno cMemCtlrUncorrectableErrFaultThreshold.	Errore	Errori di memoria ECC non correggibili rilevati sul controller di memoria: <Processor> <Memory Controller>

Per risolvere questo guasto, contattare il supporto NetApp per assistenza.

- **MemoriaUsageThreshold**

  L'utilizzo della memoria è superiore al normale. Questo guasto utilizza le seguenti severità in base all'urgenza:

  Per informazioni più dettagliate sul tipo di guasto, vedere l'intestazione **Dettagli** nell'errore.

Severità	Descrizione
Attenzione	Memoria di sistema insufficiente.
Errore	Memoria di sistema molto bassa.
Critico	La memoria di sistema è completamente consumata.

  Per risolvere questo guasto, contattare il supporto NetApp per assistenza.

- **MetadataClusterFull**

  Lo spazio di storage dei metadati non è sufficiente per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di completezza del cluster, vedere il metodo API GetClusterFullThreshold. Questo guasto del cluster indica una delle seguenti condizioni:

  - Stage3Low (Avvertenza): Soglia definita dall'utente superata. Regolare le impostazioni di Cluster Full o aggiungere altri nodi.
  - Stage4critical (errore): Spazio insufficiente per il ripristino in caso di guasto a 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
  - Stage5CompletelyConsumed (critico)1; non sono consentite operazioni di scrittura o nuove connessioni iSCSI. Verranno mantenute le attuali connessioni iSCSI. Le operazioni di scrittura non vengono eseguite fino a quando non viene aggiunta una maggiore capacità al cluster. Eliminare o eliminare i dati o aggiungere altri nodi. Per risolvere questo errore, eliminare o eliminare volumi o aggiungere un altro nodo di storage al cluster di storage.

- **MtuCheckFailure**

  Un dispositivo di rete non è configurato per le dimensioni MTU corrette.

Per risolvere questo guasto, assicurarsi che tutte le interfacce di rete e le porte dello switch siano configurate per i frame jumbo (MTU fino a 9000 byte).

- **NetworkConfig**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - Non è presente un'interfaccia prevista.
  - È presente un'interfaccia duplicata.
  - Un'interfaccia configurata non è disponibile.
  - È necessario riavviare la rete. Contattare il supporto NetApp per assistenza.
- **NoAvailableVirtualNetworkIPAddresses**

  Nessun indirizzo di rete virtuale disponibile nel blocco di indirizzi IP.

  - Il TAG virtualNetworkID n. (n. n.) non ha indirizzi IP di storage disponibili. Non è possibile aggiungere nodi aggiuntivi al cluster. Per risolvere questo guasto, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuale.
- **NodeHardwareFault (<name> interfaccia di rete non attivo o cavo scollegato)**

  Un'interfaccia di rete è inattiva o il cavo è scollegato.

  Per risolvere questo guasto, controllare la connettività di rete per il nodo o i nodi.
- **NodeHardwareFault (lo stato in grado di supportare la crittografia del disco non corrisponde allo stato in grado di supportare la crittografia del nodo per il disco nello slot <node slot> <drive slot>)**

  Un disco non corrisponde alle funzionalità di crittografia con il nodo di storage in cui è installato.
- **NodeHardwareFault (<actual size> delle dimensioni del disco <drive type> non corretto per il disco nello slot <node slot> <drive slot> per questo tipo di nodo - <expected size> previsto)**

  Un nodo di storage contiene un disco di dimensioni non corrette per questo nodo.
- **NodeHardwareFault (disco non supportato rilevato nello slot <node slot> <drive slot>; le statistiche e le informazioni sullo stato dei dischi non saranno disponibili)**

  Un nodo di storage contiene un disco non supportato.
- **NodeHardwareFault (l'unità nello slot <node slot> <drive slot> deve utilizzare la versione del firmware <expected version>, ma la versione <actual version> non è supportata)**

  Un nodo di storage contiene un disco con una versione del firmware non supportata.
- **NodeMaintenanceMode**

  Un nodo è stato posto in modalità di manutenzione. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione

Attenzione	Indica che il nodo è ancora in modalità di manutenzione.
Errore	Indica che la modalità di manutenzione non è riuscita a disattivarsi, probabilmente a causa di uno standby guasto o attivo.

Per risolvere questo guasto, disattivare la modalità di manutenzione al termine della manutenzione. Se l'errore di livello di errore persiste, contattare il supporto NetApp per assistenza.

- **NodeOffline**

  Il software Element non è in grado di comunicare con il nodo specificato. Controllare la connettività di rete.

- **NotUsingLACPBondMode**

  La modalità di bonding LACP non è configurata.

  Per risolvere questo errore, utilizzare il bonding LACP durante l'implementazione dei nodi di storage; i client potrebbero riscontrare problemi di performance se LACP non è attivato e configurato correttamente.

- **NtpServerUnreachable**

  Il cluster di storage non è in grado di comunicare con il server o i server NTP specificati.

  Per risolvere questo errore, controllare la configurazione del server NTP, della rete e del firewall.

- **NtpTimeNotInSync**

  La differenza tra il tempo del cluster di storage e il tempo del server NTP specificato è eccessiva. Il cluster di storage non è in grado di correggere automaticamente la differenza.

  Per risolvere questo errore, utilizzare server NTP interni alla rete, anziché i valori predefiniti per l'installazione. Se si utilizzano server NTP interni e il problema persiste, contattare il supporto NetApp per assistenza.

- **NvramDeviceStatus**

  Si è verificato un errore, un errore o un errore di un dispositivo NVRAM. Questo guasto ha le seguenti severità:

Severità	Descrizione

Attenzione	L’hardware ha rilevato un avviso. Questa condizione può essere transitoria, ad esempio un avviso di temperatura. • NvmLifetimeError • NvmLifetimeStatus • EnergySourceLifetimeStatus • EnergySourceTemperatureStatus • WarningThresholdExceed
Errore	L’hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere il disco slice dall’operazione (questo genera un evento di rimozione del disco). Se i servizi di slice secondaria non sono disponibili, il disco non verrà rimosso. Errori restituiti oltre agli errori di livello di avviso: • Il punto di montaggio del dispositivo NVRAM non esiste. • La partizione del dispositivo NVRAM non esiste. • La partizione del dispositivo NVRAM esiste, ma non è montata.
Critico	L’hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere il disco slice dall’operazione (questo genera un evento di rimozione del disco). Se i servizi di slice secondaria non sono disponibili, il disco non verrà rimosso. • PersistenzaLost • ArmStatusSaveNArmed • CsaveStatusError

Sostituire l’hardware guasto nel nodo. Se questo non risolve il problema, contattare il supporto NetApp per assistenza.

- **PowerSupplyError**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - Non è presente alcun alimentatore.
  - Si è verificato un guasto nell’alimentatore.
  - Un ingresso di alimentazione è mancante o fuori portata. Per risolvere questo guasto, verificare che l’alimentazione ridondante sia fornita a tutti i nodi. Contattare il supporto NetApp per assistenza.

- **ProvisionedSpaceTooFull**

  La capacità complessiva fornita dal cluster è troppo piena.

Per risolvere questo errore, aggiungere ulteriore spazio fornito o eliminare e rimuovere volumi.

- **RemoteRepAsyncDelayExced**

  Il ritardo asincrono configurato per la replica è stato superato. Controllare la connettività di rete tra i cluster.

- **RemoteRepClusterFull**

  I volumi hanno messo in pausa la replica remota perché il cluster di storage di destinazione è troppo pieno.

  Per risolvere questo guasto, liberare spazio sul cluster di storage di destinazione.

- **RemoteRepSnapshotClusterFull**

  I volumi hanno messo in pausa la replica remota degli snapshot perché il cluster di storage di destinazione è troppo pieno.

  Per risolvere questo guasto, liberare spazio sul cluster di storage di destinazione.

- **RemoteRepSnapshotsExceededededLimit**

  I volumi hanno messo in pausa la replica remota degli snapshot perché il volume del cluster di storage di destinazione ha superato il limite di snapshot.

  Per risolvere questo guasto, aumentare il limite di snapshot sul cluster di storage di destinazione.

- **ScheduleActionError**

  Una o più attività pianificate sono eseguite, ma non sono riuscite.

  L'errore viene cancellato se l'attività pianificata viene eseguita di nuovo e ha esito positivo, se l'attività pianificata viene eliminata o se l'attività viene messa in pausa e ripresa.

- **SensorReadingFailed**

  L'autotest del Baseboard Management Controller (BMC) non è riuscito o un sensore non è in grado di comunicare con il BMC.

  Contattare il supporto NetApp per assistenza.

- **ServiceNotRunning**

  Un servizio richiesto non è in esecuzione.

  Contattare il supporto NetApp per assistenza.

- **SliceServiceTooFull**

  A un servizio slice è assegnata una capacità di provisioning troppo bassa.

  Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **SliceServiceUnhealthy**

  Il sistema ha rilevato che un servizio slice non è integro e lo sta automaticamente smantellando.

- Severità = Avvertenza: Non viene intrapresa alcuna azione. Questo periodo di avviso scadrà tra 6 minuti.
- Severità = errore: Il sistema sta discommissionando automaticamente i dati e replicando i dati su altri dischi integri. Verificare la presenza di problemi di connettività di rete ed errori hardware. In caso di guasto di componenti hardware specifici, si verificheranno altri guasti. Il guasto viene disattivato quando il servizio slice è accessibile o quando il servizio è stato disattivato.

- **SshEnabled**

  Il servizio SSH è attivato su uno o più nodi nel cluster di storage.

  Per risolvere questo guasto, disattivare il servizio SSH sul nodo o sui nodi appropriati o contattare il supporto NetApp per assistenza.

- **SslCertificateExpiration**

  Il certificato SSL associato a questo nodo è in fase di scadenza o è scaduto. Questo guasto utilizza le seguenti severità in base all'urgenza:

Severità	Descrizione
Attenzione	Il certificato scade entro 30 giorni.
Errore	Il certificato scade entro 7 giorni.
Critico	Il certificato scade entro 3 giorni o è già scaduto.

  Per risolvere questo guasto, rinnovare il certificato SSL. Se necessario, contattare il supporto NetApp per assistenza.

- **StrandedCapacity**

  Un singolo nodo rappresenta oltre la metà della capacità del cluster di storage.

  Per mantenere la ridondanza dei dati, il sistema riduce la capacità del nodo più grande in modo che parte della sua capacità a blocchi sia bloccata (non utilizzata).

  Per risolvere questo guasto, aggiungere più dischi ai nodi di storage esistenti o aggiungere nodi di storage al cluster.

- **TempSensor**

  Un sensore di temperatura segnala temperature superiori al normale. Questo guasto può essere attivato in combinazione con guasti powerSupplyError o fanSensor.

  Per risolvere questo guasto, verificare l'eventuale presenza di ostruzioni nel flusso d'aria in prossimità del cluster di storage. Se necessario, contattare il supporto NetApp per assistenza.

- **upgrade**

  Un aggiornamento è in corso da oltre 24 ore.

  Per risolvere questo guasto, riprendere l'aggiornamento o contattare il supporto NetApp per assistenza.

- **UnresponsiveService**

  Un servizio non risponde.

  Contattare il supporto NetApp per assistenza.

- **VirtualNetworkConfig**

  Questo guasto del cluster indica una delle seguenti condizioni:

  - Non è presente un'interfaccia.
  - Esiste uno spazio dei nomi non corretto su un'interfaccia.
  - La netmask non è corretta.
  - Indirizzo IP errato.
  - Un'interfaccia non è attiva e in esecuzione.
  - Esiste un'interfaccia superflua su un nodo. Contattare il supporto NetApp per assistenza.

- **VolumesDegraded**

  I volumi secondari non hanno terminato la replica e la sincronizzazione. Il messaggio viene cancellato al termine della sincronizzazione.

- **VolumesOffline**

  Uno o più volumi nel cluster di storage sono offline. Sarà presente anche il guasto **volumeDegraded**.

  Contattare il supporto NetApp per assistenza.

Visualizzare l'attività delle performance dei nodi

È possibile visualizzare l'attività delle performance per ciascun nodo in un formato grafico. Queste informazioni forniscono statistiche in tempo reale per CPU e IOPS (Read/write i/o Operations per second) per ogni disco del nodo. Il grafico di utilizzo viene aggiornato ogni cinque secondi e il grafico delle statistiche del disco viene aggiornato ogni dieci secondi.

1. Fare clic su **Cluster** > **Nodes**.
2. Fare clic su **azioni** per il nodo che si desidera visualizzare.
3. Fare clic su **View Details** (Visualizza dettagli).

> ⓘ È possibile visualizzare punti specifici nel tempo sulla linea e sui grafici a barre posizionando il cursore sulla linea o sulla barra.

Visualizza le performance dei volumi

È possibile visualizzare informazioni dettagliate sulle performance per tutti i volumi nel cluster. È possibile ordinare le informazioni in base all'ID del volume o a una delle colonne delle prestazioni. È inoltre possibile utilizzare il filtro per le informazioni in base a

determinati criteri.

È possibile modificare la frequenza con cui il sistema aggiorna le informazioni sulle prestazioni nella pagina facendo clic sull'elenco **Refresh Every** (Aggiorna ogni) e scegliendo un valore diverso. L'intervallo di refresh predefinito è 10 secondi se il cluster ha meno di 1000 volumi; in caso contrario, l'intervallo predefinito è 60 secondi. Se si sceglie il valore mai, l'aggiornamento automatico della pagina viene disattivato.

È possibile riattivare l'aggiornamento automatico facendo clic su **attiva l'aggiornamento automatico**.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Actions (azioni) per un volume.
3. Fare clic su **View Details** (Visualizza dettagli).

   Nella parte inferiore della pagina viene visualizzato un vassoio contenente informazioni generali sul volume.

4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi ulteriori dettagli**.

   Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Trova ulteriori informazioni

Dettagli sulle performance dei volumi

Dettagli sulle performance dei volumi

È possibile visualizzare le statistiche delle performance dei volumi dalla pagina Volume Performance (prestazioni volume) della scheda Reporting (rapporti) nell'interfaccia utente di Element.

L'elenco seguente descrive i dettagli disponibili:

- **ID**

  L'ID generato dal sistema per il volume.

- **Nome**

  Il nome assegnato al volume al momento della creazione.

- **Account**

  Il nome dell'account assegnato al volume.

- **Gruppi di accesso**

  Il nome del gruppo o dei gruppi di accesso al volume a cui appartiene il volume.

- **Utilizzo del volume**

  Un valore percentuale che descrive quanto il client sta utilizzando il volume.

  Valori possibili:

- 0 = il client non sta utilizzando il volume
- 100 = il client sta utilizzando il valore massimo
- >100 = il client sta utilizzando il burst

- **IOPS totali**

  Il numero totale di IOPS (lettura e scrittura) attualmente eseguiti sul volume.

- **Lettura IOPS**

  Il numero totale di IOPS di lettura attualmente in esecuzione sul volume.

- **IOPS di scrittura**

  Il numero totale di IOPS di scrittura attualmente in esecuzione sul volume.

- **Throughput totale**

  La quantità totale di throughput (lettura e scrittura) attualmente eseguita sul volume.

- **Throughput in lettura**

  La quantità totale di throughput in lettura attualmente eseguita rispetto al volume.

- **Throughput in scrittura**

  La quantità totale di throughput di scrittura attualmente eseguita sul volume.

- **Latenza totale**

  Il tempo medio, in microsecondi, per completare le operazioni di lettura e scrittura su un volume.

- **Latenza di lettura**

  Il tempo medio, in microsecondi, per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.

- **Latenza di scrittura**

  Il tempo medio, in microsecondi, per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.

- **Profondità coda**

  Il numero di operazioni di lettura e scrittura in sospeso nel volume.

- **Dimensione media io**

  Dimensione media in byte di i/o recente nel volume negli ultimi 500 millisecondi.

Visualizzare le sessioni iSCSI

È possibile visualizzare le sessioni iSCSI connesse al cluster. È possibile filtrare le informazioni per includere solo le sessioni desiderate.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **iSCSI Sessions**.
2. Per visualizzare i campi relativi ai criteri di filtro, fare clic su **Filter** (filtro).

Trova ulteriori informazioni

Dettagli della sessione iSCSI

Dettagli della sessione iSCSI

È possibile visualizzare informazioni sulle sessioni iSCSI connesse al cluster.

Il seguente elenco descrive le informazioni che è possibile trovare sulle sessioni iSCSI:

- Nodo *

  Nodo che ospita la partizione dei metadati primaria per il volume.

- **Account**

  Il nome dell'account proprietario del volume. Se il valore è vuoto, viene visualizzato un trattino (-).

- **Volume**

  Il nome del volume identificato nel nodo.

- **ID volume**

  ID del volume associato all'IQN di destinazione.

- **ID iniziatore**

  ID generato dal sistema per l'iniziatore.

- **Alias iniziatore**

  Un nome opzionale per l'iniziatore che semplifica la ricerca dell'iniziatore in un elenco lungo.

- **IP Initator**

  L'indirizzo IP dell'endpoint che avvia la sessione.

- **Initiator IQN**

  L'IQN dell'endpoint che avvia la sessione.

- **IP di destinazione**

  L'indirizzo IP del nodo che ospita il volume.

- **IQN di destinazione**

  L'IQN del volume.

- **Creato il**

Data in cui è stata stabilita la sessione.

Visualizzare le sessioni Fibre Channel

È possibile visualizzare le sessioni Fibre Channel (FC) collegate al cluster. È possibile filtrare le informazioni per includere solo le connessioni che si desidera visualizzare nella finestra.

1. Nell'interfaccia utente di Element, selezionare **Reporting** > **FC Sessions**.
2. Per visualizzare i campi relativi ai criteri di filtro, fare clic su **Filter** (filtro).

Trova ulteriori informazioni

Dettagli della sessione Fibre Channel

Dettagli della sessione Fibre Channel

Sono disponibili informazioni sulle sessioni Fibre Channel (FC) attive collegate al cluster.

Il seguente elenco descrive le informazioni disponibili sulle sessioni FC connesse al cluster:

- **ID nodo**

  Il nodo che ospita la sessione per la connessione.

- **Nome nodo**

  Nome del nodo generato dal sistema.

- **ID iniziatore**

  ID generato dal sistema per l'iniziatore.

- **WWPN iniziatore**

  Il nome della porta internazionale di inizio.

- **Alias iniziatore**

  Un nome opzionale per l'iniziatore che semplifica la ricerca dell'iniziatore in un elenco lungo.

- **WWPN di destinazione**

  Il nome della porta globale di destinazione.

- **Volume Access Group**

  Nome del gruppo di accesso al volume a cui appartiene la sessione.

- **ID gruppo di accesso volume**

  ID generato dal sistema per il gruppo di accesso.

Risolvere i problemi relativi ai dischi

È possibile sostituire un disco a stato solido (SSD) guasto con un disco sostitutivo. Gli SSD per i nodi di storage SolidFire sono sostituibili a caldo. Se si sospetta un guasto a un SSD, contattare il supporto NetApp per verificare il guasto e seguire la procedura di risoluzione corretta. NetApp Support collabora inoltre con te per ottenere un disco sostitutivo in base al tuo contratto di servizio.

Come sostituire in questo caso significa che è possibile rimuovere un disco guasto da un nodo attivo e sostituirlo con un nuovo disco SSD di NetApp. Si sconsiglia di rimuovere i dischi non guasti su un cluster attivo.

È necessario mantenere le parti di ricambio on-site suggerite dal supporto NetApp per consentire la sostituzione immediata del disco in caso di guasto.

> A scopo di test, se si simula un guasto del disco estraendo un disco da un nodo, è necessario attendere 30 secondi prima di inserirlo nuovamente nello slot del disco.

Se un disco si guasta, Double Helix ridistribuisce i dati sul disco tra i nodi rimanenti nel cluster. I guasti di più dischi sullo stesso nodo non sono un problema, poiché il software Element protegge da due copie di dati che risiedono sullo stesso nodo. Un disco guasto provoca i seguenti eventi:

- I dati vengono migrati dal disco.
- La capacità complessiva del cluster è ridotta dalla capacità del disco.
- La protezione dei dati Double Helix garantisce la presenza di due copie valide dei dati.

> I sistemi storage SolidFire non supportano la rimozione di un disco se la quantità di storage necessaria per la migrazione dei dati risulta insufficiente.

Per ulteriori informazioni

- Rimuovere i dischi guasti dal cluster
- Risoluzione dei problemi di base dei dischi MDSS
- Rimuovere i dischi MDSS
- "Sostituzione delle unità per i nodi di storage SolidFire"
- "Sostituzione delle unità per i nodi storage della serie H600S"
- "Informazioni sull'hardware H410S e H610S"
- "Informazioni sull'hardware della serie SF"

Rimuovere i dischi guasti dal cluster

Il sistema SolidFire mette un disco in uno stato di errore se l'autodiagnosi del disco indica al nodo che si è verificato un errore o se la comunicazione con il disco si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco dei dischi guasti. È necessario rimuovere un disco guasto dall'elenco dei dischi guasti nel software NetApp Element.

I dischi nell'elenco **Alerts** vengono visualizzati come **blockServiceUnhealthy** quando un nodo è offline. Al

riavvio del nodo, se il nodo e i relativi dischi tornano online entro cinque minuti e mezzo, i dischi si aggiornano automaticamente e continuano come dischi attivi nel cluster.

1. Nell'interfaccia utente di Element, selezionare **Cluster** > **Drives**.
2. Fare clic su **Failed** (guasto) per visualizzare l'elenco dei dischi guasti.
3. Annotare il numero di slot del disco guasto.

   Queste informazioni sono necessarie per individuare il disco guasto nello chassis.

4. Rimuovere i dischi guasti utilizzando uno dei seguenti metodi:

Opzione	Fasi
Per rimuovere singoli dischi	a. Fare clic su **azioni** per l'unità che si desidera rimuovere. b. Fare clic su **Rimuovi**.
Per rimuovere più dischi	a. Selezionare tutte le unità che si desidera rimuovere e fare clic su **azioni in blocco**. b. Fare clic su **Rimuovi**.

Risoluzione dei problemi di base dei dischi MDSS

È possibile ripristinare i dischi di metadati (o slice) aggiungendoli di nuovo al cluster nel caso in cui uno o entrambi i dischi di metadati si guastino. È possibile eseguire l'operazione di ripristino nell'interfaccia utente di NetApp Element se la funzione MDSS è già attivata sul nodo.

Se uno o entrambi i dischi di metadati in un nodo presentano un guasto, il servizio slice viene arrestato e i dati di entrambi i dischi vengono sottoposti a backup su dischi diversi nel nodo.

I seguenti scenari delineano possibili scenari di guasto e forniscono consigli di base per correggere il problema:

Errore del disco slice del sistema

- In questo scenario, lo slot 2 viene verificato e riportato a uno stato disponibile.
- Il disco slice del sistema deve essere ripopolato prima che il servizio slice possa essere riportato online.
- Sostituire il disco slice di sistema, quando il disco slice di sistema diventa disponibile, aggiungere il disco e il disco slot 2 contemporaneamente.

> Non è possibile aggiungere l'unità nello slot 2 da sola come unità di metadati. È necessario aggiungere entrambe le unità al nodo contemporaneamente.

Lo slot 2 non funziona

- In questo scenario, il disco slice del sistema viene verificato e riportato a uno stato disponibile.
- Sostituire lo slot 2 con uno spare, quando lo slot 2 diventa disponibile, aggiungere contemporaneamente il disco slice di sistema e il disco slot 2.

Errore del disco slice di sistema e dello slot 2

- È necessario sostituire sia l'unità slice di sistema che lo slot 2 con un disco libero. Quando entrambi i dischi diventano disponibili, aggiungere contemporaneamente l'unità slice di sistema e l'unità slot 2.

Ordine delle operazioni

- Sostituire il disco hardware guasto con un disco libero (sostituire entrambi i dischi se sono guasti).
- Aggiungere nuovamente i dischi al cluster una volta ripopolati e che si trovano in uno stato disponibile.

Verificare le operazioni

- Verificare che i dischi nello slot 0 (o interno) e nello slot 2 siano identificati come dischi metadati nell'elenco Active Drives (dischi attivi).
- Verificare che il bilanciamento di tutte le sezioni sia stato completato (nel registro eventi non sono presenti ulteriori messaggi di spostamento delle sezioni per almeno 30 minuti).

Per ulteriori informazioni

Aggiungere dischi MDSS

Aggiungere dischi MDSS

È possibile aggiungere una seconda unità di metadati su un nodo SolidFire convertendo l'unità di blocco nello slot 2 in un'unità slice. Ciò si ottiene attivando la funzione multi-drive slice service (MDSS). Per attivare questa funzione, è necessario contattare il supporto NetApp.

Per portare un disco slice in uno stato disponibile potrebbe essere necessario sostituire un disco guasto con un disco nuovo o libero. È necessario aggiungere il disco slice di sistema contemporaneamente all'aggiunta del disco per lo slot 2. Se si tenta di aggiungere il disco slot 2 slice da solo o prima di aggiungere il disco slice di sistema, il sistema genera un errore.

1. Fare clic su **Cluster** > **Drives**.
2. Fare clic su **Available** (disponibile) per visualizzare l'elenco dei dischi disponibili.
3. Selezionare le unità slice da aggiungere.
4. Fare clic su **azioni in blocco**.
5. Fare clic su **Aggiungi**.
6. Verificare dalla scheda **Active Drives** che le unità siano state aggiunte.

Rimuovere i dischi MDSS

È possibile rimuovere i dischi multi-drive slice service (MDSS). Questa procedura si applica solo se il nodo ha più dischi slice.

> Se il disco slice del sistema e il disco slot 2 si guastano, il sistema arresta i servizi slice e rimuove i dischi. Se non si verifica alcun guasto e si rimuovono i dischi, entrambi devono essere rimossi contemporaneamente.

1. Fare clic su **Cluster** > **Drives**.

2. Dalla scheda **Available** drives (dischi disponibili), fare clic sulla casella di controllo relativa ai dischi slice da rimuovere.
3. Fare clic su **azioni in blocco**.
4. Fare clic su **Rimuovi**.
5. Confermare l'azione.

Risolvere i problemi dei nodi

È possibile rimuovere i nodi da un cluster per la manutenzione o la sostituzione. È necessario utilizzare l'interfaccia utente o l'API NetApp Element per rimuovere i nodi prima di portarli fuori linea.

Di seguito è riportata una panoramica della procedura per la rimozione dei nodi di storage:

- Assicurarsi che il cluster disponga di capacità sufficiente per creare una copia dei dati sul nodo.
- Rimuovere le unità dal cluster utilizzando l'interfaccia utente o il metodo API RemoveDrives.

  Ciò comporta la migrazione dei dati dal sistema ai dischi del nodo ad altri dischi nel cluster. Il tempo necessario per questo processo dipende dalla quantità di dati da migrare.

- Rimuovere il nodo dal cluster.

Tenere presenti le seguenti considerazioni prima di spegnere o accendere un nodo:

- Spegnere nodi e cluster comporta rischi se non viene eseguita correttamente.

  Lo spegnimento di un nodo deve essere eseguito sotto la direzione del supporto NetApp.

- Se un nodo è rimasto inattivo per più di 5.5 minuti in qualsiasi condizione di arresto, la protezione dei dati Double Helix inizia l'attività di scrittura di singoli blocchi replicati in un altro nodo per replicare i dati. In questo caso, contattare il supporto NetApp per assistenza nell'analisi del nodo guasto.
- Per riavviare o spegnere un nodo in modo sicuro, è possibile utilizzare il comando Shutdown API.
- Se un nodo si trova in uno stato inattivo o spento, è necessario contattare il supporto NetApp prima di riportarlo online.
- Dopo aver riportato un nodo online, è necessario aggiungerne di nuovo i dischi al cluster, a seconda del periodo di tempo in cui è rimasto fuori servizio.

Per ulteriori informazioni

"Sostituzione di uno chassis SolidFire guasto"

"Sostituzione di un nodo della serie H600S guasto"

Spegnere un cluster

Per spegnere un intero cluster, attenersi alla seguente procedura.

Fasi

1. (Facoltativo) contattare il supporto NetApp per assistenza nel completamento delle fasi preliminari.
2. Verificare che tutti i/o siano interrotti.

3. Disconnettere tutte le sessioni iSCSI:
   a. Accedere all'indirizzo IP virtuale di gestione (MVIP) sul cluster per aprire l'interfaccia utente Element.
   b. Annotare i nodi elencati nell'elenco nodi.
   c. Eseguire il metodo Shutdown API con l'opzione halt specificata su ciascun ID nodo del cluster.

> Quando si riavvia il cluster, è necessario seguire alcuni passaggi per verificare che tutti i nodi siano in linea:
>
> 1. Verificare che tutti i livelli critici di severità e. `volumesOffline` i guasti del cluster sono stati risolti.
> 2. Attendere da 10 a 15 minuti per consentire al cluster di stabilizzarsi.
> 3. Avviare la creazione degli host per accedere ai dati.
>
> Se si desidera dedicare più tempo all'accensione dei nodi e alla verifica dell'integrità dei nodi dopo la manutenzione, contattare il supporto tecnico per ricevere assistenza con il ritardo della sincronizzazione dei dati per evitare una sincronizzazione bin non necessaria.

Trova ulteriori informazioni

"Come spegnere e accendere correttamente un cluster di storage NetApp Solidfire/HCI"

Utilizzo di utility per nodo per nodi di storage

È possibile utilizzare le utility per nodo per risolvere i problemi di rete se gli strumenti di monitoraggio standard nell'interfaccia utente del software NetApp Element non forniscono informazioni sufficienti per la risoluzione dei problemi. Le utility per nodo forniscono informazioni e strumenti specifici che consentono di risolvere i problemi di rete tra nodi o con il nodo di gestione.

Trova ulteriori informazioni

- Accedere alle impostazioni per nodo utilizzando l'interfaccia utente per nodo
- Dettagli delle impostazioni di rete dall'interfaccia utente per nodo
- Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo
- Eseguire test di sistema utilizzando l'interfaccia utente per nodo
- Eseguire le utility di sistema utilizzando l'interfaccia utente per nodo

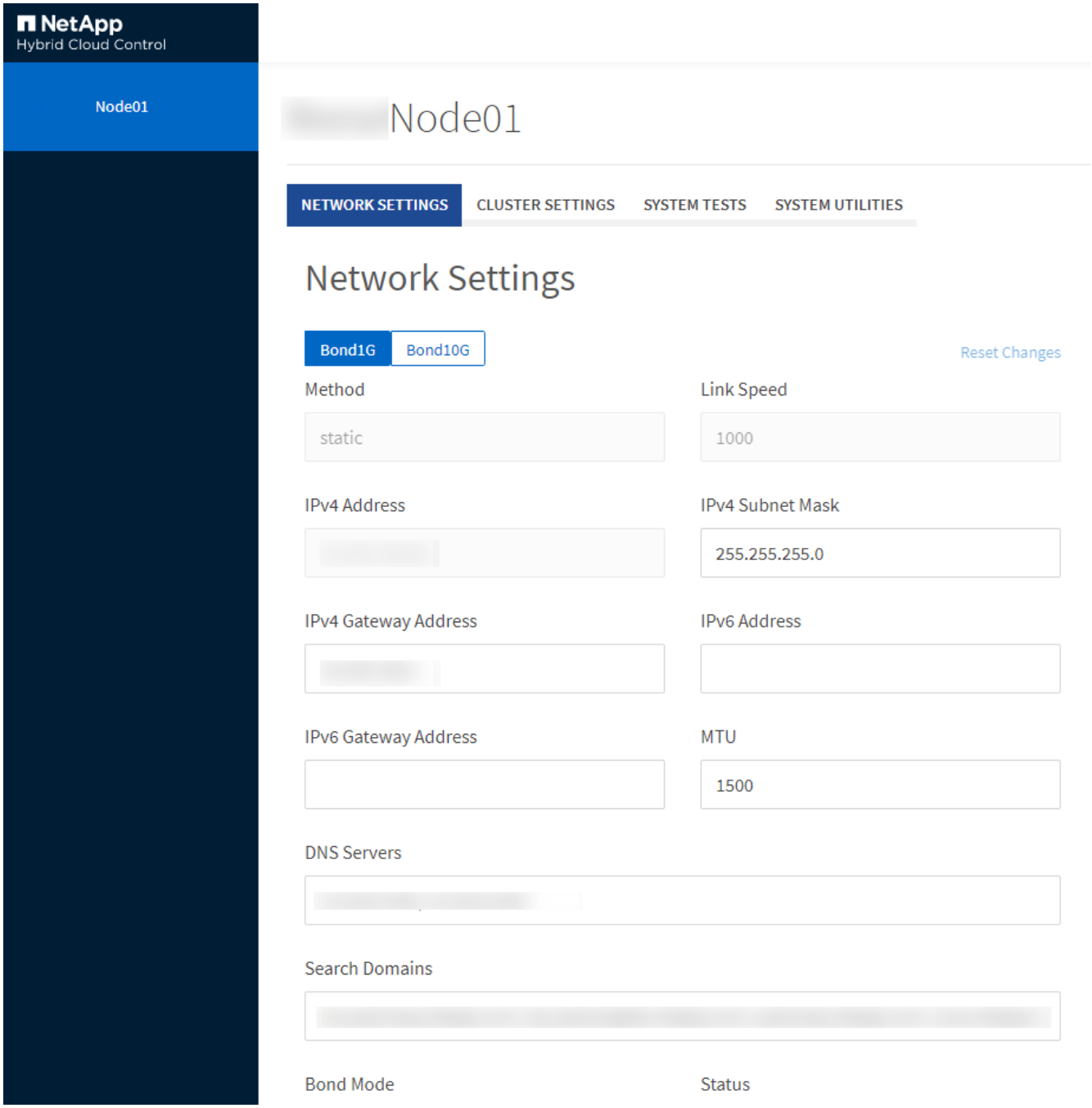
Accedere alle impostazioni per nodo utilizzando l'interfaccia utente per nodo

È possibile accedere alle impostazioni di rete, alle impostazioni del cluster, ai test e alle utility di sistema nell'interfaccia utente per nodo dopo aver inserito l'IP del nodo di gestione e autenticato.

Se si desidera modificare le impostazioni di un nodo in uno stato attivo che fa parte di un cluster, è necessario accedere come utente amministratore del cluster.

Configurare o modificare un nodo alla volta. Prima di apportare modifiche a un altro nodo, assicurarsi che le impostazioni di rete specificate abbiano l'effetto previsto e che la rete sia stabile e in grado di garantire prestazioni ottimali.

1. Aprire l'interfaccia utente per nodo utilizzando uno dei seguenti metodi:
   - Inserire l'indirizzo IP di gestione seguito da :442 in una finestra del browser e accedere utilizzando un nome utente e una password admin.
   - Nell'interfaccia utente di Element, selezionare **Cluster** > **Nodes**, quindi fare clic sul collegamento dell'indirizzo IP di gestione per il nodo che si desidera configurare o modificare. Nella finestra del browser visualizzata, è possibile modificare le impostazioni del nodo.



Dettagli delle impostazioni di rete dall'interfaccia utente per nodo

È possibile modificare le impostazioni di rete del nodo di storage per assegnare al nodo un nuovo set di attributi di rete.

Le impostazioni di rete per un nodo di storage sono visualizzate nella pagina **Impostazioni di rete** quando si effettua l'accesso al nodo (https://<node IP>:442/hcc/Node/network-settings). È possibile selezionare le impostazioni **Bond1G** (gestione) o **Bond10G** (storage). L'elenco seguente descrive le impostazioni che è possibile modificare quando un nodo di storage si trova nello stato Available (disponibile), Pending (in sospeso) o Active (attivo):

- **Metodo**

  Il metodo utilizzato per configurare l'interfaccia. Metodi possibili:

  - Loopback: Consente di definire l'interfaccia di loopback IPv4.
  - Manual (Manuale): Consente di definire le interfacce per le quali non viene eseguita alcuna configurazione per impostazione predefinita.
  - dhcp: Utilizzato per ottenere un indirizzo IP tramite DHCP.
  - Static (statico): Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.

- **Velocità di collegamento**

  La velocità negoziata dalla NIC virtuale.

- **Indirizzo IPv4**

  L'indirizzo IPv4 per la rete eth0.

- **IPv4 Subnet Mask**

  Suddivisioni di indirizzi della rete IPv4.

- **Indirizzo gateway IPv4**

  Router network address (Indirizzo di rete del router) per l'invio dei pacchetti dalla rete locale.

- **Indirizzo IPv6**

  L'indirizzo IPv6 per la rete eth0.

- **IPv6 Gateway Address**

  Router network address (Indirizzo di rete del router) per l'invio dei pacchetti dalla rete locale.

- **MTU**

  Dimensione massima dei pacchetti che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete per lo storage, il valore deve essere 9000.

- **Server DNS**

  Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Cerca domini**

  Cercare ulteriori indirizzi MAC disponibili per il sistema.

- **Modalità Bond**

  Può essere una delle seguenti modalità:

  - ActivePassive (predefinito)
  - ALB
  - LACP

- **Stato**

  Valori possibili:

  - UpandRunning
  - Giù
  - Su

- **Virtual Network Tag**

  Tag assegnato al momento della creazione della rete virtuale.

- **Percorsi**

  Route statiche verso host o reti specifici attraverso l'interfaccia associata che i route sono configurati per l'utilizzo.

Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo

È possibile verificare le impostazioni del cluster per un nodo di storage dopo la configurazione del cluster e modificare il nome host del nodo.

Il seguente elenco descrive le impostazioni del cluster per un nodo di storage indicate nella pagina **Cluster Settings** dell'interfaccia utente per nodo (https://<node IP>:442/hcc/Node/cluster-settings).

- **Ruolo**

  Ruolo del nodo nel cluster. Valori possibili:

  - Storage: Nodo storage o Fibre Channel.
  - Gestione: Il nodo è un nodo di gestione.

- **Nome host**

  Nome del nodo.

- **Cluster**

  Nome del cluster.

- **Appartenenza al cluster**

Stato del nodo. Valori possibili:

- Disponibile: Il nodo non ha un nome di cluster associato e non fa ancora parte di un cluster.
- In sospeso: Il nodo è configurato e può essere aggiunto a un cluster designato. Per accedere al nodo non è richiesta l'autenticazione.
- PendingActive: Il sistema sta installando software compatibile sul nodo. Al termine, il nodo passa allo stato attivo.
- Attivo: Il nodo partecipa a un cluster. L'autenticazione è necessaria per modificare il nodo.

- **Versione**

  Versione del software Element in esecuzione sul nodo.

- **Ensemble**

  Nodi che fanno parte dell'insieme di database.

- **ID nodo**

  ID assegnato quando un nodo viene aggiunto al cluster.

- **Interfaccia cluster**

  Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Interfaccia di gestione**

  Interfaccia di rete di gestione. Questo valore predefinito è Bond1G, ma può anche utilizzare Bond10G.

- **Interfaccia storage**

  Interfaccia di rete dello storage con Bond10G.

- **Crittografia abilitata**

  Indica se il nodo supporta o meno la crittografia del disco.

Eseguire test di sistema utilizzando l'interfaccia utente per nodo

È possibile verificare le modifiche alle impostazioni di rete dopo averle salvate nella configurazione di rete. È possibile eseguire i test per assicurarsi che il nodo di storage sia stabile e possa essere portato online senza problemi.

Si è effettuato l'accesso all'interfaccia utente per nodo per il nodo di storage.

1. Fare clic su **Test di sistema**.
2. Fare clic su **Esegui test** accanto al test che si desidera eseguire oppure selezionare **Esegui tutti test**.

   L'esecuzione di tutte le operazioni di test può richiedere molto tempo e deve essere eseguita solo sotto la direzione del supporto NetApp.

   - **Test Connected Ensemble**

Verifica e verifica la connettività a un insieme di database. Per impostazione predefinita, il test utilizza l'insieme per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un gruppo diverso per testare la connettività.

- **Test Connect MVIP**

  Esegue il ping dell'indirizzo IP virtuale di gestione (MVIP) specificato ed esegue una semplice chiamata API a MVIP per verificare la connettività. Per impostazione predefinita, il test utilizza l'MVIP per il cluster a cui è associato il nodo.

- **Test Connect Svip**

  Ping dell'indirizzo IP virtuale dello storage (SVIP) specificato utilizzando pacchetti ICMP (Internet Control message Protocol) che corrispondono alle dimensioni massime dell'unità di trasmissione (MTU) impostate sulla scheda di rete. Quindi si connette a SVIP come iniziatore iSCSI. Per impostazione predefinita, il test utilizza l'SVIP per il cluster a cui è associato il nodo.

- **Test hardware Config**

  Verifica che tutte le configurazioni hardware siano corrette, verifica la correttezza delle versioni del firmware e verifica che tutti i dischi siano installati e funzionino correttamente. Si tratta della stessa procedura utilizzata per i test di fabbrica.

  Questo test richiede un elevato numero di risorse e deve essere eseguito solo se richiesto dal supporto NetApp.

- **Verifica della connettività locale**

  Verifica la connettività a tutti gli altri nodi del cluster eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test viene visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

- **Eseguire il test per individuare il cluster**

  Convalida che il nodo sia in grado di individuare il cluster specificato nella configurazione del cluster.

- **Test Network Config**

  Verifica che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate nel sistema. Questo test non è destinato a rilevare guasti hardware quando un nodo partecipa attivamente a un cluster.

- **Test Ping**

  Ping un elenco specifico di host o, se non ne viene specificato alcuno, crea dinamicamente un elenco di tutti i nodi registrati nel cluster e esegue il ping ciascuno per una semplice connettività.

- **Verifica della connettività remota**

  Verifica la connettività a tutti i nodi dei cluster associati in remoto eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test viene visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

Eseguire le utility di sistema utilizzando l'interfaccia utente per nodo

È possibile utilizzare l'interfaccia utente per nodo per il nodo di storage per creare o eliminare pacchetti di supporto, reimpostare le impostazioni di configurazione per i dischi e riavviare i servizi di rete o cluster.

Si è effettuato l'accesso all'interfaccia utente per nodo per il nodo di storage.

1. Fare clic su **Utilità di sistema**.
2. Fare clic sul pulsante dell'utilità di sistema che si desidera eseguire.
   - **Alimentazione di controllo**

     Riavvia, spegne e riaccende il nodo.

     Questa operazione causa la perdita temporanea della connettività di rete.

     Specificare i seguenti parametri:

     - Azione: Le opzioni includono Restart (Riavvia) e Halt (arresta) (Spegni).
     - Wakeup Delay (ritardo di attivazione): Qualsiasi tempo aggiuntivo prima che il nodo ripresenti online.
   - **Collect Node Logs**

     Crea un bundle di supporto nella directory /tmp/bundle del nodo.

     Specificare i seguenti parametri:

     - Bundle Name (Nome bundle): Nome univoco per ciascun bundle di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
     - Args extra: Questo parametro viene inviato allo script sf_make_support_bundle. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp.
     - Timeout sec (sec timeout): Specificare il numero di secondi di attesa per ogni singola risposta ping.
   - **Elimina registri nodi**

     Elimina tutti i bundle di supporto correnti sul nodo creati utilizzando **Create Cluster Support Bundle** o il metodo API CreateSupportBundle.
   - **Ripristina unità**

     Inizializza i dischi e rimuove tutti i dati attualmente presenti sul disco. È possibile riutilizzare l'unità in un nodo esistente o in un nodo aggiornato.

     Specificare il seguente parametro:

     - Unità: Elenco dei nomi dei dispositivi (non degli ID unità) da ripristinare.
   - **Reset Network Config** (Ripristina configurazione di rete)

     Aiuta a risolvere i problemi di configurazione di rete per un singolo nodo e ripristina la configurazione di rete di un singolo nodo alle impostazioni predefinite di fabbrica.

- **Ripristina nodo**

  Consente di ripristinare le impostazioni predefinite di un nodo. Tutti i dati vengono rimossi, ma le impostazioni di rete del nodo vengono conservate durante questa operazione. I nodi possono essere ripristinati solo se non assegnati a un cluster e in stato disponibile.

  > Quando si utilizza questa opzione, tutti i dati, i pacchetti (aggiornamenti software), le configurazioni e i file di log vengono cancellati dal nodo.

- **Riavvia rete**

  Riavvia tutti i servizi di rete su un nodo.

  > Questa operazione può causare la perdita temporanea della connettività di rete.

- **Riavviare i servizi**

  Riavvia i servizi software Element su un nodo.

  > Questa operazione può causare un'interruzione temporanea del servizio del nodo. Questa operazione deve essere eseguita solo sotto la direzione del supporto NetApp.

  Specificare i seguenti parametri:

  - Servizio: Nome del servizio da riavviare.
  - Azione: Azione da eseguire sul servizio. Le opzioni includono avvio, arresto e riavvio.

Lavorare con il nodo di gestione

È possibile utilizzare il nodo di gestione (mNode) per aggiornare i servizi di sistema, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema, configurare Active IQ per il monitoraggio del sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

> Come Best practice, associare un solo nodo di gestione a un'istanza di VMware vCenter ed evitare di definire le stesse risorse di storage e calcolo o istanze di vCenter in più nodi di gestione.

Vedere "documentazione del nodo di gestione" per ulteriori informazioni.

Comprendere i livelli di completezza del cluster

Il software cluster running Element genera errori del cluster per avvisare l'amministratore dello storage quando il cluster sta esaurendo la capacità. Sono disponibili tre livelli di riempimento del cluster, tutti visualizzati nell'interfaccia utente di NetApp Element: Avviso, errore e critico.

Il sistema utilizza il codice di errore BlockClusterFull per avvisare della completezza dello storage a blocchi del cluster. È possibile visualizzare i livelli di severità di pienezza del cluster dalla scheda Avvisi dell'interfaccia utente di Element.

Il seguente elenco include informazioni sui livelli di severità di BlockClusterFull:

- **Attenzione**

  Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità dei blocchi del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al 3% sotto il livello di errore e può essere regolato tramite l'interfaccia utente e l'API Element. È necessario aggiungere più capacità o liberare capacità il prima possibile.

- **Errore**

  Quando il cluster si trova in questo stato, in caso di perdita di un nodo, la capacità del cluster non sarà sufficiente per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot vengono bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per qualsiasi cluster. È necessario aggiungere ulteriore capacità o liberare immediatamente capacità.

- **Critico**

  Questo errore critico si è verificato perché il cluster è consumato al 100%. Si trova in uno stato di sola lettura e non è possibile effettuare nuove connessioni iSCSI al cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente ulteriore capacità.

Il sistema utilizza il codice di errore MetadataClusterFull per avvisare sulla completezza dello storage dei metadati del cluster. È possibile visualizzare la completezza dello storage dei metadati del cluster dalla sezione Cluster Capacity (capacità cluster) nella pagina Overview (Panoramica) della scheda Reporting (rapporti) nell'interfaccia utente di Element.

Il seguente elenco include informazioni sui livelli di severità MetadataClusterFull:

- **Attenzione**

  Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità dei metatdati del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al 3% sotto il livello di errore e può essere regolato tramite l'API Element. È necessario aggiungere più capacità o liberare capacità il prima possibile.

- **Errore**

  Quando il cluster si trova in questo stato, in caso di perdita di un nodo, la capacità del cluster non sarà sufficiente per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot vengono bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per qualsiasi cluster. È necessario aggiungere ulteriore capacità o liberare immediatamente capacità.

- **Critico**

  Questo errore critico si è verificato perché il cluster è consumato al 100%. Si trova in uno stato di sola lettura e non è possibile effettuare nuove connessioni iSCSI al cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente ulteriore capacità.

Quanto segue si applica alle soglie del cluster a due nodi:

- L'errore di fullness dei metadati è inferiore del 20% al livello critico.

- L’errore di fullness del blocco è un disco a 1 blocco (inclusa la capacità inutilizzata) inferiore al livello critico, il che significa che due dischi a blocchi hanno una capacità inferiore al livello critico.

Gestione e monitoraggio dello storage con NetApp Hybrid Cloud Control

Con lo storage all-flash NetApp SolidFire, puoi gestire e monitorare le risorse di storage e configurare i componenti del tuo sistema di storage utilizzando il controllo del cloud ibrido NetApp.

- "Aggiungere e gestire cluster di storage"
- "Configurare l'accesso completo all'interfaccia utente Web Domain Name"
- "Creare e gestire gli account utente"
- "Creare e gestire i volumi"
- "Creare e gestire i gruppi di accesso ai volumi"
- "Creare e gestire gli iniziatori"
- "Creare e gestire policy di QoS per volumi"
- "Monitorate il vostro sistema SolidFire con il controllo del cloud ibrido NetApp"

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Aggiungi e gestisci cluster di storage utilizzando NetApp Hybrid Cloud Control

È possibile aggiungere cluster di storage all'inventario delle risorse dei nodi di gestione in modo che possano essere gestiti utilizzando NetApp Hybrid Cloud Control (HCC). Il primo cluster di storage aggiunto durante l'installazione del sistema è quello predefinito "cluster di storage autorevole", Ma è possibile aggiungere cluster aggiuntivi utilizzando l'interfaccia utente HCC.

Dopo l'aggiunta di un cluster di storage, è possibile monitorare le prestazioni del cluster, modificare le credenziali del cluster di storage per la risorsa gestita o rimuovere un cluster di storage dall'inventario delle risorse del nodo di gestione se non è più necessario gestirlo con HCC.

Di cosa hai bisogno

- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore su "cluster di storage autorevole". Il cluster autorevole è il primo cluster aggiunto all'inventario dei nodi di gestione durante l'installazione del sistema.
- **Software Element**: La versione del cluster di storage in uso esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 11.3 o successiva.
- **Servizi di gestione**: Il bundle di servizi di gestione è stato aggiornato alla versione 2.17 o successiva.

Opzioni

- Aggiungere un cluster di storage
- Confermare lo stato del cluster di storage
- Modificare le credenziali del cluster di storage
- Rimuovere un cluster di storage
- Attiva e disattiva la modalità di manutenzione

Aggiungere un cluster di storage

È possibile aggiungere un cluster di storage all'inventario delle risorse del nodo di gestione utilizzando NetApp Hybrid Cloud Control. Ciò consente di gestire e monitorare il cluster utilizzando l'interfaccia utente HCC.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare **Add Storage Cluster** (Aggiungi cluster di storage).
5. Inserire le seguenti informazioni:
   - Indirizzo IP virtuale per la gestione del cluster di storage

     È possibile aggiungere solo cluster di storage remoto che non sono attualmente gestiti da un nodo di gestione.

   - Nome utente e password del cluster di storage
6. Selezionare **Aggiungi**.

Dopo aver aggiunto il cluster di storage, l'inventario del cluster può impiegare fino a 2 minuti per l'aggiornamento e la visualizzazione della nuova aggiunta. Potrebbe essere necessario aggiornare la pagina del browser per visualizzare le modifiche.

Confermare lo stato del cluster di storage

È possibile monitorare lo stato di connessione delle risorse dei cluster di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Esaminare lo stato dei cluster di storage nell'inventario.
4. Dal riquadro **Storage Clusters**, selezionare **Storage Cluster Details** per ulteriori dettagli.

Modificare le credenziali del cluster di storage

È possibile modificare il nome utente e la password dell'amministratore del cluster di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare il menu **azioni** del cluster e selezionare **Modifica credenziali cluster**.
5. Aggiornare il nome utente e la password del cluster di storage.
6. Selezionare **Salva**.

Rimuovere un cluster di storage

La rimozione di un cluster di storage da NetApp Hybrid Cloud Control rimuove il cluster dall'inventario dei nodi di gestione. Dopo aver rimosso un cluster di storage, il cluster non può più essere gestito da HCC e l'accesso è possibile solo accedendo direttamente al relativo indirizzo IP di gestione.

> Non è possibile rimuovere il cluster autorevole dall'inventario. Per determinare il cluster autorevole, accedere a **User Management > Users** (Gestione utenti > utenti). Il cluster autorevole è elencato accanto all'intestazione **Users**.

Fasi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
2. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
3. Nel riquadro **Storage Clusters**, selezionare **Storage Cluster Details** (Dettagli cluster di storage).
4. Selezionare il menu **azioni** del cluster e selezionare **Rimuovi cluster di storage**.

> Selezionando **Yes** NEXT (Sì), il cluster viene rimosso dall'installazione.

5. Selezionare **Sì**.

Attiva e disattiva la modalità di manutenzione

Se è necessario disattivare un nodo di storage per la manutenzione, ad esempio aggiornamenti software o riparazioni host, è possibile ridurre al minimo l'impatto i/o sul resto del cluster di storage abilitazione in corso modalità di manutenzione per quel nodo. Quando vuoi disattiva modalità di manutenzione, il nodo viene monitorato per garantire che vengano soddisfatti determinati criteri prima che il nodo possa uscire dalla modalità di manutenzione.

Di cosa hai bisogno

- **Software Element**: La versione del cluster di storage in uso esegue il software NetApp Element 12.2 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 12.2 o successiva.
- **Servizi di gestione**: Il bundle di servizi di gestione è stato aggiornato alla versione 2.19 o successiva.
- Hai accesso per accedere al livello di amministratore.

attiva la modalità di manutenzione

È possibile utilizzare la procedura seguente per attivare la modalità di manutenzione per un nodo del cluster di storage.

Solo un nodo può essere in modalità di manutenzione alla volta.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

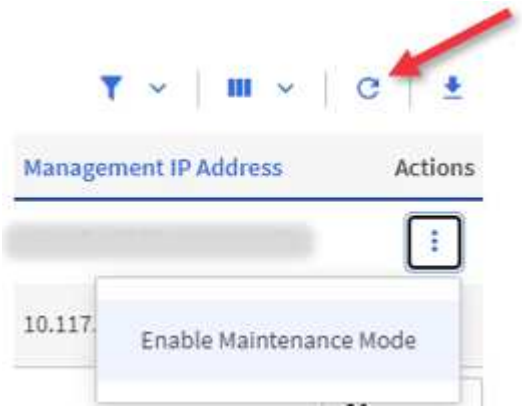
```
https://[management node IP address]
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire.

   Le opzioni della funzione della modalità di manutenzione sono disattivate a livello di sola lettura.

3. Nella casella blu di navigazione a sinistra, selezionare l'installazione SolidFire all-flash.
4. Nel riquadro di navigazione a sinistra, selezionare **Nodes** (nodi).
5. Per visualizzare le informazioni sull'inventario dello storage, selezionare **Storage**.
6. Abilitare la modalità di manutenzione su un nodo di storage:

   La tabella dei nodi di storage viene aggiornata automaticamente ogni due minuti per le azioni non avviate dall'utente. Prima di eseguire un'azione, per assicurarsi di disporre dello stato più aggiornato, è possibile aggiornare la tabella Nodes utilizzando l'icona di refresh situata nella parte superiore destra della tabella Nodes.



   a. In **azioni**, selezionare **Enable Maintenance Mode** (attiva modalità di manutenzione).

      Mentre è attivata la modalità **Maintenance Mode**, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi dello stesso cluster.

   Una volta completata l'attivazione della modalità di manutenzione*, nella colonna **Node Status** (Stato nodo) viene visualizzata l'icona di una chiave a forma di chiave e il testo "**Maintenance Mode**" (modalità di manutenzione) per il nodo in modalità di manutenzione.

Disattiva la modalità di manutenzione

Dopo che un nodo è stato impostato correttamente in modalità di manutenzione, l'azione **Disable Maintenance Mode** (Disattiva modalità di manutenzione) è disponibile per questo nodo. Le azioni sugli altri

nodi non sono disponibili fino a quando la modalità di manutenzione non viene disattivata correttamente sul nodo sottoposto a manutenzione.

Fasi

1. Per il nodo in modalità di manutenzione, in **azioni**, selezionare **Disattiva modalità di manutenzione**.

   Mentre **Maintenance Mode** è disattivato, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi dello stesso cluster.

   Una volta completata la funzione **Disabling Maintenance Mode** (disattivazione modalità di manutenzione), la colonna **Node Status** (Stato nodo) visualizza **Active** (attivo).

   > Quando un nodo è in modalità di manutenzione, non accetta nuovi dati. Di conseguenza, la disattivazione della modalità di manutenzione può richiedere più tempo, poiché il nodo deve sincronizzare il backup dei dati prima di uscire dalla modalità di manutenzione. Maggiore è il tempo impiegato in modalità di manutenzione, maggiore sarà il tempo necessario per disattivare la modalità di manutenzione.

Risolvere i problemi

Se si verificano errori durante l'attivazione o la disattivazione della modalità di manutenzione, viene visualizzato un errore di intestazione nella parte superiore della tabella Nodes (nodi). Per ulteriori informazioni sull'errore, selezionare il collegamento **Mostra dettagli** fornito sul banner per visualizzare i risultati dell'API.

Trova ulteriori informazioni

- "Creare e gestire le risorse del cluster di storage"
- "Documentazione software SolidFire ed Element"

Creare e gestire gli account utente utilizzando NetApp Hybrid Cloud Control

Nei sistemi storage basati su elementi, è possibile creare utenti di cluster autorevoli per consentire l'accesso a NetApp Hybrid Cloud Control in base alle autorizzazioni che si desidera concedere agli utenti "Administrator" o "Read-only". Oltre agli utenti del cluster, esistono anche account di volume che consentono ai client di connettersi ai volumi su un nodo di storage.

Gestire i seguenti tipi di account:

- Gestire gli account cluster autorevoli
- Gestire gli account dei volumi

Attivare LDAP

Per utilizzare LDAP per qualsiasi account utente, è necessario prima attivare LDAP.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.

2. Dalla dashboard, selezionare l'icona Opzioni in alto a destra e selezionare **Gestione utenti**.
3. Dalla pagina utenti, selezionare **Configura LDAP**.
4. Definire la configurazione LDAP.
5. Selezionare il tipo di autenticazione Search and Bind (Cerca e bind) o Direct Bind (Bind diretto).
6. Prima di salvare le modifiche, selezionare **Test LDAP Log in** (verifica accesso LDAP) nella parte superiore della pagina, inserire il nome utente e la password di un utente noto esistente e selezionare **Test**.
7. Selezionare **Salva**.

Gestire gli account cluster autorevoli

"Account utente autorevoli" Sono gestiti dal menu in alto a destra dell'opzione User Management in NetApp Hybrid Cloud Control. Questi tipi di account consentono di eseguire l'autenticazione con qualsiasi risorsa di storage associata a un'istanza di nodi e cluster di NetApp Hybrid Cloud Control. Con questo account, puoi gestire volumi, account, gruppi di accesso e molto altro in tutti i cluster.

Creare un account cluster autorevole

Puoi creare un account utilizzando NetApp Hybrid Cloud Control.

Questo account può essere utilizzato per accedere al controllo del cloud ibrido, all'interfaccia utente per nodo per il cluster e al cluster di storage nel software NetApp Element.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare l'icona Opzioni in alto a destra e selezionare **Gestione utenti**.
3. Selezionare **Create User** (Crea utente).
4. Selezionare il tipo di autenticazione del cluster o LDAP.
5. Completare una delle seguenti operazioni:
   - Se si seleziona LDAP, inserire il DN.

     Per utilizzare LDAP, è necessario prima attivare LDAP o LDAPS. Vedere Attivare LDAP.

   - Se si seleziona Cluster come tipo di autorizzazione, immettere un nome e una password per il nuovo account.
6. Selezionare le autorizzazioni di amministratore o di sola lettura.

   Per visualizzare le autorizzazioni dal software NetApp Element, selezionare **Mostra permessi legacy**. Se si seleziona un sottoinsieme di queste autorizzazioni, all'account vengono assegnate autorizzazioni di sola lettura. Se si selezionano tutte le autorizzazioni legacy, all'account vengono assegnate le autorizzazioni di amministratore.

   Per garantire che tutti i figli di un gruppo ereditino le autorizzazioni, creare un gruppo di amministratori dell'organizzazione DN nel server LDAP. Tutti gli account figlio di quel gruppo erediteranno tali autorizzazioni.
7. Selezionare la casella "ho letto e accettato il Contratto di licenza con l'utente finale di NetApp".

8. Selezionare **Create User** (Crea utente).

Modificare un account cluster autorevole

È possibile modificare le autorizzazioni o la password di un account utente utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare sull'icona in alto a destra e selezionare **Gestione utenti**.
3. È possibile filtrare l'elenco degli account utente selezionando **Cluster**, **LDAP** o **IDP**.

   Se sono stati configurati utenti sul cluster di storage con LDAP, questi account visualizzano il tipo utente "LDAP". Se sono stati configurati utenti sul cluster di storage con IDP, questi account mostrano un tipo di utente "IDP".

4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Modifica**.
5. Apportare le modifiche necessarie.
6. Selezionare **Salva**.
7. Disconnettersi da NetApp Hybrid Cloud Control.

> L'aggiornamento dell'inventario potrebbe richiedere fino a 2 minuti dall'interfaccia utente di NetApp Hybrid Cloud Control. Per aggiornare manualmente l'inventario, accedere al servizio di inventario dell'interfaccia utente REST API `https://[management node IP]/inventory/1/` ed eseguire `GET /installations/{id}` per il cluster.

8. Accedi a NetApp Hybrid Cloud Control.

Eliminare un account utente autorevole

È possibile eliminare uno o più account quando non sono più necessari. È possibile eliminare un account utente LDAP.

Non è possibile eliminare l'account utente amministratore principale per il cluster autorevole.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare sull'icona in alto a destra e selezionare **Gestione utenti**.
3. Nella colonna **azioni** della tabella utenti, espandere il menu dell'account e selezionare **Elimina**.
4. Confermare l'eliminazione selezionando **Sì**.

Gestire gli account dei volumi

"Account di volume" Sono gestiti all'interno della tabella NetApp Hybrid Cloud Control Volumes. Questi account sono specifici solo per il cluster di storage in cui sono stati creati. Questi tipi di account consentono di impostare le autorizzazioni sui volumi in rete, ma non hanno alcun effetto al di fuori di tali volumi.

Un account volume contiene l'autenticazione CHAP richiesta per accedere ai volumi assegnati.

Creare un account volume

Creare un account specifico per questo volume.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Selezionare il pulsante **Crea account**.
5. Immettere un nome per il nuovo account.
6. Nella sezione CHAP Settings (Impostazioni CHAP), immettere le seguenti informazioni:
   - Initiator Secret per l'autenticazione della sessione del nodo CHAP
   - Segreto di destinazione per l'autenticazione della sessione del nodo CHAP

   Per generare automaticamente una password, lasciare vuoti i campi delle credenziali.
7. Selezionare **Crea account**.

Modificare un account volume

È possibile modificare le informazioni CHAP e modificare se un account è attivo o bloccato.

L'eliminazione o il blocco di un account associato al nodo di gestione comporta un nodo di gestione inaccessibile.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Modifica**.
5. Apportare le modifiche necessarie.
6. Confermare le modifiche selezionando **Sì**.

Eliminare un account volume

Eliminare un account non più necessario.

Prima di eliminare un account di volume, eliminare e rimuovere i volumi associati all'account.

L'eliminazione o il blocco di un account associato al nodo di gestione comporta un nodo di gestione inaccessibile.

I volumi persistenti associati ai servizi di gestione vengono assegnati a un nuovo account durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare i volumi o l'account associato. Se si eliminano questi account, si potrebbe rendere inutilizzabile il nodo di gestione.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, selezionare **Storage** > **Volumes**.
3. Selezionare la scheda **account**.
4. Nella colonna **azioni** della tabella, espandere il menu dell'account e selezionare **Elimina**.
5. Confermare l'eliminazione selezionando **Sì**.

Trova ulteriori informazioni

- "Scopri di più sugli account"
- "Utilizzare gli account con CHAP"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Crea e gestisci i volumi utilizzando NetApp Hybrid Cloud Control

È possibile creare un volume e associarlo a un determinato account. L'associazione di un volume a un account consente all'account di accedere al volume tramite gli iniziatori iSCSI e le credenziali CHAP.

È possibile specificare le impostazioni QoS per un volume durante la creazione.

Puoi gestire i volumi in NetApp Hybrid Cloud Control nei seguenti modi:

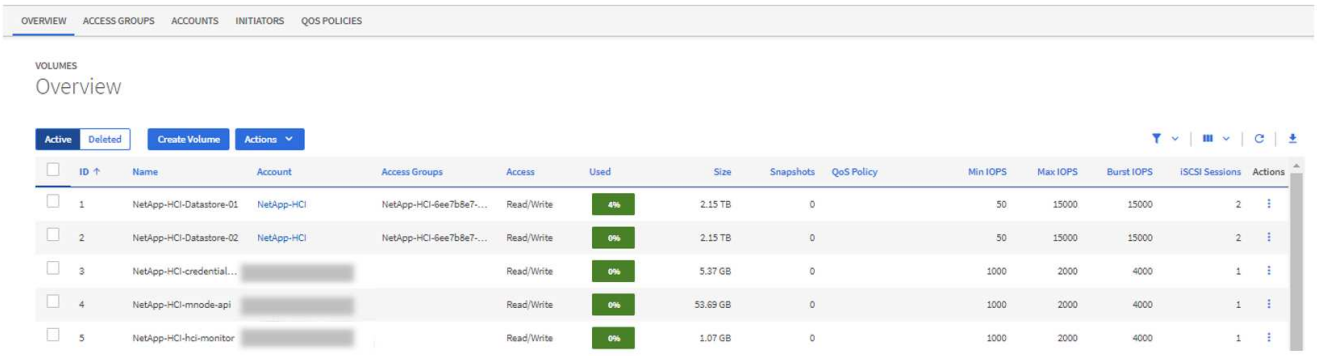
- Creare un volume
- Applicare un criterio QoS a un volume
- Modificare un volume
- Clonare i volumi
- Aggiungere volumi a un gruppo di accesso al volume
- Eliminare un volume
- Ripristinare un volume cancellato
- Eliminare un volume cancellato

Creare un volume

È possibile creare un volume di storage utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare la scheda **volumi** > **Panoramica**.



4. Selezionare **Create Volume** (Crea volume).
5. Immettere un nome per il nuovo volume.
6. Inserire le dimensioni totali del volume.

> La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB: 1 GB = 1 000 000 000 byte 1 GiB = 1 073 741 824 byte

7. Selezionare una dimensione di blocco per il volume.
8. Dall'elenco **account**, selezionare l'account che deve avere accesso al volume.

   Se non esiste un account, selezionare **Crea nuovo account**, immettere un nuovo nome account e selezionare **Crea account**. L'account viene creato e associato al nuovo volume nell'elenco **account**.

> Se sono presenti più di 50 account, l'elenco non viene visualizzato. Iniziare a digitare e la funzione di completamento automatico visualizza i valori da scegliere.

9. Per configurare la qualità del servizio per il volume, effettuare una delle seguenti operazioni:
   - In **Quality of Service Settings** (Impostazioni qualità del servizio), impostare i valori minimi, massimi e burst personalizzati per IOPS o utilizzare i valori QoS predefiniti.
   - Selezionare una policy QoS esistente attivando il comando **Assign Quality of Service Policy** (Assegna policy di qualità del servizio) e scegliendo una policy QoS esistente dall'elenco risultante.
   - Creare e assegnare una nuova policy QoS attivando il comando **Assign Quality of Service Policy** (Assegna policy di qualità del servizio) e selezionando **Create New QoS Policy** (Crea nuova policy QoS). Nella finestra visualizzata, immettere un nome per il criterio QoS, quindi immettere i valori QoS. Al termine, selezionare **Crea policy sulla qualità del servizio**.

   I volumi con un valore massimo o burst IOPS superiore a 20,000 IOPS potrebbero richiedere una profondità di coda elevata o più sessioni per ottenere questo livello di IOPS su un singolo volume.

10. Selezionare **Create Volume** (Crea volume).

Applicare un criterio QoS a un volume

È possibile applicare una policy di QoS ai volumi di storage esistenti utilizzando NetApp Hybrid Cloud Control. Se invece è necessario impostare valori QoS personalizzati per un volume, è possibile Modificare un volume. Per creare un nuovo criterio QoS, vedere "Creare e gestire policy di QoS per volumi".

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da associare a un criterio QoS.
5. Selezionare l'elenco a discesa **Actions** (azioni) nella parte superiore della tabella Volumes (volumi) e selezionare **Apply QoS Policy** (Applica policy QoS).
6. Nella finestra visualizzata, selezionare una policy QoS dall'elenco e selezionare **Apply QoS Policy** (Applica policy QoS).

> Se si utilizzano policy QoS su un volume, è possibile impostare una QoS personalizzata per rimuovere l'affiliazione della policy QoS con il volume. I valori di QoS personalizzati sovrascrivono i valori dei criteri di QoS per le impostazioni di QoS del volume.

Modificare un volume

Utilizzando NetApp Hybrid Cloud Control, è possibile modificare gli attributi del volume, ad esempio i valori QoS, le dimensioni del volume e l'unità di misura in base alla quale vengono calcolati i valori di byte. È inoltre possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

A proposito di questa attività

È possibile ridimensionare un volume quando lo spazio disponibile sul cluster è sufficiente nelle seguenti condizioni:

- Condizioni di funzionamento normali.
- Vengono segnalati errori o errori del volume.
- Il volume è in fase di clonaggio.
- Il volume è in fase di risyncing.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Nella colonna **azioni** della tabella volumi, espandere il menu del volume e selezionare **Modifica**.
5. Apportare le modifiche necessarie:

    a. Modificare le dimensioni totali del volume.

È possibile aumentare, ma non diminuire, le dimensioni del volume. È possibile ridimensionare un solo volume in una singola operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.

Se si stanno regolando le dimensioni del volume per la replica, aumentare innanzitutto le dimensioni del volume assegnato come destinazione della replica. Quindi, è possibile ridimensionare il volume di origine. Il volume di destinazione può avere dimensioni maggiori o uguali a quelle del volume di origine, ma non può essere più piccolo.

La dimensione predefinita del volume è in GB. È possibile creare volumi utilizzando dimensioni misurate in GB o GiB: 1 GB = 1 000 000 000 byte 1 GiB = 1 073 741 824 byte

b. Selezionare un diverso livello di accesso all'account:
   - Di sola lettura
   - Lettura/scrittura
   - Bloccato
   - Destinazione della replica
c. Selezionare l'account che deve avere accesso al volume.

   Inizia a digitare e la funzione di completamento automatico visualizza i valori possibili da scegliere.

   Se non esiste un account, selezionare **Crea nuovo account**, immettere un nuovo nome account e selezionare **Crea**. L'account viene creato e associato al volume esistente.
d. Modificare la qualità del servizio effettuando una delle seguenti operazioni:
   i. Selezionare un criterio esistente.
   ii. In Custom Settings (Impostazioni personalizzate), impostare i valori minimo, massimo e burst per IOPS o utilizzare i valori predefiniti.

Se si utilizzano policy QoS su un volume, è possibile impostare una QoS personalizzata per rimuovere l'affiliazione della policy QoS con il volume. La QoS personalizzata sovrascriverà i valori dei criteri QoS per le impostazioni QoS del volume.

Quando si modificano i valori IOPS, è necessario aumentare in decine o centinaia. I valori di input richiedono numeri interi validi. Configurare volumi con un valore burst estremamente elevato. Ciò consente al sistema di elaborare più rapidamente carichi di lavoro sequenziali a blocchi di grandi dimensioni occasionali, limitando al contempo gli IOPS sostenuti per un volume.

6. Selezionare **Salva**.

Clonare i volumi

È possibile creare un clone di un singolo volume di storage o clonare un gruppo di volumi per creare una copia point-in-time dei dati. Quando si clonano un volume, il sistema crea uno snapshot del volume e quindi una

copia dei dati a cui fa riferimento lo snapshot.

Prima di iniziare

- È necessario aggiungere ed eseguire almeno un cluster.
- È stato creato almeno un volume.
- È stato creato un account utente.
- Lo spazio disponibile senza provisioning deve essere uguale o superiore alle dimensioni del volume.

A proposito di questa attività

Il cluster supporta fino a due richieste di cloni in esecuzione per volume alla volta e fino a 8 operazioni di cloni di volume attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per l'elaborazione successiva.

La clonazione del volume è un processo asincrono e il tempo richiesto dal processo dipende dalle dimensioni del volume che si sta clonando e dal carico corrente del cluster.

I volumi clonati non ereditano l'appartenenza al gruppo di accesso al volume dal volume di origine.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare la scheda **volumi** > **Panoramica**.
4. Selezionare ciascun volume che si desidera clonare.
5. Selezionare l'elenco a discesa **azioni** nella parte superiore della tabella volumi e selezionare **Clona**.
6. Nella finestra visualizzata, procedere come segue:

    a. Immettere un prefisso per il nome del volume (facoltativo).

    b. Scegliere il tipo di accesso dall'elenco **Access**.

    c. Scegliere un account da associare al nuovo clone del volume (per impostazione predefinita, è selezionata l'opzione **Copy from Volume** (Copia da volume), che utilizzerà lo stesso account utilizzato dal volume originale).

    d. Se non esiste un account, selezionare **Crea nuovo account**, immettere un nuovo nome account e selezionare **Crea account**. L'account viene creato e associato al volume.

    Utilizzare le Best practice di denominazione descrittive. Ciò è particolarmente importante se nell'ambiente vengono utilizzati più cluster o server vCenter.

    L'aumento delle dimensioni del volume di un clone comporta la creazione di un nuovo volume con ulteriore spazio libero alla fine del volume. A seconda dell'utilizzo del volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per utilizzarlo.

    a. Selezionare **Clone Volumes** (Clona volumi).

Il tempo necessario per completare un'operazione di cloning dipende dalle dimensioni del volume e dal carico corrente del cluster. Aggiornare la pagina se il volume clonato non compare nell'elenco dei volumi.

Aggiungere volumi a un gruppo di accesso al volume

È possibile aggiungere un singolo volume o un gruppo di volumi a un gruppo di accesso al volume.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da associare a un gruppo di accesso al volume.
5. Selezionare l'elenco a discesa **azioni** nella parte superiore della tabella volumi e selezionare **Aggiungi a gruppo di accesso**.
6. Nella finestra visualizzata, selezionare un gruppo di accesso al volume dall'elenco **Volume Access Group**.
7. Selezionare **Add Volume** (Aggiungi volume).

Eliminare un volume

È possibile eliminare uno o più volumi da un cluster di storage Element.

A proposito di questa attività

Il sistema non elimina immediatamente i volumi cancellati, ma rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati e non più disponibili. Se si ripristina un volume prima che venga spurgato dal sistema, il volume torna online e le connessioni iSCSI vengono ripristinate.

Se un volume utilizzato per creare uno snapshot viene cancellato, le relative snapshot associate diventano inattive. Quando i volumi di origine cancellati vengono rimossi, anche le snapshot inattive associate vengono rimosse dal sistema.

I volumi persistenti associati ai servizi di gestione vengono creati e assegnati a un nuovo account durante l'installazione o l'aggiornamento. Se si utilizzano volumi persistenti, non modificare o eliminare i volumi o l'account associato. Se si eliminano questi volumi, si potrebbe rendere inutilizzabile il nodo di gestione.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare uno o più volumi da eliminare.
5. Selezionare l'elenco a discesa **azioni** nella parte superiore della tabella volumi e selezionare **Elimina**.
6. Nella finestra visualizzata, confermare l'azione selezionando **Sì**.

Ripristinare un volume cancellato

Una volta eliminato un volume di storage, è comunque possibile ripristinarlo entro otto ore dall'eliminazione.

Il sistema non elimina immediatamente i volumi cancellati, ma rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati e non più disponibili. Se si ripristina un volume prima che venga spurgato dal sistema, il volume torna online e le connessioni iSCSI vengono ripristinate.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare **Deleted**.
5. Nella colonna **Actions** della tabella Volumes, espandere il menu del volume e selezionare **Restore**.
6. Confermare il processo selezionando **Sì**.

Eliminare un volume cancellato

Una volta cancellati, i volumi di storage rimangono disponibili per circa otto ore. Dopo otto ore, vengono eliminati automaticamente e non più disponibili. Se non si desidera attendere le otto ore, è possibile eliminare

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi** > **Panoramica**.
4. Selezionare **Deleted**.
5. Selezionare uno o più volumi da eliminare.
6. Effettuare una delle seguenti operazioni:
   - Se sono stati selezionati più volumi, selezionare il filtro rapido **Purge** nella parte superiore della tabella.
   - Se è stato selezionato un singolo volume, nella colonna **Actions** della tabella Volumes (volumi), espandere il menu del volume e selezionare **Purge** (Rimuovi).
7. Nella colonna **Actions** della tabella Volumes, espandere il menu del volume e selezionare **Purge**.
8. Confermare il processo selezionando **Sì**.

Trova ulteriori informazioni

- "Scopri i volumi"
- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Creare e gestire i gruppi di accesso ai volumi

È possibile creare nuovi gruppi di accesso ai volumi, apportare modifiche al nome, agli iniziatori associati o ai volumi associati dei gruppi di accesso oppure eliminare i gruppi di accesso ai volumi esistenti utilizzando NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- Si dispone delle credenziali di amministratore per questo sistema storage all-flash SolidFire.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.15.28. La gestione dello storage NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti dei service bundle.
- Assicurarsi di disporre di uno schema di denominazione logico per i gruppi di accesso ai volumi.

Aggiungere un gruppo di accesso al volume

È possibile aggiungere un gruppo di accesso a un volume a un cluster di storage utilizzando NetApp Hybrid Cloud Control.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.
5. Selezionare il pulsante **Create Access Group** (Crea gruppo di accesso).
6. Nella finestra di dialogo visualizzata, immettere un nome per il nuovo gruppo di accesso al volume.
7. (Facoltativo) nella sezione **initiator**, selezionare uno o più iniziatori da associare al nuovo gruppo di accesso al volume.

   Se si associa un iniziatore al gruppo di accesso al volume, tale iniziatore può accedere a ciascun volume del gruppo senza necessità di autenticazione.

8. (Facoltativo) nella sezione **volumi**, selezionare uno o più volumi da includere in questo gruppo di accesso al volume.
9. Selezionare **Crea gruppo di accesso**.

Modificare un gruppo di accesso al volume

È possibile modificare le proprietà di un gruppo di accesso a un volume esistente utilizzando NetApp Hybrid Cloud Control. È possibile modificare il nome, gli iniziatori associati o i volumi associati di un gruppo di accesso.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.

5. Nella colonna **azioni** della tabella dei gruppi di accesso, espandere il menu delle opzioni del gruppo di accesso da modificare.
6. Nel menu delle opzioni, selezionare **Modifica**.
7. Apportare le modifiche necessarie al nome, agli iniziatori associati o ai volumi associati.
8. Confermare le modifiche selezionando **Salva**.
9. Nella tabella **gruppi di accesso**, verificare che il gruppo di accesso rifletta le modifiche.

Eliminare un gruppo di accesso al volume

È possibile rimuovere un gruppo di accesso al volume utilizzando NetApp Hybrid Cloud Control e, allo stesso tempo, rimuovere dal sistema gli iniziatori associati a questo gruppo di accesso.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **gruppi di accesso**.
5. Nella colonna **azioni** della tabella dei gruppi di accesso, espandere il menu delle opzioni per il gruppo di accesso da eliminare.
6. Nel menu delle opzioni, selezionare **Delete** (Elimina).
7. Se non si desidera eliminare gli iniziatori associati al gruppo di accesso, deselezionare la casella di controllo **Delete initiator in this access group** (Elimina iniziatori in questo gruppo di accesso).
8. Confermare l'operazione di eliminazione selezionando **Sì**.

Trova ulteriori informazioni

- "Informazioni sui gruppi di accesso ai volumi"
- "Aggiungere l'iniziatore a un gruppo di accesso al volume"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Creare e gestire gli iniziatori

È possibile utilizzare "iniziatori" Per l'accesso ai volumi basato su CHAP e non basato su account. È possibile creare ed eliminare gli iniziatori e assegnare loro alias semplici per semplificare l'amministrazione e l'accesso ai volumi. Quando si aggiunge un iniziatore a un gruppo di accesso al volume, tale iniziatore consente l'accesso a tutti i volumi del gruppo.

Di cosa hai bisogno

- Si dispone delle credenziali di amministratore del cluster.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.17. La gestione degli iniziatori di NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti dei service bundle.

Opzioni

- Creare un iniziatore
- Aggiungere gli iniziatori a un gruppo di accesso al volume
- Modificare un alias iniziatore
- Eliminare gli iniziatori

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnarli alias.

A proposito di questa attività

Il formato accettato di un IQN Initiator è `iqn.yyyy-mm` dove y e m sono cifre seguite da testo che deve contenere solo cifre, caratteri alfabetici minuscoli e un punto (`.`), due punti (`:`) o trattino (`-`). Un esempio del formato è il seguente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```

Il formato accettato di un iniziatore Fibre Channel WWPN è `:Aa:bB:CC:dd:11:22:33:44` oppure `AabBCCdd11223344`. Un esempio del formato è il seguente:

```
5f:47:ac:c0:5c:74:d4:02
```

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Selezionare il pulsante **Crea iniziatori**.

Opzione	Fasi
Creare uno o più iniziatori	a. Immettere l'IQN o il WWPN dell'iniziatore nel campo **IQN/WWPN**. b. Immettere un nome descrittivo per l'iniziatore nel campo **Alias**. c. (Facoltativo) selezionare **Add Initiator** (Aggiungi iniziatore) per aprire nuovi campi iniziatore o utilizzare l'opzione di creazione in blocco. d. Selezionare **Crea iniziatori**.

Opzione	Fasi
Iniziatori di creazione in blocco	a. Selezionare **Aggiungi IQN/WWPN in blocco**. b. Inserire un elenco di IQN o WWPN nella casella di testo. Ogni IQN o WWPN deve essere separato da virgole o spazi o su una propria riga. c. Selezionare **Aggiungi IQN/WWPN**. d. (Facoltativo) aggiungere alias univoci a ciascun iniziatore. e. Rimuovere dall'elenco qualsiasi iniziatore che potrebbe già esistere nell'installazione. f. Selezionare **Crea iniziatori**.

Aggiungere gli iniziatori a un gruppo di accesso al volume

È possibile aggiungere gli iniziatori a un gruppo di accesso al volume. Quando si aggiunge un iniziatore a un gruppo di accesso al volume, l'iniziatore consente l'accesso a tutti i volumi in tale gruppo di accesso al volume.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Selezionare uno o più iniziatori da aggiungere.
6. Selezionare **azioni > Aggiungi a gruppo di accesso**.
7. Selezionare il gruppo di accesso.
8. Confermare le modifiche selezionando **Add Initiator** (Aggiungi iniziatore).

Modificare un alias iniziatore

È possibile modificare l'alias di un iniziatore esistente o aggiungere un alias se non ne esiste già uno.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Nella colonna **azioni**, espandere il menu delle opzioni per l'iniziatore.
6. Selezionare **Modifica**.
7. Apportare le modifiche necessarie all'alias o aggiungere un nuovo alias.

8. Selezionare **Salva**.

Eliminare gli iniziatori

È possibile eliminare uno o più iniziatori. Quando si elimina un iniziatore, il sistema lo rimuove da qualsiasi gruppo di accesso al volume associato. Tutte le connessioni che utilizzano l'iniziatore rimangono valide fino al ripristino della connessione.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il nome del cluster di storage nel menu di navigazione a sinistra.
3. Selezionare **volumi**.
4. Selezionare la scheda **iniziatori**.
5. Eliminare uno o più iniziatori:
   a. Selezionare uno o più iniziatori da eliminare.
   b. Selezionare **azioni > Elimina**.
   c. Confermare l'operazione di eliminazione e selezionare **Sì**.

Trova ulteriori informazioni

- "Scopri di più sugli iniziatori"
- "Informazioni sui gruppi di accesso ai volumi"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Creare e gestire policy di QoS per volumi

Una policy QoS (Quality of Service) consente di creare e salvare un'impostazione di qualità del servizio standardizzata che può essere applicata a molti volumi. Il cluster selezionato deve essere l'elemento 10.0 o successivo per utilizzare i criteri QoS; in caso contrario, le funzioni dei criteri QoS non sono disponibili.

Per ulteriori informazioni sull'utilizzo, consultare il contenuto dei concetti relativi allo storage all-flash SolidFire "Policy di QoS" invece di un singolo volume "QoS".

Utilizzando NetApp Hybrid Cloud Control, è possibile creare e gestire policy QoS completando le seguenti attività:

- Creare una policy QoS
- Applicare un criterio QoS a un volume
- Modificare l'assegnazione del criterio QoS di un volume
- Modificare un criterio QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare policy QoS e applicarle a volumi che devono avere performance equivalenti.

Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascrive e regola i valori dei criteri QoS per le impostazioni QoS del volume.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare la scheda **QoS Policies** (Criteri QoS).
5. Selezionare **Crea policy**.
6. Inserire il nome * Policy Name*.

   Utilizzare le Best practice di denominazione descrittive. Ciò è particolarmente importante se nell'ambiente vengono utilizzati più cluster o server vCenter.

7. Inserire i valori minimo IOPS, massimo IOPS e burst IOPS.
8. Selezionare **Crea policy QoS**.

   Viene generato un ID di sistema per il criterio e il criterio viene visualizzato nella pagina QoS Policies (Criteri QoS) con i relativi valori QoS assegnati.

Applicare un criterio QoS a un volume

È possibile assegnare una policy QoS esistente a un volume utilizzando NetApp Hybrid Cloud Control.

Di cosa hai bisogno

Il criterio QoS che si desidera assegnare è stato creato.

A proposito di questa attività

Questa attività descrive come assegnare un criterio QoS a un singolo volume modificandone le impostazioni. La versione più recente di NetApp Hybrid Cloud Control non dispone di un'opzione di assegnazione in blocco per più di un volume. Fino a quando la funzionalità di assegnazione in blocco non sarà fornita in una release futura, è possibile utilizzare l'interfaccia utente Web Element o l'interfaccia utente del plug-in vCenter per assegnare in blocco i criteri QoS.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare il menu **azioni** accanto al volume che si desidera modificare.
5. Nel menu visualizzato, selezionare **Edit** (Modifica).
6. Nella finestra di dialogo, attivare **Assign QoS Policy** (Assegna policy QoS) e selezionare il criterio QoS

dall'elenco a discesa da applicare al volume selezionato.

> L'assegnazione di QoS sovrascriverà i valori di QoS dei singoli volumi precedentemente applicati.

7. Selezionare **Salva**.

Modificare l'assegnazione del criterio QoS di un volume

È possibile rimuovere l'assegnazione di una policy QoS da un volume o selezionare una policy QoS diversa o una QoS personalizzata.

Di cosa hai bisogno

Il volume che si desidera modificare è assegnato Una policy QoS.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare il menu **azioni** accanto al volume che si desidera modificare.
5. Nel menu visualizzato, selezionare **Edit** (Modifica).
6. Nella finestra di dialogo, eseguire una delle seguenti operazioni:
   - Disattivare **Assign QoS Policy** e modificare i valori **min IOPS**, **Max IOPS** e **Burst IOPS** per la QoS dei singoli volumi.

     > Quando i criteri QoS sono disattivati, il volume utilizza i valori IOPS QoS predefiniti, a meno che non vengano modificati diversamente.

   - Selezionare un criterio QoS diverso dall'elenco a discesa da applicare al volume selezionato.
7. Selezionare **Salva**.

Modificare un criterio QoS

È possibile modificare il nome di un criterio QoS esistente o i valori associati al criterio. La modifica dei valori delle performance dei criteri QoS influisce sulla QoS per tutti i volumi associati al criterio.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare la scheda **QoS Policies** (Criteri QoS).
5. Selezionare il menu **azioni** accanto al criterio QoS che si desidera modificare.
6. Selezionare **Modifica**.
7. Nella finestra di dialogo **Edit QoS Policy** (Modifica policy QoS), modificare una o più delle seguenti opzioni:

- **Name**: Il nome definito dall'utente per la policy QoS.
- **IOPS min**: Il numero minimo di IOPS garantito per il volume. Impostazione predefinita = 50.
- **IOPS max**: Il numero massimo di IOPS consentito per il volume. Impostazione predefinita = 15,000.
- **Burst IOPS**: Il numero massimo di IOPS consentito per un breve periodo di tempo per il volume. Impostazione predefinita = 15,000.

8. Selezionare **Salva**.

È possibile selezionare un criterio sul collegamento nella colonna **volumi attivi** per visualizzare un elenco filtrato dei volumi assegnati a tale criterio.

Eliminare una policy QoS

È possibile eliminare una policy QoS se non è più necessaria. Quando si elimina un criterio QoS, tutti i volumi assegnati con il criterio mantengono i valori QoS precedentemente definiti dal criterio, ma come QoS dei singoli volumi. Qualsiasi associazione con la policy QoS eliminata viene rimossa.

Fasi

1. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla dashboard, espandere il menu del cluster di storage.
3. Selezionare **Storage > Volumes** (Storage > volumi).
4. Selezionare la scheda **QoS Policies** (Criteri QoS).
5. Selezionare il menu **azioni** accanto al criterio QoS che si desidera modificare.
6. Selezionare **Delete** (Elimina).
7. Confermare l'azione.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Monitorate il vostro sistema SolidFire con il controllo del cloud ibrido NetApp

Monitorare le risorse di storage sul pannello di controllo del cloud ibrido

Con la dashboard di controllo del cloud ibrido di NetApp, puoi visualizzare tutte le risorse di storage in un colpo d'occhio. Inoltre, è possibile monitorare la capacità dello storage e le performance dello storage.

Quando avvii una nuova sessione di NetApp Hybrid Cloud Control per la prima volta, potrebbe verificarsi un ritardo nel caricamento della vista di NetApp Hybrid Cloud Control Dashboard quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia in base al numero di cluster gestiti attivamente dal nodo di gestione. Per i lanci successivi, si verificheranno tempi di caricamento più rapidi.

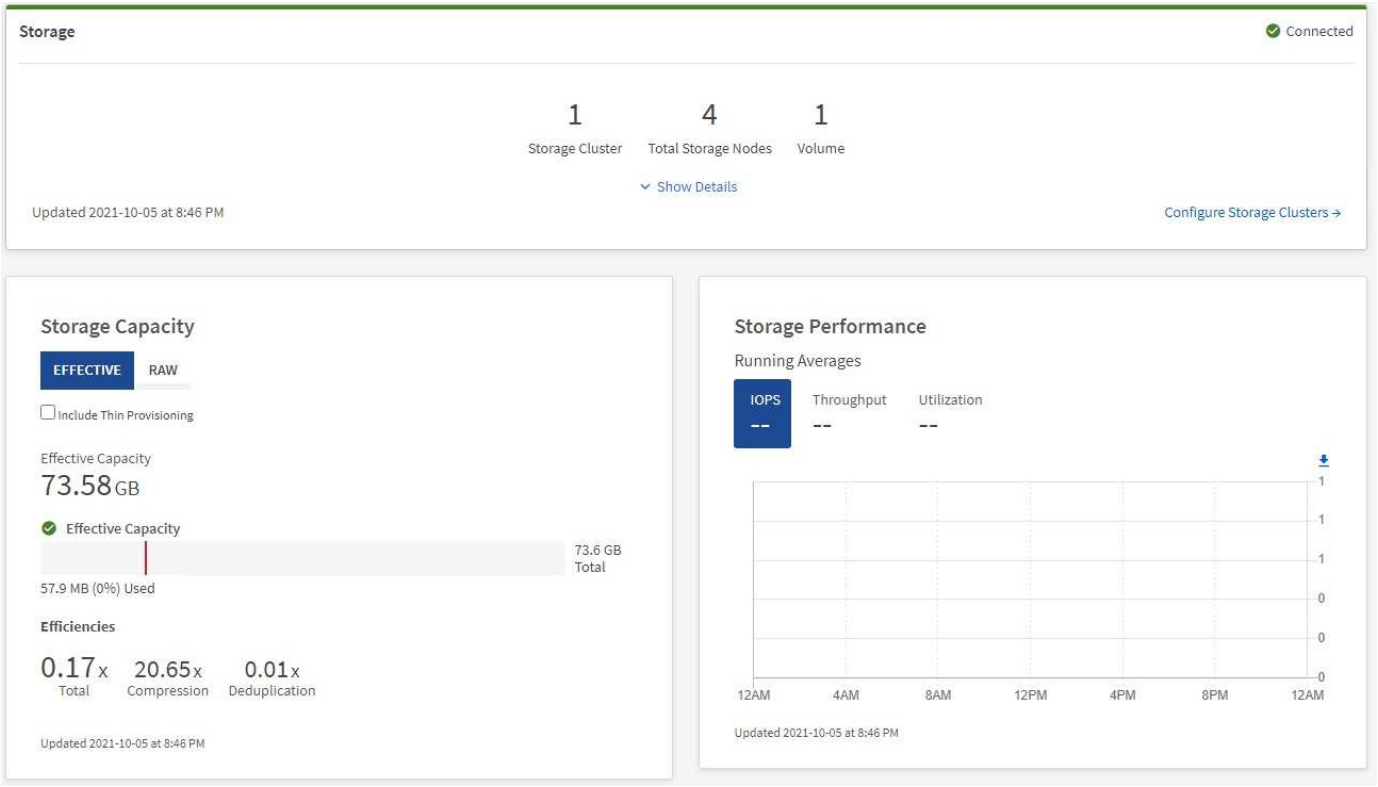
- Accedere al dashboard di NetApp HCC
- Monitorare le risorse di storage
- Monitorare la capacità dello storage
- Monitorare le performance dello storage

Accedere al dashboard di NetApp HCC

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://[management node IP address]
```

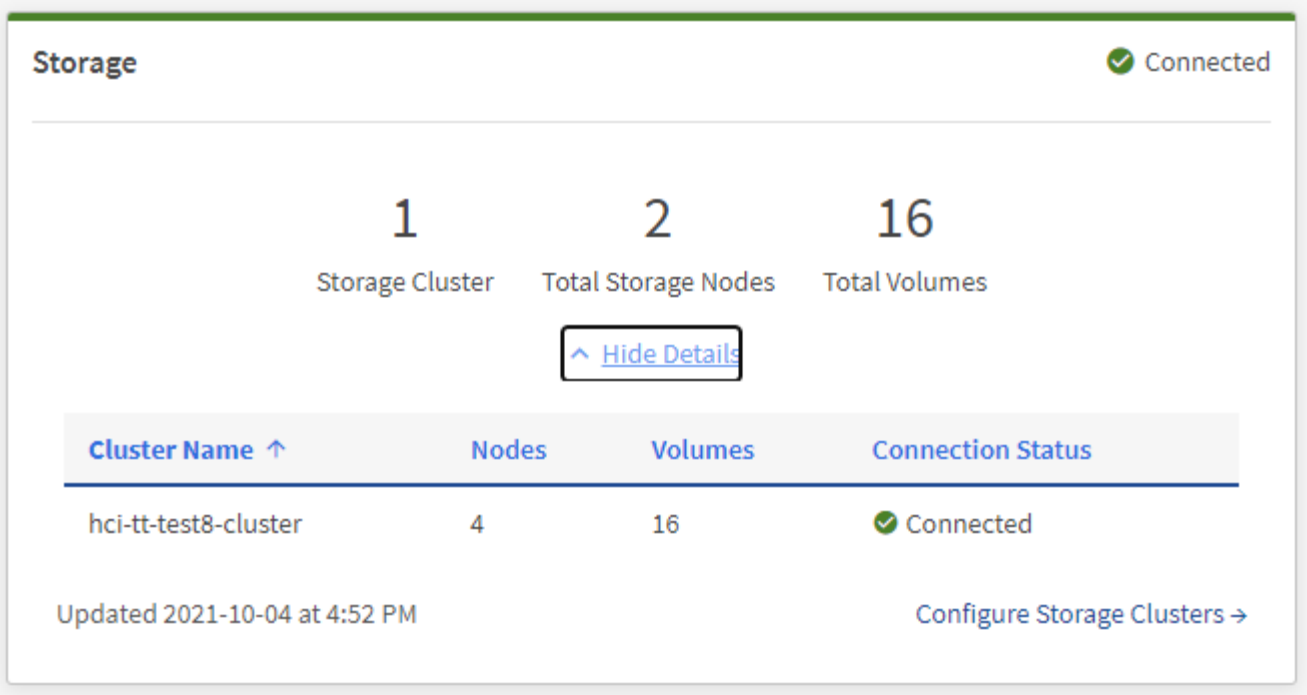
2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire.
3. Visualizza la dashboard di controllo del cloud ibrido.



Monitorare le risorse di storage

Utilizzare il riquadro **Storage** per visualizzare l'intero ambiente di storage. È possibile monitorare il numero di cluster di storage, nodi di storage e volumi totali.

Per visualizzare i dettagli, nel riquadro Storage (archiviazione), selezionare **Show Details** (Mostra dettagli).



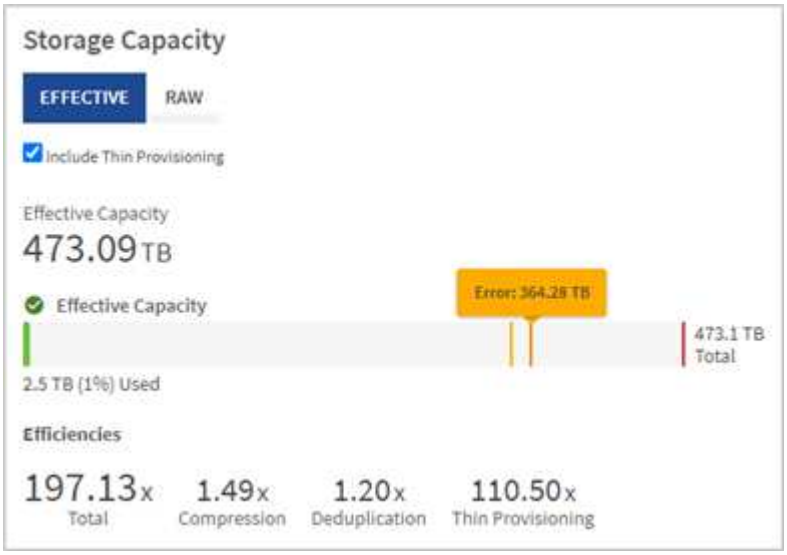
Il numero dei nodi di storage totali non include i nodi di controllo dei cluster di storage a due nodi. I nodi di controllo sono inclusi nel numero dei nodi nella sezione dei dettagli del cluster.

Per visualizzare i dati più recenti del cluster di storage, utilizzare la pagina Storage Clusters, in cui il polling viene eseguito con maggiore frequenza rispetto alla dashboard.

Monitorare la capacità dello storage

Il monitoraggio della capacità di storage del tuo ambiente è fondamentale. Il riquadro Storage Capacity (capacità storage) consente di determinare i vantaggi in termini di efficienza della capacità dello storage con o senza funzionalità di compressione, deduplica e thin provisioning abilitate.

È possibile visualizzare lo spazio fisico di storage totale disponibile nel cluster nella scheda **RAW** e le informazioni sullo storage fornito nella scheda **EFFETTIVO**.



Fasi

1. Selezionare la scheda **RAW** per visualizzare lo spazio di storage fisico totale utilizzato e disponibile nel cluster.

   Esaminare le linee verticali per determinare se la capacità utilizzata è inferiore al totale o inferiore alle soglie di avviso, errore o critico. Passare il mouse sulle linee per visualizzare i dettagli.

   È possibile impostare la soglia di avviso, che per impostazione predefinita è inferiore del 3% alla soglia di errore. Le soglie di errore e critico sono preimpostate e non configurabili in base alla progettazione. La soglia di errore indica che nel cluster rimane meno di un nodo di capacità. Per informazioni sull'impostazione della soglia, vedere "Impostazione della soglia cluster full".

   Per ulteriori informazioni sull'API degli elementi delle soglie del cluster correlati, vedere ""GetClusterFullThreshold"" Nella *documentazione API del software Element*. Per ulteriori informazioni sulla capacità di blocchi e metadati, vedere "Comprensione dei livelli di completezza del cluster" Nella *documentazione software Element*.

2. Selezionare la scheda **EFFETTIVO** per visualizzare le informazioni sullo storage totale fornito agli host connessi e le valutazioni di efficienza.
   a. Facoltativamente, selezionare **Includi thin provisioning** per visualizzare i tassi di efficienza del thin provisioning nel grafico a barre capacità effettiva.
   b. **Grafico a barre capacità effettiva**: Esaminare le linee verticali per determinare se la capacità utilizzata è inferiore al totale o inferiore alle soglie di avviso, errore o critico. Analogamente alla scheda Raw, è possibile passare il mouse sulle linee verticali per visualizzare i dettagli.
   c. **Efficienze**: Guarda queste valutazioni per determinare i tuoi guadagni in termini di efficienza della capacità dello storage con le funzionalità di compressione, deduplica e thin provisioning abilitate. Ad esempio, se la compressione viene visualizzata come "1.3x", significa che l'efficienza dello storage con compressione abilitata è 1.3 volte più efficiente che senza di essa.

      Efficienze totali pari a (fattore di efficienza maxUsedSpace *) / 2, dove EfficiencyFactor = (thinProvisioningFactor * deDuplicationFactor * compressionFactor). Quando il thin provisioning non è selezionato, non viene incluso nel Total Efficiency.

   d. Se la capacità di storage effettiva si avvicina a una soglia di errore o critica, considerare l'eliminazione dei dati nel sistema.
3. Per ulteriori analisi e contesto storico, vedere "Dettagli di NetApp SolidFire Active IQ".

Monitorare le performance dello storage

È possibile osservare la quantità di IOPS o di throughput che è possibile ottenere da un cluster senza superare le utili performance di tale risorsa utilizzando il riquadro Storage Performance (prestazioni dello storage). Le performance dello storage sono il punto in cui si ottiene il massimo utilizzo prima che la latenza diventi un problema.

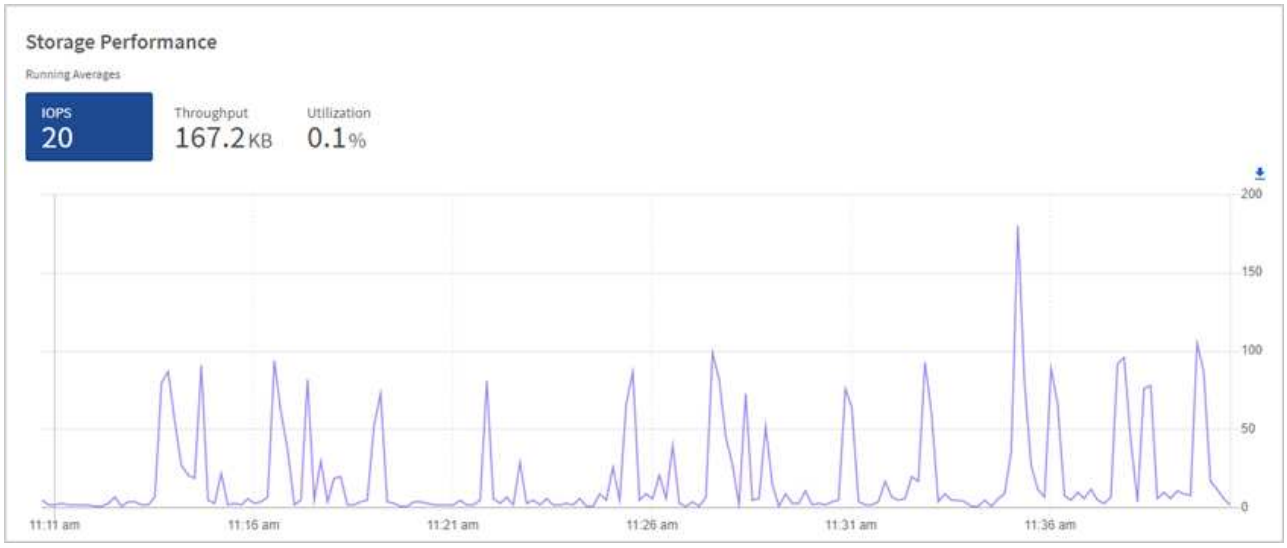
Il pannello delle performance dello storage ti aiuta a identificare se le performance stanno raggiungendo il punto in cui le performance potrebbero degradarsi se i carichi di lavoro aumentano.

Le informazioni di questo riquadro vengono aggiornate ogni 10 secondi e vengono visualizzate in media tutti i punti del grafico.

Per ulteriori informazioni sul metodo API Element associato, vedere "GetClusterStats" Metodo nella *documentazione API del software Element*.

Fasi

1. Visualizzare il riquadro Storage Performance (prestazioni storage). Per i dettagli, passare il mouse sui punti del grafico.
   a. Scheda **IOPS**: Visualizza le operazioni correnti al secondo. Cerca tendenze in termini di dati o picchi. Ad esempio, se si nota che il numero massimo di IOPS è pari a 160.000 e 100.000 di IOPS gratuiti o disponibili, si potrebbe prendere in considerazione l'aggiunta di più carichi di lavoro a questo cluster. D'altra parte, se si vede che sono disponibili solo 140K, si potrebbe prendere in considerazione l'offload dei carichi di lavoro o l'espansione del sistema.



   b. Scheda **throughput**: Monitorare gli schemi o i picchi di throughput. Inoltre, è possibile monitorare i valori di throughput costantemente elevati, che potrebbero indicare che si stanno avvicinando alle massime prestazioni utili della risorsa.

   c. Scheda **Utilization** (utilizzo): Consente di monitorare l'utilizzo degli IOPS in relazione al totale degli IOPS disponibili sommato a livello di cluster.

2. Per ulteriori analisi, esaminare le performance dello storage utilizzando il plug-in NetApp Element per vCenter Server.

   "Le performance mostrate nel plug-in NetApp Element per vCenter Server".

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Visualizzare l'inventario nella pagina nodi

È possibile visualizzare le risorse di storage nel sistema e determinare gli indirizzi IP, i nomi e le versioni software.

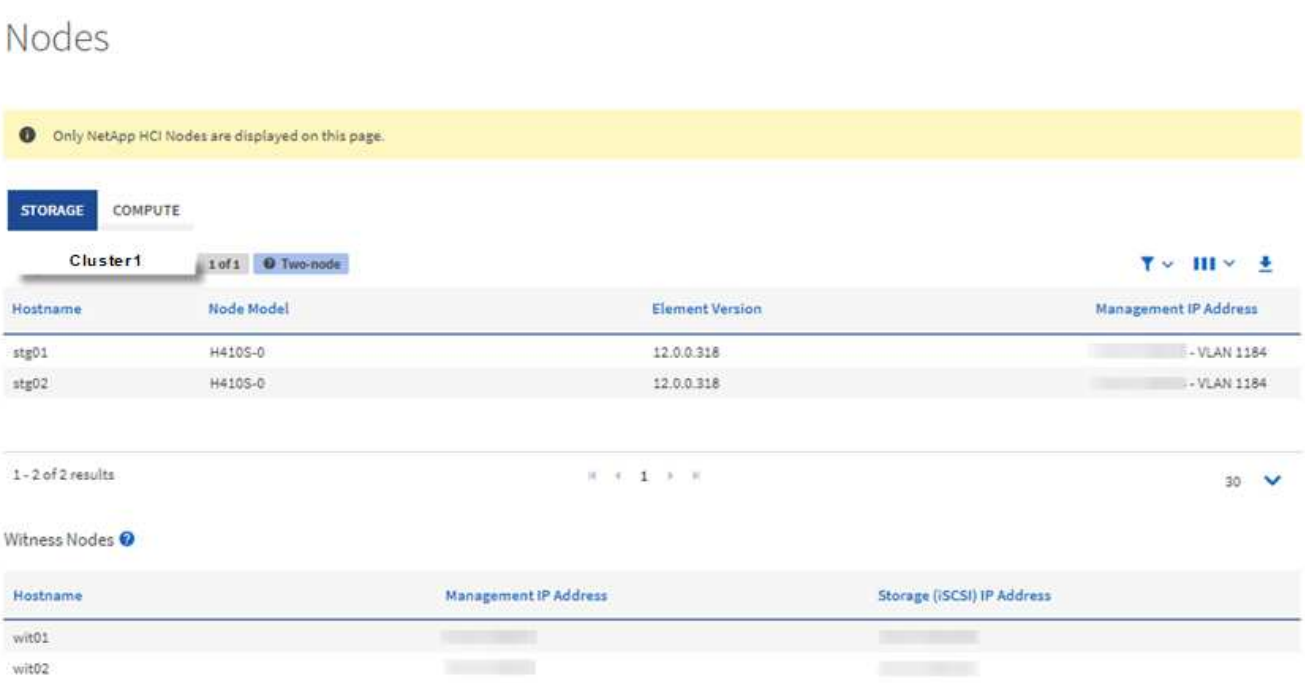
È possibile visualizzare le informazioni di storage per i sistemi a più nodi. Se "domini di protezione personalizzati" è possibile visualizzare i domini di protezione assegnati a nodi specifici.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://[management node IP address]
   ```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire.
3. Nella barra di navigazione a sinistra, selezionare **Nodes** (nodi).



Quando avvii una nuova sessione di NetApp Hybrid Cloud Control per la prima volta, potrebbe verificarsi un ritardo nel caricamento della pagina dei nodi di NetApp Hybrid Cloud Control quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia in base al numero di cluster gestiti attivamente dal nodo di gestione. Per i lanci successivi, si verificheranno tempi di caricamento più rapidi.

4. Nella scheda **Storage** della pagina Nodes (nodi), esaminare le seguenti informazioni:
   a. Cluster a due nodi: Nella scheda Storage viene visualizzata un'etichetta a due nodi e vengono elencati i nodi di controllo associati.
   b. Cluster a tre nodi: Vengono elencati i nodi di storage e i nodi di controllo associati. I cluster a tre nodi dispongono di un nodo di controllo implementato in standby per mantenere un'elevata disponibilità in caso di guasto del nodo.
   c. Cluster con quattro o più nodi: Vengono visualizzate le informazioni relative ai cluster con quattro o più nodi. I nodi di controllo non sono applicabili. Se si è iniziato con due o tre nodi di storage e sono stati aggiunti altri nodi, i nodi di controllo continuano a essere visualizzati. In caso contrario, la tabella dei nodi di controllo non viene visualizzata.
   d. Versione del bundle firmware: A partire dalla versione 2.14 dei servizi di gestione, se si utilizzano cluster con Element 12.0 o versione successiva, è possibile visualizzare la versione del bundle firmware per questi cluster. Se i nodi di un cluster hanno versioni firmware diverse, nella colonna **firmware Bundle Version** viene visualizzato **multiple**.
   e. Domini di protezione personalizzati: Se nel cluster sono in uso domini di protezione personalizzati, è possibile visualizzare le assegnazioni dei domini di protezione personalizzati per ciascun nodo del cluster. Se i domini di protezione personalizzati non sono abilitati, questa colonna non viene visualizzata.
5. È possibile modificare le informazioni presenti in queste pagine in diversi modi:
   a. Per filtrare l'elenco degli elementi nei risultati, selezionare l'icona **Filter** (filtro) e selezionare i filtri. È anche possibile inserire il testo per il filtro.
   b. Per visualizzare o nascondere le colonne, selezionare l'icona **Mostra/Nascondi colonne**.

c. Per scaricare la tabella, selezionare l'icona **Download**.

Per visualizzare il numero di storage, consulta la dashboard di NetApp Hybrid Cloud Control (HCC). Vedere "Monitorare le risorse di storage con la dashboard HCC".

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Monitorare i volumi nel cluster di storage

Il sistema SolidFire esegue il provisioning dello storage utilizzando i volumi. I volumi sono dispositivi a blocchi a cui si accede in rete dai client iSCSI o Fibre Channel. È possibile monitorare i dettagli relativi a gruppi di accesso, account, iniziatori, capacità utilizzata, stato di protezione dei dati Snapshot, numero di sessioni iSCSI e policy di qualità del servizio (QoS) associate al volume.

È inoltre possibile visualizzare i dettagli sui volumi attivi ed eliminati.

Con questa visualizzazione, è possibile monitorare prima la colonna capacità utilizzata.

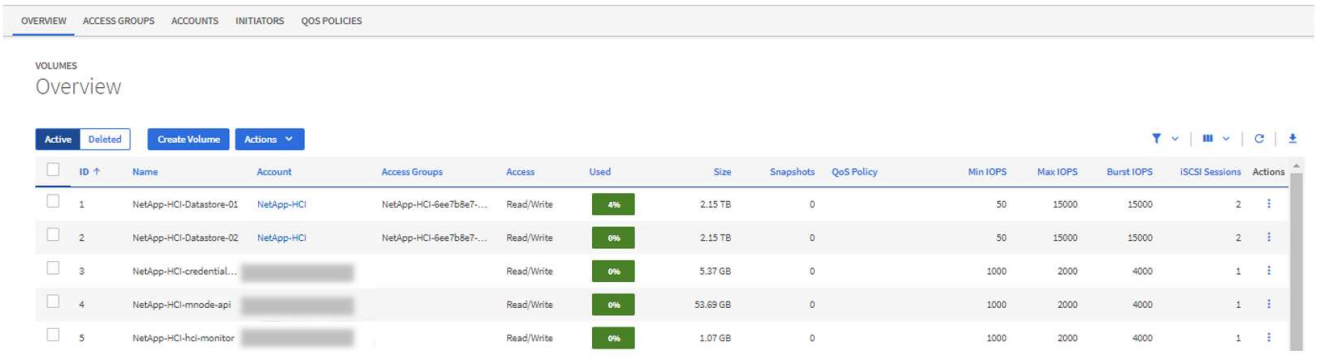
Puoi accedere a queste informazioni solo se disponi dei privilegi amministrativi di NetApp Hybrid Cloud Control.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

```
https://[management node IP address]
```

2. Accedi al controllo del cloud ibrido NetApp fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire.
3. Nella casella blu di navigazione a sinistra, selezionare l'installazione dello storage all-flash SolidFire.
4. Nella barra di navigazione a sinistra, selezionare il cluster e scegliere **Storage** > **Volumes**.



5. Nella pagina Volumes (volumi), utilizzare le seguenti opzioni:

a. Filtrare i risultati selezionando l'icona **Filter**.

b. Per nascondere o visualizzare le colonne, selezionare l'icona **Nascondi/Mostra**.

c. Aggiornare i dati selezionando l'icona **Refresh** (Aggiorna).

d. Scaricare un file CSV selezionando l'icona **Download**.

6. Monitorare la colonna capacità utilizzata. Se vengono raggiunte le soglie di avviso, errore o critico, il colore rappresenta lo stato della capacità utilizzata:

   a. Avvertenza - giallo

   b. Errore - arancione

   c. Critico - Rosso

7. Dalla vista Volumes (volumi), selezionare le schede per visualizzare ulteriori dettagli sui volumi:

   a. **Gruppi di accesso**: È possibile visualizzare i gruppi di accesso al volume mappati dagli iniziatori a un insieme di volumi per un accesso protetto.

      Vedere le informazioni su "gruppi di accesso ai volumi".

   b. **Account**: È possibile visualizzare gli account utente, che consentono ai client di connettersi ai volumi su un nodo. Quando si crea un volume, questo viene assegnato a un account utente specifico.

      Vedere le informazioni su "Account utente del sistema storage all-flash SolidFire".

   c. **Initiator**: È possibile visualizzare le WWPN iSCSI Initiator IQN o Fibre Channel per il volume. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume del gruppo senza richiedere l'autenticazione CHAP. Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso alla rete Fibre Channel ai volumi del gruppo di accesso.

   d. **QoS Policies** (Criteri QoS): È possibile visualizzare il criterio QoS applicato al volume. Una policy di QoS applica impostazioni standardizzate per IOPS minimi, IOPS massimi e IOPS burst a più volumi.

      Vedere le informazioni su "Policy di performance e QoS".

Trova ulteriori informazioni

- "SolidFire e documentazione degli elementi"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Raccogliere i registri per la risoluzione dei problemi

In caso di problemi con l'installazione dello storage all-flash SolidFire, è possibile raccogliere i registri da inviare al supporto NetApp per fornire assistenza nella diagnosi. È possibile utilizzare NetApp Hybrid Cloud Control o L'API REST per raccogliere i log su un sistema di elementi.

Di cosa hai bisogno

- Assicurarsi che la versione del cluster di storage in uso utilizzi il software NetApp Element 11.3 o versione

successiva.

- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni di raccolta dei log

Scegliere una delle seguenti opzioni:

- Utilizza NetApp Hybrid Cloud Control per raccogliere i log
- Utilizzare l'API REST per raccogliere i registri

Utilizza NetApp Hybrid Cloud Control per raccogliere i log

È possibile accedere all'area di raccolta dei log dal NetApp Hybrid Cloud Control Dashboard.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web. Ad esempio:

   ```
   https://[management node IP address]
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
3. Dalla dashboard, selezionare il menu in alto a destra.
4. Selezionare **Collect Logs** (raccolta registri).

   Se in precedenza sono stati raccolti dei log, è possibile scaricare il pacchetto di log esistente o iniziare una nuova raccolta di log.

5. Selezionare un intervallo di date nel menu a discesa **intervallo di date** per specificare le date da includere nei registri.

   Se si specifica una data di inizio personalizzata, è possibile selezionare la data in cui iniziare l'intervallo di date. I registri verranno raccolti da tale data fino all'ora corrente.

6. Nella sezione **Log Collection**, selezionare i tipi di file di log che il pacchetto di log deve includere.

   Per i registri di storage, è possibile espandere l'elenco dei nodi di storage e selezionare i singoli nodi da cui raccogliere i registri (o tutti i nodi nell'elenco).

7. Selezionare **Collect Logs** per avviare la raccolta dei log.

   La raccolta dei log viene eseguita in background e la pagina mostra lo stato di avanzamento.

   > A seconda dei registri raccolti, la barra di avanzamento potrebbe rimanere a una determinata percentuale per alcuni minuti o avanzare molto lentamente in alcuni punti.

8. Selezionare **Download Logs** per scaricare il pacchetto di log.

   Il pacchetto di log è in un formato di file .tgz UNIX compresso.

Utilizzare l'API REST per raccogliere i registri

È possibile utilizzare REST API per raccogliere i log degli elementi.

Fasi

1. Individuare l'ID del cluster di storage:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://[management node IP]/logs/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
      iii. Selezionare **autorizzare** per avviare una sessione.
2. Raccogli log da elemento:
   a. Selezionare **POST /bundle**.
   b. Selezionare **Provalo**.
   c. Modificare i valori dei seguenti parametri nel campo **corpo della richiesta** in base al tipo di log da raccogliere e all'intervallo di tempo:

Parametro	Tipo	Descrizione
`modifiedSince`	Stringa di dati	Includere solo i registri modificati dopo questa data e ora. Ad esempio, il valore "2020-07-14T20:19:00.000Z" definisce una data di inizio del 14 luglio 2020 alle 20:19 UTC.
`mnodeLogs`	Booleano	Impostare questo parametro su `true` per includere i log dei nodi di gestione.
`storageCrashDumps`	Booleano	Impostare questo parametro su `true` per includere i log di debug del crash del nodo di storage.
`storageLogs`	Booleano	Impostare questo parametro su `true` per includere i log dei nodi di storage.

Parametro	Tipo	Descrizione
`storageNodeIds`	Array UUID	Se `storageLogs` è impostato su `true`, Popolare questo parametro con gli ID dei nodi del cluster di storage per limitare la raccolta dei log a quei nodi di storage specifici. Utilizzare `GET https://[management node IP]/logs/1/bundle/options` Endpoint per visualizzare tutti i possibili ID di nodo che è possibile utilizzare.

d. Selezionare **Esegui** per iniziare la raccolta dei log. La risposta dovrebbe restituire una risposta simile a quanto segue:

```
{
  "_links": {
    "self": "https://10.1.1.5/logs/1/bundle"
  },
  "taskId": "4157881b-z889-45ce-adb4-92b1843c53ee",
  "taskLink": "https://10.1.1.5/logs/1/bundle"
}
```

3. Verificare lo stato dell'attività di raccolta dei log:
   a. Selezionare **GET /bundle**.
   b. Selezionare **Provalo**.
   c. Selezionare **Execute** (Esegui) per restituire lo stato dell'attività di raccolta.
   d. Scorrere fino alla parte inferiore del corpo della risposta.

      Viene visualizzato un `percentComplete` attributo che descrive l'avanzamento della raccolta. Se la raccolta è completa, il `downloadLink` l'attributo contiene il link completo per il download, incluso il nome del file del pacchetto di log.

   e. Copiare il nome del file alla fine di `downloadLink` attributo.
4. Scarica il pacchetto di log raccolto:
   a. Selezionare **GET /bundle/{filename}**.
   b. Selezionare **Provalo**.
   c. Incollare il nome del file precedentemente copiato in `filename` campo di testo del parametro.
   d. Selezionare **Esegui**.

      Al termine dell'esecuzione, viene visualizzato un collegamento per il download nell'area del corpo della risposta.

   e. Selezionare **Download file** (Scarica file) e salvare il file risultante sul computer.

Il pacchetto di log è in un formato di file .tgz UNIX compresso.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Gestire lo storage con Element API

È possibile gestire i cluster di storage Element utilizzando l'API software Element.

L'API Element si basa sul protocollo JSON-RPC su HTTPS. JSON-RPC è un semplice protocollo RPC basato su testo basato sul formato leggero di interscambio dati JSON. Le librerie client sono disponibili per tutti i principali linguaggi di programmazione.

- Informazioni sull'API del software Element
- Oggetti comuni
- Metodi comuni
- Metodi API dell'account
- Metodi API dell'amministratore
- Metodi API del cluster
- Metodi API per la creazione di cluster
- Metodi API del disco
- Metodi API Fibre Channel
- Metodi API initiator
- Metodi API LDAP
- Metodi API di autenticazione a più fattori
- Metodi API per l'autenticazione della sessione
- Metodi API del nodo
- Metodi API di replica
- Metodi API di sicurezza
- Metodi API di SnapMirror
- Metodi API di configurazione del sistema
- Metodi API di rete multi-tenant
- Metodi API del volume
- Metodi API del gruppo di accesso al volume
- Metodi API di Volume Snapshot
- Metodi API dei volumi virtuali
- Controllo degli accessi
- Esempi di risposte

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Centro di documentazione software SolidFire ed Element"

Informazioni sull'API del software Element

L'API Element si basa sul protocollo JSON-RPC su HTTPS. JSON-RPC è un semplice protocollo RPC basato su testo basato sul formato leggero di interscambio dati JSON. Le librerie client sono disponibili per tutti i principali linguaggi di programmazione.

È possibile effettuare richieste API tramite richieste HTTPS POST all'endpoint API. Il corpo della richiesta POST è un oggetto di richiesta JSON-RPC. L'API attualmente non supporta le richieste batch (più oggetti di richiesta in un SINGOLO POST). Quando si inviano richieste API, è necessario utilizzare "application/json-rpc" come tipo di contenuto della richiesta e assicurarsi che il corpo non sia codificato in forma.

> L'interfaccia utente Web Element utilizza i metodi API descritti in questo documento. È possibile monitorare le operazioni API nell'interfaccia utente attivando il log API; in questo modo è possibile visualizzare i metodi che vengono emessi al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi che vengono emessi.

Se non diversamente specificato, tutte le stringhe di data nelle risposte API sono in formato UTC+0.

> Quando il cluster di storage viene caricato pesantemente o vengono inviate molte richieste API consecutive senza alcun ritardo, un metodo potrebbe non riuscire e restituire l'errore "xDBVersionMismatch". In questo caso, riprovare a chiamare il metodo.

- Richiedi membri dell'oggetto
- Membri dell'oggetto di risposta
- Endpoint della richiesta
- Autenticazione API
- Metodi asincroni
- Attributi

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Richiedi membri dell'oggetto

Ogni richiesta API del software Element ha le seguenti parti di base:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
metodo	Nome del metodo da richiamare.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
parametri	Oggetto contenente i parametri del metodo da richiamare. I parametri denominati sono obbligatori. I parametri di posizione (passati come array) non sono consentiti.	Oggetto JSON	{}	No
id	Identificatore utilizzato per associare la richiesta alla risposta, restituito nel risultato.	stringa o numero intero	{}	No

Membri dell'oggetto di risposta

Ogni corpo di risposta API del software Element ha le seguenti parti di base:

Nome	Descrizione	Tipo
risultato	Oggetto restituito dal metodo. Il sistema restituisce un oggetto con membri denominati corrispondenti al valore restituito documentato per il metodo. Questo membro non è presente se si è verificato un errore.	Oggetto JSON
errore	L'oggetto restituito quando si verifica un errore. Questo membro è presente solo se si è verificato un errore.	Oggetto
id	Identificativo utilizzato per associare la richiesta alla risposta, come indicato nella richiesta.	stringa o numero intero
UnusedParameters	Un messaggio di avviso che informa che almeno un parametro non corretto è stato passato al metodo API e non è stato utilizzato.	Oggetto

Endpoint della richiesta

L'API utilizza tre tipi di endpoint di richiesta (cluster di storage, creazione di cluster di storage e per nodo). Si consiglia di utilizzare sempre l'endpoint più recente supportato dalla versione del software Element.

I tre endpoint della richiesta nell'API sono designati nei seguenti modi:

Metodi API del cluster

L'endpoint HTTPS per le richieste API a livello di cluster di storage è `https://<mvip>/json-rpc/<api-version>`, dove:

- `<mvip>` È l'indirizzo IP virtuale di gestione per il cluster di storage.
- `<api-version>` È la versione dell'API in uso.

Creazione di cluster e metodi API di bootstrap

L'endpoint HTTPS per la creazione di un cluster di storage e l'accesso alle richieste API di bootstrap è `https://<nodeIP>/json-rpc/<api-version>`, dove:

- `<nodeIP>` È l'indirizzo IP del nodo che si sta aggiungendo al cluster.
- `<api-version>` È la versione dell'API in uso.

Metodi API per nodo

L'endpoint HTTPS per le richieste API dei singoli nodi di storage è `https://<nodeIP>:442/json-rpc/<api-version>`, dove:

- `<nodeIP>` È l'indirizzo IP di gestione del nodo di storage; 442 è la porta su cui viene eseguito il server HTTPS.
- `<api-version>` È la versione dell'API in uso.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Autenticazione API

È possibile eseguire l'autenticazione con il sistema quando si utilizza l'API includendo un'intestazione di autenticazione HTTP Basic con tutte le richieste API. Se si omettono le informazioni di autenticazione, il sistema rifiuta la richiesta non autenticata con una risposta HTTP 401. Il sistema supporta l'autenticazione HTTP Basic su TLS.

Utilizzare l'account amministratore del cluster per l'autenticazione API.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Metodi asincroni

Alcuni metodi API sono asincroni, il che significa che l'operazione che eseguono potrebbe non essere completa quando il metodo restituisce. I metodi asincroni restituiscono un handle che è possibile interrogare per visualizzare lo stato dell'operazione; le informazioni di stato per alcune operazioni potrebbero includere una percentuale di completamento.

Quando si esegue una query su un'operazione asincrona, il risultato può essere uno dei seguenti tipi:

- `DriveAdd`: Il sistema sta aggiungendo un disco al cluster.
- `BulkVolume`: Il sistema sta eseguendo un'operazione di copia tra i volumi, ad esempio un backup o un ripristino.
- `Clone`: Il sistema sta clonando un volume.
- `DriveRemoval`: Il sistema sta copiando i dati da un disco in preparazione per rimuoverli dal cluster.
- `RtfiPendingNode`: Il sistema sta installando software compatibile su un nodo prima di aggiungerlo al cluster.

Tenere presente quanto segue quando si utilizzano metodi asincroni o si ottiene lo stato di un'operazione asincrona in esecuzione:

- I metodi asincroni sono indicati nella documentazione relativa ai singoli metodi.
- I metodi asincroni restituiscono un "asyncHandle", un handle noto dal metodo API di emissione. È possibile utilizzare l'handle per eseguire il polling dello stato o del risultato dell'operazione asincrona.
- È possibile ottenere il risultato di singoli metodi asincroni con il metodo GetAsyncResult. Quando si utilizza GetAsyncResult per eseguire una query su un'operazione completata, il sistema restituisce il risultato e rimuove automaticamente il risultato dal sistema. Quando si utilizza GetAsyncResult per eseguire query su un'operazione incompleta, il sistema restituisce il risultato ma non lo elimina.
- È possibile ottenere lo stato e i risultati di tutti i metodi asincroni in esecuzione o completati utilizzando il metodo ListAsyncResults. In questo caso, il sistema non elimina i risultati delle operazioni completate.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Attributi

Molte delle richieste e delle risposte API utilizzano oggetti e tipi semplici. Gli oggetti sono un insieme di coppie chiave-valore, in cui il valore è un tipo semplice o forse un altro oggetto. Gli attributi sono coppie nome-valore personalizzate che possono essere impostate dall'utente negli oggetti JSON. Alcuni metodi consentono di aggiungere

attributi durante la creazione o la modifica di oggetti.

Esiste un limite di 1000 byte per gli oggetti attributo codificati.

Membro dell'oggetto

Questo oggetto contiene il seguente membro:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON

Esempio di richiesta

Nell'esempio di richiesta riportato di seguito viene utilizzato il metodo AddClusterAdmin:

```
{
   "method": "AddClusterAdmin",
   "params": {
      "username": "joeadmin",
      "password": "68!5Aru268)$",
      "access": [
         "volume",
         "reporting"
      ],
      "attributes": {
         "name1": "value1",
         "name2": "value2",
         "name3": "value3"
      }
   }
}
```

Oggetti comuni

L'API del software Element utilizza oggetti JSON per rappresentare concetti di dati organizzati. Molti di questi metodi API utilizzano questi oggetti per l'input e l'output dei dati. Questa sezione descrive questi oggetti comunemente utilizzati; gli oggetti utilizzati solo all'interno di un singolo metodo sono documentati con tale metodo invece che in questa sezione.

- account
- AuthSessionInfo
- BulkVolumeJob
- binding (volumi virtuali)

- CertificateDettagli
- cluster
- ClusterAdmin
- Capacità del clusterCapacity
- Clusterconfig
- ClusterInfo
- ClusterPair
- ClusterStats
- Struttura del clusterStructure
- disco
- DriveStats
- errore
- evento
- guasto
- FiberChannelPort
- FipsErrorNodeReport
- FipsNodeReport
- FipsReport
- GroupSnapshot
- HardwareInfo
- host (volumi virtuali)
- IdpConfigInfo
- iniziatore
- KeyProviderKmip
- KeyServerKmip
- LdapConfiguration
- Server di loggingServer
- rete (interfacce collegate)
- rete (tutte le interfacce)
- Rete (interfacce Ethernet)
- rete (interfacce locali)
- Rete (SNMP)
- NetworkInterface
- nodo
- NodeProtectionDomini
- NodeStats
- OntapVersionInfo

- PendingActiveNode
- PendingNode
- Protection Domain (dominio di protezione)
- ProtectionDomainLevel
- ProtectionDomainResiliency
- ProtectionDomainTolerance
- ProtectionSchemeResiliency
- ProtectionSchemeTolerance
- ProtocolEndpoint
- QoS
- QoSPolicy
- RemoteClusterSnapshotStatus
- pianificazione
- Sessione (Fibre Channel)
- Sessione (iSCSI)
- SnapMirrorAggregate
- SnapMirrorClusterIdentity
- SnapMirrorEndpoint
- SnapMirrorJobScheduleCronInfo
- SnapMirrorLunInfo
- SnapMirrorNetworkInterface
- SnapMirrorNode
- SnapMirrorPolicy
- SnapMirrorPolicyRule
- SnapMirrorRelationship
- SnapMirrorVolume
- SnapMirrorVolumeInfo
- SnapMirrorVserver
- SnapMirrorVserverAggregateInfo
- snapshot
- SnmpTrapRecipient
- StorageContainer
- SyncJob
- task (volumi virtuali)
- UsmUser
- VirtualNetwork
- VirtualVolume

- volume
- VolumeAccessGroup
- VolumePair
- VolumeStats

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

account

L'oggetto account contiene informazioni su un account. Questo oggetto include solo informazioni "configurate" sull'account e non informazioni sull'utilizzo o sul runtime.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID account	L'ID account univoco per l'account.	intero
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
EnableChap	Specifica se le credenziali dell'account CHAP possono essere utilizzate da un iniziatore per accedere ai volumi.	booleano
InitatorSecret	Il segreto CHAP iniziatore.	stringa
stato	Lo stato corrente dell'account. Valori possibili: • Attivo: Un account attivo. • Locked (bloccato): Un account bloccato. • Rimosso: Un account che è stato eliminato e rimosso.	stringa
StorageContainerID	ID univoco del container di storage del volume virtuale associato a questo account.	UUID
TargetSecret	Il segreto CHAP di destinazione.	stringa

Nome	Descrizione	Tipo
nome utente	Il nome utente dell'account.	stringa
volumi	Un elenco di ID volume per i volumi di proprietà di questo account.	array intero

Trova ulteriori informazioni

- AddAccount
- GetAccountByID
- GetAccountByName
- ListAccounts

AuthSessionInfo

L'oggetto authSessionInfo contiene informazioni su una sessione auth.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AccessGroupList	Elenco dei gruppi di accesso per l'utente.	array di stringhe
AuthMethod	Il tipo di autorizzazione di cui dispone l'utente amministratore del cluster. Valori possibili: • LDAP - autenticato tramite LDAP. • Cluster - autenticato tramite un nome utente e una password memorizzati nel database del cluster. • IDP - autenticato tramite un provider di identità di terze parti.	stringa

Nome	Descrizione	Tipo
ClusterAdminID	Elenco degli AdminID del cluster associati a questa sessione. Per le sessioni relative a LDAP o a un provider di identità di terze parti (IdP), si tratta di un elenco aggregato di Cluster AdminID corrispondenti associati a questa sessione.	array intero
FinalTimeout	Ora in cui la sessione non è valida. Questa opzione viene impostata quando la sessione viene creata e non può essere modificata.	stringa
IdpConfigVersion	Versione della configurazione IDP al momento della creazione della sessione.	intero
LastAccessTimeout	Tempo in cui la sessione diventa non valida a causa di inattività.viene impostato su un nuovo valore quando si accede alla sessione per l'utilizzo, fino al momento in cui la sessione diventa non valida a causa del raggiungimento di finalTimeout.	stringa
SessionCreationTime	Ora in cui viene creata la sessione.	stringa
ID SessionID	UUID per questa sessione.	UUID
nome utente	Nome utente associato a questa sessione. Per le sessioni relative a LDAP, questo sarà il DN LDAP dell'utente. Per le sessioni correlate a un IdP di terze parti, si tratta di una coppia nome-valore arbitraria che verrà utilizzata per le operazioni di controllo all'interno della sessione. Non corrisponde necessariamente al nome dell'amministratore del cluster sul cluster. Ad esempio, un ID SAML Subject NameID, ma questo sarà dettato dalla configurazione di IdP e dal contenuto risultante dell'asserzione SAML.	stringa

BulkVolumeJob

L'oggetto bulkVolumeJob contiene informazioni sulle operazioni di lettura o scrittura di volumi in blocco, come la clonazione o la creazione di snapshot.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Attributo JSON del processo di volume in blocco.	Oggetto JSON
BulkVolumeID	L'ID del processo del volume in blocco interno.	intero
CreateTime	Data e ora creata per il job di volume in blocco in formato UTC+0.	Stringa di dati ISO 8601
SedelapTime	Il numero di secondi dall'inizio del lavoro.	stringa
formato	Il formato dell'operazione del volume in blocco. Valori possibili: • nativo • non compresso	stringa
chiave	Chiave univoca creata dalla sessione del volume in blocco.	stringa
PercentComplete	La percentuale di completamento riportata dall'operazione.	intero
Tempo residuo	Il tempo rimanente stimato in secondi.	intero
SrcVolumeID	L'ID del volume di origine.	intero
stato	Lo stato dell'operazione. Valori possibili: • preparazione in corso • in esecuzione • completo • non riuscito	stringa

Nome	Descrizione	Tipo
script	Il nome dello script, se fornito.	stringa
SnapshotID	L'ID dello snapshot se uno snapshot si trova nell'origine del processo di volume in blocco.	intero
tipo	Il tipo di operazione in blocco. Valori possibili: • leggi • di scrittura	stringa

binding (volumi virtuali)

L'oggetto binding contiene informazioni sull'associazione per un volume virtuale. È possibile recuperare un elenco di queste informazioni per tutti i volumi virtuali utilizzando `ListVirtualVolumeBindings` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtocolEndpointID	ID univoco dell'endpoint del protocollo.	UUID
ProtocolEndpointInBandID	L'ID scsiNAADeviceID dell'endpoint del protocollo.	stringa
ProtocolEndpointType	Il tipo di endpoint del protocollo. SCSI è l'unico valore restituito per il tipo di endpoint del protocollo.	stringa
VirtualVolumeBindingID	ID univoco dell'oggetto di binding del volume virtuale.	intero
VirtualVolumeHostID	L'ID univoco dell'host del volume virtuale.	UUID
VirtualVolumeID	L'ID univoco del volume virtuale.	UUID
VirtualVolumeSecondaryID	L'ID secondario del volume virtuale.	stringa

Trova ulteriori informazioni

- ListVirtualVolumeBindings
- ProtocolEndpoint

CertificateDettagli

L'oggetto certificateDetails contiene le informazioni decodificate su un certificato di sicurezza.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
emittente	Il nome dell'emittente.	stringa
modulo	Modulo della chiave pubblica.	stringa
NotAfter	La data di scadenza del certificato.	Stringa ISO 8601
Nota prima	La data di inizio del certificato.	Stringa ISO 8601
seriale	Il numero di serie del certificato.	stringa
Sha1Stampa di impronte digitali	Il digest della versione CODIFICATA DAL DER del certificato.	stringa
soggetto	Il nome del soggetto.	stringa

cluster

L'oggetto cluster contiene informazioni che il nodo utilizza per comunicare con il cluster. È possibile recuperare queste informazioni con il metodo API GetClusterConfig.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
cipi	Interfaccia di rete utilizzata per la comunicazione del cluster.	stringa
cluster	Nome cluster univoco.	stringa

Nome	Descrizione	Tipo
EncryptionCapable	Indica se il nodo supporta la crittografia del disco.	booleano
ensemble	I nodi che partecipano al cluster.	array di stringhe
FipsDriveConfiguration	Indica se il nodo supporta dischi certificati FIPS 140-2.	booleano
mipi	Interfaccia di rete utilizzata per la gestione dei nodi.	stringa
nome	Il nome del cluster.	stringa
ID NodeID	L'ID del nodo nel cluster.	stringa
PendingNodeID	L'ID del nodo in sospeso nel cluster.	intero
ruolo	Identifica il ruolo del nodo.	intero
sipi	Interfaccia di rete utilizzata per il traffico di storage.	stringa
stato	Lo stato corrente del nodo. Valori possibili: • Disponibile: Il nodo non è stato configurato con un nome di cluster. • In sospeso: Il nodo è in sospeso per uno specifico cluster denominato e può essere aggiunto. • Attivo: Il nodo è un membro attivo di un cluster e non può essere aggiunto a un altro cluster. • PendingActive (PendingActive): Il nodo viene attualmente restituito all'immagine software di fabbrica e non è ancora un membro attivo di un cluster. Al termine, passa allo stato attivo.	stringa
versione	La versione del software in esecuzione sul nodo.	stringa

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati o meno in ogni stato di nodo possibile.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
cipi	No	No	No
cluster	Sì	Sì	No
EncryptionCapable	No	No	No
ensemble	No	No	No
mipi	Sì	Sì	No
nome	Sì	Sì	Sì
ID NodeID	No	No	No
PendingNodeID	No	No	No
ruolo	No	No	No
sipi	No	No	No
stato	No	No	No
versione	No	No	No

Trova ulteriori informazioni

GetClusterConfig

ClusterAdmin

L'oggetto clusterAdmin contiene informazioni sull'utente corrente dell'amministratore del cluster. È possibile recuperare le informazioni dell'utente amministratore con il metodo API GetCurrentClusterAdmin.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	I metodi che l'amministratore del cluster può utilizzare.	array di stringhe
AuthMethod	Il tipo di autorizzazione di cui dispone l'utente amministratore del cluster. Valori possibili: • LDAP • Cluster • Locale	stringa
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
ID clusterAdminID	L'ID dell'amministratore del cluster per questo utente amministratore del cluster.	intero
nome utente	Nome utente per questo amministratore del cluster.	stringa

Trova ulteriori informazioni

GetCurrentClusterAdmin

Capacità del clusterCapacity

L'oggetto clusterCapacity contiene misurazioni di capacità di alto livello per il cluster. È possibile ottenere informazioni sulla capacità del cluster con il metodo API GetClusterCapacity. Le misurazioni dello spazio nei membri dell'oggetto vengono calcolate in byte.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ActiveBlockSpace	La quantità di spazio sui dischi a blocchi. Sono incluse informazioni aggiuntive, come ad esempio le voci di metadati e lo spazio che è possibile ripulire.	intero
ActiveSessions	Il numero di sessioni iSCSI attive che comunicano con il cluster.	intero

Nome	Descrizione	Tipo
AverageIOPS	IOPS medi per il cluster a partire dalla mezzanotte UTC (Coordinated Universal Time).	intero
ClusterRecentIOSize	La dimensione media degli IOPS per tutti i volumi nel cluster.	intero
CurrentIOPS	IOPS medi per tutti i volumi nel cluster negli ultimi 5 secondi.	intero
MaxIOPS	La capacità IOPS massima stimata del cluster corrente.	intero
MaxOverProvisionableSpace	La quantità massima di spazio disponibile per il provisioning. Si tratta di un valore calcolato. Non è possibile creare nuovi volumi se lo spazio attualmente fornito e le nuove dimensioni del volume superano questo numero. Il valore viene calcolato come segue: `maxOverProvisionableSpace = maxProvisionedSpace * maxMetadataOverProvisionFactor`	intero
MaxProvisionedSpace	La quantità totale di spazio disponibile per il provisioning se tutti i volumi sono riempiti al 100% (senza metadati con thin provisioning).	intero
MaxUsedMetadataSpace	Il numero di byte sui dischi di volume utilizzati per memorizzare i metadati.	intero
MaxUsedSpace	La quantità totale di spazio su tutti i dischi a blocchi attivi.	intero
Non ZeroBlock	Il numero totale di blocchi 4KiB che contengono dati dopo il completamento dell'ultima operazione di garbage collection.	intero
PeakActiveSessions	Il numero massimo di connessioni iSCSI dalla mezzanotte UTC.	intero

Nome	Descrizione	Tipo
PeakIOPS	Il valore più alto per i IOPS corrente a partire dalla mezzanotte UTC.	intero
Provisioning di spazio	La quantità totale di spazio fornito in tutti i volumi del cluster.	intero
data e ora	La data e l'ora, in formato UTC+0, in cui è stato prelevato questo campione di capacità del cluster.	Stringa ISO 8601
TotalOps	Il numero totale di operazioni di i/o eseguite durante l'intero ciclo di vita del cluster.	intero
UniqueBlocks	Il numero totale di blocchi memorizzati sui dischi a blocchi. Il valore include i blocchi replicati.	intero
UniqueBlocksUsedSpace	La quantità totale di dati che uniqueBlock prende sui dischi a blocchi. Consultare il metodo GetclusterCapacity per informazioni su come questo numero si riferisce al valore uniqueBlocks.	intero
UsedMetadataSpace	Il numero totale di byte sui dischi di volume utilizzati per memorizzare i metadati.	intero
UsedMetadataSpaceInSnapshot	Il numero di byte sui dischi di volume utilizzati per memorizzare dati univoci negli snapshot. Questo numero fornisce una stima della quantità di spazio di metadati che verrebbe recuperata eliminando tutte le snapshot nel sistema.	intero
UsedSpace	La quantità totale di spazio utilizzata da tutti i dischi a blocchi nel sistema.	intero
Zero-blocks	Il numero totale di blocchi 4KiB vuoti senza dati dopo il completamento dell'ultimo round dell'operazione di garbage collection.	intero

Trova ulteriori informazioni

GetClusterCapacity

Clusterconfig

L'oggetto clusterconfig restituisce le informazioni utilizzate dal nodo per comunicare con il cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
cipi	Interfaccia di rete utilizzata per la comunicazione del cluster.	stringa
cluster	Nome univoco del cluster.	stringa
EncryptionCapable	Specifica se il nodo supporta la crittografia.	booleano
ensemble	Nodi che partecipano al cluster.	array di stringhe
FipsDriveConfiguration	Specifica se il nodo supporta dischi certificati FIPS 140-2.	booleano
HasLocalAdmin	Specifica se il cluster dispone di un amministratore locale.	booleano
mipi	Interfaccia di rete utilizzata per la gestione dei nodi.	stringa
nome	Identificatore univoco del cluster.	stringa
ID NodeID	Identificatore univoco del nodo.	intero
PendingNodeID	Identificatore univoco del nodo in sospeso.	intero
ruolo	Identifica il ruolo del nodo.	stringa
sipi	Interfaccia di rete utilizzata per lo storage.	stringa
stato	Indica lo stato del nodo.	stringa

Nome	Descrizione	Tipo
versione	Indica la versione del nodo.	stringa

ClusterInfo

L'oggetto clusterInfo contiene informazioni che il nodo utilizza per comunicare con il cluster. È possibile ottenere queste informazioni con il metodo API GetClusterInfo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
DefaultProtectionScheme	Lo schema di protezione utilizzato per impostazione predefinita per i nuovi volumi, a meno che non venga fornito uno schema di protezione con CreateVolume chiamata al metodo. Questo schema di protezione deve sempre essere nell'insieme di schemi di protezione abilitati.	stringa
EnabledProtectionSchemes	Un elenco di tutti gli schemi di protezione attivati su questo cluster di storage.	array di stringhe
EncryptionAtRestState	Lo stato della funzione crittografia a riposo. Valori possibili: • Abilitazione: La crittografia a riposo è attivata. • Enabled (attivato): La crittografia a riposo è attivata. • Disattivazione: La crittografia a riposo viene disattivata. • Disabled (disattivata): La crittografia a riposo è disattivata.	stringa
ensemble	I nodi che partecipano al cluster.	array di stringhe

Nome	Descrizione	Tipo
mvip	L'indirizzo IP mobile (virtuale) per il cluster sulla rete di gestione.	stringa
MvipInterface	L'interfaccia fisica associata all'indirizzo MVIP.	stringa
MvipNodeID	Nodo che contiene l'indirizzo MVIP master.	intero
MvipVlanTag	L'identificatore VLAN per l'indirizzo MVIP.	stringa
nome	Il nome univoco del cluster.	stringa
RepCount	Il numero di repliche di ciascun dato da memorizzare nel cluster. Il valore valido è "2".	intero
SoftwareEncryptionAtRestState	Crittografia basata su software in stato di riposo.	stringa
SupportedProtectionSchemes	Elenco di tutti gli schemi di protezione supportati da questo cluster di storage.	array di stringhe
svip	L'indirizzo IP mobile (virtuale) per il cluster sulla rete di storage (iSCSI).	stringa
SvipInterface	L'interfaccia fisica associata all'indirizzo SVIP master.	stringa
SvipNodeID	Il nodo che contiene l'indirizzo SVIP master.	intero
SvipVlanTag	L'identificatore VLAN per l'indirizzo SVIP master.	stringa
ID univoco	L'ID univoco del cluster.	stringa
uuid	Identificatore univoco del cluster.	UUID

Trova ulteriori informazioni

- "GetClusterInfo"
- "Documentazione software SolidFire ed Element"

- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

ClusterPair

L'oggetto clusterPair contiene informazioni sui cluster associati al cluster locale. È possibile recuperare un elenco di oggetti ClusterPair per il cluster locale con il metodo ListClusterPairs.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
Nome cluster	Il nome dell'altro cluster della coppia.	stringa
ID PairID del clusterPairID	Un ID univoco assegnato a ciascun cluster della coppia.	intero
ClusterPairUID	Identificativo universalmente univoco per la coppia di cluster.	stringa
UUID	Identificatore univoco del cluster remoto nella coppia di cluster.	intero
latenza	La latenza, in millisecondi, tra i cluster.	intero
mvip	L'indirizzo IP della connessione di gestione per i cluster accoppiati.	stringa
stato	Lo stato della connessione tra i cluster accoppiati. Valori possibili: • Non configurato • Connesso • Configurato in modo errato • Disconnesso	stringa
versione	La versione dell'elemento dell'altro cluster della coppia.	stringa

Trova ulteriori informazioni

ListClusterPairs

ClusterStats

L'oggetto clusterStats contiene dati statistici per un cluster. Molte delle statistiche relative al volume contenute nell'oggetto vengono mediate per tutti i volumi nel cluster. È possibile utilizzare il metodo GetClusterStats per recuperare queste informazioni per un cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Calcolo	Tipo
AttualIOPS	IOPS effettivi correnti per l'intero cluster negli ultimi 500 millisecondi.	Point-in-time	intero
AverageIOPSize	Dimensione media in byte di i/o recente nel cluster negli ultimi 500 millisecondi.	Point-in-time	intero
ClientQueueDepth	Il numero di operazioni di lettura e scrittura in sospeso nel cluster.	N/A.	intero
ClusterUtilization	La percentuale di IOPS massimi del cluster attualmente in uso. Viene calcolato come clusterUtilization = normalizzatoIOPS / maxIOPS (da GetClusterCapacity).	N/A.	fluttuare
LatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni su un cluster negli ultimi 500 millisecondi.	Point-in-time	intero
NormalizzatoIOPS	Numero medio di IOPS per l'intero cluster negli ultimi 500 millisecondi.	Point-in-time	intero
ReadByte	I byte cumulativi totali letti dal cluster dalla creazione del cluster.	In aumento monotono	intero

Nome	Descrizione	Calcolo	Tipo
ReadBytesLastSample	Il numero totale di byte letti dal cluster durante l'ultimo periodo di esempio.	Point-in-time	intero
ReadLatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni di lettura al cluster negli ultimi 500 millisecondi.	Point-in-time	intero
ReadLatencyUSecTotal	Il tempo totale impiegato per le operazioni di lettura dalla creazione del cluster.	In aumento monotono	intero
ReadOps	Operazioni di lettura cumulative totali per il cluster dalla creazione del cluster.	In aumento monotono	intero
ReadOpsLastSample	Il numero totale di operazioni di lettura durante l'ultimo periodo di campionamento.	Point-in-time	intero
SamplePeriodMsec	La durata del periodo di campionamento, in millisecondi.	N/A.	intero
ServiceConteggio	Il numero di servizi in esecuzione nel cluster. Se uguale al serviceTotal, indica che sono state raccolte statistiche valide da tutti i nodi.	Point-in-time	intero
ServiceTotal	Il numero totale di servizi previsti in esecuzione nel cluster.	N/A.	intero
data e ora	L'ora corrente nel formato UTC+0.	N/A.	Stringa di dati ISO 8601
UnalignedReads	Operazioni di lettura cumulative non allineate per un cluster dalla creazione del cluster.	In aumento monotono	intero

Nome	Descrizione	Calcolo	Tipo
UnalignedWrites	Operazioni di scrittura cumulative non allineate su un cluster dopo la creazione del cluster.	In aumento monotono	intero
WriteByte	I byte cumulativi totali scritti nel cluster dalla creazione del cluster.	In aumento monotono	intero
WriteBytesLastSample	Il numero totale di byte scritti nel cluster durante l'ultimo periodo di esempio.	In aumento monotono	intero
ScriveLatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni di scrittura su un cluster negli ultimi 500 millisecondi.	Point-in-time	intero
SwriteLatencyUSecTotal	Il tempo totale impiegato per le operazioni di scrittura dalla creazione del cluster.	In aumento monotono	intero
SwriteOps	Operazioni di scrittura cumulative totali nel cluster dalla creazione del cluster.	In aumento monotono	intero
SwriteOpsLastSample	Il numero totale di operazioni di scrittura durante l'ultimo periodo di esempio.	Point-in-time	intero

Trova ulteriori informazioni

GetClusterStats

Struttura del clusterStructure

L'oggetto ClusterStructure contiene le informazioni di backup della configurazione del cluster create dal metodo GetClusterStructure. È possibile utilizzare il metodo SetClusterStructure per ripristinare queste informazioni in un cluster di storage che si sta ricostruendo.

Membri dell'oggetto

Questo oggetto contiene le informazioni di ritorno combinate dei seguenti metodi:

- GetClusterInfo
- ListAccounts
- ListInitiator
- ListVolumes (Con inclusiVirtualVolumes=false)
- ListVolumeAccessGroups
- ListStorageContainers
- ListQoSPolicies
- GetSnmpInfo
- GetNtpInfo
- ListVirtualNetworks
- ListClusterAdmins
- Elenchi
- ListSnapMirrorEndpoint
- GetFeatureStatus
- GetLdapConfiguration
- GetRemoteLoggingHost
- GetDefaultQoS
- GetVolumeAccessGroupLunAssignments

Trova ulteriori informazioni

- GetClusterStructure
- SetClusterStructure

disco

L'oggetto Drive contiene informazioni sui singoli dischi nei nodi attivi del cluster. Questo oggetto contiene informazioni dettagliate sulle unità aggiunte come metadati di volume o unità a blocchi, nonché sulle unità non ancora aggiunte e disponibili. È possibile recuperare queste informazioni con `ListDrives` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON. Questo oggetto è sempre nullo e non è modificabile.	Oggetto JSON
capacità	La capacità totale del disco, in byte.	intero
ChassisSlot	Per le piattaforme HCI, questo valore corrisponde alla lettera del nodo e al numero di slot nello chassis del server in cui si trova l'unità. Per le piattaforme di storage, il numero di slot è una rappresentazione stringa del numero intero "slot".	stringa
DriveFailureDetail	Se lo stato di un disco è "Failed" (guasto), questo campo fornisce ulteriori dettagli sul motivo per cui il disco è stato contrassegnato come guasto.	stringa
ID del driver	L'ID di questo disco.	intero
DriveSecurityFaultReason	Se l'attivazione o la disattivazione della protezione del disco non è riuscita, il motivo per cui si è verificato un errore. Se il valore è "nessuno", non si è verificato alcun errore.	stringa
KeyID (ID chiave)	L'ID chiave utilizzato dal provider di chiavi per acquisire la chiave di autenticazione per sbloccare il disco.	UUID
KeyProviderID	Identifica il provider della chiave di autenticazione per lo sblocco del disco.	intero
ID NodeID	L'ID del nodo che contiene questo disco.	intero
SegmentFileSize	La dimensione del file di segmento del disco, in byte.	intero

Nome	Descrizione	Tipo
seriale	Il numero di serie del disco.	stringa
slot	Il numero di slot nello chassis del server in cui si trova l'unità, o -1 se si utilizza un dispositivo SATADimm per l'unità di metadati interna.	intero
stato	Lo stato del disco. Valori possibili: • Disponibile: Un disco disponibile. • Active (attivo): Un disco attivo. • Cancellazione: È in corso la cancellazione sicura di un disco. Tutti i dati presenti su quel disco vengono rimossi in modo permanente. • Failed (guasto): Un disco guasto. Tutti i dati precedentemente presenti sul disco sono stati migrati su altri dischi del cluster. • Rimozione: È in corso la rimozione di un disco. Tutti i dati precedentemente presenti sul disco vengono migrati su altri dischi del cluster.	stringa
tipo	Il tipo di disco. Valori possibili: • Volume: Memorizza i metadati del volume. • Block (blocco): Memorizza i dati del blocco. • Sconosciuto: Il tipo di disco non è ancora attivo e deve essere ancora determinato.	stringa
UsableCapacity	La capacità utilizzabile del disco, in byte.	intero

Trova ulteriori informazioni

ListDrive

DriveStats

L'oggetto driveStats contiene misurazioni di attività di alto livello per un singolo disco. È possibile recuperare le informazioni di misurazione con il metodo API `GetDriveStats`.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ActiveSessions	Numero di sessioni iSCSI che attualmente utilizzano questo disco (presente solo per i dischi metadati).	intero
ID del driver	ID univoco del disco nel cluster.	intero
FailedDieCount	Numero di elementi hardware del disco guasti.	intero
IosInProgress	Il numero di i/o dell'unità in corso.	intero
LifeRemainingPercent	Indicatore di usura dei supporti dell'unità.	intero
LifetimeReadBytes	Byte totali letti da questo disco per la durata del disco.	intero
Lifetime WriteBytes	Byte totali scritti su questo disco per tutta la durata del disco.	intero
PowerOnHours	Numero di ore di accensione del disco.	intero
letture	Il numero di chiamate Read() al secondo per questa unità.	intero
ReadByte	Byte totali letti dal disco a causa delle operazioni del client.	intero
ReadsCombined	Il numero di chiamate Read() a settori adiacenti che potrebbero essere combinati in una lettura più grande.	intero
ReadMsec	Il numero di millisecondi trascorsi per la lettura.	intero

Nome	Descrizione	Tipo
ReadOps	Operazioni di lettura totali sul disco dovute alle operazioni del client.	intero
RiallocatedSettori	Numero di settori danneggiati sostituiti in questo disco.	intero
ReserveCapacityPercent	La capacità di riserva disponibile del disco.	intero
data e ora	L'ora corrente nel formato UTC+0.	Stringa di dati ISO 8601
Capacità totale	Capacità totale del disco, in byte.	intero
Uncorrectable Errors (errori non correggibili)	Il valore degli errori non correggibili riportato dal sistema DI monitoraggio Smart (Self-Monitoring, Analysis and Reporting Technology) nel disco.	intero
UsedCapacity	Capacità utilizzata del disco, in byte.	intero
UsedMemory	Quantità di memoria attualmente utilizzata dal nodo che ospita questo disco.	intero
scritture	Il numero di chiamate write() al secondo su questa unità.	intero
WriteByte	Byte totali scritti sul disco a causa dell'attività del client.	intero
Scritti Combined	Il numero di chiamate write() a settori adiacenti che potrebbero essere combinate in una scrittura più grande.	intero
WriteMsec	Il numero di millisecondi trascorsi per la scrittura.	intero
SwriteOps	Operazioni totali di scrittura sul disco a causa dell'attività del client.	intero

Trova ulteriori informazioni

GetDriveStats

errore

L'oggetto error contiene un codice di errore e un messaggio se si verifica un errore durante una chiamata al metodo. Tutti gli errori generati dal sistema hanno un codice di errore 500.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
codice	Il codice numerico utilizzato per identificare l'errore. Tutti gli errori generati dal sistema restituiscono un codice 500.	intero
nome	Identificatore univoco dell'errore specifico che si è verificato. Ogni metodo restituisce un set documentato di errori, anche se si dovrebbe essere pronti a gestire anche gli errori non riconosciuti.	stringa
messaggio	Una descrizione dell'errore, eventualmente con ulteriori dettagli.	stringa

evento

L'oggetto Event contiene dettagli sugli eventi che si verificano durante una chiamata al metodo API o durante l'esecuzione di un'operazione da parte del sistema.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
dettagli	Informazioni aggiuntive sull'evento.	Oggetto JSON
ID del driver	L'ID del disco che segnala il guasto. 0 se non applicabile.	intero
ID del driver	Un elenco degli ID dei dischi che segnalano il guasto. Un elenco vuoto, se non applicabile.	array intero
ID dell'EventId	ID univoco associato a ciascun evento.	intero

Nome	Descrizione	Tipo
EventInfoType	Il tipo di guasto.	stringa
messaggio	Una descrizione stringa dell'evento che si è verificato.	stringa
ID NodeID	Il NodeID del nodo che segnala l'errore. 0 se non applicabile.	intero
ID servizio	Il ServiceId del servizio che segnala l'errore. 0 se non applicabile.	intero
severità	Severità che l'evento sta segnalando.	intero
TimeOfPublish	L'ora in cui il registro eventi del cluster ha ricevuto l'evento, in formato UTC+0.	Stringa di dati ISO 8601
Report TimeOf	L'ora in cui si è verificato l'evento nel cluster, in formato UTC+0.	Stringa di dati ISO 8601

Nota: potrebbe esserci una leggera differenza tra timeOfReport e timeOfPublish se l'evento si è verificato e non è stato possibile pubblicarlo immediatamente.

Tipi di evento

L'elenco seguente descrive i possibili tipi di evento che il membro eventInfoType può contenere:

- ApiEvent: Eventi avviati attraverso l'API o l'interfaccia utente Web che modificano le impostazioni.
- BinAssignmentsEvent: Eventi correlati all'assegnazione di dati a container interni.
- BinSyncEvent: Eventi correlati a una riassegnazione di dati tra servizi a blocchi.
- BsCheckEvent: Eventi correlati ai controlli del servizio di blocco.
- BsKillEvent: Eventi correlati alle interruzioni del servizio di blocco.
- BulkOpEvent: Eventi che operano su un intero volume, ad esempio backup, ripristino, snapshot o clone di un volume.
- CloneEvent: Eventi correlati alla clonazione del volume.
- ClusterMasterEvent: Eventi di modifica della configurazione del cluster come l'aggiunta o la rimozione di nodi.
- DataEvent: Eventi relativi alla lettura e alla scrittura dei dati.
- DbEvent: Eventi correlati al database dei nodi ensemble.
- DriveEvent: Eventi relativi alle operazioni del disco.
- EncryptionAtRestEvent: Eventi correlati alla crittografia dei dati memorizzati.

- EnsembleEvent: Gli eventi relativi alla dimensione dell'insieme aumentano o diminuiscono.
- FiberChannelEvent: Eventi correlati alla configurazione o alle connessioni dei nodi Fibre Channel.
- GcEvent: Eventi correlati alla garbage collection. Questi processi vengono eseguiti ogni 60 minuti per recuperare lo storage su dischi a blocchi.
- IeEvent: Eventi correlati a errori interni del sistema.
- InstallEvent (evento di installazione): Informazioni relative all'installazione automatica del software sui nodi di storage in sospeso.
- ISCSIEvent: Eventi correlati a problemi di connessione o configurazione iSCSI.
- LimitEvent: Eventi correlati al numero di volumi o volumi virtuali in un account o nel cluster che si avvicina al numero massimo consentito.
- NetworkEvent: Eventi relativi alla rete virtuale.
- PlatformHardwareEvent: Eventi relativi a problemi rilevati sui dispositivi hardware.
- RemoteClusterEvent: Eventi correlati all'associazione remota del cluster.
- SchedulerEvent: Eventi correlati alle snapshot pianificate.
- ServiceEvent: Eventi correlati allo stato del servizio di sistema.
- StatEvent: Eventi correlati alle statistiche di sistema.
- SliceEvent: Eventi relativi allo storage dei metadati.
- SnmpTrapEvent: Eventi correlati ai trap SNMP.
- TsEvent: Eventi del servizio di trasporto del sistema.
- Exception: Eventi correlati a errori imprevisti.
- VasaProviderEvent: Eventi correlati a un provider VASA VMware.

Trova ulteriori informazioni

ListEvents

guasto

L'oggetto fault contiene informazioni sugli errori rilevati nel cluster. Il `ListClusterFaults` il metodo restituisce informazioni sugli errori del cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID clusterFaultID	L'ID univoco associato a ciascun guasto del cluster.	intero
codice	Il codice di guasto per il guasto specifico rilevato. Per ulteriori dettagli, vedere Cluster Fault Codes (codici di errore del cluster).	stringa

Nome	Descrizione	Tipo
dati	Ulteriori informazioni specifiche sui guasti.	Oggetto JSON
data	L'ora corrente nel formato UTC+0.	Stringa ISO 8601
dettagli	La descrizione del guasto con ulteriori dettagli.	stringa
ID del driver	Il primo ID del disco nell'elenco driveID. Se l'elenco driveID è vuoto (il che significa che non sono stati restituiti guasti che riguardano i dischi), questo valore è 0.	intero
ID del driver	Un elenco di valori ID unità per le unità a cui si riferisce questo guasto. Incluso per i guasti relativi ai dischi. In caso contrario, si tratta di un array vuoto.	array intero
NodeHardwareFaultID	L'identificatore assegnato a un guasto hardware sul cluster.	intero
ID NodeID	L'ID del nodo a cui si riferisce questo guasto. Incluso per gli errori di nodo e disco, altrimenti impostato su 0.	intero
risolto	Stato risolto del guasto. Valori possibili: • Vero: Il guasto non viene più rilevato. • Falso: Il guasto è ancora presente.	booleano
ResolvedDate	La data e l'ora in cui il guasto è stato risolto.	Stringa ISO 8601
ID servizio	Il servizio associato al guasto. Questo valore è "0" (zero) se il guasto non è associato a un servizio.	intero

Nome	Descrizione	Tipo
severità	La gravità del guasto. Valori possibili: • Attenzione: Si tratta di un problema minore. Il cluster funziona e gli aggiornamenti sono consentiti a questo livello di gravità. • Errore: Un errore che generalmente non dovrebbe influire sul servizio (ad eccezione del possibile peggioramento delle performance o perdita di ha). Alcune funzioni potrebbero essere disattivate. • Critico: Un guasto grave che influisce sul servizio. Il sistema non è in grado di fornire richieste API o i/o client ed è a rischio di perdita di dati. • BestPractice: Guasti attivati da una configurazione di sistema non ottimale.	stringa
tipo	Il tipo di guasto. Valori possibili: • Nodo: Un guasto che interessa un intero nodo. • Drive (disco): Un guasto che interessa un singolo disco. • Cluster: Un errore che interessa l'intero cluster. • Service (Servizio): Un errore che interessa un servizio nel cluster. • Volume: Un errore che interessa un singolo volume.	stringa

Trova ulteriori informazioni

- ListClusterFaults
- "Codici di guasto del cluster"

FiberChannelPort

L'oggetto fiberChannelPort contiene informazioni sulle singole porte di un nodo o su un

intero nodo del cluster. È possibile recuperare queste informazioni utilizzando `ListNodeFibreChannelPortInfo` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
firmware	La versione del firmware installata sulla porta Fibre Channel.	intero
HbaPort	L'ID della porta HBA (host bus adapter).	intero
modello	Modello dell'HBA sulla porta.	stringa
NPortID	L'ID unico del nodo della porta.	stringa
PciSlot	Lo slot contenente la scheda PCI nello chassis del nodo Fibre Channel.	intero
seriale	Il numero di serie sulla porta Fibre Channel.	stringa
velocità	La velocità dell'HBA sulla porta.	stringa
stato	Valori possibili: • Sconosciuto • Non present • Online • Offline • Bloccato • Ignorato • Diagnostica • Collegamento • Errore • Loopback • Cancellato	stringa
SwitchWwn	Il nome universale della porta dello switch Fibre Channel.	stringa

Nome	Descrizione	Tipo
wwnn	World Wide Node Name del nodo HBA.	stringa
pn. wwn	World Wide Port Name assegnato alla porta fisica dell'HBA.	stringa

Trova ulteriori informazioni

ListNodeFibreChannelPortInfo

FipsErrorNodeReport

L'oggetto fipsErrorNodeReport contiene informazioni sugli errori per ciascun nodo che non risponde con informazioni sul supporto FIPS 140-2 quando si esegue una query con `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID NodeID	L'ID del nodo che non ha risposto.	intero
errore	Oggetto JSON contenente informazioni sugli errori.	Oggetto JSON

FipsNodeReport

L'oggetto fipsNodeReport contiene informazioni sul supporto FIPS 140-2 per un singolo nodo nel cluster di storage. È possibile recuperare queste informazioni utilizzando `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID NodeID	L'ID del nodo che riporta le informazioni.	intero

Nome	Descrizione	Tipo
FipsDrive	Se la crittografia del disco FIPS 140-2 è attivata o meno per questo nodo. Valori possibili: • None (Nessuno): Questo nodo non supporta la crittografia del disco FIPS. • Parziale: Il nodo è in grado di crittografare i dischi FIPS, ma non tutti i dischi presenti sono compatibili con FIPS. • Pronto: Il nodo è in grado di crittografare i dischi FIPS e tutti i dischi presenti sono dischi compatibili con FIPS oppure non sono presenti dischi.	FipsDrivesStatusType
HttpsEnabled (httpsEnabled	Se la crittografia HTTPS FIPS 140-2 è attivata o meno per questo nodo. Valori possibili: • vero: abilitato • falso: disattivato	booleano

FipsReport

L'oggetto fipsReport contiene informazioni sul supporto FIPS 140-2 per tutti i nodi nel cluster di storage. È possibile recuperare queste informazioni utilizzando `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
nodi	Un report sullo stato del supporto FIPS 140-2 per ciascun nodo del cluster di storage.	FipsNodeReport
ErrorNode	Informazioni sugli errori per ogni nodo che non ha risposto con lo stato di supporto FIPS 140-2.	FipsErrorNodeReport

GroupSnapshot

L'oggetto groupSnapshot contiene informazioni su uno snapshot per un gruppo di volumi.

È possibile utilizzare `ListGroupSnapshots` Metodo API per recuperare le informazioni di snapshot di gruppo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
CreateTime	Il giorno e l'ora formattati con UTC+0 in cui è stata creata la snapshot di gruppo.	Stringa di dati ISO 8601
EnableRemoteReplication	Identifica se lo snapshot è abilitato per la replica remota.	booleano
GroupSnapshotID	L'ID univoco dello snapshot di gruppo.	intero
GroupSnapshotUID	UUID dello snapshot di gruppo.	stringa
membri	Matrice di oggetti contenente informazioni su ciascun membro dello snapshot di gruppo.	snapshot array
nome	Il nome dello snapshot di gruppo o, se non ne è stata fornita alcuna, il giorno e l'ora formattati con UTC in cui lo snapshot è stato creato.	Stringa o stringa di dati ISO 8601
RemoteStatuses	Array contenente l'identificatore universale e lo stato di replica di ogni snapshot remoto sul cluster di destinazione, come visualizzato dal cluster di origine.	RemoteClusterSnapshotStatus array

Nome	Descrizione	Tipo
stato	Stato corrente dello snapshot. Valori possibili: • Sconosciuto: Si è verificato un errore durante l'ottenimento dello stato dello snapshot. • Preparazione: Questo snapshot è in fase di preparazione e non è ancora scrivibile. • RemoteSyncing: Questo snapshot viene replicato da un cluster remoto. • Fatto: Questo snapshot ha terminato la preparazione o la replica ed è ora utilizzabile. • Attivo: Questo snapshot è il ramo attivo. • Cloning (clonazione): Questo snapshot è coinvolto in un'operazione CopyVolume.	stringa

Trova ulteriori informazioni

ListGroupSnapshot

HardwareInfo

L'oggetto hardwareInfo contiene informazioni dettagliate sull'hardware e sullo stato di ciascun nodo del cluster. È possibile recuperare queste informazioni con `GetHardwareInfo` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
BoardSerial	Il numero di serie della scheda DMI.	stringa
autobus	Informazioni sul bus multimediale della scheda madre.	Oggetto JSON
ChassisSerial	Il numero di serie dello chassis.	stringa

Nome	Descrizione	Tipo
Hardware del drivehardware	Un elenco di informazioni per ciascun disco nel nodo.	Array di oggetti JSON
FiberChannelPorts	Un elenco di porte Fibre Channel sul nodo.	array intero
HardwareConfig	Informazioni sulla configurazione delle periferiche della scheda madre.	Oggetto JSON
KernelCrashDumpState	Configurazione del crash dump del kernel del sistema operativo.	stringa
memoria	Informazioni sull'hardware della memoria di sistema e del firmware.	Oggetto JSON
rete	Descrizioni dell'hardware di ciascuna delle interfacce di rete del nodo.	Oggetto JSON
NetworkInterfaces	Lo stato delle interfacce di rete del nodo.	Oggetto JSON
NodeSlot	Per le piattaforme HCI, la lettera corrispondente allo slot dello chassis in cui si trova questo nodo ("A", "B", "C" o "D"). Per le piattaforme storage, questo valore è nullo.	stringa
nvram	Statistiche NVRAM per il nodo.	Oggetto JSON
origine	Il vendor della scheda madre.	stringa
piattaforma	Una descrizione della piattaforma del telaio.	Oggetto JSON
seriale	Il numero di serie del prodotto.	stringa
storage	Informazioni sul controller dello storage.	Oggetto JSON
SystemMemory	Informazioni sull'utilizzo della memoria del sistema operativo e sulle prestazioni.	Oggetto JSON

Nome	Descrizione	Tipo
sistema	Il tipo di chassis del nodo.	Oggetto JSON
uuid	L'ID univoco del nodo.	UUID

Trova ulteriori informazioni

GetHardwareInfo

host (volumi virtuali)

L'oggetto host contiene informazioni su un host di volume virtuale. È possibile utilizzare `ListVirtualVolumeHosts` metodo per ottenere queste informazioni per tutti gli host di volumi virtuali.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
associazioni	Un elenco di oggetti che descrivono le associazioni per l'host del volume virtuale.	array intero
ID cluster	L'ID univoco del cluster a cui è associato l'host.	UUID
Indirizzo host	L'indirizzo IP o il nome DNS dell'host del volume virtuale.	stringa
InitatorNames	Un elenco di IQN iniziatori per l'host del volume virtuale.	array di stringhe
VirtualVolumeHostID	L'ID univoco di questo host volume virtuale.	UUID
VisibleProtocolEndpointID	Un elenco di ID degli endpoint del protocollo visibili su questo host.	Array UUID

Trova ulteriori informazioni

ListVirtualVolumeHost

IdpConfigInfo

L'oggetto idpConfigInfo contiene dettagli di configurazione e integrazione relativi a un

provider di identità (IdP) di terze parti.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attivato	Specifica se questa configurazione IdPdi terze parti è attivata.	booleano
ID configurazione idpID	UUID per la configurazione IdP di terze parti.	UUID
IdpMetadata	Metadati per dettagli di configurazione e integrazione per SAML 2.0 Single Sign-on.	stringa
Nome ID	Nome per il recupero del provider IdP per SAML 2.0 Single Sign-on.	stringa
ServiceProviderCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM da utilizzare per la comunicazione con questo IdP.	stringa
SpMetadataUrl	URL per il recupero dei metadati del service provider (SP) dal cluster da fornire all'IdP per stabilire una relazione di trust.	stringa

iniziatore

L'oggetto Initiator contiene informazioni su iSCSI o Fibre Channel Initiator. Un oggetto Initiator può contenere identificatori IQN o WWPN. È possibile utilizzare `ListInitiators` metodo per ottenere un elenco di tutti gli iniziatori noti nel sistema. Gli oggetti Initiator vengono utilizzati per configurare l'accesso SCSI Initiator a un set di volumi attraverso gruppi di accesso al volume. Un iniziatore può essere solo un membro di un gruppo di accesso a un volume alla volta. È possibile limitare l'accesso dell'iniziatore a una o più VLAN specificando uno o più virtualNetworkID utilizzando `CreateInitiators` e. `ModifyInitiators` metodi. Se non si specificano reti virtuali, l'iniziatore può accedere a tutte le reti.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
alias	Il nome descrittivo assegnato all'iniziatore, se presente.	stringa
attributi	Insieme di attributi JSON assegnati a questo iniziatore. Vuoto se non sono assegnati attributi.	Oggetto JSON
ChapNomeUtente	Il nome utente CHAP univoco per questo iniziatore.	stringa
InitatorID	Identificativo numerico dell'iniziatore.	intero
InitiatorName (Nome iniziatore	Nome dell'iniziatore, in formato IQN o WWPN.	stringa
InitatorSecret	Il segreto CHAP utilizzato per autenticare l'iniziatore.	stringa
RequireChap	True se è richiesto CHAP per questo iniziatore.	booleano
TargetSecret	Il segreto CHAP utilizzato per autenticare la destinazione (quando si utilizza l'autenticazione CHAP reciproca).	stringa
VirtualNetworkID	L'elenco degli identificatori di rete virtuale associati a questo iniziatore. Se vengono definite una o più reti, l'iniziatore potrà accedere solo alle reti virtuali specificate. Se non sono definite reti virtuali, l'iniziatore può accedere a tutte le reti.	intero
VolumeAccessGroups	Un elenco degli ID del gruppo di accesso al volume a cui appartiene l'iniziatore.	array intero

Trova ulteriori informazioni

ListInitiator

KeyProviderKmip

L'oggetto keyProviderKmip descrive un provider di chiavi KMIP (Key Management

Interoperability Protocol). Un provider di chiavi è sia un meccanismo che un percorso per recuperare le chiavi di autenticazione da utilizzare con le funzionalità del cluster, come la crittografia a riposo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
KeyProviderID	L'ID del provider della chiave KMIP. Si tratta di un valore univoco assegnato dal cluster durante la creazione del provider di chiavi che non può essere modificato.	intero
KeyProviderIsActive	True se il provider della chiave KMIP è attivo. Un provider viene considerato attivo se sono presenti chiavi in sospeso che sono state create ma non ancora eliminate e quindi si presume che siano ancora in uso.	booleano
KeyProviderName	Il nome del provider della chiave KMIP.	stringa
KeyServerID	ID del server delle chiavi associato a questo provider. Il server deve essere aggiunto prima che questo provider possa attivarsi. Impossibile rimuovere il server mentre questo provider è attivo. Per ciascun provider è supportato un solo ID server.	array intero
KmipCapabilities	Le funzionalità di questo provider di chiavi KMIP, tra cui dettagli sulla libreria sottostante, conformità FIPS, provider SSL, ecc.	stringa

KeyServerKmip

L'oggetto keyServerKmip descrive un server di chiavi KMIP (Key Management Interoperability Protocol), un percorso per recuperare le chiavi di autenticazione da utilizzare con le funzionalità del cluster, ad esempio Encryption at REST (crittografia a riposo).

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
KeyProviderID	Se il server delle chiavi KMIP è assegnato a un provider, questo membro contiene l'ID del provider delle chiavi KMIP a cui è assegnato. In caso contrario, questo membro è nullo.	intero
KeyServerID	L'ID del server chiavi KMIP. Si tratta di un valore univoco assegnato dal cluster durante la creazione del server delle chiavi. Questo valore non può essere modificato.	intero
KmipAssignedProviderIsActive	Se il server delle chiavi KMIP è assegnato a un provider (keyProviderID non è null), questo membro indica se il provider è attivo (fornendo le chiavi attualmente in uso). In caso contrario, questo membro è nullo.	booleano
KmipCaCertificate	Il certificato a chiave pubblica della CA principale del server di chiavi esterno. Viene utilizzato per verificare il certificato presentato dal server chiavi esterno nella comunicazione TLS. Per i cluster di server chiave in cui i singoli server utilizzano CA diverse, questo membro contiene una stringa concatenata dei certificati root di tutte le CA.	stringa
KmipClientCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM utilizzato dal client KMIP dello storage di elementi.	stringa
KmipKeyServerHostnames	I nomi host o gli indirizzi IP associati a questo server chiavi KMIP.	array di stringhe

Nome	Descrizione	Tipo
KmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa
KmipKeyServerPort	Il numero di porta associato al server delle chiavi KMIP (generalmente 5696).	intero

LdapConfiguration

L'oggetto ldapConfiguration contiene informazioni sulla configurazione LDAP nel sistema di storage. È possibile recuperare le informazioni LDAP con `GetLdapConfiguration` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AuthType	Identifica il metodo di autenticazione dell'utente da utilizzare. Valori possibili: • DirectBind • SearchAndBind	stringa
attivato	Indica se il sistema è configurato per LDAP. Valori possibili: • vero • falso	booleano
GroupSearchBaseDN	Il DN di base della struttura per avviare la ricerca di gruppo (il sistema eseguirà una ricerca sotto-struttura da qui).	stringa
GroupSearchCustomFilter	Il filtro di ricerca personalizzato utilizzato.	stringa

Nome	Descrizione	Tipo
GroupSearchType	Controlla il filtro di ricerca di gruppo predefinito utilizzato. Valori possibili: • NoGroups: Nessun supporto di gruppo. • ActiveDirectory: Appartenenza nidificata a tutti i gruppi ad di un utente. • MemberDN: Gruppi di stile MemberDN (livello singolo).	stringa
SearchBindDN	Un DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente (richiede l'accesso in lettura alla directory LDAP).	stringa
Server URI	Un elenco separato da virgole degli URI del server LDAP (ad esempio, `ldap://1.2.3.4` e. `ldaps://1.2.3.4:123`.)	stringa
UserDNTemplate	Stringa utilizzata per formare un DN utente completo.	stringa
UserSearchBaseDN	Il DN di base della struttura utilizzata per avviare la ricerca (esegue una ricerca sotto-struttura da qui).	stringa
UserSearchFilter	Il filtro LDAP utilizzato.	stringa

Trova ulteriori informazioni

GetLdapConfiguration

Server di loggingServer

L'oggetto loggingServer contiene informazioni sugli host di registrazione configurati per il cluster di storage. È possibile utilizzare `GetRemoteLoggingHosts` per determinare quali sono gli host di registrazione correnti e utilizzarli `SetRemoteLoggingHosts` per impostare l'elenco desiderato di host di registrazione correnti e nuovi.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
host	Indirizzo IP del server di log.	stringa
porta	Numero di porta utilizzato per comunicare con il server di log.	intero

rete (interfacce collegate)

L'oggetto Network (Bonded Interfaces) contiene informazioni di configurazione per le interfacce di rete collegate su un nodo di storage. È possibile utilizzare `GetConfig` e. `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
indirizzo	L'indirizzo IPv4 assegnato a questa interfaccia sul nodo.	stringa
IndirizzoV6	L'indirizzo di gestione IPv6 assegnato all'interfaccia Bond1G sul nodo.	stringa
bond-downdelay	Tempo di attesa, in millisecondi, prima di disattivare uno slave dopo il rilevamento di un errore di collegamento.	stringa
bond-fail_over_mac	La configurazione dell'indirizzo MAC dell'interfaccia di rete.	stringa
bond-miimon	La frequenza, espressa in millisecondi, alla quale lo stato del collegamento MII viene ispezionato per rilevare eventuali guasti del collegamento.	stringa
modalità bond	La modalità di bonding. Valori possibili: • ActivePassive (attivo passivo) (impostazione predefinita) • ALB • LACP (consigliato)	stringa

bond-primary_reselect	Specifica quando lo slave di bond primario viene scelto come slave attivo. Valori possibili: • Sempre • Meglio • Guasto	stringa
bond-slave	L'elenco delle interfacce slave per il collegamento.	stringa
bond-lacp_rate	Quando modalità Bond è LACP, il tasso può cambiare in una delle seguenti opzioni: • LACP veloce (impostazione predefinita) • LACP lento	stringa
bond-updelay	Il tempo di attesa, espresso in millisecondi, prima di abilitare uno slave dopo il rilevamento di un collegamento.	stringa
dns-nameserver	Un elenco di indirizzi utilizzati per i servizi dei nomi di dominio, separati da virgola o spazio.	stringa
ricerca-dns	Un elenco di domini di ricerca DNS separati da spazi o virgole.	stringa
famiglia	Famiglia di indirizzi configurata per l'utilizzo da parte dell'interfaccia. Attualmente è supportato "inet" per IPv4.	stringa
gateway	Indirizzo di rete del router IPv4 utilizzato per inviare traffico dalla rete locale.	stringa
GatewayV6	L'indirizzo di rete del router IPv6 utilizzato per inviare traffico dalla rete Bond1G locale.	stringa
IpV6PrefixLength	La lunghezza del prefisso di subnet per i percorsi statici di tipo "net" per il traffico IPv6 sulla rete Bond1G.	stringa

MACAddress (Indirizzo MAC)	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	stringa
MacAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	stringa
metodo	Il metodo utilizzato per configurare l'interfaccia. Valori possibili: • Loopback: Consente di definire l'interfaccia di loopback IPv4. • Manual (Manuale): Consente di definire le interfacce non configurate automaticamente. • dhcp: Può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • Static (statico): Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.	stringa
mtu	La dimensione massima dei pacchetti (in byte) che l'interfaccia può trasmettere. Deve essere maggiore o uguale a 1500; è supportato fino a 9000.	stringa
netmask	La maschera di bit che specifica la subnet per l'interfaccia.	stringa
rete	Indica dove inizia l'intervallo di indirizzi IP in base alla netmask.	stringa
percorsi	Matrice separata da virgole di stringhe di routing da applicare alla tabella di routing.	array di stringhe

stato	Lo stato dell'interfaccia. Valori possibili: • Inattivo: L'interfaccia non è attiva. • Up: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: L'interfaccia è pronta e viene stabilito un collegamento.	stringa
SimmetricRouteRules	Le regole di routing simmetriche configurate sul nodo.	array di stringhe
UpAndRunning	Indica se l'interfaccia è pronta e dispone di un collegamento.	booleano
VirtualNetworkTag	Identificativo della rete virtuale dell'interfaccia (tag VLAN).	stringa

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati o meno in ogni stato di nodo possibile.

Nome del membro	Stato disponibile	Stato in sospeso	Stato attivo
indirizzo	Sì	Sì	No
IndirizzoV6	Sì	Sì	No
bond-downdelay	Configurato dal sistema	N/A.	N/A.
bond-fail_over_mac	Configurato dal sistema	N/A.	N/A.
bond-miimon	Configurato dal sistema	N/A.	N/A.
modalità bond	Sì	Sì	Sì
bond-primary_reselect	Configurato dal sistema	N/A.	N/A.
bond-slave	Configurato dal sistema	N/A.	N/A.
bond-lacp_rate	Sì	Sì	Sì
bond-updelay	Configurato dal sistema	N/A.	N/A.

dns-nameserver	Sì	Sì	Sì
ricerca-dns	Sì	Sì	Sì
famiglia	No	No	No
gateway	Sì	Sì	Sì
GatewayV6	Sì	Sì	Sì
IpV6PrefixLength	Sì	Sì	Sì
MACAddress (Indirizzo MAC)	Configurato dal sistema	N/A.	N/A.
MacAddressPermanent	Configurato dal sistema	N/A.	N/A.
metodo	No	No	No
mtu	Sì	Sì	Sì
netmask	Sì	Sì	Sì
rete	No	No	No
percorsi	Sì	Sì	Sì
stato	Sì	Sì	Sì
SimmetricRouteRules	Configurato dal sistema	N/A.	N/A.
UpAndRunning	Configurato dal sistema	N/A.	N/A.
VirtualNetworkTag	Sì	Sì	Sì

Trova ulteriori informazioni

- GetConfig
- GetNetworkConfig

rete (tutte le interfacce)

L'oggetto rete (tutte le interfacce) raccoglie informazioni sulla configurazione dell'interfaccia di rete per un nodo di storage. È possibile utilizzare `GetConfig` e. `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
Bond10G	Informazioni di configurazione per l'interfaccia Bond10G Bonded.	rete (interfacce collegate)
Bond1G	Informazioni di configurazione per l'interfaccia Bond1G Bonded.	rete (interfacce collegate)
eth0-5	Un oggetto per ogni interfaccia Ethernet nel nodo di storage, che descrive le informazioni di configurazione per l'interfaccia. Questi oggetti sono numerati da 0 a 5 per corrispondere al nome dell'interfaccia.	Rete (interfacce Ethernet)
lo	Informazioni di configurazione per l'interfaccia di loopback.	rete (interfacce locali)

Trova ulteriori informazioni

- GetConfig
- GetNetworkConfig

Rete (interfacce Ethernet)

L'oggetto rete (interfacce Ethernet) contiene informazioni di configurazione per singole interfacce Ethernet. È possibile utilizzare `GetConfig` e. `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
bond-master	Specifica quale interfaccia collegata a questa interfaccia fisica come slave di collegamento.	stringa
famiglia	Famiglia di indirizzi configurata per l'utilizzo da parte dell'interfaccia. Attualmente è supportato "inet" per IPv4.	stringa

MACAddress (Indirizzo MAC)	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	stringa
MacAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	stringa
metodo	Il metodo utilizzato per configurare l'interfaccia. Valori possibili: • Loopback: Consente di definire l'interfaccia di loopback IPv4. • Manual (Manuale): Consente di definire le interfacce non configurate automaticamente. • dhcp: Può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • Static (statico): Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.	stringa
stato	Lo stato dell'interfaccia. Valori possibili: • Inattivo: L'interfaccia non è attiva. • Up: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: L'interfaccia è pronta e viene stabilito un collegamento.	stringa
UpAndRunning	Indica se l'interfaccia è pronta e dispone di un collegamento.	booleano

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati o meno in ogni stato di nodo possibile.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
bond-master	No	No	No
famiglia	No	No	No

MACAddress (Indirizzo MAC)	Configurato dal sistema	N/A.	N/A.
MacAddressPermanent	Configurato dal sistema	N/A.	N/A.
metodo	No	No	No
stato	Sì	Sì	Sì
UpAndRunning	Configurato dal sistema	N/A.	N/A.

Trova ulteriori informazioni

- GetConfig
- GetNetworkConfig

rete (interfacce locali)

L'oggetto Network (Local Interfaces) contiene informazioni di configurazione per le interfacce di rete locali, come l'interfaccia di loopback, su un nodo di storage. È possibile utilizzare `GetConfig` e. `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
famiglia	Famiglia di indirizzi configurata per l'utilizzo da parte dell'interfaccia. Attualmente è supportato "inet" per IPv4.	stringa
MACAddress (Indirizzo MAC)	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	stringa
MacAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	stringa

metodo	Il metodo utilizzato per configurare l'interfaccia. Valori possibili: • Loopback: Consente di definire l'interfaccia di loopback IPv4. • Manual (Manuale): Consente di definire le interfacce non configurate automaticamente. • dhcp: Può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • Static (statico): Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.	stringa
stato	Lo stato dell'interfaccia. Valori possibili: • Inattivo: L'interfaccia non è attiva. • Up: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: L'interfaccia è pronta e viene stabilito un collegamento.	stringa
UpAndRunning	Indica se l'interfaccia è pronta e dispone di un collegamento.	booleano

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati o meno in ogni stato di nodo possibile.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
famiglia	No	No	No
MACAddress (Indirizzo MAC)	Configurato dal sistema	N/A.	N/A.
MacAddressPermanent	Configurato dal sistema	N/A.	N/A.
metodo	No	No	No
stato	Sì	Sì	Sì

UpAndRunning	Configurato dal sistema	N/A.	N/A.

Trova ulteriori informazioni

- GetConfig
- GetNetworkConfig

Rete (SNMP)

L'oggetto di rete SNMP contiene informazioni sulla configurazione SNMP v3 per i nodi del cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	Il tipo di accesso consentito per le richieste di informazioni SNMP. Valori possibili: • ro: Accesso di sola lettura. • rw: Accesso di lettura/scrittura. • rosys: Accesso in sola lettura a un set limitato di informazioni di sistema.	stringa
cidr	Una maschera di rete CIDR. Questa maschera di rete deve essere un numero intero maggiore o uguale a 0 e minore o uguale a 32. Inoltre, non deve essere uguale a 31.	intero
comunità	Stringa di comunità SNMP.	stringa
rete	Questo membro, insieme al membro cidr, controlla a quale rete si applicano le stringhe di accesso e community. Il valore speciale "default" viene utilizzato per specificare una voce che si applica a tutte le reti. La maschera CIDR viene ignorata quando questo membro è un nome host o "predefinito".	stringa

Trova ulteriori informazioni

GetSnmpInfo

NetworkInterface

L'oggetto networkInterface contiene informazioni di configurazione per singole interfacce di rete su un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
indirizzo	L'indirizzo di gestione IPv4 dell'interfaccia.	stringa
IndirizzoV6	L'indirizzo di gestione IPv6 dell'interfaccia.	stringa
trasmissione	L'indirizzo di trasmissione dell'interfaccia.	stringa
MACAddress (Indirizzo MAC)	L'indirizzo MAC dell'interfaccia.	stringa
mtu	L'unità di trasferimento massima, in byte, dell'interfaccia.	intero
nome	Il nome dell'interfaccia.	stringa
namespace	Se a questa interfaccia viene assegnato o meno uno spazio dei nomi della rete virtuale.	booleano
netmask	Subnet mask dell'interfaccia.	stringa
stato	Lo stato operativo dell'interfaccia.	stringa
tipo	Il tipo di interfaccia (master bond, slave bond, ecc.).	stringa
VirtualNetworkTag	L'ID VLAN assegnato all'interfaccia sulla rete virtuale.	intero

NetworkInterfaceStats

L'oggetto networkInterfaceStats contiene statistiche di rete, il numero totale di pacchetti

trasmessi e ricevuti e informazioni sugli errori per le singole interfacce di rete su un nodo di storage. È possibile utilizzare `ListNetworkInterfaceStats` Metodo API per elencare queste informazioni per le interfacce di rete su un nodo di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
collisioni	Il numero di collisioni rilevate.	intero
nome	Nome dell'interfaccia di rete.	stringa
RxByte	Il numero totale di byte ricevuti.	intero
RxCrcErrors	Il numero di pacchetti ricevuti con errore CRC.	intero
RxDropped	Il numero di pacchetti ricevuti che sono stati ignorati.	intero
RxErrors	Il numero di pacchetti non validi o non validi ricevuti.	intero
RxFifoErrors	Il numero di errori di sovraccarico FIFO nei dati ricevuti.	intero
RxFrameErrors	Il numero di pacchetti ricevuti con errori di allineamento dei frame.	intero
RxLengthErrors	Il numero di pacchetti ricevuti con un errore di lunghezza.	intero
RxErrors non disponibili	Il numero di pacchetti persi dal ricevitore.	intero
RxOverErrors	Il numero di errori di overflow del buffer del ricevitore per questa interfaccia.	intero
RxPacket	Il numero totale di pacchetti ricevuti.	intero
TxByte	Il numero totale di byte trasmessi.	intero
TxCarrierErrors	Il numero di errori della portante per il lato di trasmissione.	intero
TxError	Il numero di errori di trasmissione dei pacchetti.	intero
TxFifoErrors	Il numero di errori di sovraccarico FIFO sul lato di trasmissione.	intero
TxPackets	Il numero totale di pacchetti trasmessi.	intero

nodo

L'oggetto node contiene informazioni su ciascun nodo del cluster. È possibile recuperare queste informazioni utilizzando `ListActiveNodes` e. `ListAllNodes` metodi.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AssociatedFServiceID	L'ID del servizio Fibre Channel per il nodo. "0" se il nodo non è un nodo Fibre Channel.	intero
AssociatedMasterServiceID	ID servizio principale per il nodo.	intero
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
ChassisName	Identifica in modo univoco uno chassis; identico per tutti i nodi in un unico chassis.	stringa
cip	L'indirizzo IP del cluster assegnato al nodo.	stringa
cipi	Interfaccia di rete utilizzata per la comunicazione del cluster.	stringa
CustomProtectionDomainName	Identifica in modo univoco un dominio di protezione personalizzato. Questo nome è identico per tutti i nodi di storage all'interno di tutti gli chassis in un determinato dominio di protezione personalizzato.	stringa
FiberChannelTargetPortGroup	Il gruppo di destinazione associato a questo nodo. "Null" se il nodo non è un nodo Fibre Channel.	intero
MaintenanceMode	Indica la modalità in cui si trova un nodo per la manutenzione.	n/a.
mip	L'indirizzo IP utilizzato per la gestione dei nodi.	stringa

Nome	Descrizione	Tipo
mipi	Interfaccia di rete utilizzata per la gestione dei nodi.	stringa
nome	Nome host del nodo.	stringa
ID NodeID	NodeID per questo nodo.	intero
NodeSlot	Per le piattaforme HCI, la lettera corrispondente allo slot dello chassis in cui si trova questo nodo ("A", "B", "C" o "D"). Per le piattaforme storage, questo valore è nullo.	stringa
Informazioni platform	Informazioni hardware per il nodo. Membri: • ChassisType: La piattaforma hardware del nodo. • CpuModel: Il modello di CPU della piattaforma hardware. • NodeMemoryGB: La quantità di memoria installata nella piattaforma fisica in GB. • NodeType: Il nome del modello del nodo. • PlatformConfigVersion: Versione del software configurato per questo nodo hardware.	Oggetto JSON
ruolo	Ruolo del nodo nel cluster. Valori possibili: • Gestione • Storage • Calcolo • Testimone	
sip	L'indirizzo IP dello storage assegnato al nodo.	stringa
sipi	Interfaccia di rete utilizzata per il traffico di storage.	stringa

Nome	Descrizione	Tipo
Versione software	Restituisce la versione corrente del software Element in esecuzione sul nodo.	stringa
uuid	Identificatore universalmente univoco associato a questo nodo.	stringa
VirtualNetworks	Oggetto contenente gli ID e gli indirizzi IP della rete virtuale.	VirtualNetwork array

Trova ulteriori informazioni

- ListActiveNode
- ListAllNode

NodeProtectionDomini

L'oggetto nodeProtectionDomains contiene informazioni sull'identificazione di un nodo e sui domini di protezione associati a tale nodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID NodeID	Identificatore univoco del nodo.	intero
ProtectionDomini	Elenco dei domini di protezione di cui il nodo è membro.	"Protection Domain (dominio di protezione)"

NodeStats

L'oggetto nodeStats contiene misure di attività di alto livello per un nodo. È possibile utilizzare `GetNodeStats` e. `ListNodeStats` Metodi API per ottenere alcuni o tutti gli oggetti nodeStats.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
conta	Il numero di campioni totali nell'oggetto nodeStats.	intero

Nome	Descrizione	Tipo
cpu	Utilizzo della CPU, in %.	intero
CpuTotal	Aumento monotonico del valore dell'utilizzo della cpu.	intero
CBytesIn	Byte nell'interfaccia del cluster.	intero
CBytesOut	Byte in uscita sull'interfaccia del cluster.	intero
SBytesIn	Byte nell'interfaccia di storage.	intero
SBytesOut	Byte in uscita sull'interfaccia di storage.	intero
MBytesIn	Byte nell'interfaccia di gestione.	intero
MBytesOut	Byte in uscita sull'interfaccia di gestione.	intero
NetworkUtilisationCluster	Utilizzo dell'interfaccia di rete (in %) per l'interfaccia di rete del cluster.	intero
NetworkUtilisationStorage	Utilizzo dell'interfaccia di rete (in %) per l'interfaccia di rete dello storage.	intero
ReadLatencyUSecTotal	Aumento monotonico del valore del tempo totale impiegato per eseguire operazioni di lettura al nodo.	intero
ReadOps	Aumento monotonico del valore delle operazioni di lettura totali su un nodo.	intero
SsLoadHistogramma	Dati dell'istogramma che illustrano il carico di servizio della sezione nel tempo.	Oggetto JSON
data e ora	L'ora corrente nel formato UTC+0.	Stringa di dati ISO 8601
UsedMemory	Utilizzo totale della memoria in byte.	intero

Nome	Descrizione	Tipo
SwriteLatencyUSecTotal	Aumento monotonico del valore del tempo totale impiegato per eseguire operazioni di scrittura sul nodo.	intero
SwriteOps	Aumento monotonico del valore delle operazioni di scrittura totali su un nodo.	intero

Trova ulteriori informazioni

- GetNodeStats
- ListNodeStats

OntapVersionInfo

L'oggetto ontapVersionInfo contiene informazioni sulla versione API del cluster ONTAP in una relazione SnapMirror. L'interfaccia utente Web Element utilizza `GetOntapVersionInfo` Metodo API per ottenere queste informazioni.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
ClientAPIMajorVesion	La versione principale dell'API ONTAP utilizzata dal client dell'API Element.	stringa
ClientAPIMinorVesion	La versione minore dell'API ONTAP utilizzata dal client dell'API Element.	stringa
OntapAPIMAjorVersion	La versione principale dell'API corrente supportata dal sistema ONTAP.	stringa
OntapAPIMinorVesion	La versione secondaria API corrente supportata dal sistema ONTAP.	stringa

Nome	Descrizione	Tipo
OntapVersion	La versione corrente del software in esecuzione sul cluster ONTAP.	stringa

PendingActiveNode

L'oggetto pendingActiveNode contiene informazioni su un nodo che si trova attualmente nello stato pendingActive, tra lo stato in sospeso e quello attivo. Si tratta di nodi che vengono attualmente restituiti all'immagine software di fabbrica. Utilizzare `ListPendingActiveNodes` Metodo API per restituire un elenco di queste informazioni per tutti i nodi pendingActive.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ActiveNodeKey	Chiave univoca che consente al nodo di unirsi automaticamente al cluster dopo una corretta installazione del software.	stringa
AssignedNodeID	L'ID nodo assegnato per il nodo.	stringa
AsyncHandle	L'handle del metodo asincrono che è possibile utilizzare per eseguire query sullo stato dell'operazione.	intero
cip	L'indirizzo IP del cluster assegnato al nodo.	stringa
mip	L'indirizzo IP di gestione assegnato al nodo.	stringa
NodeSlot	Per le piattaforme HCI, la lettera corrispondente allo slot dello chassis in cui si trova questo nodo ("A", "B", "C" o "D"). Per le piattaforme storage, questo valore è nullo.	stringa
PendingActiveNodeID	L'ID del nodo in sospeso.	intero

Nome	Descrizione	Tipo
Informazioni platform	Informazioni hardware per il nodo. Membri: • ChassisType: La piattaforma hardware del nodo. • CpuModel: Il modello di CPU della piattaforma hardware. • NodeMemoryGB: La quantità di memoria installata nella piattaforma fisica in GB. • NodeType: Il nome del modello del nodo. • PlatformConfigVersion: Versione del software configurato per questo nodo hardware.	Oggetto JSON
ruolo	Ruolo del nodo nel cluster. Valori possibili: • Gestione • Storage • Calcolo • Testimone	
sip	L'indirizzo IP dello storage (iSCSI) assegnato al nodo.	stringa
Versione software	La versione corrente del software Element in esecuzione sul nodo.	stringa

Trova ulteriori informazioni

ListPendingActiveNode

PendingNode

L'oggetto pendingNode contiene informazioni su un nodo che può essere aggiunto a un cluster. Utilizzare `ListPendingNodes` Metodo API per restituire un elenco di queste informazioni per tutti i nodi in sospeso. È possibile aggiungere qualsiasi nodo elencato a un cluster utilizzando `AddNodes` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
cipi	L'indirizzo IP del cluster assegnato al nodo.	stringa
ActiveNodeKey	Chiave univoca che consente al nodo di unirsi automaticamente al cluster dopo una corretta installazione del software.	stringa
AssignedNodeID	L'ID nodo assegnato per il nodo.	stringa
AsyncHandle	L'handle del metodo asincrono che è possibile utilizzare per eseguire query sullo stato dell'operazione.	intero
ChassisName	Identifica in modo univoco uno chassis; identico per tutti i nodi in un unico chassis.	stringa
cip	L'indirizzo IP del cluster assegnato al nodo.	stringa
mip	L'indirizzo IP di gestione assegnato al nodo.	stringa
NodeSlot	Per le piattaforme HCI, la lettera corrispondente allo slot dello chassis in cui si trova questo nodo ("A", "B", "C" o "D"). Per le piattaforme storage, questo valore è nullo.	stringa
PendingActiveNodeID	L'ID del nodo in sospeso.	intero

Nome	Descrizione	Tipo
Informazioni platform	Informazioni hardware per il nodo. Membri: • ChassisType: La piattaforma hardware del nodo. • CpuModel: Il modello di CPU della piattaforma hardware. • NodeMemoryGB: La quantità di memoria installata nella piattaforma fisica in GB. • NodeType: Il nome del modello del nodo. • PlatformConfigVersion: Versione del software configurato per questo nodo hardware.	Oggetto JSON
ruolo	Ruolo del nodo nel cluster. Valori possibili: • Gestione • Storage • Calcolo • Testimone	
sip	L'indirizzo IP dello storage (iSCSI) assegnato al nodo.	stringa
Versione software	La versione corrente del software Element in esecuzione sul nodo.	stringa

Trova ulteriori informazioni

- AddNode
- ListPendingNode

Protection Domain (dominio di protezione)

L'oggetto ProtectionDomain contiene i dettagli relativi al nome e al tipo di un dominio di protezione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionDomainName	Il nome del dominio di protezione.	stringa
ProtectionDomainType	Il tipo di dominio di protezione. Valori possibili: • Chassis: Tutti i nodi storage in un unico chassis. • Customizzato: Tutti i nodi di storage in un singolo dominio di protezione definito dal cliente.	stringa

ProtectionDomainLevel

L'oggetto ProtectionDomainLevel contiene informazioni sugli attuali livelli di tolleranza e resilienza del cluster di storage. I livelli di tolleranza indicano la capacità del cluster di continuare a leggere e scrivere i dati in caso di errore, mentre i livelli di resilienza indicano la capacità del cluster di guarire automaticamente da uno o più guasti all'interno del tipo di dominio di protezione associato.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionDomainType	Il tipo di dominio di protezione che ha la tolleranza e la resilienza associate. Valori possibili: • Nodo: Qualsiasi nodo singolo. • Chassis: Qualsiasi nodo singolo o tutti i nodi storage in un singolo chassis. • Customizzato: Tutti i nodi di storage in un singolo dominio di protezione definito dal cliente.	stringa
resilienza	L'attuale resilienza di questo cluster dal punto di vista di questo tipo di dominio di protezione.	ProtectionDomainResiliency
tolleranza	La tolleranza corrente di questo cluster dal punto di vista di questo tipo di dominio di protezione.	ProtectionDomainTolerance

ProtectionDomainResiliency

L'oggetto ProtectionDomainResiliency contiene lo stato di resilienza di questo cluster di storage. La resilienza indica la capacità del cluster di storage di risanare automaticamente da uno o più guasti, tutti all'interno di un singolo dominio di protezione del tipo di dominio di protezione associato. Un cluster di storage viene considerato healed quando può continuare a leggere e scrivere i dati attraverso il guasto di un singolo nodo di storage (uno stato noto come tolleranza del nodo).

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionSchemeResilienze	Un elenco di oggetti (uno per ogni schema di protezione) contenente informazioni sulla resilienza degli errori per il tipo di dominio di protezione associato.	ProtectionSchemeResiliency array
SingleFailureThresholdBytesForBlockData	Il numero massimo di byte che è possibile memorizzare nel cluster di storage prima di perdere la capacità di riparare automaticamente a uno stato di tolleranza del nodo.	intero
AbleFailuresForEnsemble	Il numero previsto di errori simultanei che possono verificarsi senza perdere la capacità di correggere automaticamente uno stato di tolleranza del nodo per il quorum dell'ensemble.	intero

ProtectionDomainTolerance

L'oggetto ProtectionDomainTolerance contiene informazioni sulla capacità del cluster di storage di continuare a leggere e scrivere dati in caso di uno o più errori, tutti all'interno di un singolo dominio di protezione del tipo di dominio di protezione associato.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionSchemeTolerances	Un elenco di oggetti (uno per ogni schema di protezione) contenente informazioni sulla tolleranza di errore per il tipo di dominio di protezione associato.	ProtectionSchemeTolerance array
AbleFailuresForEnsemble	Il numero di errori simultanei all'interno del tipo di dominio di protezione associato che possono verificarsi senza perdere il quorum dell'ensemble.	intero

ProtectionSchemeResiliency

L'oggetto ProtectionSchemeResiliency contiene informazioni sulla possibilità di riparare automaticamente un cluster di storage per uno schema di protezione specifico in caso di uno o più guasti all'interno della relativa ProtectionDomainType associata. Un cluster di storage viene considerato healed quando può continuare a leggere e scrivere i dati attraverso il guasto di un singolo nodo di storage (uno stato noto come tolleranza del nodo).

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionScheme	Lo schema di protezione corrente di questo cluster di storage. L'unico valore possibile è doubleHelix.	stringa
SostenibileFailuresForBlockData	Il numero previsto di guasti simultanei che possono verificarsi senza perdere la capacità di riparare automaticamente a uno stato di tolleranza del nodo per i dati.	intero
SostenibileFailuresForMetadata	Il numero previsto di errori simultanei che possono verificarsi senza perdere la capacità di correggere automaticamente lo stato di tolleranza del nodo per i metadati.	intero

ProtectionSchemeTolerance

L'oggetto ProtectionSchemeTolerance contiene informazioni sulla possibilità per un cluster di storage, per uno schema di protezione specifico, di continuare a leggere e scrivere i dati in seguito a errori.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ProtectionScheme	Lo schema di protezione corrente di questo cluster di storage. L'unico valore possibile è doubleHelix.	stringa
SostenibileFailuresForBlockData	Il numero corrente di guasti simultanei che possono verificarsi senza perdere la disponibilità dei dati a blocchi per lo schema di protezione associato.	intero
SostenibileFailuresForMetadata	Il numero corrente di guasti simultanei che possono verificarsi senza perdere la disponibilità dei metadati per lo schema di protezione associato.	intero

ProtocolEndpoint

L'oggetto ProtocolEndpoint contiene gli attributi di un endpoint del protocollo. È possibile recuperare queste informazioni per tutti gli endpoint del protocollo nel cluster utilizzando `ListProtocolEndpoints` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
PrimariaProviderID	L'ID dell'oggetto provider dell'endpoint del protocollo primario per l'endpoint del protocollo.	intero
ProtocolEndpointID	ID univoco dell'endpoint del protocollo.	UUID

Nome	Descrizione	Tipo
ProtocolEndpointState	Lo stato dell'endpoint del protocollo. Valori possibili: • Attivo: L'endpoint del protocollo è in uso. • Start: L'endpoint del protocollo è in fase di avvio. • Failover: Si è verificato un failover dell'endpoint del protocollo. • Riservato: L'endpoint del protocollo è riservato.	stringa
ProviderType	Il tipo di provider dell'endpoint del protocollo. Valori possibili: • Primario • Secondario	stringa
ID scsiNAADeviceID	Identificatore univoco globale del dispositivo SCSI per l'endpoint del protocollo in NAA IEEE Registered Extended Format.	stringa
SecondaryProviderID	L'ID dell'oggetto provider dell'endpoint del protocollo secondario per l'endpoint del protocollo.	intero

Trova ulteriori informazioni

ListProtocolEndpoint

QoS

L'oggetto QoS contiene informazioni sulle impostazioni QoS (Quality of Service) per i volumi. I volumi creati senza valori QoS specificati vengono creati utilizzando i valori predefiniti. È possibile trovare i valori predefiniti utilizzando `GetDefaultQoS` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
BurstIOPS	Massimo IOPS di 4 KB "picco" consentito per brevi periodi di tempo. Consente di eseguire burst di attività i/o sul normale valore maxIOPS.	intero
BurstTime	La durata del burstIOPS è consentita. Il valore restituito viene rappresentato in secondi. Questo valore viene calcolato dal sistema in base agli IOPS impostati per QoS.	intero
curva	La curva è un insieme di coppie chiave-valore. Le chiavi sono di dimensioni i/o in byte. I valori rappresentano il costo dell'esecuzione di un IOP a una dimensione i/o specifica. La curva viene calcolata in relazione a un'operazione di 4096 byte impostata su 100 IOPS.	Oggetto JSON
MaxIOPS	Il massimo di 4 KB di IOPS desiderato consentito in un periodo di tempo esteso.	intero
MinIOPS	Gli IOPS minimi da 4 KB da garantire. Gli IOPS consentiti scenderanno al di sotto di questo livello solo se tutti i volumi sono stati ridotti al loro valore minIOPS e la capacità delle performance è ancora insufficiente.	intero

Trova ulteriori informazioni

GetDefaultQoS

QoSPolicy

L'oggetto QoSPolicy contiene informazioni su un criterio QoS in un cluster di storage che esegue il software Element.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
QosPolicyID	Un identificatore intero univoco per la QoSPolicy assegnata automaticamente dal cluster di storage.	intero
nome	Il nome del criterio QoS. Ad esempio: oro, platino o argento.	stringa
qos	Le impostazioni QoS rappresentate da questo criterio.	QoS
ID volume	Un elenco di volumi associati a questo criterio.	array intero

Trova ulteriori informazioni

Policy GetQoS

RemoteClusterSnapshotStatus

Il `remoteClusterSnapshotStatus` Oggetto contiene l'UUID e lo stato di uno snapshot memorizzato in un cluster di storage remoto. È possibile ottenere queste informazioni con `ListSnapshots` oppure `ListGroupSnapshots` Metodi API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
RemoteStatus	Lo stato di replica dello snapshot remoto sul cluster di destinazione, come visualizzato dal cluster di origine. Valori possibili: • Presente: Lo snapshot esiste in un cluster remoto. • NotPresent: Lo snapshot non esiste in un cluster remoto. • Sincronizzazione: Si tratta di un cluster di destinazione che sta attualmente replicando lo snapshot. • Cancellato: Si tratta di un cluster di destinazione. L'istantanea è stata eliminata e esiste ancora nell'origine.	stringa

Nome	Descrizione	Tipo
VolumePairUID	L'identificatore universale della coppia di volumi.	UUID

pianificazione

L'oggetto schedule contiene informazioni su una pianificazione creata per creare autonomamente un'istantanea di un volume. È possibile recuperare le informazioni di pianificazione per tutti i programmi con `ListSchedules` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Indica la frequenza dell'occorrenza della pianificazione. Valori possibili: • Giorno della settimana • Giorno del mese • Intervallo di tempo	Oggetto JSON
HasError	Indica se la pianificazione presenta o meno errori. Valori possibili: • vero • falso	booleano
ore	Mostra le ore che trascorreranno prima della creazione dello snapshot successivo. I valori possibili sono compresi tra 0 e 24.	intero
LastRunStatus	Indica lo stato dell'ultimo snapshot pianificato. Valori possibili: • Successo • Non riuscito	stringa
LastRunTimeStart	Indica l'ultima volta in cui è stata avviata la pianificazione.	Stringa di dati ISO 8601
minuti	Mostra i minuti che trascorreranno prima della creazione dello snapshot successivo. I valori possibili sono compresi tra 0 e 59.	intero

Nome	Descrizione	Tipo
monthdays	Indica i giorni del mese in cui verrà creata una snapshot.	array
in pausa	Indica se la pianificazione è in pausa o meno. Valori possibili: • vero • falso	booleano
ricorrente	Indica se la pianificazione è ricorrente o meno. Valori possibili: • vero • falso	booleano
RunNextInterval	Indica se la pianificazione verrà eseguita o meno alla successiva attivazione dello scheduler. Se true, la pianificazione verrà eseguita la prossima volta che lo scheduler sarà attivo, quindi questo valore viene reimpostato su false. Valori possibili: • vero • falso	booleano
ScheduleId	L'ID univoco della pianificazione.	intero

Nome	Descrizione	Tipo
ScheduleInfo	Include il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume del volume da cui è stato creato lo snapshot. Valori validi: • `enableRemoteReplication`Indica se lo snapshot deve essere incluso nella replica remota. (booleano) • `ensureSerialCreation`: Specifica se deve essere consentita la creazione di un nuovo snapshot se è in corso una replica snapshot precedente. (booleano) • `name`: Il nome dello snapshot da utilizzare. (stringa) • `retention`: Periodo di tempo durante il quale l'istantanea viene conservata. A seconda dell'ora, viene visualizzato in uno dei seguenti formati: ◦ `fifo`: L'istantanea viene conservata in base al FIFO (First-in-First-out). Se vuoto, lo snapshot viene conservato per sempre. (stringa) ◦ "HH:mm:ss" • `volumeID`: L'ID del volume da includere nello snapshot. (intero) • `volumes`: Un elenco di ID volume da includere nello snapshot di gruppo. (array intero)	Oggetto JSON
Nome scheduleName	Il nome univoco assegnato alla pianificazione.	stringa
Tipo di scheduleType	Al momento sono supportati solo i tipi di snapshot pianificati.	stringa

Nome	Descrizione	Tipo
SnapMirrorLabel	L'etichetta SnapMirrorLabel da applicare all'istantanea o all'istantanea di gruppo creata, contenuta in scheduleInfo. Se non impostato, questo valore è nullo.	stringa
Data di inizio	Indica la data alla prima volta in cui inizia o inizierà il programma; formattata in ora UTC.	Stringa di dati ISO 8601
ToDeleted	Indica se la pianificazione è contrassegnata per l'eliminazione. Valori possibili: • vero • falso	booleano
giorni feriali	Indica i giorni della settimana in cui verrà creata una snapshot.	array

Trova ulteriori informazioni

Elenchi

Sessione (Fibre Channel)

L'oggetto sessione contiene informazioni su ogni sessione Fibre Channel visibile al cluster e sulle porte di destinazione su cui è visibile. È possibile recuperare queste informazioni con `ListFibreChannelSessions` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
InitiatorWWPN	Il World Wide Port Name (WWPN) dell'iniziatore che ha effettuato l'accesso alla porta di destinazione.	stringa
ID NodeID	Nodo proprietario della sessione Fibre Channel.	intero

Nome	Descrizione	Tipo
iniziatore	Informazioni sull'iniziatore server di questa sessione Fibre Channel. Membri: • Alias: Il nome descrittivo assegnato all'iniziatore. • Attributi: Gli attributi di questo iniziatore. • InitatorID (ID inizializzatore): L'ID di questo iniziatore. • InitiatorName (Nome inizializzatore): Il nome dell'iniziatore. • VolumeAccessGroups: Un elenco di gruppi di accesso ai volumi associati a questo iniziatore.	Oggetto JSON
ID servizio	L'ID servizio della porta di destinazione coinvolta in questa sessione.	intero
TargetWWPN	Il numero WWPN della porta di destinazione coinvolta in questa sessione.	stringa
VolumeAccessGroupID	L'ID del gruppo di accesso al volume a cui appartiene l'iniziatorWWPN. Se non si trova in un gruppo di accesso al volume, questo valore è nullo.	intero

Trova ulteriori informazioni

ListFiberChannelSessions

Sessione (iSCSI)

L'oggetto session (iSCSI) contiene informazioni dettagliate sulla sessione iSCSI di ciascun volume. È possibile recuperare le informazioni sulla sessione iSCSI con `ListISCSISessions` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID account	L'ID account dell'account utilizzato per l'autenticazione CHAP, se presente.	intero
Nome account	Il nome dell'account utilizzato per l'autenticazione CHAP, se presente.	stringa
CreateTime	L'ora della creazione della sessione iSCSI, in formato UTC+0.	Stringa di dati ISO 8601
ID del driver	L'ID del driver associato al servizio di trasporto che ospita la sessione.	intero
ID del driver	Un elenco degli ID dei dischi che segnalano il guasto. Un elenco vuoto, se non applicabile.	array intero
iniziatore	Informazioni sull'iniziatore server di questa sessione iSCSI. Membri: • Alias: Il nome descrittivo assegnato all'iniziatore. • Attributi: Gli attributi di questo iniziatore. • InitatorID (ID inizializzatore): L'ID di questo iniziatore. • InitiatorName (Nome inizializzatore): Il nome dell'iniziatore. • VolumeAccessGroups: Un elenco di gruppi di accesso ai volumi associati a questo iniziatore.	Oggetto JSON
InitatorIP	L'indirizzo IP e il numero di porta dell'iniziatore del server iSCSI.	stringa
InitiatorName (Nome iniziatore	Il nome qualificato iSCSI (IQN) dell'iniziatore del server iSCSI.	stringa
InitiatorPortName	InitiatorName, insieme all'InitiatorSessionID, identifica la porta dell'iniziatore.	stringa

Nome	Descrizione	Tipo
InitiatorSessionID	ID a 48 bit fornito dall'iniziatore che identifica la sessione iSCSI come appartenente a tale iniziatore.	intero
MsSinceLastIscsiPDU	Il tempo, espresso in millisecondi, trascorso dall'ultima PDU iSCSI ricevuta per questa sessione.	intero
MsSinceLastScsiCommand	Il tempo, espresso in millisecondi, trascorso dalla ricezione dell'ultimo comando SCSI per questa sessione.	intero
ID NodeID	Il NodeID associato al servizio di trasporto che ospita la sessione.	intero
ID servizio	L'ID servizio del servizio di trasporto che ospita la sessione.	intero
ID SessionID	ID sessione iSCSI.	intero
TargetIP	L'indirizzo IP e il numero di porta della destinazione dello storage iSCSI.	stringa
TargetName	IQN della destinazione iSCSI.	stringa
TargetPortName	Il nome target, insieme al tag del gruppo di portali di destinazione, identifica la porta di destinazione.	stringa
VirtualNetworkID	L'ID della rete virtuale associato alla sessione.	intero
ID volume	ID volume del volume associato alla sessione, se presente.	intero
VolumeInstance	Identifica l'oggetto volume associato alla sessione iSCSI, se presente.	intero

Trova ulteriori informazioni

ListISCSISessions

SnapMirrorAggregate

L'oggetto SnapMirrorAggregate contiene informazioni sugli aggregati ONTAP disponibili, ovvero raccolte di dischi resi disponibili ai volumi come storage. È possibile ottenere queste informazioni utilizzando il metodo API ListSnapMirrorAggregates.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
AggregateName	Il nome dell'aggregato.	stringa
Nodename	Il nome del nodo ONTAP proprietario dell'aggregato.	stringa
Disponibile	Il numero di byte disponibili rimanenti nell'aggregato.	intero
SizeTotal	La dimensione totale (in byte) dell'aggregato.	intero
PercentoUsedCapacity	La percentuale di spazio su disco attualmente in uso.	intero
Conteggio volumi	Il numero di volumi nell'aggregato.	intero

SnapMirrorClusterIdentity

L'oggetto snapMirrorClusterIdentity contiene informazioni di identificazione sul cluster ONTAP remoto in una relazione SnapMirror.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
Nome cluster	Il nome del cluster ONTAP di destinazione.	stringa

Nome	Descrizione	Tipo
UUID clusterId	Identificatore univocamente univoco a 128 bit del cluster ONTAP di destinazione.	stringa
Numero di serie di clusterSerial	Il numero di serie del cluster ONTAP di destinazione.	stringa

SnapMirrorEndpoint

L'oggetto SnapMirrorEndpoint contiene informazioni sui sistemi storage SnapMirror remoti che comunicano con il cluster storage Element. È possibile recuperare queste informazioni con il metodo API ListSnapMirrorEndpoints.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	Identificatore univoco dell'oggetto nel cluster locale.	intero
IP gestioneIP	L'indirizzo IP di gestione del cluster dell'endpoint.	stringa
Nome cluster	Il nome del cluster ONTAP. Questo valore viene compilato automaticamente con il valore "clusterName" dall'oggetto snapMirrorClusterIdentity.	stringa
nome utente	Il nome utente di gestione per il sistema ONTAP.	stringa
Indirizzi ipAddresses	Elenco degli indirizzi IP dello storage tra cluster per tutti i nodi nel cluster. È possibile ottenere questi indirizzi IP con il metodo ListSnapMirrorNetworkInterfaces.	array di stringhe
Isconnected (connesso)	Lo stato di connettività del collegamento di controllo al cluster ONTAP.	booleano

SnapMirrorJobScheduleCronInfo

L’oggetto snapMirrorJobScheduleCronInfo contiene informazioni su una pianificazione del processo cron nel sistema ONTAP.

Membri dell’oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L’ID del sistema ONTAP di destinazione.	intero
JobScheduleName	Il nome della pianificazione del processo.	stringa
JobScheduleDescription	Un riepilogo della pianificazione generato automaticamente e leggibile dall’utente.	stringa

SnapMirrorLunInfo

L’oggetto snapMirrorLunInfo contiene informazioni sull’oggetto LUN ONTAP.

Membri dell’oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L’ID del sistema ONTAP di destinazione.	intero
CreationTimestamp	Il tempo di creazione del LUN.	Stringa di dati ISO 8601
Nome del LUN	Il nome del LUN.	stringa
percorso	Il percorso del LUN.	stringa
dimensione	La dimensione del LUN in byte.	intero
SizeUsed	Il numero di byte utilizzati dal LUN.	intero

Nome	Descrizione	Tipo
stato	Lo stato di accesso corrente del LUN. Valori possibili: • online • offline • foreign_lun_error • nvfail • errore_spazio	stringa
volume	Il nome del volume che contiene il LUN.	stringa
server virtuale	Il Vserver che contiene il LUN.	stringa

SnapMirrorNetworkInterface

L'oggetto snapMirrorNetworkInterface contiene informazioni sulle interfacce logiche (LIF) dell'intercluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AmministrativeStatus	Se l'interfaccia logica (LIF) è attivata o disattivata a livello amministrativo. Valori possibili: • su • giù	stringa
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
InterfaceName	Il nome LIF.	stringa
NetworkAddress (Indirizzo di rete)	L'indirizzo IP del LIF.	stringa
NetworkMask	La maschera di rete del LIF.	stringa

Nome	Descrizione	Tipo
InterfaceRole	Il ruolo della LIF. Valori possibili: • non def • cluster • dati • node_mgmt • intercluster • cluster_mgmt	stringa
OperationalStatus (Stato operativo)	Lo stato operativo del LIF (indipendentemente dal fatto che abbia stabilito o meno una connessione riuscita). Questo stato può differire dallo stato amministrativo se si verifica un problema di rete che impedisce il funzionamento dell'interfaccia. Valori possibili: • su • giù	stringa
VserverName	Il nome del Vserver.	stringa

SnapMirrorNode

L'oggetto SnapMirrorNode contiene informazioni sui nodi del cluster ONTAP di destinazione in una relazione SnapMirror.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
nome	Il nome del nodo ONTAP.	stringa
modello	Il modello del nodo ONTAP.	stringa
Numero di serie	Il numero di serie del nodo ONTAP.	stringa
Versione prodotto	La versione del prodotto ONTAP.	stringa

Nome	Descrizione	Tipo
IsNodeHealthy	Lo stato di salute di un nodo nel cluster ONTAP. Valori possibili: • vero • falso	stringa
IsNodeElibile	Se il nodo è idoneo o meno a partecipare a un cluster ONTAP. Valori possibili: • vero • falso	stringa

SnapMirrorPolicy

L'oggetto SnapMirrorPolicy contiene informazioni su un criterio SnapMirror memorizzato in un sistema ONTAP.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
Nome criterio	Il nome univoco assegnato al criterio.	stringa
Tipo di criterio	Il tipo di policy. Valori possibili: • mirror_asincrono • vault_mirror	stringa
commento	Descrizione leggibile associata al criterio SnapMirror.	stringa

Nome	Descrizione	Tipo
TransferPriority	La priorità di esecuzione di un trasferimento SnapMirror. Valori possibili: • Normal (normale): La priorità predefinita. Questi trasferimenti vengono pianificati prima della maggior parte dei trasferimenti a bassa priorità. • Basso: Questi trasferimenti hanno la priorità più bassa e vengono pianificati dopo la maggior parte dei trasferimenti con priorità normale.	stringa
Regole delle politiche	Un elenco di oggetti che descrivono le regole dei criteri.	SnapMirrorPolicyRule array
TotalKeepCount	Il numero totale di conservazione per tutte le regole del criterio.	intero
TotalRules	Il numero totale di regole nel criterio.	intero
VserverName	Il nome del Vserver per il criterio SnapMirror.	stringa

SnapMirrorPolicyRule

L'oggetto snapMirrorPolicyRule contiene informazioni sulle regole di un criterio SnapMirror.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorLabel	L'etichetta della copia Snapshot, utilizzata per la selezione della copia Snapshot nelle relazioni estese di protezione dei dati.	stringa
KeepCount	Specifica il numero massimo di copie Snapshot conservate nel volume di destinazione di SnapMirror per una regola.	intero

SnapMirrorRelationship

L'oggetto SnapMirrorRelationship contiene informazioni su una relazione SnapMirror tra un volume Element e un volume ONTAP.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
SnapMirrorRelationshipID	L'identificatore univoco di ogni oggetto SnapMirrorRelationship in una matrice, come restituito in ListSnapMirrorRelationships. Questo UUID viene creato e restituito dal sistema ONTAP.	stringa
SourceVolume	Oggetto che descrive il volume di origine.	SnapMirrorVolumeInfo
DestinationVolume	Oggetto che descrive il volume di destinazione.	SnapMirrorVolumeInfo
CurrentMaxTransferRate	La velocità di trasferimento massima corrente tra i volumi di origine e di destinazione, espressa in kilobyte al secondo.	intero
IsHealthy	Se il rapporto è sano o no. Valori possibili: • Vero: Il rapporto è sano. • Falso: Il rapporto non è buono. Questo può essere causato da un aggiornamento manuale o pianificato che non riesce o viene interrotto o dall'ultimo aggiornamento pianificato in ritardo.	booleano
ora	La quantità di tempo, in secondi, in cui i dati sul volume di destinazione si trovano in ritardo rispetto ai dati sul volume di origine.	intero

Nome	Descrizione	Tipo
LastTransferDuration	La quantità di tempo in secondi necessaria per il completamento dell'ultimo trasferimento.	intero
LastTransferError	Un messaggio che descrive la causa dell'ultimo errore di trasferimento.	stringa
LastTransferSize	Il numero totale di byte trasferiti durante l'ultimo trasferimento.	intero
LastTransferEndTimestamp	Data e ora della fine dell'ultimo trasferimento.	Stringa di dati ISO 8601
LastTransferType	Il tipo di trasferimento precedente nella relazione.	stringa
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero
MirrorState	Lo stato mirror della relazione SnapMirror. Valori possibili: • uninitialized (non inizializzato): Il volume di destinazione non è stato inizializzato. • snapmirrored: Il volume di destinazione è stato inizializzato ed è pronto per ricevere gli aggiornamenti di SnapMirror. • Interrotto: Il volume di destinazione è in lettura/scrittura e sono presenti snapshot.	stringa
NewestSnapshot	Il nome della copia Snapshot più recente sul volume di destinazione.	stringa

Nome	Descrizione	Tipo
Nome criterio	Specifica il nome del criterio SnapMirror di ONTAP per la relazione. Con ListSnapMirrorPolicies è possibile recuperare un elenco di policy disponibili. I valori di esempio sono “MirrorLatest” e “MirrorAndVault”.	stringa
Tipo di criterio	Il tipo di criterio SnapMirror di ONTAP per la relazione. Vedere ListSnapMirrorPolicies. Esempi: “async_mirror” o “mirror_vault”.	stringa
RelazioniProgress	Il numero totale di byte che sono stati elaborati finora per l’attività corrente della relazione come restituito nello stato della relazione. Questa opzione viene impostata solo quando il membro "relazionshipStatus" indica che è in corso un’attività.	intero
RelazionshipStatus	Lo stato della relazione SnapMirror. Valori possibili: • inattivo • trasferimento in corso • verifica in corso • quiescing • messo in quiescenza • in coda • preparazione in corso • finalizzazione • interruzione • rompere	stringa
RelazionshipType	Il tipo di relazione di SnapMirror. Nei cluster di storage che eseguono il software Element, questo valore è sempre “Extended_data_Protection”.	stringa

Nome	Descrizione	Tipo
Nome scheduleName	Il nome della pianificazione cron preesistente sul sistema ONTAP utilizzata per aggiornare la relazione SnapMirror. È possibile recuperare un elenco di pianificazioni disponibili con ListSnapMirrorSchedules.	stringa
UnhealthyReason	Il motivo per cui il rapporto non è sano.	stringa

SnapMirrorVolume

L'oggetto SnapMirrorVolume contiene informazioni su un volume ONTAP.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
nome	Il nome del volume.	stringa
tipo	Il tipo di volume. Valori possibili: • rw: Volume di lettura/scrittura • ls: Volume di condivisione del carico • dp: Volume di protezione dei dati	stringa
server virtuale	Il nome del Vserver proprietario di questo volume.	stringa
AggrName	Il nome dell'aggregato contenente.	stringa

Nome	Descrizione	Tipo
stato	Lo stato del volume. Valori possibili: • online • limitato • offline • misto	stringa
dimensione	Dimensione totale del file system (in byte) del volume.	stringa
AvailSize	La dimensione (in byte) dello spazio disponibile nel volume.	stringa

SnapMirrorVolumeInfo

L'oggetto snapMirrorVolumeInfo contiene informazioni sulla posizione di un volume in una relazione SnapMirror, ad esempio il nome e il tipo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
tipo	Il tipo di volume. Valori possibili: • SolidFire: Il volume risiede in un cluster di storage che esegue il software Element. • ONTAP: Il volume risiede in un cluster ONTAP remoto.	stringa
ID volume	L'ID del volume. Valido solo se "tipo" è SolidFire.	intero
server virtuale	Il nome del Vserver proprietario di questo volume. Valido solo se "tipo" è ONTAP.	stringa
nome	Il nome del volume.	stringa

SnapMirrorVserver

L'oggetto snapMirrorVserver contiene informazioni sulle macchine virtuali di storage (o

Vserver) nel cluster ONTAP di destinazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
SnapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
VserverName	Il nome del Vserver.	stringa
VserverType	Il tipo di Vserver. Valori possibili: • dati • amministratore • sistema • nodo	stringa
VserverSubtype	Il sottotipo del Vserver. Valori possibili: • predefinito • dp_destination • dati • sync_source • sync_destination	stringa
Volume di rootVolume	Il volume root del Vserver.	stringa
RootVolumeAggregate	L'aggregato su cui verrà creato il volume root.	stringa
VserverAggregateInfo	Matrice di oggetti SnapMirrorVserverAggregateInfo.	Oggetto JSON

Nome	Descrizione	Tipo
AdminState	Stato amministrativo dettagliato del Vserver. Valori possibili: • in esecuzione • interrotto • in corso • in arresto • inizializzazione in corso • eliminazione in corso	stringa
OperationalState	Lo stato operativo di base del Vserver. Valori possibili: • in esecuzione • interrotto	stringa

SnapMirrorVserverAggregateInfo

L'oggetto snapMirrorVserverAggregateInfo contiene informazioni sulle macchine virtuali per lo storage dei dati disponibili (chiamate anche Vserver) nel cluster ONTAP di destinazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AggrName	Il nome dell'aggregato assegnato a un Vserver.	stringa
AggrAvailSize	Dimensione disponibile dell'aggregato assegnato.	intero

snapshot

L'oggetto snapshot contiene informazioni su uno snapshot creato per un volume. È possibile utilizzare `ListSnapshots` Metodo API per recuperare un elenco di informazioni di snapshot per un volume o per tutti i volumi. L'oggetto include informazioni sullo snapshot attivo e su ogni snapshot creato per un volume.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
checksum	Una piccola rappresentazione a stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in un secondo momento per confrontare altri snapshot al fine di rilevare errori nei dati.	stringa
CreateTime	Il tempo formattato UTC+0 per la creazione dello snapshot.	Stringa di dati ISO 8601
EnableRemoteReplication	Identifica se lo snapshot è abilitato per la replica remota.	booleano
ExpirationReason	Indica come viene impostata la scadenza dello snapshot. Valori possibili: • API: La scadenza viene impostata utilizzando l'API. • None (Nessuna): Non viene impostata alcuna scadenza. • Test: Il tempo di scadenza è impostato per il test. • fifo: La scadenza si verifica in base al principio first-in-first-out.	stringa
ExpirationTime (tempo di scadenza)	L'ora in cui lo snapshot scadrà e verrà deposto dal cluster.	Stringa di dati ISO 8601
GROUPID	L'ID del gruppo se lo snapshot è membro di uno snapshot di gruppo.	intero
GroupsnapshotUID	Contiene informazioni su ogni snapshot del gruppo. Ciascuno di questi membri disporrà di un parametro UUID per l'UUID dello snapshot.	stringa
InstanceCreateTime	L'ora in cui lo snapshot è stato creato sul cluster locale.	Stringa di dati ISO 8601

Nome	Descrizione	Tipo
InstanceSnapshotUID	ID universalmente univoco dello snapshot sul cluster locale. Questo ID non viene replicato in altri cluster.	stringa
nome	Il nome univoco assegnato allo snapshot. Se non viene specificato alcun nome, il nome corrisponde all'indicatore orario formattato UTC+0 del momento in cui è stata creata la snapshot.	stringa
RemoteStatuses	Array contenente l'identificatore universale e lo stato di replica di ogni snapshot remoto sul cluster di destinazione, come visualizzato dal cluster di origine.	RemoteClusterSnapshotStatus array
SnapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot sugli endpoint SnapMirror. Se non impostato, questo valore è nullo.	stringa
SnapshotID	L'ID univoco di uno snapshot esistente.	stringa
SnapshotUID	ID universalmente univoco di uno snapshot esistente. Quando lo snapshot viene replicato tra i cluster, questo ID viene replicato insieme a esso e viene utilizzato per identificare lo snapshot tra i cluster.	stringa

Nome	Descrizione	Tipo
stato	Stato corrente dello snapshot. Valori possibili: • Sconosciuto: Si è verificato un errore durante l'ottenimento dello stato dello snapshot. • Preparazione: Questo snapshot è in fase di preparazione e non è ancora scrivibile. • RemoteSyncing: Questo snapshot viene replicato da un cluster remoto. • Fatto: Questo snapshot ha terminato la preparazione o la replica ed è ora utilizzabile. • Attivo: Questo snapshot è il ramo attivo. • Cloning (clonazione): Questo snapshot è coinvolto in un'operazione CopyVolume.	stringa
TotalSize (dimensioni totale)	La dimensione totale in byte dello snapshot.	intero
VirtualVolumeID	L'ID del volume virtuale associato a questo snapshot.	UUID
ID volume	L'ID del volume da cui è stato creato lo snapshot.	intero
VolumeName	Il nome del volume al momento della creazione dello snapshot.	stringa

Trova ulteriori informazioni

ListSnapshot

SnmpTrapRecipient

L'oggetto snmpTrapRecipient contiene informazioni su un host configurato per ricevere trap SNMP generati dal cluster di storage. È possibile utilizzare `GetSnmpTrapInfo` Metodo API per ottenere un elenco di host configurati per ricevere trap SNMP.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
host	L'indirizzo IP o il nome host dell'host di destinazione.	stringa
porta	Il numero della porta UDP sull'host in cui deve essere inviato il trap. L'intervallo valido va da 1 a 65535. 0 (zero) non è un numero di porta valido. La porta predefinita è 162.	intero
comunità	Stringa di comunità SNMP.	stringa

StorageContainer

L'oggetto storageContainer contiene gli attributi di un container di storage di un volume virtuale. È possibile recuperare queste informazioni per ciascun container di storage nel cluster utilizzando `ListStorageContainers` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID account	L'ID dell'account del sistema di storage associato al container di storage.	intero
InitatorSecret	Segreto di autenticazione CHAP per l'iniziatore associato al contenitore di storage.	stringa
nome	Il nome del contenitore di storage.	stringa
ProtocolEndpointType	Il tipo di endpoint del protocollo del container di storage. SCSI è l'unico valore valido.	stringa
stato	Lo stato del contenitore di storage. Valori possibili: • Attivo: Il contenitore di storage è in uso. • Bloccato: Il contenitore di storage è bloccato.	stringa
StorageContainerID	ID univoco del container di storage.	UUID

Nome	Descrizione	Tipo
TargetSecret	Il segreto di autenticazione CHAP per la destinazione associata al container di storage.	stringa
VirtualVolumes	Un elenco di ID dei volumi virtuali associati al container di storage.	Array UUID

Trova ulteriori informazioni

ListStorageContainers

SyncJob

L'oggetto syncJob contiene informazioni sui processi di sincronizzazione di cloni, replica remota o slice in esecuzione su un cluster.

È possibile recuperare le informazioni di sincronizzazione con `ListSyncJobs` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
BlocksPerSecond	Il numero di blocchi di dati trasferiti al secondo dal cluster di origine al cluster di destinazione. Presente solo se il membro del tipo è impostato su remoto.	intero
Tipo di ramificazione	Restituito solo per processi di sincronizzazione della replica remota. Valori possibili: • snapshot • volume	stringa
BytesPerSecond	Il numero di byte che il clone sta elaborando al secondo. Presente solo se il membro del tipo è impostato su clone o slice.	fluttuare
ID cloneID	L'identificativo dell'operazione clone in corso. Presente solo se il membro del tipo è impostato su clone.	intero

Nome	Descrizione	Tipo
CurrentBytes	Il numero di byte elaborati dal clone nel volume di origine. Presente solo se il membro del tipo è impostato su clone o slice.	intero
DstServiceID	Identificativo del servizio che ospita la replica primaria per il volume. Presente solo se il membro del tipo è impostato su remoto.	intero
DstVolumeID	L'ID del volume di destinazione. Presente solo se il membro del tipo è impostato su clone o remoto.	intero
SedelapTime	Il tempo trascorso, in secondi, dall'avvio del processo di sincronizzazione.	float o integer a seconda del tipo di operazione di sincronizzazione
ID groupCloneID	L'ID dell'operazione di clone di gruppo in corso.	intero
ID NodeID	Specifica il nodo su cui si sta verificando il clone. Presente solo se il membro del tipo è impostato su clone.	intero
PercentComplete	La percentuale di completamento del processo di sincronizzazione.	float o integer a seconda del tipo di operazione di sincronizzazione
Tempo residuo	Il tempo stimato, in secondi, per completare l'operazione.	fluttuare
ID licenza	L'ID del disco slice in fase di sincronizzazione.	intero

Nome	Descrizione	Tipo
fase	Presente solo se il membro del tipo è impostato su remoto o clone. Valori possibili: • Metadati: La replica sta determinando quali dati devono essere trasferiti al cluster remoto. Lo stato non viene riportato per questa fase del processo di replica. • Dati: La replica sta trasferendo la maggior parte dei dati al cluster remoto. • Whole (intero): Indica la compatibilità con le versioni precedenti della sezione per i lavori di sincronizzazione della sezione.	stringa
SnapshotID	L'ID dello snapshot da cui è stato creato il clone. Presente solo se il membro del tipo è impostato su clone.	intero
SrcServiceID	L'ID del servizio di origine.	intero
SrcVolumeID	L'ID del volume di origine.	intero
TotalByte	Il numero totale di byte del clone. Presente solo se il membro del tipo è impostato su clone o slice.	intero
tipo	Il tipo di operazione di sincronizzazione. Valori possibili: • clonare • sezione • blocco • remoto	stringa

Trova ulteriori informazioni

ListSyncJobs

task (volumi virtuali)

L'oggetto task contiene informazioni su un'attività di volume virtuale attualmente in

esecuzione o completata nel sistema. È possibile utilizzare `ListVirtualVolumeTasks` metodo per recuperare queste informazioni per tutte le attività dei volumi virtuali.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
annullato	Indica se l'attività è stata annullata o meno. Valori possibili: • vero • falso	booleano
CloneVirtualVolumeID	L'ID univoco del volume virtuale del volume virtuale clonato (per le attività di clonazione).	UUID
ParentMetadata	Oggetto contenente metadati dell'oggetto padre per attività che clonano o creano snapshot di un volume virtuale.	Oggetto JSON
ParentTotalSize	Lo spazio totale disponibile (in byte) sull'origine per le attività di clone o snapshot.	intero
ParentUsedSize	Lo spazio utilizzato dall'origine (in byte) per le attività di clonazione o snapshot.	intero

Nome	Descrizione	Tipo
operazione	Il tipo di operazione che l'attività sta eseguendo. Valori possibili: • Sconosciuto: Operazione non nota. • Preparazione: L'attività sta preparando un volume virtuale. • Snapshot: L'attività sta creando uno snapshot di un volume virtuale. • Rollback: L'attività sta eseguendo il rollback di un volume virtuale in uno snapshot. • Clone: L'attività sta creando un clone del volume virtuale. • FastClone: L'attività consiste nella creazione di un clone rapido di un volume virtuale. • CopyDiff: L'attività consiste nella copia di blocchi diversi in un volume virtuale.	stringa
stato	Lo stato corrente dell'attività del volume virtuale. Valori possibili: • Errore: L'attività non è riuscita e ha restituito un errore. • Accodato: L'attività è in attesa di essere eseguita. • In esecuzione: L'attività è attualmente in esecuzione. • Operazione riuscita: L'operazione è stata completata correttamente.	stringa
VirtualVolumeHostID	L'ID univoco dell'host che ha avviato l'attività.	UUID
VirtualVolumeID	Il nuovo ID univoco del volume virtuale (per le attività che creano un nuovo volume virtuale).	UUID
VirtualVolumeTaskID	L'ID univoco dell'attività.	UUID

Trova ulteriori informazioni

ListVirtualVolumeTasks

UsmUser

È possibile utilizzare l'oggetto SNMP usmUser con `SetSnmpInfo` Metodo API per configurare SNMP nel cluster di storage.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	Il tipo di accesso SNMP per questo utente. Valori possibili: • rouser: Accesso di sola lettura. • Rwuser: Accesso in lettura/scrittura. Tutti gli oggetti MIB del software Element sono di sola lettura.	stringa
nome	Il nome dell'utente.	stringa
password	La password dell'utente.	stringa
passphrase	La passphrase dell'utente.	stringa
SecLevel	Il tipo di credenziali richieste per questo utente. Valori possibili: • Noauth: Non sono richieste password o passphrase. • Auth: Per l'accesso dell'utente è necessaria una password. • PRIV: Per l'accesso dell'utente sono richiesti password e passphrase.	stringa

Trova ulteriori informazioni

SetSnmpInfo

VirtualNetwork

L'oggetto virtualNetwork contiene informazioni su una specifica rete virtuale. È possibile utilizzare `ListVirtualNetworks` Metodo API per recuperare un elenco di queste

informazioni per tutte le reti virtuali nel sistema.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
AddressBllocks	L'intervallo di blocchi di indirizzi attualmente assegnati alla rete virtuale. Membri: • Disponibile: Stringa binaria in "1" e "0" "1" indica che l'indirizzo IP è disponibile e "0" indica che l'indirizzo IP non è disponibile. La stringa viene letta da destra a sinistra con la cifra all'estrema destra che rappresenta il primo indirizzo IP nell'elenco dei blocchi di indirizzi. • Size (dimensione): La dimensione di questo blocco di indirizzi. • Start (inizio): Il primo indirizzo IP del blocco.	Array di oggetti JSON
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
nome	Il nome assegnato alla rete virtuale.	stringa
netmask	L'indirizzo IP della netmask per la rete virtuale.	stringa
svip	L'indirizzo IP dello storage per la rete virtuale.	stringa
gateway	Gateway utilizzato per la rete virtuale.	stringa
VirtualNetworkID	Identificatore univoco di una rete virtuale.	intero
VirtualNetworkTag	L'identificatore del tag VLAN.	intero

Trova ulteriori informazioni

ListVirtualNetworks

VirtualVolume

L'oggetto virtualVolume contiene informazioni di configurazione su un volume virtuale e informazioni sugli snapshot del volume virtuale. Non include informazioni sull'utilizzo o sul runtime. È possibile utilizzare `ListVirtualVolumes` metodo per recuperare queste informazioni per un cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
associazioni	Un elenco di ID di associazione per questo volume virtuale.	Array UUID
bambini	Un elenco di UUID dei volumi virtuali figlio di questo volume virtuale.	Array UUID
discendenti	Quando si passa il metodo ricorrente: True al metodo ListVirtualVolumes, contiene un elenco di UUID di volumi virtuali che sono i discendenti di questo volume virtuale.	Array UUID
metadati	Coppie chiave-valore dei metadati del volume virtuale, come il tipo di volume virtuale, il tipo di sistema operativo guest e così via.	Oggetto JSON
ParentVirtualVolumeID	L'ID del volume virtuale del volume virtuale padre. Se l'ID è pari a zero, si tratta di un volume virtuale indipendente senza collegamento a un'origine.	UUID
SnapshotID	L'ID dello snapshot del volume sottostante. Questo valore è "0" se il volume virtuale non rappresenta uno snapshot.	intero
SnapshotInfo	Oggetto snapshot per lo snapshot associato (null se non specificato).	snapshot

Nome	Descrizione	Tipo
stato	Stato corrente del volume virtuale. Valori possibili: • Cloning: Il volume virtuale viene elaborato in risposta a un'operazione di clone o snapshot. • In attesa: Il volume virtuale è in attesa del completamento di un'operazione di snapshot. • Pronto: Il volume virtuale è pronto per l'uso generico.	stringa
StorageContainer	Oggetto che descrive il container di storage proprietario di questo volume virtuale.	StorageContainer
VirtualVolumeID	L'ID univoco del volume virtuale.	UUID
VirtualVolumeType	Il tipo di volume virtuale.	stringa
ID volume	L'ID del volume sottostante.	intero
Info volumeInfo	Quando si passa Details: True al metodo ListVirtualVolumes, questo membro è un oggetto che descrive il volume.	volume

Trova ulteriori informazioni

- ListVirtualVolumes
- snapshot
- StorageContainer
- volume

volume

L'oggetto volume contiene informazioni di configurazione sui volumi non accoppiati o accoppiati. Non include informazioni sul runtime o sull'utilizzo e non contiene informazioni sui volumi virtuali.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	Il tipo di accesso consentito per il volume. Valori possibili: • `readOnly`: Sono consentite solo operazioni di lettura. • `readWrite`: Sono consentite le letture e le scritture. • `locked`: Non sono consentite letture o scritture. • `replicationTarget`: Designato come volume di destinazione in una coppia di volumi replicati.	stringa
ID account	L'ID account dell'account contenente il volume.	intero
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
Dimensione blocco	La dimensione dei blocchi sul volume.	intero
CreateTime	L'ora in cui è stato formattato UTC+0 il volume è stato creato.	Stringa ISO 8601
CurrentProtectionScheme	Lo schema di protezione utilizzato per questo volume. Se un volume si sta convertendo da uno schema di protezione a un altro, questo membro riflette lo schema di protezione in cui il volume si sta convertendo.	stringa
Ora di deleteTime	Tempo di formattazione UTC+0 per l'eliminazione del volume.	Stringa ISO 8601
enable512e	Se impostato su true, il volume fornisce l'emulazione di settore a 512 byte.	booleano
EnableSnapMirrorReplication	Se il volume può essere utilizzato o meno per la replica con gli endpoint SnapMirror.	booleano

Nome	Descrizione	Tipo
FifoSize	Specifica il numero massimo di snapshot del volume da gestire contemporaneamente se si utilizza la modalità di conservazione degli snapshot first-in-first-out (FIFO).	intero
iqn	Nome qualificato iSCSI del volume.	stringa
LastAccessTime	L'ultima volta in cui si è verificato un qualsiasi accesso (incluso l'i/o) al volume (formattato come UTC+0). Se l'ultimo tempo di accesso non è noto, questo valore è nullo.	Stringa ISO 8601
LastAccessTimeIO	L'ultima volta in cui si è verificato un i/o nel volume (formattato come UTC+0). Se l'ultimo tempo di accesso non è noto, questo valore è nullo.	Stringa ISO 8601
MinFifoSize	Specifica il numero minimo di slot di snapshot first-in-first-out (FIFO) riservati simultaneamente dal volume se si utilizza la modalità di conservazione dello snapshot first-in-first-out (FIFO).	intero
nome	Il nome del volume fornito al momento della creazione.	stringa
PreviousProtectionScheme	Se un volume si sta convertendo da uno schema di protezione a un altro, questo membro riflette lo schema di protezione da cui il volume si sta convertendo. Questo membro non cambia fino a quando non viene avviata una conversione. Se un volume non è mai stato convertito, questo membro è nullo.	stringa
Tempo di destinazione	Il tempo di formattazione UTC+0 in cui il volume è stato spurgato dal sistema.	Stringa ISO 8601
qos	Le impostazioni relative alla qualità del servizio per questo volume.	QoS

Nome	Descrizione	Tipo
QosPolicyID	L'ID del criterio QoS associato al volume. Il valore è nullo se il volume non è associato a un criterio.	intero
ScsiEUIDeviceID	Identificatore univoco globale del dispositivo SCSI per il volume nel formato a 16 byte basato su EUI-64.	stringa
ID scsiNAADeviceID	Identificatore univoco globale del dispositivo SCSI per il volume in formato NAA IEEE Registered Extended.	stringa
SliceCount	Il numero di sezioni sul volume. Questo valore è sempre "1".	intero
stato	Lo stato corrente del volume. Valori possibili: • Init (Inizializza): Volume in fase di inizializzazione e non pronto per le connessioni. • Attivo: Un volume attivo pronto per le connessioni. • Eliminato: Volume contrassegnato per l'eliminazione, ma non ancora eliminato.	stringa
TotalSize (dimensioni totale)	Byte totali di capacità fornita.	intero
VirtualVolumeID	L'ID univoco del volume virtuale associato al volume, se presente.	UUID
VolumeAccessGroups	Elenco degli ID dei gruppi di accesso al volume pf a cui appartiene un volume. Questo valore è un elenco vuoto se un volume non appartiene ad alcun gruppo di accesso al volume.	array intero
VolumeConsistencyGroupUUID	ID universalmente univoco del gruppo di coerenza del volume di cui il volume è membro.	UUID

Nome	Descrizione	Tipo
ID volume	L'ID volume univoco per il volume.	intero
VolumePair	Informazioni su un volume associato. Visibile solo se un volume è associato. Questo valore è un elenco vuoto se il volume non è associato.	VolumePair array
VolumeUID	ID universalmente univoco del volume.	UUID

Trova ulteriori informazioni

- ListActiveVolumes
- ListDeletedVolumes
- ListVolumes
- ListVolumesForAccount
- QoS

VolumeAccessGroup

L'oggetto volumeAccessGroup contiene informazioni su uno specifico gruppo di accesso a un volume. È possibile recuperare un elenco di queste informazioni per tutti i gruppi di accesso con il metodo API `ListVolumeAccessGroups`.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
DeletedVolumes	Array di volumi che sono stati eliminati dal gruppo di accesso al volume e che non sono ancora stati rimossi dal sistema.	array intero
InitiatorID	Un elenco di ID degli iniziatori mappati al gruppo di accesso al volume.	array intero

Nome	Descrizione	Tipo
iniziatori	Array di iniziatori IQN/WWPN univoci mappati al gruppo di accesso al volume.	array di stringhe
nome	Nome del gruppo di accesso al volume.	stringa
VolumeAccessGroupID	Identificatore VolumeAccessGroupID univoco per il gruppo di accesso al volume.	intero
volumi	Un elenco di VolumeID appartenenti al gruppo di accesso al volume.	array intero

Trova ulteriori informazioni

ListVolumeAccessGroups

VolumePair

L'oggetto volumePair contiene informazioni su un volume associato a un altro volume su un cluster diverso. Se il volume non è associato, l'oggetto è vuoto. È possibile utilizzare `ListActivePairedVolumes` e. `ListActiveVolumes` Metodi API per restituire informazioni sui volumi accoppiati.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID PairID del clusterPairID	Il cluster su cui viene associato il volume.	intero

Nome	Descrizione	Tipo
Replica remota	Dettagli sulla replica dei volumi. Membri: • Mode (modalità): (Stringa) uno tra "Async", "Sync" o "SnapshotsOnly". • PauseLimit: (Intero) solo per uso interno. • RemoteServiceID: (Intero) l'ID del servizio slice remoto. • Riprendi Dettagli: (Stringa) riservato per uso futuro. • SnapshotReplication (oggetto JSON) ◦ state (stato): (Stringa) lo stato della replica dello snapshot in corso, se in corso. ◦ StateDetails: (String) riservato per uso futuro. • state (stato): (Stringa) lo stato della replica del volume. • StateDetails: (String) riservato per uso futuro.	Oggetto JSON
RemoteSliceID	L'ID dello strato definito dal cluster sul cluster remoto.	intero
RemoteVolumeID	L'ID del volume sul cluster remoto a cui è associato il volume locale.	intero
RemoteVolumeName	Il nome del volume remoto.	stringa
VolumePairUID	Identificatore universale definito dal cluster per questa associazione in formato canonico.	stringa

Trova ulteriori informazioni

- ListActivePairedVolumes
- ListActiveVolumes

VolumeStats

L'oggetto volumeStats contiene dati statistici per un singolo volume.

Membri dell'oggetto

È possibile utilizzare i seguenti metodi per ottenere oggetti volumeStats per alcuni o tutti i volumi:

- GetVolumeStats
- ListVolumeStatsByAccount
- ListVolumeStatsByVolume
- ListVolumeStatsByVolumeAccessGroup

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Calcolo	Tipo
ID account	L'ID dell'account del proprietario del volume.	N/A.	intero
AttualIOPS	Gli IOPS effettivi correnti nel volume negli ultimi 500 millisecondi.	Point-in-time	intero
AsyncDelay	Il periodo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è associato, il valore è nullo. **Nota:** Un volume di destinazione in uno stato di replica attiva ha sempre un AsyncDelay pari a 0 (zero). I volumi di destinazione sono consapevoli del sistema durante la replica e presumono che asyncDelay sia sempre preciso.	N/A.	Stringa di durata ISO 8601 o nulla
AverageIOPSize	Dimensione media in byte di i/o recente nel volume negli ultimi 500 millisecondi.	Point-in-time	intero
BurstIOPSSCredit	Il numero totale di crediti IOP disponibili per l'utente. Quando i volumi non utilizzano un massimo di maxIOPS configurati, vengono accumulati crediti.	N/A.	intero

Nome	Descrizione	Calcolo	Tipo
ClientQueueDepth	Il numero di operazioni di lettura e scrittura in sospeso nel volume.	N/A.	intero
DesiredMetadataHost	I servizi di metadati (slice) in cui viene eseguita la migrazione dei metadati del volume tra i servizi di metadati. Un valore "nullo" indica che il volume non sta migrando.	N/A.	Oggetto JSON
LatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni sul volume negli ultimi 500 millisecondi. Un valore "0" (zero) indica che non vi è alcun i/o nel volume.	Point-in-time	intero
MetadataHost	Servizi di metadati (slice) su cui risiedono i metadati del volume. Valori possibili: • Primario: I servizi di metadati primari che ospitano il volume. • LiveSecondaries: Servizi di metadati secondari che sono attualmente in stato "live". • DeadSecondaries: Servizi di metadati secondari che si trovano in uno stato morto.	N/A.	Oggetto JSON
NormalizzatoIOPS	Numero medio di IOPS per l'intero cluster negli ultimi 500 millisecondi.	Point-in-time	intero
Non ZeroBIlocks	Il numero totale di blocchi 4KiB che contengono dati dopo il completamento dell'ultima operazione di garbage collection.	N/A.	intero

Nome	Descrizione	Calcolo	Tipo
ReadByte	I byte cumulativi totali letti dal volume dalla creazione del volume.	In aumento monotono	intero
ReadBytesLastSample	Il numero totale di byte letti dal volume durante l'ultimo periodo di campionamento.	Point-in-time	intero
ReadLatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.	Point-in-time	intero
ReadLatencyUSecTotal	Il tempo totale impiegato per le operazioni di lettura dal volume.	In aumento monotono	intero
ReadOps	Operazioni di lettura totali nel volume dalla creazione del volume.	In aumento monotono	intero
ReadOpsLastSample	Il numero totale di operazioni di lettura durante l'ultimo periodo di campionamento.	Point-in-time	intero
SamplePeriodMsec	La durata del periodo di campionamento, in millisecondi.	N/A.	intero
acceleratore	Un valore fluttuante compreso tra 0 e 1 che rappresenta quanto il sistema sta rallentando i client al di sotto dei massimi IOPS a causa della replica dei dati, degli errori transitori e degli snapshot acquisiti.	N/A.	fluttuare
data e ora	L'ora corrente nel formato UTC+0.	N/A.	Stringa di dati ISO 8601

Nome	Descrizione	Calcolo	Tipo
UnalignedReads	Operazioni di lettura cumulative non allineate per un volume dalla creazione del volume.	In aumento monotono	intero
UnalignedWrites	Operazioni di scrittura cumulative non allineate su un volume dopo la creazione del volume.	In aumento monotono	intero
VolumeAccessGroups	L'elenco degli ID dei gruppi di accesso ai volumi a cui appartiene un volume.	N/A.	array intero
ID volume	L'ID del volume.	N/A.	intero
VolumeDimensioni	Capacità totale fornita in byte.	N/A.	intero

Nome	Descrizione	Calcolo	Tipo
VolumeUtilization	Un valore in virgola mobile che descrive il modo in cui il client utilizza appieno le funzionalità di input/output del volume rispetto all'impostazione di maxIOPS QoS per quel volume. Valori possibili: • 0: Il client non sta utilizzando il volume. • Da 0.01 a 0.99: Il client non utilizza completamente le funzionalità IOPS del volume. • 1.00: Il client sta utilizzando completamente il volume fino al limite IOPS impostato dall'impostazione maxIOPS. • > 1.00: Il client sta utilizzando più del limite impostato da maxIOPS. Ciò è possibile quando l'impostazione burstIOPS QoS è superiore a maxIOPS. Ad esempio, se maxIOPS è impostato su 1000 e burstIOPS è impostato su 2000, il `volumeUtilization` il valore sarebbe 2.00 se il client utilizza completamente il volume.	N/A.	fluttuare
WriteByte	I byte cumulativi totali scritti nel volume dalla creazione del volume.	In aumento monotono	intero

Nome	Descrizione	Calcolo	Tipo
WriteBytesLastSample	Il numero totale di byte scritti nel volume durante l'ultimo periodo di esempio.	In aumento monotono	intero
ScriveLatencyUSec	Il tempo medio, in microsecondi, per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.	Point-in-time	intero
SwriteLatencyUSecTotal	Il tempo totale impiegato per eseguire operazioni di scrittura sul volume.	In aumento monotono	intero
SwriteOps	Operazioni di scrittura cumulative totali nel volume dalla creazione del volume.	In aumento monotono	intero
SwriteOpsLastSample	Il numero totale di operazioni di scrittura durante l'ultimo periodo di esempio.	Point-in-time	intero
Zero-blocks	Il numero totale di blocchi 4KiB vuoti senza dati dopo il completamento dell'ultimo round dell'operazione di garbage collection.	Point-in-time	intero

Metodi comuni

I metodi comuni sono metodi utilizzati per recuperare informazioni sul cluster di storage, l'API stessa o le operazioni API in corso.

- GetAPI
- GetAsyncResult
- GetCompleteStats
- GetLimits
- GetOrigin
- GetRawStats
- ListAsyncResults

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetAPI

È possibile utilizzare `GetAPI` Metodo per ottenere un elenco di tutti i metodi API e gli endpoint API supportati che possono essere utilizzati nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
<version>	Un elenco di tutti i metodi API supportati per questa versione del software, dove <version> è la versione corrente del software in esecuzione nel sistema.	array di stringhe
CurrentVersion (versione attuale)	La versione corrente del software del cluster di storage.	stringa
SupportedVersioni	Un elenco di tutti gli endpoint API supportati dal sistema.	array di stringhe

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetAPI",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
```

```
    "result": {
        "12.0": [
            "AbortSnapMirrorRelationship",
            "AddAccount",
            "AddClusterAdmin",
            "AddDrives",
            "AddIdpClusterAdmin",
            "AddInitiatorsToVolumeAccessGroup",
            "AddKeyServerToProviderKmip",
            "AddLdapClusterAdmin",
            "AddNodes",
            "AddVirtualNetwork",
            "AddVolumesToVolumeAccessGroup",
            "BreakSnapMirrorRelationship",
            "BreakSnapMirrorVolume",
            "CancelClone",
            "CancelGroupClone",
            "CheckPingOnVlan",
            "CheckProposedCluster",
            "CheckProposedNodeAdditions",
            "ClearClusterFaults",
            "CloneMultipleVolumes",
            "CloneVolume",
            "CompleteClusterPairing",
            "CompleteVolumePairing",
            "CopyVolume",
            "CreateBackupTarget",
            "CreateClusterInterfacePreference",
            "CreateClusterSupportBundle",
            "CreateGroupSnapshot",
            "CreateIdpConfiguration",
            "CreateInitiators",
            "CreateKeyProviderKmip",
            "CreateKeyServerKmip",
            "CreatePublicPrivateKeyPair",
            "CreateQoSPolicy",
            "CreateSchedule",
            "CreateSnapMirrorEndpoint",
            "CreateSnapMirrorEndpointUnmanaged",
            "CreateSnapMirrorRelationship",
            "CreateSnapMirrorVolume",
            "CreateSnapshot",
            "CreateStorageContainer",
            "CreateSupportBundle",
            "CreateVolume",
            "CreateVolumeAccessGroup",
```

```
            "DeleteAllSupportBundles",
            "DeleteAuthSession",
            "DeleteAuthSessionsByClusterAdmin",
            "DeleteAuthSessionsByUsername",
            "DeleteClusterInterfacePreference",
            "DeleteGroupSnapshot",
            "DeleteIdpConfiguration",
            "DeleteInitiators",
            "DeleteKeyProviderKmip",
            "DeleteKeyServerKmip",
            "DeleteQoSPolicy",
            "DeleteSnapMirrorEndpoints",
            "DeleteSnapMirrorRelationships",
            "DeleteSnapshot",
            "DeleteStorageContainers",
            "DeleteVolume",
            "DeleteVolumeAccessGroup",
            "DeleteVolumes",
            "DisableAutoip",
            "DisableBmcColdReset",
            "DisableClusterSsh",
            "DisableEncryptionAtRest",
            "DisableIdpAuthentication",
            "DisableLdapAuthentication",
            "DisableSnmp",
            "EnableAutoip",
            "EnableBmcColdReset",
            "EnableClusterSsh",
            "EnableEncryptionAtRest",
            "EnableFeature",
            "EnableIdpAuthentication",
            "EnableLdapAuthentication",
            "EnableSnmp",
            "GetAccountByID",
            "GetAccountByName",
            "GetAccountEfficiency",
            "GetActiveTlsCiphers",
            "GetAsyncResult",
            "GetBackupTarget",
            "GetBinAssignmentProperties",
            "GetClientCertificateSignRequest",
            "GetClusterCapacity",
            "GetClusterConfig",
            "GetClusterFullThreshold",
            "GetClusterHardwareInfo",
            "GetClusterInfo",
```

```
            "GetClusterInterfacePreference",
            "GetClusterMasterNodeID",
            "GetClusterSshInfo",
            "GetClusterState",
            "GetClusterStats",
            "GetClusterStructure",
            "GetClusterVersionInfo",
            "GetCompleteStats",
            "GetConfig",
            "GetCurrentClusterAdmin",
            "GetDefaultQoS",
            "GetDriveHardwareInfo",
            "GetDriveStats",
            "GetFeatureStatus",
            "GetFipsReport",
            "GetHardwareConfig",
            "GetHardwareInfo",
            "GetIdpAuthenticationState",
            "GetIpmiConfig",
            "GetIpmiInfo",
            "GetKeyProviderKmip",
            "GetKeyServerKmip",
            "GetLdapConfiguration",
            "GetLimits",
            "GetLldpInfo",
            "GetLoginBanner",
            "GetLoginSessionInfo",
            "GetNetworkConfig",
            "GetNetworkInterface",
            "GetNodeFipsDrivesReport",
            "GetNodeHardwareInfo",
            "GetNodeStats",
            "GetNtpInfo",
            "GetNvramInfo",
            "GetOntapVersionInfo",
            "GetOrigin",
            "GetPendingOperation",
            "GetProtectionDomainLayout",
            "GetQoSPolicy",
            "GetRawStats",
            "GetRemoteLoggingHosts",
            "GetSSLCertificate",
            "GetSchedule",
            "GetSnapMirrorClusterIdentity",
            "GetSnmpACL",
            "GetSnmpInfo",
```

```
            "GetSnmpState",
            "GetSnmpTrapInfo",
            "GetStorageContainerEfficiency",
            "GetSupportedTlsCiphers",
            "GetSystemStatus",
            "GetVirtualVolumeCount",
            "GetVolumeAccessGroupEfficiency",
            "GetVolumeAccessGroupLunAssignments",
            "GetVolumeCount",
            "GetVolumeEfficiency",
            "GetVolumeStats",
            "InitializeSnapMirrorRelationship",
            "ListAccounts",
            "ListActiveAuthSessions",
            "ListActiveNodes",
            "ListActivePairedVolumes",
            "ListActiveVolumes",
            "ListAllNodes",
            "ListAsyncResults",
            "ListAuthSessionsByClusterAdmin",
            "ListAuthSessionsByUsername",
            "ListBackupTargets",
            "ListBulkVolumeJobs",
            "ListClusterAdmins",
            "ListClusterFaults",
            "ListClusterInterfacePreferences",
            "ListClusterPairs",
            "ListDeletedVolumes",
            "ListDriveHardware",
            "ListDriveStats",
            "ListDrives",
            "ListEvents",
            "ListFibreChannelPortInfo",
            "ListFibreChannelSessions",
            "ListGroupSnapshots",
            "ListISCSISessions",
            "ListIdpConfigurations",
            "ListInitiators",
            "ListKeyProvidersKmip",
            "ListKeyServersKmip",
            "ListNetworkInterfaces",
            "ListNodeFibreChannelPortInfo",
            "ListNodeStats",
            "ListPendingActiveNodes",
            "ListPendingNodes",
            "ListProtectionDomainLevels",
```

```
            "ListProtocolEndpoints",
            "ListQoSPolicies",
            "ListSchedules",
            "ListServices",
            "ListSnapMirrorAggregates",
            "ListSnapMirrorEndpoints",
            "ListSnapMirrorLuns",
            "ListSnapMirrorNetworkInterfaces",
            "ListSnapMirrorNodes",
            "ListSnapMirrorPolicies",
            "ListSnapMirrorRelationships",
            "ListSnapMirrorSchedules",
            "ListSnapMirrorVolumes",
            "ListSnapMirrorVservers",
            "ListSnapshots",
            "ListStorageContainers",
            "ListSyncJobs",
            "ListTests",
            "ListUtilities",
            "ListVirtualNetworks",
            "ListVirtualVolumeBindings",
            "ListVirtualVolumeHosts",
            "ListVirtualVolumeTasks",
            "ListVirtualVolumes",
            "ListVolumeAccessGroups",
            "ListVolumeStats",
            "ListVolumeStatsByAccount",
            "ListVolumeStatsByVirtualVolume",
            "ListVolumeStatsByVolume",
            "ListVolumeStatsByVolumeAccessGroup",
            "ListVolumes",
            "ListVolumesForAccount",
            "ModifyAccount",
            "ModifyBackupTarget",
            "ModifyClusterAdmin",
            "ModifyClusterFullThreshold",
            "ModifyClusterInterfacePreference",
            "ModifyGroupSnapshot",
            "ModifyInitiators",
            "ModifyKeyServerKmip",
            "ModifyQoSPolicy",
            "ModifySchedule",
            "ModifySnapMirrorEndpoint",
            "ModifySnapMirrorEndpointUnmanaged",
            "ModifySnapMirrorRelationship",
            "ModifySnapshot",
```

```
            "ModifyStorageContainer",
            "ModifyVirtualNetwork",
            "ModifyVolume",
            "ModifyVolumeAccessGroup",
            "ModifyVolumeAccessGroupLunAssignments",
            "ModifyVolumePair",
            "ModifyVolumes",
            "PurgeDeletedVolume",
            "PurgeDeletedVolumes",
            "QuiesceSnapMirrorRelationship",
            "RemoveAccount",
            "RemoveBackupTarget",
            "RemoveClusterAdmin",
            "RemoveClusterPair",
            "RemoveDrives",
            "RemoveInitiatorsFromVolumeAccessGroup",
            "RemoveKeyServerFromProviderKmip",
            "RemoveNodes",
            "RemoveSSLCertificate",
            "RemoveVirtualNetwork",
            "RemoveVolumePair",
            "RemoveVolumesFromVolumeAccessGroup",
            "ResetDrives",
            "ResetNetworkConfig",
            "ResetNode",
            "ResetSupplementalTlsCiphers",
            "RestartNetworking",
            "RestartServices",
            "RestoreDeletedVolume",
            "ResumeSnapMirrorRelationship",
            "ResyncSnapMirrorRelationship",
            "RollbackToGroupSnapshot",
            "RollbackToSnapshot",
            "SecureEraseDrives",
            "SetClusterConfig",
            "SetClusterStructure",
            "SetConfig",
            "SetDefaultQoS",
            "SetLoginBanner",
            "SetLoginSessionInfo",
            "SetNetworkConfig",
            "SetNtpInfo",
            "SetProtectionDomainLayout",
            "SetRemoteLoggingHosts",
            "SetSSLCertificate",
            "SetSnmpACL",
```

```
            "SetSnmpInfo",
            "SetSnmpTrapInfo",
            "SetSupplementalTlsCiphers",
            "Shutdown",
            "SnmpSendTestTraps",
            "StartBulkVolumeRead",
            "StartBulkVolumeWrite",
            "StartClusterPairing",
            "StartVolumePairing",
            "TestAddressAvailability",
            "TestConnectEnsemble",
            "TestConnectMvip",
            "TestConnectSvip",
            "TestDrives",
            "TestHardwareConfig",
            "TestKeyProviderKmip",
            "TestKeyServerKmip",
            "TestLdapAuthentication",
            "TestLocalConnectivity",
            "TestLocateCluster",
            "TestNetworkConfig",
            "TestPing",
            "TestRemoteConnectivity",
            "UpdateBulkVolumeStatus",
            "UpdateIdpConfiguration",
            "UpdateSnapMirrorRelationship"
        ],
        "currentVersion": "12.0",
        "supportedVersions": [
            "1.0",
            "2.0",
            "3.0",
            "4.0",
            "5.0",
            "5.1",
            "6.0",
            "7.0",
            "7.1",
            "7.2",
            "7.3",
            "7.4",
            "8.0",
            "8.1",
            "8.2",
            "8.3",
            "8.4",
```

```
            "8.5",
            "8.6",
            "8.7",
            "9.0",
            "9.1",
            "9.2",
            "9.3",
            "9.4",
            "9.5",
            "9.6",
            "10.0",
            "10.1",
            "10.2",
            "10.3",
            "10.4",
            "10.5",
            "10.6",
            "10.7",
            "11.0",
            "11.1",
            "11.3",
            "11.5",
            "11.7",
            "11.8",
            "12.0"
        ]
    }
}
```

GetAsyncResult

È possibile utilizzare `GetAsyncResult` per recuperare il risultato delle chiamate asincrone ai metodi. Alcune chiamate ai metodi richiedono un certo tempo per essere eseguite e potrebbero non essere completate quando il sistema invia la risposta iniziale. Per ottenere lo stato o il risultato della chiamata al metodo, utilizzare `GetAsyncResult` Per eseguire il polling del valore asyncHandle restituito dal metodo.

`GetAsyncResult` restituisce lo stato generale dell'operazione (in corso, completata o errore) in modo standard, ma i dati effettivi restituiti per l'operazione dipendono dalla chiamata al metodo originale e i dati restituiti sono documentati con ciascun metodo.

Se il parametro keepResult è mancante o falso, asyncHandle diventa inattivo quando viene restituito il risultato e in seguito tenta di eseguire una query su asyncHandle restituisce un errore. È possibile mantenere attivo asyncHandle per le query future impostando il parametro keepResult su true.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AsyncHandle	Valore restituito dalla chiamata al metodo asincrono originale.	intero	Nessuno	Sì
KeepResult	Se true, GetAsyncResult non rimuove il risultato asincrono al momento della restituzione, abilitando le query future a quell'asyncHandle.	booleano	falso	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
stato	Stato della chiamata asincrona al metodo. Valori possibili: • In esecuzione: Il metodo è ancora in esecuzione. • Complete (completo): Il metodo è completo e il risultato o l'errore sono disponibili.	stringa
risultato	Se il metodo asincrono viene completato correttamente, questo è il risultato dell'operazione asincrona. Se l'operazione asincrona non riesce, questo membro non è presente.	stringa
errore	Se lo stato è completo e il metodo asincrono non è riuscito, questo membro include i dettagli dell'errore. Se l'operazione asincrona ha avuto esito negativo, questo membro non è presente.	stringa

Nome	Descrizione	Tipo
ResultType	Il tipo di operazione che la chiamata asincrona al metodo sta eseguendo o stava eseguendo.	stringa
dettagli	Se lo stato è in esecuzione, questo membro include informazioni relative all'operazione corrente del metodo. Se il metodo asincrono non è in esecuzione, questo membro non è presente.	Oggetto JSON
CreateTime	L'ora in cui è stato chiamato il metodo asincrono, in formato UTC+0.	Stringa di dati ISO 8601
LastUpdateTime	L'ora dell'ultimo aggiornamento dello stato del metodo asincrono, in formato UTC+0.	Stringa di dati ISO 8601

Nota: il valore restituito di GetAsyncResult è essenzialmente una versione nidificata della risposta JSON standard con un campo di stato aggiuntivo.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetAsyncResult",
  "params": {
      "asyncHandle" : 389
},
"id" : 1
}
```

Esempio di risposta: Errore di metodo

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "error": {
      "code": 500,
      "message": "DBClient operation requested on a non-existent path at
[/asyncresults/1]",
      "name": "xDBNoSuchPath"
   },
   "id": 1
}
```

Se "Response" fosse l'oggetto di risposta JSON dalla chiamata GetAsyncResult, "Response.error" corrisponderebbe a un errore con il metodo GetAsyncResult stesso (ad esempio, l'esecuzione di query su un'asyncHandle non esistente).

Esempio di risposta: Errore di task asincrono

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "createTime": "2016-01-01T02:05:53Z",
     "error": {
       "bvID": 1,
       "message": "Bulk volume job failed",
       "name": "xBulkVolumeScriptFailure",
       "volumeID": 34
     },
     "lastUpdateTime": "2016-01-21T02:06:56Z",
     "resultType": "BulkVolume",
     "status": "complete"
   }
}
```

"respusse.Result.error" corrisponde a un risultato di errore della chiamata al metodo originale.

Esempio di risposta: Operazione asincrona riuscita

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "createTime": "2016-01-01T22:29:18Z",
     "lastUpdateTime": "2016-01-01T22:45:51Z",
     "result": {
       "cloneID": 25,
       "message": "Clone complete.",
       "volumeID": 47
     },
     "resultType": "Clone",
     "status": "complete"
   }
}
```

“respusse.Result.Result” è il valore restituito per la chiamata al metodo originale se la chiamata è stata completata correttamente.

Novità dalla versione

9.6

GetCompleteStats

I tecnici NetApp utilizzano `GetCompleteStats` Metodo API per testare le nuove funzionalità. I dati restituiti da `GetCompleteStats` non è documentato, cambia frequentemente e non è garantito che sia accurato. Non utilizzare `GetCompleteStats` Per la raccolta di dati sulle performance o qualsiasi altra integrazione di gestione con un cluster di storage che esegue software Element.

Utilizzare i seguenti metodi API supportati per recuperare le informazioni statistiche:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Novità dalla versione

9.6

GetLimits

È possibile utilizzare `GetLimits` Metodo per ottenere i valori limite impostati dall’API. Questi valori potrebbero cambiare tra una release e l’altra di Element, ma non cambiano senza un aggiornamento del sistema. Conoscere i valori limite impostati dall’API può

essere utile quando si scrivono script API per strumenti rivolti all'utente.

Il `GetLimits` Method restituisce i limiti per la versione software corrente indipendentemente dalla versione dell'endpoint API utilizzata per passare il metodo.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo restituisce un oggetto JSON con coppie nome-valore contenenti i limiti API.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetLimits",
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "accountCountMax": 5000,
        "accountNameLengthMax": 64,
        "accountNameLengthMin": 1,
        "backupTargetNameLengthMax": 64,
        "backupTargetNameLengthMin": 1,
        "bulkVolumeJobsPerNodeMax": 8,
        "bulkVolumeJobsPerVolumeMax": 2,
        "chapCredentialsCountMax": 15000,
        "cloneJobsPerNodeMax": 8,
        "cloneJobsPerVirtualVolumeMax": 8,
        "cloneJobsPerVolumeMax": 2,
        "clusterAdminAccountMax": 5000,
        "clusterAdminInfoNameLengthMax": 1024,
        "clusterAdminInfoNameLengthMin": 1,
        "clusterPairsCountMax": 4,
        "fibreChannelVolumeAccessMax": 16384,
        "initiatorAliasLengthMax": 224,
        "initiatorCountMax": 10000,
```

```
        "initiatorNameLengthMax": 224,
        "initiatorsPerVolumeAccessGroupCountMax": 128,
        "iscsiSessionsFromFibreChannelNodesMax": 4096,
        "maxAuthSessionsForCluster": 1024,
        "maxAuthSessionsPerUser": 1024,
        "nodesPerClusterCountMax": 100,
        "nodesPerClusterCountMin": 3,
        "qosPolicyCountMax": 500,
        "qosPolicyNameLengthMax": 64,
        "qosPolicyNameLengthMin": 1,
        "scheduleNameLengthMax": 244,
        "secretLengthMax": 16,
        "secretLengthMin": 12,
        "snapMirrorEndpointIPAddressesCountMax": 64,
        "snapMirrorEndpointsCountMax": 4,
        "snapMirrorLabelLengthMax": 31,
        "snapMirrorObjectAttributeValueInfoCountMax": 9900000,
        "snapshotNameLengthMax": 255,
        "snapshotsPerVolumeMax": 32,
        "storageNodesPerClusterCountMin": 2,
        "virtualVolumeCountMax": 8000,
        "virtualVolumesPerAccountCountMax": 10000,
        "volumeAccessGroupCountMax": 1000,
        "volumeAccessGroupLunMax": 16383,
        "volumeAccessGroupNameLengthMax": 64,
        "volumeAccessGroupNameLengthMin": 1,
        "volumeAccessGroupsPerInitiatorCountMax": 1,
        "volumeAccessGroupsPerVolumeCountMax": 64,
        "volumeBurstIOPSMax": 200000,
        "volumeBurstIOPSMin": 100,
        "volumeCountMax": 4000,
        "volumeMaxIOPSMax": 200000,
        "volumeMaxIOPSMin": 100,
        "volumeMinIOPSMax": 15000,
        "volumeMinIOPSMin": 50,
        "volumeNameLengthMax": 64,
        "volumeNameLengthMin": 1,
        "volumeSizeMax": 17592186044416,
        "volumeSizeMin": 1000000000,
        "volumesPerAccountCountMax": 2000,
        "volumesPerGroupSnapshotMax": 32,
        "volumesPerVolumeAccessGroupCountMax": 2000,
        "witnessNodesPerClusterCountMax": 4
    }
}
```

Novità dalla versione

9.6

GetOrigin

È possibile utilizzare `GetOrigin` metodo per ottenere il certificato di origine per il punto in cui è stato creato il nodo.

Parametri

Questo metodo restituisce "null" se non esiste una certificazione di origine.

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo restituisce le informazioni sulla certificazione di origine del vendor.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
 "method": "GetOrigin",
 "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "integrator": "SolidFire",
  "<signature>": {
    "pubkey": [public key info],
    "version": 1,
    "data": [signature info]
  },
   "contract-id": "none",
   "location": "Boulder, CO",
   "organization": "Engineering",
   "type": "element-x"
  }
 ]
}
```

Novità dalla versione

9.6

GetRawStats

I tecnici NetApp utilizzano `GetRawStats` Metodo API per testare le nuove funzionalità. I dati restituiti da `GetRawStats` non è documentato, cambia frequentemente e non è garantito che sia accurato. Non utilizzare `GetRawStats` Per la raccolta di dati sulle performance o qualsiasi altra integrazione di gestione con un cluster di storage che esegue software Element.

Utilizzare i seguenti metodi API supportati per recuperare le informazioni statistiche:

- GetVolumeStats
- GetClusterStats
- GetNodeStats
- GetDriveStats

Novità dalla versione

9.6

ListAsyncResults

È possibile utilizzare `ListAsyncResults` elencare i risultati di tutti i metodi asincroni attualmente in esecuzione e completati nel sistema. Query dei risultati asincroni con `ListAsyncResults` Non provoca la scadenza di asyncHandle completati; è possibile utilizzare `GetAsyncResult` Per eseguire una query su uno qualsiasi degli asyncHandle restituiti da `ListAsyncResults`.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AsyncResultTypes	Un elenco facoltativo di tipi di risultati. È possibile utilizzare questo elenco per limitare i risultati solo a questi tipi di operazioni. Valori possibili: • DriveAdd: Operazioni che comportano l'aggiunta di un disco al cluster da parte del sistema. • BulkVolume: Operazioni di copia tra volumi, come backup o ripristini. • Clone: Operazioni di cloning del volume. • DriveRemoval (Rimozione unità): Operazioni che coinvolgono il sistema durante la copia dei dati da un disco in preparazione alla rimozione dal cluster. • RtfiPendingNode: Operazioni che coinvolgono il sistema installando software compatibile su un nodo prima di aggiungerlo al cluster.	array di stringhe	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
AsyncHandles	Risultato di un array di metodi asincroni serializzati.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListAsyncResults",
   "params": {
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "asyncHandles": [
       {
         "asyncResultID": 47,
         "completed": true,
         "createTime": "2016-01-01T22:29:19Z",
         "data": {
           "cloneID": 26,
           "message": "Clone complete.",
           "volumeID": 48
         },
         "lastUpdateTime": "2016-01-01T22:45:43Z",
         "resultType": "Clone",
         "success": true
      },
      ...]
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

GetAsyncResult

Metodi API dell'account

I metodi account consentono di aggiungere, rimuovere, visualizzare e modificare le informazioni relative all'account e alla sicurezza.

- AddAccount
- GetAccountByID
- GetAccountByName
- GetAccountEfficiency
- ListAccounts
- ModifyAccount
- RemoveAccount

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddAccount

È possibile utilizzare `AddAccount` per aggiungere un nuovo account al sistema. È inoltre possibile utilizzare questo metodo per creare nuovi volumi con il nuovo account durante la creazione dell'account. Le impostazioni CHAP (Challenge-Handshake Authentication Protocol) specificate per l'account si applicano a tutti i volumi di proprietà dell'account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`attributes`	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`enableChap`	Specifica se le credenziali dell'account CHAP possono essere utilizzate da un iniziatore per accedere ai volumi.	booleano	vero	No
`initiatorSecret`	Il segreto CHAP da utilizzare per l'iniziatore. Questo segreto deve avere una lunghezza compresa tra 12 e 16 caratteri e deve essere impenetrabile. Il segreto CHAP iniziatore deve essere univoco e non può essere lo stesso del segreto CHAP di destinazione. Se non specificato, viene creato un segreto casuale.	stringa	Nessuno	No
`targetSecret`	Il segreto CHAP da utilizzare per la destinazione (autenticazione CHAP reciproca). Questo segreto deve avere una lunghezza compresa tra 12 e 16 caratteri e deve essere impenetrabile. Il segreto CHAP di destinazione deve essere univoco e non può essere lo stesso del segreto CHAP iniziatore. Se non specificato, viene creato un segreto casuale.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
username	Il nome utente univoco per questo account. (La lunghezza deve essere compresa tra 1 e 64 caratteri).	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
account	Oggetto contenente informazioni sull'account appena creato.	account
ID account	L'ID dell'oggetto account appena creato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "AddAccount",
    "params": {
     "username"  : "bobsmith",
     "initiatorSecret" : "168[#5A757ru268)",
     "targetSecret" : "tlt&lt;,8TUYa7bC",
     "attributes" : {
       "billingcode" : 2345
     }
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "account": {
      "accountID": 90,
      "attributes": {
        "billingcode": 2345
      },
      "initiatorSecret": "168[#5A757ru268)",
      "status": "active",
      "storageContainerID": "00000000-0000-0000-0000-000000000000",
      "targetSecret": "tlt&lt;,8TUYa7bC",
      "username": "bobsmith",
      "volumes": [],
      "enableChap": true
    },
    "accountID": 90
  }
}
```


Novità dalla versione

9.6

GetAccountByID

È possibile utilizzare `GetAccountByID` Per ottenere dettagli su un account specifico, dato il relativo ID account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID account	L'ID account dell'account per il quale ottenere informazioni.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
account	Dettagli dell'account.	account

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetAccountByID",
   "params": {
     "accountID"  : 3
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "account": {
        "attributes": {},
        "username": "account3",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 3,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Novità dalla versione

9.6

GetAccountByName

È possibile utilizzare `GetAccountByName` per ottenere dettagli su un account specifico, dato il suo nome utente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome utente	Nome utente dell'account.	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
account	Dettagli dell'account.	account

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetAccountByName",
   "params": {
     "username"  : "jimmyd"
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "account": {
        "attributes": {},
        "username": "jimmyd",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 1,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
}
```

Novità dalla versione

9.6

GetAccountEfficiency

È possibile utilizzare `GetAccountEfficiency` per ottenere statistiche sull'efficienza di un account volume. Questo metodo restituisce le informazioni di efficienza solo per l'account fornito come parametro.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID account	Specifica l'account del volume per il quale vengono restituite le statistiche di efficienza.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
compressione	La quantità di spazio salvata dalla compressione dei dati per tutti i volumi dell'account. Indicato come rapporto in cui il valore "1" indica che i dati sono stati memorizzati senza compressione.	fluttuare
deduplica	La quantità di spazio risparmiata non duplicando i dati per tutti i volumi nell'account. Indicato come rapporto.	fluttuare
MissingVolumes	I volumi che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati dal ciclo di Garbage Collection (GC) che ha meno di un'ora, dalla perdita temporanea della connettività di rete o dal riavvio dei servizi dal ciclo GC.	array intero

Nome	Descrizione	Tipo
ThinProvisioning	Il rapporto tra lo spazio utilizzato e la quantità di spazio allocato per la memorizzazione dei dati. Indicato come rapporto.	fluttuare
data e ora	L'ultima volta che i dati di efficienza sono stati raccolti dopo la Garbage Collection (GC), in formato UTC+0.	Stringa di dati ISO 8601

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetAccountEfficiency",
   "params": {
     "accountID": 3
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
       "compression": 2.020468042933262,
       "deduplication": 2.042488619119879,
       "missingVolumes": [],
       "thinProvisioning": 1.010087163391013,
       "timestamp": "2014-03-10T14:06:02Z"
   }
}
```

Novità dalla versione

9.6

ListAccounts

È possibile utilizzare `ListAccounts` per ottenere l'intero elenco degli account del tenant di storage, con supporto paging opzionale. Gli account Element consentono l'accesso ai

volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include StorageContainers	I container di storage dei volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i contenitori di storage, impostare su false.	booleano	vero	No
StartAccountID	Inizio AccountID per la restituzione. Se non esiste alcun account con questo ID account, l'account successivo per ordine ID account viene utilizzato come inizio dell'elenco. Per scorrere l'elenco, passare l'ID account dell'ultimo account nella risposta precedente + 1.	intero	Nessuno	No
limite	Numero massimo di oggetti account da restituire.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
account	L'elenco degli account.	account array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListAccounts",
   "params": {
     "startAccountID"  : 0,
     "limit" : 1000
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "result" : {
    "accounts": [
    {
        "attributes": {},
        "username": "jamesw",
        "targetSecret": "168#5A757ru268)",
        "volumes": [],
        "enableChap": false,
        "status": "active",
        "accountID": 16,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "168#5A757ru268)"
    },
    {
        "attributes": {},
        "username": "jimmyd",
        "targetSecret": "targetsecret",
        "volumes": [],
        "enableChap": true,
        "status": "active",
        "accountID": 5,
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "initiatorSecret": "initiatorsecret"
    }
  ]
}
}
```

Novità dalla versione

9.6

ModifyAccount

È possibile utilizzare `ModifyAccount` metodo per modificare un account esistente.

Quando si blocca un account, tutte le connessioni esistenti da tale account vengono immediatamente interrotte. Quando si modificano le impostazioni CHAP di un account, tutte le connessioni esistenti rimangono attive e le nuove impostazioni CHAP vengono utilizzate per le connessioni o le riconnessione successive. Per cancellare gli attributi di un account, specificare {} come parametro degli attributi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID account	AccountID dell'account da modificare.	intero	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
EnableChap	Specifica se le credenziali dell'account CHAP possono essere utilizzate da un iniziatore per accedere ai volumi.	booleano	Nessuno	No
InitatorSecret	Il segreto CHAP da utilizzare per l'iniziatore. Questo segreto deve essere di 12-16 caratteri e deve essere impenetrabile. Il segreto CHAP iniziatore deve essere univoco e non può essere lo stesso del segreto CHAP di destinazione.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
stato	Stato dell'account. Valori possibili: • Attivo: L'account è attivo e le connessioni sono consentite. • Bloccato: L'account è bloccato e le connessioni vengono rifiutate.	stringa	Nessuno	No
TargetSecret	Il segreto CHAP da utilizzare per la destinazione (autenticazione CHAP reciproca). Questo segreto deve essere di 12-16 caratteri e deve essere impenetrabile. Il segreto CHAP di destinazione deve essere univoco e non può essere lo stesso del segreto CHAP iniziatore.	stringa	Nessuno	No
nome utente	Consente di modificare il nome utente associato all'account. (La lunghezza deve essere compresa tra 1 e 64 caratteri).	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
account	Oggetto contenente informazioni sull'account modificato.	account

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente. In questo esempio, gli attributi vengono cancellati specificando {}:

```
{
   "method": "ModifyAccount",
   "params": {
     "accountID"  : 25,
     "status"   : "locked",
     "attributes" : {}
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "account": {
        "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
        "username": "user1",
        "accountID": 1,
        "volumes": [
        ],
        "enableChap": true,
        "initiatorSecret": "txz123456q890",
        "attributes": {
        },
        "status": active",
        "targetSecret": "rxe123b567890"
    }
}
```

Novità dalla versione

9.6

RemoveAccount

È possibile utilizzare `RemoveAccount` metodo per rimuovere un account esistente. È necessario eliminare ed eliminare tutti i volumi associati all'account utilizzando `DeleteVolume` prima di rimuovere l'account. Se i volumi dell'account sono ancora in attesa di eliminazione, non è possibile utilizzare `RemoveAccount` per rimuovere

l'account.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID account	L'ID dell'account da rimuovere.	intero	Nessuno	Sì

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente.

```
{
   "method": "RemoveAccount",
   "params": {
     "accountID"  : 25
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id" : 1,
 "result" : { }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

DeleteVolume

Metodi API dell'amministratore

È possibile utilizzare i metodi API dell'amministratore per creare, modificare, visualizzare

e rimuovere gli amministratori del cluster di storage e assegnare livelli di accesso e privilegi a coloro che hanno accesso a un cluster di storage.

- AddClusterAdmin
- GetCurrentClusterAdmin
- GetLoginBanner
- ListClusterAdmins
- ModifyClusterAdmin
- RemoveClusterAdmin
- SetLoginBanner

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddClusterAdmin

È possibile utilizzare `AddClusterAdmin` metodo per aggiungere un nuovo account amministratore del cluster. Un amministratore del cluster può gestire il cluster tramite API e strumenti di gestione. Gli amministratori dei cluster sono completamente separati e non correlati agli account dei tenant standard.

Ogni amministratore del cluster può essere limitato a un sottoinsieme dell'API. È necessario utilizzare più account di amministrazione del cluster per utenti e applicazioni diversi. Come Best practice, assegnare a ciascun amministratore del cluster le autorizzazioni minime necessarie; in questo modo si riduce il potenziale impatto della compromissione delle credenziali.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Controlla i metodi che l'amministratore del cluster può utilizzare.	array di stringhe	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AccetteEula	Accettare il Contratto di licenza con l'utente finale. Impostare su true per aggiungere un account amministratore del cluster al sistema. Se omesso o impostato su false, la chiamata al metodo non riesce.	booleano	Nessuno	Sì
attributi	Elenco delle coppie nome/valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
password	Password utilizzata per autenticare questo amministratore del cluster.	stringa	Nessuno	Sì
nome utente	Nome utente univoco per questo amministratore del cluster. La lunghezza deve essere compresa tra 1 e 1024 caratteri.	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ID clusterAdminID	ClusterAdminID per l'amministratore del cluster appena creato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "attributes": {},
    "acceptEula": true,
    "access": ["volumes", "reporting", "read"]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id":1,
  "result" : {
    "clusterAdminID": 2
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

Controllo degli accessi

GetCurrentClusterAdmin

È possibile utilizzare `GetCurrentClusterAdmin` Metodo per restituire informazioni per l'attuale amministratore del cluster primario L'amministratore principale del cluster è stato creato al momento della creazione del cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterAdmin	Informazioni sull'amministratore del cluster.	ClusterAdmin

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "GetCurrentClusterAdmin",
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
"result": {
    "clusterAdmin":
        "access": [
           "administrator"
        ],
         "attributes": null,
         "authMethod": "Cluster"
         "clusterAdminID": 1,
         "username": "admin"
     }
   }
}
```

Novità dalla versione

10.0

GetLoginBanner

È possibile utilizzare `GetLoginBanner` Metodo per ottenere il banner delle Condizioni d'uso attualmente attivo che gli utenti visualizzano quando accedono all'interfaccia web di Element.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
banner	Il testo corrente del banner Termini di utilizzo. Questo valore può contenere testo anche quando il banner è disattivato.	stringa
attivato	Lo stato del banner Termini di utilizzo. Valori possibili: • Vero: Il banner Termini di utilizzo viene visualizzato al momento dell'accesso all'interfaccia Web. • Falso: Il banner delle Condizioni d'uso non viene visualizzato al momento dell'accesso all'interfaccia Web.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 3411,
  "method": "GetLoginBanner",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 3411,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": false
    }
  }
}
```

Novità dalla versione

10.0

ListClusterAdmins

È possibile utilizzare `ListClusterAdmins` metodo per restituire l'elenco di tutti gli amministratori del cluster per il cluster.

Possono essere presenti diversi account amministratore del cluster con diversi livelli di autorizzazioni. Nel sistema può essere presente un solo amministratore principale del cluster. L'amministratore principale del cluster è l'amministratore creato al momento della creazione del cluster. Gli amministratori LDAP possono essere creati anche durante la configurazione di un sistema LDAP nel cluster.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ShowHidden	Mostra gli utenti nascosti dell'amministratore del cluster, ad esempio SNMP admin.	booleano	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterAdmins	Informazioni su tutti gli amministratori del cluster e LDAP esistenti per un cluster.	ClusterAdmin array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListClusterAdmins",
   "params": {},
    "showHidden": true
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id":1,
"result":{
  "clusterAdmins":[
     {
       "access":[
           "administrator"
       ],
       "attributes":null,
       "authMethod":"Cluster",
       "clusterAdminID":1,
       "username":"admin"
   },
   {
       "access":[
           "read",
           "administrator"
       ],
       "attributes":{
       },
       "authMethod":"Ldap",
       "clusterAdminID":7,
       "username":"john.smith"
   },
   {
       "access":[
           "read",
           "administrator"
       ],
       "attributes":{},
       "authMethod":"Ldap",
       "clusterAdminID":6,
       "username":"cn=admin1
jones,ou=ptusers,c=prodtest,dc=solidfire,dc=net"
       }
     ]
   }
}
```


Novità dalla versione

9.6

ModifyClusterAdmin

È possibile utilizzare `ModifyClusterAdmin` Metodo per modificare le impostazioni di un amministratore del cluster, di un amministratore del cluster LDAP o di un amministratore del cluster IdP (Identity Provider) di terze parti. Non è possibile modificare l'accesso per l'account amministratore del cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Controlla i metodi che l'amministratore del cluster può utilizzare.	array di stringhe	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
ID clusterAdminID	ClusterAdminID per l'amministratore del cluster, l'amministratore del cluster LDAP o l'amministratore del cluster IdP da modificare.	intero	Nessuno	Sì
password	Password utilizzata per autenticare questo amministratore del cluster. Questo parametro non si applica a un amministratore del cluster LDAP o IdP.	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ModifyClusterAdmin",
   "params": {
     "clusterAdminID"  : 2,
     "password"    : "7925Brc429a"
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id" : 1
 "result" : { }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

Controllo degli accessi

RemoveClusterAdmin

È possibile utilizzare `RemoveClusterAdmin` Metodo per rimuovere un amministratore del cluster, un amministratore del cluster LDAP o un amministratore del cluster IdP (Identity Provider) di terze parti. Non è possibile rimuovere l'account "admin" Cluster Admin.

Parametro

Quando viene rimosso un amministratore del cluster IdP che ha autenticato sessioni associate a un ID provider di identità di terze parti, tali sessioni si disconnetteranno o probabilmente subiranno una perdita dei diritti di accesso nella sessione corrente. La perdita dei diritti di accesso dipende dalla corrispondenza tra l'amministratore del cluster IdP rimosso e uno dei diversi amministratori del cluster IdP degli attributi SAML di un determinato utente. Il set rimanente di amministratori del cluster IdP corrispondenti determina una riduzione dei diritti di accesso aggregati. Gli altri tipi di utenti amministratori del cluster vengono disconnessi quando vengono rimossi gli amministratori del cluster.

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID clusterAdminID	ClusterAdminID per l'amministratore del cluster da rimuovere.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveClusterAdmin",
   "params": {
     "clusterAdminID"  : 2
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id" : 1
 "result" : { }
}
```

Novità dalla versione

9.6

SetLoginBanner

È possibile utilizzare `SetLoginBanner` Metodo per configurare il banner Termini di utilizzo visualizzato dagli utenti quando accedono all'interfaccia web Element.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
banner	Il testo desiderato del banner Termini di utilizzo. La lunghezza massima consentita è di 4,096 caratteri.	stringa	Nessuno	No
attivato	Lo stato del banner Termini di utilizzo. Valori possibili: • `true`: Il banner Condizioni d'uso viene visualizzato al momento dell'accesso all'interfaccia Web. • `false`: Il banner Condizioni d'uso non viene visualizzato al momento dell'accesso all'interfaccia Web.	booleano	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
banner	Il testo corrente del banner Termini di utilizzo. Questo valore può contenere testo anche quando il banner è disattivato.	stringa

Nome	Descrizione	Tipo
attivato	Lo stato del banner Termini di utilizzo. Valori possibili: • Vero: Il banner Termini di utilizzo viene visualizzato al momento dell'accesso all'interfaccia Web. • Falso: Il banner delle Condizioni d'uso non viene visualizzato al momento dell'accesso all'interfaccia Web.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 3920,
  "method": "SetLoginBanner",
  "params": {
    "banner": "Welcome to NetApp!",
    "enabled": true
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 3920,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": true
    }
  }
}
```

Novità dalla versione

10.0

Metodi API del cluster

I metodi API del cluster di software Element consentono di gestire la configurazione e la topologia del cluster di storage e dei nodi che appartengono a un cluster di storage.

Alcuni metodi API del cluster operano su nodi che fanno parte di un cluster o che sono stati configurati per unirsi a un cluster. È possibile aggiungere nodi a un nuovo cluster o a un cluster esistente. I nodi pronti per essere aggiunti a un cluster si trovano in uno stato "in sospeso", il che significa che sono stati configurati ma non ancora aggiunti al cluster.

- AddNode
- ClearClusterFaults
- CreateClusterInterfacePreference
- DeleteClusterInterfacePreference
- EnableFeature
- GetClusterCapacity
- GetClusterFullThreshold
- GetClusterHardwareInfo
- GetClusterInfo
- GetClusterInterfacePreference
- GetClusterMasterNodeID
- GetClusterStats
- GetClusterVersionInfo
- GetFeatureStatus
- GetLoginSessionInfo
- GetNodeHardwareInfo
- GetNodeStats
- ListActiveNode
- ListAllNode
- ListClusterFaults
- ListClusterInterfacePreferences
- ListEvents
- ListNodeStats
- ListISCSISessions
- ListServices
- ListPendingNode
- ListPendingActiveNode
- ModifyClusterFullThreshold
- ModifyClusterInterfacePreference
- RemoveNode

- SetLoginSessionInfo
- Spegnere

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddNode

È possibile utilizzare `AddNodes` metodo per aggiungere uno o più nuovi nodi a un cluster.

Quando un nodo non configurato viene avviato per la prima volta, viene richiesto di configurarlo. Una volta configurato, il nodo viene registrato come "nodo in sospeso" con il cluster. I cluster di storage che eseguono il software Element image automaticamente un nodo alla versione del cluster. Quando si aggiunge un nodo in sospeso, la risposta del metodo include un valore asyncHandle che è possibile utilizzare con `GetAsyncResult` metodo per interrogare lo stato del processo di imaging automatico.

Il processo di aggiunta di un nodo Fibre Channel equivale all'aggiunta di nodi storage iSCSI a un cluster. I nodi Fibre Channel sono registrati nel sistema con un NodeID. Quando diventano accessibili, vengono posti in uno stato di "nodo in sospeso". Il `ListAllNodes` Il metodo restituisce il pendingNodeID per i nodi iSCSI e per tutti i nodi Fibre Channel disponibili per l'aggiunta al cluster.

Quando si aggiunge un nodo a un cluster configurato per la rete virtuale, il sistema richiede un numero sufficiente di indirizzi IP dello storage virtuale per allocare un IP virtuale al nuovo nodo. Se non sono disponibili indirizzi IP virtuali per il nuovo nodo, il `AddNode` operazione non riuscita. Utilizzare `ModifyVirtualNetwork` Metodo per aggiungere altri indirizzi IP dello storage alla rete virtuale.

Una volta aggiunto un nodo, tutte le unità del nodo vengono rese disponibili ed è possibile aggiungerle utilizzando `AddDrives` metodo per aumentare la capacità di storage del cluster.

> Dopo l'aggiunta di un nuovo nodo, l'avvio e la registrazione dei dischi potrebbero richiedere alcuni secondi.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Installazione automatica	Se vero, al momento dell'aggiunta verrà eseguito un ritorno all'immagine di fabbrica (RTFI) sul nodo. Il comportamento predefinito è quello di eseguire RTFI. Se il `cEnableAutoInstall` la costante del cluster è falsa e ha priorità su questo parametro. Se è in corso un aggiornamento, il processo RTFI non si verificherà indipendentemente dal valore di questo parametro.	booleano	Nessuno	No
PendingNodes	NodeID in sospeso per i nodi da aggiungere. È possibile elencare tutti i nodi in sospeso utilizzando il metodo ListPendingNodes.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
Installazione automatica	Se i nodi aggiunti vengono restituiti o meno all'immagine di fabbrica.	booleano

nodi	Matrice di oggetti che mappano il precedente "pendingNodeID" a "NodeID". Quando si aggiunge un nodo in sospeso che esegue una versione software incompatibile, questo array include un valore asyncHandle che è possibile utilizzare con il metodo GetAsyncResult per eseguire query sullo stato del processo di imaging automatico.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "AddNodes",
   "params": {
     "autoInstall" : true,
     "pendingNodes" : [1]
   },
   "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  id: null,
  result: {
    autoInstall: true,
    nodes: [
      {
        activeNodeKey: "giAm2ep1hA",
        assignedNodeID: 6,
        asyncHandle: 3,
        cip: "10.10.5.106",
        mip: "192.168.133.106",
        pendingNodeID: 2,
        platformInfo: {
          chassisType: "R620",
          cpuModel: "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
          nodeMemoryGB: 72,
          nodeType: "SF3010"
        },
        sip: "10.10.5.106",
        softwareVersion: "9.0.0.1077"
      }
    ]
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

- AddDrive
- GetAsyncResult
- ListAllNode
- ModifyVirtualNetwork

ClearClusterFaults

È possibile utilizzare `ClearClusterFaults` metodo per cancellare le informazioni sui guasti rilevati in precedenza e correnti. I guasti risolti e quelli non risolti possono essere cancellati.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
FaultTypes (tipi di errore)	Determina i tipi di guasti da eliminare. Valori possibili: • corrente: Guasti rilevati attualmente e non risolti. • Risolto: Guasti precedentement e rilevati e risolti. • All (tutti): Guasti attuali e risolti. Lo stato di guasto può essere determinato dal campo “rerisolto” dell’oggetto guasto.	stringa	risolto	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all’esempio seguente:

```
{
   "method": "ClearClusterFaults",
   "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all’esempio seguente:

```
{
  "id" : 1,
    "result" : {}
}
```

Novità dalla versione

9.6

CreateClusterInterfacePreference

Il `CreateClusterInterfacePreference` Il metodo consente ai sistemi integrati con i cluster di storage che eseguono il software Element di creare e memorizzare informazioni arbitrarie nel cluster di storage. Questo metodo è per uso interno.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome della preferenza dell'interfaccia del cluster.	stringa	Nessuno	Sì
valore	Il valore della preferenza dell'interfaccia del cluster.	stringa	Nessuno	Sì

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
        "method": "CreateClusterInterfacePreference",
        "params": {
            "name": "prefname",
            "value": "testvalue"
        },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {}
}
```

Novità dalla versione

11.0

DeleteClusterInterfacePreference

Il `DeleteClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di storage che eseguono il software Element di eliminare una preferenza di interfaccia cluster esistente. Questo metodo è per uso interno.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome della preferenza dell'interfaccia del cluster da eliminare.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "DeleteClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {}
}
```

Novità dalla versione

11.0

EnableFeature

È possibile utilizzare `EnableFeature` Metodo per attivare le funzionalità del cluster, ad esempio i VVol, disabilitate per impostazione predefinita.

Parametro

Questo metodo ha il seguente parametro di input.

> Per i sistemi che eseguono il software Element 11.x, l'abilitazione dei volumi virtuali prima o dopo l'impostazione del monitoraggio del dominio di protezione fa sì che la funzione dei domini di protezione del cluster funzioni solo a livello di nodo.

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
funzione	Attivare una funzione del cluster. Valori possibili: • `fips`: Attiva la crittografia certificata FIPS 140-2 per le comunicazioni HTTPS. • `FipsDrives`: Abilitare il supporto del disco FIPS 140-2 per il cluster di storage. • `SnapMirror`: Attivare la funzione del cluster di replica di SnapMirror. • `vvols`: Attivare la funzione cluster di VVols del software Element.	stringa	Nessuno	Sì

Valore restituito

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableFeature",
    "params": {
        "feature" : "vvols"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9.6

GetClusterCapacity

È possibile utilizzare `GetClusterCapacity` per restituire misurazioni di capacità di alto livello per un intero cluster di storage. Questo metodo restituisce i campi che è possibile utilizzare per calcolare i tassi di efficienza mostrati nell'interfaccia utente Web elemento. È possibile utilizzare i calcoli di efficienza negli script per restituire i tassi di efficienza per il thin provisioning, la deduplica, la compressione e l'efficienza complessiva.

Calcoli di efficienza

Utilizzare le seguenti equazioni per calcolare il thin provisioning, la deduplica e la compressione. Queste equazioni si applicano all'elemento 8.2 e versioni successive.

- ThinProvisioningFactor = (non ZeroBlocks + zero oBlocks) / non ZeroBlocks
- DeDuplicationFactor = (nonZeroBlocks + snapshotNonZeroBlocks) / uniqueBlocks
- Fattore di compressione = (uniqueBlocks * 4096) / (uniqueBlocksUsedSpace * 0.93)

Calcolo del tasso di efficienza globale

Utilizzare la seguente equazione per calcolare l'efficienza complessiva del cluster utilizzando i risultati dei calcoli di thin provisioning, deduplica ed efficienza della compressione.

- EpiencyFactor = thinProvisioningFactor * deDuplicationFactor * compressionFactor

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
Capacità del clusterCapacity	Misurazioni della capacità per il cluster di storage.	Capacità del clusterCapacity

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterCapacity",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "clusterCapacity": {
      "activeBlockSpace": 236015557096,
      "activeSessions": 20,
      "averageIOPS": 0,
      "clusterRecentIOSize": 0,
      "currentIOPS": 0,
      "maxIOPS": 150000,
      "maxOverProvisionableSpace": 259189767127040,
      "maxProvisionedSpace": 51837953425408,
      "maxUsedMetadataSpace": 404984011161,
      "maxUsedSpace": 12002762096640,
      "nonZeroBlocks": 310080350,
      "peakActiveSessions": 20,
      "peakIOPS": 0,
      "provisionedSpace": 1357931085824,
      "snapshotNonZeroBlocks": 0,
      "timestamp": "2016-10-17T21:24:36Z",
      "totalOps": 1027407650,
      "uniqueBlocks": 108180156,
      "uniqueBlocksUsedSpace": 244572686901,
      "usedMetadataSpace": 8745762816,
      "usedMetadataSpaceInSnapshots": 8745762816,
      "usedSpace": 244572686901,
      "zeroBlocks": 352971938
    }
  }
}
```

Novità dalla versione

9.6

GetClusterFullThreshold

È possibile utilizzare `GetClusterFullThreshold` metodo per visualizzare le fasi impostate per i livelli di completezza del cluster. Questo metodo restituisce tutte le metriche di completezza per il cluster.

> Quando un cluster raggiunge la fase Error di Block Cluster Fullness, gli IOPS massimi su tutti i volumi vengono ridotti linearmente agli IOPS minimi del volume man mano che il cluster si avvicina alla fase critica. In questo modo si evita che il cluster raggiunga la fase critica della piena funzionalità del cluster a blocchi.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
BlockFullness	Il livello corrente calcolato di riempimento del blocco del cluster. • Stage1Happy: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage2Aware: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage3Low: Il sistema non è in grado di fornire una protezione dei dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato **Warning** nell'interfaccia utente Web. È possibile configurare questo livello nell'interfaccia utente Web (per impostazione predefinita, il sistema attiva questo avviso a una capacità del 3% inferiore allo stato di errore). • Stage4criticità: Il sistema non è in grado di fornire una protezione dei dati ridondante in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato **Error** nell'interfaccia utente dell'elemento. • Stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture vengono sospese. Corrisponde allo stato **critico** nell'interfaccia utente dell'elemento.	stringa
pienezza	Riflette il massimo livello di pienezza tra "blockFullness" e "metadataFullness".	stringa

Nome	Descrizione	Tipo
MaxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio di metadati può essere sottoposto a un provisioning eccessivo in relazione alla quantità di spazio disponibile. Ad esempio, se c'era spazio di metadati sufficiente per memorizzare 100 TIB di volumi e questo numero era impostato su 5, è possibile creare 500 TIB di volumi.	intero

Nome	Descrizione	Tipo
MetadataFullness	Il livello corrente calcolato di riempimento dei metadati del cluster. • Stage1Happy: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage2Aware: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage3Low: Il sistema non è in grado di fornire una protezione dei dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato **Warning** nell'interfaccia utente Web. È possibile configurare questo livello nell'interfaccia utente Web (per impostazione predefinita, il sistema attiva questo avviso a una capacità del 3% inferiore allo stato di errore). • Stage4criticità: Il sistema non è in grado di fornire una protezione dei dati ridondante in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato **Error** nell'interfaccia utente dell'elemento. • Stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture vengono sospese. Corrisponde allo stato **critico** nell'interfaccia utente dell'elemento.	stringa
SliceReserveUsedThresholdPct	Condizione di errore. Viene generato un avviso di sistema se l'utilizzo dello strato riservato è superiore a questo valore.	intero

Nome	Descrizione	Tipo
Stage2AwareThreshold	Condizione di consapevolezza. Il valore impostato per il livello di soglia del cluster di fase 2.	intero
Stage2BlockThresholdByte	Il numero di byte utilizzati dal cluster in cui si verifica una condizione di fase 2.	intero
Stage2MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness fase 2.	
Stage3BlockThresholdBytes	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness fase 3.	intero
Stage3BlockThresholdPercent	Il valore percentuale impostato per la fase 3. Con questa percentuale piena, viene visualizzato un avviso nel registro degli avvisi.	intero
Stage3LowThreshold	Condizione di errore. La soglia alla quale viene creato un avviso di sistema a causa della bassa capacità di un cluster.	intero
Stage3MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 3.	intero
Stage3MetadataThresholdPercent	Il valore percentuale impostato per lo stage3 della fullness dei metadati. Con questa percentuale piena, viene visualizzato un avviso nel registro degli avvisi.	intero
Stage4BlockThresholdByte	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness fase 4.	intero
Stage4CriticalThreshold	Condizione di errore. La soglia alla quale viene creato un avviso di sistema per avvisare in caso di capacità estremamente bassa su un cluster.	intero

Nome	Descrizione	Tipo
Stage4MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 4.	intero
Stage5BlockThresholdByte	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness della fase 5.	intero
Stage5MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 5.	intero
SumTotalClusterBytes	La capacità fisica del cluster, misurata in byte.	intero
SumTotalMetadataClusterBytes	La quantità totale di spazio che è possibile utilizzare per memorizzare i metadati.	intero
SumUsedClusterBytes	Il numero di byte di storage utilizzati nel cluster.	intero
SumUsedMetadataClusterBytes	La quantità di spazio utilizzata sui dischi dei volumi per memorizzare i metadati.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method" : "GetClusterFullThreshold",
   "params" : {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id":1,
  "result":{
    "blockFullness":"stage1Happy",
    "fullness":"stage3Low",
    "maxMetadataOverProvisionFactor":5,
    "metadataFullness":"stage3Low",
    "sliceReserveUsedThresholdPct":5,
    "stage2AwareThreshold":3,
    "stage2BlockThresholdBytes":2640607661261,
    "stage3BlockThresholdBytes":8281905846682,
    "stage3BlockThresholdPercent":5,
    "stage3LowThreshold":2,
    "stage4BlockThresholdBytes":8641988709581,
    "stage4CriticalThreshold":1,
    "stage5BlockThresholdBytes":12002762096640,
    "sumTotalClusterBytes":12002762096640,
    "sumTotalMetadataClusterBytes":404849531289,
    "sumUsedClusterBytes":45553617581,
    "sumUsedMetadataClusterBytes":31703113728
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

ModifyClusterFullThreshold

GetClusterHardwareInfo

È possibile utilizzare `GetClusterHardwareInfo` Metodo per recuperare lo stato dell'hardware e le informazioni per tutti i nodi Fibre Channel, i nodi iSCSI e le unità del cluster. In genere, sono inclusi produttori, vendor, versioni e altre informazioni di identificazione hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
tipo	Includere nella risposta solo uno dei seguenti tipi di informazioni hardware. Valori possibili: • dischi: Elenca solo le informazioni sul disco nella risposta. • Nodi: Elenca solo le informazioni sui nodi nella risposta. • All (tutti): Include le informazioni su disco e nodo nella risposta. Se questo parametro viene omesso, viene assunto un tipo di tutto.	stringa	tutto	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterHardwareInfo	Informazioni sull'hardware per tutti i nodi e i dischi nel cluster. Ogni oggetto in questo output viene etichettato con il NodeID del nodo specificato.	HardwareInfo

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetClusterHardwareInfo",
    "params": {
        "type": "all"
    },
    "id": 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

GetClusterHardwareInfo

GetClusterInfo

È possibile utilizzare `GetClusterInfo` metodo per restituire le informazioni di configurazione relative al cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterInfo	Informazioni sul cluster.	ClusterInfo

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterInfo",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:


```
{
    "id": 1,
    "result": {
        "clusterInfo": {
            "attributes": {},
            "defaultProtectionScheme": "doubleHelix",
            "enabledProtectionSchemes": [
                "doubleHelix"
            ],
            "encryptionAtRestState": "disabled",
            "ensemble": [
                "10.10.10.32",
                "10.10.10.34",
                "10.10.10.35",
                "10.10.10.36",
                "10.10.10.37"
            ],
            "mvip": "10.10.11.225",
            "mvipInterface": "team1G",
            "mvipNodeID": 3,
            "mvipVlanTag": "0",
            "name": "ClusterName",
            "repCount": 2,
            "softwareEncryptionAtRestState": "enabled",
            "supportedProtectionSchemes": [
                "doubleHelix"
            ],
            "svip": "10.10.10.111",
            "svipInterface": "team10G",
            "svipNodeID": 3,
            "svipVlanTag": "0",
            "uniqueID": "psmp",
            "uuid": "2f575d0c-36fe-406d-9d10-dbc1c306ade7"
        }
    }
}
```


Novità dalla versione

9.6

GetClusterInterfacePreference

Il `GetClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di storage che eseguono il software Element di ottenere informazioni sulle preferenze di un'interfaccia cluster esistente. Questo metodo è per uso interno.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome della preferenza dell'interfaccia del cluster.	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
preferenza	Il nome e il valore della preferenza di interfaccia del cluster richiesta.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "GetClusterInterfacePreference",
    "params": {
        "name": "prefname"
        },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "preference": {
            "name": "prefname",
            "value": "testvalue"
        }
    }
}
```

Novità dalla versione

11.0

GetClusterMasterNodeID

È possibile utilizzare `GetClusterMasterNodeID` Metodo per recuperare l'ID del nodo che esegue le attività di amministrazione a livello di cluster e contiene l'indirizzo IP virtuale dello storage (SVIP) e l'indirizzo IP virtuale di gestione (MVIP).

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ID NodeID	ID del nodo master.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetClusterMasterNodeID",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1
  "result": {
    "nodeID": 1
   }
}
```

Novità dalla versione

9.6

GetClusterStats

È possibile utilizzare `GetClusterStats` metodo per recuperare le misurazioni delle attività di alto livello per il cluster. I valori restituiti sono cumulativi dalla creazione del cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterStats	Informazioni sull'attività del cluster.	ClusterStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterStats",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "clusterStats": {
      "actualIOPS": 9376,
      "averageIOPSize": 4198,
      "clientQueueDepth": 8,
      "clusterUtilization": 0.09998933225870132,
      "latencyUSec": 52,
      "normalizedIOPS": 15000,
      "readBytes": 31949074432,
      "readBytesLastSample": 30883840,
      "readLatencyUSec": 27,
      "readLatencyUSecTotal": 182269319,
      "readOps": 1383161,
      "readOpsLastSample": 3770,
      "samplePeriodMsec": 500,
      "servicesCount": 3,
      "servicesTotal": 3,
      "timestamp": "2017-09-09T21:15:39.809332Z",
      "unalignedReads": 0,
      "unalignedWrites": 0,
      "writeBytes": 8002002944,
      "writeBytesLastSample": 7520256,
      "writeLatencyUSec": 156,
      "writeLatencyUSecTotal": 231848965,
      "writeOps": 346383,
      "writeOpsLastSample": 918
    }
  }
}
```


Novità dalla versione

9.6

GetClusterVersionInfo

È possibile utilizzare `GetClusterVersionInfo` Metodo per recuperare informazioni sulla versione del software Element in esecuzione su ciascun nodo del cluster. Questo metodo restituisce anche informazioni sui nodi attualmente in fase di aggiornamento del software.

Membri dell'oggetto informazioni sulla versione del cluster

Questo metodo ha i seguenti membri dell'oggetto:

Nome	Descrizione	Tipo
ID NodeID	ID del nodo.	intero
NodeInternalRevision	Versione software interna del nodo.	stringa
NodeVersion	Versione software del nodo.	stringa

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ClusterAPIVersion	La versione API corrente sul cluster.	stringa
ClusterVersion	Versione del software Element attualmente in esecuzione sul cluster.	stringa
ClusterVersionInfo	Elenco dei nodi nel cluster con informazioni sulla versione per ciascun nodo.	Array di oggetti JSON
PendingClusterVersion	Se presente, si tratta della versione attualmente in fase di aggiornamento o ripristino del software del cluster.	stringa

Nome	Descrizione	Tipo
SoftwareVersionInfo	Lo stato di un aggiornamento. Membri dell'oggetto: • Versione attuale: La versione software corrente su un nodo. • NodeID: ID del nodo da aggiornare da CurrentVersion a pendingVersion. Questo campo è 0 (zero) se non è in corso alcun aggiornamento. • Packagename (Nome pacchetto): Nome del pacchetto software da installare. • PendingVersion: Versione del software da installare. • StartTime: Data e ora di inizio dell'installazione, in formato UTC+0.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterVersionInfo",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id": 1,
 "result": {
   "clusterAPIVersion": "6.0",
   "clusterVersion": "6.1382",
   "clusterVersionInfo": [
   {
      "nodeID": 1,
      "nodeInternalRevision": "BuildType=Release Element=carbon
Release=carbon ReleaseShort=carbon Version=6.1382 sfdev=6.28
Repository=dev Revision=061511b1e7fb BuildDate=2014-05-28T18:26:45MDT",
      "nodeVersion": "6.1382"
   },
   {
      "nodeID": 2,
      "nodeInternalRevision": "BuildType=Release Element=carbon
Release=carbon ReleaseShort=carbon Version=6.1382 sfdev=6.28
Repository=dev Revision=061511b1e7fb BuildDate=2014-05-28T18:26:45MDT",
      "nodeVersion": "6.1382"
   },
   {
      "nodeID": 3,
      "nodeInternalRevision": "BuildType=Release Element=carbon
Release=carbon ReleaseShort=carbon Version=6.1382 sfdev=6.28
Repository=dev Revision=061511b1e7fb BuildDate=2014-05-28T18:26:45MDT",
      "nodeVersion": "6.1382"
   },
   {
      "nodeID": 4,
      "nodeInternalRevision": "BuildType=Release Element=carbon
Release=carbon ReleaseShort=carbon Version=6.1382 sfdev=6.28
Repository=dev Revision=061511b1e7fb BuildDate=2014-05-28T18:26:45MDT",
      "nodeVersion": "6.1382"
   }
 ],
   "softwareVersionInfo": {
      "currentVersion": "6.1382",
      "nodeID": 0,
      "packageName": "",
      "pendingVersion": "6.1382",
      "startTime": ""
    }
  }
}
```

Novità dalla versione

9.6

GetFeatureStatus

È possibile utilizzare `GetFeatureStatus` metodo per recuperare lo stato di una funzione del cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
funzione	Lo stato di una funzione del cluster. Se non viene fornito alcun valore, il sistema restituisce lo stato di tutte le funzioni. Valori possibili: • Vvols: Recuperare lo stato della funzione cluster VVols. • SnapMirror: Recuperare lo stato della funzione del cluster di replica di SnapMirror. • FIPS: Recuperare lo stato della crittografia FIPS 140-2 per la funzione di comunicazione HTTPS. • FipsDrives: Recupera lo stato della funzione di crittografia del disco FIPS 140-2.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
caratteristiche	Matrice di oggetti feature che indica il nome della feature e il relativo stato. Membri dell'oggetto: • Feature (funzione): (Stringa) il nome della funzione. • Enabled (attivato): (booleano) se la funzione è attivata o meno.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetFeatureStatus",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "features": [
            {
                "enabled": true,
                "feature": "Vvols"
            },
            {
                "enabled": true,
                "feature": "SnapMirror"
            },
            {
                "enabled": true,
                "feature": "Fips"
            },
            {
                "enabled": true,
                "feature": "FipsDrives"
            }
        ]
    }
}
```


Novità dalla versione

9.6

GetLoginSessionInfo

È possibile utilizzare `GetLoginSessionInfo` Metodo per restituire il periodo di tempo in cui una sessione di autenticazione dell'accesso è valida sia per le shell di accesso che per l'interfaccia telefonica utente (TUI).

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
LoginSessionInfo	Oggetto contenente il periodo di scadenza dell'autenticazione. Possibili oggetti restituiti: • timeout: L'intervallo di tempo, espresso in minuti, in cui la sessione scadrà. Formattato in H:mm:ss. Ad esempio: 1:30:00, 20:00, 5:00. Tutti gli zeri e i due punti iniziali vengono rimossi indipendentemente dal formato in cui è stato inserito il timeout.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetLoginSessionInfo",
    "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
  "result" : {
    "loginSessionInfo" : {
      "timeout" : "30:00"
    }
  }
}
```

Novità dalla versione

9.6

GetNodeHardwareInfo

È possibile utilizzare `GetNodeHardwareInfo` metodo per restituire tutte le informazioni

hardware e lo stato del nodo specificato. In genere, sono inclusi produttori, vendor, versioni e altre informazioni di identificazione hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID NodeID	L'ID del nodo per il quale vengono richieste informazioni hardware. Le informazioni su un nodo Fibre Channel vengono restituite se viene specificato un nodo Fibre Channel.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
NodeHardwareInfo	Informazioni hardware per il NodeID specificato. Ogni oggetto in questo output viene etichettato con il NodeID del nodo specificato.	HardwareInfo

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetNodeHardwareInfo",
   "params": {
     "nodeID": 1
   },
"id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

GetNodeHardwareInfo (output per nodi Fibre Channel)

GetNodeHardwareInfo (output per iSCSI)

GetNodeStats

È possibile utilizzare `GetNodeStats` metodo per recuperare le misurazioni di attività di alto livello per un singolo nodo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID NodeID	Specifica l'ID del nodo per il quale verranno restituite le statistiche.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
NodeStats	Informazioni sull'attività del nodo.	NodeStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetNodeStats",
   "params": {
     "nodeID": 5
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
     "nodeStats" : {
       "cBytesIn" : 9725856460404,
       "cBytesOut" : 16730049266858,
       "cpu" : 98,
       "mBytesIn" : 50808519,
       "mBytesOut" : 52040158,
       "networkUtilizationCluster" : 84,
       "networkUtilizationStorage" : 0,
       "sBytesIn" : 9725856460404,
       "sBytesOut" : 16730049266858,
       "timestamp" : "2012-05-16T19:14:37.167521Z",
       "usedMemory" : 41195708000
     }
   }
}
```

Novità dalla versione

9.6

ListActiveNode

È possibile utilizzare `ListActiveNodes` metodo per restituire l'elenco dei nodi attualmente attivi nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
nodi	Elenco dei nodi attivi nel cluster.	nodo array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListActiveNodes",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

ListActiveNode

ListAllNode

È possibile utilizzare `ListAllNodes` metodo per elencare i nodi attivi e in sospeso nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
nodi	Elenco degli oggetti che descrivono i nodi attivi nel cluster.	nodo
PendingActiveNodes	Elenco degli oggetti che descrivono i nodi attivi in sospeso per il cluster.	PendingActiveNode array
PendingNodes	Elenco degli oggetti che descrivono i nodi in sospeso per il cluster.	PendingNode array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListAllNodes",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "nodes": [
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 1,
                "attributes": {},
                "chassisName": "CT5TV12",
                "cip": "10.1.1.1",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "10.1.1.1",
                "mipi": "Bond1G",
                "name": "NLABP0704",
                "nodeID": 1,
                "nodeSlot": "",
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010",
                    "platformConfigVersion": "0.0.0.0"
                },
                "sip": "10.1.1.1",
                "sipi": "Bond10G",
                "softwareVersion": "11.0",
                "uuid": "4C4C4544-0054",
                "virtualNetworks": []
            }
        ],
        "pendingActiveNodes": [],
        "pendingNodes": []
    }
}
```


Novità dalla versione

9.6

ListClusterFaults

È possibile utilizzare `ListClusterFaults` metodo per elencare le informazioni sugli eventuali guasti rilevati sul cluster. Con questo metodo, è possibile elencare sia gli errori correnti che quelli risolti. Il sistema memorizza i guasti nella cache ogni 30 secondi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Best Practice	Includere gli errori generati dalla configurazione di sistema non ottimale. Valori possibili: • vero • falso	booleano	Nessuno	No
FaultTypes (tipi di errore)	Determina i tipi di guasti restituiti. Valori possibili: • Current (corrente): Elenco dei guasti attivi, non risolti. • Resolved (risolto): Elenca i guasti precedentemente rilevati e risolti. • All (tutti): Elenca sia i guasti correnti che quelli risolti. È possibile visualizzare lo stato di errore nel membro “rerisolto” dell’oggetto di errore.	stringa	tutto	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
guasti	Oggetto che descrive i guasti del cluster richiesti.	guasto

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListClusterFaults",
    "params": {
      "faultTypes": "current",
      "bestPractices": true
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "faults": [
      {
        "clusterFaultID": 1,
        "code": "notUsingLACPBondMode",
        "data": null,
        "date": "2016-04-26T14:57:04.275286Z",
        "details": "Bond1G interfaces found not using LACP bond mode.
Nodes not set to LACP bond mode: {1,2,4,5}",
        "driveID": 0,
        "driveIDs": [],
        "nodeHardwareFaultID": 0,
        "nodeID": 0,
        "resolved": false,
        "resolvedDate": "",
        "serviceID": 0,
        "severity": "bestPractice",
        "type": "cluster"
      },
      {
        "clusterFaultID": 9,
        "code": "disconnectedClusterPair",
        "data": null,
        "date": "2016-04-26T20:40:08.736597Z",
        "details": "One of the clusters in a pair may have become
misconfigured or disconnected.  Remove the local pairing and retry pairing
the clusters. Disconnected Cluster Pairs: []. Misconfigured Cluster Pairs:
[3]",
        "driveID": 0,
        "driveIDs": [],
        "nodeHardwareFaultID": 0,
        "nodeID": 0,
        "resolved": false,
        "resolvedDate": "",
        "serviceID": 0,
        "severity": "warning",
        "type": "cluster"
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListClusterInterfacePreferences

Il `ListClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di storage che eseguono il software Element di elencare le preferenze esistenti dell'interfaccia del cluster memorizzate nel sistema. Questo metodo è per uso interno.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
preferenze	Un elenco di oggetti di interfaccia del cluster attualmente memorizzati nel cluster di storage, ciascuno contenente il nome e il valore della preferenza.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "ListClusterInterfacePreferences",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "preferences": [
            {
                "name": "prefname",
                "value": "testvalue"
            }
        ]
    }
}
```

Novità dalla versione

11.0

ListEvents

È possibile utilizzare `ListEvents` metodo per elencare gli eventi rilevati nel cluster, ordinati da meno recente a più recente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID del driver	Specifica che verranno restituiti solo gli eventi con questo ID disco.	intero	0	No
EndEventID	Identifica la fine di un intervallo di ID evento da restituire.	intero	(senza limiti)	No
EndPublishTime	Specifica che verranno restituiti solo gli eventi pubblicati prima di questo orario.	stringa	0	No
EndReportTime	Specifica che verranno restituiti solo gli eventi riportati prima di questo orario.	stringa	0	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
EventType	Specifica il tipo di eventi da restituire. Vedere evento per i possibili tipi di evento.	stringa	0	No
MaxEvents	Specifica il numero massimo di eventi da restituire.	intero	(senza limiti)	No
ID NodeID	Specifica che verranno restituiti solo gli eventi con questo ID nodo.	intero		
ID servizio	Specifica che verranno restituiti solo gli eventi con questo ID servizio.			
StartEventID	Identifica l'inizio di un intervallo di eventi da restituire.	intero	0	No
StartPublishTime	Specifica che verranno restituiti solo gli eventi pubblicati dopo questo intervallo di tempo.	stringa	0	No
StartReportTime	Specifica che verranno restituiti solo gli eventi riportati dopo questo intervallo di tempo.	stringa	0	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
eventi	Elenco degli eventi.	evento array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListEvents",
   "params": {
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id":1,
  "result":{
    "events":[
       {
          "details":
            {
              "paramGCGeneration":1431550800,
              "paramServiceID":2
            },
          "driveID":0,
          "eventID":2131,
          "eventInfoType":"gcEvent",
          "message":"GC Cluster Coordination Complete",
          "nodeID":0,
          "serviceID":2,
          "severity":0,
          "timeOfPublish":"2015-05-13T21:00:02.361354Z",
          "timeOfReport":"2015-05-13T21:00:02.361269Z"
       },{
          "details":
               {

"eligibleBS":[5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,24,25,26,27,28,29,30
,31,40,41,42,43,44,45,46,47,52,53,54,55,56,57,58,59,60],
                  "generation":1431550800,
                  "participatingSS":[23,35,39,51]
               },
          "driveID":0,
          "eventID":2130,
          "eventInfoType":"gcEvent",
          "message":"GCStarted",
          "nodeID":0,
          "serviceID":2,
```

```
            "severity":0,
            "timeOfPublish":"2015-05-13T21:00:02.354128Z",
            "timeOfReport":"2015-05-13T21:00:02.353894Z"
         },{
            "details":"",
            "driveID":0,
            "eventID":2129,
            "eventInfoType":"tSEvent",
            "message":"return code:2 t:41286 tt:41286 qcc:1 qd:1 qc:1 vrc:1
tt:2 ct:Write etl:524288",
            "nodeID":0,
            "serviceID":0,
            "severity":0,
            "timeOfPublish":"2015-05-13T20:45:21.586483Z",
            "timeOfReport":"2015-05-13T20:45:21.586311Z"
         }
      ]
   }
}
```


Novità dalla versione

9.6

ListNodeStats

È possibile utilizzare `ListNodeStats` metodo per visualizzare le misurazioni delle attività di alto livello per tutti i nodi di storage in un cluster di storage.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
NodeStats	Informazioni sull'attività del nodo di storage.	NodeStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListNodeStats",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "nodeStats": {
       "nodes": [
         {
         "cBytesIn": 46480366124,
         "cBytesOut": 46601523187,
         "cpu": 0,
         "mBytesIn": 59934129,
         "mBytesOut": 41620976,
         "networkUtilizationCluster": 0,
         "networkUtilizationStorage": 0,
         "nodeID": 1,
         "sBytesIn": 46480366124,
         "sBytesOut": 46601523187,
         "timestamp": 1895558254814,
         "usedMemory": 31608135680
         }
       ]
     }
 }
```

Novità dalla versione

9.6

ListISCSISessions

È possibile utilizzare `ListISCSISessions` Metodo per elencare le informazioni di connessione iSCSI per i volumi nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Informazioni su ogni sessione iSCSI.	sessione

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListISCSISessions",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
 {
  "id": 1,
  "result": {
    "sessions": [
      {
        "accountID": 1,
        "accountName": "account1",
        "createTime": "2017-04-11T03:39:32.030291Z",
        "driveID": 23,
        "driveIDs": [23],
        "initiator": null,
        "initiatorIP": "10.1.1.1:37138",
        "initiatorName": "iqn.2010-01.net.solidfire.eng:c",
        "initiatorPortName": "iqn.2010-
01.net.solidfire.eng:c,i,0x23d860000",
        "initiatorSessionID": 9622126592,
        "msSinceLastIscsiPDU": 243,
        "msSinceLastScsiCommand": 141535021,
        "nodeID": 3,
        "serviceID": 6,
        "sessionID": 25769804943,
        "targetIP": "10.1.1.2:3260",
        "targetName": "iqn.2010-01.com.solidfire:a7sd.3",
        "targetPortName": "iqn.2010-01.com.solidfire:a7sd.3,t,0x1",
        "virtualNetworkID": 0,
        "volumeID": 3,
        "volumeInstance": 140327214758656
      }
     ...
    ]
  }
}
```


Novità dalla versione

9.6

ListServices

È possibile utilizzare `ListServices` metodo per elencare le informazioni sui servizi per nodi, dischi, software corrente e altri servizi in esecuzione nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
servizi	Servizi in esecuzione su dischi e nodi.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListServices",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
"id": 1,
"result": {
    "services": [
        {
            "drive": {
                "assignedService": 22,
                "asyncResultIDs": [],
                "attributes": {},
                "capacity": 300069052416,
                "customerSliceFileCapacity": 0,
                "driveID": 5,
                "driveStatus": "assigned",
                "driveType": "block",
                "failCount": 0,
                "nodeID": 4,
                "reservedSliceFileCapacity": 0,
                "serial": "scsi-SATA_INTEL_SSDSC2",
                "slot": 3
            },
            "drives": [
                {
                    "assignedService": 22,
                    "asyncResultIDs": [],
```

```
                "attributes": {},
                "capacity": 300069052416,
                "customerSliceFileCapacity": 0,
                "driveID": 5,
                "driveStatus": "assigned",
                "driveType": "Block",
                "failCount": 0,
                "nodeID": 4,
                "reservedSliceFileCapacity": 0,
                "serial": "scsi-SATA_INTEL_SSDSC2",
                "slot": 3
            }
        ],
        "node": {
            "associatedFServiceID": 0,
            "associatedMasterServiceID": 1,
            "attributes": {},
            "cip": "10.117.63.18",
            "cipi": "Bond10G",
            "fibreChannelTargetPortGroup": null,
            "mip": "10.117.61.18",
            "mipi": "Bond1G",
            "name": "node4",
            "nodeID": 4,
            "nodeSlot": "",
            "platformInfo": {
                "chassisType": "R620",
                "cpuModel": "Intel(R) Xeon(R) CPU",
                "nodeMemoryGB": 72,
                "nodeType": "SF3010",
                "platformConfigVersion": "10.0"
            },
            "sip": "10.117.63.18",
            "sipi": "Bond10G",
            "softwareVersion": "10.0",
            "uuid": "4C4C4544-0053",
            "virtualNetworks": []
        },
        "service": {
            "associatedBV": 0,
            "associatedTS": 0,
            "associatedVS": 0,
            "asyncResultIDs": [
                1
            ],
            "driveID": 5,
```

```
                "driveIDs": [
                    5
                ],
                "firstTimeStartup": true,
                "ipcPort": 4008,
                "iscsiPort": 0,
                "nodeID": 4,
                "serviceID": 22,
                "serviceType": "block",
                "startedDriveIDs": [],
                "status": "healthy"
            }
        }
    ]
}
```


Novità dalla versione

9.6

ListPendingNode

È possibile utilizzare `ListPendingNodes` metodo per elencare i nodi di storage in sospeso nel sistema. I nodi in sospeso sono nodi di storage in esecuzione e configurati per unirsi al cluster di storage, ma non ancora aggiunti utilizzando il metodo API AddNodes.

Indirizzi di gestione IPv4 e IPv6

Notare che `ListPendingNodes` Non elenca i nodi in sospeso con diversi tipi di indirizzo per l'indirizzo IP di gestione (MIP) e l'indirizzo IP virtuale di gestione (MVIP). Ad esempio, se un nodo in sospeso ha un MVIP IPv6 e un MIP IPv4, `ListPendingNodes` non includerà il nodo come parte del risultato.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
PendingNodes	Elenco dei nodi in sospeso nel cluster.	PendingNode array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListPendingNodes",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 3,
  "result": {
    "pendingNodes": [
      {
        "assignedNodeID": 0,
        "cip": "10.26.65.101",
        "cipi": "Bond10G",
        "compatible": true,
        "mip": "172.26.65.101",
        "mipi": "Bond1G",
        "name": "VWC-EN101",
        "pendingNodeID": 1,
        "platformInfo": {
          "chassisType": "R620",
          "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
          "nodeMemoryGB": 72,
          "nodeType": "SF3010"
        },
        "sip": "10.26.65.101",
        "sipi": "Bond10G",
        "softwareVersion": "9.0.0.1554",
        "uuid": "4C4C4544-0048-4410-8056-C7C04F395931"
      }
    ]
  }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

AddNode

ListPendingActiveNode

È possibile utilizzare `ListPendingActiveNodes` Metodo per elencare i nodi nel cluster che si trovano nello stato PendingActive, tra gli stati in sospeso e attivo. I nodi in questo stato vengono ripristinati all'immagine di fabbrica.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
PendingActiveNodes	Elenco di oggetti con informazioni dettagliate su tutti i nodi PendingActive nel sistema.	PendingActiveNode array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListPendingActiveNodes",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  id: null,
  result: {
    pendingActiveNodes: [
    {
      activeNodeKey: "5rPHP3lTAO",
      assignedNodeID: 5,
      asyncHandle: 2,
      cip: "10.10.5.106",
      mip: "192.168.133.106",
      pendingNodeID: 1,
      platformInfo: {
        chassisType: "R620",
        cpuModel: "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
        nodeMemoryGB: 72,
        nodeType: "SF3010"
      },
     sip: "10.10.5.106",
     softwareVersion: "9.0.0.1077"
    }
    ]
  }
}
```

Novità dalla versione

9.6

ModifyClusterFullThreshold

È possibile utilizzare `ModifyClusterFullThreshold` metodo per modificare il livello a cui il sistema genera un evento quando il cluster di storage si avvicina a un determinato utilizzo della capacità. È possibile utilizzare l'impostazione della soglia per indicare la quantità accettabile di storage a blocchi utilizzato prima che il sistema generi un avviso.

Ad esempio, se si desidera essere avvisati quando il sistema raggiunge il 3% al di sotto del livello di "errore" nell'utilizzo dello storage a blocchi, immettere il valore "3" per il parametro stage3BlockHoldPercent. Se viene raggiunto questo livello, il sistema invia un avviso al registro eventi nella Console di gestione cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

	Selezionare almeno un parametro.

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
MaxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio di metadati può essere sottoposto a un provisioning eccessivo in relazione alla quantità di spazio disponibile. Ad esempio, se c'era spazio di metadati sufficiente per memorizzare 100 TIB di volumi e questo numero era impostato su 5, è possibile creare 500 TIB di volumi.	intero	5	No
Stage2AwareThreshold	Il numero di nodi di capacità rimanenti nel cluster prima che il sistema attivi una notifica di capacità.	intero	Nessuno	No
Stage3BlockThresholdPercent	La percentuale di utilizzo dello storage a blocchi al di sotto della soglia di "errore" che provoca l'attivazione di un avviso di "avviso" del cluster.	intero	Nessuno	No
Stage3MetadataThresholdPercent	La percentuale di utilizzo dello storage dei metadati al di sotto della soglia "Error" che fa sì che il sistema innesca un avviso "Warning" del cluster.	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

BlockFullness	Il livello corrente calcolato di riempimento del blocco del cluster. • Stage1Happy: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage2Aware: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage3Low: Il sistema non è in grado di fornire una protezione dei dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato **Warning** nell'interfaccia utente Web. È possibile configurare questo livello nell'interfaccia utente Web (per impostazione predefinita, il sistema attiva questo avviso a una capacità del 3% inferiore allo stato di errore). • Stage4criticità: Il sistema non è in grado di fornire una protezione dei dati ridondante in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato **Error** nell'interfaccia utente dell'elemento. • Stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture vengono sospese. Corrisponde allo stato **critico** nell'interfaccia utente dell'elemento.	stringa
pienezza	Riflette il massimo livello di pienezza tra "blockFullness" e "metadataFullness".	stringa

MaxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio di metadati può essere sottoposto a un provisioning eccessivo in relazione alla quantità di spazio disponibile. Ad esempio, se c'era spazio di metadati sufficiente per memorizzare 100 TIB di volumi e questo numero era impostato su 5, è possibile creare 500 TIB di volumi.	intero

MetadataFullness	Il livello corrente calcolato di riempimento dei metadati del cluster. • Stage1Happy: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage2Aware: Nessun avviso o condizione di errore. Corrisponde allo stato **integro** nell'interfaccia utente Web. • Stage3Low: Il sistema non è in grado di fornire una protezione dei dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato **Warning** nell'interfaccia utente Web. È possibile configurare questo livello nell'interfaccia utente Web (per impostazione predefinita, il sistema attiva questo avviso a una capacità del 3% inferiore allo stato di errore). • Stage4criticità: Il sistema non è in grado di fornire una protezione dei dati ridondante in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato **Error** nell'interfaccia utente dell'elemento. • Stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture vengono sospese. Corrisponde allo stato **critico** nell'interfaccia utente dell'elemento.	stringa
SliceReserveUsedThresholdPct	Condizione di errore. Viene generato un avviso di sistema se l'utilizzo riservato dello strato è superiore al valore sliceReserveUsedThresholdPct restituito.	intero

Stage2AwareThreshold	Condizione di consapevolezza. Il valore impostato per il livello di soglia del cluster "fase 2".	intero
Stage2BlockThresholdByte	Il numero di byte utilizzati dal cluster in cui si verifica una condizione di fullness fase 2.	intero
Stage2MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness fase 2.	
Stage3BlockThresholdBytes	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness fase 3.	intero
Stage3BlockThresholdPercent	Il valore percentuale impostato per la fase 3. Con questa percentuale piena, viene visualizzato un avviso nel registro degli avvisi.	intero
Stage3LowThreshold	Condizione di errore. La soglia alla quale viene creato un avviso di sistema a causa della bassa capacità di un cluster.	intero
Stage3MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 3.	
Stage4BlockThresholdByte	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness fase 4.	intero
Stage4CriticalThreshold	Condizione di errore. La soglia alla quale viene creato un avviso di sistema per avvisare in caso di capacità estremamente bassa su un cluster.	intero
Stage4MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 4.	

Stage5BlockThresholdByte	Il numero di byte di storage utilizzati dal cluster in cui si verifica una condizione di fullness della fase 5.	intero
Stage5MetadataThresholdBytes	Il numero di byte di metadati utilizzati dal cluster in cui si verifica una condizione di fullness della fase 5.	
SumTotalClusterBytes	La capacità fisica del cluster, misurata in byte.	intero
SumTotalMetadataClusterBytes	La quantità totale di spazio che è possibile utilizzare per memorizzare i metadati.	intero
SumUsedClusterBytes	Il numero di byte di storage utilizzati nel cluster.	intero
SumUsedMetadataClusterBytes	La quantità di spazio utilizzata sui dischi dei volumi per memorizzare i metadati.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method" : "ModifyClusterFullThreshold",
   "params" : {
               "stage3BlockThresholdPercent" : 3
               },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "blockFullness": "stage1Happy",
    "fullness": "stage3Low",
    "maxMetadataOverProvisionFactor": 5,
    "metadataFullness": "stage3Low",
    "sliceReserveUsedThresholdPct": 5,
    "stage2AwareThreshold": 3,
    "stage2BlockThresholdBytes": 2640607661261,
    "stage3BlockThresholdBytes": 8281905846682,
    "stage3BlockThresholdPercent": 3,
    "stage3LowThreshold": 2,
    "stage4BlockThresholdBytes": 8641988709581,
    "stage4CriticalThreshold": 1,
    "stage5BlockThresholdBytes": 12002762096640,
    "sumTotalClusterBytes": 12002762096640,
    "sumTotalMetadataClusterBytes": 404849531289,
    "sumUsedClusterBytes": 45553617581,
    "sumUsedMetadataClusterBytes": 31703113728
  }
}
```


Novità dalla versione

9.6

ModifyClusterInterfacePreference

Il `ModifyClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di storage che eseguono il software Element di modificare una preferenza di interfaccia cluster esistente. Questo metodo è per uso interno.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome della preferenza dell'interfaccia del cluster da modificare.	stringa	Nessuno	Sì

valore	Il nuovo valore della preferenza dell'interfaccia del cluster.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "ModifyClusterInterfacePreference",
    "params": {
    "name": "testname",
    "value": "newvalue"
},
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {}
}
```

Novità dalla versione

11.0

RemoveNode

È possibile utilizzare `RemoveNodes` per rimuovere uno o più nodi che non devono più partecipare al cluster.

Prima di rimuovere un nodo, è necessario rimuovere tutti i dischi contenuti nel nodo utilizzando `RemoveDrives` metodo. Non è possibile rimuovere un nodo fino a. `RemoveDrives` il processo è stato completato e tutti i dati sono stati migrati lontano dal nodo. Dopo aver rimosso un nodo, si registra come nodo in sospeso. È possibile aggiungere di nuovo il nodo o spegnerlo (la disattivazione del nodo lo rimuove dall'elenco dei nodi in sospeso).

Rimozione del nodo master del cluster

Se si utilizza `RemoveNodes` per rimuovere il nodo master del cluster, il metodo potrebbe scadere prima di restituire una risposta. Se la chiamata al metodo non riesce a rimuovere il nodo, eseguire nuovamente la chiamata al metodo. Si noti che se si rimuove il nodo master del cluster insieme ad altri nodi, è necessario utilizzare una chiamata separata per rimuovere il nodo master del cluster da solo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
IgnoreEnsembleTolerranceChange	Ignora le modifiche apportate alla tolleranza di errore del nodo dell'ensemble durante la rimozione dei nodi. Se il cluster di storage utilizza schemi di protezione dei dati che tollerano guasti a più nodi e la rimozione dei nodi ridurrebbe la tolleranza di errore del nodo dell'insieme, la rimozione del nodo normalmente non riesce con un errore. È possibile impostare questo parametro su true per disattivare la verifica della tolleranza dell'insieme in modo che la rimozione del nodo abbia esito positivo.	booleano	falso	No
nodi	Elenco di NodeID per i nodi da rimuovere.	array intero	Nessuno	Sì

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveNodes",
   "params": {
     "nodes"  : [3,4,5]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1
  "result" : {},
}
```

Novità dalla versione

9.6

SetLoginSessionInfo

È possibile utilizzare `SetLoginSessionInfo` metodo per impostare il periodo di validità dell'autenticazione di accesso per una sessione. Una volta trascorso il periodo di accesso senza attività sul sistema, l'autenticazione scade. Sono necessarie nuove credenziali di accesso per continuare l'accesso al cluster dopo lo scadere del periodo di accesso.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
timeout	Periodo di scadenza dell'autenticazione del cluster. Formattato in HH:mm:ss. Ad esempio, è possibile utilizzare 01:30:00, 00:90:00 e 00:00:5400 per un periodo di timeout di 90 minuti. Il valore di timeout minimo è di 1 minuto. Quando un valore non viene fornito o viene impostato su zero, la sessione di accesso non presenta alcun valore di timeout.	stringa	30 minuti	No

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "SetLoginSessionInfo",
  "params": {
    "timeout" : "01:30:00"
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

Spegnere

È possibile utilizzare `Shutdown` metodo per riavviare o arrestare i nodi in un cluster. Questo metodo consente di arrestare un singolo nodo, più nodi o tutti i nodi del cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nodi	Elenco di NodeID per i nodi da riavviare o arrestare.	array intero	Nessuno	Sì
opzione	Azione da intraprendere per il cluster. Valori possibili: * Restart: Riavvia il cluster. * Halt: Esegue uno spegnimento completo.	stringa	riavviare	No

Valore restituito

Questo metodo non ha alcun valore restituito. == Richieste di esempio per questo metodo sono simili all'esempio seguente:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Novità dalla versione

9.6

Metodi API per la creazione di cluster

È possibile utilizzare questi metodi API per creare un cluster di storage. Tutti questi metodi devono essere utilizzati rispetto all'endpoint API su un singolo nodo.

- CheckProposedCluster
- CreateCluster
- GetBootstrapConfig

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CheckProposedCluster

È possibile utilizzare `CheckProposedCluster` metodo per testare un insieme di nodi di storage prima di creare un cluster di storage con essi per identificare possibili errori o errori che si verificherebbero dal tentativo, come funzionalità di nodi misti non bilanciati o tipi di nodi non supportati per cluster di storage a due nodi.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nodi	Un elenco degli indirizzi IP dello storage del set iniziale di nodi di storage che compongono il cluster di storage.	array di stringhe	Nessuno	Sì
forza	Impostare su true per l'esecuzione su tutti i nodi di storage nel cluster di storage.	booleano	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ProposedClusterValid	Indica se i nodi di storage proposti costituirebbero o meno un cluster di storage valido. Valori possibili: • vero • falso	booleano
ProposedClusterErrors	Errori che si verificano se un cluster di storage è stato creato utilizzando i nodi di storage proposti.	array di stringhe

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "CheckProposedCluster",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Novità dalla versione

11.0

CreateCluster

È possibile utilizzare `CreateCluster` metodo per inizializzare il nodo in un cluster che ha la proprietà degli indirizzi "mvip" e "svip". Ogni nuovo cluster viene inizializzato utilizzando l'IP di gestione (MIP) del primo nodo del cluster. Questo metodo aggiunge automaticamente tutti i nodi configurati nel cluster. È necessario utilizzare questo metodo solo una volta ogni volta che viene inizializzato un nuovo cluster.

> Dopo aver effettuato l'accesso al nodo master del cluster ed eseguito GetBootStrapConfig Metodo per ottenere gli indirizzi IP per gli altri nodi che si desidera includere nel cluster, è possibile eseguire il metodo CreateCluster sul nodo master del cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AccetteEula	Indicare l'accettazione del Contratto di licenza con l'utente finale al momento della creazione del cluster. Per accettare l'EULA, impostare questo parametro su true.	booleano	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
EnableSoftwareEncryptionAtRest	Attivare questo parametro per utilizzare la crittografia basata su software a riposo. Il valore predefinito è false su tutti i cluster. Una volta attivata, la crittografia software a riposo non può essere disattivata nel cluster.	booleano	vero	No
mvip	Indirizzo IP mobile (virtuale) per il cluster sulla rete di gestione.	stringa	Nessuno	Sì
nodi	Indirizzi CIP/SIP dell'insieme iniziale di nodi che compongono il cluster. L'IP di questo nodo deve essere presente nell'elenco.	array di stringhe	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Numero d'ordine	Numero ordine di vendita alfanumerico. Richiesto su piattaforme basate su software.	stringa	Nessuno	No (piattaforme basate su hardware) Sì (piattaforme basate su software)
password	Password iniziale per l'account di amministrazione del cluster.	stringa	Nessuno	Sì
Numero di serie	Numero di serie alfanumerico a nove cifre. Potrebbe essere richiesto sulle piattaforme basate su software.	stringa	Nessuno	No (piattaforme basate su hardware) Sì (piattaforme basate su software)
svip	Indirizzo IP mobile (virtuale) per il cluster sulla rete di storage (iSCSI).	stringa	Nessuno	Sì
nome utente	Nome utente dell'amministratore del cluster.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "CreateCluster",
  "params": {
    "acceptEula": true,
    "mvip": "10.0.3.1",
    "svip": "10.0.4.1",
    "username": "Admin1",
    "password": "9R7ka4rEPa2uREtE",
    "attributes": {
      "clusteraccountnumber": "axdf323456"
    },
    "nodes": [
      "10.0.2.1",
      "10.0.2.2",
      "10.0.2.3",
      "10.0.2.4"
    ]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id" : 1,
"result" : {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- "GetBootstrapConfig"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetBootstrapConfig

È possibile utilizzare `GetBootstrapConfig` metodo per ottenere informazioni sul cluster e sul nodo dal file di configurazione di bootstrap. Utilizzare questo metodo API su un singolo nodo prima di unirsi a un cluster. Le informazioni restituite da questo metodo

vengono utilizzate nell'interfaccia di configurazione del cluster quando si crea un cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
Nome cluster	Nome del cluster.	stringa
mvip	Indirizzo MVIP del cluster. Vuoto se il nodo non fa parte di un cluster.	stringa
Nodename	Nome del nodo.	stringa
nodi	Elenco di informazioni relative a ciascun nodo in attesa di unirsi al cluster. Valori possibili: • ChassisType: (Stringa) piattaforma hardware del nodo. • cip: (String) Indirizzo IP del cluster del nodo. • Compatibile: (booleano) indica se il nodo è compatibile con il nodo su cui è stata eseguita la chiamata API. • Hostname (Nome host): (Stringa) Nome host del nodo. • mip: (String) l'indirizzo IP di gestione IPv4 del nodo. • MipV6: (Stringa) l'indirizzo IP di gestione IPv6 del nodo. • NodeType: (String)Nome del modello del nodo. • Version (versione): (Stringa)versione del software attualmente installato sul nodo.	Array di oggetti JSON
svip	Indirizzo SVIP del cluster. Null se il nodo non fa parte di un cluster.	stringa

Nome	Descrizione	Tipo
versione	Versione del software Element attualmente installato sul nodo chiamato da questo metodo API.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetBootstrapConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id":1,
    "result":{
        "clusterName":"testname",
        "nodeName":"testnode",
        "svip": "10.117.1.5",
        "mvip": "10.117.1.6",
        "nodes":[
            {
                "chassisType":"R630",
                "cip":"10.117.115.16",
                "compatible":true,
                "hostname":"NLABP1132",
                "mip":"10.117.114.16",
                "mipV6":"fd20:8b1e:b256:45a::16",
                "nodeType":"SF2405",
                "role":"Storage",
                "version":"11.0"
            },
            {
                "chassisType":"R630",
                "cip":"10.117.115.17",
                "compatible":true,
                "hostname":"NLABP1133",
                "mip":"10.117.114.17",
                "mipV6":"fd20:8b1e:b256:45a::17",
                "nodeType":"SF2405",
                "role":"Storage",
                "version":"11.0"
            },
            {
                "chassisType":"R630",
                "cip":"10.117.115.18",
                "compatible":true,
                "hostname":"NLABP1134",
                "mip":"10.117.114.18",
                "mipV6":"fd20:8b1e:b256:45a::18",
                "nodeType":"SF2405",
                "role":"Storage",
                "version":"11.0"
            }
        ],
        "version":"11.0"
    }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

CreateCluster

Metodi API del disco

È possibile utilizzare i metodi API del disco per aggiungere e gestire dischi disponibili per un cluster di storage. Quando si aggiunge un nodo di storage al cluster di storage o si installano nuove unità in un nodo di storage esistente, le unità sono disponibili per essere aggiunte al cluster di storage.

- AddDrive
- GetDriveHardwareInfo
- GetDriveStats
- ListDrive
- ListDriveStats
- RemoveDrives
- SecureEraseDrive

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddDrive

È possibile utilizzare `AddDrives` metodo per aggiungere uno o più dischi disponibili al cluster, consentendo ai dischi di ospitare una parte dei dati per il cluster.

Quando si aggiunge un nodo di storage al cluster o si installano nuove unità in un nodo esistente, le nuove unità vengono contrassegnate come disponibili e devono essere aggiunte tramite AddDrives prima di poter essere utilizzate. Utilizzare ListDrive metodo per visualizzare le unità disponibili per l'aggiunta. Quando si aggiunge un disco, il sistema determina automaticamente il tipo di disco che deve essere.

Il metodo è asincrono e viene restituito non appena vengono avviati i processi di ribilanciamento dei dischi nel cluster. Tuttavia, potrebbe essere necessario più tempo per il ribilanciamento dei dati nel cluster utilizzando le nuove unità aggiunte; il ribilanciamento continua anche dopo il completamento della chiamata al metodo AddDrives. È possibile utilizzare GetAsyncResult Metodo per eseguire query su asyncHandle restituito dal metodo. Una volta restituito il metodo AddDrives, è possibile utilizzare ListSyncJobs metodo per vedere l'avanzamento del ribilanciamento dei dati con i nuovi dischi.

Quando si aggiungono più dischi, è più efficiente aggiungerli in una singola chiamata al metodo AddDrives piuttosto che in più singoli metodi con un singolo disco ciascuno. In questo modo si riduce la quantità di bilanciamento dei dati necessaria per stabilizzare il carico di storage sul cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dischi	Informazioni su ciascun disco da aggiungere al cluster. Valori possibili: • DriveID: L'ID del disco da aggiungere (numero intero). • Type (tipo): Il tipo di disco da aggiungere (stringa). I valori validi sono "slice", "block" o "volume". Se omesso, il sistema assegna il tipo corretto.	Array di oggetti JSON	Nessuno	Sì (il tipo è opzionale)

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
AsyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1,
  "method": "AddDrives",
  "params": {
    "drives": [
      {
        "driveID": 1,
        "type": "slice"
      },
      {
        "driveID": 2,
        "type": "block"
      },
      {
        "driveID": 3,
        "type": "block"
      }
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListDrive
- ListSyncJobs

GetDriveHardwareInfo

È possibile utilizzare `GetDriveHardwareInfo` metodo per ottenere tutte le informazioni

hardware per il disco specificato. In genere, sono inclusi produttori, vendor, versioni e altre informazioni di identificazione hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID del driver	ID del disco per la richiesta.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
risultato	Sono state restituite informazioni hardware per l'ID unità specificato.	HardwareInfo

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetDriveHardwareInfo",
   "params": {
     "driveID": 5
   },
   "id" : 100
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 100,
   "result" : {
     "driveHardwareInfo" : {
       "description" : "ATA Drive",
       "dev" : "8:80",
       "devpath" :
"/devices/pci0000:40/0000:40:01.0/0000:41:00.0/host6/port-6:0/expander-
6:0/port-6:0:4/end_device-6:0:4/target6:0:4/6:0:4:0/block/sdf",
       "driveSecurityAtMaximum" : false,
       "driveSecurityFrozen" : false
       "driveSecurityLocked" : false,
       "logicalname" : "/dev/sdf",
       "product" : "INTEL SSDSA2CW300G3",
       "securityFeatureEnabled" : false,
       "securityFeatureSupported" : true,
       "serial" : "CVPR121400NT300EGN",
       "size" : "300069052416",
       "uuid" : "7e1fd5b9-5acc-8991-e2ac-c48f813a3884",
       "version" : "4PC10362"
     }
   }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

ListDrive

GetDriveStats

È possibile utilizzare `GetDriveStats` metodo per ottenere misurazioni di attività di alto livello per un singolo disco. I valori sono cumulativi dall'aggiunta del disco al cluster. Alcuni valori sono specifici dei dischi a blocchi. Quando si esegue questo metodo, vengono restituiti dati statistici per i tipi di unità a blocchi o metadati.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID del driver	ID del disco per la richiesta.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
DriveStats	Informazioni sull'attività del disco per l'ID unità specificato.	DriveStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetDriveStats",
   "params": {
     "driveID": 3
   },
   "id" : 1
}
```

Esempio di risposta (disco a blocchi)

Questo metodo restituisce una risposta simile all'esempio seguente per un disco a blocchi:

```
{
  "id": 1,
  "result": {
    "driveStats": {
      "driveID": 10,
      "failedDieCount": 0,
      "lifeRemainingPercent": 99,
      "lifetimeReadBytes": 26471661830144,
      "lifetimeWriteBytes": 13863852441600,
      "powerOnHours": 33684,
      "readBytes": 10600432105,
      "readOps": 5101025,
      "reallocatedSectors": 0,
      "reserveCapacityPercent": 100,
      "timestamp": "2016-10-17T20:23:45.456834Z",
      "totalCapacity": 300069052416,
      "usedCapacity": 6112226545,
      "usedMemory": 114503680,
      "writeBytes": 53559500896,
      "writeOps": 25773919
    }
  }
}
```


Esempio di risposta (unità di metadati del volume)

Questo metodo restituisce una risposta simile all'esempio seguente per un'unità di metadati di un volume:

```
{
  "id": 1,
  "result": {
    "driveStats": {
      "activeSessions": 8,
      "driveID": 12,
      "failedDieCount": 0,
      "lifeRemainingPercent": 100,
      "lifetimeReadBytes": 2308544921600,
      "lifetimeWriteBytes": 1120986464256,
      "powerOnHours": 16316,
      "readBytes": 1060152152064,
      "readOps": 258826209,
      "reallocatedSectors": 0,
      "reserveCapacityPercent": 100,
      "timestamp": "2016-10-17T20:34:52.456130Z",
      "totalCapacity": 134994670387,
      "usedCapacity": null,
      "usedMemory": 22173577216,
      "writeBytes": 353346510848,
      "writeOps": 86266238
    }
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

ListDrive

ListDrive

È possibile utilizzare `ListDrives` metodo per elencare i dischi presenti nei nodi attivi del cluster. Questo metodo restituisce i dischi che sono stati aggiunti come metadati di volume o dischi a blocchi, nonché i dischi che non sono stati aggiunti e che sono disponibili.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dischi	Elenco dei dischi nel cluster.	disco array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListDrives",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
     "drives" : [
       {
         "attributes" : {},
         "capacity" : 299917139968,
         "driveID" : 35,
         "nodeID" : 5,
         "serial" : "scsi-SATA_INTEL_SSDSA2CW6CVPR141502R3600FGN-part2",
         "slot" : 0,
         "status" : "active",
         "type" : "volume"
       },
       {
         "attributes" : {},
         "capacity" : 600127266816,
         "driveID" : 36,
         "nodeID" : 5,
         "serial" : "scsi-SATA_INTEL_SSDSA2CW6CVPR1415037R600FGN",
         "slot" : 6,
         "status" : "active",
         "type" : "block"
       }
     }
   ]
}
```


Novità dalla versione

9.6

ListDriveStats

È possibile utilizzare `ListDriveStats` metodo per elencare le misurazioni delle attività di alto livello per più dischi nel cluster. Per impostazione predefinita, questo metodo restituisce statistiche per tutti i dischi nel cluster e queste misurazioni sono cumulative dall'aggiunta del disco al cluster. Alcuni valori restituiti da questo metodo sono specifici per i dischi a blocchi, mentre altri sono specifici per i dischi metadati.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dischi	Elenco degli ID del disco (ID disco) per i quali restituire le statistiche del disco. Se si omette questo parametro, vengono restituite le misurazioni per tutti i dischi.	array intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
DriveStats	Elenco delle informazioni sull'attività del disco per ciascun disco.	DriveStats array
errori	Questo elenco contiene l'ID del driver e il relativo messaggio di errore. È sempre presente e vuoto se non ci sono errori.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1,
  "method": "ListDriveStats",
  "params": {
    "drives":[22,23]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "driveStats": [
      {
        "driveID": 22,
        "failedDieCount": 0,
        "lifeRemainingPercent": 84,
        "lifetimeReadBytes": 30171004403712,
        "lifetimeWriteBytes": 103464755527680,
        "powerOnHours": 17736,
        "readBytes": 14656542,
         "readOps": 3624,
        "reallocatedSectors": 0,
        "reserveCapacityPercent": 100,
        "timestamp": "2016-03-01T00:19:24.782735Z",
        "totalCapacity": 300069052416,
        "usedCapacity": 1783735635,
        "usedMemory": 879165440,
        "writeBytes": 2462169894,
        "writeOps": 608802
      }
    ],
    "errors": [
      {
        "driveID": 23,
        "exception": {
          "message": "xStatCheckpointDoesNotExist",
          "name": "xStatCheckpointDoesNotExist"
        }
      }
    ]
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

GetDriveStats

RemoveDrives

È possibile utilizzare `RemoveDrives` metodo per rimuovere in modo proattivo i dischi

che fanno parte del cluster. È possibile utilizzare questo metodo per ridurre la capacità del cluster o prepararsi alla sostituzione dei dischi in via di esaurimento. `RemoveDrives` Crea una terza copia dei dati del blocco sugli altri nodi nel cluster e attende il completamento della sincronizzazione prima di spostare le unità nell'elenco "disponibili". Le unità presenti nell'elenco "disponibili" vengono completamente rimosse dal sistema e non dispongono di servizi in esecuzione o di dati attivi.

`RemoveDrives` è un metodo asincrono. A seconda della capacità totale dei dischi da rimuovere, la migrazione di tutti i dati potrebbe richiedere alcuni minuti.

Quando si rimuovono più dischi, utilizzare un disco singolo `RemoveDrives` chiamata al metodo piuttosto che a più singoli metodi con un singolo disco ciascuno. In questo modo si riduce la quantità di bilanciamento dei dati necessaria per stabilizzare in modo uniforme il carico di storage sul cluster.

È inoltre possibile rimuovere i dischi con stato "failed" (guasto) utilizzando `RemoveDrives`. Quando si rimuove un disco con uno stato "failed" (guasto), il disco non torna allo stato "Available" (disponibile) o "Active" (attivo). L'unità non è disponibile per l'utilizzo nel cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dischi	Elenco di driveID da rimuovere dal cluster.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
AsyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveDrives",
   "params": {
      "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result" : {
     "asyncHandle": 1
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListDrive

SecureEraseDrive

È possibile utilizzare `SecureEraseDrives` metodo per rimuovere eventuali dati residui dalle unità con stato "disponibile". È possibile utilizzare questo metodo per sostituire un'unità prossima alla fine della sua vita utile che conteneva dati sensibili. Questo metodo utilizza un comando Security Erase Unit per scrivere un modello predeterminato sul disco e reimpostare la chiave di crittografia sul disco. Il completamento di questo metodo asincrono potrebbe richiedere alcuni minuti.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dischi	Elenco degli ID del disco da cancellare in modo sicuro.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
AsyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "SecureEraseDrives",
   "params": {
     "drives"  : [3, 4, 5]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1
   "result" : {
     "asyncHandle" : 1
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListDrive

Metodi API Fibre Channel

È possibile utilizzare i metodi API Fibre Channel per aggiungere, modificare o rimuovere i membri del nodo Fibre Channel di un cluster di storage.

- GetVolumeAccessGroupLunAssignments
- ListFiberChannelPortInfo
- ListFiberChannelSessions
- ListNodeFibreChannelPortInfo
- ModifyVolumeAccessGroupLunAssignments

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetVolumeAccessGroupLunAssignments

È possibile utilizzare `GetVolumeAccessGroupLunAssignments` Metodo per recuperare i dettagli sulle mappature LUN di un gruppo di accesso a un volume specificato.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	Un ID univoco del gruppo di accesso al volume utilizzato per restituire informazioni.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroupLunAssignments	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetVolumeAccessGroupLunAssignments",
   "params": {
      "volumeAccessGroupID": 5
    },
  "id" : 1
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
    "volumeAccessGroupLunAssignments" : {
       "volumeAccessGroupID" : 5,
       "lunAssignments" : [
          {"volumeID" : 5, "lun" : 0},
          {"volumeID" : 6, "lun" : 1},
          {"volumeID" : 7, "lun" : 2},
          {"volumeID" : 8, "lun" : 3}
       ],
       "deletedLunAssignments" : [
           {"volumeID" : 44, "lun" : 44}
       ]
    }
  }
}
```

Novità dalla versione

9.6

ListFiberChannelPortInfo

È possibile utilizzare `ListFibreChannelPortInfo` Metodo per elencare le informazioni sulle porte Fibre Channel.

Questo metodo API è destinato all'utilizzo su singoli nodi; sono richiesti un ID utente e una password per l'accesso a singoli nodi Fibre Channel. Tuttavia, questo metodo può essere utilizzato nel cluster se il parametro force è impostato su true. Se utilizzate nel cluster, vengono elencate tutte le interfacce Fibre Channel.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare su true per l'esecuzione su tutti i nodi del cluster.	booleano	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
FiberChannelPorts	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	FiberChannelPort array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListFibreChannelPortInfo",
    "params": {},
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "fibreChannelPortInfo": {
      "5": {
        "result": {
          "fibreChannelPorts": [
            {
             "firmware": "7.04.00 (d0d5)",
             "hbaPort": 1,
             "model": "QLE2672",
             "nPortID": "0xc70084",
             "pciSlot": 3,
             "serial": "BFE1335E03500",
             "speed": "8 Gbit",
             "state": "Online",
             "switchWwn": "20:01:00:2a:6a:98:a3:41",
             "wwnn": "5f:47:ac:c8:3c:e4:95:00",
             "wwpn": "5f:47:ac:c0:3c:e4:95:0a"
            },
            {
              "firmware": "7.04.00 (d0d5)",
```

```
            "hbaPort": 2,
            "model": "QLE2672",
            "nPortID": "0x0600a4",
            "pciSlot": 3,
            "serial": "BFE1335E03500",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:9c:71:01",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:0b"
          },
          {
            "firmware": "7.04.00 (d0d5)",
            "hbaPort": 1,
            "model": "QLE2672",
            "nPortID": "0xc70044",
            "pciSlot": 2,
            "serial": "BFE1335E04029",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:98:a3:41",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:08"
          },
          {
            "firmware": "7.04.00 (d0d5)",
            "hbaPort": 2,
            "model": "QLE2672",
            "nPortID": "0x060044",
            "pciSlot": 2,
            "serial": "BFE1335E04029",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:9c:71:01",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:09"
          }
        ]
      }
    },
    "6": {
      "result": {
          "fibreChannelPorts": [
        {
           "firmware": "7.04.00 (d0d5)",
           "hbaPort": 1,
```

```
            "model": "QLE2672",
            "nPortID": "0x060084",
            "pciSlot": 3,
            "serial": "BFE1335E04217",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:9c:71:01",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:02"
        },
        {
            "firmware": "7.04.00 (d0d5)",
            "hbaPort": 2,
            "model": "QLE2672",
            "nPortID": "0xc700a4",
            "pciSlot": 3,
            "serial": "BFE1335E04217",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:98:a3:41",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:03"
        },
        {
            "firmware": "7.04.00 (d0d5)",
            "hbaPort": 1,
            "model": "QLE2672",
            "nPortID": "0xc70064",
            "pciSlot": 2,
            "serial": "BFE1341E09515",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:98:a3:41",
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:00"
        },
        {
            "firmware": "7.04.00 (d0d5)",
            "hbaPort": 2,
            "model": "QLE2672",
            "nPortID": "0x060064",
            "pciSlot": 2,
            "serial": "BFE1341E09515",
            "speed": "8 Gbit",
            "state": "Online",
            "switchWwn": "20:01:00:2a:6a:9c:71:01",
```

```
            "wwnn": "5f:47:ac:c8:3c:e4:95:00",
            "wwpn": "5f:47:ac:c0:3c:e4:95:01"
          }
        ]
      }
    }
  }
}
```

Novità dalla versione

9.6

ListFiberChannelSessions

È possibile utilizzare `ListFibreChannelSessions` Metodo per elencare informazioni sulle sessioni Fibre Channel su un cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Un elenco di oggetti che descrivono sessioni Fibre Channel attive nel cluster.	sessione array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListFibreChannelSessions",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
     "sessions" : [
    {
       "initiatorWWPN" : "21:00:00:0e:1e:14:af:40",
       "nodeID" : 5,
       "serviceID" : 21,
       "targetWWPN": "5f:47:ac:c0:00:00:00:10",
       "volumeAccessGroupID": 7
    },
    {
       "initiatorWWPN" : "21:00:00:0e:1e:14:af:40",
       "nodeID" : 1,
       "serviceID" : 22,
       "targetWWPN": "5f:47:ac:c0:00:00:00:11",
       "volumeAccessGroupID": 7
    }
    ]
  }
}
```

Novità dalla versione

9.6

ListNodeFibreChannelPortInfo

È possibile utilizzare `ListNodeFibreChannelPortInfo` Metodo per elencare informazioni sulle porte Fibre Channel di un nodo.

Questo metodo API è destinato all'utilizzo su singoli nodi; sono richiesti un ID utente e una password per l'accesso a singoli nodi Fibre Channel. Se utilizzate nel cluster, vengono elencate tutte le interfacce Fibre Channel.

Parametro

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
FiberChannelPorts	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	FiberChannelPort array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListNodeFibreChannelPortInfo",
   "params": {
       "nodeID": 5,
       "force": true
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "fibreChannelPorts": [
      {
        "firmware": "7.04.00 (d0d5)",
        "hbaPort": 1,
        "model": "QLE2672",
        "nPortID": "0xc7002c",
        "pciSlot": 3,
        "serial": "BFE1335E03500",
        "speed": "8 Gbit",
        "state": "Online",
        "switchWwn": "20:01:00:2a:6a:98:a3:41",
        "wwnn": "5f:47:ac:c8:35:54:02:00",
        "wwpn": "5f:47:ac:c0:35:54:02:02"
      },
      {
         "firmware": "7.04.00 (d0d5)",
         "hbaPort": 2,
         "model": "QLE2672",
         "nPortID": "0x06002d",
```

```
          "pciSlot": 3,
          "serial": "BFE1335E03500",
          "speed": "8 Gbit",
          "state": "Online",
          "switchWwn": "20:01:00:2a:6a:9c:71:01",
          "wwnn": "5f:47:ac:c8:35:54:02:00",
          "wwpn": "5f:47:ac:c0:35:54:02:03"
       },
       {
          "firmware": "7.04.00 (d0d5)",
          "hbaPort": 1,
          "model": "QLE2672",
          "nPortID": "0xc7002a",
          "pciSlot": 2,
          "serial": "BFE1335E04029",
          "speed": "8 Gbit",
          "state": "Online",
          "switchWwn": "20:01:00:2a:6a:98:a3:41",
          "wwnn": "5f:47:ac:c8:35:54:02:00",
          "wwpn": "5f:47:ac:c0:35:54:02:00"
       },
       {
          "firmware": "7.04.00 (d0d5)",
          "hbaPort": 2,
          "model": "QLE2672",
          "nPortID": "0x06002a",
          "pciSlot": 2,
          "serial": "BFE1335E04029",
          "speed": "8 Gbit",
          "state": "Online",
          "switchWwn": "20:01:00:2a:6a:9c:71:01",
          "wwnn": "5f:47:ac:c8:35:54:02:00",
          "wwpn": "5f:47:ac:c0:35:54:02:01"
       }
     ]
   }
}
```


Novità dalla versione

9.6

ModifyVolumeAccessGroupLunAssignments

È possibile utilizzare `ModifyVolumeAccessGroupLunAssignments` Metodo per definire assegnazioni LUN personalizzate per volumi specifici.

Questo metodo modifica solo i valori LUN impostati nel parametro lunAssignments nel gruppo di accesso al volume. Tutte le altre assegnazioni LUN rimangono invariate.

I valori di assegnazione del LUN devono essere univoci per i volumi in un gruppo di accesso al volume. Non è possibile definire valori LUN duplicati all'interno di un gruppo di accesso al volume. Tuttavia, è possibile utilizzare nuovamente gli stessi valori LUN in diversi gruppi di accesso ai volumi.

I valori LUN validi vanno da 0 a 16383. Il sistema genera un'eccezione se si passa un valore LUN al di fuori di questo intervallo. Nessuna delle assegnazioni LUN specificate viene modificata in caso di eccezione.

ATTENZIONE:

Se si modifica l'assegnazione di un LUN per un volume con i/o attivo, l'i/o può essere interrotto. È necessario modificare la configurazione del server prima di modificare le assegnazioni dei LUN dei volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	ID univoco del gruppo di accesso al volume per il quale verranno modificate le assegnazioni del LUN.	intero	Nessuno	Sì
LunAssignment	Gli ID del volume con nuovi valori LUN assegnati.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroupLunAssignments	Oggetto contenente i dettagli delle assegnazioni LUN del gruppo di accesso volume modificato.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ModifyVolumeAccessGroupLunAssignments",
   "params": {
       "volumeAccessGroupID" : 218,
       "lunAssignments" : [
           {"volumeID" : 832, "lun" : 0},
           {"volumeID" : 834, "lun" : 1}
        ]
    },
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroupLunAssignments": {
      "deletedLunAssignments": [],
      "lunAssignments": [
        {
          "lun": 0,
          "volumeID": 832
        },
        {
          "lun": 1,
          "volumeID": 834
        }
      ],
      "volumeAccessGroupID": 218
    }
  }
}
```

Novità dalla versione

9.6

Metodi API initiator

I metodi Initiator consentono di aggiungere, rimuovere, visualizzare e modificare gli oggetti iSCSI Initiator, che gestiscono la comunicazione tra il sistema di storage e i client

di storage esterni.

- CreateInitiator
- DeleteInitiator
- ListInitiator
- ModifyInitiator

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CreateInitiator

È possibile utilizzare `CreateInitiators` Per creare più nuovi IQN iniziatori o nomi di World Wide Port (WWPN) e, facoltativamente, assegnarli alias e attributi. Quando si utilizza `CreateInitiators` per creare nuovi iniziatori, è anche possibile aggiungerli ai gruppi di accesso ai volumi.

Se l'operazione non riesce a creare uno degli iniziatori forniti nel parametro, il metodo restituisce un errore e non crea alcun iniziatore (non è possibile un completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
iniziatori	Un elenco di oggetti contenente le caratteristiche di ciascun nuovo iniziatore. Oggetti: • `alias`(Facoltativo) il soprannome da assegnare a questo iniziatore. (stringa) • `attributes`(Facoltativo) un insieme di attributi JSON da assegnare a questo iniziatore. (Oggetto JSON) • `chapUsername`: (Opzionale) il nome utente CHAP univoco per questo iniziatore. Il valore predefinito è il nome dell'iniziatore (IQN) se non viene specificato durante la creazione e requireChap è true. (stringa) • `initiatorSecret`(Facoltativo) il segreto CHAP utilizzato per autenticare l'iniziatore. Il valore predefinito è un segreto generato casualmente se non specificato durante la creazione e requireChap è true. (stringa)	Array di oggetti JSON	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
iniziatori	Elenco di oggetti che descrivono gli iniziatori appena creati.	iniziatore array

Errore

Questo metodo può restituire il seguente errore:

Nome	Descrizione
XInitialatorExists	Restituito se il nome dell'iniziatore scelto esiste già.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 3291,
  "method": "CreateInitiators",
  "params": {
    "initiators": [
      {
        "name": "iqn.1993-08.org.debian:01:288170452",
        "alias": "example1"
      },
      {
        "name": "iqn.1993-08.org.debian:01:297817012",
        "alias": "example2"
      }
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

- `name`: (Obbligatorio) il
- `requireChap`: (Opzionale) True se è richiesto CHAP durante (booleano)
- `targetSecret`(Facoltativo) il segreto CHAP
- `virtualNetworkIDs`(Facoltativo) l'elenco degli identificatori di rete virtuale associati a questo iniziatore. Se si definiscono una o più reti virtuali, l'iniziatore è in grado di accedere solo a tali reti virtuali. Se non si definiscono reti virtuali, questo

```
{
  "id": 3291,
  "result": {
    "initiators": [
      {
        "alias": "example1",
        "attributes": {},
        "initiatorID": 145,
        "initiatorName": "iqn.1993-08.org.debian:01:288170452",
        "volumeAccessGroups": []
      },
      {
        "alias": "example2",
        "attributes": {},
        "initiatorID": 146,
        "initiatorName": "iqn.1993-08.org.debian:01:297817012",
        "volumeAccessGroups": []
      }
    ]
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

ListInitiator

DeleteInitiator

È possibile utilizzare `DeleteInitiators` per eliminare uno o più iniziatori dal sistema (e da eventuali volumi o gruppi di accesso al volume associati).

Se `DeleteInitiators` non riesce a eliminare uno degli iniziatori forniti nel parametro, il sistema restituisce un errore e non elimina gli iniziatori (non è possibile un completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
iniziatori	Array di ID di iniziatori da eliminare.	array intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Errore

Questo metodo può restituire il seguente errore:

Nome	Descrizione
XInitialatorDoesNotExist	Restituito se il nome dell'iniziatore scelto non esiste.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 5101,
  "method": "DeleteInitiators",
  "params": {
    "initiators": [
      145,
      147
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 5101,
  "result": {}
}
```

Novità dalla versione

9.6

ListInitiator

È possibile utilizzare `ListInitiators` Metodo per ottenere l'elenco degli IQN iniziatori o dei nomi delle World Wide Port (WWPN).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
iniziatori	Un elenco di ID iniziatore da recuperare. È possibile fornire questo parametro o il parametro startInitialorID, ma non entrambi.	array intero	Nessuno	No
ID startInitialatorID	L'ID iniziatore in cui iniziare l'elenco. È possibile fornire questo parametro o il parametro Initiator, ma non entrambi.	intero	0	No
limite	Il numero massimo di oggetti iniziatore da restituire.	intero	(senza limiti)	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
iniziatori	Elenco delle informazioni sull'iniziatore.	iniziatore array

Eccezioni

Questo metodo può avere la seguente eccezione:

Nome	Descrizione
XInvalidParameter	Viene generato se si includono sia l'ID startInitialatorID che i parametri degli iniziatori nella stessa chiamata al metodo.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListInitiators",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "initiators": [
      {
        "alias": "",
        "attributes": {},
        "initiatorID": 2,
        "initiatorName": "iqn.1993-08.org.debian:01:c84ffd71216",
        "volumeAccessGroups": [
          1
        ]
      }
    ]
  }
}
```

Novità dalla versione

9.6

ModifyInitiator

È possibile utilizzare `ModifyInitiators` metodo per modificare gli attributi di uno o più iniziatori esistenti.

Non è possibile modificare il nome di un iniziatore esistente. Se è necessario modificare il nome di un iniziatore, eliminarlo con il DeleteInitiator e crearne uno nuovo con CreateInitiator metodo.

Se ModifyInitiator non riesce a modificare uno degli iniziatori forniti nel parametro, il metodo restituisce un errore e non modifica alcun iniziatore (non è possibile un completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio

iniziatori	Un elenco di oggetti contenente le caratteristiche di ciascun iniziatore da modificare. Oggetti possibili: • `alias`(Facoltativo) un nuovo soprannome da assegnare all'iniziatore. (stringa) • `attributes`(Facoltativo) un nuovo set di attributi JSON da assegnare all'iniziatore. (Oggetto JSON) • `chapUsername`(Facoltativo) un nuovo nome utente CHAP univoco per questo iniziatore. (stringa) • `forceDuringUpgrade`: Completare la modifica dell'iniziatore durante un aggiornamento. • `initiatorID`: (Obbligatorio) l'ID dell'iniziatore da modificare. (intero) • `initiatorSecret`(Facoltativo) un nuovo segreto CHAP utilizzato per autenticare l'iniziatore. (stringa) `requireChap`: (Opzionale) True se CHAP è richiesto per	Array di oggetti JSON	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
iniziatori	Elenco di oggetti che descrivono gli iniziatori appena modificati.	iniziatore array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 6683,
  "method": "ModifyInitiators",
  "params": {
    "initiators": [
      {
        "initiatorID": 2,
        "alias": "alias1",
        "volumeAccessGroupID": null
      },
      {
        "initiatorID": 3,
        "alias": "alias2",
        "volumeAccessGroupID": 1
      }
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

- questo iniziatore. (booleano)
- per autenticare la destinazione (quando si utilizza l'autenticazione
- le reti.
- `volumeAccessGroupID`(Facoltativo) l'ID del gruppo di accesso al volume a cui aggiungere l'iniziatore. Se in precedenza l'iniziatore si trovava in un gruppo di accesso a un volume diverso, viene rimosso dal vecchio gruppo di accesso a un volume. Se questa chiave è

```
{
  "id": 6683,
  "result": {
    "initiators": [
      {
        "alias": "alias1",
        "attributes": {},
        "initiatorID": 2,
        "initiatorName": "iqn.1993-08.org.debian:01:395543635",
        "volumeAccessGroups": []
      },
      {
        "alias": "alias2",
        "attributes": {},
        "initiatorID": 3,
        "initiatorName": "iqn.1993-08.org.debian:01:935573135",
        "volumeAccessGroups": [
          1
        ]
      }
    ]
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

- CreateInitiator
- DeleteInitiator

Metodi API LDAP

È possibile utilizzare il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare l'accesso allo storage Element. I metodi API LDAP descritti in questa sezione consentono di configurare l'accesso LDAP al cluster di storage.

- AddLdapClusterAdmin
- EnableLdapAuthentication
- DisableLdapAuthentication
- GetLdapConfiguration
- TestLdapAuthentication

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddLdapClusterAdmin

È possibile utilizzare `AddLdapClusterAdmin` Per aggiungere un nuovo utente amministratore del cluster LDAP. Un amministratore del cluster LDAP può gestire il cluster utilizzando l'API e gli strumenti di gestione. Gli account amministratore del cluster LDAP sono completamente separati e non correlati agli account tenant standard.

Parametri

È inoltre possibile utilizzare questo metodo per aggiungere un gruppo LDAP definito in Active Directory®. Il livello di accesso assegnato al gruppo viene passato ai singoli utenti del gruppo LDAP.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Controlla i metodi che l'amministratore del cluster può utilizzare.	array di stringhe	Nessuno	Sì
AccetteEula	Accettare il Contratto di licenza con l'utente finale. Impostare su true per aggiungere un account amministratore del cluster al sistema. Se omesso o impostato su false, la chiamata al metodo non riesce.	booleano	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
nome utente	Il nome utente distinto per il nuovo amministratore del cluster LDAP.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "AddLdapClusterAdmin",
  "params": {"username":"cn=mike
jones,ou=ptusers,dc=prodtest,dc=solidfire,dc=net",
    "access": ["administrator", "read"
    ]
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id": 1,
 "result": {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

Controllo degli accessi

EnableLdapAuthentication

È possibile utilizzare `EnableLdapAuthentication` Metodo per configurare una connessione alla directory LDAP per l'autenticazione LDAP a un cluster. Gli utenti che sono membri della directory LDAP possono quindi accedere al sistema di storage utilizzando le proprie credenziali LDAP.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AuthType	Identifica il metodo di autenticazione dell'utente da utilizzare. Valori possibili: • `DirectBind` • `SearchAndBind`	stringa	SearchAndBind	No
GroupSearchBaseDN	Il DN di base della struttura per avviare la ricerca della sottostruttura di gruppo.	stringa	Nessuno	No
GroupSearchType	Controlla il filtro di ricerca di gruppo predefinito utilizzato. Valori possibili: • NoGroups: Nessun supporto di gruppo. • ActiveDirectory: Appartenenza nidificata a tutti i gruppi Active Directory di un utente. • MemberDN: Gruppi di stile MemberDN (livello singolo).	stringa	ActiveDirectory	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Server URI	Elenco separato da virgole degli URI del server LDAP o LDAPS. È possibile aggiungere una porta personalizzata alla fine di un URI LDAP o LDAPS utilizzando i due punti seguiti dal numero della porta. Ad esempio, l'URI "ldap://1.2.3.4" utilizza la porta predefinita e l'URI "ldaps://1.2.3.4:123" utilizza la porta personalizzata 123.	array di stringhe	Nessuno	Sì
UserSearchBaseDN	Il DN di base della struttura per avviare la ricerca nella sottostruttura. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	No
SearchBindDN	Un DN completo con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente. Il DN richiede l'accesso in lettura alla directory LDAP. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SearchBindPassword	La password per l'account searchBindDN utilizzato per la ricerca. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	Sì
UserSearchFilter	Il filtro di ricerca LDAP da utilizzare quando si esegue una query sul server LDAP. La stringa deve avere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente autenticante. Ad esempio, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizzerà il campo sAMAccountName in Active Directory per corrispondere al nome utente immesso al momento dell'accesso al cluster. Questo parametro è necessario quando si utilizza un AuthType di SearchAndBind.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
UserDNTemplate	Modello di stringa utilizzato per definire un modello per la costruzione di un nome distinto utente (DN) completo. La stringa deve avere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente autenticante. Questo parametro è necessario quando si utilizza un AuthType di DirectBind.	stringa	Nessuno	Sì
GroupSearchCustomFilter	Da utilizzare con il tipo di ricerca CustomFilter, un filtro LDAP da utilizzare per restituire il DNS dei gruppi di utenti. La stringa può contenere il testo segnaposto %USERNAME% e %USERDN% da sostituire con il nome utente e il nome utente completo in base alle necessità.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableLdapAuthentication",
  "params": {
     "authType": "SearchAndBind",
     "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
     "groupSearchType": "ActiveDirectory",
     "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
     "searchBindPassword": "zsw@#edcASD12",
     "sslCert": "",
     "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
     "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))",
     "serverURIs":[
           "ldaps://111.22.333.444",
           "ldap://555.66.777.888"
           ]
       },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
"result": {
  }
}
```

Novità dalla versione

9.6

DisableLdapAuthentication

È possibile utilizzare `DisableLdapAuthentication` Metodo per disattivare l'autenticazione LDAP e rimuovere tutte le impostazioni di configurazione LDAP. Questo metodo non rimuove gli account amministratore del cluster configurati per utenti o gruppi. Una volta disattivata l'autenticazione LDAP, gli amministratori del cluster configurati per l'utilizzo dell'autenticazione LDAP non possono più accedere al cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
"result": {}
}
```

Novità dalla versione

9.6

GetLdapConfiguration

È possibile utilizzare `GetLdapConfiguration` Metodo per ottenere la configurazione LDAP attualmente attiva sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito.

Nome	Descrizione	Tipo
LdapConfiguration	Elenco delle impostazioni di configurazione LDAP correnti. Questa chiamata API non restituisce il testo normale della password dell'account di ricerca. **Nota:** se l'autenticazione LDAP è attualmente disattivata, tutte le impostazioni restituite sono vuote ad eccezione di "AuthType" e "groupSearchType", rispettivamente impostate su "SearchAndBind" e "ActiveDirectory".	LdapConfiguration

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "ldapConfiguration": {
        "authType": "SearchAndBind",
        "enabled": true,
        "groupSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
        "groupSearchCustomFilter": "",
        "groupSearchType": "ActiveDirectory",
        "searchBindDN": "SFReadOnly@prodtest.solidfire.net",
        "serverURIs": [
           "ldaps://111.22.333.444",
           "ldap://555.66.777.888"
            ],
        "userDNTemplate": "",
        "userSearchBaseDN": "dc=prodtest,dc=solidfire,dc=net",
        "userSearchFilter":
"(&(objectClass=person)(sAMAccountName=%USERNAME%))"
     }
   }
}
```

Novità dalla versione

9.6

TestLdapAuthentication

È possibile utilizzare `TestLdapAuthentication` Metodo per convalidare le impostazioni di autenticazione LDAP attualmente attivate. Se la configurazione è corretta, la chiamata API restituisce l'appartenenza di gruppo dell'utente testato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome utente	Il nome utente da verificare.	stringa	Nessuno	Sì
password	La password per il nome utente da verificare.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
LdapConfiguration	Oggetto ldapConfiguration da testare. Se si fornisce questo parametro, il sistema verifica la configurazione fornita anche se l'autenticazione LDAP è attualmente disattivata.	LdapConfiguration	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
gruppi	Elenco dei gruppi LDAP che includono l'utente testato come membro.	array
Nome utente	Nome distinto LDAP completo dell'utente testato.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "TestLdapAuthentication",
"params": {"username":"admin1",
           "password":"admin1PASS"
      },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id": 1,
 "result": {
    "groups": [
        "CN=StorageMgmt,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
      ],
        "userDN": "CN=Admin1
Jones,OU=PTUsers,DC=prodtest,DC=solidfire,DC=net"
  }
}
```

Novità dalla versione

9.6

Metodi API di autenticazione a più fattori

È possibile utilizzare l'autenticazione a più fattori (MFA) per gestire le sessioni utente utilizzando un provider di identità (IdP) di terze parti tramite il linguaggio SAML (Security Assertion Markup Language).

- AddIdpClusterAdmin
- CreateIdpConfiguration
- DeleteAuthSession
- DeleteAuthSessionsByClusterAdmin
- DeleteAuthSessionsByNomeUtente
- DeleteIdpConfiguration (Configurazione DeleteIdp)
- DisableIdpAuthentication
- EnableIdpAuthentication
- GetIdpAuthenticationState
- ListActiveAuthSessions
- ListIdpconfigurazioni
- UpdateIdpConfiguration

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddIdpClusterAdmin

È possibile utilizzare `AddIpdClusterAdmin` Metodo per aggiungere un utente amministratore del cluster autenticato da un provider di identità (IdP) di terze parti. Gli

account di amministrazione del cluster IDP sono configurati in base alle informazioni sul valore dell'attributo SAML fornite nell'asserzione SAML di IdP associata all'utente. Se un utente esegue correttamente l'autenticazione con IdP e dispone di istruzioni degli attributi SAML all'interno dell'asserzione SAML corrispondenti a più account di amministrazione del cluster IdP, l'utente disporrà del livello di accesso combinato di quelli corrispondenti agli account di amministrazione del cluster IdP.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Controlla i metodi che l'amministratore del cluster IdP può utilizzare.	array di stringhe	Nessuno	Sì
AccetteEula	Accettare il Contratto di licenza con l'utente finale. Impostare su true per aggiungere un account amministratore del cluster al sistema. Se omesso o impostato su false, la chiamata al metodo non riesce.	booleano	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome utente	Mapping attributo-valore SAML a un amministratore del cluster IdP (ad esempio, email=test@example.com). Questo può essere definito utilizzando un soggetto SAML specifico utilizzando `NameID` O come voce nell'istruzione SAML Attribute, ad esempio `eduPersonAffiliation`.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ID clusterAdminID	Identificatore univoco del nuovo amministratore del cluster creato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "AddIdpClusterAdmin",
    "params": {
        "username": "email=test@example.com",
        "acceptEula": true,
        "access": ["administrator"]
    }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "result": {
        "clusterAdminID": 13
    }
}
```

Novità dalla versione

12.0

CreateIdpConfiguration

È possibile utilizzare `CreateIpdConfiguration` Metodo per creare una potenziale relazione di trust per l'autenticazione utilizzando un provider di identità (IdP) di terze parti per il cluster. Per le comunicazioni IdP è richiesto un certificato SAML Service Provider. Questo certificato viene generato come richiesto e restituito da questa chiamata API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
IdpMetadata	Metadati IDP da memorizzare.	stringa	Nessuno	Sì
Nome ID	Nome utilizzato per identificare un provider IdP per SAML 2.0 Single Sign-on.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
IdpConfigInfo	Informazioni sulla configurazione del provider di identità (IdP) di terze parti.	"IdpConfigInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "CreateIdpConfiguration",
    "params": {
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>
             <EntityDescriptor
               xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"
               xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"
               xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"
               xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"
               ...</Organization>
             </EntityDescriptor>",
        "idpName": "https://provider.name.url.com"
    },
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": false,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ... </Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MIID...SlBHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```

Novità dalla versione

12.0

DeleteAuthSession

È possibile utilizzare `DeleteAuthSession` metodo per eliminare una singola sessione di autenticazione dell'utente. Se l'utente chiamante non si trova in ClusterAdmins / Administrator AccessGroup, è possibile eliminare solo la sessione di autenticazione dell'utente chiamante.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID SessionID	Identificatore univoco della sessione auth da eliminare.	UUID	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessione	Informazioni sulla sessione per la sessione Delete auth.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "DeleteAuthSession",
    "params": {
        "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "session": {
            "accessGroupList": [
                "administrator"
            ],
            "authMethod": "Cluster",
            "clusterAdminIDs": [
                1
            ],
            "finalTimeout": "2020-04-09T17:51:30Z",
            "idpConfigVersion": 0,
            "lastAccessTimeout": "2020-04-06T18:21:33Z",
            "sessionCreationTime": "2020-04-06T17:51:30Z",
            "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713",
            "username": "admin"
        }
    }
}
```


Novità dalla versione

12.0

DeleteAuthSessionsByClusterAdmin

È possibile utilizzare `DeleteAuthSessionsByClusterAdmin` metodo per eliminare tutte le sessioni di autenticazione associate al specificato `ClusterAdminID`. Se ClusterAdminID specificato viene mappato a un gruppo di utenti, tutte le sessioni di autenticazione per tutti i membri del gruppo verranno eliminate. Per visualizzare un elenco di sessioni per la possibile eliminazione, utilizzare il metodo ListAuthSessionsByClusterAdmin con `ClusterAdminID` parametro.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID clusterAdminID	Identificatore univoco dell'amministratore del cluster.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione eliminate.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

Novità dalla versione

12.0

DeleteAuthSessionsByNomeUtente

È possibile utilizzare `DeleteAuthSessionsByUsername` metodo per eliminare tutte le sessioni di autenticazione per un dato utente. Un chiamante che non si trova in AccessGroup ClusterAdmins/Administrator può eliminare solo le proprie sessioni. Un chiamante con privilegi ClusterAdmins/Administrator può eliminare le sessioni appartenenti a qualsiasi utente. Per visualizzare l'elenco delle sessioni che è possibile eliminare, utilizzare `ListAuthSessionsByUsername` con gli stessi parametri. Per visualizzare un elenco di sessioni per la possibile eliminazione, utilizzare `ListAuthSessionsByUsername` metodo con lo stesso parametro.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AuthMethod	Metodo di autenticazione delle sessioni utente da eliminare. Solo un chiamante in ClusterAdmins/Administrator AccessGroup può fornire questo parametro. I valori possibili sono: • **AuthMethod=Cluster** specifica il nome utente di ClusterAdmin. • **AuthMethod=LDAP** specifica il DN LDAP dell'utente. • **AuthMethod=IDP** specifica l'ID utente IdP UUID o NameID. Se IdP non è configurato per restituire nessuna opzione, viene specificato un UUID casuale emesso al momento della creazione della sessione.	AuthMethod	Nessuno	No
nome utente	Identificatore univoco dell'utente.	stringa	Nessuno	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione eliminate.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

Novità dalla versione

12.0

DeleteIdpConfiguration (Configurazione DeleteIdp)

È possibile utilizzare `DeleteIdpConfiguration` Metodo per eliminare una configurazione esistente di un IdP di terze parti per il cluster. L'eliminazione dell'ultima configurazione IdP rimuove il certificato del provider di servizi SAML dal cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID configurazione idpID	UUID per la configurazione IdP di terze parti.	UUID	Nessuno	No
Nome ID	Nome utilizzato per identificare e recuperare un provider IdP per SAML 2.0 Single Sign-on.	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "result":{}
}
```

Novità dalla versione

12.0

DisableIdpAuthentication

È possibile utilizzare `DisableIdpAuthentication` Metodo per disattivare il supporto per l'autenticazione utilizzando IDP di terze parti per il cluster. Una volta disattivata, gli utenti autenticati da IDP di terze parti non possono più accedere al cluster e le sessioni autenticate attive vengono invalidate/disconnesse. LDAP e gli amministratori del cluster possono accedere al cluster tramite interfacce utente supportate.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"result": {}
}
```

Novità dalla versione

12.0

EnableIdpAuthentication

È possibile utilizzare `EnableIdpAuthentication` Metodo per abilitare il supporto per l'autenticazione utilizzando IDP di terze parti per il cluster. Una volta attivata l'autenticazione IdP, gli amministratori LDAP e del cluster non possono più accedere al cluster tramite interfacce utente supportate e le sessioni autenticate attive vengono invalidate/disconnesse. Solo gli utenti autenticati da IDP di terze parti possono accedere al cluster tramite le interfacce utente supportate.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID configurazione idpID	UUID per la configurazione IdP di terze parti. Se esiste una sola configurazione IdP, l'impostazione predefinita è quella di attivare tale configurazione. Se si dispone di una sola IdpConfiguration, non è necessario fornire il parametro idpConfigurationID.	UUID	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"result": {}
}
```

Novità dalla versione

12.0

GetIdpAuthenticationState

È possibile utilizzare `GetIdpAuthenticationState` Metodo per la restituzione di informazioni relative allo stato di autenticazione mediante IDP di terze parti.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
attivato	Indica se l'autenticazione IdP di terze parti è attivata.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "result": {"enabled": true}
}
```

Novità dalla versione

12.0

ListActiveAuthSessions

È possibile utilizzare `ListActiveAuthSessions` metodo per elencare tutte le sessioni autenticate attive. Solo gli utenti con diritti di accesso amministrativo possono chiamare questo metodo.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListActiveAuthSessions"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

Novità dalla versione

12.0

ListIdpconfigurazioni

È possibile utilizzare `ListIdpConfigurations` Metodo per elencare le configurazioni per gli IDP di terze parti. In alternativa, è possibile fornire il `enabledOnly` Flag per recuperare la configurazione IdP attualmente attivata o un UID metadati IdP o un nome IdP per eseguire query sulle informazioni di una configurazione IdP specifica.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AbilitataOnly	Filtra il risultato per restituire la configurazione IdP attualmente attivata.	booleano	Nessuno	No
ID configurazione idpID	UUID per la configurazione IdP di terze parti.	UUID	Nessuno	No
Nome ID	Recupera le informazioni di configurazione IdP per un nome IdP specifico.	stringa	Nessuno	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
IdpConfigInfos	Informazioni sulle configurazioni IdP di terze parti.	"IdpConfigInfo" array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```

Novità dalla versione

12.0

UpdateIdpConfiguration

È possibile utilizzare `UpdateIdpConfiguration` Metodo per aggiornare una configurazione esistente con un IdP di terze parti per il cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
GenerateNewCertificate	Quando viene specificato true, viene generata una nuova chiave SAML e un nuovo certificato che sostituisce la coppia esistente. Nota: La sostituzione del certificato esistente interrompe l'attendibilità stabilita tra il cluster e l'IdP fino a quando i metadati del service provider del cluster non vengono ricaricati nell'IdP. Se non viene fornito o impostato su false, il certificato SAML e la chiave rimangono invariati.	booleano	Nessuno	No
ID configurazione idpID	UUID per la configurazione IdP di terze parti.	UUID	Nessuno	No
IdpMetadata	Metadati IDP per dettagli di configurazione e integrazione per SAML 2.0 Single Sign-on.	stringa	Nessuno	No
Nome ID	Nome utilizzato per identificare e recuperare un provider IdP per SAML 2.0 Single Sign-on.	stringa	Nessuno	No
NewIdpName	Se specificato, questo nome sostituisce il vecchio nome IdP.	stringa	Nessuno	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
IdpConfigInfo	Informazioni sulla configurazione IdP di terze parti.	"IdpConfigInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "UpdateIdpConfiguration",
"params": {
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "generateNewCertificate": true
    }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "result": {
        "idpConfigInfo": {
        "enabled": true,
        "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
        "idpMetadata": "<?xml version=\"1.0\" encoding=\"UTF-8\"?>\r\n
        <EntityDescriptor
xmlns=\"urn:oasis:names:tc:SAML:2.0:metadata\"\r\n
        xmlns:ds=\"http://www.w3.org/2000/09/xmldsig#\"\r\n
        xmlns:shibmd=\"urn:mace:shibboleth:metadata:1.0\"\r\n
        xmlns:xml=\"http://www.w3.org/XML/1998/namespace\"\r\n
        ...</Organization>\r\n
        </EntityDescriptor>",
        "idpName": "https://privider.name.url.com",
        "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
        MI...BHi\n
        -----END CERTIFICATE-----\n",
        "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
        }
    }
}
```


Novità dalla versione

12.0

Metodi API per l'autenticazione della sessione

È possibile utilizzare l'autenticazione basata su sessione per gestire le sessioni utente.

- ListAuthSessionsByClusterAdmin
- ListAuthSessionsByNomeUtente

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

ListAuthSessionsByClusterAdmin

È possibile utilizzare `ListAuthSessionsByClusterAdmin` metodo per elencare tutte le sessioni di autenticazione associate a quelle specificate `ClusterAdminID`. Se specificato `ClusterAdminID` viene mappato a un gruppo di utenti, verranno elencate tutte le sessioni di autenticazione per tutti i membri di quel gruppo.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID clusterAdminID	Identificatore univoco dell'amministratore del cluster.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Elenco delle informazioni sulla sessione per le sessioni auth.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "ListAuthSessionsByClusterAdmin",
    "clusterAdminID": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```


Novità dalla versione

12.0

ListAuthSessionsByNomeUtente

È possibile utilizzare `ListAuthSessionsByUsername` metodo per elencare tutte le sessioni auth per l'utente specificato. Un chiamante non in AccessGroup ClusterAdmins / privilegi di amministratore può elencare solo le proprie sessioni. Un chiamante con privilegi ClusterAdmins/Administrator può elencare le sessioni appartenenti a qualsiasi utente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AuthMethod	Metodo di autenticazione delle sessioni utente da elencare. Solo un chiamante in ClusterAdmins/Administrator AccessGroup può fornire questo parametro. I valori possibili sono: • **AuthMethod=Cluster** specifica il nome utente di ClusterAdmin. • **AuthMethod=LDAP** specifica il DN LDAP dell'utente. • **AuthMethod=IDP** specifica l'ID utente IdP UUID o NameID. Se IdP non è configurato per restituire nessuna opzione, viene specificato un UUID casuale emesso al momento della creazione della sessione.	AuthMethod	Nessuno	Sì
nome utente	Identificatore univoco dell'utente.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sessioni	Elenco delle informazioni sulla sessione per le sessioni auth.	"AuthSessionInfo"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "ListAuthSessionsByUsername",
    "authMethod": "Cluster",
    "username": "admin"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"sessions": [
      {
        "accessGroupList": [
          "administrator"
        ],
        "authMethod": "Cluster",
        "clusterAdminIDs": [
          1
        ],
        "finalTimeout": "2020-03-14T19:21:24Z",
        "idpConfigVersion": 0,
        "lastAccessTimeout": "2020-03-11T19:51:24Z",
        "sessionCreationTime": "2020-03-11T19:21:24Z",
        "sessionID": "b12bfc64-f233-44df-8b9f-6fb6c011abf7",
        "username": "admin"
      }
    ]
}
```

Novità dalla versione

12.0

Metodi API del nodo

È possibile utilizzare i metodi API dei nodi per configurare i singoli nodi. Questi metodi operano su nodi singoli che devono essere configurati, configurati ma non ancora partecipanti a un cluster o che partecipano attivamente a un cluster. I metodi Node API consentono di visualizzare e modificare le impostazioni per i singoli nodi e la rete del cluster utilizzata per comunicare con il nodo. È necessario eseguire questi metodi su

singoli nodi; non è possibile eseguire metodi API per nodo rispetto all'indirizzo del cluster.

- CheckPingOnVlan
- CheckProposedNodeAdditions
- CreateClusterSupportBundle
- CreateSupportBundle
- DeleteAllSupportBundles
- DisableMaintenanceMode
- DisableSsh
- EnableMaintenanceMode
- EnableSsh
- GetClusterConfig
- GetClusterState
- GetConfig
- GetDriveConfig
- GetHardwareConfig
- GetHardwareInfo
- GetIpmiConfig
- GetIpmiInfo
- GetNetworkConfig
- Interfaccia GetNetworkInterface
- GetNodeActiveTlsCiphers
- GetNodeFipsDrivesReport
- GetNodeSSLCertificate
- GetNodeSupportedTlsCiphers
- GetPendingOperation
- GetSshInfo
- ListDrivehardware
- ListNetworkInterfaces
- ListTest
- ListUtilities
- RemoveNodeSSLCertificate
- ResetDrive
- ResetNode
- ResetNodeSupplementalTlsCiphers
- Restart Networking (Ripristino rete)
- RestartServices
- SetClusterConfig

- SetConfig
- SetNetworkConfig
- SetNodeSSLCertificate
- SetNodeSupplementalTlsCiphers
- Spegnere
- TestConnectEnsemble
- TestConnectMvip
- TestConnectSvip
- TestDrive
- TestHardwareConfig
- TestLocateCluster
- TestLocalConnectivity
- TestNetworkConfig
- Test Ping
- TestRemoteConnectivity

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CheckPingOnVlan

È possibile utilizzare `CheckPingOnVlan` Metodo per testare la connettività di rete su una VLAN temporanea durante l'esecuzione della convalida di rete pre-implementazione. `CheckPingOnVlan` Crea un'interfaccia VLAN temporanea, invia pacchetti ICMP a tutti i nodi del cluster di storage utilizzando l'interfaccia VLAN, quindi rimuove l'interfaccia.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
tentativi	Specifica il numero di volte in cui il sistema deve ripetere il test ping.	intero	5	No
host	Specifica un elenco separato da virgole di indirizzi o nomi host delle periferiche da ping.	stringa	I nodi nel cluster	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
interfaccia	L'interfaccia (base) esistente da cui devono essere inviati i ping. Valori possibili: • Bond10G: Invio di ping dall'interfaccia Bond10G. • Bond1G: Invio di ping dall'interfaccia Bond1G.	stringa	Nessuno	Sì
Dimensione pacchetto	Specifica il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore al valore MTU massimo specificato nella configurazione di rete.	intero	Nessuno	No
PingTimeoutMsec	Specifica il numero di millisecondi da attendere per ogni singola risposta ping.	intero	500 ms.	No
ProibitFragmentation	Attiva il flag DF (Do Not Fragment) per i pacchetti ICMP.	booleano	falso	No
SourceIndirizzoV4	L'indirizzo IPv4 di origine da utilizzare nei pacchetti ping ICMP.	stringa	Nessuno	Sì
SourceIndirizzoV6	L'indirizzo IPv6 di origine da utilizzare nei pacchetti ping ICMP.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
TotalTimeoutSec	Specifica il tempo in secondi in cui il ping deve attendere una risposta di sistema prima di eseguire il successivo tentativo di ping o terminare il processo.	intero	5	No
VirtualNetworkTag	L'ID VLAN da utilizzare per l'invio dei pacchetti ping.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
dettagli	Elenco di ciascun IP con cui il nodo è stato in grado di comunicare e statistiche di risposta ping.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "CheckPingOnVlan",
    "params": {
        "interface": "Bond10G",
        "virtualNetworkTag": 4001,
        "sourceAddressV4": "192.168.41.4",
        "hosts": "192.168.41.2"
},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "details": {
      "192.168.41.2": {
        "individualResponseCodes": [
          "Success",
          "Success",
          "Success",
          "Success",
          "Success"
        ],
        "individualResponseTimes": [
          "00:00:00.000373",
          "00:00:00.000098",
          "00:00:00.000097",
          "00:00:00.000074",
          "00:00:00.000075"
        ],
        "individualStatus": [
          true,
          true,
          true,
          true,
          true
        ],
        "interface": "Bond10G",
        "responseTime": "00:00:00.000143",
        "sourceAddressV4": "192.168.41.4",
        "successful": true,
        "virtualNetworkTag": 4001
      }
    },
    "duration": "00:00:00.244379",
    "result": "Passed"
  }
}
```


Novità dalla versione

11.1

CheckProposedNodeAdditions

È possibile utilizzare `CheckProposedNodeAdditions` metodo per testare un insieme

di nodi di storage per verificare se è possibile aggiungerli a un cluster di storage senza errori o violazioni delle best practice.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nodi	Un elenco degli indirizzi IP dello storage dei nodi di storage pronti per essere aggiunti a un cluster di storage.	array di stringhe	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ProposedClusterValid	Indica se i nodi di storage proposti costituirebbero o meno un cluster di storage valido. Valori possibili: • vero • falso	booleano

ProposedClusterErrors	Errori che si verificano se un cluster di storage è stato creato utilizzando i nodi di storage proposti. Codici di errore possibili: • `nodesNoCapacity`: I nodi non avevano alcuna capacità utilizzabile. • `nodesTooLarge`: I nodi costituiscono una parte troppo grande della capacità del cluster per lo schema di protezione attivo. • `nodesConnectFailed`: Impossibile connettersi ai nodi per eseguire query sulla configurazione hardware. • `nodesQueryFailed`: Impossibile eseguire query sui nodi per la configurazione hardware. • `nodesClusterMember`: Gli indirizzi IP dei nodi sono già in uso nel cluster. • `nonFipsNodeCapable`: Impossibile aggiungere un nodo non compatibile con FIPS al cluster di storage mentre la funzione di crittografia del disco FIPS 140-2 è attivata. • `nonFipsDrivesCapable`: Impossibile aggiungere un nodo con dischi non compatibili con FIPS al cluster mentre la funzione di crittografia del disco FIPS 140-2 è attivata.	array di stringhe

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "CheckProposedNodeAdditions",
    "params": {
    "nodes": [
        "192.168.1.11",
        "192.168.1.12",
        "192.168.1.13",
        "192.168.1.14"
    ]
},
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "proposedClusterValid": true,
        "proposedClusterErrors": [ ]
    }
}
```

Novità dalla versione

11.0

CreateClusterSupportBundle

È possibile utilizzare `CreateClusterSupportBundle` sul nodo di gestione per raccogliere bundle di supporto da tutti i nodi di un cluster. I bundle di supporto dei singoli nodi sono compressi in tar.gz file. Il bundle di supporto del cluster è un file tar contenente i bundle di supporto dei nodi. Questo metodo può essere eseguito solo su un nodo di gestione, ma non su un nodo di storage.

Parametri

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AllowIncomplete (non completo)	Consente di continuare l'esecuzione dello script se non è possibile raccogliere bundle da uno o più nodi.	booleano	Nessuno	No
Nome bundle	Nome univoco per ciascun bundle di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo	stringa	Nessuno	No
mvip	MVIP del cluster. I bundle vengono raccolti da tutti i nodi del cluster. Questo parametro è obbligatorio se il parametro Nodes non è specificato.	stringa	Nessuno	Sì
nodi	Gli indirizzi IP dei nodi da cui raccogliere i bundle. Utilizzare nodi o mvip, ma non entrambi, per specificare i nodi da cui raccogliere i bundle. Questo parametro è obbligatorio se mvip non è specificato.	array di stringhe	Nessuno	Sì
password	La password di amministrazione del cluster. **Nota:** questa password viene visualizzata come testo una volta immessa.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome utente	Il nome utente dell'amministratore del cluster.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "CreateClusterSupportBundle",
"params": {
          "bundlename": "clusterbundle",
          "mvip": "132.119.120.100"
     }
   },
 "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id":1,
  "result":{
   "details":{
      "bundleName":"clusterbundle",
      "extraArgs":"",
      "files":[
          "/tmp/supportbundles/clusterbundle.cl-4SD5.tar"
      ],
      "output":"timeout -s KILL 1790s
/usr/local/bin/sfclustersupportbundle --quiet --name=\"clusterbundle\"
--target-directory=\"/tmp/solidfire-dtemp.MM7f0m\" --user=\"admin\"
--pass=\"admin\" --mvip=132.119.120.100"
       },
       "duration":"00:00:24.938127",
       "result":"Passed"
    }
}
```

Novità dalla versione

9.6

CreateSupportBundle

È possibile utilizzare `CreateSupportBundle` per creare un file bundle di supporto nella directory del nodo. Dopo la creazione, il bundle viene memorizzato nel nodo come file tar (l'opzione di compressione gz è disponibile tramite il parametro extraArgs).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Nome bundle	Nome univoco del bundle di supporto. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ExtraArgs	Utilizzare '--compress gz' per creare il bundle di supporto come file tar.gz.	stringa	Nessuno	No
Timeout Sec	Il numero di secondi in cui viene eseguito lo script del bundle di supporto.	intero	1500	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
dettagli	I dettagli del bundle di supporto. Valori possibili: • BundleName: Il nome specificato nel metodo CreateSupportBundleAPI. Se non è stato specificato alcun nome, viene utilizzato "supportbundle". • ExtraArgs: Gli argomenti passati con questo metodo. • File: Un elenco dei file bundle di supporto creati dal sistema. • Output: Output della riga di comando dallo script che ha creato il bundle di supporto. • TimeoutSec: Il numero di secondi in cui lo script del bundle di supporto viene eseguito prima dell'arresto. • url: URL del bundle di supporto creato.	Oggetto JSON
durata	Il tempo utilizzato per creare il bundle di supporto nel formato: HH:MM:SS.sssss.	stringa
risultato	Il successo o il fallimento dell'operazione del bundle di supporto.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
 "method": "CreateSupportBundle",
"params": {
  "extraArgs": "--compress gz"
 },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
"result": {
  "details": {
    "bundleName": "supportbundle",
    "extraArgs": "--compress gz",
    "files": [
         "supportbundle.nodehostname.tar.gz"
     ],
     "output": "timeout -s KILL 1500s /sf/scripts/sfsupportbundle --quiet
--compress gz /tmp/solidfire-dtemp.1L6bdX/supportbundle<br><br>Moved
'/tmp/solidfire-dtemp.1L6bdX/supportbundle.nodehostname.tar.gz' to
/tmp/supportbundles",
      "timeoutSec": 1500,
      "url": [

"https://nodeIP:442/config/supportbundles/supportbundle.nodehostname.tar.g
z"
      ]
    },
    "duration": "00:00:43.101627",
    "result": "Passed"
  }
}
```

Novità dalla versione

9.6

DeleteAllSupportBundles

È possibile utilizzare `DeleteAllSupportBundles` metodo per eliminare tutti i bundle di supporto generati con `CreateSupportBundle` Metodo API.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteAllSupportBundles",
   "params": {}
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
 }
}
```

Novità dalla versione

9.6

DisableMaintenanceMode

È possibile utilizzare `DisableMaintenanceMode` metodo per portare un nodo di storage fuori dalla modalità di manutenzione. La modalità di manutenzione deve essere disattivata solo dopo aver completato la manutenzione e dopo che il nodo è in linea.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nodi	Elenco degli ID dei nodi di storage da rimuovere dalla modalità di manutenzione.	array intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	È possibile utilizzare il metodo GetAsyncResult per recuperare questo asyncHandle e determinare quando la transizione della modalità di manutenzione è completa.	intero
CurrentMode	Lo stato corrente della modalità di manutenzione del nodo. Valori possibili: • Disabled (Disattivato): Non è stata richiesta alcuna manutenzione. • FailedToRecover: Impossibile ripristinare il nodo dalla modalità di manutenzione. • Inaspettato: Il nodo è stato rilevato non in linea, ma in modalità Disabled (Disattivato). • RecoveringFromMaintenance: Il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: Sono in corso azioni per preparare un nodo a eseguire la manutenzione. • ReadyForMaintenance: Il nodo è pronto per la manutenzione.	MaintenanceMode (stringa)

RequestedMode	Lo stato della modalità di manutenzione richiesta del nodo. Valori possibili: • Disabled (Disattivato): Non è stata richiesta alcuna manutenzione. • FailedToRecover: Impossibile ripristinare il nodo dalla modalità di manutenzione. • Inaspettato: Il nodo è stato rilevato non in linea, ma in modalità Disabled (Disattivato). • RecoveringFromMaintenance: Il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: Sono in corso azioni per preparare un nodo a eseguire la manutenzione. • ReadyForMaintenance: Il nodo è pronto per la manutenzione.	MaintenanceMode (stringa)

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableMaintenanceMode",
  "params": {
    "nodes": [6]
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "Disabled",
        "asyncHandle": 1,
        "currentMode": "Enabled"
     }
}
```

Novità dalla versione

12.2

Trova ulteriori informazioni

"Concetti relativi alla modalità di manutenzione dello storage NetApp HCI"

DisableSsh

È possibile utilizzare `DisableSsh` Metodo per disattivare il servizio SSH per un singolo nodo di storage. Questo metodo non influisce sulla durata del timeout del servizio SSH a livello di cluster.

Parametro

Questo metodo non ha alcun parametro di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
attivato	Lo stato del servizio SSH per questo nodo.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableSsh",
  "params": {
      },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {"enabled": false}
}
```

EnableMaintenanceMode

È possibile utilizzare `EnableMaintenanceMode` metodo per preparare un nodo di storage per la manutenzione. Gli scenari di manutenzione includono qualsiasi attività che richiede lo spegnimento o il riavvio del nodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ForceWithUnresolvedFaults	Forzare l'attivazione della modalità di manutenzione per questo nodo anche in presenza di guasti del cluster di blocco.	booleano	Falso	No
nodi	L'elenco degli ID del nodo da mettere in modalità di manutenzione. È supportato un solo nodo alla volta.	array intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
PerMinutePrimarySwapLimit	Il numero di strati primari da scambiare al minuto. Se non specificato, tutti gli strati primari verranno scambiati contemporaneamente.	intero	Nessuno	No
timeout	Specifica per quanto tempo la modalità di manutenzione deve rimanere attivata prima che venga disattivata automaticamente. Formattato come stringa di tempo (ad esempio, HH:mm:ss). Se non specificato, la modalità di manutenzione rimane attivata fino a quando non viene disattivata esplicitamente.	stringa	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	È possibile utilizzare il metodo GetAsyncResult per recuperare questo asyncHandle e determinare quando la transizione della modalità di manutenzione è completa.	intero

CurrentMode	Lo stato corrente della modalità di manutenzione del nodo. Valori possibili: • Disabled (Disattivato): Non è stata richiesta alcuna manutenzione. • FailedToRecover: Impossibile ripristinare il nodo dalla modalità di manutenzione. • RecoveringFromMaintenance: Il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: Sono in corso azioni per preparare un nodo a eseguire la manutenzione. • ReadyForMaintenance: Il nodo è pronto per la manutenzione.	MaintenanceMode (stringa)
RequestedMode	Lo stato della modalità di manutenzione richiesta del nodo. Valori possibili: • Disabled (Disattivato): Non è stata richiesta alcuna manutenzione. • FailedToRecover: Impossibile ripristinare il nodo dalla modalità di manutenzione. • RecoveringFromMaintenance: Il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: Sono in corso azioni per preparare un nodo a eseguire la manutenzione. • ReadyForMaintenance: Il nodo è pronto per la manutenzione.	MaintenanceMode (stringa)

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableMaintenanceMode",
  "params": {
    "forceWithUnresolvedFaults": False,
    "nodes": [6],
    "perMinutePrimarySwapLimit" : 40,
    "timeout" : "01:00:05"
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "requestedMode": "ReadyForMaintenance",
        "asyncHandle": 1,
        "currentMode": "Disabled"
     }
}
```

Novità dalla versione

12.2

Trova ulteriori informazioni

"Concetti relativi alla modalità di manutenzione dello storage NetApp HCI"

EnableSsh

È possibile utilizzare `EnableSsh` Metodo per attivare il servizio Secure Shell (SSH) per un singolo nodo. Questo metodo non influisce sulla durata del timeout SSH a livello di cluster e non esenta il nodo dalla disattivazione di SSH da parte del timeout SSH globale.

Parametro

Questo metodo non ha alcun parametro di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
attivato	Lo stato del servizio SSH per questo nodo.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableSsh",
  "params": {
     },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {"enabled": true}
}
```

GetClusterConfig

È possibile utilizzare `GetClusterConfig` Metodo API per restituire informazioni sulla configurazione del cluster utilizzata dal nodo per comunicare con il cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
cluster	Informazioni di configurazione del cluster utilizzate dal nodo per comunicare con il cluster.	cluster

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "cluster": {
      "cipi": "Bond10G",
      "cluster": "ClusterName",
      "ensemble": [
        "1:10.30.65.139",
        "2:10.30.65.140",
        "3:10.30.65.141"
      ],
      "fipsDriveConfiguration": true,
      "mipi": "Bond1G",
      "name": "xxx-en142",
      "nodeID": 4,
      "pendingNodeID": 0,
      "role": "Storage",
      "sipi": "Bond10G",
      "state": "Active",
      "version": "9.1.0"
    }
  }
}
```

Novità dalla versione

9.6

GetClusterState

È possibile utilizzare `GetClusterState` Metodo API per indicare se un nodo fa parte o meno di un cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
cluster	Nome del cluster.	stringa
stato	• Disponibile: Il nodo non è stato configurato con un nome di cluster. • In sospeso: Il nodo è in sospeso per uno specifico cluster denominato e può essere aggiunto. • Attivo: Il nodo è un membro attivo di un cluster e non può essere aggiunto a un altro cluster.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetClusterState",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" :
      "cluster" :  "Cluster101"
      "state" : "Active"
}
```

Novità dalla versione

9.6

GetConfig

È possibile utilizzare `GetConfig` Metodo API per ottenere tutte le informazioni di configurazione per un nodo. Questo metodo API include le stesse informazioni disponibili in entrambi `GetClusterConfig` e. `GetNetworkConfig` Metodi API.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
config	I dettagli di configurazione del cluster. Questo oggetto contiene: • cluster: Informazioni sul cluster che identificano il modo in cui il nodo di storage comunica con il cluster di storage a cui è associato. • rete (tutte le interfacce): Tipi di connessione di rete e impostazioni correnti per ciascuna interfaccia di rete del nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetClusterConfig
- GetNetworkConfig
- GetConfig

GetDriveConfig

È possibile utilizzare `GetDriveConfig` metodo per ottenere informazioni sull'unità per i conteggi previsti di unità a blocchi e a sezioni, nonché il numero di unità a blocchi e a sezioni attualmente connesse al nodo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
DriveConfig	Informazioni sui dischi collegati al nodo.	disco

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetDriveConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Le risposte per questo metodo sono simili all'esempio seguente. A causa della lunghezza, la risposta contiene informazioni per un disco di un solo nodo di storage.

```
{
    "id": 1,
    "result": {
            "driveConfig": {
                    "drives": [
                        {
                            "canonicalName": "sda",
                            "connected": true,
                            "dev": 2052,
                            "devPath": "/dev/sdimm0p4",
                            "driveType": "Slice",
                            "name": "scsi-SATA_VRFSD3400GNCVMT205581853-
part4",
                            "path": "/dev/sda4",
                            "pathLink": "/dev/sdimm0p4",
                            "product": "VRFSD3400GNCVMTKS1",
                            "scsiCompatId": "scsi-
SATA_VRFSD3400GNCVMT205581853-part4",
                            "scsiState": "Running",
                            "securityAtMaximum": false,
                            "securityEnabled": false,
                            "securityFrozen": true,
                            "securityLocked": false,
                            "securitySupported": true,
                            "serial": "205581853",
                            "size": 299988156416,
                            "slot": -1,
                            "uuid": "9d4b198b-5ff9-4f7c-04fc-
3bc4e2f38974",
                            "vendor": "Viking",
                            "version": "612ABBF0"
                        }
                    ],
                    "numBlockActual": 10,
                    "numBlockExpected": 10,
                    "numSliceActual": 1,
                    "numSliceExpected": 1,
                    "numTotalActual": 11,
                    "numTotalExpected": 11
            }
    }
}
```

GetHardwareConfig

È possibile utilizzare `GetHardwareConfig` metodo per ottenere le informazioni di configurazione hardware per un nodo. Questi dati di configurazione sono destinati all'uso interno. Per ottenere un inventario dei componenti hardware del sistema più utile, utilizzare `GetHardwareInfo` metodo invece.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
HardwareConfig	Elenco delle informazioni hardware e delle impostazioni correnti.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetHardwareConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Le risposte per questo metodo sono simili all'esempio seguente.

```
{
    "id": 1,
    "result": {
        "hardwareConfig": {
            "biosRevision": "1.0",
            "biosVendor": [
                "NetApp",
                "SolidFire"
            ],
            "biosVersion": "1.1.2",
            "blockDriveSizeBytes": 300069052416,
            "blockDrives": [
                "/dev/slot0",
```

```
            "/dev/slot1",
            "/dev/slot2",
            "/dev/slot3",
            "/dev/slot4",
            "/dev/slot5",
            "/dev/slot6",
            "/dev/slot7",
            "/dev/slot8",
            "/dev/slot9"
        ],
        "blockServiceFormat": "Standard",
        "bmcFirmwareRevision": "1.6",
        "bmcIpmiVersion": "2.0",
        "chassisType": "R620",
        "cpuCores": 6,
        "cpuCoresEnabled": 6,
        "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
        "cpuThreads": 12,
        "driveSizeBytesInternal": 400088457216,
        "fibreChannelFirmwareRevision": "",
        "fibreChannelModel": "",
        "fibreChannelPorts": {},
        "idracVersion": "1.06.06",
        "ignoreFirmware": [],
        "memoryGB": 72,
        "memoryMhz": 1333,
        "networkDriver": [
            "bnx2x"
        ],
        "nicPortMap": {
            "PortA": "eth2",
            "PortB": "eth3",
            "PortC": "eth0",
            "PortD": "eth1"
        },
        "nodeType": "SF3010",
        "numCpu": 2,
        "numDrives": 10,
        "numDrivesInternal": 1,
        "nvramTempMonitorEnable": false,
        "rootDrive": "/dev/sdimm0",
        "scsiBusExternalDriver": "mpt3sas",
        "scsiBusInternalDriver": "ahci",
        "sliceDriveSizeBytes": 299988156416,
        "sliceDrives": [
            "/dev/sdimm0p4"
```

```
            ],
            "slotOffset": 0,
            "solidfireDefaults": {
                "bufferCacheGB": 12,
                "configuredIops": 50000,
                "cpuDmaLatency": -1,
                "driveWriteThroughputMBPerSleep": 10,
                "maxDriveWriteThroughputMBPerSec": 175,
                "maxIncomingSliceSyncs": 10,
                "postCallbackThreadCount": 8,
                "sCacheFileCapacity": 100000000,
                "sliceFileLogFileCapacity": 5000000000
            }
        }
    }
}
```


Novità dalla versione

9.6

GetHardwareInfo

È possibile utilizzare `GetHardwareInfo` metodo per ottenere informazioni hardware e stato per un singolo nodo. Le informazioni sull'hardware generalmente includono produttori, vendor, versioni, dischi e altre informazioni di identificazione associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare questo parametro "force" su true per l'esecuzione su tutti i nodi del cluster.	booleano	falso	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
HardwareInfo	Informazioni hardware per il nodo.	HardwareInfo

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetHardwareInfo",
   "params": {
   },
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "hardwareInfo": {
      "bus": {
        "core_DMI:0200": {
          "description": "Motherboard",
          "physid": "0",
          "product": "0A47AA",
          "serial": "..AB123456C12354.",
          "version": "C07"
        }
      },
      "driveHardware": [
        {
          "canonicalName": "sdh",
          "connected": true,
          "dev": 2160,
          "devPath": "/dev/disk/by-path/pci-0000:41:00.0-sas-
0x500056b37789abf0-lun-0",
          "driveEncryptionCapability": "fips",
          "driveType": "Block",
          "lifeRemainingPercent": 92,
          "lifetimeReadBytes": 175436696911872,
          "lifetimeWriteBytes": 81941097349120,
          "name": "scsi-SATA_INTEL_SSDSC2BB3BTWL12345686300AAA",
          "path": "/dev/sdh",
          "pathLink": "/dev/disk/by-path/pci-0000:41:00.0-sas-
0x500056b37789abf0-lun-0",
          "powerOnHours": 17246,
          "product": "INTEL SSDAA2AA300A4",
```

```
          "reallocatedSectors": 0,
          "reserveCapacityPercent": 100,
          "scsiCompatId": "scsi-SATA_INTEL_SSDSC2BB3BTWL12345686300AAA",
          "scsiState": "Running",
          "securityAtMaximum": false,
          "securityEnabled": false,
          "securityFrozen": false,
          "securityLocked": false,
          "securitySupported": true,
          "serial": "AAAA33710886300AAA",
          "size": 300069052416,
          "slot": 1,
          "smartSsdWriteCapable": false,
          "uuid": "aea178b9-c336-6bab-a61d-87b615e8120c",
          "vendor": "Intel",
          "version": "D2010370"
        },
      ...
      ]
    }
  }
}
```


Novità dalla versione

9.6

GetIpmiConfig

È possibile utilizzare `GetIpmiConfig` metodo per recuperare le informazioni sui sensori hardware dai sensori presenti nel nodo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo
ChassisType	Utilizzato per visualizzare le informazioni relative a ciascun tipo di chassis del nodo. Valori possibili: • all (tutti): restituisce le informazioni del sensore per ciascun tipo di chassis. • {chassis type} (tipo di telaio): restituisce le informazioni del sensore per un tipo di telaio specifico.	stringa

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
Nome sensore	Nome del sensore trovato.	stringa
UniqueSensorID	Identificatore univoco del sensore.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetIpmiConfig",
  "params": {
     "chassisType"; "all"
     },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id": 1,
   "result": {
     "nodes": [
         {
           "nodeID": 1,
           "result": {
```

```
            "ipmiConfig": {
               "C220M4": [
                    {
                     "sensorName": "Fan1A RPM",
                     "uniqueSensorID": "29.1:0xf"
                    },
                    {
                      "sensorName": "Fan1B RPM",
                      "uniqueSensorID": "29.1:0x10"
                    },
                    {
                      "sensorName": "Fan2A RPM",
                      "uniqueSensorID": "29.2:0x11"
                    },
                    {
                      "sensorName": "Fan2B RPM",
                      "uniqueSensorID": "29.2:0x12"
                    },
                    {
                      "sensorName": "Fan3A RPM",
                      "uniqueSensorID": "29.3:0x13"
                    },
                    {
                      "sensorName": "Fan3B RPM",
                      "uniqueSensorID": "29.3:0x14"
                    },
                    {
                      "sensorName": "Fan4A RPM",
                      "uniqueSensorID": "29.4:0x15"
                    },
                    {
                      "sensorName": "Fan4B RPM",
                      "uniqueSensorID": "29.4:0x16"
                    },
                    {
                      "sensorName": "Fan5A RPM",
                      "uniqueSensorID": "29.5:0x17"
                    },
                    {
                      "sensorName": "Fan5B RPM",
                      "uniqueSensorID": "29.5:0x18"
                    },
                    {
                      "sensorName": "Fan6A RPM",
                      "uniqueSensorID": "29.6:0x19"
                    },
```

```
            {
              "sensorName": "Fan6B RPM",
              "uniqueSensorID": "29.6:0x1a"
            },
            {
              "sensorName": "Exhaust Temp",
              "uniqueSensorID": "7.1:0x1"
            },
            {
              "sensorName": "Inlet Temp",
              "uniqueSensorID": "7.1:0x4"
            },
            {
              "sensorName": "PS1",
              "uniqueSensorID": "10.1:0x26"
            },
            {
              "sensorName": "PS2",
              "uniqueSensorID": "10.2:0x2c"
            }
        ],
        "R620": [
            {
              "sensorName": "Fan1A RPM",
              "uniqueSensorID": "7.1:0x30"
            },
            {
              "sensorName": "Fan1B RPM",
              "uniqueSensorID": "7.1:0x31"
            },
            {
              "sensorName": "Fan2A RPM",
              "uniqueSensorID": "7.1:0x32"
            },
            {
              "sensorName": "Fan2B RPM",
              "uniqueSensorID": "7.1:0x33"
            },
            {
              "sensorName": "Fan3A RPM",
              "uniqueSensorID": "7.1:0x34"
            },
            {
              "sensorName": "Fan3B RPM",
              "uniqueSensorID": "7.1:0x35"
            },
```

```
                    {
                      "sensorName": "Fan4A RPM",
                      "uniqueSensorID": "7.1:0x36"
                    },
                    {
                      "sensorName": "Fan4B RPM",
                      "uniqueSensorID": "7.1:0x37"
                    },
                    {
                      "sensorName": "Fan5A RPM",
                      "uniqueSensorID": "7.1:0x38"
                    },
                    {
                      "sensorName": "Fan5B RPM",
                      "uniqueSensorID": "7.1:0x39"
                    },
                    {
                      "sensorName": "Fan6A RPM",
                      "uniqueSensorID": "7.1:0x3a"
                    },
                    {
                      "sensorName": "Fan6B RPM",
                      "uniqueSensorID": "7.1:0x3b"
                    },
                    {
                      "sensorName": "Fan7A RPM",
                      "uniqueSensorID": "7.1:0x3c"
                    },
                    {
                      "sensorName": "Fan7B RPM",
                      "uniqueSensorID": "7.1:0x3d"
                    },
                    {
                      "sensorName": "Exhaust Temp",
                      "uniqueSensorID": "7.1:0x1"
                    },
                    {
                      "sensorName": "Inlet Temp",
                      "uniqueSensorID": "7.1:0x4"
                    },
                    {
                      "sensorName": "PS1",
                      "uniqueSensorID": "10.1:0x62"
                    },
                    {
                      "sensorName": "PS2",
```

```
                    "uniqueSensorID": "10.2:0x63"
                }
            ],
        }
```

Novità dalla versione

9.6

GetIpmiInfo

È possibile utilizzare `GetIpmiInfo` metodo per visualizzare un report dettagliato dei sensori (oggetti) per le ventole del nodo, le temperature di aspirazione e scarico e gli alimentatori monitorati dal sistema.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
sensori	Informazioni dettagliate da ciascun sensore all'interno di un nodo.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetIpmiInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

A causa della lunghezza della risposta restituita per questo metodo API, parti della risposta sono state intenzionalmente eliminate da questo documento. Sono incluse le parti delle informazioni hardware monitorate dal sistema per garantire che il nodo funzioni con performance ottimali.

```
{
  "id": 1,
    "result": {
```

```
    "ipmiInfo": {
        "sensors": [
          {
            "entityID": "7.1 (System Board)",
            "sensorID": "0x72",
            "sensorName": "SEL",
            "sensorType": "Event Logging Disabled",
            "uniqueSensorID": "7.1:0x72"
          },
          {
            "assertionsEnabled": [ "General Chassis intrusion" ],
            "deassertionsEnabled": [ "General Chassis intrusion" ],
            "entityID": "7.1 (System Board)", "sensorID": "0x73",
            "sensorName": "Intrusion",
            "sensorType": "Physical Security",
            "uniqueSensorID": "7.1:0x73"
          },
          {THIS ENTIRE SECTION IS REPEATED FOR EACH FAN IN THE SYSTEM
            "assertionEvents": [],
            "assertionsEnabled": [],
            "deassertionsEnabled": [],
            "entityID": "7.1 (System Board)",
            "eventMessageControl": "Per-threshold",
            "lowerCritical": "720.000",
            "lowerNonCritical": "840.000",
            "maximumSensorRange": "Unspecified",
            "minimumSensorRange": "Unspecified",
            "negativeHysteresis": "600.000",
            "nominalReading": "10080.000",
            "normalMaximum": "23640.000",
            "normalMinimum": "16680.000",
            "positiveHysteresis": "600.000",
            "readableThresholds": "lcr lnc",
            "sensorID": "0x30",
            "sensorName": "Fan1A RPM",
            "sensorReading": "4440 (+/- 120) RPM",
            "sensorType": "Fan",
            "settableThresholds": "",
            "status": "ok",
            "thresholdReadMask": "lcr lnc",
            "uniqueSensorID": "7.1:0x30"
          },
          .
          .
          .
          {THIS ENTIRE SECTION IS REPEATED FOR THE EXHAUST TEMPERATURE
```

```
OF EACH NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "entityID": "7.1 (System Board)",
              "eventMessageControl": "Per-threshold",
              "lowerCritical": "3.000",
              "lowerNonCritical": "8.000",
              "maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "1.000",
              "nominalReading": "23.000",
              "normalMaximum": "69.000",
              "normalMinimum": "11.000",
              "positiveHysteresis": "1.000",
              "readableThresholds": "lcr lnc unc ucr",
              "sensorID": "0x1",
              "sensorName": "Exhaust Temp",
              "sensorReading": "44 (+/- 1) degrees C",
              "sensorType": "Temperature",
              "settableThresholds": "",
              "status": "ok",
              "uniqueSensorID": "7.1:0x1",
              "upperCritical": "75.000",
              "upperNonCritical": "70.000"
            },
            {THIS ENTIRE SECTION IS REPEATED FOR THE INLET TEMPERATURE OF
EACH NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "deassertionsEnabled": [],
              "entityID": "7.1 (System Board)",
              "eventMessageControl": "Per-threshold",
              "lowerCritical": "-7.000",
              "lowerNonCritical": "3.000",
              "maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "1.000",
              "nominalReading": "23.000",
              "normalMaximum": "69.000",
              "normalMinimum": "11.000",
              "positiveHysteresis": "1.000",
              "readableThresholds": "lcr lnc unc ucr",
              "sensorID": "0x4",
              "sensorName": "Inlet Temp",
              "sensorReading": "20 (+/- 1) degrees C",
              "sensorType": "Temperature",
```

```
              "settableThresholds": "lcr lnc unc ucr",
              "status": "ok",
              "thresholdReadMask": "lcr lnc unc ucr",
              "uniqueSensorID": "7.1:0x4",
              "upperCritical": "47.000",
              "upperNonCritical": "42.000"
            },
            {THIS ENTIRE SECTION IS REPEATED FOR EACH POWER SUPPLY ON EACH
NODE
              "assertionEvents": [],
              "assertionsEnabled": [],
              "entityID": "10.2 (Power Supply)",
              "eventMessageControl": "Per-threshold",
"maximumSensorRange": "Unspecified",
              "minimumSensorRange": "Unspecified",
              "negativeHysteresis": "Unspecified",
              "nominalReading": "0.000",
              "normalMaximum": "0.000",
              "positiveHysteresis": "Unspecified",
              "readableThresholds": "No Thresholds",
              "sensorID": "0x6d",
              "sensorName": "Voltage 2",
              "sensorReading": "118 (+/- 0) Volts",
              "sensorType": "Voltage",
              "settableThresholds": "No Thresholds", "status": "ok",
"uniqueSensorID": "10.2:0x6d"
            },
              .
              .
              .
            }
          ]
        }
      }
    }
```


Novità dalla versione

9.6

GetNetworkConfig

È possibile utilizzare `GetNetworkConfig` metodo per visualizzare le informazioni di configurazione di rete per un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
rete	Tipi di connessione di rete e impostazioni correnti per ciascuna interfaccia di rete del nodo.	rete (tutte le interfacce)

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

GetNetworkConfig

Interfaccia GetNetworkInterface

È possibile utilizzare `GetNetworkInterface` metodo per ottenere informazioni su un'interfaccia di rete su un nodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
interfaccia	Il nome dell'interfaccia su cui ottenere informazioni per ciascun nodo. Valori possibili: • Bond1G • Bond10G	stringa	Nessuno	No
forza	Impostare questo parametro su true per l'esecuzione su tutti i nodi del cluster.	booleano	falso	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
nodi	Matrice di oggetti che descrivono l'interfaccia per ciascun nodo di storage nel cluster di storage. Ogni oggetto all'interno della matrice contiene i seguenti elementi: • NodeID: (Intero) ID del nodo di storage nel cluster di storage a cui si applicano le informazioni dell'interfaccia. • risultato: (NetworkInterface) Informazioni di configurazione dell'interfaccia per questo nodo di storage.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "GetNetworkInterface",
    "params": {
        "interface": "Bond1G",
        "force": true
        },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "nodes": [
            {
                "nodeID": 1,
                "result": {
                    "interface": {
                        "address": "10.117.64.32",
                        "addressV6": "::",
                        "broadcast": "10.117.79.255",
                        "macAddress": "90:b1:1c:42:e0:1e",
                        "mtu": 1500,
                        "name": "Bond1G",
                        "namespace": false,
                        "netmask": "255.255.240.0",
                        "status": "UpAndRunning",
                        "type": "BondMaster",
                        "virtualNetworkTag": 0
                    }
                }
            },
            {
                "nodeID": 2,
                "result": {
                    "interface": {
                        "address": "10.117.64.35",
                        "addressV6": "::",
                        "broadcast": "10.117.79.255",
                        "macAddress": "d4:ae:52:7a:ae:23",
                        "mtu": 1500,
                        "name": "Bond1G",
```

```
                    "namespace": false,
                    "netmask": "255.255.240.0",
                    "status": "UpAndRunning",
                    "type": "BondMaster",
                    "virtualNetworkTag": 0
                }
            }
        },
        {
            "nodeID": 3,
            "result": {
                "interface": {
                    "address": "10.117.64.39",
                    "addressV6": "::",
                    "broadcast": "10.117.79.255",
                    "macAddress": "c8:1f:66:f0:9d:17",
                    "mtu": 1500,
                    "name": "Bond1G",
                    "namespace": false,
                    "netmask": "255.255.240.0",
                    "status": "UpAndRunning",
                    "type": "BondMaster",
                    "virtualNetworkTag": 0
                }
            }
        },
        {
            "nodeID": 4,
            "result": {
                "interface": {
                    "address": "10.117.64.107",
                    "addressV6": "::",
                    "broadcast": "10.117.79.255",
                    "macAddress": "b8:ca:3a:f5:24:f8",
                    "mtu": 1500,
                    "name": "Bond1G",
                    "namespace": false,
                    "netmask": "255.255.240.0",
                    "status": "UpAndRunning",
                    "type": "BondMaster",
                    "virtualNetworkTag": 0
                }
            }
        }
    ]
}
```

```
}
```

Novità dalla versione

9.6

GetNodeActiveTlsCiphers

È possibile utilizzare `GetNodeActiveTlsCiphers` Metodo su un singolo nodo per ottenere un elenco dei cifrari TLS attualmente accettati su questo nodo. È possibile utilizzare questo metodo sui nodi di gestione e storage.

Parametro

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
MandatoryCipher	Elenco delle suite di crittografia TLS obbligatorie per il nodo. Si tratta di cifrari che sono sempre attivi sul nodo.	stringa
SuppementalCipher	Elenco delle suite di crittografia TLS supplementari per il nodo.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNodeActiveTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
      "id" : 1,
      "result" : {
        "mandatoryCiphers": [
            "DHE-RSA-AES256-SHA256",
            "DHE-RSA-AES256-GCM-SHA384",
            "ECDHE-RSA-AES256-SHA384",
            "ECDHE-RSA-AES256-GCM-SHA384"
        ],
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
    }
}
```

GetNodeFipsDrivesReport

È possibile utilizzare `GetNodeFipsDrivesReport` Metodo per controllare lo stato della funzionalità di crittografia del disco FIPS 140-2 di un singolo nodo nel cluster di storage. È necessario eseguire questo metodo su un singolo nodo di storage.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
FipsDrive	Oggetto JSON contenente lo stato del supporto della funzionalità FIPS 140-2 per questo nodo. Valori possibili: • None (Nessuno): Il nodo non supporta FIPS. • Parziale: Il nodo supporta FIPS, ma non tutti i dischi nel nodo sono dischi FIPS. • Pronto: Il nodo è compatibile con FIPS e tutti i dischi nel nodo sono dischi FIPS (o non sono presenti dischi).	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Novità dalla versione

11.5

GetNodeSSLCertificate

È possibile utilizzare `GetNodeSSLCertificate` Metodo per recuperare il certificato SSL attualmente attivo nel nodo di gestione.

Parametri

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
certificato	Il testo completo del certificato con codifica PEM.	stringa
dettagli	Le informazioni decodificate del certificato.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "GetNodeSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
```

```
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n",
        "details": {
            "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
            "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
            "notAfter": "2027-03-06T22:50:26Z",
            "notBefore": "2017-03-08T22:50:26Z",
            "serial": "CC1B221598E37FF3",
            "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
            "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
        }
    }
}
```


GetNodeSupportedTlsCiphers

È possibile utilizzare `GetNodeSupportedTlsCiphers` Metodo su un singolo nodo per ottenere un elenco dei cifrari TLS attualmente supportati su questo nodo. È possibile utilizzare questo metodo sui nodi di gestione e storage.

Parametro

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
MandatoryCipher	Elenco delle suite di crittografia TLS obbligatorie per il nodo. Si tratta di cifrari che sono sempre attivi sul nodo.	stringa
DefaultSupplementalCipher	Elenco delle suite di crittografia TLS supplementari predefinite per il nodo. I cifrari supplementari vengono ripristinati in questo elenco quando si esegue il metodo API ResetNodeSupplementalTlsCiphers.	stringa
SupportedSupplementalCipher	Elenco delle suite di crittografia TLS supplementari disponibili che è possibile configurare con il metodo API SetNodeSupplementalTlsCipher.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNodeSupportedTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
    "defaultSupplementalCiphers": [
        "DHE-RSA-AES128-SHA256",
        "DHE-RSA-AES128-GCM-SHA256",
        "ECDHE-RSA-AES128-SHA256",
        "ECDHE-RSA-AES128-GCM-SHA256"
    ],
    "mandatoryCiphers": [
        "DHE-RSA-AES256-SHA256",
        "DHE-RSA-AES256-GCM-SHA384",
        "ECDHE-RSA-AES256-SHA384",
        "ECDHE-RSA-AES256-GCM-SHA384"
    ],
    "supportedSupplementalCiphers": [
        "DHE-RSA-AES128-SHA256",
        "DHE-RSA-AES128-GCM-SHA256",
        "ECDHE-RSA-AES128-SHA256",
        "ECDHE-RSA-AES128-GCM-SHA256",
        "DHE-RSA-AES256-SHA",
        "ECDHE-RSA-AES256-SHA",
        "DHE-RSA-CAMELLIA256-SHA",
        "DHE-RSA-AES128-SHA",
        "ECDHE-RSA-AES128-SHA",
        "DHE-RSA-CAMELLIA128-SHA"
    ]
}
}
```

GetPatchInfo

È possibile utilizzare `GetPatchInfo` Metodo per ottenere informazioni sulle patch software Element installate su un nodo di storage.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`force`	Forzare l'esecuzione del metodo su tutti i nodi del cluster di storage. Ciò è necessario solo quando si invia l'API a un indirizzo IP del cluster anziché a un singolo nodo. Valori possibili: • `true` • `false`	booleano	`false`	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
patch	Oggetto contenente informazioni sulle patch installate su questo nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetPatchInfo",
   "params": {
      "force": false,
      },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "patches": {
          "SUST936": {
          "date": "Wed 09 Dec 2020 10:41:59 PM UTC",
          "description": "BMC fixes",
          "newFiles": [
              "None"
          ],
          "patchedFiles": [
              "Patched_file_1.bin",
              "Patched_file_2.dat",
              "Patched_file_3.tgz"
          ]
          }
        }
    }
}
```

Novità dalla versione

12.3

GetPendingOperation

È possibile utilizzare `GetPendingOperation` metodo per rilevare un'operazione su un nodo attualmente in corso. Questo metodo può essere utilizzato anche per generare un report quando un'operazione è stata completata.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
in sospeso	Valori possibili: • Vero: L'operazione è ancora in corso. • falso: L'operazione non è più in corso.	booleano
operazione	Nome dell'operazione in corso o completata.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetPendingOperation",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "pendingOperation" : {
         "pending" : "true",
         "operation" : "TestDrivesInternal",
      }
   }
}
```

Novità dalla versione

9.6

GetSshInfo

È possibile utilizzare `GetSshInfo` Metodo per eseguire query sullo stato del servizio SSH su un singolo nodo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
risultato	Lo stato del servizio SSH per questo nodo.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "GetSshInfo",
    "params" : {},
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "enabled": false
    }
}
```

ListDrivehardware

È possibile utilizzare `ListDriveHardware` metodo per elencare tutti i dischi collegati a un nodo. Se utilizzato su singoli nodi, questo metodo restituisce informazioni sull'hardware del disco. Se utilizzato sul nodo master del cluster MVIP, questo metodo restituisce informazioni per tutti i dischi su tutti i nodi.

Parametri

La risposta "securitySupported": True line of the method non implica che i dischi siano in grado di eseguire la crittografia, ma solo che sia possibile eseguire una query sullo stato di sicurezza. Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", i comandi per abilitare le funzioni di sicurezza su questi dischi non avranno esito positivo.

Questo metodo ha il seguente parametro:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare su true per eseguire questo metodo su tutti i nodi.	booleano	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
Hardware del drivehardware	Informazioni sull'hardware del disco restituite per il nodo.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "ListDriveHardware",
"params": {},
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "driveHardware": [
      {
        "canonicalName": "sda",
        "connected": true,
        "dev": 2048,
        "devPath": "/dev/slot0",
        "driveEncryptionCapability": "fips",
        "driveType": "Slice",
        "lifeRemainingPercent": 98,
        "lifetimeReadBytes": 0,
        "lifetimeWriteBytes": 14012129542144,
        "name": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
        "path": "/dev/sda",
        "pathLink": "/dev/slot0",
        "powerOnHours": 15489,
        "product": "SAMSUNG MZ7GE240HMGR-00003",
        "reallocatedSectors": 0,
        "reserveCapacityPercent": 100,
        "scsiCompatId": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
        "scsiState": "Running",
        "securityAtMaximum": false,
        "securityEnabled": true,
        "securityFrozen": false,
        "securityLocked": false,
        "securitySupported": true,
        "serial": "S1M9NWAG501251",
        "size": 240057409536,
        "slot": 0,
        "uncorrectableErrors": 0,
        "uuid": "789aa05d-e49b-ff4f-f821-f60eed8e43bd",
        "vendor": "Samsung",
        "version": "EXT1303Q"
      }
    ]
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

EnableEncryptionAtRest

ListNetworkInterfaces

È possibile utilizzare `ListNetworkInterfaces` metodo per elencare le informazioni relative a ciascuna interfaccia di rete su un nodo. Questo metodo API è destinato all'utilizzo su singoli nodi; per l'accesso ai singoli nodi è richiesta l'autenticazione di ID utente e password. Tuttavia, è possibile utilizzare questo metodo nel cluster se al parametro force viene assegnato il valore true nella chiamata al metodo. Quando il parametro viene utilizzato nel cluster, vengono elencate tutte le interfacce.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Valori possibili: • True: Vengono restituite informazioni su tutte le interfacce di rete nel cluster. • Falso: Non viene restituita alcuna informazione.	booleano	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
interfacce	Un elenco di informazioni di configurazione per ciascuna interfaccia di rete del nodo di storage (o dell'intero cluster di storage, se force = `true`).	NetworkInterface array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "ListNetworkInterfaces",
"params": {},
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "nodes": [
            {
                "nodeID": 1,
                "result": {
                    "interfaces": [
                        {
                            "address": "10.117.80.32",
                            "addressV6": "::",
                            "broadcast": "10.117.95.255",
                            "macAddress": "90:b1:1c:42:e0:1a",
                            "mtu": 9000,
                            "name": "Bond10G",
                            "namespace": false,
                            "netmask": "255.255.240.0",
                            "status": "UpAndRunning",
                            "type": "BondMaster",
                            "virtualNetworkTag": 0
                        },
                        {
                            "address": "10.117.64.32",
                            "addressV6": "::",
                            "broadcast": "10.117.79.255",
                            "macAddress": "90:b1:1c:42:e0:1e",
                            "mtu": 1500,
                            "name": "Bond1G",
                            "namespace": false,
                            "netmask": "255.255.240.0",
                            "status": "UpAndRunning",
                            "type": "BondMaster",
                            "virtualNetworkTag": 0
                        },
                        {
```

```
                            "address": "0.0.0.0",
                            "addressV6": "::",
                            "broadcast": "0.0.0.0",
                            "macAddress": "90:b1:1c:42:e0:1a",
                            "mtu": 9000,
                            "name": "eth0",
                            "namespace": false,
                            "netmask": "0.0.0.0",
                            "status": "UpAndRunning",
                            "type": "BondSlave",
                            "virtualNetworkTag": 0
                        },
                        {
                            "address": "127.0.0.1",
                            "addressV6": "::",
                            "broadcast": "0.0.0.0",
                            "macAddress": "00:00:00:00:00:00",
                            "mtu": 0,
                            "name": "lo",
                            "namespace": false,
                            "netmask": "0.0.0.0",
                            "status": "UpAndRunning",
                            "type": "Loopback",
                            "virtualNetworkTag": 0
                        }
                    ]
                }
            }
        ]
    }
}
```


Novità dalla versione

9.6

ListNetworkInterfaceStats

È possibile utilizzare `ListNetworkInterfaceStats` metodo per elencare statistiche come il numero di pacchetti ignorati e vari tipi di errori per ogni interfaccia di rete su un nodo. Questo metodo API è destinato all'utilizzo su singoli nodi; per l'accesso ai singoli nodi è richiesta l'autenticazione di ID utente e password. Tuttavia, è possibile utilizzare questo metodo nel cluster se al parametro force viene assegnato il valore true nella chiamata al metodo. Quando il parametro viene utilizzato nel cluster, vengono elencate le statistiche di rete per tutte le interfacce.

Parametro

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
NetworkInterfaceStats	Un elenco di informazioni statistiche di rete, come il numero di pacchetti interrotti e vari tipi di errori di rete, per ogni interfaccia di rete di un nodo di storage.	NetworkInterfaceStats array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "ListNetworkInterfaceStats",
"params": {},
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "networkInterfaceStats": [
        {
            "rxErrors": 1,
            "rxPackets": 1,
            "txErrors": 1,
            "rxDropped": 1,
            "txCarrierErrors": 1,
            "rxOverErrors": 1,
            "rxMissedErrors": 1,
            "txPackets": 1,
            "name": "if_name",
            "rxLengthErrors": 1,
            "collisions": 1,
            "rxFifoErrors": 1,
            "txBytes": 1,
            "rxBytes": 1,
            "rxFrameErrors": 1,
            "rxCrcErrors": 1,
            "txFifoErrors": 1
        }
    ]
}
```

Novità dalla versione

12.3

ListTest

È possibile utilizzare `ListTests` metodo per elencare i test disponibili per l'esecuzione su un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
test	Elenco dei test che è possibile eseguire sul nodo.	array di stringhe

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListTests",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
   "tests": [
             "TestConnectEnsemble",
             "TestConnectMvip",
             "TestConnectSvip",
             "TestDrives",
             "TestHardwareConfig",
             "TestLocateCluster",
             "TestPing",
             "TestLocalConnectivity",
             "TestRemoteConnectivity",
             "TestNetworkConfig"
           ]
      }
}
```

Novità dalla versione

9.6

ListUtilities

È possibile utilizzare `ListUtilities` metodo per elencare le operazioni disponibili per l'esecuzione su un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
utilità	Elenco delle utility attualmente disponibili per l'esecuzione sul nodo.	array di stringhe

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListUtilities",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "utilities": [
      "ResetDrives",
      "ResetNode",
      "RestartNetworking",
      "RestartServices",
      "CreateSupportBundle",
      "DeleteAllSupportBundles",
      "CreateClusterSupportBundle"
    ]
  }
}
```

Novità dalla versione

9.6

RemoveNodeSSLCertificate

È possibile utilizzare `RemoveNodeSSLCertificate` Metodo per rimuovere il certificato

SSL dell'utente e la chiave privata per il nodo di gestione. Una volta rimossi il certificato e la chiave privata, il nodo di gestione viene configurato per utilizzare il certificato e la chiave privata predefiniti.

Parametri

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "RemoveNodeSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 3,
    "result" : {}
}
```

ResetDrive

È possibile utilizzare `ResetDrives` metodo per inizializzare in maniera proattiva i dischi e rimuovere tutti i dati attualmente presenti su un disco. L'unità può quindi essere riutilizzata in un nodo esistente o in un nodo aggiornato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dischi	Elenco dei nomi dei dispositivi (non degli ID unità) da ripristinare.	stringa	Nessuno	Sì
forza	Impostare su true per ripristinare l'unità.	booleano	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Dettagli dei dischi che si stanno ripristinando.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ResetDrives",
   "params": {
      "drives" : "slot3",
      "force" : true
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
   "details": {
    "drives": [
    {
      "drive": "slot3",
      "returnCode": 0,
      "stderr": " * Unlocking /dev/slot9 .[ ok ]\ * Setting master
password /dev/slot9 .[ ok ]\ * Secure erasing /dev/slot9 (hdparm)
[tries=0/1] .........................[ ok ]",
      "stdout": ""
    }
   ]
  },
  "duration": "00:00:28.501269",
  "result": "Passed"
  }
}
```


Novità dalla versione

9.6

ResetNode

È possibile utilizzare `ResetNode` metodo per ripristinare le impostazioni predefinite di un nodo. Tutti i dati, i pacchetti (aggiornamenti software, ecc.), le configurazioni e i file di log vengono cancellati dal nodo quando si chiama questo metodo. Tuttavia, le impostazioni di rete per il nodo vengono mantenute durante questa operazione. I nodi che partecipano a un cluster non possono essere ripristinati alle impostazioni predefinite.

Parametri

L'API ResetNode può essere utilizzata solo su nodi che si trovano in uno stato "disponibile". Non può essere utilizzato su nodi "attivi" in un cluster o in uno stato "in sospeso".

ATTENZIONE:

Questo metodo consente di eliminare tutti i dati del cliente presenti nel nodo.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
costruire	Consente di specificare l'URL di un'immagine software dell'elemento remoto in cui il nodo verrà reimpostato.	URL	Nessuno	No
forza	Impostare su true per ripristinare il nodo.	booleano	Nessuno	Sì
opzioni	Consente di immettere le specifiche per l'esecuzione delle operazioni di ripristino. I dettagli sono forniti dal supporto NetApp, se necessario.	Oggetto JSON	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ResetNode",
   "params": {
      "build" : "file:///sf/rtfi/image/filesystem.squashfs",
      "force" : true
              },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": null,
  "result": {
```

```
    "rtfiInfo": {
      "build": "file:///sf/rtfi/image/filesystem.squashfs",
      "generation": "9",
      "options": {
        "edebug": "",
        "sf_auto": "0",
        "sf_bond_mode": "ActivePassive",
        "sf_check_hardware": "0",
        "sf_disable_otpw": "0",
        "sf_fa_host": "",
        "sf_hostname": "SF-FA18",
        "sf_inplace": "1",
        "sf_inplace_die_action": "kexec",
        "sf_inplace_safe": "0",
        "sf_keep_cluster_config": "0",
        "sf_keep_data": "0",
        "sf_keep_hostname": "0",
        "sf_keep_network_config": "0",
        "sf_keep_paths": "\"/var/log/hardware.xml\"",
        "sf_max_archives": "5",
        "sf_nvram_size": "",
        "sf_oldroot": "",
        "sf_postinst_erase_root_drive": "0",
        "sf_root_drive": "",
        "sf_rtfi_cleanup_state": "",
        "sf_secure_erase": "1",
        "sf_secure_erase_retries": "5",
        "sf_slice_size": "",
        "sf_ssh_key": "1",
        "sf_ssh_root": "1",
        "sf_start_rtfi": "1",
        "sf_status_httpserver": "1",
        "sf_status_httpserver_stop_delay": "5m",
        "sf_status_inject_failure": "",
        "sf_status_json": "0",
        "sf_support_host": "sfsupport.solidfire.com",
        "sf_test_hardware": "0",
        "sf_upgrade": "0",
        "sf_upgrade_firmware": "0",
        "sf_upload_logs_url": ""
      },
      "statusUrlAll": "http://192.168.130.20/status/all.json",
      "statusUrlCurrent": "http://192.168.130.20/status/current.json"
    }
  }
}
```

Novità dalla versione

9.6

ResetNodeSupplementalTlsCiphers

È possibile utilizzare `ResetNodeSupplementalTlsCiphers` Metodo per ripristinare l'elenco di crittografia TLS supplementari ai valori predefiniti. È possibile utilizzare questo comando sui nodi di gestione.

Parametro

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ResetNodeSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Restart Networking (Ripristino rete)

È possibile utilizzare `RestartNetworking` metodo per riavviare i servizi di rete su un nodo.

ATTENZIONE:

Questo metodo riavvia tutti i servizi di rete su un nodo, causando la perdita temporanea della connettività di rete.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare su true per riavviare i servizi di rete su un nodo.	booleano	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RestartNetworking",
   "params": {
              "force" : true
             },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{ "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

RestartServices

È possibile utilizzare `RestartServices` metodo per riavviare i servizi su un nodo.

Parametri

ATTENZIONE:

Questo metodo causa l'interruzione temporanea dei servizi del nodo.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare su true per riavviare i servizi su un nodo.	booleano	Nessuno	Sì
servizio	Nome del servizio da riavviare.	stringa	Nessuno	No
azione	Azione da eseguire sul servizio (avvio, arresto, riavvio).	stringa	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
dettagli	L'output della procedura di riavvio del servizio, inclusi gli errori (se presenti).	Oggetto JSON
durata	Il tempo, in secondi, impiegato per riavviare i servizi al nodo.	stringa
risultato	Risultati del riavvio.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RestartServices",
   "params": {
              "force" : true
              "action" : restart,
             }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "details": "solidfire stop/waiting\nsolidfire start/running, process
7284\n",
    "duration": "00:00:02.541594",
    "result": "Passed"
  }
}
```

Novità dalla versione

9.6

SetClusterConfig

È possibile utilizzare `SetClusterConfig` metodo per impostare la configurazione utilizzata da un nodo per comunicare con il cluster a cui è associato. Per visualizzare le impostazioni correnti dell'interfaccia del cluster per un nodo, eseguire `GetClusterConfig` Metodo API.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
cluster	Attributi di configurazione che devono essere modificati durante questa chiamata al metodo. Solo i campi che si desidera modificare devono essere aggiunti a questo metodo come membri di questo parametro.	cluster	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
cluster	Informazioni di configurazione utilizzate dal nodo per comunicare con il cluster.	cluster

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "SetClusterConfig",
   "params": {
      "cluster": {
         "name": "myhost",
         "mipi": "Bond10G"
      },
    "id" : 1
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "cluster" : {
         "cipi" : "Bond10G",
         "cluster" : "QoS",
         "ensemble" : [
            "1:10.10.5.42",
            "2:10.10.5.43",
            "3:10.10.5.44",
            "4:10.10.5.46",
            "5:10.10.5.47"
         ],
          "hostname" : "myhost",
          "mipi" : "Bond10G",
          "nodeID" : 1,
          "sipi" : "Bond10G",
          "state" : "Active"
      }
   }
}
```

Novità dalla versione

9.6

SetConfig

È possibile utilizzare `SetConfig` metodo per impostare le informazioni di rete e del cluster per il nodo. Questo metodo include le stesse impostazioni in un singolo metodo API che sono disponibili utilizzando entrambi `SetClusterConfig` e. `SetNetworkConfig` metodi. Solo i campi che si desidera modificare devono essere inclusi con questo metodo.

Parametro

ATTENZIONE:

La modifica della modalità bond su un nodo può causare una perdita temporanea della connettività di rete.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
cluster	Informazioni sul cluster che identificano il modo in cui il nodo di storage comunica con il cluster di storage a cui è associato.	cluster	Nessuno	No
rete	Tipi di connessione di rete e impostazioni correnti per ciascuna interfaccia di rete del nodo.	rete (tutte le interfacce)	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
config	La configurazione nuova e corrente del nodo. Questo oggetto contiene: • cluster: Informazioni sul cluster che identificano il modo in cui il nodo di storage comunica con il cluster di storage a cui è associato. • rete (tutte le interfacce): Tipi di connessione di rete e impostazioni correnti per ciascuna interfaccia di rete del nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "SetConfig",
    "params": {
        "cluster": {
            "name": "MyHostname"
        },
        "network": {
            "Bond10G": {
                "bond-mode": "ALB"
            }
        }
    }
}
```

Esempio di risposta

La risposta di questo metodo è la stessa del ritorno per il metodo GetConfig. Tutti i campi per la visualizzazione dell'oggetto e i valori aggiornati vengono visualizzati quando si utilizza SetConfig.

Novità dalla versione

9.6

Trova ulteriori informazioni

- SetClusterConfig
- SetNetworkConfig
- GetConfig

SetNetworkConfig

È possibile utilizzare `SetNetworkConfig` metodo per impostare la configurazione di rete per un nodo. Per visualizzare le impostazioni di rete correnti per un nodo, eseguire `GetNetworkConfig` Metodo API.

Parametro

ATTENZIONE:

La modifica della modalità bond su un nodo può causare una perdita temporanea della connettività di rete.

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
rete	Oggetto contenente le impostazioni di rete del nodo da modificare. In questo parametro è necessario solo aggiungere i campi che si desidera modificare a questo metodo come attributi.	rete (tutte le interfacce)	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
rete	La configurazione di rete nuova e corrente per il nodo.	rete (tutte le interfacce)

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "SetNetworkConfig",
        "params": {
            "network": {
                "Bond10G": {
                    "bond-mode": "ALB"
                },
                "Bond1G": {
                    "netmask": "255.255.224.0"
                },
                "eth0": {
                    "method": "bond"
                },
                "lo": {
                    "method": "loopback"
                }
            }
        }
}
```

Esempio di risposta

La risposta di questo metodo è la stessa del metodo GetNetworkConfig. Il metodo visualizza tutti i membri per ciascun oggetto e include i nuovi valori per tutti i membri modificati.

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetNetworkConfig
- GetNetworkConfig

SetNodeSSLCertificate

È possibile utilizzare `SetNodeSSLCertificate` Metodo per impostare un certificato SSL utente e una chiave privata per il nodo di gestione.

Dopo aver utilizzato l'API, riavviare il nodo di gestione.

Parametri

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
certificato	Versione del certificato con codifica PEM.**Nota:** quando si imposta un certificato di nodo o cluster, il certificato deve includere l'estensione extideKeyUsage per serverAuth. Questa estensione consente di utilizzare il certificato senza errori nei sistemi operativi e nei browser più comuni. Se l'estensione non è presente, l'API rifiuterà il certificato come non valido.	stringa	Nessuno	Sì
PrivateKey	Versione del testo con codifica PEM della chiave privata.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "SetNodeSSLCertificate",
    "params" : {
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEWMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrgpGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yjUGQO352ylc9HXHcn6lb
/jyl0DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAoIBAH1jlIZr6/sltqVW\nO0qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuHl1esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIJIMEgnfuLZp8IelJQXn\nSFJbk2ECgYEA
```

```
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nlHzPlhms6hxexwz1dzAp
gog/NOM+2bAc0rn0dqvtV4doejtlDZKRqrNCf/cuN2QX\njaCJClCWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhzXpLr+v30Hy2h0yAlBS\nny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nC9MJtXGfhp//G0bzwsRzZxOBsUJb15tppaZIs9MCgYAJricpkKjM
0xlZ1jdvXsos\nPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+AOeQXw3vgAhJ/qNJ\njQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nzPssy6t+QE
La1fFbAXkZ5Pg1ITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\n+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\njS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\n3rnR8AqAm4VMzqRahs2PWNe2Hl4J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nInDXvTgXMdMoet4BKnftelrXFKHgGqXJoczq4JWzGS
IHNgvkrH60\n-----END RSA PRIVATE KEY-----\n",
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}
```


Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 2,
    "result" : {}
}
```

SetNodeSupplementalTlsCiphers

È possibile utilizzare `SetNodeSupplementalTlsCiphers` Metodo per specificare l'elenco di crittografia TLS supplementari. È possibile utilizzare questo comando sui nodi di gestione.

Parametro

È necessario chiamare questo metodo per il nodo di gestione. Ad esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SuppementalCipher	I nomi della suite di crittografia supplementare che utilizzano lo schema di denominazione OpenSSL. L'utilizzo dei nomi delle suite di crittografia non fa distinzione tra maiuscole e minuscole.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
MandatoryCipher	Elenco delle suite di crittografia TLS obbligatorie per il nodo. Si tratta di cifrari che sono sempre attivi sul nodo.	stringa
SuppementalCipher	Elenco delle suite di crittografia TLS supplementari per il nodo.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "SetNodeSupplementalTlsCiphers",
   "params": {
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
        "mandatoryCiphers": [
            "DHE-RSA-AES256-SHA256",
            "DHE-RSA-AES256-GCM-SHA384",
            "ECDHE-RSA-AES256-SHA384",
            "ECDHE-RSA-AES256-GCM-SHA384"
        ],
        "supplementalCiphers": [
            "DHE-RSA-AES128-SHA256",
            "DHE-RSA-AES128-GCM-SHA256",
            "ECDHE-RSA-AES128-SHA256",
            "ECDHE-RSA-AES128-GCM-SHA256"
        ]
    }
}
```

Spegnere

È possibile utilizzare `Shutdown` metodo per riavviare o arrestare i nodi in un cluster. Questo metodo consente di arrestare un singolo nodo, più nodi o tutti i nodi del cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nodi	Elenco di NodeID per i nodi da riavviare o arrestare.	array intero	Nessuno	Sì
opzione	Azione da intraprendere per il cluster. Valori possibili: * Restart: Riavvia il cluster. * Halt: Esegue uno spegnimento completo.	stringa	riavviare	No

Valore restituito

Questo metodo non ha alcun valore restituito. == Richieste di esempio per questo metodo sono simili all'esempio seguente:

```
{
   "method": "Shutdown",
   "params": {
     "nodes": [
       2,
       3,
       4
     ],
     "option": "halt"
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
     "failed": [],
     "successful": [
          6
      [
   }
}
```

Novità dalla versione

9.6

TestConnectEnsemble

È possibile utilizzare `TestConnectEnsemble` metodo per verificare la connettività con un insieme di database specificato. Per impostazione predefinita, utilizza l'insieme per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un gruppo diverso per testare la connettività.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ensemble	Un elenco separato da virgole di indirizzi IP del cluster di nodi ensemble per il test di connettività.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Oggetti restituiti: • `nodes`: (Oggetto) un elenco di ciascun nodo dell'ensemble nel test e dei risultati dei test. • `duration`: (String) il tempo necessario per eseguire il test. • `result`: (String) i risultati dell'intero test.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "TestConnectEnsemble",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
      "details": {
         "nodes":  {
            "1:10.10.20.70": "Passed",
            "2:10.10.20.71": "Passed",
            "3:10.10.20.72": "Passed",
            "4:10.10.20.73": "Passed",
            "5:10.10.20.74": "Passed"
        }
      },
        "duration": "00:00:00:756072",
        "result": "Passed"
   }
}
```

Novità dalla versione

9.6

TestConnectMvip

È possibile utilizzare `TestConnectMvip` metodo per verificare la connessione di gestione al cluster di storage. Il test esegue il ping di MVIP ed esegue un semplice metodo API per verificare la connettività.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
mvip	È possibile superare questo valore per verificare la connessione di gestione di un diverso MVIP. Non è necessario utilizzare questo valore durante il test della connessione al cluster di destinazione.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test (oggetto JSON): • `connected`: Indica se il test potrebbe connettersi a MVIP (booleano) • `mvip`: L'MVIP testato rispetto a (stringa) • `pingBytes`: Dettagli dei test ping con 56 byte e 1500 byte (oggetto) ◦ `56`: Risultati del test ping a 56 byte (oggetto JSON): ▪ `individualResponseTimes`: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ `individualStatus`: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ `responseTime`: Tempo medio di risposta ping (stringa) ▪ `successful`: Indica se il test ping ha avuto esito positivo (booleano) ◦ `1500`: Risultati del test ping a 1500 byte (oggetto JSON): ▪ `individualResponseTimes`: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ `individualStatus`: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ `responseTime`: Tempo medio di risposta ping (stringa)	Oggetto JSON
	`successful`: Se il test ping ha avuto esito	

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestConnectMvip",
   "params": {
       "mvip" : "172.27.62.50"
       },
    "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "details": {
      "connected": true,
      "mvip": "172.27.62.50",
      "pingBytes": {
        "1500": {
          "individualResponseTimes": [
            "00:00:00.000250",
            "00:00:00.000206",
            "00:00:00.000200",
            "00:00:00.000199",
            "00:00:00.000199"
         ],
          "individualStatus": [
             true,
             true,
             true,
             true,
             true
         ],
         "responseTime": "00:00:00.000211",
         "successful": true
       },
       "56": {
          "individualResponseTimes": [
            "00:00:00.000217",
            "00:00:00.000122",
            "00:00:00.000117",
```

```
            "00:00:00.000119",
            "00:00:00.000121"
         ],
         "individualStatus": [
            true,
            true,
            true,
            true,
            true
         ],
         "responseTime": "00:00:00.000139",
         "successful": true
        }
      }
    },
    "duration": "00:00:00.271244",
    "result": "Passed"
  }
}
```


Novità dalla versione

9.6

TestConnectSvip

È possibile utilizzare `TestConnectSvip` metodo per verificare la connessione dello storage al cluster di storage. Il test esegue il ping dell'SVIP utilizzando i pacchetti ICMP e, una volta eseguito correttamente, si connette come iniziatore iSCSI.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
svip	È possibile superare questo valore per verificare la connessione di gestione di un SVIP diverso. Non è necessario utilizzare questo valore durante il test della connessione al cluster di destinazione.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test (oggetto JSON): • `connected`: Indica se il test potrebbe connettersi a SVIP (booleano) • `svip`: SVIP testato rispetto a (stringa) • `pingBytes`: Dettagli dei test ping con 56 byte e 9000 byte (oggetto) ◦ `56`: Risultati del test ping a 56 byte (oggetto JSON): ▪ `individualResponseTimes`: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ `individualStatus`: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ `responseTime`: Tempo medio di risposta ping (stringa) ▪ `successful`: Indica se il test ping ha avuto esito positivo (booleano) ◦ `9000`: Risultati del test ping a 9000 byte (oggetto JSON): ▪ `individualResponseTimes`: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ `individualStatus`: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ `responseTime`: Tempo medio di risposta ping (stringa)	stringa
	`successful`: Indica se il test ping ha avuto	

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestConnectSvip",
   "params": {
      "svip" : "172.27.62.50"
      },
   "id" : 1
}
```

- esito positivo (booleano)

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "details": {
      "connected": true,
      "pingBytes": {
           "56": {
               "individualResponseTimes": [
                   "00:00:00.000152",
                   "00:00:00.000132",
                   "00:00:00.000119",
                   "00:00:00.000114",
                   "00:00:00.000112"
              ],
              "individualStatus": [
                  true,
                  true,
                  true,
                  true,
                  true
              ],
              "responseTime": "00:00:00.000126",
              "successful": true
           },
          "9000": {
                "individualResponseTimes": [
                    "00:00:00.000295",
                    "00:00:00.000257",
                    "00:00:00.000172",
                    "00:00:00.000172",
```

```
                    "00:00:00.000267"
                ],
                "individualStatus": [
                    true,
                    true,
                    true,
                    true,
                    true
                ],
                "responseTime": "00:00:00.000233",
                "successful": true
            }
          },
          "svip": "172.27.62.50"
        },
        "duration": "00:00:00.421907",
        "result": "Passed"
    }
}
```


Novità dalla versione

9.6

TestDrive

È possibile utilizzare `TestDrives` metodo per eseguire una convalida dell'hardware su tutti i dischi del nodo. Questo metodo rileva i guasti hardware sui dischi e riporta i risultati dei test di convalida.

Parametri

È possibile utilizzare solo `TestDrives` Metodo su nodi non "attivi" in un cluster.

Il test richiede circa 10 minuti.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Impostare su true per testare i dischi sul nodo.	booleano	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
minuti	Specifica il numero di minuti per l'esecuzione del test.	intero	10	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test riuscita o non riuscita.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestDrives",
   "params": {
              "force": true,
              "minutes" : 10
             },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una tabella contenente i risultati dei test per ogni disco nel nodo.

Novità dalla versione

9.6

TestHardwareConfig

È possibile utilizzare `TestHardwareConfig` metodo per eseguire test hardware su un nodo. Le opzioni di test includono la verifica delle configurazioni hardware, delle versioni del firmware e della presenza di tutti i dischi.

Parametri

Questi test non sono destinati a rilevare guasti hardware.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
pulito	Avvia il test di configurazione dell'hardware con una cache pulita. Valori possibili: • Vero: Elimina il file di risultati dei test memorizzato nella cache e riesegue i test. • Falso: Recupera i risultati di un test memorizzato nella cache.	booleano	falso	No
forza	Il parametro force deve essere incluso in questo metodo per ripristinare correttamente il nodo.	booleano	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Dettagli sulla configurazione dell'hardware.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestHardwareConfig",
   "params": {
      "force": true
     },
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

TestHardwareConfig

TestLocateCluster

È possibile utilizzare `TestLocateCluster` metodo per verificare che il nodo sia in grado di individuare il cluster specificato nella configurazione del cluster. L'output convalida la creazione del cluster ed elenca i nodi nell'insieme del cluster.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test riuscita o non riuscita.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestLocateCluster",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
      "details": {
         "complete": true,
         "ensemble": {
            "nodes": [
               {
                 "IP": "10.10.5.94",
                 "nodeID": 1
               },
               {
                 "IP": "10.10.5.107",
                 "nodeID": 2
               },
               {
                 "IP": "10.10.5.108",
                 "nodeID": 3
               }
            ]
         },
         "version": "5.749"
      },
      "duration": "0.0384478sec",
      "result": "Passed"
   }
}
```


Novità dalla versione

9.6

TestLocalConnectivity

È possibile utilizzare `TestLocalConnectivity` Metodo per eseguire il ping dell'IP del cluster (CIP) di ciascun nodo in un cluster attivo.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Tempi di risposta ping singoli per ciascun nodo del cluster attivo locale.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "TestLocalConnectivity",
    "params": {},
    "id": 1
}
```

Esempio di risposta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "id": null,
   "result": {
      "details": {
                  "10.26.86.17": {
                     individualResponseTimes: [
                          "00:00:00.006868",
                          "00:00:00.005933",
                          "00:00:00.006655",
                          "00:00:00.006584",
                          "00:00:00.006334"
                     ],
                     individualStatus: [
                           true,
                           true,
                           true,
                           true,
                           true
                     ],
                     responseTime: "00:00:00.006475",
                     successful: true
                        },
                        "10.26.86.18": {
                     individualResponseTimes: [
                          "00:00:00.006201",
```

```
                    "00:00:00.006187",
                    "00:00:00.005990",
                    "00:00:00.006029",
                    "00:00:00.005917"],
                individualStatus: [
                     true,
                     true,
                     true,
                     true,
                     true
                ],
                "responseTime": "00:00:00.006065",
                "successful": true
    },
                  "10.26.86.19": {
                individualResponseTimes: [
                    "00:00:00.005988",
                    "00:00:00.006948",
                    "00:00:00.005981",
                    "00:00:00.005964",
                    "00:00:00.005942"
                 ],
                individualStatus: [
                           "true",
                           "true",
                     true,
                     true,
                     true
                 ],
                 responseTime: "00:00:00.006165",
                 successful: true,
           },
                     "10.26.86.20": {
                individualResponseTimes: [
                     "00:00:00.005926",
                     "00:00:00.006072",
                     "00:00:00.005675",
                     "00:00:00.009904",
                     "00:00:00.006225"
                 ],
                         "individualStatus": [
                     true,
                     true,
                     true,
                     true,
                     true
```

```
                    ],
                     responseTime: "00:00:00.006760",
                     successful: true
                   }
              },
      "duration": "00:00:00.595982",
      "result": "Passed"
   }
 }
```

Novità dalla versione

9.6

TestNetworkConfig

È possibile utilizzare `TestNetworkConfig` metodo per verificare che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate nel sistema.

Parametri

Quando si configura un nodo con il metodo SetNetworkConfig, nell'interfaccia utente o nell'interfaccia telefonica utente, la configurazione viene convalidata e memorizzata. Il test dell'API TestNetworkConfig utilizza la configurazione memorizzata per la logica post-convalida. Ad esempio, in caso di interruzione dell'alimentazione o di errore di rete, è possibile utilizzare questo metodo API per garantire che un nodo sia in esecuzione con la configurazione di rete attualmente memorizzata. In questo modo si conferma l'assenza di errori nella configurazione e l'utilizzo della configurazione corrente.

Questo test è progettato per mostrare solo gli errori nell'output della risposta. Se non ci sono errori, questo test non restituisce alcun output. Vedere gli esempi di risposta riportati di seguito.

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Contiene eventuali errori rilevati durante la convalida delle impostazioni di rete attualmente memorizzate con la configurazione di rete in esecuzione.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "TestNetworkConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta 1

Se non vengono rilevati errori, non viene restituita alcuna risposta.

```
{
   "id" : 1,
   "result": {
   "details": {
   "network": {...}
  },
   "duration": "00:00:00.144514",
   "result": "Passed"
  }
}
```

Esempio di risposta 2

Esempio di mancata corrispondenza MTU.

```
{
  "id" : 1,
  "result":
  {
     "details" :
     {
        "error":
        {
           "message" : "Network configuration mismatch on Bond10G:
Incorrect MTU expectedMTU=[1500]  actualMTU=[9600]", name:
"xAssertionFailure"
        }
     },
     "duration": "0.125213sec",
     "result": "Failed"
  }
}
```

Esempio di risposta 3

Esempio di percorso statico mancante.

```
{
  "id": 1,
  "result":
  {
     "details" :
     {
     "error":
        {
        "message" : "Network configuration mismatch on Bond1G: Routing
table missing route=[192.168.137.2 via 192.168.159.254 dev Bond1G]", name:
"xAssertionFailure"
        }
     },
     "duration" : "0.128547sec",
     "result" : "Failed"
  }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

SetNetworkConfig

Test Ping

È possibile utilizzare `TestPing` Metodo per testare la connettività di rete a tutti i nodi del cluster su interfacce 1G e 10G utilizzando pacchetti ICMP. Il test utilizza le dimensioni MTU appropriate per ciascun pacchetto in base alle impostazioni MTU nella configurazione di rete. `TestPing` Non crea un'interfaccia VLAN temporanea.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
tentativi	Specifica il numero di volte in cui il sistema deve ripetere il test ping.	intero	5	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
host	Specifica un elenco separato da virgole di indirizzi o nomi host delle periferiche da ping. Se non viene specificato alcun host, il metodo esegue il ping degli host nel cluster di storage.	stringa	Nessuno	No
interfaccia	L'interfaccia (base) esistente da cui devono essere inviati i ping. Valori possibili: • `Bond10G`: Consente di inviare ping dall'interfaccia Bond10G. • `Bond1G`: Consente di inviare ping dall'interfaccia Bond1G.	stringa	Nessuno	No
Dimensione pacchetto	Specifica il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore al valore MTU massimo specificato nella configurazione di rete.	intero	Nessuno	No
PingTimeoutMsec	Specifica il numero di millisecondi da attendere per ogni singola risposta ping.	intero	500 millisecondi	No
ProibitFragmentation	Attiva il flag DF (Do Not Fragment) per i pacchetti ICMP.	booleano	falso	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SourceIndirizzoV4	L'indirizzo IPv4 di origine da utilizzare nei pacchetti ping ICMP.	stringa	Nessuno	No
SourceIndirizzoV6	L'indirizzo IPv6 di origine da utilizzare nei pacchetti ping ICMP.	stringa	Nessuno	No
TotalTimeoutSec	Specifica il tempo in secondi in cui il ping deve attendere una risposta di sistema prima di eseguire il successivo tentativo di ping o terminare il processo.	intero	5	No
VirtualNetworkTag	L'ID VLAN da utilizzare per l'invio dei pacchetti ping.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Elenco di ciascun IP con cui il nodo è stato in grado di comunicare e statistiche di risposta ping.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "TestPing",
    "params": {
        "interface": "Bond1G",
        "hosts": "192.168.0.1"
    },
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:


```
{
  "id": 1,
  "result": {
    "details": {
      "192.168.0.1": {
        "individualResponseCodes": [
          "Success",
          "Success",
          "Success",
          "Success",
          "Success"
        ],
        "individualResponseTimes": [
          "00:00:00.000304",
          "00:00:00.000123",
          "00:00:00.000116",
          "00:00:00.000113",
          "00:00:00.000111"
        ],
        "individualStatus": [
          true,
          true,
          true,
          true,
          true
        ],
        "interface": "Bond1G",
        "responseTime": "00:00:00.000154",
        "sourceAddressV4": "192.168.0.5",
        "successful": true
      }
    },
    "duration": "00:00:00.001747",
    "result": "Passed"
  }
}
```


Novità dalla versione

5.0

TestRemoteConnectivity

È possibile utilizzare `TestRemoteConnectivity` metodo per eseguire il ping di ciascun nodo del cluster remoto e controllare la connessione del database dell'ensemble remoto. I cluster devono essere associati per ottenere risultati utili con questo metodo. Se la connessione al database remoto non riesce, la risposta del sistema elenca le eccezioni.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
dettagli	Tempi di risposta ping singoli per ciascun nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "TestRemoteConnectivity",
    "params": {
      "force": "true"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": null,
  "result": {
    "details": {
      "1": {
        "details": {
          "10.26.86.17": {
            "individualResponseTimes": [
              "00:00:00.006868",
              "00:00:00.005933",
              "00:00:00.006655",
```

```
            "00:00:00.006584",
            "00:00:00.006334"
          ],
          "individualStatus": [
            "true",
            "true",
            "true",
            "true",
            "true"
          ],
          "responseTime": "00:00:00.006475",
          "successful": true
        },
        "10.26.86.18": {
          "individualResponseTimes": [
            "00:00:00.006201",
            "00:00:00.006187",
            "00:00:00.005990",
            "00:00:00.006029",
            "00:00:00.005917"
          ],
          "individualStatus": [
            "true",
            "true",
            "true",
            "true",
            "true"
          ],
          "responseTime": "00:00:00.006065",
          "successful": true
        },
        "10.26.86.19": {
          "individualResponseTimes": [
            "00:00:00.005988",
            "00:00:00.006948",
            "00:00:00.005981",
            "00:00:00.005964",
            "00:00:00.005942"
          ],
          "individualStatus": [
            "true",
            "true",
            "true",
            "true",
            "true"
          ],
```

```
            "responseTime": "00:00:00.006165",
            "successful": true,
          },
          "10.26.86.20": {
            "individualResponseTimes": [
              "00:00:00.005926",
              "00:00:00.006072",
              "00:00:00.005675",
              "00:00:00.009904",
              "00:00:00.006225"
            ],
            "individualStatus": [
              "true",
              "true",
              "true",
              "true",
              "true"
            ],
            "responseTime": "00:00:00.006760",
            "successful": true
          }
        },
          "successful": true
      }
    },
  "duration": "00:00:00.595982",
  "result": "Passed"
  }
}
```


Novità dalla versione

9.6

Metodi API di replica

I metodi API di replica consentono di collegare due cluster per la protezione continua dei dati (CDP). Quando si collegano due cluster, i volumi attivi all'interno di un cluster possono essere replicati in modo continuo in un secondo cluster per fornire il ripristino dei dati. Associando i volumi per la replica, è possibile proteggere i dati da eventi che potrebbero renderli inaccessibili.

- Ordine delle operazioni di abbinamento dei cluster
- Ordine delle operazioni di abbinamento dei volumi
- Modalità di replica supportate per i cluster accoppiati

- CompleteClusterPairing
- CompleteVolumePairing
- ListClusterPairs
- ListActivePairedVolumes
- ModifyVolumePair
- RemoveClusterPair
- RemoveVolumePair
- StartClusterPairing
- StartVolumePairing

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Ordine delle operazioni di abbinamento dei cluster

È necessario stabilire una connessione tra una coppia di cluster di storage che eseguono il software Element prima di poter utilizzare la replica remota.

Utilizzare il seguente set di metodi API per stabilire una connessione cluster:

- StartClusterPairing:

  Questo metodo API crea e restituisce una chiave di accoppiamento utilizzata per stabilire una coppia di cluster. La chiave è codificata e contiene informazioni utilizzate per stabilire le comunicazioni tra i cluster. Un singolo cluster può essere associato a un massimo di quattro altri cluster. Tuttavia, è necessario generare una nuova chiave per ogni accoppiamento del cluster. Il StartClusterPairing method genera una nuova chiave ogni volta che viene chiamato il metodo. Utilizzare ciascuna chiave univoca con CompleteClusterPairing metodo per associare ciascun cluster aggiuntivo.

  > Per motivi di sicurezza, la chiave di accoppiamento non deve essere inviata ad altri utenti via email. La chiave contiene un nome utente e una password.

- CompleteClusterPairing:

  Questo metodo utilizza la chiave di accoppiamento creata con StartClusterPairing Metodo API per creare una coppia di cluster. Eseguire il CompleteClusterPairing Metodo API con il parametro clusterPairingKey per la destinazione. Il cluster di origine è il cluster che ha creato la chiave.

Trova ulteriori informazioni

- StartClusterPairing
- CompleteClusterPairing

Ordine delle operazioni di abbinamento dei volumi

È necessario creare una coppia di cluster tra due cluster corrispondenti prima di poter associare i volumi.

Utilizzare il seguente set di metodi API per stabilire una connessione cluster:

- StartVolumePairing:

  Questo metodo API crea e restituisce una chiave di accoppiamento del volume utilizzata per creare una coppia di volumi. La chiave contiene informazioni utilizzate per stabilire le comunicazioni tra i volumi.

- CompleteVolumePairing:

  Questo metodo utilizza la chiave di accoppiamento creata con StartVolumePairing Metodo API per creare una coppia di volumi. Eseguire il CompleteVolumePairing Metodo API con i parametri volumeID e volumePairingKey per il volume di destinazione.

Solo uno dei volumi accoppiati può essere identificato come volume di destinazione della replica. Utilizzare ModifyVolumePair Metodo API per stabilire la direzione della replica dei dati del volume identificando il volume di destinazione. I dati vengono replicati dal volume di origine al volume di destinazione.

Trova ulteriori informazioni

- StartVolumePairing
- CompleteVolumePairing
- ModifyVolumePair

Modalità di replica supportate per i cluster accoppiati

I cluster accoppiati supportano le seguenti modalità di replica:

- Replica asincrona dei dati: I dati inviati al volume di destinazione della replica vengono inviati in modo asincrono. Il sistema non attende l'invio di una conferma prima di scrivere i dati.
- Replica sincrona dei dati: I dati inviati al volume di destinazione della replica vengono inviati in modo sincrono. Quando le operazioni di i/o inviate dall'host vengono riconosciute dal sistema, la conferma di sistema viene inviata all'host e i dati vengono inviati al volume di destinazione della replica.
- Replica dei dati solo snapshot: Solo le snapshot dei volumi vengono replicate nel cluster di destinazione.

CompleteClusterPairing

Il `CompleteClusterPairing` il metodo è la seconda fase del processo di accoppiamento del cluster. Utilizzare questo metodo con la chiave codificata ricevuta da `StartClusterPairing` metodo per completare il processo di abbinamento del cluster.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ClusterPairingKey	Stringa di caratteri restituita da StartClusterPairing Metodo API.	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ID PairID del clusterPairID	Identificatore univoco della coppia di cluster.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CompleteClusterPairing",
   "params": {
        "clusterPairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393533643263
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f5465737432 2d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
       "clusterPairID" : 1
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

StartClusterPairing

CompleteVolumePairing

È possibile utilizzare `CompleteVolumePairing` per completare l'associazione di due volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	L'ID del volume che completerà la coppia di volumi.	intero	Nessuno	Sì
VolumePairingKey	La chiave restituita da StartVolumePairing Metodo API.	stringa	Nessuno	Sì

Valore restituito

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CompleteVolumePairing",
   "params": {
        "volumeID" : 12,
        "volumePairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393533643263
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
        },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
"id": 1,
"result": {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

StartVolumePairing

ListClusterPairs

È possibile utilizzare `ListClusterPairs` metodo per elencare tutti i cluster associati al cluster corrente. Questo metodo restituisce informazioni sugli abbinamenti dei cluster attivi e in sospeso, come le statistiche sull'accoppiamento corrente, nonché la connettività e la latenza (in millisecondi) dell'accoppiamento dei cluster.

Parametro

Questo metodo non ha alcun parametro di input:

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ClusterPairs	Informazioni su ciascun cluster associato.	ClusterPair array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListClusterPairs",
   "params": {
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
 "id": 1,
 "result": {
   "clusterPairs": [
     {
      "clusterName": "cluster2",
      "clusterPairID": 3,
      "clusterPairUUID": "9866fbeb-c2f8-4df3-beb9-58a5c4e49c9b",
      "clusterUUID": 5487,
      "latency": 1,
      "mvip": "172.1.1.5",
      "status": "Connected"
      "version": "8.0.0.1361"
     },
     {
      "clusterName": "cluster3",
      "clusterPairID": 2,
      "clusterPairUUID": "8132a699-ce82-41e0-b406-fb914f976042",
      "clusterUUID": 1383,
      "latency": 1,
      "mvip": "172.1.1.6",
      "status": "Connected"
      "version": "8.0.0.1361"
     }
   ]
 }
```


Novità dalla versione

9.6

ListActivePairedVolumes

È possibile utilizzare `ListActivePairedVolumes` metodo per elencare tutti i volumi attivi associati a un volume. Questo metodo restituisce informazioni sui volumi con abbinamenti attivi e in sospeso.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
volumi	Informazioni sul volume per i volumi associati.	VolumePair array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListActivePairedVolumes",
   "params": {
      },
   "id" : 1
}
```

Esempio di risposta

Le risposte per questo metodo sono simili al seguente esempio:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-06-24T15:21:59Z",
                "deleteTime": "",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:0oto.bk.24",
                "name": "BK",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
```

```
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000018f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000018",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 10737418240,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 24,
                "volumePairs": [
                    {
                        "clusterPairID": 2,
                        "remoteReplication": {
                            "mode": "Async",
                            "pauseLimit": 3145728000,
                            "remoteServiceID": 14,
                            "resumeDetails": "",
                            "snapshotReplication": {
                                "state": "Idle",
                                "stateDetails": ""
                            },
                            "state": "Active",
                            "stateDetails": ""
                        },
                        "remoteSliceID": 8,
                        "remoteVolumeID": 8,
                        "remoteVolumeName": "PairingDoc",
                        "volumePairUUID": "229fcbf3-2d35-4625-865a-
d04bb9455cef"
                    }
                ]
            }
        ]
    }
}
```


Novità dalla versione

9.6

ModifyVolumePair

È possibile utilizzare `ModifyVolumePair` metodo per sospendere o riavviare la replica tra una coppia di volumi. Questo metodo viene impostato sul volume di origine (il volume con accesso in lettura/scrittura).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Numero di identificazione del volume da modificare.	intero	Nessuno	Sì
PausedManual (PausedManual)	La replica remota può essere messa in pausa o riavviata sul volume di origine (lettura/scrittura). Valori possibili: • Vero: Sospendere la replica del volume. • Falso: Riavviare la replica del volume. Se non viene specificato alcun valore, non viene eseguita alcuna modifica nella replica.	booleano	Nessuno	No

modalità	Modalità di replica del volume. Valori possibili: • Async: Le scritture vengono riconosciute quando vengono completate localmente. Il cluster non attende la replica delle scritture nel cluster di destinazione. • Sync: L'origine riconosce la scrittura quando i dati vengono memorizzati localmente e sul cluster remoto. • SnapshotsOnly (solo snapshot): Vengono replicati solo gli snapshot creati nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.	stringa	Nessuno	No

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyVolumePair",
  "params": {
    "pausedManual": false,
    "volumeID": 5,
    "mode": "sync"
   },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {}
}
```

Novità dalla versione

9.6

RemoveClusterPair

È possibile utilizzare `RemoveClusterPair` metodo per chiudere le connessioni aperte tra due cluster accoppiati.

Parametro

> Prima di rimuovere una coppia di cluster, è necessario rimuovere tutte le associazioni di volumi ai cluster con il metodo API RemoveVolumePair.

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID PairID del clusterPairID	Identificatore univoco utilizzato per associare due cluster.	intero	Nessuno	Sì

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveClusterPair",
   "params": {
              "clusterPairID": 1
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {}
}
```

Novità dalla versione

9.6

RemoveVolumePair

È possibile utilizzare `RemoveVolumePair` metodo per rimuovere l'associazione remota tra due volumi. Utilizzare questo metodo sui volumi di origine e di destinazione associati. Quando si rimuovono le informazioni di accoppiamento del volume, i dati non vengono più replicati nel o dal volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	ID del volume su cui interrompere il processo di replica.	intero	Nessuno	Sì

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveVolumePair",
   "params": {
      "volumeID": 5
   "id" : 1
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
   }
}
```

Novità dalla versione

9.6

StartClusterPairing

È possibile utilizzare `StartClusterPairing` metodo per creare una chiave codificata da un cluster utilizzato per l'associazione con un altro cluster. La chiave creata da questo metodo API viene utilizzata in `CompleteClusterPairing` metodo per stabilire un'associazione di cluster. È possibile associare un cluster a un massimo di quattro altri cluster.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ClusterPairingKey	Stringa di caratteri utilizzata da CompleteClusterPairing Metodo API.	stringa

Nome	Descrizione	Tipo
ID PairID del clusterPairID	Identificatore univoco della coppia di cluster.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "StartClusterPairing",
   "params": {
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "clusterPairID": 1,
     "clusterPairingKey":
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d373435363661393536432
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a393133313432363439 2c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

CompleteClusterPairing

StartVolumePairing

È possibile utilizzare `StartVolumePairing` metodo per creare una chiave codificata da

un volume utilizzato per l'associazione con un altro volume. La chiave creata da questo metodo viene utilizzata in `CompleteVolumePairing` metodo per stabilire un'associazione di volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
modalità	La modalità del volume su cui avviare il processo di associazione. La modalità può essere impostata solo se il volume è il volume di origine. Valori possibili: • `Async`: Le scritture vengono riconosciute quando vengono completate localmente. Il cluster non attende la replica delle scritture nel cluster di destinazione. (Impostazione predefinita se non è stato specificato alcun parametro di modalità). • `Sync`: L'origine riconosce la scrittura quando i dati vengono memorizzati localmente e nel cluster remoto. • `SnapshotsOnly`: Vengono replicati solo gli snapshot creati nel cluster di origine. Le scritture attive dal volume di origine non vengono replicate.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	L'ID del volume su cui avviare il processo di associazione.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumePairingKey	Stringa di caratteri utilizzata da CompleteVolumePairing Metodo API.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "StartVolumePairing",
   "params": {
         "mode": "Async",
     "volumeID" : 14
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "volumePairingKey" :
"7b226d766970223a223139322e3136382e3133392e313232222c22766f6c756d654944223
a312c22766f6c756d654e616d65223a2254657374222c22766f6c756d65506169725555494
4223a2236393632346663622d323032652d343332352d613536392d656339633635356337 6
23561227d"
      }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

CompleteVolumePairing

Metodi API di sicurezza

È possibile integrare il software Element con servizi esterni correlati alla sicurezza, ad esempio un server di gestione delle chiavi esterno. Questi metodi relativi alla sicurezza consentono di configurare le funzionalità di sicurezza degli elementi, ad esempio la gestione delle chiavi esterne per la crittografia a riposo.

- AddKeyServerToProviderKmip
- CreateKeyProviderKmip
- CreateKeyServerKmip
- CreatePublicPrivateKeyPair
- DeleteKeyProviderKmip
- DeleteKeyServerKmip
- DisableEncryptionAtRest
- EnableEncryptionAtRest
- GetClientCertificateSignRequest
- GetKeyProviderKmip
- GetKeyServerKmip
- ListKeyProvidersKmip
- ListKeyServerKmip
- ModifyKeyServerKmip
- RemoveKeyServerFromProviderKmip
- TestKeyProviderKmip
- TestKeyServerKmip

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddKeyServerToProviderKmip

È possibile utilizzare `AddKeyServerToProviderKmip` Metodo per assegnare un server di chiavi KMIP (Key Management Interoperability Protocol) al provider di chiavi specificato. Durante l'assegnazione, il server viene contattato per verificarne la funzionalità. Se il server chiavi specificato è già assegnato al provider di chiavi

specificato, non viene eseguita alcuna azione e non viene restituito alcun errore. È possibile rimuovere l'assegnazione utilizzando `RemoveKeyServerFromProviderKmip` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID del provider di chiavi a cui assegnare il server di chiavi.	intero	Nessuno	Sì
KeyServerID	L'ID del server chiavi da assegnare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha alcun valore restituito. L'assegnazione viene considerata riuscita a condizione che non venga restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "AddKeyServerToProviderKmip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
    },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Novità dalla versione

11.7

CreateKeyProviderKmip

È possibile utilizzare `CreateKeyProviderKmip` Metodo per creare un provider di chiavi KMIP (Key Management Interoperability Protocol) con il nome specificato. Un provider di chiavi definisce un meccanismo e una posizione per recuperare le chiavi di autenticazione. Quando si crea un nuovo provider di chiavi KMIP, non sono assegnati server di chiavi KMIP. Per creare un server chiavi KMIP, utilizzare `CreateKeyServerKmip` metodo. Per assegnarlo a un provider, vedere `AddKeyServerToProviderKmip`.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderName	Il nome da associare al provider di chiavi KMIP creato. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProvider	Oggetto contenente dettagli sul provider di chiavi appena creato.	"KeyProviderKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "CreateKeyProviderKmip",
  "params": {
    "keyProviderName": "ProviderName",
    },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
    "kmipKeyProvider": {
        "keyProviderName": "ProviderName",
        "keyProviderIsActive": true,
        "kmipCapabilities": "SSL",
        "keyServerIDs": [
            15
        ],
        "keyProviderID": 1
    }
}
}
```

Novità dalla versione

11.7

CreateKeyServerKmip

È possibile utilizzare `CreateKeyServerKmip` Metodo per creare un server di chiavi KMIP (Key Management Interoperability Protocol) con gli attributi specificati. Durante la creazione, il server non viene contattato; non è necessario che esista prima di utilizzare questo metodo. Per le configurazioni dei server delle chiavi in cluster, è necessario fornire i nomi host o gli indirizzi IP di tutti i nodi del server nel parametro kmipKeyServerHostnames. È possibile utilizzare `TestKeyServerKmip` metodo per testare un server di chiavi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipCaCertificate	Il certificato a chiave pubblica della CA principale del server di chiavi esterno. Questa opzione viene utilizzata per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server di chiavi in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati root di tutte le CA.	stringa	Nessuno	Sì
KmipClientCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM utilizzato dal client KMIP di SolidFire.	stringa	Nessuno	Sì
KmipKeyServerHostnames	Array dei nomi host o degli indirizzi IP associati al server delle chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server delle chiavi sono in una configurazione in cluster.	array di stringhe	Nessuno	Sì
KmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipKeyServerPort	Il numero di porta associato al server delle chiavi KMIP (generalmente 5696).	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server chiavi appena creato.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "CreateKeyServerKmip",
  "params": {
    "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
     }
}
```

Novità dalla versione

11.7

CreatePublicPrivateKeyPair

È possibile utilizzare `CreatePublicPrivateKeyPair` Metodo per creare chiavi SSL pubbliche e private. È possibile utilizzare queste chiavi per generare richieste di firma del certificato. Per ogni cluster di storage può essere utilizzata una sola coppia di chiavi. Prima di utilizzare questo metodo per sostituire le chiavi esistenti, assicurarsi che le chiavi non siano più utilizzate da alcun provider.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Nome comune	Il campo Nome distinto X.509 **Nome comune** (CN).	stringa	Nessuno	No
paese	Il campo Nome distinto X.509 **Paese** ©.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
EmailAddress	Il campo Nome distinto X.509 **Indirizzo e-mail** (E-MAIL).	stringa	Nessuno	No
località	Il campo Nome distinto X.509 **Nome località** (L).	stringa	Nessuno	No
organizzazione	Il campo Nome distinto X.509 **Nome organizzazione** (o).	stringa	Nessuno	No
OrganisationalUnit	Il campo Nome distinto X.509 **Nome unità organizzativa** (OU).	stringa	Nessuno	No
stato	Il campo Nome distinto X.509 **Stato** o **Nome provincia** (ST o SP o S).	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti. Se non si verificano errori, la creazione della chiave viene considerata corretta.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
   },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
}
```

Novità dalla versione

11.7

DeleteKeyProviderKmip

È possibile utilizzare `DeleteKeyProviderKmip` Metodo per eliminare il provider di chiavi KMIP (Key Management Interoperability Protocol) inattivo specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID del provider di chiavi da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. L'operazione di eliminazione viene considerata riuscita finché non si verifica alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
    },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
}
```

Novità dalla versione

11.7

DeleteKeyServerKmip

È possibile utilizzare `DeleteKeyServerKmip` Metodo per eliminare un server di chiavi KMIP (Key Management Interoperability Protocol) esistente. È possibile eliminare un server chiavi a meno che non sia l'ultimo assegnato al proprio provider e il provider non stia fornendo chiavi attualmente in uso.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. L'operazione di eliminazione viene considerata corretta se non si verificano errori.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
}
```

Novità dalla versione

11.7

DisableEncryptionAtRest

È possibile utilizzare `DisableEncryptionAtRest` metodo per rimuovere la crittografia precedentemente applicata al cluster utilizzando `EnableEncryptionAtRest` metodo. Questo metodo di disattivazione è asincrono e restituisce una risposta prima che la crittografia venga disattivata. È possibile utilizzare `GetClusterInfo` metodo per eseguire il polling del sistema per verificare il completamento del processo.

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare "ottieni il metodo delle informazioni sul cluster". È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi".

Non è possibile utilizzare questo metodo per disattivare la crittografia software a riposo. Per disattivare la crittografia software a riposo, è necessario "creare un nuovo cluster" con crittografia software a riposo disattivata.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DisableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- "GetClusterInfo"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

EnableEncryptionAtRest

È possibile utilizzare `EnableEncryptionAtRest` Metodo per attivare la crittografia AES (Advanced Encryption Standard) a 256 bit sul cluster in modo che il cluster possa gestire la chiave di crittografia utilizzata per i dischi su ciascun nodo. Questa funzione non è attivata per impostazione predefinita.

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo nel cluster, utilizzare "ottieni il metodo delle informazioni sul cluster". È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` "metodo per ottenere informazioni utilizzate dal cluster per crittografare i dati inattivi".

Questo metodo non attiva la crittografia software a riposo. Questa operazione può essere eseguita solo utilizzando "creare il metodo del cluster" con `enableSoftwareEncryptionAtRest` impostare su `true`.

Quando si attiva la crittografia a riposo, il cluster gestisce automaticamente le chiavi di crittografia interne per i dischi su ciascun nodo del cluster.

Se viene specificato keyProviderID, la password viene generata e recuperata in base al tipo di provider di chiavi. In genere, questa operazione viene eseguita utilizzando un server di chiavi KMIP (Key Management Interoperability Protocol) nel caso di un provider di chiavi KMIP. Dopo questa operazione, il provider specificato viene considerato attivo e non può essere eliminato fino a quando la crittografia a riposo non viene disattivata tramite `DisableEncryptionAtRest` metodo.

Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", la `EnableEncryptionAtRest` La chiamata al metodo non riesce e viene visualizzato il messaggio "crittografia non consentita. Il cluster ha rilevato un nodo non crittografabile".

Attivare o disattivare la crittografia solo quando il cluster è in esecuzione e in stato di integrità. È possibile attivare o disattivare la crittografia a propria discrezione e con la frequenza richiesta.

Questo processo è asincrono e restituisce una risposta prima dell'attivazione della crittografia. È possibile utilizzare `GetClusterInfo` metodo per eseguire il polling del sistema per verificare il completamento del processo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID di un provider di chiavi KMIP da utilizzare.	intero	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "EnableEncryptionAtRest",
   "params": {},
   "id": 1
}
```

Esempi di risposte

Questo metodo restituisce una risposta simile all'esempio seguente dal metodo EnableEncryptionAtRest. Nessun risultato da segnalare.

```
{
   "id": 1,
   "result": {}
}
```

Durante l'attivazione della crittografia a riposo su un cluster, GetClusterInfo restituisce un risultato che descrive lo stato di crittografia a riposo ("EncryptionAtRestState") come "abilitazione". Una volta attivata la crittografia a riposo, lo stato restituito diventa "Enabled" (attivato).

```
{
   "id": 1,
      "result": {
         "clusterInfo": {
            "attributes": { },
               "encryptionAtRestState": "enabling",
            "ensemble": [
               "10.10.5.94",
               "10.10.5.107",
               "10.10.5.108"
            ],
            "mvip": "192.168.138.209",
            "mvipNodeID": 1,
            "name": "Marshall",
            "repCount": 2,
            "svip": "10.10.7.209",
            "svipNodeID": 1,
            "uniqueID": "91dt"
      }
   }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

- "SecureEraseDrive"
- "GetClusterInfo"
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetClientCertificateSignRequest

È possibile utilizzare `GetClientCertificateSignRequest` metodo per generare una richiesta di firma del certificato che può essere firmata da un'autorità di certificazione per generare un certificato client per il cluster. I certificati firmati sono necessari per stabilire una relazione di trust per l'interazione con i servizi esterni.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ClientCertificateSignRequest	Una richiesta di firma del certificato client X.509 con codifica PKCS n. 10 in formato PEM Base64.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "clientCertificateSignRequest":
"MIIByjCCATMCAQAwgYkxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
   }
}
```

Novità dalla versione

11.7

GetKeyProviderKmip

È possibile utilizzare `GetKeyProviderKmip` Metodo per recuperare informazioni sul provider di chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID dell'oggetto provider della chiave KMIP da restituire.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProvider	Oggetto contenente dettagli sul provider di chiavi richiesto.	"KeyProviderKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetKeyProviderKmip",
  "params": {
    "keyProviderID": 15
    },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProvider": {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
            1
        ],
        "keyProviderName": "ProviderName"
    }
   }
}
```

Novità dalla versione

11.7

GetKeyServerKmip

È possibile utilizzare `GetKeyServerKmip` Metodo per restituire informazioni sul server di chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP su cui restituire le informazioni.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server delle chiavi richiesto.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetKeyServerKmip",
  "params": {
     "keyServerID": 15
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":15
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
    }
}
```

Novità dalla versione

11.7

GetSoftwareEncryptionAtRestInfo

È possibile utilizzare `GetSoftwareEncryptionAtRestInfo` metodo per ottenere informazioni sulla crittografia software a riposo utilizzate dal cluster per crittografare i dati a riposo.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Parametro	Descrizione	Tipo	Opzionale
MasterKeyInfo	Informazioni sulla chiave master di crittografia a riposo software corrente.	EncryptionKeyInfo	Vero
RekeyMasterKeyAsyncResultID	L'ID risultato asincrono dell'operazione di rekey corrente o più recente (se presente), se non ancora eliminata. `GetAsyncResult` l'output includerà un `newKey` campo contenente informazioni sulla nuova chiave master e su `keyToDecommission` campo che contiene informazioni sulla vecchia chiave.	intero	Vero
stato	Lo stato corrente di crittografia software a riposo. I valori possibili sono `disabled` oppure `enabled`.	stringa	Falso
versione	Numero di versione incrementato ogni volta che viene attivata la crittografia software a riposo.	intero	Falso

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
 "method": "getsoftwareencryptionatrestinfo"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "masterKeyInfo": {
            "keyCreatedTime": "2021-09-20T23:15:56Z",
            "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
            "keyManagementType": "internal"
        },
        "state": "enabled",
        "version": 1
    }
}
```


Novità dalla versione

12.3

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

ListKeyProvidersKmip

È possibile utilizzare `ListKeyProvidersKmip` Metodo per recuperare un elenco di tutti i provider di chiavi KMIP (Key Management Interoperability Protocol) esistenti. È possibile filtrare l'elenco specificando parametri aggiuntivi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderIsActive	I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili: • Vero: Restituisce solo i provider di chiavi KMIP attivi (fornendo le chiavi attualmente in uso). • Falso: Restituisce solo i provider di chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati). Se omessi, i provider di chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipKeyProviderHasServerAssigned	I filtri hanno restituito i provider di chiavi KMIP in base all'assegnazione o meno di un server di chiavi KMIP. Valori possibili: • Vero: Restituisce solo i provider di chiavi KMIP a cui è stato assegnato un server di chiavi KMIP. • Falso: Restituisce solo i provider di chiavi KMIP che non hanno un server di chiavi KMIP assegnato. Se omessi, i provider di chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un server di chiavi KMIP.	booleano	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyProviders	Elenco dei provider di chiavi KMIP creati.	"KeyProviderKmip" array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
    {
    "kmipKeyProviders": [
        {
            "keyProviderID": 15,
            "kmipCapabilities": "SSL",
            "keyProviderIsActive": true,
            "keyServerIDs": [
                1
            ],
            "keyProviderName": "KeyProvider1"
        }
    ]
}
}
```

Novità dalla versione

11.7

ListKeyServerKmip

È possibile utilizzare `ListKeyServersKmip` Metodo per elencare tutti i server chiave KMIP (Key Management Interoperability Protocol) creati. È possibile filtrare i risultati specificando parametri aggiuntivi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	Quando specificato, il metodo restituisce solo i server delle chiavi KMIP assegnati al provider di chiavi KMIP specificato. Se omessi, i server delle chiavi KMIP restituiti non verranno filtrati in base all'assegnazione o meno al provider di chiavi KMIP specificato.	intero	Nessuno	No
KmipAssignedProviderIsActive	I filtri hanno restituito oggetti KMIP Key Server in base all'attivazione o meno. Valori possibili: • Vero: Restituisce solo i server delle chiavi KMIP attivi (fornendo le chiavi attualmente in uso). • Falso: Restituisce solo i server delle chiavi KMIP inattivi (non fornendo alcuna chiave e che possono essere cancellati). Se omessi, i server delle chiavi KMIP restituiti non vengono filtrati in base alla loro attivazione o meno.	booleano	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KmipHasProviderAssigned	I filtri hanno restituito i server delle chiavi KMIP in base all'assegnazione o meno di un provider di chiavi KMIP. Valori possibili: • Vero: Restituisce solo i server delle chiavi KMIP a cui è stato assegnato un provider di chiavi KMIP. • Falso: Restituisce solo i server di chiavi KMIP che non hanno un provider di chiavi KMIP assegnato. Se omessi, i server delle chiavi KMIP restituiti non vengono filtrati in base all'assegnazione o meno di un provider di chiavi KMIP.	booleano	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServers	L'elenco completo dei server delle chiavi KMIP creati.	"KeyServerKmip" array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListKeyServersKmip",
  "params": {},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "kmipKeyServers": [
        {
            "kmipKeyServerName": "keyserverName",
            "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
            "keyServerID": 15,
            "kmipAssignedProviderIsActive": true,
            "kmipKeyServerPort": 5696,
            "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames": [
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID": 1
        }
    ]
}
```

Novità dalla versione

11.7

ModifyKeyServerKmip

È possibile utilizzare `ModifyKeyServerKmip` Metodo per modificare un server chiavi KMIP (Key Management Interoperability Protocol) esistente con gli attributi specificati. Sebbene l'unico parametro richiesto sia keyServerID, una richiesta contenente solo keyServerID non eseguirà alcuna azione e non restituirà alcun errore. Qualsiasi altro parametro specificato sostituirà i valori esistenti per il server chiavi con il keyServerID specificato. Il server delle chiavi viene contattato durante l'operazione per assicurarne il funzionamento. È possibile fornire più nomi host o indirizzi IP con il parametro kmipKeyServerHostnames, ma solo se i server delle chiavi sono in una configurazione in cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del KMIP Key Server da modificare.	intero	Nessuno	Sì
KmipCaCertificate	Il certificato a chiave pubblica della CA principale del server di chiavi esterno. Questa opzione viene utilizzata per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server di chiavi in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati root di tutte le CA.	stringa	Nessuno	No
KmipClientCertificate	Un certificato PKCS 10 X.509 con codifica Base64 in formato PEM utilizzato dal client KMIP di SolidFire.	stringa	Nessuno	No
KmipKeyServerHostnames	Array dei nomi host o degli indirizzi IP associati al server delle chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server delle chiavi sono in una configurazione in cluster.	array di stringhe	Nessuno	No

KmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo per scopi di visualizzazione e non deve essere univoco.	stringa	Nessuno	No
KmipKeyServerPort	Il numero di porta associato al server delle chiavi KMIP (generalmente 5696).	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
KmipKeyServer	Oggetto contenente dettagli sul server delle chiavi appena modificato.	"KeyServerKmip"

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyKeyServerKmip",
  "params": {
    "keyServerID": 15
    "kmipCaCertificate": "CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
    "kmipClientCertificate": "kirWmnWXbj9T/UWZYB2oK0z5...",
    "kmipKeyServerHostnames" : ["server1.hostname.com",
"server2.hostname.com"],
    "kmipKeyServerName" : "keyserverName",
    "kmipKeyServerPort" : 5696
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "kmipKeyServer": {
            "kmipCaCertificate":"CPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
            "kmipKeyServerHostnames":[
                "server1.hostname.com", "server2.hostname.com"
            ],
            "keyProviderID":1,
            "kmipKeyServerName":"keyserverName",
            "keyServerID":1
            "kmipKeyServerPort":1,
            "kmipClientCertificate":"kirWmnWXbj9T/UWZYB2oK0z5...",
            "kmipAssignedProviderIsActive":true
        }
     }
}
```


Novità dalla versione

11.7

RekeySoftwareEncryptionAtRestMasterKey

È possibile utilizzare `RekeySoftwareEncryptionAtRestMasterKey` Metodo per reimmettere la chiave master di crittografia a riposo del software utilizzata per crittografare le chiavi di crittografia dei dati (DEK). Durante la creazione del cluster, la crittografia software a riposo viene configurata per l'utilizzo di IKM (Internal Key Management). Questo metodo di rekey può essere utilizzato dopo la creazione del cluster per utilizzare IKM o External Key Management (EKM).

Parametri

Questo metodo ha i seguenti parametri di input. Se il `keyManagementType` parametro non specificato, l'operazione di rekey viene eseguita utilizzando la configurazione di gestione delle chiavi esistente. Se il `keyManagementType` è specificato e il provider di chiavi è esterno, il `keyProviderID` deve essere utilizzato anche il parametro.

Parametro	Descrizione	Tipo	Opzionale
KeyManagementType	Il tipo di gestione delle chiavi utilizzato per gestire la chiave master. I valori possibili sono: `Internal`: Eseguire la riskey utilizzando la gestione interna delle chiavi. `External`: Eseguire la riskey utilizzando la gestione esterna delle chiavi. Se questo parametro non viene specificato, l'operazione di rekey viene eseguita utilizzando la configurazione di gestione delle chiavi esistente.	stringa	Vero
KeyProviderID	L'ID del provider di chiavi da utilizzare. Si tratta di un valore univoco restituito come parte di uno dei `CreateKeyProvider` metodi. L'ID è richiesto solo quando `keyManagementType` è `External` e non è altrimenti valido.	intero	Vero

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Parametro	Descrizione	Tipo	Opzionale
AsyncHandle	Determinare lo stato dell'operazione di rekey utilizzando questo comando `asyncHandle` valore con `GetAsyncResult`. `GetAsyncResult` l'output includerà un `newKey` campo contenente informazioni sulla nuova chiave master e su `keyToDecommission` campo che contiene informazioni sulla vecchia chiave.	intero	Falso

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
 "method": "rekeysoftwareencryptionatrestmasterkey",
 "params": {
   "keyManagementType": "external",
   "keyProviderID": "<ID number>"
 }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "asyncHandle": 1
}
```

Novità dalla versione

12.3

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

RemoveKeyServerFromProviderKmip

È possibile utilizzare `RemoveKeyServerFromProviderKmip` Metodo per annullare l'assegnazione del server delle chiavi KMIP (Key Management Interoperability Protocol) specificato dal provider a cui è stato assegnato. È possibile annullare l'assegnazione di un server chiavi dal proprio provider, a meno che non sia l'ultimo e il relativo provider sia attivo (fornendo le chiavi attualmente in uso). Se il server chiavi specificato non è assegnato a un provider, non viene eseguita alcuna azione e non viene restituito alcun errore.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da annullare l'assegnazione.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. La rimozione viene considerata riuscita a condizione che non venga restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
   },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Novità dalla versione

11.7

TestKeyProviderKmip

È possibile utilizzare `TestKeyProviderKmip` Metodo per verificare se il provider di chiavi KMIP (Key Management Interoperability Protocol) specificato è raggiungibile e funziona normalmente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyProviderID	L'ID del provider di chiavi da testare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. Il test viene considerato riuscito finché non viene restituito alcun errore.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "TestKeyProviderKmip",
  "params": {
    "keyProviderID": 15
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
    }
}
```

Novità dalla versione

11.7

TestKeyServerKmip

È possibile utilizzare `TestKeyServerKmip` Metodo per verificare se il server delle chiavi KMIP (Key Management Interoperability Protocol) specificato è raggiungibile e funziona normalmente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
KeyServerID	L'ID del server chiavi KMIP da testare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti. Se non vengono restituiti errori, il test viene considerato di successo.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "TestKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {}
    }
```

Novità dalla versione

11.7

Metodi API di SnapMirror

I metodi API di SnapMirror vengono utilizzati dall'interfaccia utente Web Element per la gestione delle snapshot mirrorate con sistemi ONTAP remoti. Questi metodi sono destinati all'utilizzo solo da parte dell'interfaccia utente web Element. Se si desidera accedere alle funzionalità di SnapMirror tramite API, utilizzare le API di ONTAP. Non vengono forniti esempi di richiesta e restituzione per i metodi API di SnapMirror.

- AbortSnapMirrorRelationship
- BreakSnapMirrorRelationship
- BreakSnapMirrorVolume
- CreateSnapMirrorEndpoint
- CreateSnapMirrorEndpointUnmanaged
- CreateSnapMirrorRelationship
- CreateSnapMirrorVolume
- DeleteSnapMirrorEndpoint
- DeleteSnapMirrorRelationships
- GetOntapVersionInfo
- GetSnapMirrorClusterIdentity
- InitializeSnapMirrorRelationship
- ListSnapMirrorAggregates
- ListSnapMirrorEndpoint
- ListSnapMirrorLun
- ListSnapMirrorNetworkInterfaces
- ListSnapMirrorNode
- ListSnapMirrorPolicies
- ListSnapMirrorSchedules
- ListSnapMirrorRelationships
- ListSnapMirrorVolumes
- ListSnapMirrorVservers
- ModifySnapMirrorEndpoint
- ModifySnapMirrorEndpoint (non gestito)
- ModifySnapMirrorRelationship
- UpdateSnapMirrorRelationship
- QuiesceSnapMirrorRelationship
- ResumeSnapMirrorRelationship
- ResyncSnapMirrorRelationship

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AbortSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `AbortSnapMirrorRelationship` Metodo per arrestare i trasferimenti SnapMirror avviati ma non ancora completati.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeInfo	Nessuno	Sì
Clear Checkpoint	Determina se cancellare o meno il checkpoint di riavvio. Valori possibili: • vero • falso	booleano	falso	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror interrotta.	SnapMirrorRelationship

Novità dalla versione

10.1

BreakSnapMirrorRelationship

L'interfaccia utente Web Element utilizza `BreakSnapMirrorRelationship` Metodo per interrompere una relazione SnapMirror. Quando una relazione SnapMirror viene interrotta, il volume di destinazione viene reso indipendente e di lettura/scrittura e può quindi divergere dall'origine. È possibile ristabilire la relazione con `ResyncSnapMirrorRelationship` Metodo API. Questo metodo richiede la disponibilità del cluster ONTAP.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeInfo	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror interrotta.	SnapMirrorRelationship

Novità dalla versione

10.1

Trova ulteriori informazioni

BreakSnapMirrorVolume

BreakSnapMirrorVolume

L'interfaccia utente Web Element utilizza `BreakSnapMirrorVolume` Metodo per interrompere la relazione di SnapMirror tra un container di origine ONTAP e un volume di destinazione dell'elemento. L'interruzione di un volume SnapMirror Element è utile se un sistema ONTAP non è più disponibile durante la replica dei dati in un volume Element. Questa funzione consente a un amministratore dello storage di assumere il controllo di un volume SnapMirror Element, interrompere la relazione con il sistema ONTAP remoto e ripristinare il volume a uno snapshot precedente.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Il volume su cui eseguire l'operazione di interruzione. La modalità di accesso al volume deve essere SnapMirrorTarget.	intero	Nessuno	Sì
SnapshotID	Eseguire il rollback del volume allo snapshot identificato da questo ID. Per impostazione predefinita, eseguire il rollback allo snapshot più recente.	intero	Nessuno	No
preservare	Conservare le snapshot più recenti rispetto a quelle identificate da snapshotID. Valori possibili: • Vero: Conserva le snapshot più recenti di snapshotID. • Falso: Non conservare snapshot più recenti di snapshotID. Se false, tutte le snapshot più recenti di snapshotID vengono eliminate.	booleano	falso	No
accesso	Modalità di accesso al volume risultante. Valori possibili: • Riscrivere • ReadOnly • bloccato	stringa	Riscrivere	No

Valori restituiti

Questo metodo non ha valori restituiti.

Novità dalla versione

10.0

Trova ulteriori informazioni

BreakSnapMirrorRelationship

CreateSnapMirrorEndpoint

L'interfaccia utente Web Element utilizza `CreateSnapMirrorEndpoint` Metodo per creare una relazione con un endpoint SnapMirror remoto.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
IP gestioneIP	L'indirizzo IP di gestione dell'endpoint remoto SnapMirror.	stringa	Nessuno	Sì
nome utente	Il nome utente di gestione per il sistema ONTAP.	stringa	Nessuno	Sì
password	La password di gestione per il sistema ONTAP.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorEndpoint	Endpoint SnapMirror appena creato.	SnapMirrorEndpoint

Novità dalla versione

10.0

CreateSnapMirrorEndpointUnmanaged

Il sistema di storage software Element utilizza `CreateSnapMirrorEndpointUnmanaged` Metodo per consentire agli endpoint SnapMirror remoti e non gestiti di comunicare con un cluster di storage Element. Gli endpoint non gestiti non possono essere amministrati utilizzando le API di Element SnapMirror. Devono essere gestiti con il software di gestione ONTAP o le API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Nome cluster	Il nome dell'endpoint.	stringa	Nessuno	Sì
Indirizzi ipAddresses	L'elenco degli indirizzi IP di un cluster di sistemi storage ONTAP che devono comunicare con questo cluster di storage Element.	array di stringhe	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorEndpoint	Endpoint SnapMirror appena creato.	SnapMirrorEndpoint

Novità dalla versione

10.3

CreateSnapMirrorRelationship

L'interfaccia utente Web Element utilizza `CreateSnapMirrorRelationship` Metodo per creare una relazione di protezione dei dati estesa di SnapMirror tra un endpoint di origine e di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
SourceVolume	Il volume di origine nella relazione.	SnapMirrorVolumeInfo	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione.	SnapMirrorVolumeInfo	Nessuno	Sì
RelazionshipType	Il tipo di relazione. Nei sistemi storage che eseguono il software Element, questo valore è sempre "Extended_data_Protection".	stringa	Nessuno	No
Nome criterio	Specifica il nome del criterio SnapMirror di ONTAP per la relazione. Se non specificato, il nome predefinito del criterio è MirrorLatest.	stringa	Nessuno	No
Nome scheduleName	Il nome della pianificazione cron preesistente sul sistema ONTAP utilizzata per aggiornare la relazione SnapMirror. Se non viene specificata alcuna pianificazione, gli aggiornamenti di SnapMirror non vengono pianificati e devono essere aggiornati manualmente.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Informazioni sulla relazione SnapMirror appena creata.	SnapMirrorRelationship

Novità dalla versione

10.1

CreateSnapMirrorVolume

L'interfaccia utente Web Element utilizza `CreateSnapMirrorVolume` Metodo per creare un volume sul sistema ONTAP remoto.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
server virtuale	Il nome del Vserver.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome del volume ONTAP di destinazione.	stringa	Nessuno	Sì
tipo	Il tipo di volume. Valori possibili: • rw: Volume di lettura/scrittura • ls: Volume di condivisione del carico • dp: Volume di protezione dei dati Se non viene fornito alcun tipo, il tipo predefinito è dp.	stringa	Nessuno	No
aggregato	Aggregato ONTAP contenente in cui creare il volume. È possibile utilizzare ListSnapMirrorAggregates per ottenere informazioni sugli aggregati ONTAP disponibili.	stringa	Nessuno	Sì
dimensione	La dimensione del volume in byte.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorVolume	Informazioni su un volume SnapMirror.	SnapMirrorVolume

Novità dalla versione

10.1

DeleteSnapMirrorEndpoint

L'interfaccia utente Web Element utilizza `DeleteSnapMirrorEndpoints` Per eliminare uno o più endpoint SnapMirror dal sistema.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Array di ID degli endpoint SnapMirror da eliminare.	array intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Novità dalla versione

10.0

DeleteSnapMirrorRelationships

L'interfaccia utente Web Element utilizza `DeleteSnapMirrorRelationships` Metodo per rimuovere una o più relazioni SnapMirror tra un endpoint di origine e di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolumes	Volume o volumi di destinazione nella relazione SnapMirror.	SnapMirrorVolumeInfo array	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
risultato	Se l'azione di eliminazione ha avuto esito positivo, questo oggetto contiene un messaggio di successo. Se l'azione non riesce, viene visualizzato un messaggio di errore.	Oggetto JSON

Novità dalla versione

10.1

GetOntapVersionInfo

L'interfaccia utente Web Element utilizza `GetOntapVersionInfo` Per ottenere informazioni sul supporto della versione API dal cluster ONTAP in una relazione SnapMirror.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Se disponibili, il sistema elenca le informazioni sulla versione dell'endpoint con l'ID snapMirrorEndpointID specificato. Se non vengono fornite, il sistema elenca le informazioni sulla versione di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
OntapVersionInfo	Le informazioni sulla versione software dell'endpoint ONTAP.	OntapVersionInfo array

Novità dalla versione

10.1

GetSnapMirrorClusterIdentity

L'interfaccia utente Web del software Element utilizza `GetSnapMirrorClusterIdentity` Per ottenere informazioni sull'identità del cluster ONTAP.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Se fornito, il sistema elenca l'identità del cluster dell'endpoint con l'ID snapMirrorEndpointID specificato. Se non viene fornito, il sistema elenca l'identità del cluster di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorClusterIdentity	Un elenco di identità del cluster degli endpoint SnapMirror.	SnapMirrorClusterIdentity array

Novità dalla versione

10.1

InitializeSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `InitializeSnapMirrorRelationship` Metodo per inizializzare il volume di destinazione in una relazione SnapMirror eseguendo un trasferimento iniziale di riferimento tra i cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID del sistema ONTAP remoto.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeInfo	Nessuno	Sì
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Informazioni sulla relazione SnapMirror inizializzata.	SnapMirrorRelationship

Novità dalla versione

10.1

ListSnapMirrorAggregates

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorAggregates` Metodo per elencare tutti gli aggregati SnapMirror disponibili nel sistema ONTAP remoto. Un aggregato descrive un insieme di risorse di storage fisiche.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Restituisce solo gli aggregati associati all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca gli aggregati di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorAggregate	Un elenco degli aggregati disponibili nel sistema storage ONTAP.	SnapMirrorAggregate array

Novità dalla versione

10.1

ListSnapMirrorEndpoint

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorEndpoints` Metodo per elencare tutti gli endpoint SnapMirror con cui il cluster di storage Element sta comunicando.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Restituisce solo gli oggetti associati a questi ID. Se non vengono forniti ID o se l'array è vuoto, il metodo restituisce tutti gli ID endpoint SnapMirror.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorEndpoint	Un elenco di endpoint SnapMirror esistenti.	SnapMirrorEndpoint array

Novità dalla versione

10.0

ListSnapMirrorLun

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorLuns` Metodo per elencare le informazioni sul LUN per la relazione SnapMirror dal cluster ONTAP remoto.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Elencare solo le informazioni del LUN associate all'ID endpoint specificato.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeInfo	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
SnapMirrorLunInfos	Un elenco di oggetti contenente informazioni sulle LUN di SnapMirror.	SnapMirrorLunInfo array

Novità dalla versione

10.1

ListSnapMirrorNetworkInterfaces

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorNetworkInterfaces` Metodo per elencare tutte le interfacce SnapMirror disponibili su un sistema ONTAP remoto.

Parametro

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Restituisce solo le interfacce di rete associate all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca le interfacce di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No
InterfaceRole	Elencare solo l'interfaccia di rete che serve il ruolo specificato.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorNetworkInterfaces	Un elenco delle interfacce di rete SnapMirror disponibili sul sistema di storage remoto ONTAP.	SnapMirrornetworkInterface array

Novità dalla versione

10.1

ListSnapMirrorNode

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorNodes` Metodo per ottenere un elenco di nodi in un cluster ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Se fornito, il sistema elenca i nodi dell'endpoint con l'ID snapMirrorEndpointID specificato. Se non viene fornito, il sistema elenca i nodi di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorNode	Un elenco dei nodi nel cluster ONTAP.	SnapMirrorNode array

Novità dalla versione

10.1

ListSnapMirrorPolicies

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorPolicies` Metodo per elencare tutti i criteri SnapMirror su un sistema ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Elencare solo i criteri associati all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca i criteri di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorPolicies	Un elenco dei criteri di SnapMirror sul sistema di storage ONTAP.	SnapMirrorPolicy array

Novità dalla versione

10.1

ListSnapMirrorSchedules

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorSchedules` Metodo per ottenere un elenco di pianificazioni disponibili in un cluster ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Se fornito, il sistema elenca le pianificazioni dell'endpoint con l'ID endpoint SnapMirror specificato. Se non viene fornito, il sistema elenca le pianificazioni di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorSchedules	Un elenco delle pianificazioni di SnapMirror sul cluster ONTAP remoto.	SnapMirrorJobScheduleCronInfo array

Novità dalla versione

10.1

ListSnapMirrorRelationships

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorRelationships` Metodo per elencare una o tutte le relazioni

SnapMirror su un cluster di storage a elementi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Elencare solo le relazioni associate all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca le relazioni di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No
DestinationVolume	Elenca le relazioni associate al volume di destinazione specificato.	SnapMirrorVolumeInfo	Nessuno	No
SourceVolume	Elenca le relazioni associate al volume di origine specificato.	SnapMirrorVolumeInfo	Nessuno	No
server virtuale	Elenca le relazioni sul Vserver specificato.	stringa	Nessuno	No
ID relazione	Elenca le relazioni associate all'ID relazione specificato.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationships	Un elenco di oggetti contenente informazioni sulle relazioni di SnapMirror.	SnapMirrorRelationship array

Novità dalla versione

10.1

ListSnapMirrorVolumes

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorVolumes` Metodo per elencare tutti i volumi SnapMirror disponibili su un sistema ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Elenca solo i volumi associati all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca i volumi di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No
server virtuale	Elenca i volumi ospitati sul Vserver specificato. Il Vserver deve essere di tipo "dati".	stringa	Nessuno	No
nome	Elenca solo i volumi ONTAP con il nome specificato.	stringa	Nessuno	No
tipo	Elenca solo i volumi ONTAP del tipo specificato. Valori possibili: • rw: Volumi di lettura/scrittura • ls: Volumi di condivisione del carico • dp: Volumi di protezione dei dati	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorVolumes	Elenco dei volumi SnapMirror disponibili nel sistema storage ONTAP.	SnapMirrorVolume array

Novità dalla versione

10.1

ListSnapMirrorVservers

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorVservers` Metodo per elencare tutti i server virtuali SnapMirror disponibili su un sistema ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Elenca solo i Vserver associati all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca i Vserver di tutti gli endpoint SnapMirror noti.	intero	Nessuno	No
VserverType	Elenca solo i server virtuali del tipo specificato. Valori possibili: • amministratore • dati • nodo • sistema	stringa	Nessuno	No
VserverName	Elenca solo i server virtuali con il nome specificato.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorVservers	Un elenco dei server virtuali SnapMirror disponibili nel sistema storage ONTAP.	SnapMirrorVserver array

Novità dalla versione

10.1

ModifySnapMirrorEndpoint

L'interfaccia utente Web del software Element utilizza `ModifySnapMirrorEndpoint` Metodo per modificare il nome e gli attributi di gestione di un endpoint SnapMirror.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Endpoint SnapMirror da modificare.	intero	Nessuno	Sì
IP gestioneIP	Il nuovo indirizzo IP di gestione per il sistema ONTAP.	stringa	Nessuno	No
nome utente	Il nuovo nome utente di gestione per il sistema ONTAP.	stringa	Nessuno	No
password	La nuova password di gestione per il sistema ONTAP.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorEndpoint	Informazioni sull'endpoint SnapMirror modificato.	SnapMirrorEndpoint

Novità dalla versione

10.0

ModifySnapMirrorEndpoint (non gestito)

Il software Element utilizza questa versione di `ModifySnapMirrorEndpoint` Metodo per modificare gli attributi del nome del cluster di storage o dell'indirizzo IP per un endpoint SnapMirror non gestito. Gli endpoint non gestiti non possono essere amministrati utilizzando le API di Element SnapMirror. Devono essere gestiti con il software di gestione ONTAP o le API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	Endpoint SnapMirror da modificare.	intero	Nessuno	Sì
Nome cluster	Il nuovo nome dell'endpoint.	stringa	Nessuno	No
Indirizzi ipAddresses	Nuovo elenco di indirizzi IP per un cluster di sistemi storage ONTAP che devono comunicare con questo cluster storage Element.	array di stringhe	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorEndpoint	Informazioni sull'endpoint SnapMirror modificato.	SnapMirrorEndpoint

Novità dalla versione

10.3

ModifySnapMirrorRelationship

È possibile utilizzare `ModifySnapMirrorRelationship` per modificare gli intervalli in cui si verifica uno snapshot pianificato. Questo metodo consente inoltre di eliminare o

mettere in pausa un programma.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	Sì
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero	Nessuno	No
Nome criterio	Specifica il nome del criterio SnapMirror di ONTAP per la relazione.	stringa	Nessuno	No
Nome scheduleName	Il nome della pianificazione cron preesistente sul sistema ONTAP utilizzata per aggiornare la relazione SnapMirror.	stringa	Nessuno	No
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente gli attributi di relazione SnapMirror modificati.	SnapMirrorRelationship

Novità dalla versione

10.1

UpdateSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `UpdateSnapMirrorRelationship` Metodo per rendere il volume di destinazione in una relazione SnapMirror un mirror aggiornato del volume di origine.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	Sì
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror aggiornata.	SnapMirrorRelationship

Novità dalla versione

10.1

QuiesceSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `QuiesceSnapMirrorRelationship` Metodo per disattivare i trasferimenti di dati futuri per una relazione SnapMirror. Se è in corso un trasferimento, lo stato della relazione diventa "quiescente" fino al completamento del trasferimento. Se il trasferimento corrente viene interrotto, non verrà riavviato. È possibile riabilitare i trasferimenti di dati per la relazione utilizzando `ResumeSnapMirrorRelationship` Metodo API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror quiescente.	SnapMirrorRelationship

Novità dalla versione

10.1

ResumeSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `ResumeSnapMirrorRelationship` Metodo per consentire trasferimenti futuri per una relazione SnapMirror quiescente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror ripresa.	SnapMirrorRelationship

Novità dalla versione

10.1

ResyncSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `ResyncSnapMirrorRelationship` metodo per stabilire o ristabilire una relazione mirror tra un endpoint di origine e di destinazione. Quando si esegue nuovamente la sincronizzazione di una relazione, il sistema rimuove gli snapshot sul volume di destinazione più recenti della copia snapshot comune, quindi monta il volume di destinazione come volume di protezione dati con la copia snapshot comune come copia

snapshot esportata.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapMirrorEndpointID	L'ID endpoint del sistema storage ONTAP remoto che comunica con il cluster storage Element.	intero	Nessuno	Sì
DestinationVolume	Il volume di destinazione nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	Sì
MaxTransferRate	Specifica la velocità massima di trasferimento dei dati tra i volumi in kilobyte al secondo. Il valore predefinito, 0, è illimitato e consente alla relazione SnapMirror di utilizzare completamente la larghezza di banda di rete disponibile.	intero	Nessuno	No
SourceVolume	Il volume di origine nella relazione SnapMirror.	SnapMirrorVolumeinfo	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SnapMirrorRelationship	Oggetto contenente informazioni sulla relazione SnapMirror resynced.	SnapMirrorRelationship

Novità dalla versione

10.1

Metodi API di configurazione del sistema

I metodi API di configurazione del sistema consentono di ottenere e impostare i valori di configurazione applicabili a tutti i nodi del cluster.

- DisableBmcColdReset
- DisableClusterSsh
- DisableSnmp
- EnableBmcColdReset
- EnableClusterSsh
- EnableSnmp
- Proprietà GetBinAssignment
- GetClusterSshInfo
- GetClusterStructure
- GetFipsReport
- GetLldpConfig
- GetLldpInfo
- GetNodeFipsDrivesReport
- GetNtpInfo
- GetNvramInfo
- GetProtectionDomainLayout
- GetRemoteLoggingHost
- GetSnmpACL
- GetSnmpInfo
- GetSnmpState
- GetSnmpTrapInfo
- GetSSLCertificate
- ListProtectionDomainLevels
- RemoveSSLCertificate
- ResetNetworkConfig
- ResetSupplementalTlsCipher
- SetClusterStructure
- SetLldpConfig
- SetNtpInfo
- SetProtectionDomainLayout

- SetRemoteLoggingHost
- SetSnmpACL
- SetSnmpInfo
- SetSnmpTrapInfo
- SetSSLCertificate
- SnmpSendTestTrap
- TestAddressAvailability

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

DisableBmcColdReset

È possibile utilizzare `DisableBmcColdReset` Metodo per disattivare l'attività in background che ripristina periodicamente il Baseboard Management Controller (BMC) per tutti i nodi del cluster.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
CBmcResetDurationMinutes	Restituisce il tempo tra gli intervalli di ripristino. L'intervallo deve essere sempre 0 dopo il completamento del comando.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 0
    }
}
```

Novità dalla versione

12.0

DisableClusterSsh

È possibile utilizzare `DisableClusterSsh` Metodo per disattivare il servizio SSH per l'intero cluster di storage. Quando si aggiungono nodi al cluster di storage, i nuovi nodi erediteranno questa impostazione a livello di cluster.

Parametro

Questo metodo non ha alcun parametro di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
risultato	Oggetto JSON contenente lo stato del servizio SSH per il cluster di storage, il tempo rimanente prima della disattivazione di SSH e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableClusterSsh",
  "params": {
      },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result" : {
    "enabled": true,
    "timeRemaining": "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```

Novità dalla versione

10.3

DisableSnmp

È possibile utilizzare `DisableSnmp` Metodo per disattivare SNMP sui nodi del cluster.

Parametro

Questo metodo non ha alcun parametro di input.

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "result" : {},
  "id" : 1
}
```

Novità dalla versione

9.6

EnableBmcColdReset

È possibile utilizzare `EnableBmcColdReset` Metodo per abilitare un'attività in background che reimposta periodicamente il Baseboard Management Controller (BMC) per tutti i nodi del cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
timeout	Il tempo che intercorre tra le operazioni di ripristino BMC, in minuti.	intero	20160 minuti	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
CBmcResetDurationMinutes	Restituisce il tempo tra gli intervalli di ripristino. L'intervallo deve essere sempre 0 dopo il completamento del comando.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "EnableBmcColdReset",
    "params": {
                "timeout": 36000
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "cBmcResetDurationMinutes": 36000
    }
}
```

Novità dalla versione

12.0

EnableClusterSsh

È possibile utilizzare `EnableClusterSsh` Metodo per attivare il servizio SSH su tutti i nodi del cluster di storage.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
durata	Il periodo di tempo in cui il servizio SSH rimane attivato.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
risultato	Oggetto JSON contenente lo stato del servizio SSH per il cluster di storage, il tempo rimanente prima della disattivazione di SSH e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableClusterSsh",
  "params": {
      "duration"  : "02:00:00.00"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result" : {
    "enabled": true,
    "timeRemaining": "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```

Novità dalla versione

10.3

EnableSnmp

È possibile utilizzare `EnableSnmp` Metodo per attivare SNMP sui nodi del cluster. Quando si attiva SNMP, l'azione viene applicata a tutti i nodi del cluster e i valori passati sostituiscono tutti i valori impostati in qualsiasi chiamata precedente a. `EnableSnmp`.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnmpV3Enabled (snmpV3Enabled)	Se impostato su true, SNMP v3 viene attivato su ciascun nodo del cluster. Se impostato su false, SNMP v2 viene attivato.	booleano	falso	No

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "EnableSnmp",
  "params": {
      "snmpV3Enabled"  : "true"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

Proprietà GetBinAssignment

È possibile utilizzare `GetBinAssignmentProperties` metodo per recuperare le proprietà di assegnazione del bin nel database.

Parametro

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
proprietà	Descrive in dettaglio le proprietà di tutte le assegnazioni correnti dei bin nel database.	Array binAssignmentProperties

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "GetBinAssignmentProperties",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "properties": {
            "algorithmRuntimeMS": 1105,
            "areReplicasValid": true,
            "binCount": 65536,
            "isBalanced": true,
            "isStable": true,
            "isWellCoupled": false,
            "layout": [
                {
                    "protectionDomainName": "1",
                    "services": [
                        {
                            "budget": 7281,
                            "serviceID": 16
                        },
                        {
                            "budget": 7281,
                            "serviceID": 19
```

```
                    },
                    {
                        "budget": 7281,
                        "serviceID": 24
                    }
                ]
            },
            {
                "protectionDomainName": "2",
                "services": [
                    {
                        "budget": 7281,
                        "serviceID": 17
                    },
                    {
                        "budget": 7281,
                        "serviceID": 20
                    },
                    {
                        "budget": 7281,
                        "serviceID": 22
                    }
                ]
            },
            {
                "protectionDomainName": "3",
                "services": [
                    {
                        "budget": 7281,
                        "serviceID": 18
                    },
                    {
                        "budget": 7281,
                        "serviceID": 21
                    },
                    {
                        "budget": 7281,
                        "serviceID": 23
                    }
                ]
            }
        ],
        "numSwaps": 0,
        "numUpdatingBins": 0,
        "protectionDomainType": "node",
        "reason": "Final",
```

```
            "replicationCount": 2,
            "requestRebalance": false,
            "serviceStrandedCapacities": [],
            "timePublished": "2020-04-02T18:34:07.807681Z",
            "validSchemes": []
        }
    }
}
```

Novità dalla versione

12.0

GetClusterSshInfo

È possibile utilizzare `GetClusterSshInfo` Metodo per eseguire query sullo stato del servizio SSH per l'intero cluster di storage.

Parametro

Questo metodo non ha alcun parametro di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
risultato	Oggetto JSON contenente lo stato del servizio SSH per il cluster di storage, il tempo rimanente prima della disattivazione di SSH e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetClusterSshInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result" : {
    "enabled": "true",
    "timeRemaining": "00:43:21",
    "nodes": [
    {
        "nodeID": 1,
        "enabled": true
    },
    {
        "nodeID": 2,
        "enabled": true
    },
    {
        "nodeID": 3,
        "enabled": false
    },
    {
        "nodeID": 4,
        "enabled": false
    } ]
            }
    }
```

Novità dalla versione

10.3

GetClusterStructure

È possibile utilizzare `GetClusterStructure` metodo per eseguire il backup delle informazioni di configurazione del cluster di storage corrente. Se la configurazione del cluster di storage viene modificata mentre questo metodo è in esecuzione, il contenuto del backup della configurazione sarà imprevedibile. È possibile salvare questi dati in un file di testo e ripristinarli su altri cluster o sullo stesso cluster in caso di disastro.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
risultato	Oggetto JSON contenente le informazioni di configurazione del cluster di storage corrente.	Struttura del clusterStructure

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetClusterStructure",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result" : <clusterStructure object containing configuration
information>
    }
```

Novità dalla versione

10.3

GetFipsReport

È possibile utilizzare `GetFipsReport` Metodo per verificare lo stato di supporto della funzione di crittografia FIPS 140-2 di tutti i nodi nel cluster di storage.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
risultato	Oggetto JSON contenente lo stato del supporto delle funzionalità FIPS 140-2 per ogni nodo e le informazioni sugli errori per ogni nodo che non ha risposto alla query.	FipsReport

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetFipsReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
    "nodes": [
        {
           "nodeID": 1,
           "fipsDrives": "None",
           "httpsEnabled": true
        },
        {
           "nodeID": 3,
           "fipsDrives": "None",
           "httpsEnabled": true
        }
    ],
    "errorNodes": [
        {
           "nodeID": 2,
           "error": {
               "message": "The RPC timed out.",
               "name": "xRpcTimeout"
               }
        }
    ]
    }
}
```


Novità dalla versione

10.3

GetLldpConfig

È possibile utilizzare `GetLldpConfig` Metodo per ottenere la configurazione LLDP (link Layer Discovery Protocol) per ciascun nodo di un cluster di storage.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
LldpConfig	Informazioni sulla configurazione LLDP del cluster di storage.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetLldpConfig",
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": null,
        "result": {
            "lldpConfig": {
                "enableLldp": true,
                "enableMed": false,
                "enableOtherProtocols": true
        }
    }
}
```

GetLldpInfo

È possibile utilizzare `GetLldpInfo` Metodo per ottenere la configurazione LLDP (link Layer Discovery Protocol) per ciascun nodo di un cluster di storage o di un singolo nodo di storage.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
LldpInfo	Informazioni su chassis, interfaccia e impostazioni LLDP adiacenti per ciascun nodo di un cluster di storage.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetLldpInfo",
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

11.0

Trova ulteriori informazioni

GetLldpInfo

GetNodeFipsDrivesReport

È possibile utilizzare `GetNodeFipsDrivesReport` Metodo per controllare lo stato della funzionalità di crittografia del disco FIPS 140-2 di un singolo nodo nel cluster di storage. È necessario eseguire questo metodo su un singolo nodo di storage.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
FipsDrive	Oggetto JSON contenente lo stato del supporto della funzionalità FIPS 140-2 per questo nodo. Valori possibili: • None (Nessuno): Il nodo non supporta FIPS. • Parziale: Il nodo supporta FIPS, ma non tutti i dischi nel nodo sono dischi FIPS. • Pronto: Il nodo è compatibile con FIPS e tutti i dischi nel nodo sono dischi FIPS (o non sono presenti dischi).	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "fipsDrives": "None"
    }
}
```

Novità dalla versione

11.5

GetNtpInfo

È possibile utilizzare `GetNtpInfo` Metodo per ottenere le informazioni di configurazione NTP (Network Time Protocol) correnti.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
server	Elenco dei server NTP.	array di stringhe
client di trasmissione	Indica se i nodi nel cluster sono in attesa di messaggi NTP di trasmissione. Valori possibili: • vero • falso	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNtpInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
    "broadcastclient" : false,
    "servers" : [ "us.pool.ntp.org" ]
   }
}
```

Novità dalla versione

9.6

GetNvramInfo

È possibile utilizzare `GetNvramInfo` Metodo per ottenere informazioni da ciascun nodo sulla scheda NVRAM.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
forza	Il parametro force deve essere incluso in questo metodo per poter essere eseguito correttamente su tutti i nodi del cluster.	booleano	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
NvramInfo	Array di eventi ed errori rilevati sulla scheda NVRAM.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetNvramInfo",
  "params": {
      "force": true
      },
  "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

Trova ulteriori informazioni

GetNvramInfo

GetProtectionDomainLayout

È possibile utilizzare `GetProtectionDomainLayout` metodo per restituire tutte le informazioni sul dominio di protezione per un cluster, inclusi lo chassis e il dominio di protezione personalizzato in cui si trova ciascun nodo.

Parametro

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ProtectionDomainLayout	Elenco di nodi, ciascuno con i relativi domini di protezione associati.	Elenco JSON di "NodeProtectionDomini" oggetti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetProtectionDomainLayout",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR2914008D",
            "protectionDomainType": "chassis"
```

```
        },
        {
          "protectionDomainName": "Rack-1",
          "protectionDomainType": "custom"
        }
      ]
    },
    {
      "nodeID": 2,
      "protectionDomains": [
        {
          "protectionDomainName": "QTFCR291500EA",
          "protectionDomainType": "chassis"
        },
        {
          "protectionDomainName": "Rack-1",
          "protectionDomainType": "custom"
        }
      ]
    },
    {
      "nodeID": 3,
      "protectionDomains": [
        {
          "protectionDomainName": "QTFCR291500C3",
          "protectionDomainType": "chassis"
        },
        {
          "protectionDomainName": "Rack-2",
          "protectionDomainType": "custom"
        }
      ]
    },
    {
      "nodeID": 4,
      "protectionDomains": [
        {
          "protectionDomainName": "QTFCR291400E6",
          "protectionDomainType": "chassis"
        },
        {
          "protectionDomainName": "Rack-2",
          "protectionDomainType": "custom"
        }
      ]
    }
```

```
      ]
    }
}
```

Novità dalla versione

12.0

GetRemoteLoggingHost

È possibile utilizzare `GetRemoteLoggingHosts` metodo per ottenere l'elenco corrente dei server di log.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
Remote	Elenco di indirizzi IP e informazioni sulle porte relative agli host configurati per ricevere informazioni di registrazione inoltrate.	Server di loggingServer array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "id": 3386609,
   "method": "GetRemoteLoggingHosts",
   "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 3386609,
   "result": {
      "remoteHosts": [
         {
           "host": "172.16.1.20",
           "port": 10514
         },
         {
           "host": "172.16.1.25"
         }
      ]
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

SetRemoteLoggingHost

GetSnmpACL

È possibile utilizzare `GetSnmpACL` Metodo per ottenere le autorizzazioni di accesso SNMP correnti sui nodi del cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
reti	Elenco delle reti e tipo di accesso ai server SNMP in esecuzione sui nodi del cluster. Questo valore è presente se SNMP v3 è disattivato.	rete array
UsmUsers	Elenco di utenti e tipo di accesso ai server SNMP in esecuzione sui nodi del cluster. Questo valore è presente se SNMP v3 è attivato.	UsmUser array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "GetSnmpACL",
"params": {},
"id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
     "usmUsers"  : [
       {
          "name": "jdoe",
          "access": "rouser",
          "secLevel": "priv",
          "password": "mypassword",
          "passphrase": "mypassphrase",
       }
     ]
   }
}
```

Novità dalla versione

9.6

GetSnmpInfo

È possibile utilizzare `GetSnmpInfo` Metodo per ottenere le informazioni di configurazione SNMP (Simple Network Management Protocol) correnti.

Parametri

GetSnmpInfo è obsoleto per le versioni successive a Element versione 8.0. Il GetSnmpState e. SetSnmpACL I metodi sostituiscono il metodo GetSnmpInfo.

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
reti	Elenco delle reti e dei tipi di accesso abilitati per SNMP. **Nota:** le reti vengono visualizzate solo se SNMP v3 è disattivato.	rete
attivato	Indica se i nodi nel cluster sono configurati per SNMP. Valori possibili: • vero • falso	booleano
SnmpV3Enabled (snmpV3Enabled)	Se il nodo nel cluster è configurato per SNMP v3. Valori possibili: • vero • falso	booleano
UsmUsers	Se SNMP v3 è attivato, dal cluster viene restituito un elenco di parametri di accesso utente per SNMP. Viene restituito al posto del parametro networks.	UsmUser

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetSnmpInfo",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "enabled" : true,
      "networks" : [
         {
            "access" : "rosys",
            "cidr" : 0,
            "community" : "public",
            "network" : "localhost"
         }
      ]
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetSnmpState
- SetSnmpACL

GetSnmpState

È possibile utilizzare `GetSnmpState` Metodo per ottenere lo stato corrente della funzione SNMP.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
attivato	Valori possibili: • vero • falso Il valore predefinito è false. Restituisce true se i nodi nel cluster sono configurati per SNMP.	booleano

Nome	Descrizione	Tipo
SnmpV3Enabled (snmpV3Enabled)	Valori possibili: • vero • falso Il valore predefinito è false. Restituisce true se i nodi nel cluster sono configurati per SNMP v3.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {
   "enabled": true,
   "snmpV3Enabled": false
   }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

SetSnmpACL

GetSnmpTrapInfo

È possibile utilizzare `GetSnmpTrapInfo` Metodo per ottenere le informazioni di configurazione correnti del trap SNMP.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
TrapiRecipients	Elenco degli host che devono ricevere i trap generati dal cluster.	SnmpTrapRecipient array
ClusterFaultTrappsEnabled (ClusterFaultTrappsEnabled)	Il valore true indica che è stata configurata una notifica solidFireClusterFaultNotification per essere inviata all'elenco di destinatari trap quando viene registrato un errore del cluster.	booleano
ClusterFaultResolvedTrappsEnabled	Il valore true indica che è stata configurata una notifica di solidFireClusterFaultResolvedNotification per essere inviata all'elenco di destinatari trap quando viene risolto un errore del cluster.	booleano
ClusterEventTrappsEnabled (ClusterEventTrappsEnabled)	Il valore true indica che è stata configurata una notifica solidFireClusterEventNotification per essere inviata all'elenco di destinatari trap quando viene registrato un evento del cluster.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method":"GetSnmpTrapInfo"
   "params":{},
   "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "clusterEventTrapsEnabled": true,
    "clusterFaultResolvedTrapsEnabled": true,
    "clusterFaultTrapsEnabled": true,
    "trapRecipients": [
     {
      "community": "public",
      "host": "192.168.151.60",
      "port": 162
     },
     {
      "community": "solidfireAlerts",
      "host": "NetworkMonitor",
      "port": 162
     },
     {
      "community": "wakeup",
      "host": "PhoneHomeAlerter",
      "port": 1008
     }
   ]
 }
}
```


Novità dalla versione

9.6

GetSSLCertificate

È possibile utilizzare `GetSSLCertificate` Metodo per recuperare il certificato SSL attualmente attivo sui nodi di storage del cluster.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
certificato	Il testo completo del certificato con codifica PEM.	stringa
dettagli	Le informazioni decodificate del certificato.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "GetSSLCertificate",
    "params" : {},
    "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
```

```
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n",
        "details": {
            "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
            "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F0146396
4B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03
A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB82
9199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA9
5BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05
DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BE
A6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
            "notAfter": "2027-03-06T22:50:26Z",
            "notBefore": "2017-03-08T22:50:26Z",
            "serial": "CC1B221598E37FF3",
            "sha1Fingerprint":
"1D:70:7A:6F:18:8A:CD:29:50:C7:95:B1:DD:5E:63:21:F4:FA:6E:21",
            "subject":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org"
        }
    }
}
```


Novità dalla versione

10.0

ListProtectionDomainLevels

È possibile utilizzare `ListProtectionDomainLevels` metodo per elencare i livelli di tolleranza e resilienza del cluster di storage. I livelli di tolleranza indicano la capacità del cluster di continuare a leggere e scrivere i dati in caso di guasto, mentre i livelli di resilienza indicano la capacità del cluster di storage di guarire automaticamente da uno o più guasti.

Parametro

Questo metodo non ha alcun parametro di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
ProtectionDomainLevels	Un elenco dei diversi livelli di dominio di protezione, in cui ciascuno fornisce le informazioni di resilienza e tolleranza del cluster di storage.	ProtectionDomainLevel

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListProtectionDomainLevels",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "protectionDomainLevels": [
            {
                "protectionDomainType": "node",
                "resiliency": {
                    "protectionSchemeResiliencies": [
                            {
                                "protectionScheme": "doubleHelix",
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
                    ],
                    "singleFailureThresholdBytesForBlockData": 0,
                    "sustainableFailuresForEnsemble": 1
                },
                "tolerance": {
                    "protectionSchemeTolerances": [
                            {
                                "protectionScheme": "doubleHelix",
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
```

```
                    ],
                    "sustainableFailuresForEnsemble": 1
                }
            },
            {
                "protectionDomainType": "chassis",
                "resiliency": {
                    "protectionSchemeResiliencies": [
                            {
                                "protectionScheme": "doubleHelix",
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
                    ],
                    "singleFailureThresholdBytesForBlockData": 0,
                    "sustainableFailuresForEnsemble": 1
                },
                "tolerance": {
                    "protectionSchemeTolerances": [
                            {
                                "protectionScheme": "doubleHelix",
                                "sustainableFailuresForBlockData": 0,
                                "sustainableFailuresForMetadata": 1
                            }
                    ],
                    "sustainableFailuresForEnsemble": 1
                }
            }
        ]
    }
}
```


Novità dalla versione

11.0

RemoveSSLCertificate

È possibile utilizzare `RemoveSSLCertificate` Metodo per rimuovere il certificato SSL dell'utente e la chiave privata per i nodi di storage nel cluster. Una volta rimossi il certificato e la chiave privata, i nodi di storage vengono configurati per utilizzare il certificato e la chiave privata predefiniti.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "RemoveSSLCertificate",
    "params" : {},
    "id" : 3
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 3,
    "result" : {}
}
```

Novità dalla versione

10.0

ResetNetworkConfig

È possibile utilizzare `ResetNetworkConfig` metodo per risolvere i problemi di configurazione di rete per un singolo nodo. Questo metodo ripristina la configurazione di rete di un singolo nodo alle impostazioni predefinite di fabbrica.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ResetNetworkConfig",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo non restituisce una risposta.

Novità dalla versione

11.0

ResetSupplementalTlsCipher

È possibile utilizzare `ResetSupplementalTlsCiphers` Metodo per ripristinare l'elenco di crittografia TLS supplementari ai valori predefiniti. È possibile utilizzare questo metodo sull'intero cluster.

Parametro

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

11.3

SetClusterStructure

È possibile utilizzare `SetClusterStructure` metodo per ripristinare le informazioni di configurazione del cluster di storage da un backup. Quando si chiama il metodo, si passa l'oggetto clusterStructure contenente le informazioni di configurazione che si desidera ripristinare come parametro params.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo
parametri	Oggetto JSON contenente le informazioni di configurazione del cluster di storage corrente.	Struttura del clusterStructure

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
risultato	Handle asincrono dei risultati.	AsyncHandle

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "SetClusterStructure",
  "params": <insert clusterStructure object here>,
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result" : {
    "asyncHandle": 1
    }
}
```

Novità dalla versione

10.3

SetLldpConfig

È possibile utilizzare `SetLldpConfig` Metodo per configurare le impostazioni LLDP (link Layer Discovery Protocol) per un cluster di storage.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
EnableOtherProtocols	Abilita l'utilizzo automatico di altri protocolli di rilevamento: CDP, FDP, EDP e SONMP.	booleano	vero	No
EnableMed	Attiva Media Endpoint Discovery (LLDP-MED).	booleano	falso	No
EnableLldp	Attiva o disattiva LLDP.	booleano	vero	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
LldpConfig	Informazioni sulla configurazione LLDP corrente del cluster di storage, incluse le impostazioni appena modificate.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 3920,
  "method":"SetLldpConfig",
    "params": {
        "lldpConfig": {
            "enableMed": true
        }
    }
  }
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 3920,
  "result": {
    "lldpConfig": {
        "enableLldp": true,
        "enableMed": true,
        "enableOtherProtocols": true
     }
  }
}
```

SetNtpInfo

È possibile utilizzare `SetNtpInfo` Metodo per configurare NTP sui nodi del cluster. I valori impostati con questa interfaccia si applicano a tutti i nodi del cluster. Se un server di trasmissione NTP trasmette periodicamente informazioni sull'ora sulla rete, è possibile configurare i nodi come client di trasmissione.

Parametri

Assicurarsi di utilizzare server NTP interni alla rete, anziché i valori predefiniti per l'installazione.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
server	Elenco dei server NTP da aggiungere a ciascuna configurazione NTP del nodo.	array di stringhe	Nessuno	Sì
client di trasmissione	Attiva ogni nodo del cluster come client di broadcast.	booleano	falso	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "SetNtpInfo",
   "params": {
     "servers"  : [
       "ntpserver1.example.org",
       "ntpserver2.example.org",
       "ntpserver3.example.org"
     ],
     "broadcastclient" : false
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 1,
    "result" : {}
}
```

Novità dalla versione

9.6

SetProtectionDomainLayout

È possibile utilizzare `SetProtectionDomainLayout` metodo per assegnare nodi a domini di protezione personalizzati.

Devono essere fornite informazioni per tutti i nodi attivi nel cluster e non è possibile fornire informazioni per i nodi inattivi. Tutti i nodi di un determinato chassis devono essere assegnati allo stesso dominio di protezione personalizzato. Lo stesso protectionDomainType deve essere fornito per tutti i nodi. ProtectionDomainTypes non personalizzati, come nodo e chassis, non devono essere inclusi. Se viene fornito uno di questi, i domini di protezione personalizzati vengono ignorati e viene restituito un errore appropriato.

I domini di protezione personalizzati non sono supportati con le seguenti configurazioni:

- Cluster di storage contenenti chassis condivisi
- Cluster di storage a due nodi

Il metodo restituisce un errore quando viene utilizzato su cluster di storage con queste configurazioni.

Parametro

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ProtectionDomainLayout	Informazioni sul dominio di protezione per ciascun nodo.	Elenco JSON di "NodeProtectionDomini" oggetti.	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ProtectionDomainLayout	Elenco di nodi, ciascuno con i relativi domini di protezione associati.	Elenco JSON di "NodeProtectionDomini" oggetti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1,
  "method": "SetProtectionDomainLayout",
  "params": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 2,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 3,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 4,
        "protectionDomains": [
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
      }
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:


```
{
  "id": 1,
  "result": {
    "protectionDomainLayout": [
      {
        "nodeID": 1,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR2914008D",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 2,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500EA",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-1",
            "protectionDomainType": "custom"
          }
        ]
      },
      {
        "nodeID": 3,
        "protectionDomains": [
          {
            "protectionDomainName": "QTFCR291500C3",
            "protectionDomainType": "chassis"
          },
          {
            "protectionDomainName": "Rack-2",
            "protectionDomainType": "custom"
          }
        ]
```

```
        },
        {
          "nodeID": 4,
          "protectionDomains": [
            {
              "protectionDomainName": "QTFCR291400E6",
              "protectionDomainType": "chassis"
            },
            {
              "protectionDomainName": "Rack-2",
              "protectionDomainType": "custom"
            }
          ]
        }
      ]
    }
}
```

Novità dalla versione

12.0

SetRemoteLoggingHost

È possibile utilizzare `SetRemoteLoggingHosts` metodo per configurare la registrazione remota dai nodi del cluster di storage a uno o più server di log centralizzati. La registrazione remota viene eseguita su TCP utilizzando la porta predefinita 514. Questa API non viene aggiunta agli host di registrazione esistenti. Invece, sostituisce ciò che attualmente esiste con i nuovi valori specificati da questo metodo API. È possibile utilizzare `GetRemoteLoggingHosts` per determinare quali sono gli host di registrazione correnti e utilizzarli `SetRemoteLoggingHosts` per impostare l'elenco desiderato di host di registrazione correnti e nuovi.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Remote	Elenco degli host destinatari dei messaggi di log.	Server di loggingServer array	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "id": 1,
   "method": "SetRemoteLoggingHosts",
   "params": {
     "remoteHosts": [
        {
          "host": "172.16.1.20",
          "port": 10514
        },
        {
          "host": "172.16.1.25"
        }
      ]
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 1,
    "result" : {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

GetRemoteLoggingHost

SetSnmpACL

È possibile utilizzare `SetSnmpACL` Metodo per configurare le autorizzazioni di accesso SNMP sui nodi del cluster. I valori impostati con questa interfaccia si applicano a tutti i nodi del cluster e i valori passati sostituiscono tutti i valori impostati in qualsiasi chiamata precedente a. `SetSnmpACL`. Si noti inoltre che i valori impostati con questa interfaccia sostituiscono tutti i valori di rete o usmUsers impostati con `SetSnmpInfo` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
reti	Elenco delle reti e tipo di accesso ai server SNMP in esecuzione sui nodi del cluster. Vedere oggetto di rete SNMP per i possibili valori di rete. Questo parametro è obbligatorio se SNMP v3 è disattivato.	rete	Nessuno	No
UsmUsers	Elenco di utenti e tipo di accesso ai server SNMP in esecuzione sui nodi del cluster. Questo parametro è obbligatorio se SNMP v3 è attivato.	UsmUser	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "SetSnmpACL",
  "params": {
    "usmUsers"  : [
      {
         "name": "jdoe",
         "access": "rouser",
         "secLevel": "priv",
         "password": "mypassword",
         "passphrase": "mypassphrase",
      }
    ]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

SetSnmpInfo

SetSnmpInfo

È possibile utilizzare `SetSnmpInfo` Metodo per configurare SNMP versione 2 e versione 3 sui nodi del cluster. I valori impostati con questa interfaccia si applicano a tutti i nodi del cluster e i valori passati sostituiscono tutti i valori impostati in qualsiasi chiamata precedente a. `SetSnmpInfo`.

Parametri

> SetSnmpInfo è obsoleto per Element versione 6.0 e successive. Utilizzare EnableSnmp e. SetSnmpACL invece.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
reti	Elenco delle reti e tipo di accesso ai server SNMP in esecuzione sui nodi del cluster. Consultare la sezione SNMP rete oggetto per i valori possibili. Questo parametro è obbligatorio solo per SNMP v2.	rete array	Nessuno	No
attivato	Se impostato su true, SNMP viene attivato su ciascun nodo del cluster.	booleano	falso	No
SnmpV3Enabled (snmpV3Enabled)	Se impostato su true, SNMP v3 viene attivato su ciascun nodo del cluster.	booleano	falso	No
UsmUsers	Se SNMP v3 è attivato, questo valore deve essere passato al posto del parametro networks. Questo parametro è necessario solo per SNMP v3.	UsmUser	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta con SNMP v3 attivato

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":true,
    "usmUsers":[
      {
        "name":"user1",
        "access":"rouser",
        "secLevel":"auth",
        "password":"namex1",
        "passphrase":"yourpassphrase"
      }
    ]
  },
 "id":1
}
```

Esempio di richiesta con SNMP v2 attivato

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method":"SetSnmpInfo",
"params":{
    "enabled":true,
    "snmpV3Enabled":false,
    "networks":[
      {
        "community":"public",
        "access":"ro",
        "network":"localhost",
      }
    ]
  },
  "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1
  "result" :{
  }
}
```

Novità dalla versione

9.6

SetSnmpTrapInfo

È possibile utilizzare `SetSnmpTrapInfo` Metodo per attivare e disattivare la generazione di notifiche SNMP (trap) del cluster e per specificare il set di host che ricevono le notifiche. I valori che passi con ciascuno `SetSnmpTrapInfo` la chiamata al metodo sostituisce tutti i valori impostati in una chiamata precedente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo
TrapiRecipients	Elenco degli host che devono ricevere i trap generati dal cluster di storage. Se uno dei tipi di trap è attivato, è necessario almeno un oggetto. Questo parametro è obbligatorio solo se i parametri booleani sono impostati su true. (Nessun valore predefinito. Non richiesto.)	SnmpTrapRecipient array
ClusterFaultTrappsEnabled (ClusterFaultTrappsEnabled)	Se impostata su true, una notifica di guasto del cluster corrispondente viene inviata all'elenco configurato di destinatari trap quando viene registrato un guasto del cluster. (Valore predefinito: False. Non richiesto.)	booleano
ClusterFaultResolvedTrappsEnabled	Se impostata su true, una notifica corrispondente alla risoluzione dei guasti del cluster viene inviata all'elenco configurato di destinatari trap quando viene risolto un guasto del cluster. (Valore predefinito: False. Non richiesto.)	booleano

Nome	Descrizione	Tipo
ClusterEventTrappsEnabled (ClusterEventTrappsEnabled)	Se impostata su true, una notifica di evento del cluster corrispondente viene inviata all'elenco configurato di destinatari trap quando viene registrato un evento del cluster. (Valore predefinito: False. Non richiesto.)	booleano

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method":"SetSnmpTrapInfo",
"params":{
    "clusterFaultTrapsEnabled":true,
    "clusterFaultResolvedTrapsEnabled":true,
    "clusterEventTrapsEnabled":true,
    "trapRecipients":[
    {
      "host":"192.30.0.10",
      "port":162,
      "community":"public"
    }
   ]
  },
  "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id" : 1,
    "result" : {}
}
```

Novità dalla versione

9.6

SetSSLCertificate

È possibile utilizzare `SetSSLCertificate` Metodo per impostare un certificato SSL utente e una chiave privata per i nodi di storage nel cluster.

Dopo aver utilizzato l'API, riavviare il nodo di gestione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
certificato	Versione del certificato con codifica PEM. **Nota:** quando si imposta un certificato di nodo o cluster, il certificato deve includere l'estensione extendedKeyUsage per serverAuth. Questa estensione consente di utilizzare il certificato senza errori nei sistemi operativi e nei browser più comuni. Se l'estensione non è presente, l'API rifiuterà il certificato come non valido.	stringa	Nessuno	Sì
PrivateKey	Versione del testo con codifica PEM della chiave privata.	stringa	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method" : "SetSSLCertificate",
    "params" : {
        "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEWMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrgpGZQF3iOSIcBHtLKE5186JVT6j5dg\n6yjUGQO352ylc9HXHcn6lb
/jyl0DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzxF+ACq+itaw
IDAQABAoIBAH1jlIZr6/sltqVW\nO0qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw92O8D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuHl1esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIJIMEgnfuLZp8IelJQXn\nSFJbk2ECgYEA
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nlHzPlhms6hxexwz1dzAp
gog/NOM+2bAc0rn0dqvtV4doejtlDZKRqrNCf/cuN2QX\njaCJClCWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhzXpLr+v30Hy2h0yAlBS\nny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nC9MJtXGfhp//G0bzwsRzZxOBsUJb15tppaZIs9MCgYAJricpkKjM
0xlZ1jdvXsos\nPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+AOeQXw3vgAhJ/qNJ\njQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nzPssy6t+QE
La1fFbAXkZ5Pg1ITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\n+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\njS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\n3rnR8AqAm4VMzqRahs2PWNe2Hl4J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nInDXvTgXMdMoet4BKnftelrXFKHgGqXJoczq4JWzGS
IHNgvkrH60\n-----END RSA PRIVATE KEY-----\n",
        "certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\nA1UEChMYV2hhdC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\naGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMTcwMzA4MjI1MDI2WhcN\nMjcwMzA2MjI1MDI2WjCBgzELMAkGA1
UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYD\nVQQHFAxWZWdhcywgQmFieSExITAfBgNVBAoTGF
doYXQgSGFwcGVucyBpbiBWZWdh\ncy4uLjEtMCsGCSqGSIb3DQEJARYed2hhdGhhcHBlbnNAdm
VnYXNzdGF5c2luLnZl\nZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEWMR\n6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovxl5wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nmrgp
GZQF3iOSIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\n7dg9cyXu4afXcgKy14Ji
NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQQHFAxW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbiBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7JyfS37l4rRolFpX6N\niebEgAaE5e
```

```
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dHOlQ+WYnoO/eIMy0coT26JBl5H\nDEwvdl+DwkxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
l0QoQDWNDoTeRBsz80nwiouA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}
```


Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:


```
{
    "id" : 2,
    "result" : {}
}
```


Novità dalla versione

10.0

SnmpSendTestTrap

`SnmpSendTestTraps` Consente di verificare la funzionalità SNMP di un cluster. Questo metodo indica al cluster di inviare trap SNMP di test al gestore SNMP attualmente configurato.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
stato	Stato del test.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "SnmpSendTestTraps",
    "params": {},
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
      "status": "complete"
   }
}
```

Novità dalla versione

9.6

TestAddressAvailability

È possibile utilizzare `TestAddressAvailability` Metodo per verificare se un determinato indirizzo IP è in uso su un'interfaccia all'interno del cluster di storage.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
interfaccia	L'interfaccia di rete di destinazione (ad esempio eth0, Bond10G, ecc.).	stringa	Nessuno	Sì
indirizzo	L'indirizzo IP da ricercare nell'interfaccia di destinazione.	stringa	Nessuno	Sì
VirtualNetworkTag	L'ID VLAN di destinazione.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
timeout	Timeout in secondi per il test dell'indirizzo di destinazione.	intero	5	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
indirizzo	Indirizzo IP verificato.	stringa
disponibile	True se l'indirizzo IP richiesto è in uso e false in caso contrario.	booleano

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "TestAddressAvailability",
    "params": {
        "interface": "Bond10G",
        "address": "10.0.0.1",
        "virtualNetworkTag": 1234
    }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "address":"10.0.0.1",
        "available": true
    }
}
```

Novità dalla versione

11.0

Metodi API di rete multi-tenant

La rete multi-tenant nei cluster di storage Element consente di collegare il traffico tra più client su reti logiche separate a un cluster di storage a un elemento senza routing di livello 3.

Le connessioni al cluster di storage vengono separate nello stack di rete attraverso l'utilizzo del tagging VLAN.

Prerequisiti per la configurazione di una rete virtuale multi-tenant

- È necessario aver identificato il blocco di indirizzi IP della rete client da assegnare alle reti virtuali sui nodi di storage.
- È necessario aver identificato un indirizzo IP della rete di storage client (SVIP) da utilizzare come endpoint per tutto il traffico di storage.

Ordine delle operazioni di rete virtuale

1. Utilizzare il metodo AddVirtualNetwork per eseguire il provisioning in blocco degli indirizzi IP immessi.

   Dopo aver aggiunto una rete virtuale, il cluster esegue automaticamente le seguenti operazioni:

   - Ogni nodo di storage crea un'interfaccia di rete virtuale.
   - A ciascun nodo di storage viene assegnato un indirizzo VLAN a cui è possibile instradare utilizzando l'SVIP virtuale.
   - Gli indirizzi IP della VLAN persistono su ciascun nodo in caso di riavvio del nodo.
2. Una volta assegnati l'interfaccia di rete virtuale e gli indirizzi VLAN, è possibile assegnare il traffico di rete del client al SVIP virtuale.

Trova ulteriori informazioni

- Convenzioni di naming della rete virtuale
- AddVirtualNetwork
- ModifyVirtualNetwork
- ListVirtualNetworks
- RemoveVirtualNetwork
- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Convenzioni di naming della rete virtuale

I sistemi di storage NetApp Element utilizzano numeri in aumento monotonicamente come identificatori univoci per tutti gli oggetti del sistema.

Quando si crea un nuovo volume, il nuovo volume ID corrisponde a un incremento di esattamente 1. Questa convenzione è valida per le reti virtuali nei cluster di storage che eseguono il software Element. La prima rete virtuale creata in un cluster di elementi ha un ID VirtualNetworkID pari a 1. Questo ID non corrisponde al numero del tag VLAN.

È possibile utilizzare in modo intercambiabile VirtualNetworkID e VirtualNetworkTag (tag VLAN), dove indicato nei metodi API.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddVirtualNetwork

È possibile utilizzare `AddVirtualNetwork` metodo per aggiungere una nuova rete virtuale a una configurazione del cluster.

Quando si aggiunge una rete virtuale, viene creata un'interfaccia per ciascun nodo e ogni interfaccia richiede un indirizzo IP della rete virtuale. Il numero di indirizzi IP specificati come parametro per questo metodo API deve essere uguale o superiore al numero di nodi nel cluster. Il sistema esegue il provisioning in blocco degli indirizzi di rete virtuali e li assegna automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi.

Il metodo AddVirtualNetwork viene utilizzato solo per creare una nuova rete virtuale. Se si desidera apportare modifiche a una rete virtuale esistente, utilizzare ModifyVirtualNetwork metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AddressBllocks	Intervallo univoco di indirizzi IP da includere nella rete virtuale. Membri richiesti per l'oggetto: • Start (inizio): Inizio dell'intervallo di indirizzi IP. (stringa) • Size (dimensione): Il numero di indirizzi IP da includere nel blocco. (intero)	Array di oggetti JSON	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
gateway	L'indirizzo IP di un gateway della rete virtuale. Questo parametro è valido solo se il parametro namespace è impostato su true.	stringa	Nessuno	No
nome	Un nome definito dall'utente per la nuova rete virtuale.	stringa	Nessuno	Sì
namespace	Se impostata su true, attiva la funzionalità delle VLAN di storage instradabili creando e configurando uno spazio dei nomi e la rete virtuale da esso contenuta.	booleano	Nessuno	No
netmask	Maschera di rete univoca per la rete virtuale in fase di creazione.	stringa	Nessuno	Sì
svip	Indirizzo IP dello storage univoco per la rete virtuale creata.	stringa	Nessuno	Sì
VirtualNetworkTag	Un tag VLAN (Virtual Network) univoco. I valori supportati sono compresi tra 1 e 4094.	intero	Nessuno	Sì

Nota: i parametri della rete virtuale devono essere univoci per ogni rete virtuale quando si imposta lo spazio dei nomi su false.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VirtualNetworkID	L'ID della rete virtuale della nuova rete virtuale.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "AddVirtualNetwork",
  "params": {
    "virtualNetworkTag": 2010,
    "name": "network1",
    "addressBlocks" : [
        { "start": "192.86.5.1", "size": 10 },
        { "start": "192.86.5.50", "size": 20 }
    ],
    "netmask" : "255.255.192.0",
    "gateway" : "10.0.1.254",
    "svip" : "192.86.5.200",
    "attributes" : {}
    "namespace" : true
  },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result":
      {
        "virtualNetworkID": 5
   }
}
```

Novità dalla versione

9.6

ModifyVirtualNetwork

È possibile utilizzare `ModifyVirtualNetwork` metodo per modificare gli attributi di una rete virtuale esistente.

Questo metodo consente di aggiungere o rimuovere blocchi di indirizzi, modificare la netmask o modificare il nome o la descrizione della rete virtuale. È inoltre possibile utilizzarlo per attivare o disattivare gli spazi dei nomi, nonché per aggiungere o rimuovere un gateway se gli spazi dei nomi sono attivati sulla rete virtuale.

Questo metodo richiede virtualNetworkID o virtualNetworkTag come parametro, ma non entrambi.

ATTENZIONE:

L'attivazione o la disattivazione della funzionalità delle VLAN di storage instradabili per una rete virtuale esistente modificando il parametro namespace interrompe qualsiasi traffico gestito dalla rete virtuale. Si consiglia di modificare il parametro namespace durante una finestra di manutenzione pianificata.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualNetworkID	Identificatore univoco della rete virtuale da modificare. Si tratta dell'ID della rete virtuale assegnato dal cluster.	intero	Nessuno	No
VirtualNetworkTag	Tag di rete che identifica la rete virtuale da modificare.	intero	Nessuno	No

AddressBllocks	Il nuovo blocco di indirizzi da impostare per questa rete virtuale. Ciò potrebbe includere nuovi blocchi di indirizzi da aggiungere all'oggetto esistente o omettere blocchi di indirizzi inutilizzati che devono essere rimossi. In alternativa, è possibile estendere o ridurre le dimensioni dei blocchi di indirizzi esistenti. È possibile solo aumentare la dimensione degli indirizzi iniziali per un oggetto di rete virtuale; non è possibile ridurla. Membri obbligatori per questo oggetto: • Start (inizio): Inizio dell'intervallo di indirizzi IP. (stringa) • Size (dimensione): Il numero di indirizzi IP da includere nel blocco. (intero)	Oggetto JSON	Nessuno	No
gateway	L'indirizzo IP di un gateway della rete virtuale. Questo parametro è valido solo se il parametro namespace è impostato su true.	stringa	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No

nome	Il nuovo nome della rete virtuale.	stringa	Nessuno	No
namespace	Se impostata su true, attiva la funzionalità delle VLAN di storage instradabili ricreando la rete virtuale e configurando uno spazio dei nomi in modo da contenerla. Se impostata su false, disattiva la funzionalità VRF per la rete virtuale. La modifica di questo valore interrompe il traffico in esecuzione su questa rete virtuale.	booleano	Nessuno	No
netmask	Nuova maschera di rete per questa rete virtuale.	stringa	Nessuno	No
svip	L'indirizzo IP virtuale dello storage per questa rete virtuale. Non è possibile modificare l'SVIP di una rete virtuale. È necessario creare una nuova rete virtuale per utilizzare un indirizzo SVIP diverso.	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyVirtualNetwork",
  "params": {
    "virtualNetworkID": 2,
    "name": "ESX-VLAN-3112",
    "addressBlocks": [
     {
      "start": "10.1.112.1",
      "size": 20
     },
     {
      "start": "10.1.112.100",
      "size": 20
     }
   ],
    "netmask": "255.255.255.0",
    "gateway": "10.0.1.254",
    "svip": "10.1.112.200",
    "attributes": {}
  },
  "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
  }
}
```

Novità dalla versione

9.6

ListVirtualNetworks

È possibile utilizzare `ListVirtualNetworks` metodo per elencare tutte le reti virtuali configurate per il cluster.

È possibile utilizzare questo metodo per verificare le impostazioni della rete virtuale nel cluster. Non sono necessari parametri per questo metodo. Tuttavia, per filtrare i risultati, è possibile passare uno o più valori virtualNetworkID o virtualNetworkTag.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualNetworkID	Network ID (ID di rete) per filtrare l'elenco per una singola rete virtuale.	intero	Nessuno	No
VirtualNetworkTag	Tag di rete per filtrare l'elenco per una singola rete virtuale.	intero	Nessuno	No
VirtualNetworkID	ID di rete da includere nell'elenco.	array intero	Nessuno	No
VirtualNetworkTags	Tag di rete da includere nell'elenco.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VirtualNetworks	Oggetto contenente gli indirizzi IP della rete virtuale.	VirtualNetwork

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVirtualNetworks",
  "params": {
     "virtualNetworkIDs": [5,6]
   },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "virtualNetworks": [
   {
    "addressBlocks": [
   {
    "available": "11000000",
    "size": 8,
    "start": "10.26.250.207"
   }
 ],
    "attributes": null,
    "gateway": "10.26.250.254",
    "name": "2250",
    "namespace": false,
    "netmask": "255.255.255.0",
    "svip": "10.26.250.200",
    "virtualNetworkID": 2250
   },
   {
     "addressBlocks": [
   {
     "available": "11000000",
     "size": 8,
     "start": "10.26.241.207"
   }
  ],
     "attributes": null,
     "gateway": "10.26.241.254",
     "name": "2241",
     "namespace": false,
     "netmask": "255.255.255.0",
     "svip": "10.26.241.200",
     "virtualNetworkID": 2241
   },
  {
     "addressBlocks": [
  {
     "available": "11000000",
     "size": 8,
     "start": "10.26.240.207"
   }
  ],
     "attributes": null,
     "gateway": "10.26.240.254",
```

```
      "name": "2240",
      "namespace": false,
      "netmask": "255.255.255.0",
      "svip": "10.26.240.200",
      "virtualNetworkID": 2240
     },
    {
   }
  ]
}
```

Novità dalla versione

9.6

RemoveVirtualNetwork

È possibile utilizzare `RemoveVirtualNetwork` metodo per rimuovere una rete virtuale aggiunta in precedenza.

Questo metodo richiede virtualNetworkID o virtualNetworkTag come parametro, ma non entrambi.

Non è possibile rimuovere una rete virtuale se vi sono iniziatori associati. Disassociare prima gli iniziatori, quindi rimuovere la rete virtuale.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualNetworkID	ID di rete che identifica la rete virtuale da rimuovere.	intero	Nessuno	Sì
VirtualNetworkTag	Tag di rete che identifica la rete virtuale da rimuovere.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "RemoveVirtualNetwork",
  "params": {
     "virtualNetworkID": 5
    }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {}
}
```

Novità dalla versione

9.6

Metodi API del volume

I metodi API dei volumi software Element consentono di gestire i volumi che risiedono su un nodo di storage. Con questi metodi è possibile creare, modificare, clonare ed eliminare volumi. È inoltre possibile utilizzare i metodi API dei volumi per raccogliere e visualizzare le misurazioni dei dati di un volume.

- CancelClone
- CancelGroupClone
- CloneMultipleVolumes
- CloneVolume
- CopyVolume
- CreateQoSPolicy
- CreateVolume
- CreateBackupTarget
- Policy DeleteQoS
- DeleteVolume
- DeleteVolumes
- GetBackupTarget

- GetVolumeStats
- GetDefaultQoS
- Policy GetQoS
- GetVolumeCount
- GetVolumeEfficiency
- ListActiveVolumes
- ListBackupTargets
- ListBulkVolumeJobs
- ListDeletedVolumes
- ListQoSPolicies
- ListSyncJobs
- ListVolumeQoSIstogrammi
- ListVolumes
- ListVolumeStats
- ListVolumesForAccount
- ListVolumeStatsByAccount
- ListVolumeStatsByVirtualVolume
- ListVolumeStatsByVolume
- ListVolumeStatsByVolumeAccessGroup
- ModifyBackupTarget
- ModifyQoSPolicy
- ModifyVolume
- ModifyVolumes
- PurgeDeletedVolume
- PurgeDeletedVolumes
- RemoveBackupTarget
- RestoreDeletedVolume
- SetDefaultQoS
- StartBulkVolumeRead
- StartBulkVolumeWrite
- UpdateBulkVolumeStatus

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CancelClone

È possibile utilizzare `CancelClone` metodo per arrestare un processo di copia di un volume o di un clone in corso. Quando si annulla un'operazione di cloni di gruppo, il sistema completa e rimuove l'operazione asyncHandle associata.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID cloneID	Il cloneID per il processo di clonazione in corso.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CancelClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

CancelGroupClone

È possibile utilizzare `CancelGroupClone` metodo per arrestare un processo di clonazione in corso su un gruppo di volumi. Quando si annulla un'operazione di cloni di gruppo, il sistema completa e rimuove l'operazione asyncHandle associata.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID groupCloneID	Il cloneID per il processo di clonazione in corso.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CancelGroupClone",
   "params": {
      "cloneID" : 5,
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result" : {}
}
```

Novità dalla versione

9.6

CloneMultipleVolumes

È possibile utilizzare `CloneMultipleVolumes` metodo per creare un clone di un gruppo di volumi specificati. È possibile assegnare un insieme coerente di caratteristiche a un gruppo di volumi multipli quando vengono clonati insieme.

Prima di utilizzare il parametro groupSnapshotID per clonare i volumi in uno snapshot di gruppo, è necessario creare lo snapshot di gruppo utilizzando CreateGroupSnapshot Metodo API o interfaccia utente Web. L'utilizzo di groupSnapshotID è facoltativo quando si clonano più volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Nuovo metodo di accesso predefinito per i nuovi volumi se non sovrascritto dalle informazioni passate nell'array del volume.	stringa	Nessuno	No
EnableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con gli endpoint SnapMirror. Valori possibili: • vero • falso	booleano	falso	No
GroupSnapshotID	ID dello snapshot di gruppo da utilizzare come base per il clone.	intero	Nessuno	No
NewAccountID	Nuovo ID account per i volumi se non sovrascritto dalle informazioni passate nell'array di volumi.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
volumi	Raccolta di membri specificati per i nuovi volumi. Membri: • ID volume: (Obbligatorio) • Access (accesso): (Opzionale) può essere uno dei seguenti: ReadOnly (ReadOnly), Readwrite (lettura), Locked (bloccato) o ReplicationTarget. • Attributi: (Facoltativo) elenco delle coppie nome-valore nel formato oggetto JSON. • Nome: (Opzionale) nuovo nome per il clone. • NewAccountID (ID account): (Facoltativo) ID account per i nuovi volumi. • NewSize (dimensioni nuove): (Opzionale) dimensione totale del volume, in byte. Le dimensioni vengono arrotondate al megabyte più vicino. Se non vengono specificati membri facoltativi, i valori vengono ereditati dai volumi di origine.	Array di oggetti JSON	Nessuno	Sì (ID volume)

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	Valore restituito da una chiamata asincrona al metodo.	intero
ID groupCloneID	ID univoco del nuovo clone di gruppo.	intero
membri	Elenco di ID volume per le coppie di volumi di origine e di destinazione.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CloneMultipleVolumes",
   "params": {
       "volumes": [
           {
              "volumeID": 5
              "name":"foxhill",
              "access":"readOnly"
              },
           {
              "volumeID": 18
              },
           {
             "volumeID": 20
              }
     ]
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 12,
    "groupCloneID": 4,
    "members": [
     {
      "srcVolumeID": 5,
      "volumeID": 29
     },
     {
      "srcVolumeID": 18,
      "volumeID": 30
     },
     {
      "srcVolumeID": 20,
      "volumeID": 31
      }
    ]
  }
}
```


Novità dalla versione

9.6

CloneVolume

È possibile utilizzare `CloneVolume` metodo per creare una copia di un volume. Questo metodo è asincrono e potrebbe richiedere un periodo di tempo variabile.

Il processo di cloning inizia immediatamente quando si crea il `CloneVolume` Richiedere ed è rappresentativo dello stato del volume al momento dell'emissione del metodo API. È possibile utilizzare GetAsyncResult metodo per determinare quando il processo di cloning è completo e il nuovo volume è disponibile per le connessioni. È possibile utilizzare ListSyncJobs per vedere lo stato di avanzamento della creazione del clone. Gli attributi iniziali e le impostazioni della qualità del servizio per il volume vengono ereditati dal volume clonato. È possibile modificare queste impostazioni con ModifyVolume.

> I volumi clonati non ereditano l'appartenenza al gruppo di accesso al volume dal volume di origine.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Accesso consentito per il nuovo volume. Se non viene specificato alcun valore, il valore di accesso non cambia. Valori possibili: • `readOnly`: (Opzionale) sono consentite solo le operazioni di lettura. • `readWrite`: (Opzionale) sono consentite le letture e le scritture. • `locked`: (Opzionale) non sono consentite letture o scritture. Se non specificato, viene utilizzato il valore di accesso del volume clonato. • `replicationTarget`(Facoltativo) identificare un volume come volume di destinazione per un set di volumi accoppiati. Se il volume non è associato, lo stato di accesso è bloccato.	stringa	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
enable512e	Specifica se il nuovo volume deve utilizzare l'emulazione di settore a 512 byte. Se non specificato, viene utilizzata l'impostazione del volume clonato.	booleano	Impostazione del volume originale	No
EnableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con gli endpoint SnapMirror. Valori possibili: • vero • falso	booleano	falso	No
nome	Nome del nuovo volume clonato; deve contenere da 1 a 64 caratteri.	stringa	Nessuno	Sì
NewAccountID	AccountID per il proprietario del nuovo volume. Se non specificato, viene utilizzato l'AccountID del proprietario del volume clonato.	intero	AccountID del proprietario del volume originale	No
NewSize	Nuove dimensioni del volume, in byte. Potrebbe essere maggiore o minore della dimensione del volume clonato. Se non specificato, le dimensioni del volume non vengono modificate. La dimensione viene arrotondata alla dimensione più vicina di 1 MB.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapshotID	ID dello snapshot utilizzato come origine del clone. Se non viene fornito alcun ID, viene utilizzato il volume attivo corrente.	intero	Nessuno	No
ID volume	VolumeID per il volume da clonare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	Il valore handle utilizzato per ottenere il risultato dell'operazione.	intero
ID cloneID	Il cloneID per il volume appena clonato.	intero
curva	I valori della curva QoS applicati al clone.	Oggetto JSON
volume	Oggetto contenente informazioni sul volume appena clonato.	volume
ID volume	VolumeID per il volume appena clonato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CloneVolume",
   "params": {
      "volumeID" : 5,
      "name"  : "mysqldata-snapshot1",
      "access" : "readOnly"
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:


```
{
  "id": 1,
  "result": {
      "asyncHandle": 42,
      "cloneID": 37,
      "volume": {
          "access": "readOnly",
          "accountID": 1,
          "attributes": {},
          "blockSize": 4096,
          "createTime": "2016-03-31T22:26:03Z",
          "deleteTime": "",
          "enable512e": true,
          "iqn": "iqn.2010-01.com.solidfire:jyay.mysqldata-snapshot1.680",
          "name": "mysqldata-snapshot1",
          "purgeTime": "",
          "qos": {
              "burstIOPS": 100,
              "burstTime": 60,
              "curve": {
                  "4096": 100,
                  "8192": 160,
                  "16384": 270,
                  "32768": 500,
                  "65536": 1000,
                  "131072": 1950,
                  "262144": 3900,
                  "524288": 7600,
                  "1048576": 15000
              },
              "maxIOPS": 100,
              "minIOPS": 50
          },
          "scsiEUIDeviceID": "6a796179000002a8f47acc0100000000",
          "scsiNAADeviceID": "6f47acc1000000006a796179000002a8",
          "sliceCount": 0,
          "status": "init",
          "totalSize": 1000341504,
          "virtualVolumeID": null,
          "volumeAccessGroups": [],
          "volumeID": 680,
          "volumePairs": []
```

```
        },
        "volumeID": 680
    }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListSyncJobs
- ModifyVolume

CopyVolume

È possibile utilizzare `CopyVolume` metodo per sovrascrivere il contenuto dei dati di un volume esistente con il contenuto dei dati di un altro volume (o snapshot). Gli attributi del volume di destinazione come IQN, le impostazioni QoS, le dimensioni, l'account e l'appartenenza al gruppo di accesso al volume non vengono modificati. Il volume di destinazione deve già esistere e avere le stesse dimensioni del volume di origine.

È consigliabile che i client smontino il volume di destinazione prima dell'inizio dell'operazione. Se il volume di destinazione viene modificato durante l'operazione, le modifiche andranno perse. Il completamento di questa operazione può richiedere una quantità variabile di tempo. È possibile utilizzare GetAsyncResult metodo per determinare quando il processo è terminato, e. ListSyncJobs per visualizzare l'avanzamento della copia.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
DstVolumeID	VolumeID del volume da sovrascrivere.	intero	Nessuno	Sì
ID volume	VolumeID del volume da cui si desidera leggere.	intero	Nessuno	Sì
SnapshotID	ID dello snapshot utilizzato come origine del clone. Se non viene fornito alcun ID, viene utilizzato il volume attivo corrente.	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero
ID cloneID	CloneID per il volume appena clonato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CopyVolume",
   "params": {
      "volumeID" : 3,
      "dstVolumeID" : 2
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 9,
    "cloneID": 5
  }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListSyncJobs

CreateQoSPolicy

È possibile utilizzare `CreateQoSPolicy` Metodo per creare un oggetto QoSPolicy che sarà possibile applicare in seguito a un volume al momento della creazione o della modifica. Un criterio QoS ha un ID univoco, un nome e impostazioni QoS.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Il nome del criterio QoS, ad esempio oro, platino o argento.	stringa	Nessuno	Sì
qos	Le impostazioni QoS rappresentate da questo criterio.	QoS	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
QosPolicy	Oggetto QoSPolicy appena creato.	QoSPolicy

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 68,
  "method": "CreateQoSPolicy",
  "params": {
    "name": "bronze",
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 15000,
      "burstIOPS": 15000
    }
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 68,
  "result": {
    "qosPolicy": {
      "name": "bronze",
      "qos": {
        "burstIOPS": 15000,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 15000,
        "minIOPS": 50
      },
      "qosPolicyID": 2,
      "volumeIDs": []
    }
  }
}
```

Novità dalla versione

10.0

CreateVolume

È possibile utilizzare `CreateVolume` metodo per creare un nuovo volume vuoto nel cluster. Non appena il volume viene creato, il volume è disponibile per la connessione tramite iSCSI.

I volumi creati senza valori QoS specificati utilizzano i valori predefiniti. È possibile visualizzare i valori predefiniti di un volume utilizzando `GetDefaultQoS` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`access`	La modalità di accesso per il volume. Se questo parametro è incluso, l'unico valore supportato è `snapMirrorTarget`.	stringa	Nessuno	No
`accountID`	L'ID dell'account proprietario di questo volume.	intero	Nessuno	Sì
`associateWithQoSPolicy`	Associare il volume al criterio QoS specificato. Valori possibili: • `true`: Associare il volume al criterio QoS specificato nel parametro QoSPolicyID. • `false`: Non associare il volume al criterio QoS specificato nel parametro QoSPolicyID. Se false, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi o meno un policy QoS nel parametro QoSPolicy.	booleano	vero	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`attributes`	Elenco delle coppie nome-valore nel formato oggetto JSON. La dimensione totale dell'attributo deve essere inferiore a 1000B o 1KB, inclusi i caratteri di formattazione JSON.	Oggetto JSON	Nessuno	No
`enable512e`	Abilitare l'emulazione di settore a 512 byte. Valori possibili: • `true`: Il volume fornisce l'emulazione di settore a 512 byte. • `false`: l'emulazione 512e non è abilitata.	booleano	Nessuno	Sì
`enableSnapMirrorReplication`	Determina se il volume può essere utilizzato per la replica con gli endpoint SnapMirror. Valori possibili: • `true` • `false`	booleano	falso	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`fifoSize`	Specifica il numero massimo di snapshot first-in-first-out (FIFO) supportati dal volume. Si noti che gli snapshot FIFO e non FIFO utilizzano entrambi lo stesso pool di slot di snapshot disponibili su un volume. Utilizzare questa opzione per limitare il consumo di snapshot FIFO degli slot snapshot disponibili. Se omesso, il valore predefinito è 24.	intero	24	No
`minFifoSize`	Specifica il numero minimo di slot di snapshot FIFO (first-in-first-out) riservati dal volume. In questo modo, se si utilizzano snapshot FIFO e snapshot non FIFO su un volume, gli snapshot non FIFO non consumano involontariamente troppi slot FIFO. Inoltre, garantisce che almeno questo numero di snapshot FIFO sia sempre disponibile. Poiché le snapshot FIFO e non FIFO condividono lo stesso pool, il `minFifoSize` Riduce il numero totale di possibili snapshot non FIFO della stessa quantità. Se omesso, il valore predefinito è 0.	intero	0	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`name`	Nome del gruppo di accesso al volume (può essere specificato dall'utente). Non è necessario essere unici, ma consigliato. La lunghezza deve essere compresa tra 1 e 64 caratteri.	stringa	Nessuno	Sì
`qos`	Le impostazioni iniziali della qualità del servizio per questo volume. I valori predefiniti vengono utilizzati se non sono specificati. Valori possibili: • `minIOPS` • `maxIOPS` • `burstIOPS`	Oggetto QoS	Nessuno	No
`qosPolicyID`	ID del criterio le cui impostazioni QoS devono essere applicate ai volumi specificati. Questo parametro si esclude reciprocamente con `qos` parametro.	intero	Nessuno	No
`totalSize`	Dimensione totale del volume, in byte. Le dimensioni vengono arrotondate al megabyte più vicino.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
volume	Oggetto contenente informazioni sul volume appena creato.	volume

ID volume	ID volume per il volume appena creato.	intero
curva	La curva è un insieme di coppie chiave-valore. Le chiavi sono le dimensioni i/o in byte. I valori rappresentano il costo dell'esecuzione di un IOP a una dimensione i/o specifica. La curva viene calcolata in relazione a un'operazione di 4096 byte impostata su 100 IOPS.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CreateVolume",
   "params": {
      "name": "mysqldata",
      "accountID": 1,
      "totalSize": 107374182400,
      "enable512e": false,
      "attributes": {
         "name1": "value1",
         "name2": "value2",
         "name3": "value3"
      },
      "qos": {
         "minIOPS": 50,
         "maxIOPS": 500,
         "burstIOPS": 1500,
         "burstTime": 60
      }
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
```

```
        "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
        },
        "volume": {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {
                "name1": "value1",
                "name2": "value2",
                "name3": "value3"
            },
            "blockSize": 4096,
            "createTime": "2016-03-31T22:20:22Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:mysqldata.677",
            "name": "mysqldata",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 500,
                "minIOPS": 50
            },
            "scsiEUIDeviceID": "6a796179000002a5f47acc0100000000",
            "scsiNAADeviceID": "6f47acc1000000006a796179000002a5",
            "sliceCount": 0,
```

```
            "status": "active",
            "totalSize": 107374182400,
            "virtualVolumeID": null,
            "volumeAccessGroups": [],
            "volumeID": 677,
            "volumePairs": []
        },
        "volumeID": 677
    }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

GetDefaultQoS

CreateBackupTarget

È possibile utilizzare `CreateBackupTarget` per creare e memorizzare le informazioni di destinazione del backup in modo che non sia necessario reimmetterle ogni volta che viene creato un backup.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Nome della destinazione del backup.	stringa	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	Sì (ma può essere vuoto)

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
BackupTargetID	Identificatore univoco assegnato alla nuova destinazione di backup.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CreateBackupTarget",
   "params": {
      "name": "mytargetbackup"
   },
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
      "backupTargetID": 1
   }
}
```

Novità dalla versione

9.6

Policy DeleteQoS

È possibile utilizzare `DeleteQoSPolicy` Metodo per eliminare un criterio QoS dal sistema. Le impostazioni di QoS per tutti i volumi creati o modificati con questo criterio non sono influenzate.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
QosPolicyID	L'ID del criterio QoS da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 663,
  "method": "DeleteQoSPolicy",
  "params": {
    "qosPolicyID": 4
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 663,
  "result": {}
}
```

Novità dalla versione

9.6

DeleteVolume

È possibile utilizzare `DeleteVolume` metodo per contrassegnare un volume attivo per l'eliminazione. Se contrassegnato, il volume viene eliminato (cancellato in modo permanente) allo scadere dell'intervallo di pulizia.

Dopo aver richiesto di eliminare un volume, tutte le connessioni iSCSI attive al volume vengono immediatamente interrotte e non sono consentite ulteriori connessioni mentre il volume si trova in questo stato. Un volume contrassegnato non viene restituito nelle richieste di rilevamento di destinazione.

Gli snapshot di un volume che sono stati contrassegnati per l'eliminazione non sono interessati. Le snapshot vengono conservate fino a quando il volume non viene spurgato dal sistema. Se un volume è contrassegnato per l'eliminazione e dispone di un'operazione di lettura o scrittura di volumi in blocco in corso, l'operazione di lettura o scrittura di volumi in blocco viene interrotta.

Se il volume eliminato è associato a un volume, la replica tra i volumi accoppiati viene sospesa e non viene trasferito alcun dato su di esso o da esso mentre si trova in uno stato cancellato. Il volume remoto con cui è stato associato il volume cancellato entra in uno stato PausedMisconfigured e i dati non vengono più inviati ad esso o dal volume cancellato. Fino a quando il volume cancellato non viene eliminato, può essere ripristinato e il trasferimento dei dati riprende. Se il volume cancellato viene rimosso dal sistema, il volume con cui è stato associato entra in uno stato StoppedMisconfigured (StoppedMisconfigurato) e lo stato di associazione del volume viene rimosso. Il volume eliminato diventa permanentemente non disponibile.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	L'ID del volume da eliminare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
volume	Oggetto contenente informazioni sul volume cancellato.	volume
ID volume	L'ID volume del volume cancellato.	intero
curva	La curva è un insieme di coppie chiave-valore. Le chiavi sono le dimensioni i/o in byte. I valori rappresentano il costo dell'esecuzione di un IOP a una dimensione i/o specifica. La curva viene calcolata in relazione a un'operazione di 4096 byte impostata su 100 IOPS.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
```

```
  "result": {
    "volume": {
      "access": "readWrite",
      "accountID": 1,
      "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
      },
      "blockSize": 4096,
      "createTime": "2016-03-28T16:16:13Z",
      "deleteTime": "2016-03-31T22:59:42Z",
      "enable512e": true,
      "iqn": "iqn.2010-01.com.solidfire:jyay.1459181777648.5",
      "name": "1459181777648",
      "purgeTime": "2016-04-01T06:59:42Z",
      "qos": {
        "burstIOPS": 150,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 100,
        "minIOPS": 60
      },
      "scsiEUIDeviceID": "6a79617900000005f47acc0100000000",
      "scsiNAADeviceID": "6f47acc1000000006a79617900000005",
      "sliceCount": 1,
      "status": "deleted",
      "totalSize": 1000341504,
      "virtualVolumeID": null,
      "volumeAccessGroups": [
        1
      ],
      "volumeID": 5,
      "volumePairs": []
    }
  }
```

```
}
```

Novità dalla versione

9.6

DeleteVolumes

È possibile utilizzare `DeleteVolumes` metodo per contrassegnare più (fino a 500) volumi attivi per l'eliminazione. Se contrassegnato, il volume viene eliminato (cancellato in modo permanente) allo scadere dell'intervallo di pulizia.

Dopo aver richiesto di eliminare i volumi, tutte le connessioni iSCSI attive ai volumi vengono immediatamente interrotte e non sono consentite ulteriori connessioni mentre i volumi si trovano in questo stato. Un volume contrassegnato non viene restituito nelle richieste di rilevamento di destinazione.

Gli snapshot di un volume che sono stati contrassegnati per l'eliminazione non sono interessati. Le snapshot vengono conservate fino a quando il volume non viene spurgato dal sistema. Se un volume è contrassegnato per l'eliminazione e dispone di un'operazione di lettura o scrittura di volumi in blocco in corso, l'operazione di lettura o scrittura di volumi in blocco viene interrotta.

Se i volumi eliminati sono associati a un volume, la replica tra i volumi accoppiati viene sospesa e non viene trasferito alcun dato su di essi o da essi mentre si trova in uno stato cancellato. I volumi remoti con cui i volumi cancellati sono stati associati a Enter in uno stato PausedMisconfigured e i dati non vengono più inviati a essi o dai volumi cancellati. Fino alla rimozione dei volumi cancellati, è possibile ripristinarli e riprendere il trasferimento dei dati. Se i volumi cancellati vengono rimossi dal sistema, i volumi con cui sono stati associati entrano in uno stato StoppedMisconfigured e lo stato di associazione del volume viene rimosso. I volumi rimossi diventano permanentemente non disponibili.

Parametri

Questo metodo ha i seguenti parametri di input.

> Almeno uno dei seguenti parametri è obbligatorio ed è necessario utilizzare solo uno dei parametri (tutti si escludono a vicenda).

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	L'elenco degli ID dei volumi da eliminare dal sistema.	array intero	Nessuno	Vedere la nota.
VolumeAccessGroupID	Elenco degli ID dei gruppi di accesso al volume. Tutti i volumi di tutti i gruppi di accesso ai volumi specificati in questo elenco vengono eliminati dal sistema.	array intero	Nessuno	Vedere la nota.

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
AccountID	Un elenco di ID account. Tutti i volumi di questi account vengono cancellati dal sistema.	array intero	Nessuno	Vedere la nota.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
volumi	Informazioni sul volume appena cancellato.	volume
curva	La curva è un insieme di coppie chiave-valore. Le chiavi sono le dimensioni i/o in byte. I valori rappresentano il costo dell'esecuzione di un IOP a una dimensione i/o specifica. La curva viene calcolata in relazione a un'operazione di 4096 byte impostata su 100 IOPS.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result": {
    "volumes" : [ {
      "access": "readWrite",
      "accountID": 1,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2015-03-06T18:50:56Z",
      "deleteTime": "",
      "enable512e": False,
      "iqn": "iqn.2010-01.com.solidfire:pzsr.vclient-030-v00001.1",
      "name": "vclient-030-v00001",
      "qos": {
        "burstIOPS": 15000,
        "burstTime": 60,
        "curve": {},
        "maxIOPS": 15000,
        "minIOPS": 100
      },
      "purgeTime": "",
      "sliceCount": 1,
      "scsiEUIDeviceID": "707a737200000001f47acc0100000000",
      "scsiNAADeviceID": "6f47acc100000000707a737200000001",
      "status": "active",
      "totalSize": 10000003072,
      "virtualVolumeID": 5,
      "volumeAccessGroups": [],
      "volumePairs": [],
      "volumeID": 1
    } ]
  }
}
```


Novità dalla versione

9.6

GetBackupTarget

È possibile utilizzare `GetBackupTarget` metodo per restituire informazioni su una destinazione di backup specifica creata.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
BackupTargetID	Identificatore univoco assegnato alla destinazione del backup.	intero	Nessuno	Sì
nome	Nome della destinazione del backup.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
Destinazione di backupTarget	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1,
  "method": "GetBackupTarget",
  "params": {
      "backupTargetID": 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "backupTarget": {
     "attributes" : {
        "size" : 100
     },
     "backupTargetID" : 1,
     "name" : "mytargetbackup"
    }
  }
}
```

Novità dalla versione

9.6

GetVolumeStats

È possibile utilizzare `GetVolumeStats` metodo per ottenere misurazioni di attività di alto livello per un singolo volume. I valori sono cumulativi dalla creazione del volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Specifica il volume per il quale vengono raccolte le statistiche.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Informazioni sull'attività del volume.	VolumeStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetVolumeStats",
   "params": {
      "volumeID": 32
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeStats": {
      "accountID": 1,
      "actualIOPS": 0,
      "asyncDelay": null,
      "averageIOPSize": 0,
      "burstIOPSCredit": 0,
      "clientQueueDepth": 0,
      "desiredMetadataHosts": null,
      "latencyUSec": 0,
      "metadataHosts": {
        "deadSecondaries": [],
        "liveSecondaries": [
          32
        ],
        "primary": 60
      },
      "nonZeroBlocks": 0,
      "readBytes": 0,
      "readBytesLastSample": 0,
      "readLatencyUSec": 0,
      "readOps": 0,
      "readOpsLastSample": 0,
      "samplePeriodMSec": 0,
      "throttle": 0,
      "timestamp": "2016-04-01T21:01:39.130840Z",
      "unalignedReads": 0,
      "unalignedWrites": 0,
      "volumeAccessGroups": [],
      "volumeID": 1,
      "volumeSize": 5000658944,
      "volumeUtilization": 0,
      "writeBytes": 0,
      "writeBytesLastSample": 0,
      "writeLatencyUSec": 0,
      "writeOps": 0,
      "writeOpsLastSample": 0,
      "zeroBlocks": 1220864
    }
  }
}
```

Novità dalla versione

9.6

GetDefaultQoS

È possibile utilizzare `GetDefaultQoS` Metodo per ottenere i valori di qualità del servizio (QoS) predefiniti per un volume appena creato.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
QoS	I valori QoS predefiniti.	QoS

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetDefaultQoS",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "burstIOPS" : 15000,
      "burstTime" : 60,
      "curve" : {
         "1048576" : 15000,
         "131072" : 1900,
         "16384" : 270,
         "262144" : 3000,
         "32768" : 500,
         "4096" : 100,
         "524288" : 7500,
         "65536" : 1000,
         "8192" : 160
      },
      "maxIOPS" : 15000,
      "minIOPS" : 100
   }
}
```

Novità dalla versione

9.6

Policy GetQoS

È possibile utilizzare `GetQoSPolicy` Metodo per ottenere dettagli su una policy QoS specifica dal sistema.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
QosPolicyID	L'ID del criterio da recuperare.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
QosPolicy	Dettagli della policy QoS richiesta.	QoSPolicy

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "GetQoSPolicy",
    "params": {
        "qosPolicyID": 2
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "qosPolicy": {
      "name": "bronze",
      "qos": {
        "burstIOPS": 15002,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 15002,
        "minIOPS": 51
      },
      "qosPolicyID": 2,
      "volumeIDs": [
          2
      ]
    }
  }
}
```

Novità dalla versione

10.0

GetVolumeCount

È possibile utilizzare `GetVolumeCount` metodo per ottenere il numero di volumi attualmente presenti nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
conta	Il numero di volumi attualmente presenti nel sistema.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetVolumeCount",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "count": 7
  }
}
```

Novità dalla versione

9.6

GetVolumeEfficiency

È possibile utilizzare `GetVolumeEfficiency` metodo per ottenere informazioni su un volume. Per calcolare la capacità viene utilizzato solo il volume indicato come parametro in questo metodo API.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Specifica il volume per il quale viene calcolata la capacità.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
compressione	La quantità di spazio salvata comprimendo i dati su un singolo volume. Indicato come rapporto, dove 1 indica che i dati sono stati memorizzati senza essere compressi.	fluttuare
deduplica	La quantità di spazio salvata su un singolo volume non duplicando i dati. Indicato come rapporto.	fluttuare
MissingVolumes	I volumi che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati da una raccolta di rifiuti (GC) di meno di un'ora, da una perdita temporanea di rete o da servizi riavviati dal ciclo GC.	array intero
ThinProvisioning	Il rapporto tra lo spazio utilizzato e la quantità di spazio allocato per la memorizzazione dei dati. Indicato come rapporto.	fluttuare
data e ora	L'ultima volta in cui sono stati raccolti i dati di efficienza dopo GC.	Stringa di dati ISO 8601

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetVolumeEfficiency",
   "params": {
      "volumeID": 606
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
       "compression": 2.001591240821456,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T16:06:33Z"
   }
}
```

Novità dalla versione

9.6

ListActiveVolumes

È possibile utilizzare `ListActiveVolumes` metodo per ottenere l'elenco dei volumi attivi attualmente nel sistema. L'elenco dei volumi viene ordinato in ordine VolumeID e può essere restituito in più parti (pagine).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No
StartVolumeID	Avvio di VolumeID per la restituzione. Se non esiste alcun volume con questo VolumeID, il volume successivo per ordine VolumeID viene utilizzato come inizio dell'elenco. Per scorrere l'elenco, passare il VolumeID dell'ultimo volume nella risposta precedente + 1.	intero	0	No
limite	Numero massimo di oggetti info volume da restituire. 0 (zero) restituisce tutti i volumi (senza limiti).	intero	(senza limiti)	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi attivi.	volume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListActiveVolumes",
   "params": {
      "startVolumeID"  : 0,
      "limit" : 1000
   },
   "id" : 1
}
```

Esempio di risposta

A causa della lunghezza di questo esempio di risposta, è documentata in un argomento supplementare.

Novità dalla versione

9.6

ListBackupTargets

È possibile utilizzare `ListBackupTargets` metodo per ottenere informazioni su tutte le destinazioni di backup create.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
BackupTargets	Oggetti restituiti per ciascuna destinazione di backup. Oggetti inclusi: • Attributi: Elenco delle coppie nome-valore nel formato oggetto JSON. (Oggetto JSON) • BackupTargetID: Identificatore univoco assegnato alla destinazione del backup. (intero) • Name (Nome): Nome della destinazione del backup. (stringa)	Oggetto JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListBackupTargets",
   "params": {},
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
     "backupTargets": [
       {
        "attributes" : {},
        "backupTargetID" : 1,
        "name" : "mytargetbackup"
       }
    ]
  }
}
```

Novità dalla versione

9.6

ListBulkVolumeJobs

È possibile utilizzare `ListBulkVolumeJobs` metodo per ottenere informazioni su ogni operazione di lettura o scrittura di volumi in blocco che si verifica nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
BulkVolumeJobs	Una matrice di informazioni per ogni processo di volume in blocco.	BulkVolumeJob array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListBulkVolumeJobs",
   "params": {
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "bulkVolumeJobs": [
        {
          "attributes": {
            "blocksPerTransfer": 1024,
            "firstPendingLba": 216064,
            "nLbas": 2441472,
            "nextLba": 226304,
            "pendingLbas": "[220160, 223232, 221184, 224256, 217088,
225280, 222208, 218112, 219136, 216064]",
            "percentComplete": 8,
            "startLba": 0
          },
          "bulkVolumeID": 2,
          "createTime": "2015-05-07T14:52:17Z",
          "elapsedTime": 44,
          "format": "native",
          "key": "eaffb0526d4fb47107061f09bfc9a806",
          "percentComplete": 8,
          "remainingTime": 506,
          "script": "bv_internal.py",
          "snapshotID": 509,
          "srcVolumeID": 3,
          "status": "running",
          "type": "read"
        }
      ]
   }
}
```


Novità dalla versione

9.6

ListDeletedVolumes

È possibile utilizzare `ListDeletedVolumes` metodo per recuperare l'elenco dei volumi contrassegnati per l'eliminazione e rimossi dal sistema.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi cancellati.	volume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListDeletedVolumes",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Le risposte per questo metodo sono simili al seguente esempio:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 2,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2018-06-24T03:13:13Z",
                "deleteTime": "2018-07-22T16:12:39Z",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:0oto.deletethis.23",
                "name": "deleteThis",
                "purgeTime": "2016-07-23T00:12:39Z",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000017f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000017",
                "sliceCount": 1,
                "status": "deleted",
                "totalSize": 1396703232,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 23,
                "volumePairs": []
            }
        ]
    }
}
```

Novità dalla versione

9.6

ListQoSPolicies

È possibile utilizzare `ListQoSPolicies` Metodo per elencare le impostazioni di tutti i criteri QoS sul sistema.

Parametri

Questo metodo non ha parametri di input.

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
QosPolicies	Un elenco di dettagli su ogni policy QoS.	QoSPolicy array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 231,
  "method": "ListQoSPolicies",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 231,
  "result": {
    "qosPolicies": [
      {
        "name": "silver",
        "qos": {
          "burstIOPS": 15000,
          "burstTime": 60,
          "curve": {
            "4096": 100,
```

```
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 14000,
          "minIOPS": 50
        },
        "qosPolicyID": 1,
        "volumeIDs": [
          1
        ]
      },
      {
        "name": "bronze",
        "qos": {
          "burstIOPS": 15000,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 15000,
          "minIOPS": 50
        },
        "qosPolicyID": 2,
        "volumeIDs": [
          2
        ]
      }
    ]
  }
}
```

Novità dalla versione

10.0

ListSyncJobs

È possibile utilizzare `ListSyncJobs` Metodo per ottenere informazioni sui processi di sincronizzazione in esecuzione in un cluster di storage Element. Questo metodo restituisce informazioni su sezioni, cloni, blocchi e processi di sincronizzazione remota.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
SyncJobs	Elenco degli oggetti che descrivono i processi di sincronizzazione attualmente in esecuzione nel sistema.	SyncJob array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListSyncJobs",
   "params": { },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id":1,
    "result":{
      "syncJobs":[
        {
           "bytesPerSecond":275314.8834458956,
           "currentBytes":178257920,
           "dstServiceID":36,
           "elapsedTime":289.4568382049871,
```

```
            "percentComplete":8.900523560209423,
            "remainingTime":2962.675921065957,
            "sliceID":5,
            "srcServiceID":16,
            "stage":"whole",
            "totalBytes":2002780160,
            "type":"slice"
        },
        {
            "bytesPerSecond":305461.3198607744,
            "cloneID":1,
            "currentBytes":81788928,
            "dstServiceID":16,
            "dstVolumeID":6,
            "elapsedTime":291.7847648200743,
            "nodeID":1,
            "percentComplete":8.167539267015707,
            "remainingTime":3280.708270981153,
            "sliceID":6,
            "srcServiceID":16,
            "srcVolumeID":5,
            "stage":"whole",
            "totalBytes":1001390080,
            "type":"clone"
         },
         {
            "blocksPerSecond":0,
            "branchType": "snapshot",
            "dstServiceID":8,
            "dstVolumeID":2,
            "elapsedTime":0,
            "percentComplete":0,
            "remainingTime":0,
            "sliceID":2,
            "stage":"metadata",
            "type":"remote"
        }
      ]
    }
}
```


Novità dalla versione

9.6

ListVolumeQoSIstogrammi

È possibile utilizzare `ListVolumeQoSHistograms` Metodo per generare un istogramma dell'utilizzo della QoS del volume per uno o più volumi. Ciò consente di comprendere meglio come i volumi utilizzano la QoS.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Un elenco opzionale di ID volume che specifica quali volumi devono avere istogrammi QoS generati.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
QosIstogrammi	Un elenco di oggetti che descrivono l'utilizzo di un volume per uno o più volumi.	Array di oggetti JSON

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
    "method": "ListVolumeQoSHistograms",
        "params": {
            "volumeIDs": [1]
        },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
```

```
        "qosHistograms": [
        {
            "histograms": {
            "belowMinIopsPercentages": {
                "Bucket1To19": 2406,
                "Bucket20To39": 3,
                "Bucket40To59": 0,
                "Bucket60To79": 4,
                "Bucket80To100": 0
            },
                "minToMaxIopsPercentages": {
                "Bucket101Plus": 0,
                "Bucket1To19": 0,
                "Bucket20To39": 0,
                "Bucket40To59": 2,
                "Bucket60To79": 0,
                "Bucket80To100": 0
            },
                "readBlockSizes": {
                "Bucket131072Plus": 0,
                "Bucket16384To32767": 0,
                "Bucket32768To65535": 0,
                "Bucket4096To8191": 0,
                "Bucket65536To131071": 0,
                "Bucket8192To16383": 0
            },
                "targetUtilizationPercentages": {
                "Bucket0": 134943,
                "Bucket101Plus": 0,
                "Bucket1To19": 2409,
                "Bucket20To39": 4,
                "Bucket40To59": 0,
                "Bucket60To79": 2,
                "Bucket80To100": 0
            },
                "throttlePercentages": {
                "Bucket0": 137358,
                "Bucket1To19": 0,
                "Bucket20To39": 0,
                "Bucket40To59": 0,
                "Bucket60To79": 0,
                "Bucket80To100": 0
            },
                "writeBlockSizes": {
                "Bucket131072Plus": 0,
                "Bucket16384To32767": 0,
```

```
                "Bucket32768To65535": 0,
                "Bucket4096To8191": 0,
                "Bucket65536To131071": 0,
                "Bucket8192To16383": 0
            }
        },
            "timestamp": "2018-06-21T18:45:52.010844Z",
            "volumeID": 1
        }
    ]
}
}
```

ListVolumes

È possibile utilizzare `ListVolumes` metodo per ottenere un elenco di volumi che si trovano in un cluster. È possibile specificare i volumi che si desidera restituire nell'elenco utilizzando i parametri disponibili.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
account	Vengono restituiti solo i volumi di proprietà degli account specificati qui. Si escludono a vicenda con il parametro volumeIDS.	array intero	Nessuno	No
Include VirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
IsPaired	Restituisce volumi che sono associati o non associati. Valori possibili: • True: Restituisce tutti i volumi accoppiati. • Falso: Restituisce tutti i volumi non associati.	booleano	Nessuno	No
limite	Consente di impostare il numero massimo di risultati del volume restituiti. Si escludono a vicenda con il parametro volumeIDS.	intero	10000	No
StartVolumeID	Vengono restituiti solo i volumi con un ID maggiore o uguale a questo valore. Si escludono a vicenda con il parametro volumeIDS.	intero	Nessuno	No
ID volume	Un elenco di ID volume. Se si specifica questo parametro, gli altri parametri funzionano solo su questo set di volumi. Si escludono a vicenda con i parametri account, startVolumeID e Limit.	array intero	No	No
VolumeName	Vengono restituite solo le informazioni dell'oggetto volume corrispondenti al nome del volume.	stringa	No	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeStatus (Stato volume)	Vengono restituiti solo i volumi con uno stato uguale al valore di stato. Valori possibili: • creazione in corso • scatto • attivo • cancellato	stringa	No	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi.	volume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVolumes",
    "params": {
        "volumeIDs": [1],
        "volumeStatus": "active",
        "isPaired": "false"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-03-28T14:39:05Z",
                "deleteTime": "",
                "enable512e": true,
                "iqn": "iqn.2010-01.com.solidfire:testvolume1.1",
                "name": "testVolume1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "6a79617900000001f47acc0100000000",
                "scsiNAADeviceID": "6f47acc1000000006a79617900000001",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 5000658944,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 1,
                "volumePairs": []
            }
        ]
    }
}
```

Novità dalla versione

9.6

ListVolumeStats

È possibile utilizzare `ListVolumeStats` Metodo per ottenere misurazioni di attività di alto livello per un singolo volume, un elenco di volumi o tutti i volumi (se si omette il parametro volumeID). I valori di misurazione sono cumulativi dalla creazione del volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No
ID volume	Un elenco di volumi da cui recuperare le informazioni sulle attività.	array intero	No	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Elenco delle informazioni sull'attività del volume.	VolumeStats array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVolumeStats",
    "params": {
        "volumeIDs": [1]
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 1,
        "actualIOPS": 0,
        "asyncDelay": null,
        "averageIOPSize": 0,
        "burstIOPSCredit": 30000,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 0,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
            47
          ],
          "primary": 33
        },
        "nonZeroBlocks": 22080699,
        "readBytes": 657262370816,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readOps": 160464446,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "throttle": 0,
        "timestamp": "2016-03-09T19:39:15.771697Z",
        "unalignedReads": 0,
        "unalignedWrites": 0,
        "volumeAccessGroups": [
          1
```

```
        ],
        "volumeID": 1,
        "volumeSize": 107374182400,
        "volumeUtilization": 0,
        "writeBytes": 219117547520,
        "writeBytesLastSample": 0,
        "writeLatencyUSec": 0,
        "writeOps": 53495495,
        "writeOpsLastSample": 0,
        "zeroBlocks": 4133701
      }
    ]
  }
}
```


Novità dalla versione

9.6

ListVolumesForAccount

È possibile utilizzare `ListVolumesForAccount` metodo per elencare i volumi attivi e (in sospeso) cancellati per un account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No
ID account	Vengono restituiti tutti i volumi di proprietà di questo ID account.	intero	No	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo

volumi	Elenco delle informazioni sul volume.	volume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListVolumesForAccount",
   "params": {
      "accountID"  : 1
   },
   "id" : 1
}
```

Esempio di risposta

Le risposte per questo metodo sono simili al seguente esempio:

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2018-07-22T16:15:25Z",
                "deleteTime": "",
                "enable512e": false,
                "iqn": "iqn.2010-01.com.solidfire:0oto.test1.25",
                "name": "test1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 15000,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 15000,
                    "minIOPS": 50
                },
                "scsiEUIDeviceID": "306f746f00000019f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000019",
                "sliceCount": 1,
                "status": "active",
                "totalSize": 1000341504,
                "virtualVolumeID": null,
                "volumeAccessGroups": [],
                "volumeID": 25,
                "volumePairs": []
            }
        ]
    }
}
```

Novità dalla versione

9.6

ListVolumeStatsByAccount

È possibile utilizzare `ListVolumeStatsByAccount` metodo per elencare le misurazioni di volume di attività di alto livello per ogni account. I valori vengono sommati da tutti i volumi di proprietà dell'account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No
account	Un elenco di ID account per i quali restituire le statistiche del volume. Se omesso, vengono restituite le statistiche per tutti gli account.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Elenco delle informazioni sulle attività di volume per ciascun account.**Nota:** il membro volumeID è 0 per ogni voce, in quanto i valori rappresentano la somma di tutti i volumi di proprietà dell'account.	VolumeStats array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "ListVolumeStatsByAccount",
  "params": {"accounts": [3]},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 3,
        "nonZeroBlocks": 155040175,
        "readBytes": 3156273328128,
        "readBytesLastSample": 0,
        "readOps": 770574543,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "timestamp": "2016-10-17T20:42:26.231661Z",
        "unalignedReads": 0,
        "unalignedWrites": 0,
        "volumeAccessGroups": [],
        "volumeID": 0,
        "volumeSize": 1127428915200,
        "writeBytes": 1051988406272,
        "writeBytesLastSample": 0,
        "writeOps": 256833107,
        "writeOpsLastSample": 0,
        "zeroBlocks": 120211025
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListVolumeStatsByVirtualVolume

È possibile utilizzare `ListVolumeStatsByVirtualVolume` metodo per elencare le

statistiche dei volumi per tutti i volumi del sistema associati al volume virtuale. Le statistiche sono cumulative a partire dalla creazione del volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualVolumeID	Elenco di uno o più ID di volumi virtuali per i quali recuperare le informazioni. Se si specifica questo parametro, il metodo restituisce informazioni solo su questi volumi virtuali.	Array di stringhe UUID	No	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Un elenco di oggetti contenente informazioni sulle attività per ciascun volume virtuale nel sistema.	VolumeStats array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVolumeStatsByVirtualVolume",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
```

```
  "result": {
    "volumeStats": [
      {
        "accountID": 17,
        "actualIOPS": 0,
        "asyncDelay": null,
        "averageIOPSize": 1074265444,
        "burstIOPSCredit": 0,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 0,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
            26
          ],
          "primary": 56
        },
        "nonZeroBlocks": 36,
        "readBytes": 18366464,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readOps": 156,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "throttle": 0,
        "timestamp": "2016-10-10T17:46:35.914642Z",
        "unalignedReads": 156,
        "unalignedWrites": 185,
        "virtualVolumeID": "070ac0ba-f344-4f4c-b79c-142efa3642e8",
        "volumeAccessGroups": [],
        "volumeID": 12518,
        "volumeSize": 91271200768,
        "volumeUtilization": 0,
        "writeBytes": 23652213248,
        "writeBytesLastSample": 0,
        "writeLatencyUSec": 0,
        "writeOps": 185,
        "writeOpsLastSample": 0,
        "zeroBlocks": 22282972
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListVolumeStatsByVolume

È possibile utilizzare `ListVolumeStatsByVolume` metodo per elencare le misurazioni di attività di alto livello per ogni volume, in base al volume. I valori sono cumulativi dalla creazione del volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
IncludeVirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Elenco delle informazioni sull'attività del volume.	VolumeStats array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListVolumeStatsByVolume",
   "params": {},
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
```

```
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 3,
        "actualIOPS": 0,
        "asyncDelay": null,
        "averageIOPSize": 4096,
        "burstIOPSCredit": 30000,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 0,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
              16
          ],
          "primary": 12
        },
        "nonZeroBlocks": 7499205,
        "readBytes": 159012818944,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readOps": 38821489,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "throttle": 0,
        "timestamp": "2016-10-17T20:55:31.087537Z",
        "unalignedReads": 0,
        "unalignedWrites": 0,
        "volumeAccessGroups": [
          1
        ],
        "volumeID": 1,
        "volumeSize": 53687091200,
        "volumeUtilization": 0,
        "writeBytes": 52992585728,
        "writeBytesLastSample": 0,
        "writeLatencyUSec": 0,
        "writeOps": 12937643,
        "writeOpsLastSample": 0,
        "zeroBlocks": 5607995
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListVolumeStatsByVolumeAccessGroup

È possibile utilizzare `ListVolumeStatsByVolumeAccessGroup` metodo per elencare le misurazioni dell'attività totale per tutti i volumi che sono membri dei gruppi di accesso al volume specificati.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
Include VirtualVolumes	I volumi virtuali sono inclusi nella risposta per impostazione predefinita. Per escludere i volumi virtuali, impostare su false.	booleano	vero	No
VolumeAccessGroups	Array di VolumeAccessGroupID per i quali viene restituita l'attività del volume. Se omesso, vengono restituite le statistiche per tutti i gruppi di accesso ai volumi.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeStats	Elenco delle informazioni sull'attività del volume per tutti i volumi nel gruppo di accesso del volume specificato.**Nota:** il membro volumeID è 0 per ogni voce, perché i valori rappresentano la somma di tutti i volumi di proprietà dell'account.	VolumeStats

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVolumeStatsByVolumeAccessGroup",
    "params": {"volumeAccessGroups": [1]},
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 0,
        "nonZeroBlocks": 149366393,
        "readBytes": 3156273328128,
        "readBytesLastSample": 0,
        "readOps": 770574543,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "timestamp": "2016-10-17T21:04:10.712370Z",
        "unalignedReads": 0,
        "unalignedWrites": 0,
        "volumeAccessGroups": [
            1
        ],
        "volumeID": 0,
        "volumeSize": 1073741824000,
        "writeBytes": 1051988406272,
        "writeBytesLastSample": 0,
        "writeOps": 256833107,
        "writeOpsLastSample": 0,
        "zeroBlocks": 112777607
      }
    ]
  }
}
```

Novità dalla versione

9.6

ModifyBackupTarget

È possibile utilizzare `ModifyBackupTarget` metodo per modificare gli attributi di una destinazione di backup.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
BackupTargetID	ID di destinazione univoco per la destinazione da modificare.	intero	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
nome	Nuovo nome per la destinazione del backup.	stringa	Nessuno	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ModifyBackupTarget",
   "params": {
      "backupTargetID" : 1,
      "name": "yourtargetS3"
      "attributes" : {
          "size" : 500,
      }
   },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {}
}
```

Novità dalla versione

9.6

ModifyQoSPolicy

È possibile utilizzare `ModifyQoSPolicy` Metodo per modificare un criterio QoS esistente nel sistema.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
QosPolicyID	L'ID del criterio da modificare.	intero	Nessuno	Sì
nome	Se fornito, il nome della policy QoS (ad esempio oro, platino, argento) viene modificato in questo valore.	stringa	Nessuno	No
qos	Se fornite, le impostazioni QoS per questo criterio vengono modificate in queste impostazioni. È possibile fornire valori QoS parziali e modificare solo alcune impostazioni QoS.	Oggetto QoS	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
QosPolicy	Dettagli della policy QoS appena modificata.	QoSPolicy

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1950,
  "method": "ModifyQoSPolicy",
  "params": {
    "qosPolicyID": 2,
    "qos": {
      "minIOPS": 51,
      "maxIOPS": 15002,
      "burstIOPS": 15002
    }
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1950,
  "result": {
    "qosPolicy": {
      "name": "bronze",
      "qos": {
        "burstIOPS": 15002,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 15002,
        "minIOPS": 51
      },
      "qosPolicyID": 2,
      "volumeIDs": [
        2
      ]
    }
  }
}
```


Novità dalla versione

10.0

ModifyVolume

È possibile utilizzare `ModifyVolume` metodo per modificare le impostazioni di un volume esistente. È possibile apportare modifiche a un volume alla volta e le modifiche vengono eseguite immediatamente.

Se non si specificano i valori QoS quando si modifica un volume, questi rimangono gli stessi di prima della modifica. È possibile recuperare i valori QoS predefiniti per un volume appena creato eseguendo `GetDefaultQoS` metodo.

Per evitare errori di replica, è necessario aumentare le dimensioni di un volume da replicare nel seguente ordine:

1. Aumentare le dimensioni del volume con l'accesso ReplicationTarget.
2. Aumentare le dimensioni dell'origine o del volume con l'accesso in lettura/scrittura.

Assicurarsi che i volumi di destinazione e di origine abbiano le stesse dimensioni.

Se si imposta lo stato di accesso su Locked o ReplicationTarget, tutte le connessioni iSCSI esistenti vengono interrotte.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	L'ID volume per il volume da modificare.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
accesso	Accesso consentito per il volume. Valori possibili: • `readOnly`: Sono consentite solo operazioni di lettura. • `readWrite`: Sono consentite le letture e le scritture. • `locked`: Non sono consentite letture o scritture. Se non specificato, il valore di accesso non cambia. • `replicationTarget`: Identifica un volume come volume di destinazione per un set di volumi accoppiati. Se il volume non è associato, lo stato di accesso è bloccato. Se non viene specificato alcun valore, il valore di accesso non cambia. • `snapMirrorTarget`: Identifica un volume come volume di destinazione per la replica di SnapMirror.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID account	L'ID account a cui viene riassegnato il volume. Se non viene specificato alcun valore, viene utilizzato il nome dell'account precedente.	intero	Nessuno	No
AssociateWithQoSPolicy	Associare il volume al criterio QoS specificato. Valori possibili: • `true`: Associare il volume al criterio QoS specificato nel parametro QoSPolicyID. • `false`: Non associare il volume al criterio QoS specificato nel parametro QoSPolicyID. Se false, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi o meno un policy QoS nel parametro QoSPolicy.	booleano	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
CreateTime	Stringa di dati ISO 8601 da impostare come data di creazione del nuovo volume. Obbligatorio se setCreateTime è impostato su true.	Stringa ISO 8601	Nessuno	No
EnableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con gli endpoint SnapMirror. Valori possibili: • `true` • `false`	booleano	falso	No
FifoSize	Specifica il numero massimo di snapshot first-in-first-out (FIFO) supportati dal volume. Si noti che gli snapshot FIFO e non FIFO utilizzano entrambi lo stesso pool di slot di snapshot disponibili su un volume. Utilizzare questa opzione per limitare il consumo di snapshot FIFO degli slot snapshot disponibili. Si noti che non è possibile modificare questo valore in modo che sia inferiore al numero corrente di snapshot FIFO.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
MinFifoSize	Specifica il numero di slot di snapshot riservati solo per le istantanee FIFO (first-in-first-out). Poiché le snapshot FIFO e non FIFO condividono lo stesso pool, il parametro minFifuoSize riduce il numero totale di possibili snapshot non FIFO della stessa quantità. Si noti che non è possibile modificare questo valore in modo che sia in conflitto con il numero corrente di snapshot non FIFO.	intero	Nessuno	No
modalità	Modalità di replica del volume. Valori possibili: • `asynch`: Attende che il sistema riconosca che i dati sono memorizzati sull'origine prima di scrivere sulla destinazione. • `sync`: Non attende che la conferma della trasmissione dei dati dall'origine inizi a scrivere i dati sulla destinazione.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
qos	Le nuove impostazioni della qualità del servizio per questo volume. Se non specificato, le impostazioni QoS non vengono modificate. Valori possibili: • `minIOPS` • `maxIOPS` • `burstIOPS`	QoS	Nessuno	No
QosPolicyID	ID del criterio le cui impostazioni QoS devono essere applicate ai volumi specificati. Questo parametro si esclude a vicenda con il parametro qos.	intero	Nessuno	No
SetCreateTime	Impostare su vero per modificare la data di creazione del volume registrata.	booleano	Nessuno	No
TotalSize (dimensioni totale)	La nuova dimensione del volume in byte. 1000000000 equivale a 1 GB. Le dimensioni vengono arrotondate al megabyte più vicino. Questo parametro può essere utilizzato solo per aumentare le dimensioni di un volume.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo

volume	Oggetto contenente informazioni sul volume appena modificato.	volume

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyVolume",
  "params": {
     "volumeID": 5,
     "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
     },
     "qos": {
        "minIOPS": 60,
        "maxIOPS": 100,
        "burstIOPS": 150,
        "burstTime": 60
     },
      "access" :"readWrite"
     },
      "totalSize": 20000000000,
     "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
      "volume": {
          "access": "readWrite",
          "accountID": 1,
          "attributes": {
              "name1": "value1",
              "name2": "value2",
              "name3": "value3"
          },
          "blockSize": 4096,
          "createTime": "2016-03-28T16:16:13Z",
```

```
            "deleteTime": "",
            "enable512e": true,
            "iqn": "iqn.2010-01.com.solidfire:jyay.1459181777648.5",
            "name": "1459181777648",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 150,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 100,
                "minIOPS": 60
            },
            "scsiEUIDeviceID": "6a79617900000005f47acc0100000000",
            "scsiNAADeviceID": "6f47acc1000000006a79617900000005",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 1000341504,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 5,
            "volumePairs": []
        }
    }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

GetDefaultQoS

ModifyVolumes

È possibile utilizzare `ModifyVolumes` metodo per configurare fino a 500 volumi esistenti contemporaneamente. Le modifiche vengono eseguite immediatamente. Se `ModifyVolumes` impossibile modificare uno dei volumi specificati, nessuno dei volumi specificati viene modificato.

Se non si specificano i valori QoS quando si modificano i volumi, i valori QoS per ciascun volume rimangono invariati. È possibile recuperare i valori QoS predefiniti per un volume appena creato eseguendo `GetDefaultQoS` metodo.

Per evitare errori di replica, è necessario aumentare le dimensioni dei volumi che vengono replicati nel seguente ordine:

1. Aumentare le dimensioni del volume con l'accesso ReplicationTarget.
2. Aumentare le dimensioni dell'origine o del volume con l'accesso in lettura/scrittura.

Assicurarsi che i volumi di destinazione e di origine abbiano le stesse dimensioni.

Se si imposta lo stato di accesso su Locked o ReplicationTarget, tutte le connessioni iSCSI esistenti vengono interrotte.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio

accesso	Accesso consentito per i volumi. Valori possibili: • `readOnly`: Sono consentite solo operazioni di lettura. • `readWrite`: Sono consentite le letture e le scritture. • `locked`: Non sono consentite letture o scritture. Se non specificato, il valore di accesso non cambia. • `replicationTarget`: Identifica un volume come volume di destinazione per un set di volumi accoppiati. Se il volume non è associato, lo stato di accesso è bloccato. Se non viene specificato alcun valore, il valore di accesso non cambia.	stringa	Nessuno	No
ID account	L'ID account a cui vengono riassegnati i volumi. Se non viene specificato alcun valore, viene utilizzato il nome dell'account precedente.	intero	Nessuno	No

AssociateWithQoSPolicy	Associare il volume al criterio QoS specificato. Valori possibili: • Vero: Associare il volume al criterio QoS specificato nel parametro QoSPolicyID. • Falso: Non associare il volume al criterio QoS specificato nel parametro QoSPolicyID. Se false, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi o meno un policy QoS nel parametro QoSPolicy.	booleano	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
CreateTime	Stringa di dati ISO 8601 da impostare come data di creazione del nuovo volume. Obbligatorio se setCreateTime è impostato su true.	Stringa ISO 8601	Nessuno	No

EnableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con gli endpoint SnapMirror. Valori possibili: • `true` • `false`	booleano	falso	No
FifoSize	Specifica il numero massimo di snapshot first-in-first-out (FIFO) supportati dal volume. Si noti che gli snapshot FIFO e non FIFO utilizzano entrambi lo stesso pool di slot di snapshot disponibili su un volume. Utilizzare questa opzione per limitare il consumo di snapshot FIFO degli slot snapshot disponibili. Si noti che non è possibile modificare questo valore in modo che sia inferiore al numero corrente di snapshot FIFO.	intero	Nessuno	No

MinFifoSize	Specifica il numero di slot di snapshot riservati solo per le istantanee FIFO (first-in-first-out). Poiché le snapshot FIFO e non FIFO condividono lo stesso pool, il parametro minFifuoSize riduce il numero totale di possibili snapshot non FIFO della stessa quantità. Si noti che non è possibile modificare questo valore in modo che sia in conflitto con il numero corrente di snapshot non FIFO.	intero	Nessuno	No
modalità	Modalità di replica del volume. Valori possibili: • `asynch`: Attende che il sistema riconosca che i dati sono memorizzati sull'origine prima di scrivere sulla destinazione. • `sync`: Non attende che la conferma della trasmissione dei dati dall'origine inizi a scrivere i dati sulla destinazione.	stringa	Nessuno	No

qos	Le nuove impostazioni della qualità del servizio per i volumi. Se non specificato, le impostazioni QoS non vengono modificate. Valori possibili: • `minIOPS` • `maxIOPS` • `burstIOPS`	QoS	Nessuno	No
QosPolicyID	ID del criterio le cui impostazioni QoS devono essere applicate ai volumi specificati. Questo parametro si esclude a vicenda con il parametro qos.	intero	Nessuno	No
SetCreateTime	Impostare su vero per modificare la data di creazione del volume registrata.	booleano	Nessuno	No
TotalSize (dimensioni totale)	La nuova dimensione dei volumi in byte. 1000000000 equivale a 1 GB. Le dimensioni vengono arrotondate al megabyte più vicino. Questo parametro può essere utilizzato solo per aumentare le dimensioni di un volume.	intero	Nessuno	No
ID volume	Un elenco di volumeID per i volumi da modificare.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
volume	Matrice di oggetti contenente informazioni su ciascun volume appena modificato.	volume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyVolumes",
  "params": {
    "volumeIDs": [2,3],
    "attributes": {
      "name1": "value1",
      "name2": "value2",
      "name3": "value3"
    },
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 100,
      "burstIOPS": 150,
      "burstTime": 60
    },
    "access" : "replicationTarget"
  },
  "totalSize": 80000000000,
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumes": [
      {
        "access": "replicationTarget",
        "accountID": 1,
```

```
      "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
      },
      "blockSize": 4096,
      "createTime": "2016-04-06T17:25:13Z",
      "deleteTime": "",
      "enable512e": false,
      "iqn": "iqn.2010-01.com.solidfire:jo73.2",
      "name": "doctest1",
      "purgeTime": "",
      "qos": {
        "burstIOPS": 150,
        "burstTime": 60,
        "curve": {
          "4096": 100,
          "8192": 160,
          "16384": 270,
          "32768": 500,
          "65536": 1000,
          "131072": 1950,
          "262144": 3900,
          "524288": 7600,
          "1048576": 15000
        },
        "maxIOPS": 100,
        "minIOPS": 50
      },
      "scsiEUIDeviceID": "6a6f373300000002f47acc0100000000",
      "scsiNAADeviceID": "6f47acc1000000006a6f373300000002",
      "sliceCount": 1,
      "status": "active",
      "totalSize": 1000341504,
      "virtualVolumeID": null,
      "volumeAccessGroups": [],
      "volumeID": 2,
      "volumePairs": []
    },
    {
      "access": "replicationTarget",
      "accountID": 1,
      "attributes": {
        "name1": "value1",
        "name2": "value2",
        "name3": "value3"
```

```
        },
        "blockSize": 4096,
        "createTime": "2016-04-06T17:26:31Z",
        "deleteTime": "",
        "enable512e": false,
        "iqn": "iqn.2010-01.com.solidfire:jo73.3",
        "name": "doctest2",
        "purgeTime": "",
        "qos": {
          "burstIOPS": 150,
          "burstTime": 60,
          "curve": {
            "4096": 100,
            "8192": 160,
            "16384": 270,
            "32768": 500,
            "65536": 1000,
            "131072": 1950,
            "262144": 3900,
            "524288": 7600,
            "1048576": 15000
          },
          "maxIOPS": 100,
          "minIOPS": 50
        },
        "scsiEUIDeviceID": "6a6f373300000003f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000006a6f373300000003",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 3,
        "volumePairs": []
      }
    ]
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

GetDefaultQoS

PurgeDeletedVolume

È possibile utilizzare `PurgeDeletedVolume` metodo per eliminare immediatamente e in modo permanente un volume che è stato eliminato. È necessario eliminare un volume utilizzando `DeleteVolume` prima di poter essere spurgato.

I volumi vengono eliminati automaticamente dopo un determinato periodo di tempo, pertanto l'utilizzo di questo metodo non è generalmente richiesto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	ID volume del volume da purgare.	intero	No	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "PurgeDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result": {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

DeleteVolume

PurgeDeletedVolumes

È possibile utilizzare `PurgeDeletedVolumes` metodo per eliminare immediatamente e in modo permanente i volumi che sono stati eliminati; è possibile utilizzare questo metodo per eliminare fino a 500 volumi alla volta.

È necessario eliminare i volumi utilizzando `DeleteVolumes` prima di poter essere rimossi. I volumi vengono eliminati automaticamente dopo un determinato periodo di tempo, pertanto l'utilizzo di questo metodo non è generalmente richiesto.

> Se si elimina un numero elevato di volumi alla volta o se ciascuno di essi dispone di molti snapshot associati, il metodo potrebbe non riuscire e restituire l'errore "xDBConnectionLoss". In questo caso, riprovare a chiamare il metodo con un numero inferiore di volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Un elenco di volumeID di volumi da dispurgare dal sistema.	array intero	No	No
AccountID	Un elenco di ID account. Tutti i volumi di tutti gli account specificati vengono rimossi dal sistema.	array intero	No	No
VolumeAccessGroupID	Un elenco di volumeAccessGroupID. Tutti i volumi di tutti i gruppi di accesso ai volumi specificati vengono rimossi dal sistema.	array intero	No	No

Nota: è possibile specificare solo uno dei parametri sopra indicati per ogni chiamata al metodo. Se si specifica più di uno o nessuno, si verifica un errore.

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "PurgeDeletedVolumes",
   "params": {
      "accountIDs" : [1, 2, 3]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result": {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

DeleteVolumes

RemoveBackupTarget

È possibile utilizzare `RemoveBackupTarget` metodo per rimuovere le destinazioni di backup.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
BackupTargetID	ID di destinazione univoco della destinazione da rimuovere.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveBackupTarget",
   "params": {
        "backupTargetID" : 1
   },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {}
}
```

Novità dalla versione

9.6

RestoreDeletedVolume

È possibile utilizzare `RestoreDeletedVolume` metodo per contrassegnare nuovamente un volume cancellato come attivo. Questa azione rende il volume immediatamente disponibile per la connessione iSCSI.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	ID volume del volume cancellato da ripristinare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RestoreDeletedVolume",
   "params": {
      "volumeID"  : 5
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id" : 1,
  "result": {}
}
```

Novità dalla versione

9.6

SetDefaultQoS

È possibile utilizzare `SetDefaultQoS` Metodo per configurare i valori QoS (Quality of Service) predefiniti (misurati in input e output al secondo, o IOPS) per un volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
MinIOPS	Il numero minimo di IOPS sostenuti forniti dal cluster a un volume.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
MaxIOPS	Il numero massimo di IOPS sostenuti forniti dal cluster a un volume.	intero	Nessuno	No
BurstIOPS	Il numero massimo di IOPS consentito in uno scenario a burst breve.	intero	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
MinIOPS	Il numero minimo di IOPS sostenuti forniti dal cluster a un volume.	intero
MaxIOPS	Il numero massimo di IOPS sostenuti forniti dal cluster a un volume.	intero
BurstIOPS	Il numero massimo di IOPS consentito in uno scenario a burst breve.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "SetDefaultQoS",
    "params": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
    "id":1,
    "result": {
        "burstIOPS":8000,
        "maxIOPS":1000,
        "minIOPS":200
    }
}
```

Novità dalla versione

9.6

StartBulkVolumeRead

È possibile utilizzare `StartBulkVolumeRead` metodo per avviare una sessione di lettura di un volume in blocco su un volume specificato.

Solo due processi di volume in blocco possono essere eseguiti contemporaneamente su un volume. Quando si inizializza la sessione, i dati vengono letti da un volume di storage SolidFire per essere memorizzati in un'origine di backup esterna. L'accesso ai dati esterni viene effettuato da un server Web in esecuzione su un nodo di storage Element. Le informazioni sull'interazione con il server per l'accesso ai dati esterni vengono trasmesse da uno script in esecuzione sul sistema di storage.

All'inizio di un'operazione di lettura di volume in blocco, viene creata una snapshot del volume e la snapshot viene eliminata al termine della lettura. È inoltre possibile leggere uno snapshot del volume immettendo l'ID dello snapshot come parametro. Quando si legge uno snapshot precedente, il sistema non crea un nuovo snapshot del volume, né elimina lo snapshot precedente al termine della lettura.

> Questo processo crea un nuovo snapshot se non viene fornito l'ID di uno snapshot esistente. È possibile creare snapshot se la completezza del cluster è nella fase 2 o 3. Gli snapshot non vengono creati quando la completezza del cluster è nella fase 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
formato	Il formato dei dati del volume. Può essere: • `uncompressed`: Ogni byte del volume viene restituito senza compressione. • `native`: Vengono restituiti dati opachi più piccoli e memorizzati e scritti in modo più efficiente su una successiva scrittura di volume in blocco.	stringa	Nessuno	Sì
ID volume	L'ID del volume da leggere.	intero	Nessuno	Sì
SnapshotID	L'ID di uno snapshot creato in precedenza utilizzato per le letture di volumi in blocco. Se non viene inserito alcun ID, viene creata un'istantanea dell'immagine del volume attivo corrente.	intero	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
script	Il nome di uno script eseguibile. Se non viene fornito alcun nome di script, la chiave e l'URL sono necessari per accedere ai nodi di storage degli elementi. Lo script viene eseguito sul nodo primario e la chiave e l'URL vengono restituiti allo script in modo da poter contattare il server Web locale.	stringa	Nessuno	No
Parametri di scriptParameters	Parametri JSON da passare allo script.	Oggetto JSON	Nessuno	No
attributi	Attributi JSON per il processo di volume in blocco.	Oggetto JSON	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	L'ID del processo asincrono da controllare per il completamento.	intero
chiave	Chiave opaca che identifica in modo univoco la sessione.	stringa
url	URL per accedere al server Web del nodo.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "StartBulkVolumeRead",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
      "snapshotID" : 2
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
      "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Novità dalla versione

9.6

StartBulkVolumeWrite

È possibile utilizzare `StartBulkVolumeWrite` metodo per avviare una sessione di scrittura di un volume in blocco su un volume specificato.

Solo due processi di volume in blocco possono essere eseguiti contemporaneamente su un volume. Quando si inizializza la sessione, i dati vengono scritti in un volume di storage Element da un'origine di backup esterna. L'accesso ai dati esterni viene effettuato da un server Web in esecuzione su un nodo di storage Element. Le informazioni sull'interazione con il server per l'accesso ai dati esterni vengono trasmesse da uno script in esecuzione sul sistema di storage.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
formato	Il formato dei dati del volume. Può essere: • `uncompressed`: Ogni byte del volume viene restituito senza compressione. • `native`: Vengono restituiti dati opachi più piccoli e memorizzati e scritti in modo più efficiente su una successiva scrittura di volume in blocco.	stringa	Nessuno	Sì
ID volume	L'ID del volume in cui si desidera eseguire la scrittura.	intero	Nessuno	Sì
script	Il nome di uno script eseguibile. Se non viene fornito alcun nome di script, la chiave e l'URL sono necessari per accedere ai nodi di storage degli elementi. Lo script viene eseguito sul nodo primario e la chiave e l'URL vengono restituiti allo script in modo da poter contattare il server Web locale.	stringa	Nessuno	No
Parametri di scriptParameters	Parametri JSON da passare allo script.	Oggetto JSON	Nessuno	No
attributi	Attributi JSON per il processo di volume in blocco.	Oggetto JSON	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
AsyncHandle	L'ID del processo asincrono da controllare per il completamento.	intero
chiave	Chiave opaca che identifica in modo univoco la sessione.	stringa
url	URL per accedere al server Web del nodo.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "StartBulkVolumeWrite",
   "params": {
      "volumeID" : 5,
      "format"  : "native",
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result" : {
      "asyncHandle" : 1,
      "key" : "11eed8f086539205beeaadd981aad130",
      "url" : "https://127.0.0.1:44000/"
   }
}
```

Novità dalla versione

9.6

UpdateBulkVolumeStatus

È possibile utilizzare `UpdateBulkVolumeStatus` metodo per aggiornare lo stato di un processo di volume in blocco avviato con `StartBulkVolumeRead` oppure `StartBulkVolumeWrite` metodi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
chiave	Il tasto assegnato durante l'inizializzazione di StartBulkVolumeRead oppure StartBulkVolumeWrite sessione.	stringa	Nessuno	Sì
stato	Il sistema imposta lo stato del processo di volume in blocco specificato. Valori possibili: • In esecuzione: Processi ancora attivi. • Complete (completo): Lavori eseguiti. • Non riuscito: Lavori non riusciti.	stringa	Nessuno	Sì
PercentComplete	L'avanzamento completo del processo di volume in blocco come percentuale.	stringa	Nessuno	No
messaggio	Restituisce lo stato del processo di volume in blocco una volta completato il processo.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
attributi	Attributi JSON; aggiorna ciò che si trova nel processo di volume in blocco.	Oggetto JSON	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
stato	Stato della sessione richiesta. Stato restituito: • preparazione in corso • attivo • fatto • non riuscito	stringa
attributi	Restituisce gli attributi specificati nella chiamata al metodo. I valori vengono restituiti indipendentemente dal fatto che siano stati modificati o meno.	stringa
url	L'URL per accedere al server Web del nodo; fornito solo se la sessione è ancora attiva.	stringa

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "UpdateBulkVolumeStatus",
   "params": {
          "key": "0b2f532123225febda2625f55dcb0448",
          "status": "running"
      },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result": {
      "status" : "running",
      "url" : "https://10.10.23.47:8443/"
    }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- StartBulkVolumeRead
- StartBulkVolumeWrite

Metodi API del gruppo di accesso al volume

I metodi dei gruppi di accesso ai volumi consentono di aggiungere, rimuovere, visualizzare e modificare i gruppi di accesso ai volumi, ovvero raccolte di volumi a cui gli utenti possono accedere utilizzando gli iniziatori iSCSI o Fibre Channel.

- AddInitiatorsToVolumeAccessGroup
- AddVolumesToVolumeAccessGroup
- CreateVolumeAccessGroup
- DeleteVolumeAccessGroup
- ListVolumeAccessGroups
- RemoveVolumesFromVolumeAccessGroup
- RemoveInitialisFromVolumeAccessGroup
- ModifyVolumeAccessGroup
- GetVolumeAccessGroupEfficiency

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

AddInitiatorsToVolumeAccessGroup

È possibile utilizzare `AddInitiatorsToVolumeAccessGroup` metodo per aggiungere gli iniziatori a un gruppo di accesso a un volume specificato.

Il formato accettato di un IQN iniziatore è iqn.yyyy-mm, dove y e m sono cifre, seguite da testo che deve

contenere solo cifre, caratteri alfabetici minuscoli, un punto (.), due punti (:) o trattino (-). Vedere il seguente esempio:

```
iqn.2010-01.com.solidfire:17oi.solidfire-0.1
```

Il formato accettato di un iniziatore Fibre Channel WWPN è AA:BB:CC:dd:11:22:33:44 o AabBCCdd11223344. Vedere il seguente esempio:

```
21:00:00:0e:1e:11:f1:81
```

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
iniziatori	Elenco degli ID o dei nomi degli iniziatori (IQN e WWPN) da includere nel gruppo di accesso al volume. Se si passa un elenco di nomi di iniziatori, gli iniziatori vengono creati se non esistono già. Se si passa un elenco di ID iniziatore, il metodo restituisce un errore se uno degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è obsoleto; se possibile, è necessario utilizzare gli ID degli iniziatori.	array intero o array di stringhe (obsoleto)		Sì
VolumeAccessGroupID	L'ID del gruppo di accesso al volume per aggiungere l'iniziatore.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	VolumeAccessGroup

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 13171,
  "method": "AddInitiatorsToVolumeAccessGroup",
  "params": {
    "initiators": [116,117],
    "volumeAccessGroupID": 96
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 13171,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [
        116,
        117
      ],
      "initiators": [
        "iqn.1993-08.org.debian:01:181324777",
        "iqn.1993-08.org.debian:01:181324888"
      ],
      "name": "northbanktest",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```


Novità dalla versione

9.6

AddVolumesToVolumeAccessGroup

È possibile utilizzare `AddVolumesToVolumeAccessGroup` metodo per aggiungere volumi a un gruppo di accesso a un volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
volumi	Elenco di ID volume da aggiungere al gruppo di accesso al volume.	array intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	VolumeAccessGroupID del gruppo di accesso al volume a cui vengono aggiunti i volumi.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	VolumeAccessGroup

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "AddVolumesToVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        346
      ],
      "initiatorIDs": [
        116,
        117
      ],
      "initiators": [
        "iqn.1993-08.org.debian:01:181324777",
        "iqn.1993-08.org.debian:01:181324888"
      ],
      "name": "northbanktest",
      "volumeAccessGroupID": 96,
      "volumes": [
        1,
        2
      ]
    }
  }
}
```


Novità dalla versione

9.6

CreateVolumeAccessGroup

È possibile utilizzare `CreateVolumeAccessGroup` per creare un nuovo gruppo di accesso al volume. Quando si crea il gruppo di accesso al volume, è necessario assegnargli un nome e, facoltativamente, è possibile inserire iniziatori e volumi.

Qualsiasi IQN iniziatore aggiunto al gruppo di accesso al volume può accedere a qualsiasi volume del gruppo senza autenticazione CHAP.

> I volumi clonati non ereditano l'appartenenza al gruppo di accesso al volume dal volume di origine.

Quando si creano gruppi di accesso ai volumi, considerare quanto segue:

- Un gruppo di accesso al volume può contenere fino a 64 IQN iniziatori.
- Un iniziatore può appartenere a un solo gruppo di accesso al volume.

- Un gruppo di accesso al volume può contenere fino a 2000 volumi.
- Ciascun gruppo di accesso al volume può appartenere a un massimo di quattro gruppi di accesso al volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
iniziatori	Elenco degli ID o dei nomi degli iniziatori (IQN e WWPN) da includere nel gruppo di accesso al volume. Se si passa un elenco di nomi di iniziatori, gli iniziatori vengono creati se non esistono già. Se si passa un elenco di ID iniziatore, il metodo restituisce un errore se uno degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è obsoleto; se possibile, è necessario utilizzare gli ID degli iniziatori.	array intero o array di stringhe (obsoleto)		No
nome	Nome del gruppo di accesso al volume. Non è necessario essere unici, ma consigliato. La lunghezza deve essere compresa tra 1 e 64 caratteri.	stringa	Nessuno	Sì
volumi	Elenco dei volumeID da includere nel gruppo di accesso al volume.	array intero		No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	{}	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena creato.	VolumeAccessGroup
VolumeAccessGroupID	L'ID del gruppo di accesso al volume appena creato.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CreateVolumeAccessGroup",
   "params": {
      "name": "myaccessgroup",
      "initiators": ["iqn.1993-08.org.debian: 01: a31b1d799d5c"],
      "volumes": [327],
      "attributes": {}
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": null,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [],
      "initiatorIDs": [
        95
      ],
      "initiators": [
        "iqn.1993-08.org.debian: 01: a31b1d799d5c"
      ],
      "name": "myaccessgroup",
      "volumeAccessGroupID": 96,
      "volumes": [
        327
      ]
    },
    "volumeAccessGroupID": 96
  }
}
```


Novità dalla versione

9.6

Trova ulteriori informazioni

- GetAsyncResult
- ListSyncJobs
- ModifyVolume

DeleteVolumeAccessGroup

È possibile utilizzare `DeleteVolumeAccessGroup` per eliminare un gruppo di accesso al volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	L'ID del gruppo di accesso al volume da eliminare.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
DeleteOrphanInitialators	Specifica se eliminare o meno gli oggetti initiator. Valori possibili: • True: Elimina gli oggetti iniziatore dopo che sono stati rimossi da un gruppo di accesso al volume. • Falso: Non eliminare gli oggetti Initiator dopo che sono stati rimossi da un gruppo di accesso al volume. Questa è l'impostazione predefinita.	booleano	falso	No
forza	L'aggiunta di questo flag forzerà l'eliminazione del gruppo di accesso al volume anche se dispone di un tag o ID di rete virtuale. Valori possibili: • Vero: Il gruppo di accesso al volume verrà eliminato. • Falso: Impostazione predefinita. Non eliminare il gruppo di accesso al volume se dispone di un ID o di un tag di rete virtuale.	booleano	falso	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteVolumeAccessGroup",
   "params": {
          "force": true,
      "volumeAccessGroupID"  : 3
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id" : 1,
   "result": {}
}
```

Novità dalla versione

9.6

ListVolumeAccessGroups

È possibile utilizzare `ListVolumeAccessGroups` metodo per ottenere informazioni sui gruppi di accesso al volume attualmente presenti nel sistema.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
limite	Numero massimo di oggetti volumeAccessGroup da restituire. Si escludono a vicenda con il parametro volumeAccessGroups.	intero	Senza limiti	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
StartVolumeAccessGroupID	L'ID del gruppo di accesso al volume in cui iniziare l'elenco. Si escludono a vicenda con il parametro volumeAccessGroups.	intero	0	No
VolumeAccessGroups	Elenco dei valori volumeAccessGroupID da recuperare. Si escludono a vicenda con i parametri startVolumeAccessGroupID e Limit.	array intero		No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
VolumeAccessGroups	Un elenco di oggetti che descrivono ciascun gruppo di accesso al volume.	VolumeAccessGroup array
VolumeAccessGroupsNotFound	Un elenco di gruppi di accesso al volume non trovati dal sistema. Presente se è stato utilizzato il parametro volumeAccessGroups e il sistema non è stato in grado di trovare uno o più gruppi di accesso al volume specificati.	array intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListVolumeAccessGroups",
   "params": {
      "startVolumeAccessGroupID": 3,
      "limit"   : 1
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroups": [
      {
        "attributes": {},
        "deletedVolumes": [],
        "initiatorIDs": [],
        "initiators": [],
        "name": "example1",
        "volumeAccessGroupID": 3,
        "volumes": []
      }
    ]
  }
}
```

Novità dalla versione

9.6

RemoveVolumesFromVolumeAccessGroup

È possibile utilizzare `RemoveVolumesFromVolumeAccessGroup` metodo per rimuovere i volumi da un gruppo di accesso a un volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	VolumeAccessGroupID da cui rimuovere i volumi.	intero	Nessuno	Sì
volumi	VolumeID dei volumi da rimuovere dal gruppo di accesso al volume.	array intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	VolumeAccessGroup

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "RemoveVolumesFromVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "volumes": [1,2]
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        346
      ],
      "initiatorIDs": [
        116,
        117
      ],
      "initiators": [
        "iqn.1993-08.org.debian:01:181324777",
        "iqn.1993-08.org.debian:01:181324888"
      ],
      "name": "northbanktest",
      "volumeAccessGroupID": 96,
      "volumes": []
    }
  }
}
```

Novità dalla versione

9.6

RemoveInitialisFromVolumeAccessGroup

È possibile utilizzare `RemoveInitiatorsFromVolumeAccessGroup` metodo per rimuovere gli iniziatori da un gruppo di accesso a un volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	L'ID del gruppo di accesso al volume da cui vengono rimossi gli iniziatori.	intero	Nessuno	Sì
iniziatori	Elenco degli ID o dei nomi degli iniziatori (IQN e WWPN) da includere nel gruppo di accesso al volume. Se si passa un elenco di nomi di iniziatori, gli iniziatori vengono creati se non esistono già. Se si passa un elenco di ID iniziatore, il metodo restituisce un errore se uno degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è obsoleto; se possibile, è necessario utilizzare gli ID degli iniziatori.	array intero (consigliato) o array di stringhe (obsoleto)	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
DeleteOrphanInitialators	Specifica se eliminare gli oggetti iniziatore dopo che sono stati rimossi da un gruppo di accesso al volume o meno. Valori possibili: • True: Elimina gli oggetti iniziatore dopo che sono stati rimossi da un gruppo di accesso al volume. • Falso: Non eliminare gli oggetti Initiator dopo che sono stati rimossi da un gruppo di accesso al volume. Questa è l'impostazione predefinita.	booleano	falso	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	VolumeAccessGroup

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 13171,
  "method": "RemoveInitiatorsFromVolumeAccessGroup",
  "params": {
    "initiators": [114,115],
    "volumeAccessGroupID": 96
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 13171,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [],
      "initiators": [],
      "name": "test",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```

Novità dalla versione

9.6

ModifyVolumeAccessGroup

È possibile utilizzare `ModifyVolumeAccessGroup` metodo per aggiornare gli iniziatori e aggiungere o rimuovere volumi da un gruppo di accesso al volume.

Se un iniziatore o un volume specificato è un duplicato di ciò che esiste attualmente, il gruppo di accesso al volume viene lasciato così com'è. Se non si specifica un valore per volumi o iniziatori, l'elenco corrente di iniziatori e volumi non viene modificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	L'ID del gruppo di accesso al volume da modificare.	intero	Nessuno	Sì
nome	Il nuovo nome per questo gruppo di accesso al volume.	stringa	Nessuno	No
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
iniziatori	Elenco degli ID o dei nomi degli iniziatori (IQN e WWPN) da includere nel gruppo di accesso al volume. Se si passa un elenco di nomi di iniziatori, gli iniziatori vengono creati se non esistono già. Se si passa un elenco di ID iniziatore, il metodo restituisce un errore se uno degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è obsoleto; se possibile, è necessario utilizzare gli ID degli iniziatori.	array intero (consigliato) o array di stringhe (obsoleto)	Nessuno	No

DeleteOrphanInitialators	Specifica se eliminare gli oggetti iniziatore dopo che sono stati rimossi da un gruppo di accesso al volume o meno. Valori possibili: • True: Elimina gli oggetti iniziatore dopo che sono stati rimossi da un gruppo di accesso al volume. • Falso: Non eliminare gli oggetti Initiator dopo che sono stati rimossi da un gruppo di accesso al volume. Questa è l'impostazione predefinita.	booleano	falso	No
volumi	Un elenco di ID di volumi da modificare.	array intero	Nessuno	VolumeAccessGroup

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
VolumeAccessGroup	Oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	VolumeAccessGroup

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ModifyVolumeAccessGroup",
   "params": {
      "volumeAccessGroupID": 96,
      "name": "accessgrouptest",
      "initiators": [115,114],
      "volumes": [
         346
    ],
      "attributes": {}
   }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": null,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [
        114,
        115
      ],
      "initiators": [
        "iqn.1998-01.com.vmware:desk1-esx1-577b283a",
        "iqn.1998-01.com.vmware:donesq-esx1-421b281b"
      ],
      "name": "accessgrouptest",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

- AddInitiatorsToVolumeAccessGroup
- AddVolumesToVolumeAccessGroup
- RemoveInitialisFromVolumeAccessGroup
- RemoveVolumesFromVolumeAccessGroup

GetVolumeAccessGroupEfficiency

È possibile utilizzare `GetVolumeAccessGroupEfficiency` metodo per ottenere informazioni sull'efficienza di un gruppo di accesso a un volume. Solo il gruppo di accesso al volume fornito come parametro in questo metodo API viene utilizzato per calcolare la capacità.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VolumeAccessGroupID	Specifica il gruppo di accesso al volume per il quale viene calcolata la capacità.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
compressione	La quantità di spazio salvata dalla compressione dei dati per tutti i volumi nel gruppo di accesso al volume. Indicato come rapporto in cui il valore 1 indica che i dati sono stati memorizzati senza compressione.	fluttuare
deduplica	La quantità di spazio risparmiata non duplicando i dati per tutti i volumi nel gruppo di accesso al volume. Indicato come rapporto.	fluttuare

ThinProvisioning	Il rapporto tra lo spazio utilizzato e la quantità di spazio allocato per la memorizzazione dei dati. Indicato come rapporto.	fluttuare
data e ora	L'ultima volta che sono stati raccolti i dati di efficienza dopo la garbage collection.	Stringa di dati ISO 8601
MissingVolumes	I volumi che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati da una recente garbage collection, da una perdita temporanea di rete o da servizi riavviati dal ciclo di garbage collection.	array intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "GetVolumeAccessGroupEfficiency",
   "params": {
      "volumeAccessGroupID": 1
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
   "id": 1,
   "result": {
       "compression": 2.006012925331075,
       "deduplication": 1,
       "missingVolumes": [],
       "thinProvisioning": 1.009861932938856,
       "timestamp": "2014-03-10T17:05:27Z"
   }
}
```

Metodi API di Volume Snapshot

I metodi API di snapshot dei volumi software Element consentono di gestire le snapshot dei volumi. È possibile creare, modificare, clonare ed eliminare le snapshot dei volumi utilizzando i metodi API di snapshot dei volumi.

- Panoramica delle istantanee
- CreateGroupSnapshot
- CreateSchedule
- CreateSnapshot
- DeleteGroupSnapshot
- DeleteSnapshot
- GetSchedule
- ListGroupSnapshot
- Elenchi
- ListSnapshot
- ModifyGroupSnapshot
- ModifySchedule
- ModifySnapshot
- RollbackToGroupSnapshot
- RollbackToSnapshot

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

Panoramica delle istantanee

Uno snapshot di un volume è una copia point-in-time di un volume. È possibile utilizzare le snapshot per riportare un volume nello stato in cui si trovava al momento della creazione dello snapshot.

È possibile raggruppare le snapshot dei volumi in modo che sia possibile eseguire il backup o il rollback dei volumi correlati in modo coerente. Uno snapshot di gruppo acquisisce un'immagine point-in-time di tutti i file di slice del volume. È quindi possibile utilizzare l'immagine per eseguire il rollback di un gruppo di volumi in uno stato point-in-time e garantire che tutti i dati siano coerenti in tutti i volumi del gruppo.

È possibile pianificare le snapshot dei volumi in modo che vengano eseguite autonomamente a intervalli definiti. È possibile definire gli intervalli in base all'ora, ai giorni della settimana o ai giorni del mese. È inoltre possibile utilizzare snapshot pianificate per garantire il backup degli snapshot sullo storage remoto a scopo di

archiviazione.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CreateGroupSnapshot

È possibile utilizzare `CreateGroupSnapshot` per creare una copia point-in-time di un gruppo di volumi.

È possibile utilizzare questo snapshot in un secondo momento come backup o rollback per garantire che i dati nel gruppo di volumi siano coerenti per il momento in cui è stata creata lo snapshot.

CLUSTER_FULLNESS

> È possibile creare snapshot se la completezza del cluster è nella fase 1, 2 o 3. Non è possibile creare snapshot quando la pienezza del cluster raggiunge la fase 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`attributes`	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
`enableRemoteReplication`	Specifica se lo snapshot verrà replicato o meno nello storage remoto. Valori possibili: • `true`: Lo snapshot verrà replicato nello storage remoto. • `false`: Lo snapshot non verrà replicato nello storage remoto.	booleano	falso	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`ensureSerialCreation`	Specifica che lo snapshot non deve essere creato se è in corso una replica dello snapshot precedente. I valori possibili sono: • `true`: In questo modo si garantisce la replica di un solo snapshot alla volta. La creazione di un nuovo snapshot non avrà esito positivo se è ancora in corso la replica di uno snapshot precedente. • `false`: Predefinito. Questa creazione di snapshot è consentita se è ancora in corso la replica di un altro snapshot.	booleano	`false`	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`expirationTime`	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con `retention`. In caso contrario `expirationTime`, o. `retention` sono specificati, lo snapshot non scadrà. Il formato dell'ora è una stringa di date ISO 8601 per la scadenza basata sull'ora, altrimenti non scadrà. Un valore di `null` fa sì che lo snapshot venga conservato in modo permanente. Un valore di `fifo` Fa in modo che lo snapshot venga conservato in base al principio FIFO (first-in-first-out), rispetto ad altri snapshot FIFO sul volume. L'API non riesce se non è disponibile spazio FIFO.	Stringa di dati ISO 8601	Nessuno	No
`name`	Il nome dello snapshot di gruppo. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stata eseguita l'istantanea del gruppo. La lunghezza massima consentita per il nome è di 255 caratteri.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`retention`	Questo parametro è lo stesso di `expirationTime` Il parametro, ad eccezione del formato dell'ora, è HH:mm:ss. In caso contrario `expirationTime` né così `retention` sono specificati, lo snapshot non scadrà.	stringa	Nessuno	No
`snapMirrorLabel`	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No
`volumes`	ID univoco dell'immagine del volume da cui copiare.	Array volumeID	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

membri	Elenco di checksum, volumeID e snapshotID per ciascun membro del gruppo. Valori validi: • Checksum: Una piccola rappresentazione a stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in un secondo momento per confrontare altri snapshot al fine di rilevare errori nei dati. (stringa) • SnapshotID: ID univoco di uno snapshot da cui viene creato il nuovo snapshot. Lo snapshotID deve provenire da uno snapshot sul volume specificato. (intero) • VolumeID (ID volume): L'ID del volume di origine per lo snapshot. (intero)	Array di oggetti JSON
GroupSnapshotID	ID univoco del nuovo snapshot di gruppo.	ID groupSnapshot
GroupSnapshot	Oggetto contenente informazioni sullo snapshot di gruppo appena creato.	GroupSnapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CreateGroupSnapshot",
   "params": {
      "volumes": [1,2]
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
```

```
  "id": 1,
  "result": {
    "groupSnapshot": {
      "attributes": {},
      "createTime": "2016-04-04T22:43:29Z",
      "groupSnapshotID": 45,
      "groupSnapshotUUID": "473b78a3-ef85-4541-9438-077306b2d3ca",
      "members": [
        {
          "attributes": {},
          "checksum": "0x0",
          "createTime": "2016-04-04T22:43:29Z",
          "enableRemoteReplication": false,
          "expirationReason": "None",
          "expirationTime": null,
          "groupID": 45,
          "groupSnapshotUUID": "473b78a3-ef85-4541-9438-077306b2d3ca",
          "name": "2016-04-04T22:43:29Z",
          "snapshotID": 3323,
          "snapshotUUID": "7599f200-0092-4b41-b362-c431551937d1",
          "status": "done",
          "totalSize": 5000658944,
          "virtualVolumeID": null,
          "volumeID": 1
        },
        {
          "attributes": {},
          "checksum": "0x0",
          "createTime": "2016-04-04T22:43:29Z",
          "enableRemoteReplication": false,
          "expirationReason": "None",
          "expirationTime": null,
          "groupID": 45,
          "groupSnapshotUUID": "473b78a3-ef85-4541-9438-077306b2d3ca",
          "name": "2016-04-04T22:43:29Z",
          "snapshotID": 3324,
          "snapshotUUID": "a0776a48-4142-451f-84a6-5315dc37911b",
          "status": "done",
          "totalSize": 6001000448,
          "virtualVolumeID": null,
          "volumeID": 2
        }
      ],
      "name": "2016-04-04T22:43:29Z",
      "status": "done"
    },
```

```
    "groupSnapshotID": 45,
    "members": [
      {
        "checksum": "0x0",
        "snapshotID": 3323,
        "snapshotUUID": "7599f200-0092-4b41-b362-c431551937d1",
        "volumeID": 1
      },
      {
        "checksum": "0x0",
        "snapshotID": 3324,
        "snapshotUUID": "a0776a48-4142-451f-84a6-5315dc37911b",
        "volumeID": 2
      }
    ]
  }
}
```


Novità dalla versione

9.6

CreateSchedule

È possibile utilizzare `CreateSchedule` per pianificare uno snapshot automatico di un volume a un intervallo definito.

È possibile utilizzare lo snapshot creato in un secondo momento come backup o rollback per garantire che i dati di un volume o gruppo di volumi siano coerenti per il momento in cui è stato creato lo snapshot. Se si pianifica l'esecuzione di uno snapshot in un periodo di tempo non divisibile di 5 minuti, lo snapshot verrà eseguito nel periodo di tempo successivo, divisibile di 5 minuti. Ad esempio, se si pianifica l'esecuzione di uno snapshot alle 12:42:00 UTC, questo verrà eseguito alle 12:45:00 UTC. Non è possibile pianificare l'esecuzione di uno snapshot a intervalli inferiori a 5 minuti.

È possibile creare snapshot se la completezza del cluster è nella fase 1, 2 o 3. Non è possibile creare snapshot quando la pienezza del cluster raggiunge la fase 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`attributes`	Utilizzare la stringa “frequency” per indicare la frequenza dell’istantanea. Valori possibili: • `Days of Week` • `Days of Month` • `Time Interval`	Oggetto JSON	Nessuno	No
`hasError`	**Guida con descrizione necessaria**	booleano	`false`	No
`hours`	Numero di ore tra snapshot ricorrenti o ore in GMT in cui lo snapshot viene eseguito in modalità giorni della settimana o giorni del mese. I valori validi vanno da 0 a 23.	intero	Nessuno	No
`lastRunStatus`	Il risultato o lo stato dell’ultima creazione di snapshot pianificata.	stringa	Nessuno	No
`name`	Il nome dello snapshot. Se non viene immesso alcun nome, vengono utilizzate la data e l’ora in cui è stata eseguita l’istantanea del gruppo. La lunghezza massima consentita per il nome è di 244 caratteri.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`minutes`	Numero di minuti tra snapshot ricorrenti o il minuto nell'ora GMT in cui lo snapshot viene eseguito in modalità giorni della settimana o giorni del mese. I valori validi vanno da 5 a 59.	intero	Nessuno	No
`paused`	Indica se il programma deve essere messo in pausa o meno. Valori validi: • `true` • `false`	booleano	Nessuno	No
`recurring`	Indica se la pianificazione sarà ricorrente o meno. I valori validi sono: • `true` • `false`	booleano	Nessuno	No
`runNextInterval`	Specifica se eseguire o meno lo snapshot alla successiva attivazione dello scheduler. Se impostato su true, lo snapshot pianificato viene eseguito alla successiva attivazione dello scheduler e viene reimpostato su false. I valori validi sono: • `true` • `false`	booleano	`false`	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`scheduleName`	Nome univoco per la pianificazione. La lunghezza massima consentita per il nome del programma è di 244 caratteri.	stringa	Nessuno	Sì
`scheduleType`	Indica il tipo di pianificazione da creare. Il valore valido è snapshot.	stringa	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`scheduleInfo`	Il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume del volume da cui è stato creato lo snapshot. Valori validi: • `volumeID`: L'ID del volume da includere nello snapshot. (intero) • `volumes`: Un elenco di ID volume da includere nello snapshot di gruppo. (array intero) • `name`: Il nome dello snapshot da utilizzare. (stringa) • `enableRemote Replication`Indica a se lo snapshot deve essere incluso nella replica remota. (booleano) • `retention`: La quantità di tempo in cui lo snapshot viene conservato in HH:mm:ss. Se vuoto, lo snapshot viene conservato per sempre. (stringa) • `fifo`: Lo snapshot viene conservato in base al principio FIFO (first-in-first-out). (stringa)	Oggetto JSON	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`snapMirrorLabel`	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No
`startingDate`	Tempo dopo il quale verrà eseguito il programma. Se non impostato, la pianificazione viene avviata immediatamente. Formattato in ora UTC.	Stringa di dati ISO 8601	Nessuno	No
`toBeDeleted`	Specifica che questa pianificazione di snapshot deve essere eliminata una volta completata la creazione dello snapshot.	booleano	`false`	No
`monthdays`	I giorni del mese in cui verrà creata un'istantanea. I valori validi vanno da 1 a 31.	array intero	Nessuno	Sì (se si pianifica per i giorni del mese)

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`weekdays`	Giorno della settimana in cui deve essere creata l'istantanea. Valori richiesti (se utilizzati): • `Day`: Da 0 a 6 (da domenica a sabato) • `Offset`: Per ogni settimana possibile in un mese, da 1 a 6 (se maggiore di 1, corrisponde solo il giorno n-1 della settimana. Ad esempio, offset:3 per domenica indica la terza domenica del mese, mentre offset:4 per mercoledì indica il quarto mercoledì del mese. Offset:0 significa che non viene eseguita alcuna azione. Offset:1 (impostazione predefinita) significa che lo snapshot viene creato per questo giorno della settimana, indipendentemente dalla posizione in cui cade nel mese)	Array di oggetti JSON	Nessuno	Sì (se si pianificano i giorni della settimana)

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

ScheduleId	ID della pianificazione creata.	intero
pianificazione	Oggetto contenente informazioni sulla pianificazione appena creata.	pianificazione

Richiedi esempio 1

Il seguente programma di esempio presenta i seguenti parametri:

- Non vengono specificati orari o minuti di inizio, pertanto il programma inizia il più vicino possibile fino alla mezzanotte (00:00:00Z).
- Non è ricorrente (viene eseguita una sola volta).
- Viene eseguito una volta la prima domenica o il mercoledì successivo al 1° giugno 2015, UTC 19:17:15Z (a seconda del giorno che si verifica per primo).
- Include un solo volume (ID volume = 1).

```
{
  "method":"CreateSchedule",
  "params":{
    "hours":0,
    "minutes":0,
    "paused":false,
    "recurring":false,
    "scheduleName":"MCAsnapshot1",
    "scheduleType":"snapshot",
    "attributes":{
      "frequency":"Days Of Week"
    },
    "scheduleInfo":{
      "volumeID":"1",
      "name":"MCA1"
    },
    "monthdays":[],
    "weekdays":[
      {
        "day":0,
        "offset":1
      },
      {
        "day":3,
        "offset":1
      }
    ],
    "startingDate":"2015-06-01T19:17:54Z"
  },
   "id":1
}
}
}
```

Esempio di risposta 1

La richiesta precedente restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "schedule": {
      "attributes": {
        "frequency": "Days Of Week"
      },
      "hasError": false,
      "hours": 0,
      "lastRunStatus": "Success",
      "lastRunTimeStarted": null,
      "minutes": 0,
      "monthdays": [],
      "paused": false,
      "recurring": false,
      "runNextInterval": false,
      "scheduleID": 4,
      "scheduleInfo": {
        "name": "MCA1",
        "volumeID": "1"
      },
      "scheduleName": "MCAsnapshot1",
      "scheduleType": "Snapshot",
      "startingDate": "2015-06-01T19:17:54Z",
      "toBeDeleted": false,
      "weekdays": [
        {
          "day": 0,
          "offset": 1
        },
        {
          "day": 3,
          "offset": 1
        }
      ]
    },
    "scheduleID": 4
  }
}
```


Richiedere l'esempio 2

Il seguente programma di esempio presenta i seguenti parametri:

- È ricorrente (viene eseguita a ogni intervallo pianificato del mese all'ora specificata).

- Viene eseguito il 1°, il 10°, il 15° e il 30° mese successivo alla data di inizio.
- Viene eseguito alle 12:15 ogni giorno in cui è pianificato.
- Include un solo volume (ID volume = 1).

```
{
  "method":"CreateSchedule",
    "params":{
      "hours":12,
      "minutes":15,
      "paused":false,
      "recurring":true,
      "scheduleName":"MCASnapshot1",
      "scheduleType":"snapshot",
      "attributes":{
        "frequency":"Days Of Month"
      },
      "scheduleInfo":{
        "volumeID":"1"
      },
      "weekdays":[
      ],
      "monthdays":[
        1,
        10,
        15,
        30
      ],
      "startingDate":"2015-04-02T18:03:15Z"
    },
    "id":1
}
```

Esempio di risposta 2

La richiesta precedente restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "schedule": {
      "attributes": {
        "frequency": "Days Of Month"
      },
      "hasError": false,
      "hours": 12,
      "lastRunStatus": "Success",
      "lastRunTimeStarted": null,
      "minutes": 15,
      "monthdays": [
        1,
        10,
        15,
        30
      ],
      "paused": false,
      "recurring": true,
      "runNextInterval": false,
      "scheduleID": 5,
      "scheduleInfo": {
        "volumeID": "1"
      },
      "scheduleName": "MCASnapshot1",
      "scheduleType": "Snapshot",
      "startingDate": "2015-04-02T18:03:15Z",
      "toBeDeleted": false,
      "weekdays": []
    },
      "scheduleID": 5
  }
}
```


Richiedere l'esempio 3

Il seguente programma di esempio presenta i seguenti parametri:

- Inizia entro 5 minuti dall'intervallo pianificato del 2 aprile 2015.
- È ricorrente (viene eseguita a ogni intervallo pianificato del mese all'ora specificata).
- Viene eseguito il secondo, il terzo e il quarto mese successivo alla data di inizio.
- Viene eseguito alle 14:45 ogni giorno in cui è pianificato.
- Include un gruppo di volumi (volumi = 1 e 2).

```
{
  "method":"CreateSchedule",
  "params":{
    "hours":14,
    "minutes":45,
    "paused":false,
    "recurring":true,
    "scheduleName":"MCASnapUser1",
    "scheduleType":"snapshot",
    "attributes":{
      "frequency":"Days Of Month"
    },
    "scheduleInfo":{
      "volumes":[1,2]
    },
    "weekdays":[],
    "monthdays":[2,3,4],
    "startingDate":"2015-04-02T20:38:23Z"
  },
  "id":1
}
```

Esempio di risposta 3

La richiesta precedente restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "schedule": {
      "attributes": {
        "frequency": "Days Of Month"
      },
      "hasError": false,
      "hours": 14,
      "lastRunStatus": "Success",
      "lastRunTimeStarted": null,
      "minutes": 45,
      "monthdays": [
        2,
        3,
        4
      ],
      "paused": false,
      "recurring": true,
      "runNextInterval": false,
      "scheduleID": 6,
      "scheduleInfo": {
        "volumes": [
          1,
          2
        ]
      },
      "scheduleName": "MCASnapUser1",
      "scheduleType": "Snapshot",
      "startingDate": "2015-04-02T20:38:23Z",
      "toBeDeleted": false,
      "weekdays": []
    },
    "scheduleID": 6
  }
}
```


Novità dalla versione

9.6

CreateSnapshot

È possibile utilizzare `CreateSnapshot` per creare una copia point-in-time di un volume. È possibile creare uno snapshot da qualsiasi volume o da uno snapshot esistente.

Se non si fornisce un SnapshotID con questo metodo API, viene creata una snapshot dalla diramazione attiva del volume. Se il volume da cui viene creato lo snapshot viene replicato in un cluster remoto, lo snapshot può essere replicato anche nella stessa destinazione. Utilizzare il parametro enableRemoteReplication per attivare la replica dello snapshot.

> È possibile creare snapshot se la completezza del cluster è nella fase 1, 2 o 3. Non è possibile creare snapshot quando la pienezza del cluster raggiunge la fase 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`attributes`	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
`enableRemoteReplication`	Specifica se lo snapshot verrà replicato o meno nello storage remoto. Valori possibili: • `true`: Lo snapshot verrà replicato nello storage remoto. • `false`: Lo snapshot non verrà replicato nello storage remoto.	booleano	falso	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`ensureSerialCreation`	Specifica che lo snapshot non deve essere creato se è in corso una replica dello snapshot precedente. I valori possibili sono: • `true`: In questo modo si garantisce la replica di un solo snapshot alla volta. La creazione di un nuovo snapshot non avrà esito positivo se è ancora in corso la replica di uno snapshot precedente. • `false`: Predefinito. Questa creazione di snapshot è consentita se è ancora in corso la replica di un altro snapshot.	booleano	`false`	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ExpirationTime (tempo di scadenza)	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con `retention`. Se non si specifica ExpirationTime o Retention, lo snapshot non scadrà. Il formato dell'ora è una stringa di date ISO 8601 per la scadenza basata sull'ora, altrimenti non scadrà. Un valore di `null` fa sì che lo snapshot venga conservato in modo permanente. Un valore di `fifo` Fa in modo che lo snapshot venga conservato in base al principio "first-in-first-out", rispetto ad altri snapshot FIFO sul volume. L'API non riesce se non è disponibile spazio FIFO.	stringa	Nessuno	No
`name`	Il nome dello snapshot. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stata eseguita l'istantanea. La lunghezza massima consentita per il nome è di 255 caratteri.	stringa	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`retention`	Questo parametro è lo stesso di `expirationTime` Il parametro, ad eccezione del formato dell'ora, è HH:mm:ss. In caso contrario `expirationTime` né così `retention` sono specificati, lo snapshot non scadrà.	stringa	Nessuno	No
`snapMirrorLabel`	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No
`snapshotID`	ID univoco di uno snapshot da cui viene creato il nuovo snapshot. Lo snapshotID passato deve essere uno snapshot sul volume specificato.	intero	Nessuno	No
`volumeID`	ID univoco dell'immagine del volume da cui copiare.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

checksum	Stringa che rappresenta le cifre corrette nello snapshot memorizzato. Questo checksum può essere utilizzato in un secondo momento per confrontare altri snapshot al fine di rilevare errori nei dati.	stringa
SnapshotID	ID univoco della nuova istantanea.	ID snapshot
snapshot	Oggetto contenente informazioni sullo snapshot appena creato.	snapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "CreateSnapshot",
   "params": {
      "volumeID": 1
   },
   "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "checksum": "0x0",
      "snapshot": {
        "attributes": {},
        "checksum": "0x0",
        "createTime": "2016-04-04T17:14:03Z",
        "enableRemoteReplication": false,
        "expirationReason": "None",
        "expirationTime": null,
        "groupID": 0,
        "groupSnapshotUUID": "00000000-0000-0000-0000-000000000000",
        "name": "2016-04-04T17:14:03Z",
        "snapshotID": 3110,
        "snapshotUUID": "6f773939-c239-44ca-9415-1567eae79646",
        "status": "done",
        "totalSize": 5000658944,
        "virtualVolumeID": null,
        "volumeID": 1
      },
        "snapshotID": 3110
  }
}
```


Eccezione

Viene visualizzata un'eccezione xNotPrimary quando `CreateSnapshot` API viene chiamata e lo snapshot non viene creato. Questo è il comportamento previsto. Riprovare `CreateSnapshot` Chiamata API.

Novità dalla versione

9.6

DeleteGroupSnapshot

È possibile utilizzare `DeleteGroupSnapshot` per eliminare uno snapshot di gruppo.

È possibile utilizzare il parametro saveMembers per conservare tutte le snapshot create per i volumi nel gruppo, ma l'associazione di gruppo verrà rimossa.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
GroupSnapshotID	ID univoco dello snapshot di gruppo.	intero	Nessuno	Sì
SaveMembers	Specifica cosa eliminare quando si elimina uno snapshot di gruppo. Valori validi: • Vero: Gli snapshot vengono conservati, ma l'associazione di gruppo viene rimossa. • Falso: Il gruppo e le istantanee vengono cancellati.	booleano	falso	No

Valore restituito

Questo metodo non ha alcun valore restituito.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteGroupSnapshot",
     "params": {
       "groupSnapshotID": 10,
       "saveMembers" : true
        },
     "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9.6

DeleteSnapshot

È possibile utilizzare `DeleteSnapshot` metodo per eliminare uno snapshot.

Non è possibile eliminare uno snapshot attualmente attivo. È necessario eseguire il rollback e rendere attivo un altro snapshot prima di poter eliminare lo snapshot corrente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SnapshotID	L'ID dello snapshot da eliminare.	intero	Nessuno	Sì
OverrideSnapMirror Hold	Eseguire l'override del blocco posizionato sugli snapshot durante la replica. È possibile utilizzare questo parametro per eliminare le snapshot di SnapMirror obsolete dopo l'eliminazione della relazione SnapMirror associata.	booleano	falso	No

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "DeleteSnapshot",
"params": {
"snapshotID": 8,
"overrideSnapMirrorHold": true
},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9.6

Trova ulteriori informazioni

RollbackToSnapshot

GetSchedule

È possibile utilizzare `GetSchedule` per ottenere informazioni su uno snapshot pianificato.

È possibile visualizzare informazioni su una pianificazione specifica se nel sistema sono presenti molte pianificazioni di snapshot. È inoltre possibile recuperare informazioni su più pianificazioni con questo metodo specificando ID aggiuntivi nel parametro ScheduleId.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ScheduleId	ID univoco della pianificazione o di più pianificazioni da visualizzare.	intero	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
pianificazione	Un array di attributi di pianificazione.	pianificazione array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
"method": "GetSchedule",
  "params": {
              "scheduleID" : 2
      },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "schedule": {
      "attributes": {
        "frequency": "Time Interval"
      },
       "hasError": false,
       "hours": 0,
       "lastRunStatus": "Success",
       "lastRunTimeStarted": "2015-03-23T21:25:00Z",
       "minutes": 2,
       "monthdays": [],
       "paused": false,
       "recurring": true,
       "runNextInterval": false,
       "scheduleID": 2,
       "scheduleInfo": {
          "name": "MCA2",
          "volumeID": "3"
       },
       "scheduleName": "MCAsnapshot2",
       "scheduleType": "Snapshot",
       "startingDate": "2015-03-23T19:28:57Z",
       "toBeDeleted": false,
       "weekdays": []
      }
   }
}
```


Novità dalla versione

9.6

ListGroupSnapshot

È possibile utilizzare `ListGroupSnapshots` metodo per restituire informazioni su tutti gli snapshot di gruppo creati.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
GroupSnapshotID	Recuperare le informazioni per un ID snapshot di gruppo singolo.	intero	Nessuno	No
volumi	Array di ID di volume univoci da interrogare. Se non si specifica questo parametro, vengono incluse tutte le snapshot di gruppo nel cluster.	Array volumeID	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
GroupSnapshot	Un elenco di oggetti contenente informazioni su ogni snapshot di gruppo.	GroupSnapshot array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListGroupSnapshots",
  "params": {
  "volumes": [
     31,
     49
    ]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "groupSnapshots": [
```

```
      {
          "status": "Done",
          "remoteStatuses": [
              {
                "volumePairUUID": "abcdef-1234-5678-90ab-cdef0123",
                "remoteStatus": "Present"
              }
          ],
          "attributes": {},
          "groupSnapshotID": 1,
          "createTime": "2014-06-17T17:35:05Z",
          "members": [
              {
                "snapshotUUID": "abcdef-1234-5678-90ab-cdef0123",
                "expirationReason": "None",
                "virtualVolumeID": "abcdef-1234-5678-90ab-cdef0123",
                "groupID": 1,
                "createTime": "2014-06-17T17:35:05Z",
                "totalSize": 1,
                "snapMirrorLabel": "test1",
                "volumeName": "test1",
                "instanceCreateTime": "2014-06-17T17:35:05Z",
                "volumeID": 1,
                "checksum": "0x0",
                "attributes": {},
                "instanceSnapshotUUID": "abcdef-1234-5678-90ab-cdef0123",
                "snapshotID": 1,
                "status": "Done",
                "groupSnapshotUUID": "abcdef-1234-5678-90ab-cdef0123",
                "expirationTime": "2014-06-17T17:35:05Z",
                "enableRemoteReplication": true,
                "name": "test1",
                "remoteStatuses": [
                      {
                        "volumePairUUID": "abcdef-1234-5678-90ab-
cdef0123",
                        "remoteStatus": "Present"
                      }
                  ]
              }
          ],
          "enableRemoteReplication": true,
          "name": "test1",
          "groupSnapshotUUID": "abcdef-1234-5678-90ab-cdef0123"
      }
    ]
```

```
}
```

Novità dalla versione

9.6

Elenchi

È possibile utilizzare `ListSchedules` per ottenere informazioni su tutti gli snapshot pianificati creati.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
pianificazioni	Un elenco delle pianificazioni attualmente presenti nel cluster.	pianificazione array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListSchedules",
    "params": {},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "schedules": [
      {
       "attributes": {
         "frequency": "Days Of Week"
       },
       "hasError": false,
```

```
      "hours": 0,
      "lastRunStatus": "Success",
      "lastRunTimeStarted": null,
      "minutes": 1,
      "monthdays": [],
      "paused": false,
      "recurring": false,
      "runNextInterval": false,
      "scheduleID": 3,
      "scheduleInfo": {
           "name": "Wednesday Schedule",
           "retention": "00:02:00",
           "volumeID": "2"
    },
    "scheduleName": "Vol2Schedule",
    "scheduleType": "Snapshot",
    "startingDate": "2015-03-23T20:08:33Z",
    "toBeDeleted": false,
    "weekdays": [
        {
          "day": 3,
          "offset": 1
        }
   ]
  },
  {
    "attributes": {
        "frequency": "Time Interval"
    },
     "hasError": false,
     "hours": 0,
     "lastRunStatus": "Success",
     "lastRunTimeStarted": "2015-03-23T21:40:00Z",
     "minutes": 2,
     "monthdays": [],
     "paused": false,
     "recurring": true,
     "runNextInterval": false,
     "scheduleID": 2,
     "scheduleInfo": {
          "name": "MCA2",
          "volumeID": "3"
     },
     "scheduleName": "MCAsnapshot2",
     "scheduleType": "Snapshot",
     "startingDate": "2015-03-23T19:28:57Z",
```

```
        "toBeDeleted": false,
        "weekdays": []
        }
      ]
   }
}
```

Novità dalla versione

9.6

ListSnapshot

È possibile utilizzare `ListSnapshots` per restituire gli attributi di ogni snapshot creato sul volume.

Le informazioni sugli snapshot che risiedono nel cluster di destinazione verranno visualizzate nel cluster di origine quando questo metodo viene chiamato dal cluster di origine.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	Recupera le snapshot di un volume. Se volumeID non viene fornito, vengono restituiti tutti gli snapshot per tutti i volumi.	intero	Nessuno	No
SnapshotID	Recupera le informazioni per un singolo ID snapshot.	intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
snapshot	Informazioni su ogni snapshot per ciascun volume. Se volumeID non viene fornito, vengono restituiti tutti gli snapshot per tutti i volumi. Gli snapshot di un gruppo vengono restituiti con un ID di gruppo.	snapshot array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListSnapshots",
   "params": {
             "volumeID": "1"
       },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "snapshots": [
        {
          "attributes": {},
          "checksum": "0x0",
          "createTime": "2015-05-08T13:15:00Z",
          "enableRemoteReplication": true,
          "expirationReason": "None",
          "expirationTime": "2015-05-08T21:15:00Z",
          "groupID": 0,
          "groupSnapshotUUID": "00000000-0000-0000-0000-000000000000",
          "name": "Hourly",
          "remoteStatuses": [
              {
                "remoteStatus": "Present",
                "volumePairUUID": "237e1cf9-fb4a-49de-a089-a6a9a1f0361e"
              }
         ],
          "snapshotID": 572,
          "snapshotUUID": "efa98e40-cb36-4c20-a090-a36c48296c14",
          "status": "done",
          "totalSize": 10000269312,
          "volumeID": 1
        }
      ]
    }
  }
```


Novità dalla versione

9.6

ModifyGroupSnapshot

È possibile utilizzare `ModifyGroupSnapshot` per modificare gli attributi di un gruppo di snapshot. È inoltre possibile utilizzare questo metodo per consentire la replica remota degli snapshot creati sul volume di lettura/scrittura (di origine) in un sistema di storage di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio

EnableRemoteReplication	Consente di attivare la replica dello snapshot creato in un cluster remoto. Valori possibili: • `true`: Lo snapshot verrà replicato nello storage remoto. • `false`: Lo snapshot non verrà replicato nello storage remoto.	booleano	falso	No
ExpirationTime (tempo di scadenza)	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con la conservazione. Se non vengono specificati né expirationTime, né la conservazione sullo snapshot originale, lo snapshot non scadrà. Il formato dell'ora è una stringa di date ISO 8601 per la scadenza basata sull'ora, altrimenti non scadrà. Un valore di `null` fa sì che lo snapshot venga conservato in modo permanente. Un valore di fifo fa sì che lo snapshot venga conservato in base al principio FIFO (first-in-first-out), rispetto ad altri snapshot FIFO sul volume. L'API non riesce se non è disponibile spazio FIFO.	Stringa di dati ISO 8601	Nessuno	No

nome	Il nome dello snapshot di gruppo. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stata eseguita l'istantanea del gruppo. La lunghezza massima consentita per il nome è di 255 caratteri.	stringa	Nessuno	No
GroupSnapshotID	L'ID del gruppo di snapshot.	stringa	Nessuno	Sì
SnapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
GroupSnapshot	Oggetto contenente informazioni sullo snapshot di gruppo appena modificato.	GroupSnapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 695,
  "method": "ModifyGroupSnapshot",
  "params": {
    "groupSnapshotID": 3,
    "enableRemoteReplication": true,
    "expirationTime": "2016-04-08T22:46:25Z"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 695,
  "result": {
    "groupSnapshot": {
      "attributes": {},
      "createTime": "2016-04-06T17:31:41Z",
      "groupSnapshotID": 3,
      "groupSnapshotUUID": "8b2e101d-c5ab-4a72-9671-6f239de49171",
      "members": [
        {
          "attributes": {},
          "checksum": "0x0",
          "createTime": "2016-04-06T17:31:41Z",
          "enableRemoteReplication": true,
          "expirationReason": "None",
          "expirationTime": "2016-04-08T22:46:25Z",
          "groupID": 3,
          "groupSnapshotUUID": "8b2e101d-c5ab-4a72-9671-6f239de49171",
          "name": "grpsnap1-2",
          "snapshotID": 2,
          "snapshotUUID": "719b162c-e170-4d80-b4c7-1282ed88f4e1",
          "status": "done",
          "totalSize": 1000341504,
          "virtualVolumeID": null,
          "volumeID": 2
        }
      ],
      "name": "grpsnap1",
      "status": "done"
    }
  }
}
```


Novità dalla versione

9.6

ModifySchedule

È possibile utilizzare `ModifySchedule` per modificare gli intervalli in cui si verifica uno snapshot pianificato. Questo metodo consente inoltre di eliminare o mettere in pausa un programma.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
attributi	Consente di modificare la frequenza dell'occorrenza dello snapshot. Valori possibili: • `Days of Week` • `Days of Month` • `Time Interval`	Oggetto JSON	Nessuno	No
ore	Numero di ore tra snapshot o ore in cui lo snapshot viene eseguito in modalità giorni della settimana o giorni del mese. I valori validi vanno da 0 a 24.	stringa	Nessuno	No
nome	Il nome dello snapshot. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stata eseguita l'istantanea del gruppo. La lunghezza massima consentita per il nome è di 244 caratteri.	stringa	Nessuno	No

minuti	Numero di minuti tra snapshot o minuti in cui si verificherà l'istantanea in modalità giorni della settimana o giorni del mese. I valori validi vanno da 0 a 59.	intero	Nessuno	No
LastRunStatus	Il risultato o lo stato dell'ultima creazione di snapshot pianificata.	stringa	Nessuno	No
in pausa	Indica se il programma deve essere messo in pausa o meno. Valori validi: • `true` • `false`	booleano	Nessuno	No
ricorrente	Indica se la pianificazione sarà ricorrente o meno. I valori validi sono: • `true` • `false`	booleano	Nessuno	No

RunNextInterval	Consente di scegliere se eseguire o meno lo snapshot alla successiva attivazione dello scheduler. Valori validi: • `true` • `false` Se impostato su true, lo snapshot pianificato viene eseguito alla successiva attivazione dello scheduler, quindi viene reimpostato su false.	booleano	falso	No
ScheduleId	ID univoco della pianificazione.	intero	Nessuno	Sì
Nome scheduleName	Nome univoco per la pianificazione. La lunghezza massima consentita per il nome del programma è di 244 caratteri.	stringa	Nessuno	No
Tipo di scheduleType	Indica il tipo di pianificazione da creare. L'unico valore supportato è `snapshot`.	stringa	Nessuno	Sì

`scheduleInfo`	Il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume del volume da cui è stato creato lo snapshot. Valori validi: • `enableRemoteReplication`Indica se lo snapshot deve essere incluso nella replica remota. (booleano) • `ensureSerialCreation`: Specifica se deve essere consentita la creazione di un nuovo snapshot se è in corso una replica snapshot precedente. (booleano) • `name`: Il nome dello snapshot da utilizzare. (stringa) • `retention`: Periodo di tempo durante il quale l'istantanea viene conservata. A seconda dell'ora, viene visualizzato in uno dei seguenti formati: ◦ `fifo`: L'istantanea viene conservata in base al FIFO (First-in-First-out). Se vuoto, lo	"pianificazione"	Nessuno	No

SnapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No
ToDeleted	Indica se la pianificazione è contrassegnata per l'eliminazione. Valori validi: • `true` • `false`	booleano	Nessuno	No
Data di inizio	Indica la data alla prima volta in cui inizia o inizierà la pianificazione.	Stringa di dati ISO 8601	Nessuno	No
monthdays	I giorni del mese in cui verrà creata un'istantanea. I valori validi vanno da 1 a 31.	array intero	Nessuno	Sì
giorni feriali	Giorno della settimana in cui deve essere creata l'istantanea. Il giorno della settimana inizia la domenica con il valore 0 e un offset di 1.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
pianificazione	Oggetto contenente gli attributi di pianificazione modificati.	pianificazione

Esempio di richiesta

```
{
  "method": "ModifySchedule",
  "params": {
    "scheduleName" : "Chicago",
    "scheduleID" : 3
    },
  "id": 1
}
```

Esempio di risposta

```
{
  "id": 1,
  "result": {
    "schedule": {
      "attributes": {
        "frequency": "Days Of Week"
            },
      "hasError": false,
      "hours": 5,
      "lastRunStatus": "Success",
      "lastRunTimeStarted": null,
      "minutes": 0,
      "monthdays": [],
      "paused": false,
      "recurring": true,
      "runNextInterval": false,
      "scheduleID": 3,
      "scheduleInfo": {
        "volumeID": "2"
            },
      "scheduleName": "Chicago",
      "scheduleType": "Snapshot",
      "startingDate": null,
      "toBeDeleted": false,
      "weekdays": [
        {
          "day": 2,
          "offset": 1
      }
      ]
    }
  }
}
```


Novità dalla versione

9.6

ModifySnapshot

È possibile utilizzare `ModifySnapshot` per modificare gli attributi attualmente assegnati a uno snapshot. È inoltre possibile utilizzare questo metodo per consentire la replica remota degli snapshot creati sul volume di lettura/scrittura (di origine) in un cluster di storage di destinazione che esegue il software Element.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
EnableRemoteReplication	Consente di replicare lo snapshot creato in un cluster di storage remoto. Valori possibili: • `true`: Lo snapshot verrà replicato nello storage remoto. • `false`:Lo snapshot non verrà replicato nello storage remoto.	booleano	falso	No

ExpirationTime (tempo di scadenza)	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con la conservazione. Se non vengono specificati né expirationTime, né la conservazione sullo snapshot originale, lo snapshot non scadrà. Il formato dell'ora è una stringa di date ISO 8601 per la scadenza basata sull'ora, altrimenti non scadrà. Il valore Null fa sì che lo snapshot venga conservato in modo permanente. Un valore di fifo fa sì che lo snapshot venga conservato in base al principio FIFO (first-in-first-out), rispetto ad altri snapshot FIFO sul volume. L'API non riesce se non è disponibile spazio FIFO.	Stringa di dati ISO 8601	Nessuno	No
nome	Il nome dello snapshot. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stata eseguita l'istantanea. La lunghezza massima consentita per il nome è di 255 caratteri.	stringa	Nessuno	No

SnapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare il criterio di conservazione delle snapshot su un endpoint SnapMirror.	stringa	Nessuno	No
SnapshotID	Identificatore dello snapshot.	stringa	Nessuno	Sì

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
snapshot	Oggetto contenente informazioni sullo snapshot appena modificato.	snapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifySnapshot",
  "params": {
    "snapshotID": 3114,
    "enableRemoteReplication": "true",
    "name" : "Chicago"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "snapshot": {
      "attributes": {},
      "checksum": "0x0",
      "createTime": "2016-04-04T17:26:20Z",
      "enableRemoteReplication": true,
      "expirationReason": "None",
      "expirationTime": null,
      "groupID": 0,
      "groupSnapshotUUID": "00000000-0000-0000-0000-000000000000",
      "name": "test1",
      "snapshotID": 3114,
      "snapshotUUID": "5809a671-4ad0-4a76-9bf6-01cccf1e65eb",
      "status": "done",
      "totalSize": 5000658944,
      "virtualVolumeID": null,
      "volumeID": 1
    }
  }
}
```


Novità dalla versione

9.6

RollbackToGroupSnapshot

È possibile utilizzare `RollbackToGroupSnapshot` per eseguire il rollback di tutti i singoli volumi di un gruppo di snapshot in ogni singolo snapshot del volume.

Il rollback a uno snapshot di gruppo crea uno snapshot temporaneo di ciascun volume all'interno dello snapshot di gruppo.

- La creazione di uno snapshot è consentita se la completezza del cluster è nella fase 1, 2 o 3. Gli snapshot non vengono creati quando la completezza del cluster è nella fase 4 o 5.
- Il rollback dei volumi in uno snapshot di gruppo potrebbe non riuscire quando è in corso la sincronizzazione delle sezioni. Riprovare `RollbackToGroupSnapshot` al termine della sincronizzazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
`groupSnapshotID`	ID univoco dello snapshot di gruppo.	intero	Nessuno	Sì
`attributes`	Elenco delle coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	No
`name`	Nome dello snapshot di gruppo dello stato corrente del volume creato se `saveCurrentState` è impostato su true. Se non si assegna un nome, il nome degli snapshot (gruppo e volume singolo) viene impostato su un'indicazione temporale dell'ora in cui si è verificato il rollback.	stringa	Nessuno	No
`saveCurrentState`	Specifica se salvare o meno l'immagine del volume attivo precedente. Valori validi: • `true`: Viene mantenuta l'immagine del volume attivo precedente. • `false`: L'immagine del volume attivo precedente viene eliminata.	booleano	falso	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

membri	Array contenente volumeID e snapshotID dei membri dello snapshot di gruppo. Valori: • Checksum: Una piccola rappresentazione a stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in un secondo momento per confrontare altri snapshot al fine di rilevare errori nei dati. (stringa) • SnapshotID: ID univoco di uno snapshot da cui viene creato il nuovo snapshot. Lo snapshotID deve essere uno snapshot sul volume specificato. (intero) • VolumeID (ID volume): L'ID del volume di origine per lo snapshot. (intero)	Array di oggetti JSON
GroupSnapshotID	Se `saveCurrentState` è stato impostato su false, questo valore è nullo. Se `saveCurrentState` È stato impostato su true, l'ID univoco dello snapshot di gruppo appena creato.	intero
GroupSnapshot	Se `saveCurrentState` è stato impostato su false, questo valore è nullo. Se `saveCurrentState` è stato impostato su true, un oggetto contenente informazioni sullo snapshot di gruppo che `RollbackToGroupSnapshot` è stato appena eseguito il rollback a.	GroupSnapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 438,
  "method": "RollbackToGroupSnapshot",
  "params": {
    "groupSnapshotID": 1,
    "name": "grpsnap1",
    "saveCurrentState": true
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 438,
  "result": {
    "groupSnapshot": {
      "attributes": {},
      "createTime": "2016-04-06T17:27:17Z",
      "groupSnapshotID": 1,
      "groupSnapshotUUID": "468fe181-0002-4b1d-ae7f-8b2a5c171eee",
      "members": [
        {
          "attributes": {},
          "checksum": "0x0",
          "createTime": "2016-04-06T17:27:17Z",
          "enableRemoteReplication": false,
          "expirationReason": "None",
          "expirationTime": null,
          "groupID": 1,
          "groupSnapshotUUID": "468fe181-0002-4b1d-ae7f-8b2a5c171eee",
          "name": "2016-04-06T17:27:17Z",
          "snapshotID": 4,
          "snapshotUUID": "03563c5e-51c4-4e3b-a256-a4d0e6b7959d",
          "status": "done",
          "totalSize": 1000341504,
          "virtualVolumeID": null,
          "volumeID": 2
        }
      ],
      "name": "2016-04-06T17:27:17Z",
      "status": "done"
    },
    "groupSnapshotID": 3,
    "members": [
      {
        "checksum": "0x0",
        "snapshotID": 2,
        "snapshotUUID": "719b162c-e170-4d80-b4c7-1282ed88f4e1",
        "volumeID": 2
      }
    ]
  }
}
```


Novità dalla versione

9.6

RollbackToSnapshot

È possibile utilizzare `RollbackToSnapshot` metodo per creare un'istantanea esistente dell'immagine del volume attivo. Questo metodo crea un nuovo snapshot da uno snapshot esistente.

Il nuovo snapshot diventa attivo e lo snapshot esistente viene conservato fino a quando non viene eliminato manualmente. Lo snapshot precedentemente attivo viene cancellato a meno che non si imposta il parametro saveCurrentState su true.

CLUSTER_FULLNESS

- È possibile creare snapshot se la completezza del cluster è nella fase 1, 2 o 3. Non è possibile creare snapshot quando la pienezza del cluster raggiunge la fase 4 o 5.
- Il rollback di un volume a uno snapshot potrebbe non riuscire quando è in corso la sincronizzazione delle sezioni. Riprovare `RollbackToSnapshot` al termine della sincronizzazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ID volume	VolumeID per il volume.	intero	Nessuno	Sì
attributi	Elenco delle coppie nome-valore nel formato oggetto JSON.	Attributi JSON	Nessuno	No
nome	Nome dello snapshot. Se non viene fornito alcun nome, il nome dello snapshot di cui viene eseguito il rollback viene utilizzato con "-copy" aggiunto alla fine del nome.	stringa	Nessuno	No
SnapshotID	ID di uno snapshot creato in precedenza sul volume specificato.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
SaveCurrentState	Consente di specificare se salvare o meno l'immagine del volume attivo precedente. Valori validi: • True (vero): Viene mantenuta l'immagine del volume attivo precedente. • Falso: L'immagine del volume attivo precedente viene eliminata.	booleano	falso	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
checksum	Una piccola rappresentazione a stringa dei dati nello snapshot memorizzato.	stringa
SnapshotID	Se saveCurrentState è stato impostato su false, questo valore è nullo. Se saveCurrentState è stato impostato su true, l'ID univoco dello snapshot appena creato.	intero
snapshot	Se saveCurrentState è stato impostato su false, questo valore è nullo. Se saveCurrentState è stato impostato su true, un oggetto contenente informazioni sullo snapshot appena creato.	snapshot

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
 "method": "RollbackToSnapshot",
 "params": {
    "volumeID": 1,
    "snapshotID": 3114,
    "saveCurrentState": true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "checksum": "0x0",
    "snapshot": {
      "attributes": {},
      "checksum": "0x0",
      "createTime": "2016-04-04T17:27:32Z",
      "enableRemoteReplication": false,
      "expirationReason": "None",
      "expirationTime": null,
      "groupID": 0,
      "groupSnapshotUUID": "00000000-0000-0000-0000-000000000000",
      "name": "test1-copy",
      "snapshotID": 1,
      "snapshotUUID": "30d7e3fe-0570-4d94-a8d5-3cc8097a6bfb",
      "status": "done",
      "totalSize": 5000658944,
      "virtualVolumeID": null,
      "volumeID": 1
    },
    "snapshotID": 1
  }
}
```

Novità dalla versione

9.6

Metodi API dei volumi virtuali

I metodi API dei volumi virtuali del software Element consentono di gestire i volumi virtuali (VVol). È possibile visualizzare i VVol esistenti con questi metodi API, nonché creare, modificare ed eliminare i container di storage dei volumi virtuali. Sebbene non sia possibile utilizzare questi metodi per operare su volumi normali, è possibile utilizzare i normali metodi API del volume per elencare le informazioni su VVol.

- CreateStorageContainer
- DeleteStorageContainers
- GetStorageContainerEfficiency
- GetVirtualVolumeCount
- ListProtocolEndpoint
- ListStorageContainers
- ListVirtualVolumeBindings
- ListVirtualVolumeHost
- ListVirtualVolumes
- ListVirtualVolumeTasks
- ModifyStorageContainer

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

CreateStorageContainer

È possibile utilizzare `CreateStorageContainer` Metodo per creare un contenitore di storage Virtual Volume (Vol). È possibile utilizzare i container di storage per la creazione di report e l'allocazione delle risorse. Per utilizzare la funzione volumi virtuali, è necessario creare almeno un container di storage.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
nome	Nome del contenitore di storage. Segue le restrizioni di denominazione degli account software Element.	stringa	Nessuno	Sì
ID account	Account container non di storage che diventerà un container di storage.	intero	Nessuno	No
InitatorSecret	Il segreto per l'autenticazione CHAP per l'iniziatore.	stringa	Nessuno	No
TargetSecret	Il segreto per l'autenticazione CHAP per la destinazione.	stringa	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
StorageContainer	Oggetto contenente informazioni sul contenitore di storage appena creato.	StorageContainer

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "CreateStorageContainer",
    "params": {
        "name" : "example"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "storageContainer": {
      "accountID": 8,
      "initiatorSecret": "rVTOi25^H.d;cP}l",
      "name": "example",
      "protocolEndpointType": "SCSI",
      "status": "active",
      "storageContainerID": "a9ec1138-e386-4a44-90d7-b9acbbc05176",
      "targetSecret": "6?AEIxWpvo6,!boM"
    }
  }
}
```

Novità dalla versione

9.6

DeleteStorageContainers

È possibile utilizzare `DeleteStorageContainers` Metodo per rimuovere fino a 2000 container di storage Virtual Volume (Vol) dal sistema contemporaneamente. I contenitori di storage rimossi non devono contenere VVol.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
StorageContainerID	Un elenco di ID dei contenitori di storage da eliminare. È possibile specificare fino a 2000 ID nell'elenco.	Array UUID	Nessuno	Sì

Valori restituiti

Questo metodo non ha valori restituiti.

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "DeleteStorageContainers",
    "params": {
        "storageContainerIDs" : ["a9ec1138-e386-4a44-90d7-b9acbbc05176"]
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {}
}
```

Novità dalla versione

9.6

GetStorageContainerEfficiency

È possibile utilizzare `GetStorageContainerEfficiency` metodo per recuperare informazioni sull'efficienza di un container di storage di volumi virtuali.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
StorageContainerID	ID del container di storage per il quale recuperare le informazioni sull'efficienza.	intero	Nessuno	Sì

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo

compressione	La quantità di spazio risparmiata dalla compressione dei dati per tutti i volumi virtuali nel container di storage. Indicato come rapporto in cui il valore 1 indica che i dati sono stati memorizzati senza compressione.	fluttuare
deduplica	La quantità di spazio risparmiata non duplicando i dati per tutti i volumi virtuali nel container di storage. Indicato come rapporto.	fluttuare
MissingVolumes	I volumi virtuali che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati dal ciclo di Garbage Collection (GC) che ha meno di un'ora, dalla perdita temporanea della connettività di rete o dal riavvio dei servizi dal ciclo GC.	array intero
ThinProvisioning	Il rapporto tra lo spazio utilizzato e la quantità di spazio allocato per la memorizzazione dei dati. Indicato come rapporto.	fluttuare
data e ora	L'ultima volta in cui sono stati raccolti i dati di efficienza dopo GC.	Stringa di dati ISO 8601

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetStorageContainerEfficiency",
  "params": {
    "storageContainerID" : "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "compression": 1,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1,
    "timestamp": "2016-04-12T15:39:49Z"
  }
}
```

Novità dalla versione

9.6

GetVirtualVolumeCount

È possibile utilizzare `GetVirtualVolumeCount` metodo per recuperare il numero di volumi virtuali attualmente presenti nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
conta	Il numero di volumi virtuali attualmente presenti nel sistema.	intero

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "GetVirtualVolumeCount",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "count": 5
  }
}
```

Novità dalla versione

9.6

ListProtocolEndpoint

È possibile utilizzare `ListProtocolEndpoints` metodo per recuperare informazioni su tutti gli endpoint del protocollo nel cluster. Gli endpoint del protocollo regolano l'accesso ai contenitori di storage dei volumi virtuali associati.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
ProtocolEndpointID	Un elenco di ID endpoint del protocollo per i quali recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti gli endpoint del protocollo.	Array UUID ProtocolEndpointID	Nessuno	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
ProtocolEndpoint	Elenco di oggetti contenenti informazioni su ciascun endpoint del protocollo nel sistema.	ProtocolEndpoint array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "id": 1,
  "method": "ListProtocolEndpoints",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "protocolEndpoints": [
      {
        "primaryProviderID": 1,
        "protocolEndpointID": "1387e257-d2e3-4446-be6d-39db71583e7b",
        "protocolEndpointState": "Active",
        "providerType": "Primary",
        "scsiNAADeviceID": "6f47acc2000000016970687200000000",
        "secondaryProviderID": 2
      },
      {
        "primaryProviderID": 2,
        "protocolEndpointID": "1f16ed86-3f31-4c76-b004-a1251187700b",
        "protocolEndpointState": "Active",
        "providerType": "Primary",
        "scsiNAADeviceID": "6f47acc2000000026970687200000000",
        "secondaryProviderID": 3
      },
      {
        "primaryProviderID": 4,
        "protocolEndpointID": "c6458dfe-9803-4350-bb4e-68a3feb7e830",
        "protocolEndpointState": "Active",
        "providerType": "Primary",
        "scsiNAADeviceID": "6f47acc2000000046970687200000000",
        "secondaryProviderID": 1
      },
      {
        "primaryProviderID": 3,
        "protocolEndpointID": "f3e7911d-0e86-4776-97db-7468c272213f",
        "protocolEndpointState": "Active",
        "providerType": "Primary",
        "scsiNAADeviceID": "6f47acc2000000036970687200000000",
        "secondaryProviderID": 4
      }
    ]
  }
}
```


Novità dalla versione

9.6

ListStorageContainers

È possibile utilizzare `ListStorageContainers` metodo per recuperare informazioni su tutti i container di storage dei volumi virtuali noti al sistema.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
StorageContainerID	Un elenco di ID container di storage per i quali recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti i contenitori di storage nel sistema.	Array UUID	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
StorageContainers	Elenco di oggetti contenenti informazioni su tutti i contenitori di storage nel sistema.	StorageContainer array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
   "method": "ListStorageContainers",
   "params": {
      "storageContainerIDs": ["efda8307-b916-4424-979e-658a3f16894d"]
   },
   "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 6395,
  "result": {
    "storageContainers": [
      {
        "accountID": 64,
        "initiatorSecret": "EJ:08An1MyNQmL!7",
        "name": "VvolContainer",
        "protocolEndpointType": "SCSI",
        "status": "active",
        "storageContainerID": "efda8307-b916-4424-979e-658a3f16894d",
        "targetSecret": "g38}zWBK%206jQr~",
        "virtualVolumes": []
      }
    ]
  }
}
```


Novità dalla versione

9.6

ListVirtualVolumeBindings

È possibile utilizzare `ListVirtualVolumeBindings` metodo per ottenere un elenco di tutti i volumi virtuali nel cluster associati agli endpoint del protocollo.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualVolumeBindingID	Un elenco di ID di binding dei volumi virtuali per i quali recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti i binding di volumi virtuali.	array intero	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
associazioni	Un elenco di oggetti che descrivono tutti i volumi virtuali nel cluster associati agli endpoint del protocollo.	binding

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVirtualVolumeBindings",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "bindings": [
      {
        "protocolEndpointID": "5dd53da0-b9b7-43f9-9b7e-b41c2558e92b",
        "protocolEndpointInBandID":
"naa.6f47acc2000000016a67746700000000",
        "protocolEndpointType": "SCSI",
        "virtualVolumeBindingID": 177,
        "virtualVolumeHostID": "564de1a4-9a99-da0f-8b7c-3a41dfd64bf1",
        "virtualVolumeID": "269d3378-1ca6-4175-a18f-6d4839e5c746",
        "virtualVolumeSecondaryID": "0xe200000000a6"
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListVirtualVolumeHost

È possibile utilizzare `ListVirtualVolumeHosts` metodo per ottenere un elenco di tutti gli host di volumi virtuali noti al cluster. Un host di volume virtuale è un host VMware ESX che ha avviato una sessione con il provider API VASA.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualVolumeHostID	Un elenco di ID host del volume virtuale per i quali recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti gli host di volumi virtuali.	Array UUID virtualVolumeHostID	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
host	Un elenco di oggetti che descrivono gli host dei volumi virtuali nel cluster.	host array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVirtualVolumeHosts",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "hosts": [
      {
        "bindings": [],
        "clusterID": "5ebdb4ad-9617-4647-adfd-c1013578483b",
        "hostAddress": "172.30.89.117",
        "initiatorNames": [
          "iqn.1998-01.com.vmware:zdc-dhcp-0-c-29-d6-4b-f1-1a0cd614",
          "iqn.1998-01.com.vmware:zdc-dhcp-0-c-29-d6-4b-f1-5bcf9254"
        ],
        "virtualVolumeHostID": "564de1a4-9a99-da0f-8b7c-3a41dfd64bf1",
        "visibleProtocolEndpointIDs": [
          "5dd53da0-b9b7-43f9-9b7e-b41c2558e92b"
        ]
      }
    ]
  }
}
```

Novità dalla versione

9.6

ListVirtualVolumes

È possibile utilizzare `ListVirtualVolumes` metodo per elencare i volumi virtuali attualmente presenti nel sistema. È possibile utilizzare questo metodo per elencare tutti i volumi virtuali o solo un sottoinsieme.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
dettagli	Il livello di dettaglio nella risposta. Valori possibili: • Vero: Includi ulteriori dettagli su ciascun volume nella risposta. • Falso: Includere nella risposta il livello standard di dettaglio relativo a ciascun volume.	booleano	Falso	No
limite	Il numero massimo di volumi virtuali da elencare.	intero	10000	No
ricorrente	Specifica se includere o meno informazioni sui figli di ogni Vol nella risposta. Valori possibili: • Vero: Includere nella risposta le informazioni relative ai figli di ciascun volume. • Falso: Non includere nella risposta le informazioni relative ai figli di ciascun volume.	booleano	Falso	No
StartVirtualVolumeID	L'ID del volume virtuale in cui iniziare l'elenco nella risposta.	UUIDType	Nessuno	No

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualVolumeID	Un elenco di ID dei volumi virtuali per i quali recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni solo su questi volumi virtuali.	Array UUUID virtualVolumeID	Nessuno	No

Valori restituiti

Questo metodo ha i seguenti valori restituiti:

Nome	Descrizione	Tipo
NextVirtualVolumeID	L'ID del volume virtuale successivo nell'elenco.	UUID
VirtualVolumes	Un elenco di oggetti che descrivono i volumi virtuali attualmente presenti nel sistema.	VirtualVolume array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVirtualVolumes",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "nextVirtualVolumeID": "00000000-0000-0000-0000-000000000000",
    "virtualVolumes": [
      {
        "bindings": [
          177
        ],
        "children": [],
        "metadata": {
          "SFProfileId": "f4e5bade-15a2-4805-bf8e-52318c4ce443",
          "SFgenerationId": "0",
          "VMW_ContainerId": "abaab415-bedc-44cd-98b8-f37495884db0",
          "VMW_VVolName": "asdf",
          "VMW_VVolType": "Config",
          "VMW_VmID": "502e0676-e510-ccdd-394c-667f6867fcdf",
          "VMW_VvolProfile": "f4e5bade-15a2-4805-bf8e-52318c4ce443:0"
        },
        "parentVirtualVolumeID": "00000000-0000-0000-0000-000000000000",
        "snapshotID": 0,
        "snapshotInfo": null,
        "status": "done",
        "storageContainer": {
          "accountID": 1,
          "initiatorSecret": "B5)D1y10K)8IDN58",
          "name": "test",
          "protocolEndpointType": "SCSI",
          "status": "active",
          "storageContainerID": "abaab415-bedc-44cd-98b8-f37495884db0",
          "targetSecret": "qgae@{o{~8\"2U)U^"
        },
        "virtualVolumeID": "269d3378-1ca6-4175-a18f-6d4839e5c746",
        "virtualVolumeType": "config",
        "volumeID": 166,
        "volumeInfo": null
      }
    ]
  }
}
```


Novità dalla versione

9.6

ListVirtualVolumeTasks

È possibile utilizzare `ListVirtualVolumeTasks` metodo per ottenere un elenco delle attività dei volumi virtuali nel sistema.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio
VirtualVolumeTaskID	Un elenco di ID attività del volume virtuale per cui recuperare le informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutte le attività dei volumi virtuali.	Array UUID	Nessuno	No

Valore restituito

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
attività	Un elenco di oggetti che descrivono le attività dei volumi virtuali nel cluster.	attività array

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ListVirtualVolumeTasks",
    "params": {
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "tasks": [
      {
        "cancelled": false,
        "cloneVirtualVolumeID": "fafeb3a0-7dd9-4c9f-8a07-80e0bbf6f4d0",
        "operation": "clone",
        "parentMetadata": {
          "SFProfileId": "f4e5bade-15a2-4805-bf8e-52318c4ce443",
          "SFgenerationId": "0",
          "VMW_ContainerId": "abaab415-bedc-44cd-98b8-f37495884db0",
          "VMW_GosType": "windows7Server64Guest",
          "VMW_VVolName": "asdf.vmdk",
          "VMW_VVolNamespace": "/vmfs/volumes/vvol:abaab415bedc44cd-
98b8f37495884db0/rfc4122.269d3378-1ca6-4175-a18f-6d4839e5c746",
          "VMW_VVolType": "Data",
          "VMW_VmID": "502e0676-e510-ccdd-394c-667f6867fcdf",
          "VMW_VvolAllocationType": "4",
          "VMW_VvolProfile": "f4e5bade-15a2-4805-bf8e-52318c4ce443:0"
        },
        "parentTotalSize": 42949672960,
        "parentUsedSize": 0,
        "status": "success",
        "virtualVolumeHostID": "564de1a4-9a99-da0f-8b7c-3a41dfd64bf1",
        "virtualVolumeTaskID": "a1b72df7-66a6-489a-86e4-538d0dbe05bf",
        "virtualvolumeID": "fafeb3a0-7dd9-4c9f-8a07-80e0bbf6f4d0"
      }
    ]
  }
}
```


Novità dalla versione

9.6

ModifyStorageContainer

È possibile utilizzare `ModifyStorageContainer` metodo per apportare modifiche a un container di storage di volumi virtuali esistente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Obbligatorio

StorageContainerID	ID univoco del contenitore di storage del volume virtuale da modificare.	UUID	Nessuno	Sì
InitatorSecret	Il nuovo segreto per l'autenticazione CHAP per l'iniziatore.	stringa	Nessuno	No
TargetSecret	Il nuovo segreto per l'autenticazione CHAP per la destinazione.	stringa	Nessuno	No

Valori restituiti

Questo metodo ha il seguente valore restituito:

Nome	Descrizione	Tipo
StorageContainer	Informazioni sul container di storage appena creato.	StorageContainer

Esempio di richiesta

Le richieste per questo metodo sono simili all'esempio seguente:

```
{
  "method": "ModifyStorageContainer",
    "params": {
      "storageContainerID": "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1",
      "targetSecret": "O,IM;tOQdn9$JJ*8"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile all'esempio seguente:

```
{
  "id": 1,
  "result": {
    "storageContainer": {
      "accountID": 8,
      "initiatorSecret": "T$|5TO>2IY5sk4@k",
      "name": "doctest1",
      "protocolEndpointType": "SCSI",
      "status": "active",
      "storageContainerID": "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1",
      "targetSecret": "O,IM;tOQdn9$JJ*8"
    }
  }
}
```


Novità dalla versione

9.6

Controllo degli accessi

I metodi API Element disponibili variano in base al tipo di accesso impostato.

account

Per il tipo di accesso agli account sono disponibili i seguenti metodi:

AddAccount
GetAccountByID
ModifyAccount
GetAccountByName
ListAccounts
GetAccountEfficiency
RemoveAccount

amministratore

Tutti i metodi sono disponibili per il tipo di accesso amministratore.

ClusterAdmin

Per il tipo di accesso di amministratore del cluster sono disponibili i seguenti metodi:

AddClusterAdmin
ListBackupTargets
AddInitiatorsToVolumeAccessGroup
ListBulkVolumeJobs
AddLdapClusterAdmin
ListClusterAdmins
AddVirtualNetwork
ListClusterPairs
AddVirtualNetwork
ListNodeFibreChannelPortInfo
AddVolumetoVolumeAccessGroup
ListBackupTargets
CloneMultipleVolumes
ListDrivehardware
CompleteClusterPairing
ListFiberChannelSessions
CompleteVolumePairing
ListFiberChannelPortInfo
CreateBackupTarget
ListGroupSnapshot
CreateSchedule

ListActivePairedVolumes
CreateSnapshot
ModifyBackupTarget
CreateSupportBundle
ModifyClusterAdmin
CreateClusterSupportBundle
ModifyGroupSnapshot
CreateGroupSnapshot
ModifyClusterFullThreshold
CreateVolumeAccessGroup
ModifyVolumeAccessGroup
DeleteAllSupportBundles
ModifyVolumeAccessGroupLunAssignments
DeleteSnapshot
ModifyVolumePair
DeleteGroupSnapshot
ModifyVirtualNetwork
DeleteVolumeAccessGroup
RemoveClusterAdmin
DisableEncryptionAtRest
RemoveVolumePair
DisableLdapAuthentication

RemoveVirtualNetwork
DisableSnmp
RemoveVolumesFromVolumeAccessGroup
EnableEncryptionAtRest
RemoveInitialisFromVolumeAccessGroup
EnableLdapAuthentication
RollbackToSnapshot
EnableSnmp
RollbackToGroupSnapshot
GetBackupTarget
SetLoginSessionInfo
GetClusterFullThreshold
SetNtpInfo
GetClusterMasterNodeID
SetSnmpACL
GetHardwareConfig
SetSnmpInfo
GetLdapConfiguration
SetSnmpTrapInfo
GetLoginSessionInfo
SetRemoteLoggingHost
GetNtpInfo

Spegnere
GetNvramInfo
StartBulkVolumeRead
GetRawStats
StartBulkVolumeWrite
GetSnmpACL
StartClusterPairing
GetVolumeAccessGroupEfficiency
StartVolumePairing
GetVolumeAccessLunAssignments
TestLdapAuthentication
GetVirtualNetwork

dischi

Per il tipo di accesso ai dischi sono disponibili i seguenti metodi:

ListDrive
RemoveDrives
AddDrive
SecureEraseDrive

nodi

Per il tipo di accesso ai nodi sono disponibili i seguenti metodi:

AddNode
ListPendingNode

ListActiveNode
RemoveNode

leggi

Per il tipo di accesso in lettura sono disponibili i seguenti metodi:

GetAccountByID
ListCloneJobs
GetAccountByName
ListDeletedVolumes
GetAsyncResult
ListDrivehardware
GetClusterCapacity
ListDrive
GetDefaultQoS
ListEvents
GetDriveStats
ListISCSISessions
GetSoftwareUpgrade
ListPendingNode
GetVolumeStats
ListSyncJobs
ListAccounts
ListVolumeAccessGroups

ListActiveNode
ListVolumeStatsByAccount
ListActiveNode
ListVolumeStatsByVolume
ListActiveVolumes
ListVolumeStatsByVolumeAccessGroup
ListAllNode
ListVolumesForAccount
ListBackupTargets

creazione di report

Per il tipo di accesso al reporting sono disponibili i seguenti metodi:

ClearClusterFaults
GetVolumeEfficiency
GetAccountEfficiency
GetVolumeStats
GetClusterCapacity
ListCloneJobs
GetClusterHardwareInfo
ListClusterFaults
GetClusterInfo
ListClusterPairs
GetClusterMasterNodeID

ListDrivehardware
GetClusterStats
ListEvents
GetDriveHardwareInfo
ListISCSISessions
GetDriveStats
Elenchi
GetNetworkConfig
ListServices
GetNodeHardwareInfo
ListSyncJobs
GetNodeStats
ListVirtualNetworks
GetSnmpInfo
ListVolumeStatsByAccount
GetSnmpTrapInfo
ListVolumeStatsByVolume
GetVolumeAccessGroupEfficiency
ListVolumeStatsByVolumeAccessGroup

repository

Il metodo ListAllNodes è disponibile per il tipo di accesso ai repository.

volumi

Per il tipo di accesso ai volumi sono disponibili i seguenti metodi:

CreateVolume
DeleteVolume
ModifyBackupTarget
CloneVolume
DeleteVolumePairing
ModifyVolumes
CloneMultipleVolumes
GetBackupTarget
ModifyVolumePair
CreateBackupTarget
GetDefaultQoS
PurgeDeletedVolume
CreateSnapshot
ListActiveVolumes
RemoveBackupTarget
CreateGroupSnapshot
ListBackupTarget
RemoveVolumePair
CompleteVolumePairing
ListGroupSnapshot
RestoreDeletedVolume
CloneMultipleVolumes

ListVolumesForAccount
RollbackToGroupSnapshot
DeleteGroupSnapshot
ListDeletedVolumes
RollbackToSnapshot
DeleteSnapshot
ListGroupSnapshot
StartBulkVolumeRead
StartBulkVolumeWrite
StartVolumePairing
UpdateBulkVolumeStatus

di scrittura

Per il tipo di accesso in scrittura sono disponibili i seguenti metodi:

AddDrive
RemoveNode
AddNode
RemoveAccount
AddAccount
RemoveVolumesFromVolumeAccessGroup
AddVolumeToVolumeAccessGroup
RemoveInitialisFromVolumeAccessGroup
AddInitiatorsToVolumeAccessGroup

DeleteVolumeAccessGroup
CreateVolumeAccessGroup
DeleteVolume
ModifyVolumeAccessGroup
RestoreDeletedVolume
ModifyAccount
PurgeDeletedVolume
CreateVolume
ModifyVolume
CloneVolume
GetAsyncResult
RemoveDrives

Esempi di risposte

Di seguito sono riportati alcuni esempi completi di risposte.

- GetConfig
- GetClusterHardwareInfo
- GetLldpInfo
- GetNetworkConfig
- GetNodeHardwareInfo (output per iSCSI)
- GetNodeHardwareInfo (output per nodi Fibre Channel)
- GetNvramInfo
- ListActiveNode
- ListActiveVolumes
- TestHardwareConfig

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Documentazione per le versioni precedenti dei prodotti SolidFire ed Element di NetApp"

GetConfig

Il `GetConfig` method restituisce una risposta simile all'esempio seguente. A causa della lunghezza, la risposta contiene informazioni solo per un nodo del cluster.


```
{
    "id": 1,
    "result": {
        "config": {
            "cluster": {
                "cipi": "Bond10G",
                "cluster": "AutoTest2-Fjqt",
                "encryptionCapable": true,
                "ensemble": [
                    "1:10.1.1.0",
                    "3:10.1.1.0",
                    "4:10.1.1.0"
                ],
                "mipi": "Bond1G",
                "name": "NLABP2605",
                "nodeID": 1,
                "pendingNodeID": 0,
                "role": "Storage",
                "sipi": "Bond10G",
                "state": "Active",
                "version": "11.0"
            },
            "network": {
            "Bond10G": {
                "#default": false,
                "address": "10.1.1.0",
                "auto": true,
                "bond-downdelay": "0",
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth0 eth1",
                "bond-updelay": "200",
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
                "family": "inet",
                "gateway": "10.1.1.0",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "00:00:00:00:00:00",
```

```
                "method": "static",
                "mtu": "9000",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "9000",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "eth0": {
                "auto": true,
                "bond-master": "Bond10G",
                "family": "inet",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:b9",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "c8:1f:66:ee:59:b9",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "lo": {
                "auto": true,
                "family": "inet",
```

```
                "linkSpeed": 0,
                "macAddress": "00:00:00:00:00:00",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "loopback",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "00:00:00:00:00:00",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            }
        }
        }
    }
}
```

GetClusterHardwareInfo

Il `GetClusterHardwareInfo` method restituisce una risposta simile all'esempio seguente.

```
{
 "id": null,
  "result": {
   "clusterHardwareInfo": {
     "drives": {
      "1": {
        "description": "ATA      Drive",
        "dev": "8:0",
        "devpath": "/dev/disk/by-id/scsi-SATA_VRFSD3400GNCVMT205121562-
part4",
        "driveSecurityAtMaximum": false,
        "driveSecurityFrozen": true,
        "driveSecurityLocked": false,
        "logicalname": "/dev/sda",
        "product": "VRFSD3400GNCVMTJS1",
        "securityFeatureEnabled": false,
        "securityFeatureSupported": true,
        "serial": "205121562",
        "size": 299988156416,
        "uuid": "febe39ae-4984-edc0-e3a7-3c47608cface",
```

```
        "version": "515ABBF0"
      },
      "2": {...
      },
      "3": {...
      },
      "4": {...
      },
      "5": {...
      },
      "6": {...
      },
         .
         .
         .
    "44": {...
      }
      },
"nodes":{
  "1":{                       Storage Node
    "core_DMI:0200": {
    "description": "Motherboard",
    "physid": "0",
    "vendor": "SolidFire"
  },
    "fiber:0_PCI:0000:04:00.0": {
      "businfo": "pci@0000:04:00.0",
      "clock": "33000000",
      "description": "Fibre Channel",
      "physid": "0",
      "product": "ISP8324-based 16Gb Fibre Channel to PCI Express
Adapter",
      "vendor": "QLogic Corp.",
      "version": "02",
      "width": "64"
  },
    "Repeat fiber information": {...}
    "Repeat fiber": {...},
    "Repeat fiber": {...},
   }
 },
   "fans": {
     "Fan1A RPM": {
     "baseUnit": "RPM",
     "threshold": 840,
     "value": 4800
```

```
  },
      "Fan1B RPM": {...},
          .
          .
          .
      "Fan7B RPM": {...
      },
      "fibreChannelPorts": [
        {
         "firmware": "7.04.00 (d0d5)",
         "hbaPort": 1,
         "model": "QLE2672",
         "nPortID": "0x110c36",
         "pciSlot": 3,
         "serial": "BFE1341E09329",
         "speed": "8 Gbit",
         "state": "Online",
         "switchWwn": "20:01:00:2a:6a:a0:25:01",
         "wwnn": "5f:47:ac:c8:82:23:e0:00",
         "wwpn": "5f:47:ac:c0:82:23:e0:02"
        },
        {
         "firmware": "7.04.00 (d0d5)", {...}
         "firmware": "7.04.00 (d0d5)", {...}
         "firmware": "7.04.00 (d0d5)", {...}
        }
      ],
      "hardwareConfig": {
        "BIOS_REVISION": {
         "Passed": true,
         "actual": "1.1",
         "comparator": ">=",
         "expected": "1.0"
        },
        "BIOS_VENDOR": {
         "Passed": true,
         "actual": "SolidFire",
         "comparator": "==",
         "expected": "SolidFire"
        },
        "BIOS_VERSION": {
         "Passed": true,
         "actual": "1.1.2",
         "comparator": ">=",
         "expected": "1.1.2"
        },
```

```
"BMC_FIRMWARE_REVISION": {
 "Passed": true,
 "actual": "1.6",
 "comparator": ">=",
 "expected": "1.6"
},
"BMC_IPMI_VERSION": {
 "Passed": true,
 "actual": "2.0",
 "comparator": ">=",
 "expected": "2.0"
},
"CHASSIS_TYPE": {
 "Passed": true,
 "actual": "R620",
 "comparator": "==",
 "expected": "R620"
},
"CPU_CORES_00": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_01": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_ENABLED_00": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_CORES_ENABLED_01": {
 "Passed": true,
 "actual": "6",
 "comparator": "==",
 "expected": "6"
},
"CPU_MODEL_00": {
 "Passed": true,
 "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
 "comparator": "==",
```

```
 "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
},
"CPU_MODEL_01": {
 "Passed": true,
 "actual": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
 "comparator": "==",
 "expected": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz"
},
"CPU_THREADS_00": {
 "Passed": true,
 "actual": "12",
 "comparator": "==",
 "expected": "12"
},
"CPU_THREADS_01": {
 "Passed": true,
 "actual": "12",
 "comparator": "==",
 "expected": "12"
},
"DRIVE_SIZE_BYTES_SDIMM0": {
 "Passed": true,
 "actual": "100030242816",
 "comparator": ">=",
 "expected": "100030242816"
},
"FIBRE_CHANNEL_FIRMWARE_REVISION": {
 "Passed": true,
 "actual": "FW:v7.04.00",
 "comparator": "==",
 "expected": "FW:v7.04.00"
},
"FIBRE_CHANNEL_MODEL": {
 "Passed": true,
 "actual": "QLE2672",
 "comparator": "==",
 "expected": "QLE2672"
},
"IDRAC_VERSION": {
 "Passed": true,
 "actual": "1.06.06",
 "comparator": ">=",
 "expected": "1.06.06"
},
"LIFECYCLE_VERSION": {
 "Passed": true,
```

```
        "actual": "1.0.0.5747",
        "comparator": ">=",
        "expected": "1.0.0.5747"
       },
       "MEMORY_GB": {
        "Passed": true,
        "actual": "32",
        "comparator": ">=",
        "expected": "32"
       },
       "MEMORY_MHZ_00": {
        "Passed": true,
        "actual": "1333",
        "comparator": ">=",
        "expected": "1333"
       },
       "MEMORY_MHZ_01": {
        "Passed": true,
        "actual": "1333",
        "comparator": ">=",
        "expected": "1333"
       },
       "MEMORY_MHZ_02": {
       "Passed": true,
       "actual": "1333",
       "comparator": ">=",
       "expected": "1333"
      },
      "MEMORY_MHZ_03": {
       "Passed": true,
       "actual": "1333",
       "comparator": ">=",
       "expected": "1333"
      },
      "NETWORK_DRIVER_ETH0": {
       "Passed": true,
       "actual": "bnx2x",
       "comparator": "=~",
       "expected": "^bnx2x$"
      },
      {
       "NETWORK_DRIVER_ETH1":, {...
      },
       "NETWORK_DRIVER_ETH2":, {...
      },
       "NETWORK_DRIVER_ETH3":, {...
```

```
      },
       "NETWORK_DRIVER_ETH4":, {...
      },
       "NETWORK_DRIVER_ETH5":, {...
      },
       "NODE_TYPE": {
       "Passed": true,
       "actual": "FC0025",
       "comparator": "==",
       "expected": "FC0025"
      },
      "NUM_CPU": {
       "Passed": true,
       "actual": "2",
       "comparator": "==",
       "expected": "2"
      },
      "NUM_DRIVES": {
       "Passed": true,
       "actual": "0",
       "comparator": "==",
       "expected": "0"
      },
      "NUM_DRIVES_INTERNAL": {
       "Passed": true,
       "actual": "1",
       "comparator": "==",
       "expected": "1"
      },
      "NUM_FIBRE_CHANNEL_PORTS": {
       "Passed": true,
       "actual": "4",
       "comparator": "==",
       "expected": "4"
      },
      "NVRAM_VENDOR": {
       "Passed": true,
       "actual": "",
       "comparator": "==",
       "expected": ""
      },
      "ROOT_DRIVE_REMOVABLE": {
       "Passed": true,
       "actual": "false",
       "comparator": "==",
       "expected": "false"
```

```
      }
      },
      "memory": {
        "firmware_": {
         "capacity": "8323072",
         "date": "03/08/2012",
         "description": "BIOS",
         "physid": "0",
         "size": "65536",
         "vendor": "SolidFire",
         "version": "1.1.2"
      },
      "memory_DMI:1000": {
        "description": "System Memory",
        "physid": "1000",
        "size": "34359738368",
        "slot": "System board or motherboard"
      }
      },
      "network": {
       "network:0_PCI:0000:01:00.0": {
        "businfo": "pci@0000:01:00.0",
        "capacity": "1000000000",
        "clock": "33000000",
        "description": "Ethernet interface",
        "logicalname": "eth0",
        "physid": "0",
        "product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
        "serial": "c8:1f:66:e0:97:2a",
        "vendor": "Broadcom Corporation",
        "version": "10",
        "width": "64"
      },
       "network:0_PCI:0000:41:00.0": {...
      },
       "network:1_PCI:0000:01:00.1": {...
      },
       "network:1_PCI:0000:41:00.1": {...
      },
       "network:2_PCI:0000:01:00.2": {...
      },
       "network:3_PCI:0000:01:00.3": {...
      }
      },
      "networkInterfaces": {
       "Bond10G": {
```

```
        "isConfigured": true,
        "isUp": true
      },
      "Bond1G": {
       "isConfigured": true,
       "isUp": true
      },
      "eth0": {
       "isConfigured": true,
       "isUp": true
      },
      "eth1": {...
      },
      "eth2": {...
      },
      "eth3": {...
      },
      "eth4": {...
      },
      "eth5": {...
      }
     },
     "nvram": {
       "errors": {
        "numOfErrorLogEntries": "0"
       },
       "extended": {
        "dialogVersion": "4",
        "event": [
        {
         "name": "flushToFlash",
         "time": "2015-08-06 01:19:39",
         "value": "0"
        },
        {
         "name": "flushToFlash",
         "time": "2015-08-06 01:26:44",
         "value": "0"
        },
        {... next "flushToFlash"
        },
        {... next "flushToFlash"
        },
        {... next "flushToFlash"
        },
        {... next "flushToFlash"
```

```
        },
        {... next "flushToFlash"
        },
        {... next "flushToFlash"
        },
        {... next "flushToFlash"
        }
      ],
      "eventOccurrences": [
        {
          "count": "740",
          "name": "flushToFlash"
        },
        {
          "count": "1",
          "name": "excessiveCurrent"
        }
      ],
      "initialCapacitance": "6.630 F",
      "initialEsr": "0.101 Ohm",
      "measurement": [
       {
         "level_0": " 0",
         "level_1": " 3969",
         "level_2": " 4631",
         "level_3": " 12875097",
         "level_4": " 1789948",
         "level_5": " 0",
         "level_6": " 0",
         "level_7": " 0",
         "level_8": " 0",
         "level_9": " 0",
         "name": "enterpriseFlashControllerTemperature",
         "recent": "66 C"
      },
      {
         "level_0": " 0",
         "level_1": " 58",
         "level_2": " 1479058",
         "level_3": " 12885356",
         "level_4": " 308293",
         "level_5": " 851",
         "level_6": " 29",
         "level_7": " 0",
         "level_8": " 0",
         "level_9": " 0",
```

```
        "name": "capacitor1And2Temperature",
        "recent": "30.69 C"
      },
      {...next temp measurement
      },
      {...next temp measurement
      },
      {...next temp measurement
      },
      }
       "name": "voltageOfCapacitor1",
       "recent": "2.198 V"
      },
      {
       "name": "voltageOfCapacitor2",
       "recent": "2.181 V"
      },
      {
       "name": "voltageOfCapacitor3",
       "recent": "2.189 V"
      },
      {
       "name": "voltageOfCapacitor4",
       "recent": "2.195 V"
      },
      {
       "level_0": " 4442034",
       "level_1": " 6800018",
       "level_2": " 2846869",
       "level_3": " 119140",
       "level_4": " 29506",
       "level_5": " 428935",
       "level_6": " 7143",
       "level_7": " 0",
       "level_8": " 0",
       "level_9": " 0",
       "name": "capacitorPackVoltage",
       "recent": "8.763 V"
      },
      {
       "level_0": " 0",
       "level_1": " 0",
       "level_2": " 0",
       "level_3": " 0",
       "level_4": " 189",
       "level_5": " 17",
```

```
      "level_6": " 36",
      "level_7": " 0",
      "level_8": " 2",
      "level_9": " 490",
      "name": "capacitorPackVoltageAtEndOfFlushToFlash",
      "recent": "4.636 V"
    },
    {
      "name": "currentDerivedFromV3V4",
      "recent": "-0.004 A"
    },
    {
      "level_0": " 230",
      "level_1": " 482",
      "level_2": " 22",
      "level_3": " 0",
      "level_4": " 0",
      "level_5": " 0",
      "level_6": " 0",
      "level_7": " 0",
      "level_8": " 0",
      "level_9": " 0",
      "name": "derivedEnergy",
      "recent": "172 Joules"
    },
    {...next voltage measurement
    },
    {...next voltage measurement
    },
    {...next voltage measurement
    },
  ],
  "smartCounters": [
    {
      "name": "numberOf512ByteBlocksReadFromDdr",
      "value": "10530088847"
    },
    {
      "name": "numberOf512ByteBlocksWrittenToDdr",
      "value": "1752499453837"
    },
    {
      "name": "numberOfHostReadCommands",
      "value": "235317769"
    },
    {...next smartCounters measurement
```

```
      },
      {...next smartCounters measurement
      },
      {...next smartCounters measurement
      },
    ],
    "snapshotTime": "2015-08-20 16:30:01"
  },
  "firmware": {
    "activeSlotNumber": "2",
    "slot1Version": "1e5817bc",
    "slot2Version": "5fb7565c",
    "slot3Version": "1e5817bc",
    "slot4Version": "1e5817bc"
  },
  "identify": {
    "firmwareVersion": "5fb7565c on slot 2",
    "hardwareRevision": "B04",
    "modelNumber": "RMS-200",
    "serialNumber": "0000862"
  },
  "smart": {
    "availableSpace": "0%",
    "availableSpaceThreshold": "0%",
    "controllerBusyTimeMinutes": "6793",
    "criticalErrorVector": "0x0",
    "mediaErrors": "0",
    "numberOf512ByteBlocksRead": "10530088847",
    "numberOf512ByteBlocksWritten": "1752499439063",
    "numberOfErrorInfoLogs": "1",
    "numberOfHostReadCommands": "235317769",
    "numberOfHostWriteCommands": "126030374065",
    "numberOfPowerCycles": "709",
    "powerOnHours": "11223",
    "temperature": "324 Kelvin",
    "unsafeShutdowns": "357"
    }
    },
    "origin": null,
    "platform": {
      "chassisType": "R620",
      "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
      "nodeMemoryGB": 32,
      "nodeType": "FC0025"
    },
    "powerSupplies": {
```

```
      "PS1 status": {
       "powerSupplyFailureDetected": false,
       "powerSupplyHasAC": true,
       "powerSupplyPredictiveFailureDetected": false,
       "powerSupplyPresent": true,
       "powerSupplyPresentLastCheck": true
      },
      "PS2 status": {
       "powerSupplyFailureDetected": false,
       "powerSupplyHasAC": true,
       "powerSupplyPredictiveFailureDetected": false,
       "powerSupplyPresent": true,
       "powerSupplyPresentLastCheck": true
      }
     },
     "storage": {
      "storage_PCI:0000:00:1f.2": {
       "businfo": "pci@0000:00:1f.2",
       "clock": "66000000",
       "description": "SATA controller",
       "physid": "1f.2",
       "product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
       "vendor": "Intel Corporation",
       "version": "05",
       "width": "32"
      }
     },
     "system": {
      "ubuntu_DMI:0100": {
       "description": "Rack Mount Chassis",
       "product": "SFx010 ()",
       "serial": "HTW1DZ1",
       "vendor": "SolidFire",
       "width": "64"
      }
     },
     "temperatures": {
      "Exhaust Temp": {
       "baseUnit": "C",
       "threshold": 70,
       "value": 41
      },
      "Inlet Temp": {
       "baseUnit": "C",
       "threshold": 42,
       "value": 18
```

```
      }
      },
      "uuid": "4C4C4544-0054-5710-8031-C8C04F445A31"
    },
  "2": {...},                    Storage Node "2"
  "3": {...},                    Storage Node "3"
  "4": {...},                    Storage Node "4"
  "5": {                      Fibre Channel Node
       }
      }
    }
  }
```

GetLldpInfo

Il `GetLldpInfo` method restituisce una risposta simile all'esempio seguente.

```
{
  "id": null,
  "result": {
    "lldpInfo": {
        "lldpChassis": {
        "local-chassis": [
        {
          "chassis": [
            {
              "capability": [
                {
                  "enabled": false,
                  "type": "Bridge"
                },
                {
                  "enabled": false,
                  "type": "Router"
                },
                {
                  "enabled": false,
                  "type": "Wlan"
                },
                {
                  "enabled": true,
                  "type": "Station"
                }
              ],
              "descr": [
```

```
            {
              "value": "Element OS 11.0"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "08:00:27:3c:0a:f4"
            }
          ],
          "mgmt-ip": [
            {
              "value": "10.0.2.15"
            },
            {
              "value": "fe80::a00:27ff:fe3c:af4"
            }
          ],
          "name": [
            {
              "value": "SF-93FF"
            }
          ]
        }
      ],
      "lldp-med": [
        {
          "capability": [
            {
              "available": true,
              "type": "Capabilities"
            },
            {
              "available": true,
              "type": "Policy"
            },
            {
              "available": true,
              "type": "Location"
            },
            {
              "available": true,
              "type": "MDI/PSE"
            },
            {
              "available": true,
```

```
        "type": "MDI/PD"
      },
      {
        "available": true,
        "type": "Inventory"
      }
    ],
    "device-type": [
      {
        "value": "Generic Endpoint (Class I)"
      }
    ],
    "inventory": [
      {
        "firmware": [
          {
            "value": "VirtualBox"
          }
        ],
        "hardware": [
          {
            "value": "1.2"
          }
        ],
        "manufacturer": [
          {
            "value": "innotek GmbH"
          }
        ],
        "model": [
          {
            "value": "VirtualBox"
          }
        ],
        "serial": [
          {
            "value": "0"
          }
        ],
        "software": [
          {
            "value": "4.14.27-solidfire2"
          }
        ]
      }
    ]
```

```
            }
          ]
        }
      ]
    },
    "lldpInterfaces": {
      "lldp": [
        {
          "interface": [
            {
              "age": "0 day, 00:01:04",
              "chassis": [
                {
                  "capability": [
                    {
                      "enabled": false,
                      "type": "Bridge"
                    },
                    {
                      "enabled": false,
                      "type": "Router"
                    },
                    {
                      "enabled": false,
                      "type": "Wlan"
                    },
                    {
                      "enabled": true,
                      "type": "Station"
                    }
                  ],
                  "descr": [
                    {
                      "value": "Element OS 11.0"
                    }
                  ],
                  "id": [
                    {
                      "type": "mac",
                      "value": "08:00:27:3c:0a:f4"
                    }
                  ],
                  "mgmt-ip": [
                    {
                      "value": "10.0.2.15"
                    },
```

```
                {
                  "value": "fe80::a00:27ff:fe3c:af4"
                }
              ],
              "name": [
                {
                  "value": "SF-93FF"
                }
              ]
            }
          ],
          "lldp-med": [
            {
              "capability": [
                {
                  "available": true,
                  "type": "Capabilities"
                },
                {
                  "available": true,
                  "type": "Policy"
                },
                {
                  "available": true,
                  "type": "Location"
                },
                {
                  "available": true,
                  "type": "MDI/PSE"
                },
                {
                  "available": true,
                  "type": "MDI/PD"
                },
                {
                  "available": true,
                  "type": "Inventory"
                }
              ],
              "device-type": [
                {
                  "value": "Generic Endpoint (Class I)"
                }
              ],
              "inventory": [
                {
```

```
                "firmware": [
                  {
                    "value": "VirtualBox"
                  }
                ],
                "hardware": [
                  {
                    "value": "1.2"
                  }
                ],
                "manufacturer": [
                  {
                    "value": "innotek GmbH"
                  }
                ],
                "model": [
                  {
                    "value": "VirtualBox"
                  }
                ],
                "serial": [
                  {
                    "value": "0"
                  }
                ],
                "software": [
                  {
                    "value": "4.14.27-solidfire2"
                  }
                ]
              }
            ]
          }
        ],
        "name": "eth0",
        "port": [
          {
            "aggregation": [
              {
                "value": "7"
              }
            ],
            "auto-negotiation": [
              {
                "advertised": [
                  {
```

```
                    "fd": true,
                    "hd": true,
                    "type": "10Base-T"
                  },
                  {
                    "fd": true,
                    "hd": true,
                    "type": "100Base-TX"
                  },
                  {
                    "fd": true,
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "full duplex mode"
                  }
                ],
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ]
          }
        ],
        "ttl": [
          {
            "ttl": "120"
          }
        ],
        "via": "unknown"
      },
      {
        "age": "17722 days, 17:14:28",
```

```
            "chassis": [
              {
                "capability": [
                  {
                    "enabled": false,
                    "type": "Bridge"
                  },
                  {
                    "enabled": false,
                    "type": "Router"
                  },
                  {
                    "enabled": false,
                    "type": "Wlan"
                  },
                  {
                    "enabled": true,
                    "type": "Station"
                  }
                ],
                "descr": [
                  {
                    "value": "Element OS 11.0"
                  }
                ],
                "id": [
                  {
                    "type": "mac",
                    "value": "08:00:27:3c:0a:f4"
                  }
                ],
                "mgmt-ip": [
                  {
                    "value": "10.0.2.15"
                  },
                  {
                    "value": "fe80::a00:27ff:fe3c:af4"
                  }
                ],
                "name": [
                  {
                    "value": "SF-93FF"
                  }
                ]
              }
            ],
```

```
            "lldp-med": [
              {
                "capability": [
                  {
                    "available": true,
                    "type": "Capabilities"
                  },
                  {
                    "available": true,
                    "type": "Policy"
                  },
                  {
                    "available": true,
                    "type": "Location"
                  },
                  {
                    "available": true,
                    "type": "MDI/PSE"
                  },
                  {
                    "available": true,
                    "type": "MDI/PD"
                  },
                  {
                    "available": true,
                    "type": "Inventory"
                  }
                ],
                "device-type": [
                  {
                    "value": "Generic Endpoint (Class I)"
                  }
                ],
                "inventory": [
                  {
                    "firmware": [
                      {
                        "value": "VirtualBox"
                      }
                    ],
                    "hardware": [
                      {
                        "value": "1.2"
                      }
                    ],
                    "manufacturer": [
```

```
                    {
                      "value": "innotek GmbH"
                    }
                  ],
                  "model": [
                    {
                      "value": "VirtualBox"
                    }
                  ],
                  "serial": [
                    {
                      "value": "0"
                    }
                  ],
                  "software": [
                    {
                      "value": "4.14.27-solidfire2"
                    }
                  ]
                }
              ]
            }
          ],
          "name": "eth1",
          "port": [
            {
              "aggregation": [
                {
                  "value": "7"
                }
              ],
              "auto-negotiation": [
                {
                  "advertised": [
                    {
                      "fd": true,
                      "hd": true,
                      "type": "10Base-T"
                    },
                    {
                      "fd": true,
                      "hd": true,
                      "type": "100Base-TX"
                    },
                    {
                      "fd": true,
```

```
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "unknown"
                  }
                ],
                "enabled": true,
                "supported": true
              }
            ],
            "descr": [
              {
                "value": "eth1"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:36:79:78"
              }
            ]
          }
        ],
        "ttl": [
          {
            "ttl": "120"
          }
        ],
        "via": "unknown"
      },
      {
        "age": "0 day, 00:01:01",
        "chassis": [
          {
            "capability": [
              {
                "enabled": false,
                "type": "Bridge"
              },
              {
                "enabled": false,
                "type": "Router"
              },
```

```
            {
              "enabled": false,
              "type": "Wlan"
            },
            {
              "enabled": true,
              "type": "Station"
            }
          ],
          "descr": [
            {
              "value": "Element OS 11.0"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "08:00:27:3c:0a:f4"
            }
          ],
          "mgmt-ip": [
            {
              "value": "10.0.2.15"
            },
            {
              "value": "fe80::a00:27ff:fe3c:af4"
            }
          ],
          "name": [
            {
              "value": "SF-93FF"
            }
          ]
        }
      ],
      "lldp-med": [
        {
          "capability": [
            {
              "available": true,
              "type": "Capabilities"
            },
            {
              "available": true,
              "type": "Policy"
            },
```

```
      {
        "available": true,
        "type": "Location"
      },
      {
        "available": true,
        "type": "MDI/PSE"
      },
      {
        "available": true,
        "type": "MDI/PD"
      },
      {
        "available": true,
        "type": "Inventory"
      }
    ],
    "device-type": [
      {
        "value": "Generic Endpoint (Class I)"
      }
    ],
    "inventory": [
      {
        "firmware": [
          {
            "value": "VirtualBox"
          }
        ],
        "hardware": [
          {
            "value": "1.2"
          }
        ],
        "manufacturer": [
          {
            "value": "innotek GmbH"
          }
        ],
        "model": [
          {
            "value": "VirtualBox"
          }
        ],
        "serial": [
          {
```

```
                    "value": "0"
                  }
                ],
                "software": [
                  {
                    "value": "4.14.27-solidfire2"
                  }
                ]
              }
            ]
          }
        ],
        "name": "eth2",
        "port": [
          {
            "aggregation": [
              {
                "value": "6"
              }
            ],
            "auto-negotiation": [
              {
                "advertised": [
                  {
                    "fd": true,
                    "hd": true,
                    "type": "10Base-T"
                  },
                  {
                    "fd": true,
                    "hd": true,
                    "type": "100Base-TX"
                  },
                  {
                    "fd": true,
                    "hd": false,
                    "type": "1000Base-T"
                  }
                ],
                "current": [
                  {
                    "value": "full duplex mode"
                  }
                ],
                "enabled": true,
                "supported": true
```

```
            }
          ],
          "descr": [
            {
              "value": "eth2"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "08:00:27:fc:f0:a9"
            }
          ]
        }
      ],
      "ttl": [
        {
          "ttl": "120"
        }
      ],
      "via": "LLDP"
    },
    {
      "age": "0 day, 00:01:01",
      "chassis": [
        {
          "capability": [
            {
              "enabled": false,
              "type": "Bridge"
            },
            {
              "enabled": false,
              "type": "Router"
            },
            {
              "enabled": false,
              "type": "Wlan"
            },
            {
              "enabled": true,
              "type": "Station"
            }
          ],
          "descr": [
            {
```

```
                "value": "Element OS 11.0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ],
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
              },
              {
                "value": "fe80::a00:27ff:fe3c:af4"
              }
            ],
            "name": [
              {
                "value": "SF-93FF"
              }
            ]
          }
        ],
        "lldp-med": [
          {
            "capability": [
              {
                "available": true,
                "type": "Capabilities"
              },
              {
                "available": true,
                "type": "Policy"
              },
              {
                "available": true,
                "type": "Location"
              },
              {
                "available": true,
                "type": "MDI/PSE"
              },
              {
                "available": true,
                "type": "MDI/PD"
```

```
      },
      {
        "available": true,
        "type": "Inventory"
      }
    ],
    "device-type": [
      {
        "value": "Generic Endpoint (Class I)"
      }
    ],
    "inventory": [
      {
        "firmware": [
          {
            "value": "VirtualBox"
          }
        ],
        "hardware": [
          {
            "value": "1.2"
          }
        ],
        "manufacturer": [
          {
            "value": "innotek GmbH"
          }
        ],
        "model": [
          {
            "value": "VirtualBox"
          }
        ],
        "serial": [
          {
            "value": "0"
          }
        ],
        "software": [
          {
            "value": "4.14.27-solidfire2"
          }
        ]
      }
    ]
  }
```

```
            ],
            "name": "eth3",
            "port": [
              {
                "aggregation": [
                  {
                    "value": "6"
                  }
                ],
                "auto-negotiation": [
                  {
                    "advertised": [
                      {
                        "fd": true,
                        "hd": true,
                        "type": "10Base-T"
                      },
                      {
                        "fd": true,
                        "hd": true,
                        "type": "100Base-TX"
                      },
                      {
                        "fd": true,
                        "hd": false,
                        "type": "1000Base-T"
                      }
                    ],
                    "current": [
                      {
                        "value": "full duplex mode"
                      }
                    ],
                    "enabled": true,
                    "supported": true
                  }
                ],
                "descr": [
                  {
                    "value": "eth3"
                  }
                ],
                "id": [
                  {
                    "type": "mac",
                    "value": "08:00:27:2c:e4:f8"
```

```
                    }
                  ]
                }
              ],
              "ttl": [
                {
                  "ttl": "120"
                }
              ],
              "via": "LLDP"
            }
          ]
        }
      ]
    },
    "lldpNeighbors": {
      "lldp": [
        {
          "interface": [
            {
              "age": "0 day, 00:04:34",
              "chassis": [
                {
                  "capability": [
                    {
                      "enabled": true,
                      "type": "Bridge"
                    },
                    {
                      "enabled": true,
                      "type": "Router"
                    },
                    {
                      "enabled": true,
                      "type": "Wlan"
                    },
                    {
                      "enabled": false,
                      "type": "Station"
                    }
                  ],
                  "descr": [
                    {
                      "value": "x86_64"
                    }
                  ],
```

```
            "id": [
              {
                "type": "mac",
                "value": "50:7b:9d:2b:36:84"
              }
            ],
            "mgmt-ip": [
              {
                "value": "192.168.100.1"
              },
              {
                "value": "fe80::a58e:843:952e:d8eb"
              }
            ],
            "name": [
              {
                "value": "ConventionalWisdom.wlan.netapp.com"
              }
            ]
          }
        ],
        "name": "eth2",
        "port": [
          {
            "auto-negotiation": [
              {
                "current": [
                  {
                    "value": "full duplex mode"
                  }
                ],
                "enabled": false,
                "supported": false
              }
            ],
            "descr": [
              {
                "value": "vboxnet1"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "0a:00:27:00:00:01"
              }
            ],
```

```
            "ttl": [
              {
                "value": "120"
              }
            ]
          }
        ],
        "rid": "2",
        "via": "LLDP"
      },
      {
        "age": "0 day, 00:01:01",
        "chassis": [
          {
            "capability": [
              {
                "enabled": false,
                "type": "Bridge"
              },
              {
                "enabled": false,
                "type": "Router"
              },
              {
                "enabled": false,
                "type": "Wlan"
              },
              {
                "enabled": true,
                "type": "Station"
              }
            ],
            "descr": [
              {
                "value": "Element OS 11.0"
              }
            ],
            "id": [
              {
                "type": "mac",
                "value": "08:00:27:3c:0a:f4"
              }
            ],
            "mgmt-ip": [
              {
                "value": "10.0.2.15"
```

```
            },
            {
              "value": "fe80::a00:27ff:fe3c:af4"
            }
          ],
          "name": [
            {
              "value": "SF-93FF"
            }
          ]
        }
      ],
      "lldp-med": [
        {
          "capability": [
            {
              "available": true,
              "type": "Capabilities"
            },
            {
              "available": true,
              "type": "Policy"
            },
            {
              "available": true,
              "type": "Location"
            },
            {
              "available": true,
              "type": "MDI/PSE"
            },
            {
              "available": true,
              "type": "MDI/PD"
            },
            {
              "available": true,
              "type": "Inventory"
            }
          ],
          "device-type": [
            {
              "value": "Generic Endpoint (Class I)"
            }
          ],
          "inventory": [
```

```
                {
                  "firmware": [
                    {
                      "value": "VirtualBox"
                    }
                  ],
                  "hardware": [
                    {
                      "value": "1.2"
                    }
                  ],
                  "manufacturer": [
                    {
                      "value": "innotek GmbH"
                    }
                  ],
                  "model": [
                    {
                      "value": "VirtualBox"
                    }
                  ],
                  "serial": [
                    {
                      "value": "0"
                    }
                  ],
                  "software": [
                    {
                      "value": "4.14.27-solidfire2"
                    }
                  ]
                }
              ]
            }
          ],
          "name": "eth2",
          "port": [
            {
              "aggregation": [
                {
                  "value": "6"
                }
              ],
              "auto-negotiation": [
                {
                  "advertised": [
```

```
                    {
                      "fd": true,
                      "hd": true,
                      "type": "10Base-T"
                    },
                    {
                      "fd": true,
                      "hd": true,
                      "type": "100Base-TX"
                    },
                    {
                      "fd": true,
                      "hd": false,
                      "type": "1000Base-T"
                    }
                  ],
                  "current": [
                    {
                      "value": "full duplex mode"
                    }
                  ],
                  "enabled": true,
                  "supported": true
                }
              ],
              "descr": [
                {
                  "value": "eth3"
                }
              ],
              "id": [
                {
                  "type": "mac",
                  "value": "08:00:27:2c:e4:f8"
                }
              ],
              "ttl": [
                {
                  "value": "120"
                }
              ]
            }
          ],
          "rid": "1",
          "via": "LLDP"
        },
```

```
            {
              "age": "0 day, 00:04:34",
              "chassis": [
                {
                  "capability": [
                    {
                      "enabled": true,
                      "type": "Bridge"
                    },
                    {
                      "enabled": true,
                      "type": "Router"
                    },
                    {
                      "enabled": true,
                      "type": "Wlan"
                    },
                    {
                      "enabled": false,
                      "type": "Station"
                    }
                  ],
                  "descr": [
                    {
                      "value": "x86_64"
                    }
                  ],
                  "id": [
                    {
                      "type": "mac",
                      "value": "50:7b:9d:2b:36:84"
                    }
                  ],
                  "mgmt-ip": [
                    {
                      "value": "192.168.100.1"
                    },
                    {
                      "value": "fe80::a58e:843:952e:d8eb"
                    }
                  ],
                  "name": [
                    {
                      "value": ""
                    }
                  ]
```

```
      }
    ],
    "name": "eth3",
    "port": [
      {
        "auto-negotiation": [
          {
            "current": [
              {
                "value": "full duplex mode"
              }
            ],
            "enabled": false,
            "supported": false
          }
        ],
        "descr": [
          {
            "value": "vboxnet1"
          }
        ],
        "id": [
          {
            "type": "mac",
            "value": "0a:00:27:00:00:01"
          }
        ],
        "ttl": [
          {
            "value": "120"
          }
        ]
      }
    ],
    "rid": "2",
    "via": "LLDP"
  },
  {
    "age": "0 day, 00:01:01",
    "chassis": [
      {
        "capability": [
          {
            "enabled": false,
            "type": "Bridge"
          },
```

```
            {
              "enabled": false,
              "type": "Router"
            },
            {
              "enabled": false,
              "type": "Wlan"
            },
            {
              "enabled": true,
              "type": "Station"
            }
          ],
          "descr": [
            {
              "value": "Element OS 11.0"
            }
          ],
          "id": [
            {
              "type": "mac",
              "value": "08:00:27:3c:0a:f4"
            }
          ],
          "mgmt-ip": [
            {
              "value": "10.0.2.15"
            },
            {
              "value": "fe80::a00:27ff:fe3c:af4"
            }
          ],
          "name": [
            {
              "value": "SF-93FF"
            }
          ]
        }
      ],
      "lldp-med": [
        {
          "capability": [
            {
              "available": true,
              "type": "Capabilities"
            },
```

```
        {
          "available": true,
          "type": "Policy"
        },
        {
          "available": true,
          "type": "Location"
        },
        {
          "available": true,
          "type": "MDI/PSE"
        },
        {
          "available": true,
          "type": "MDI/PD"
        },
        {
          "available": true,
          "type": "Inventory"
        }
      ],
      "device-type": [
        {
          "value": "Generic Endpoint (Class I)"
        }
      ],
      "inventory": [
        {
          "firmware": [
            {
              "value": "VirtualBox"
            }
          ],
          "hardware": [
            {
              "value": "1.2"
            }
          ],
          "manufacturer": [
            {
              "value": "innotek GmbH"
            }
          ],
          "model": [
            {
              "value": "VirtualBox"
```

```
                    }
                  ],
                  "serial": [
                    {
                      "value": "0"
                    }
                  ],
                  "software": [
                    {
                      "value": "4.14.27-solidfire2"
                    }
                  ]
                }
              ]
            }
          ],
          "name": "eth3",
          "port": [
            {
              "aggregation": [
                {
                  "value": "6"
                }
              ],
              "auto-negotiation": [
                {
                  "advertised": [
                    {
                      "fd": true,
                      "hd": true,
                      "type": "10Base-T"
                    },
                    {
                      "fd": true,
                      "hd": true,
                      "type": "100Base-TX"
                    },
                    {
                      "fd": true,
                      "hd": false,
                      "type": "1000Base-T"
                    }
                  ],
                  "current": [
                    {
                      "value": "1000BaseTFD"
```

```
                        }
                      ],
                      "enabled": true,
                      "supported": true
                    }
                  ],
                  "descr": [
                    {
                      "value": "eth2"
                    }
                  ],
                  "id": [
                    {
                      "type": "mac",
                      "value": "08:00:27:fc:f0:a9"
                    }
                  ],
                  "ttl": [
                    {
                      "value": "120"
                    }
                  ]
                }
              ],
              "rid": "1",
              "via": "LLDP"
            }
          ]
        }
      ]
    }
    }
 }
}
```


GetNetworkConfig

Il `GetNetworkConfig` method restituisce una risposta simile all'esempio seguente.


```
{
    "id": 1,
    "result": {
        "network": {
            "Bond10G": {
                "#default": false,
```

```
                "address": "10.1.1.0",
                "auto": true,
                "bond-downdelay": "0",
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth0 eth1",
                "bond-updelay": "200",
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
                "family": "inet",
                "gateway": "10.1.1.0",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "static",
                "mtu": "9000",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "9000",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "Bond1G": {
                "#default": true,
                "address": "10.1.1.0",
                "addressV6": "",
                "auto": true,
                "bond-downdelay": "0",
```

```
                "bond-fail_over_mac": "None",
                "bond-miimon": "100",
                "bond-mode": "ActivePassive",
                "bond-primary_reselect": "Failure",
                "bond-slaves": "eth2 eth3",
                "bond-updelay": "200",
                "dns-nameservers": "10.1.1.0, 10.1.1.0",
                "dns-search": "ten.test.company.net., company.net.",
                "family": "inet",
                "gateway": "10.1.1.254",
                "gatewayV6": "",
                "linkSpeed": 1000,
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "static",
                "mtu": "1500",
                "netmask": "255.255.240.0",
                "network": "10.1.1.0",
                "physical": {
                    "address": "10.1.1.0",
                    "macAddress": "c8:1f:66:ee:59:bd",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "mtu": "1500",
                    "netmask": "255.255.240.0",
                    "network": "10.1.1.0",
                    "upAndRunning": true
                },
                "routes": [],
                "status": "UpAndRunning",
                "symmetricRouteRules": [
                    "ip route add 10.1.1.1/20 dev Bond1G src 10.1.2.2
table Bond1G",
                    "ip rule add from 10.1.1.1 table Bond1G",
                    "ip route add default via 10.1.1.254"
                ],
                "upAndRunning": true,
                "virtualNetworkTag": "0"
            },
            "eth0": {
                "auto": true,
                "bond-master": "Bond10G",
                "family": "inet",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:b9",
                "method": "bond",
```

```
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "c8:1f:66:ee:59:b9",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "eth1": {
                "auto": true,
                "bond-master": "Bond10G",
                "family": "inet",
                "linkSpeed": 10000,
                "macAddress": "c8:1f:66:ee:59:b9",
                "macAddressPermanent": "c8:1f:66:ee:59:bb",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:b9",
                    "macAddressPermanent": "c8:1f:66:ee:59:bb",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "eth2": {
                "auto": true,
                "bond-master": "Bond1G",
                "family": "inet",
                "linkSpeed": 1000,
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "c8:1f:66:ee:59:bd",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:bd",
                    "macAddressPermanent": "c8:1f:66:ee:59:bd",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
```

```
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "eth3": {
                "auto": true,
                "bond-master": "Bond1G",
                "family": "inet",
                "linkSpeed": 1000,
                "macAddress": "c8:1f:66:ee:59:bd",
                "macAddressPermanent": "c8:1f:66:ee:59:bf",
                "method": "bond",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "c8:1f:66:ee:59:bd",
                    "macAddressPermanent": "c8:1f:66:ee:59:bf",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            },
            "lo": {
                "auto": true,
                "family": "inet",
                "linkSpeed": 0,
                "macAddress": "00:00:00:00:00:00",
                "macAddressPermanent": "00:00:00:00:00:00",
                "method": "loopback",
                "physical": {
                    "address": "0.0.0.0",
                    "macAddress": "00:00:00:00:00:00",
                    "macAddressPermanent": "00:00:00:00:00:00",
                    "netmask": "N/A",
                    "network": "N/A",
                    "upAndRunning": true
                },
                "status": "UpAndRunning",
                "upAndRunning": true
            }
        }
    }
}
```

GetNodeHardwareInfo (output per iSCSI)

Il `GetNodeHardwareInfo` Method for iSCSI restituisce una risposta simile all'esempio seguente.


```
{
    "id": 1,
    "result": {
        "nodeHardwareInfo": {
            "bus": {
                "core_DMI:0200": {
                    "description": "Motherboard",
                    "physid": "0",
                    "product": "0H47HH",
                    "serial": "..CN7475141I0271.",
                    "vendor": "SolidFire",
                    "version": "A07"
                }
            },
            "driveHardware": [
                {
                "canonicalName": "sda",
                "connected": true,
                "dev": 2048,
                "devPath": "/dev/slot0",
                "driveEncryptionCapability": "fips",
                "driveType": "Slice",
                "lifeRemainingPercent": 98,
                "lifetimeReadBytes": 0,
                "lifetimeWriteBytes": 14012129342144,
                "name": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
                "path": "/dev/sda",
                "pathLink": "/dev/slot0",
                "powerOnHours": 15489,
                "product": "SAMSUNG MZ7GE240HMGR-00003",
                "reallocatedSectors": 0,
                "reserveCapacityPercent": 100,
                "scsiCompatId": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
                "scsiState": "Running",
                "securityAtMaximum": false,
                "securityEnabled": true,
                "securityFrozen": false,
                "securityLocked": false,
                "securitySupported": true,
                "serial": "S1M9NWAG501251",
                "size": 240057409536,
```

```
                "slot": 0,
                "uncorrectableErrors": 0,
                "uuid": "789aa05d-e49b-ff4f-f821-f60eed8e43bd",
                "vendor": "Samsung",
                "version": "EXT1303Q"
                },
                {
                "canonicalName": "sda",
                "connected": true,
                "dev": 2048,
                "devPath": "/dev/slot1",
                "driveEncryptionCapability": "fips",
                "driveType": "Slice",
                "lifeRemainingPercent": 98,
                "lifetimeReadBytes": 0,
                "lifetimeWriteBytes": 14112129567184,
                "name": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
                "path": "/dev/sda",
                "pathLink": "/dev/slot0",
                "powerOnHours": 15489,
                "product": "SAMSUNG MZ7GE240HMGR-00003",
                "reallocatedSectors": 0,
                "reserveCapacityPercent": 100,
                "scsiCompatId": "scsi-SATA_SAMSUNG_MZ7GE24S1M9NWAG501251",
                "scsiState": "Running",
                "securityAtMaximum": false,
                "securityEnabled": true,
                "securityFrozen": false,
                "securityLocked": false,
                "securitySupported": true,
                "serial": "S1M9NWAG501252",
                "size": 240057409536,
                "slot": 0,
                "uncorrectableErrors": 0,
                "uuid": "789aa05d-e49b-ff4f-f821-f60eed8e43bd",
                "vendor": "Samsung",
                "version": "EXT1303Q"
                }
    }
```


GetNodeHardwareInfo (output per nodi Fibre Channel)

Il `GetNodeHardwareInfo` Method for Fibre Channel Node restituisce una risposta simile all'esempio seguente.

```
{
"id": null,
"result": {
"nodeHardwareInfo": {
"bus": {
"core_DMI:0200": {
"description": "Motherboard",
"physid": "0",
"product": "0H47HH",
"serial": "..CN747513AA0541.",
"version": "A07"
},
"fiber:0_PCI:0000:04:00.0": {
"businfo": "pci@0000:04:00.0",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:0_PCI:0000:42:00.0": {
"businfo": "pci@0000:42:00.0",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:1_PCI:0000:04:00.1": {
"businfo": "pci@0000:04:00.1",
"clock": "33000000",
"description": "Fibre Channel",
"physid": "0.1",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
},
"fiber:1_PCI:0000:42:00.1": {
"businfo": "pci@0000:42:00.1",
"clock": "33000000",
"description": "Fibre Channel",
```

```
"physid": "0.1",
"product": "ISP8324-based 16Gb Fibre Channel to PCI Express Adapter",
"vendor": "QLogic Corp.",
"version": "02",
"width": "64"
}
},
"fans": {
"Fan1A RPM": {
"baseUnit": "RPM",
"threshold": 840,
"value": 3360
},
"Fan1B RPM": {
"baseUnit": "RPM",
"threshold": 840,
"value": 3120
}
},
"fibreChannelPorts": [
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 1,
"internalPortID": 2,
"model": "QLE2672",
"nPortID": "0x060019",
"nodeID": 6,
"pciSlot": 3,
"serial": "BFE1335E04217",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:9c:71:01",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:0a"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 2,
"internalPortID": 3,
"model": "QLE2672",
"nPortID": "0xc70019",
"nodeID": 6,
"pciSlot": 3,
"serial": "BFE1335E04217",
"speed": "8 Gbit",
"state": "Online",
```

```
"switchWwn": "20:01:00:2a:6a:98:a3:41",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:0b"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 1,
"internalPortID": 0,
"model": "QLE2672",
"nPortID": "0xc70017",
"nodeID": 6,
"pciSlot": 2,
"serial": "BFE1341E09515",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:98:a3:41",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:08"
},
{
"firmware": "7.04.00 (d0d5)",
"hbaPort": 2,
"internalPortID": 1,
"model": "QLE2672",
"nPortID": "0x060017",
"nodeID": 6,
"pciSlot": 2,
"serial": "BFE1341E09515",
"speed": "8 Gbit",
"state": "Online",
"switchWwn": "20:01:00:2a:6a:9c:71:01",
"wwnn": "5f:47:ac:c8:30:26:c9:00",
"wwpn": "5f:47:ac:c0:30:26:c9:09"
}
],
"memory": {
"firmware_": {
"capacity": "8323072",
"date": "08/29/2013",
"description": "BIOS",
"physid": "0",
"size": "65536",
"version": "2.0.19"
},
"memory_DMI:1000": {
"description": "System Memory",
```

```
"physid": "1000",
"size": "34359738368",
"slot": "System board or motherboard"
}
},
"network": {
"network:0_": {
"description": "Ethernet interface",
"logicalname": "Bond1G",
"physid": "1",
"serial": "c8:1f:66:df:04:da"
},
"network:0_PCI:0000:01:00.0": {
"businfo": "pci@0000:01:00.0",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth0",
"physid": "0",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:d6",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:0_PCI:0000:41:00.0": {
"businfo": "pci@0000:41:00.0",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth4",
"physid": "0",
"product": "NetXtreme II BCM57810 10 Gigabit Ethernet",
"serial": "00:0a:f7:41:7a:30",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:1_": {
"description": "Ethernet interface",
"logicalname": "Bond10G",
"physid": "2",
"serial": "c8:1f:66:df:04:d6"
},
"network:1_PCI:0000:01:00.1": {
"businfo": "pci@0000:01:00.1",
```

```
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth1",
"physid": "0.1",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:d8",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:1_PCI:0000:41:00.1": {
"businfo": "pci@0000:41:00.1",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth5",
"physid": "0.1",
"product": "NetXtreme II BCM57810 10 Gigabit Ethernet",
"serial": "00:0a:f7:41:7a:32",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:2_PCI:0000:01:00.2": {
"businfo": "pci@0000:01:00.2",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth2",
"physid": "0.2",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
"serial": "c8:1f:66:df:04:da",
"size": "1000000000",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
},
"network:3_PCI:0000:01:00.3": {
"businfo": "pci@0000:01:00.3",
"capacity": "1000000000",
"clock": "33000000",
"description": "Ethernet interface",
"logicalname": "eth3",
"physid": "0.3",
"product": "NetXtreme II BCM57800 1/10 Gigabit Ethernet",
```

```
"serial": "c8:1f:66:df:04:dc",
"size": "1000000000",
"vendor": "Broadcom Corporation",
"version": "10",
"width": "64"
}
},
"networkInterfaces": {
"Bond10G": {
"isConfigured": true,
"isUp": true
},
"Bond1G": {
"isConfigured": true,
"isUp": true
},
"eth0": {
"isConfigured": true,
"isUp": true
},
"eth1": {
"isConfigured": true,
"isUp": true
},
"eth2": {
"isConfigured": true,
"isUp": true
},
"eth3": {
"isConfigured": true,
"isUp": true
},
"eth4": {
"isConfigured": true,
"isUp": true
},
"eth5": {
"isConfigured": true,
"isUp": true
}
},
"platform": {
"chassisType": "R620",
"cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz",
"nodeMemoryGB": 32,
"nodeType": "SFFC"
```

```
},
"powerSupplies": {
"PS1 status": {
"powerSupplyFailureDetected": false,
"powerSupplyHasAC": true,
"powerSupplyPredictiveFailureDetected": false,
"powerSupplyPresent": true
},
"PS2 status": {
"powerSupplyFailureDetected": false,
"powerSupplyHasAC": true,
"powerSupplyPredictiveFailureDetected": false,
"powerSupplyPresent": true
}
},
"storage": {
"storage_PCI:0000:00:1f.2": {
"businfo": "pci@0000:00:1f.2",
"clock": "66000000",
"description": "SATA controller",
"physid": "1f.2",
"product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
"vendor": "Intel Corporation",
"version": "05",
"width": "32"
}
},
"system": {
"fcn-2_DMI:0100": {
"description": "Rack Mount Chassis",
"product": "(SKU=NotProvided;ModelName=)",
"serial": "HTX1DZ1",
"width": "64"
}
},
"temperatures": {
"Exhaust Temp": {
"baseUnit": "C",
"threshold": 70,
"value": 38
},
"Inlet Temp": {
"baseUnit": "C",
"threshold": 42,
"value": 13
  },
```

```
"uuid": "4C4C4544-004D-5310-8052-C4C04F335431"
    }
   }
  }
 }
}
```

GetNvramInfo

Il `GetNvramInfo` method restituisce una risposta simile all'esempio seguente.

```
{
  id: 1,
  result: {
    nvramInfo: {
      details: {
         errors: {
           numOfErrorLogEntries: "0"
         },
         extended: {
            dialogVersion: "4",
            event: [
               {
                   name: "flushToFlash",
                   time: "2014-02-24 20:30:28",
                   value: "0"
         },
         {
                   name: "flushToFlash",
                   time: "1946-02-06 17:16:42",
                   value: "0"
         },
         {
                   name: "flushToFlash",
                   time: "2014-02-25 00:48:06",
                   value: "0"
         },
         {
                   name: "flushToFlash",
                   time: "2014-02-25 15:44:07",
                   value: "0"
         },
         {
                   name: "flushToFlash",
                   time: "2014-03-17 17:21:46",
```

```
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 17:59:30",
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 18:06:27",
                value: "0"
        },
        {
                name: "flushToFlash",
                time: "2014-03-17 21:43:17",
                value: "0"
        },
        {
                name: "excessiveCurrent",
                time: "2014-02-25 00:00:29",
                value: "39"
        },
         {
                name: "excessiveCurrent",
                time: "2014-03-01 00:00:24",
                value: "23"
         }
      ],
           eventOccurrences: [
        {
                count: "15",
                name: "flushToFlash"
        },
        {
                count: "2",
                name: "excessiveCurrent"
        }
                initialCapacitance: "6.653 F",
                initialEsr: "0.097 Ohm",
           measurement: [
        {
                level_0: " 0",
                level_1: " 112",
                level_2: " 670919",
                level_3: " 455356",
                level_4: " 90215",
```

```
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "enterpriseFlashControllerTemperature",
                recent: "64 C"
        },
        {
                level_0: " 0",
                level_1: " 27",
                level_2: " 456896",
                level_3: " 717565",
                level_4: " 39422",
                level_5: " 2692",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitor1And2Temperature",
                recent: "28.64 C"
        },
        {
                level_0: " 0",
                level_1: " 2080",
                level_2: " 907196",
                level_3: " 280178",
                level_4: " 26539",
                level_5: " 609",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitor3And4Temperature",
                recent: "28.60 C"
        },
        {
                errorPeriod: {
                    duration: "24",
                    startTime: "2014-02-06 00:23:54",
                    worst: "8"
                },
                level_0: " 0",
                level_1: " 839",
                level_2: " 272794",
                level_3: " 404758",
```

```
                level_4: " 35216",
                level_5: " 377818",
                level_6: " 103891",
                level_7: " 21274",
                level_8: " 12",
                level_9: " 0",
                name: "rearVentAmbientTemperature",
                recent: "46.82 C"
        },
        {
                level_0: " 0",
                level_1: " 742749",
                level_2: " 460016",
                level_3: " 13837",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "rms200BoardTemperature",
                recent: "50.62 C"
        },
        {
                name: "voltageOfCapacitor1",
                recent: "2.308 V"
        },
        {
                name: "voltageOfCapacitor2",
                recent: "2.305 V"},
        {
                name: "voltageOfCapacitor3",
                recent: "2.314 V"
        },
        {
                name: "voltageOfCapacitor4",
                recent: "2.307 V"
        },
        {
               level_0: " 175052",
               level_1: " 51173",
               level_2: " 435788",
               level_3: " 12766",
               level_4: " 4",
               level_5: " 6",
               level_6: " 541813",
```

```
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "capacitorPackVoltage",
                recent: "9.233 V"
         },
         {
                level_0: " 0",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 4",
                level_7: " 1",
                level_8: " 4",
                level_9: " 6",
                name: "capacitorPackVoltageAtEndOfFlushToFlash",
                recent: "5.605 V"
        },
        {
                name: "currentDerivedFromV3V4",
                recent: "0.000 A"
        },
        {
                level_0: " 7",
                level_1: " 4",
                level_2: " 3",
                level_3: " 1",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "derivedEnergy",
                recent: "175 Joules"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
```

```
                level_7: " 17",
                level_8: " 19",
                level_9: " 7",
                name: "derivedCapacitanceOfThePack",
                recent: "5.959 F"
         },
         {
                level_0: " 0",
                level_1: " 43",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "derivedEsrOfCapacitorPack",
                recent: "0.104 Ohm"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 15",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "timeToRunFlushToFlash",
                recent: "22.40 Seconds"
        },
        {
                level_0: " 0",
                level_1: " 0",
                level_2: " 7",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "timeToRunRestore",
```

```
                recent: "20.44 Seconds"
        },
        {
                level_0: " 0",
                level_1: " 1",
                level_2: " 3",
                level_3: " 2",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 1",
                name: "timeToChargeCapacitors",
                recent: "48 Seconds"
        },
        {
                level_0: " 448586",
                level_1: " 2998",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name: "correctableBitsInErrorOnReadingAPage"
        },
        {
                level_0: " 2998",
                level_1: " 0",
                level_2: " 0",
                level_3: " 0",
                level_4: " 0",
                level_5: " 0",
                level_6: " 0",
                level_7: " 0",
                level_8: " 0",
                level_9: " 0",
                name:
"correctableBitsInErrorOnReadingTheWorstBchRegionOfAPage"
        },
        {
                level_0: " 0",
                level_1: " 37",
```

```
                level_2: " 280274",
                level_3: " 422999",
                level_4: " 245814",
                level_5: " 242470",
                level_6: " 24447",
                level_7: " 561",
                level_8: " 0",
                level_9: " 0",
                name: "fanInletAmbientTemperature",
                recent: "41.74 C"
        }
        ],
                predictedCapacitanceDepletion: "504328 uF",
                smartCounters: [
        {
                name: "numberOf512ByteBlocksReadFromDdr",
                value: "218284648"
        },
        {
                name: "numberOf512ByteBlocksWrittenToDdr",
                value: "12031567354"
        },
        {
                name: "numberOfHostReadCommands",
                value: "5366315"
        },
        {
                name: "numberOfHostWriteCommands",
                value: "1266099334"
        },
        {
                name: "controllerBusyTimeMinutes",
                value: "0"
        },
        {
                name: "numberOfPowerCycles",
                value: "13"
        },
        {
                name: "powerOnHours",
                value: "1009"
        },
        {
                name: "unsafeShutdowns",
                value: "5"
        },
```

```
        {
                name: "mediaErrors",
                value: "0"
        },
        {
                name: "numberOfErrorLogs",
                value: "2"
        }
        ],
         snapshotTime: "2014-03-20 16:43:49"
     },
     firmware: {
         activeSlotNumber: "2",
         slot1Version: "1e5817bc",
         slot2Version: "1e0d70ac",
         slot3Version: "1e5817bc",
         slot4Version: "1e5817bc"
    },
     smart: {
         availableSpace: "0%",
         availableSpaceThreshold: "0%",
         controllerBusyTimeMinutes: "0",
         criticalErrorVector: "0x0",
         mediaErrors: "0",
         numberOf512ByteBlocksRead: "218284648",
         numberOf512ByteBlocksWritten: "12031567354",
         numberOfErrorInfoLogs: "2",
         numberOfHostReadCommands: "5366315",
         numberOfHostWriteCommands: "1266099334",
         numberOfPowerCycles: "13",
         powerOnHours: "1009",
         temperature: "323 Kelvin",
         unsafeShutdowns: "5"
      }
     },
     status: "Warning",
     statusInfo: {
     warning: [
         "excessiveCurrent (2x)"
       ]
     },
     type: "RMS-200"
    }
  }
}
```

ListActiveNode

Il `ListActiveNodes` method restituisce una risposta simile all'esempio seguente.

```
 {
    "id": 1,
    "result": {
        "nodes": [
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 1,
                "attributes": {},
                "cip": "172.27.21.23",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.23",
                "mipi": "Bond1G",
                "name": "PSN-1-23",
                "nodeID": 1,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.23",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0056-3810-804E-B5C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.4",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.10",
                        "virtualNetworkID": 2
                    }
                ]
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 4,
                "attributes": {},
                "cip": "172.27.21.24",
```

```
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.24",
                "mipi": "Bond1G",
                "name": "PSN-1-24",
                "nodeID": 2,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.24",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0042-4210-804E-C3C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.5",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.11",
                        "virtualNetworkID": 2
                    }
                ]
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 2,
                "attributes": {},
                "cip": "172.27.21.25",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.25",
                "mipi": "Bond1G",
                "name": "PSN-1-25",
                "nodeID": 3,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
```

```
                "sip": "172.27.21.25",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0053-4210-8051-C6C04F515631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.6",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.12",
                        "virtualNetworkID": 2
                    }
                ]
            },
            {
                "associatedFServiceID": 0,
                "associatedMasterServiceID": 3,
                "attributes": {},
                "cip": "172.27.21.26",
                "cipi": "Bond10G",
                "fibreChannelTargetPortGroup": null,
                "mip": "172.27.1.26",
                "mipi": "Bond1G",
                "name": "PSN-1-26",
                "nodeID": 4,
                "platformInfo": {
                    "chassisType": "R620",
                    "cpuModel": "Intel(R) Xeon(R) CPU E5-2640 0 @
2.50GHz",
                    "nodeMemoryGB": 72,
                    "nodeType": "SF3010"
                },
                "sip": "172.27.21.26",
                "sipi": "Bond10G",
                "softwareVersion": "9.0.0.1298",
                "uuid": "4C4C4544-0056-3810-804E-B4C04F4C5631",
                "virtualNetworks": [
                    {
                        "address": "10.1.2.7",
                        "virtualNetworkID": 1
                    },
                    {
                        "address": "10.2.2.13",
                        "virtualNetworkID": 2
                    }
```

```
                ]
            }
        ]
    }
 }
```

ListActiveVolumes

Il `ListActiveVolumes` method restituisce una risposta simile all'esempio seguente.

```
{
    "id": 1,
    "result": {
        "volumes": [
            {
                "access": "readWrite",
                "accountID": 1,
                "attributes": {},
                "blockSize": 4096,
                "createTime": "2016-06-23T14:19:12Z",
                "deleteTime": "",
                "enable512e": false,
                "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo1.1",
                "name": "HulkDemo1",
                "purgeTime": "",
                "qos": {
                    "burstIOPS": 1500,
                    "burstTime": 60,
                    "curve": {
                        "4096": 100,
                        "8192": 160,
                        "16384": 270,
                        "32768": 500,
                        "65536": 1000,
                        "131072": 1950,
                        "262144": 3900,
                        "524288": 7600,
                        "1048576": 15000
                    },
                    "maxIOPS": 1000,
                    "minIOPS": 100
                },
                "scsiEUIDeviceID": "306f746f00000001f47acc0100000000",
                "scsiNAADeviceID": "6f47acc100000000306f746f00000001",
                "sliceCount": 1,
```

```
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 1,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:14Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo6.6",
            "name": "HulkDemo6",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000006f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000006",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
```

```
            "volumeID": 6,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:14Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo7.7",
            "name": "HulkDemo7",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000007f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000007",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 7,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
```

```
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:15Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo8.8",
            "name": "HulkDemo8",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000008f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000008",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 8,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:15Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo9.9",
```

```
            "name": "HulkDemo9",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000009f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000009",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 9,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:16Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo12.12",
            "name": "HulkDemo12",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
```

```
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f0000000cf47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f0000000c",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 12,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo16.16",
            "name": "HulkDemo16",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
```

```
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000010f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000010",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 16,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo17.17",
            "name": "HulkDemo17",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
```

```
            },
            "scsiEUIDeviceID": "306f746f00000011f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000011",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 17,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-23T14:19:18Z",
            "deleteTime": "",
            "enable512e": false,
            "iqn": "iqn.2010-01.com.solidfire:0oto.hulkdemo18.18",
            "name": "HulkDemo18",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 1500,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 1000,
                "minIOPS": 100
            },
            "scsiEUIDeviceID": "306f746f00000012f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000012",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 53687091200,
```

```
            "virtualVolumeID": null,
            "volumeAccessGroups": [
                1
            ],
            "volumeID": 18,
            "volumePairs": []
        },
        {
            "access": "readWrite",
            "accountID": 1,
            "attributes": {},
            "blockSize": 4096,
            "createTime": "2016-06-24T15:21:59Z",
            "deleteTime": "",
            "enable512e": true,
            "iqn": "iqn.2010-01.com.solidfire:0oto.bk.24",
            "name": "BK",
            "purgeTime": "",
            "qos": {
                "burstIOPS": 15000,
                "burstTime": 60,
                "curve": {
                    "4096": 100,
                    "8192": 160,
                    "16384": 270,
                    "32768": 500,
                    "65536": 1000,
                    "131072": 1950,
                    "262144": 3900,
                    "524288": 7600,
                    "1048576": 15000
                },
                "maxIOPS": 15000,
                "minIOPS": 50
            },
            "scsiEUIDeviceID": "306f746f00000018f47acc0100000000",
            "scsiNAADeviceID": "6f47acc100000000306f746f00000018",
            "sliceCount": 1,
            "status": "active",
            "totalSize": 10737418240,
            "virtualVolumeID": null,
            "volumeAccessGroups": [],
            "volumeID": 24,
            "volumePairs": [
                {
                    "clusterPairID": 2,
```

```
                        "remoteReplication": {
                            "mode": "Async",
                            "pauseLimit": 3145728000,
                            "remoteServiceID": 14,
                            "resumeDetails": "",
                            "snapshotReplication": {
                                "state": "Idle",
                                "stateDetails": ""
                            },
                            "state": "Active",
                            "stateDetails": ""
                        },
                        "remoteSliceID": 8,
                        "remoteVolumeID": 8,
                        "remoteVolumeName": "PairingDoc",
                        "volumePairUUID": "229fcbf3-2d35-4625-865a-
d04bb9455cef"
                    }
                ]
            }
        ]
    }
}
```

TestHardwareConfig

Il `TestHardwareConfig` method restituisce una risposta simile all'esempio seguente.

```
{
"id": 1,
"result": {
    "nodes": [
        {
            "nodeID": 1,
            "result": {
                "details": {
                    "BIOS_REVISION": {
                        "Passed": true,
                        "actual": "2.0",
                        "comparator": ">=",
                        "expected": "1.0.0.0"
                    },
                    "BIOS_VENDOR": {
                        "Passed": true,
                        "actual": "SolidFire",
```

```
                        "comparator": "==",
                        "expected": "SolidFire"
                    },
                    "BIOS_VERSION": {
                        "Passed": true,
                        "actual": "2.0.19",
                        "comparator": ">=",
                        "expected": "2.0.19"
                    },
                    "CPU_CORES_00": {
                        "Passed": true,
                        "actual": "6",
                        "comparator": "==",
                        "expected": "6"
                    },
                    "CPU_CORES_01": {
                        "Passed": true,
                        "actual": "6",
                        "comparator": "==",
                        "expected": "6"
                    },
                    "CPU_CORES_ENABLED_00": {
                        "Passed": true,
                        "actual": "6",
                        "comparator": "==",
                        "expected": "6"
                    },
                    "CPU_CORES_ENABLED_01": {
                        "Passed": true,
                        "actual": "6",
                        "comparator": "==",
                        "expected": "6"
                    },
                    "CPU_MODEL_00": {
                        "Passed": true,
                        "actual": "Intel(R) Xeon(R) CPU E5-2620 v2 @
2.10GHz",
                        "comparator": "==",
                        "expected": "Intel(R) Xeon(R) CPU E5-2620 v2 @
2.10GHz"
                    },
                    "CPU_MODEL_01": {
                        "Passed": true,
                        "actual": "Intel(R) Xeon(R) CPU E5-2620 v2 @
2.10GHz",
                        "comparator": "==",
```

```
                        "expected": "Intel(R) Xeon(R) CPU E5-2620 v2 @
2.10GHz"
                    },
                    "CPU_THREADS_00": {
                        "Passed": true,
                        "actual": "12",
                        "comparator": "==",
                        "expected": "12"
                    },
                    "CPU_THREADS_01": {
                        "Passed": true,
                        "actual": "12",
                        "comparator": "==",
                        "expected": "12"
                    },
                    "CPU_THREADS_ENABLED": {
                        "Passed": true,
                        "actual": "24",
                        "comparator": "==",
                        "expected": "24"
                    },
                    "IDRAC_VERSION": {
                        "Passed": true,
                        "actual": "2.41.40.40",
                        "comparator": ">=",
                        "expected": "1.06.06"
                    },
                    "MEMORY_GB": {
                        "Passed": true,
                        "actual": "64",
                        "comparator": ">=",
                        "expected": "64"
                    },
                    "MEMORY_MHZ_00": {
                        "Passed": true,
                        "actual": "1600",
                        "comparator": ">=",
                        "expected": "1333"
                    },
                    "MEMORY_MHZ_01": {
                        "Passed": true,
                        "actual": "1600",
                        "comparator": ">=",
                        "expected": "1333"
                    },
                    "MEMORY_MHZ_02": {
```

```
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MEMORY_MHZ_03": {
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MEMORY_MHZ_04": {
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MEMORY_MHZ_05": {
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MEMORY_MHZ_06": {
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MEMORY_MHZ_07": {
                    "Passed": true,
                    "actual": "1600",
                    "comparator": ">=",
                    "expected": "1333"
                },
                "MPTSAS_BIOS_VERSION": {
                    "Passed": true,
                    "actual": "07.24.01.00",
                    "comparator": "ANY",
                    "expected": "7.25.0.0"
                },
                "MPTSAS_FIRMWARE_VERSION": {
                    "Passed": true,
                    "actual": "13.00.57.00",
                    "comparator": "==",
                    "expected": "13.0.57.0"
```

```
                    },
                    "NETWORK_DRIVER_ETH0": {
                        "Passed": true,
                        "actual": "bnx2x",
                        "comparator": "==",
                        "expected": "bnx2x"
                    },
                    "NETWORK_DRIVER_ETH1": {
                        "Passed": true,
                        "actual": "bnx2x",
                        "comparator": "==",
                        "expected": "bnx2x"
                    },
                    "NETWORK_DRIVER_ETH2": {
                        "Passed": true,
                        "actual": "bnx2x",
                        "comparator": "==",
                        "expected": "bnx2x"
                    },
                    "NETWORK_DRIVER_ETH3": {
                        "Passed": true,
                        "actual": "bnx2x",
                        "comparator": "==",
                        "expected": "bnx2x"
                    },
                    "NETWORK_FIRMWARE_VERSION_ETH0": {
                        "Passed": true,
                        "actual": "7.10.18-solidfire-5f3ccbc781d53",
                        "comparator": "==",
                        "expected": "7.10.18-solidfire-5f3ccbc781d53"
                    },
                    "NETWORK_FIRMWARE_VERSION_ETH1": {
                        "Passed": true,
                        "actual": "7.10.18-solidfire-5f3ccbc781d53",
                        "comparator": "==",
                        "expected": "7.10.18-solidfire-5f3ccbc781d53"
                    },
                    "NETWORK_FIRMWARE_VERSION_ETH2": {
                        "Passed": true,
                        "actual": "7.10.18-solidfire-5f3ccbc781d53",
                        "comparator": "==",
                        "expected": "7.10.18-solidfire-5f3ccbc781d53"
                    },
                    "NETWORK_FIRMWARE_VERSION_ETH3": {
                        "Passed": true,
                        "actual": "7.10.18-solidfire-5f3ccbc781d53",
```

```
                        "comparator": "==",
                        "expected": "7.10.18-solidfire-5f3ccbc781d53"
                    },
                    "NUM_CPU": {
                        "Passed": true,
                        "actual": "2",
                        "comparator": "==",
                        "expected": "2"
                    },
                    "Parse failure in /var/log/sf-bios.info": {
                        "Passed": true,
                        "actual": "false",
                        "comparator": "==",
                        "expected": "false"
                    }
                },
                "duration": "00:00:00.195067",
                "result": "Passed"
            }
        }
    ]
}
}
```

Plug-in NetApp Element per server vCenter

Il plug-in NetApp Element per vCenter Server offre un plug-in per l'interfaccia VMware vSphere, che consente di gestire e monitorare i cluster di storage che eseguono il software NetApp Element.

Per ulteriori informazioni su Element Plug-in per vCenter Server, consultare la "Plug-in NetApp Element per la documentazione del server vCenter".

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"

Monitorare lo storage con SolidFire Active IQ

"SolidFire Active IQ" è uno strumento basato sul web che offre viste storiche costantemente aggiornate dei dati a livello di cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le performance e la capacità del sistema, oltre a essere sempre informato sullo stato dei cluster.

In SolidFire Active IQ sono disponibili le seguenti informazioni relative al sistema in uso:

- Numero di nodi e stato dei nodi: Integro, offline o guasto
- Rappresentazione grafica della CPU, dell'utilizzo della memoria e della limitazione dei nodi
- Dettagli sul nodo, come il numero di serie, la posizione dello slot nello chassis, il modello e la versione del software NetApp Element in esecuzione sul nodo di storage
- Informazioni relative a CPU e storage sulle macchine virtuali

Per ulteriori informazioni su SolidFire Active IQ, consultare "Documentazione SolidFire Active IQ".

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"
- **Sito di supporto NetApp › Tool per Active IQ**

Lavorare con il nodo di gestione

Panoramica del nodo di gestione

È possibile utilizzare il nodo di gestione (mNode) per utilizzare i servizi di sistema, gestire le risorse e le impostazioni del cluster, eseguire test e utility di sistema, configurare Active IQ per il monitoraggio del sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

> Come Best practice, associare un solo nodo di gestione a un'istanza di VMware vCenter ed evitare di definire le stesse risorse di storage e calcolo o istanze di vCenter in più nodi di gestione.

Per i cluster che eseguono Element Software versione 11.3 o successiva, è possibile utilizzare il nodo di gestione utilizzando una delle due interfacce seguenti:

- Con l'interfaccia utente del nodo di gestione (`https://[mNode IP]:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.
- Con l'interfaccia utente API REST integrata (`https://[mNode IP]/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

Installare o ripristinare un nodo di gestione:

- "Installare un nodo di gestione"
- "Configurazione di un NIC (Network Interface Controller) per lo storage"
- "Ripristinare un nodo di gestione"

Accedere al nodo di gestione:

- "Accedere al nodo di gestione (UI o REST API)"

Modificare il certificato SSL predefinito:

- "Modificare il certificato SSL predefinito del nodo di gestione"

Eseguire le attività con l'interfaccia utente del nodo di gestione:

- "Panoramica dell'interfaccia utente del nodo di gestione"

Eseguire le attività con le API REST del nodo di gestione:

- "Panoramica dell'interfaccia utente REST API del nodo di gestione"

Disattivare o attivare la funzionalità SSH remota o avviare una sessione di tunnel di supporto remoto con il supporto NetApp per risolvere i problemi:

- "Abilitare le connessioni remote del supporto NetApp"
- "Gestire la funzionalità SSH sul nodo di gestione"

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Installare o ripristinare un nodo di gestione

Installare un nodo di gestione

È possibile installare manualmente il nodo di gestione del cluster che esegue il software NetApp Element utilizzando l'immagine appropriata per la configurazione.

Questo processo manuale è destinato agli amministratori dello storage all-flash SolidFire che non utilizzano il motore di implementazione NetApp per l'installazione del nodo di gestione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- L'installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.

  Se è necessario supportare IPv6, è possibile utilizzare il nodo di gestione 11.1.

- Hai il permesso di scaricare il software dal NetApp Support Site.
- Hai identificato il tipo di immagine del nodo di gestione corretto per la tua piattaforma:

Piattaforma	Tipo di immagine di installazione
Microsoft Hyper-V.	iso
KVM	iso
VMware vSphere	iso, .ova
Citrix XenServer	iso
OpenStack	iso

- (Nodo di gestione 12.0 e versioni successive con server proxy) hai aggiornato NetApp Hybrid Cloud Control alla versione 2.16 dei servizi di gestione prima di configurare un server proxy.

A proposito di questa attività

Il nodo di gestione di Element 12.2 è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Prima di seguire questa procedura, è necessario conoscere "Volumi persistenti" e se si desidera o meno utilizzarli. I volumi persistenti sono opzionali ma consigliati per il ripristino dei dati di configurazione del nodo di gestione in caso di perdita di una macchina virtuale (VM).

Fasi

1. Scarica ISO o OVA e implementa la macchina virtuale
2. Creare il nodo di gestione admin e configurare la rete
3. Configurare la sincronizzazione dell'ora

4. Configurare il nodo di gestione
5. Configurare le risorse dei controller

Scarica ISO o OVA e implementa la macchina virtuale

1. Scaricare l'OVA o l'ISO per l'installazione dal "Software Element" Sul sito di supporto NetApp.
   a. Selezionare **Download Latest Release** (Scarica ultima versione) e accettare il contratto EULA.
   b. Selezionare l'immagine del nodo di gestione che si desidera scaricare.
2. Se l'OVA è stato scaricato, attenersi alla seguente procedura:
   a. Implementare OVA.
   b. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla VM sulla subnet di storage (ad esempio eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di storage.
3. Se è stato scaricato l'ISO, attenersi alla seguente procedura:
   a. Creare una nuova VM a 64 bit dall'hypervisor con la seguente configurazione:
      - Sei CPU virtuali
      - 24 GB DI RAM
      - Tipo di scheda di storage impostato su LSI Logic Parallel

        L'impostazione predefinita per il nodo di gestione potrebbe essere LSI Logic SAS. Nella finestra **Nuova macchina virtuale**, verificare la configurazione della scheda di storage selezionando **Personalizza hardware** > **hardware virtuale**. Se necessario, modificare LSI Logic SAS in **LSI Logic Parallel**.

      - Disco virtuale da 400 GB, con thin provisioning
      - Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
      - (Opzionale) un'interfaccia di rete virtuale con accesso alla rete di gestione al cluster di storage. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla macchina virtuale sulla subnet di storage (eth1) o assicurarsi che la rete di gestione possa essere instradata alla rete di storage.

        Non accendere la macchina virtuale prima della fase indicata in questa procedura.

   b. Collegare l'ISO alla macchina virtuale e avviare l'immagine di installazione .iso.

      L'installazione di un nodo di gestione mediante l'immagine potrebbe causare un ritardo di 30 secondi prima della visualizzazione della schermata iniziale.

4. Al termine dell'installazione, accendere la macchina virtuale per il nodo di gestione.

Creare il nodo di gestione admin e configurare la rete

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente admin del nodo di gestione.

Per spostarsi tra le opzioni di menu, premere i tasti freccia su o giù. Per spostarsi tra i pulsanti, premere Tab. Per spostarsi dai pulsanti ai campi, premere Tab. Per spostarsi tra i campi, premere i tasti freccia su o giù.

2. Se sulla rete è presente un server DHCP (Dynamic host Configuration Protocol) che assegna indirizzi IP con un numero massimo di unità di trasmissione (MTU) inferiore a 1500 byte, attenersi alla seguente procedura:

   a. Posizionare temporaneamente il nodo di gestione su una rete vSphere senza DHCP, ad esempio iSCSI.

   b. Riavviare la macchina virtuale o la rete della macchina virtuale.

   c. Utilizzando l'interfaccia telefonica utente, configurare l'IP corretto sulla rete di gestione con una MTU maggiore o uguale a 1500 byte.

   d. Riassegnare la rete VM corretta alla macchina virtuale.

   Un DHCP che assegna IP con un MTU inferiore a 1500 byte può impedire la configurazione della rete del nodo di gestione o l'utilizzo dell'interfaccia utente del nodo di gestione.

3. Configurare la rete dei nodi di gestione (eth0).

   Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di storage, consultare le istruzioni per la configurazione di un'altra scheda di rete: "Configurazione di un NIC (Network Interface Controller) per lo storage".

Configurare la sincronizzazione dell'ora

1. Assicurarsi che il tempo sia sincronizzato tra il nodo di gestione e il cluster di storage utilizzando NTP:

   A partire dall'elemento 12.3.1, i passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1, passare a. sottopase (f) per completare la configurazione di time sync.

1. Accedere al nodo di gestione utilizzando SSH o la console fornita dall'hypervisor.
2. Stop NTPD:

```
sudo service ntpd stop
```

3. Modificare il file di configurazione NTP `/etc/ntp.conf`:

   a. Commentare i server predefiniti (`server 0.gentoo.pool.ntp.org`) aggiungendo un `#` davanti a ciascuno.

   b. Aggiungere una nuova riga per ciascun server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati nel cluster di storage in "passo successivo".

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Al termine, salvare il file di configurazione.

4. Forzare una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

5. Riavviare NTPD.

```
sudo service ntpd start
```

6. Disattiva la sincronizzazione dell'ora con l'host tramite l'hypervisor (il seguente è un esempio VMware):

> Se si implementa mNode in un ambiente hypervisor diverso da VMware, ad esempio dall'immagine .iso in un ambiente OpenStack, fare riferimento alla documentazione dell'hypervisor per i comandi equivalenti.

a. Disattivare la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

b. Visualizzare e confermare lo stato corrente del servizio:

```
vmware-toolbox-cmd timesync status
```

c. In vSphere, verificare che `Synchronize guest time with host` Nelle opzioni della macchina virtuale, la casella di controllo non è selezionata.

> Non attivare questa opzione se si apportano modifiche future alla macchina virtuale.

> Non modificare l'NTP dopo aver completato la configurazione di Time Sync, in quanto influisce sull'NTP quando si esegue "comando di installazione" sul nodo di gestione.

Configurare il nodo di gestione

1. Configurare ed eseguire il comando di setup del nodo di gestione:

   Viene richiesto di inserire le password in un prompt sicuro. Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

   ```
   sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
   --storage_mvip [mvip] --storage_username [username] --telemetry_active
   [true]
   ```

   a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri richiesti:

      La forma abbreviata del nome del comando è tra parentesi ( ) e può essere sostituita con il nome completo.

      - **--mnode_admin_user (-mu) [nome utente]**: Il nome utente per l'account amministratore del nodo di gestione. Probabilmente si tratta del nome utente dell'account utente utilizzato per accedere al nodo di gestione.
      - **--storage_mvip (-SM) [indirizzo MVIP]**: L'indirizzo IP virtuale di gestione (MVIP) del cluster di storage che esegue il software Element. Configurare il nodo di gestione con lo stesso cluster di storage utilizzato durante "Configurazione dei server NTP".
      - **--storage_Username (-su) [Username]**: Il nome utente dell'amministratore del cluster di storage per il cluster specificato da `--storage_mvip` parametro.
      - **--Telemetry_Active (-t) [true]**: Conserva il valore true che consente la raccolta dei dati per l'analisi di Active IQ.

   b. (Facoltativo): Aggiungere i parametri dell'endpoint Active IQ al comando:

      - **--Remote_host (-rh) [AIQ_endpoint]**: L'endpoint in cui vengono inviati i dati di telemetria Active IQ per l'elaborazione. Se il parametro non è incluso, viene utilizzato l'endpoint predefinito.

   c. (Consigliato): Aggiungere i seguenti parametri di volume persistente. Non modificare o eliminare l'account e i volumi creati per la funzionalità dei volumi persistenti, altrimenti si verificherà una perdita delle funzionalità di gestione.

      - **--use_persistent_Volumes (-pv) [true/false, default: False]**: Attiva o disattiva i volumi persistenti. Inserire il valore true per abilitare la funzionalità dei volumi persistenti.
      - **--Persistent_Volumes_account (-pva) [nome_account]**: IF `--use_persistent_volumes` è impostato su true, utilizzare questo parametro e inserire il nome dell'account di storage che verrà utilizzato per i volumi persistenti.

        Utilizzare un nome account univoco per i volumi persistenti diverso da qualsiasi nome account esistente nel cluster. È di fondamentale importanza mantenere l'account dei volumi persistenti separato dal resto dell'ambiente.

      - **--persistent_Volumes_mvip (-pvm) [mvip]**: Immettere l'indirizzo IP virtuale di gestione (MVIP) del cluster di storage che esegue il software Element che verrà utilizzato con i volumi persistenti. Questo è necessario solo se il nodo di gestione gestisce più cluster di storage. Se non vengono gestiti più cluster, viene utilizzato il cluster predefinito MVIP.

d. Configurare un server proxy:

- **--use_proxy (-up) [true/false, default: False]**: Attiva o disattiva l'utilizzo del proxy. Questo parametro è necessario per configurare un server proxy.
- **--proxy_hostname_or_ip (-pi) [host]**: Il nome host o l'IP del proxy. Questa opzione è necessaria se si desidera utilizzare un proxy. Se si specifica questa opzione, viene richiesto di immettere `--proxy_port`.
- **--proxy_Username (-pu) [nome utente]**: Il nome utente del proxy. Questo parametro è facoltativo.
- **--proxy_password (-pp) [password]**: La password del proxy. Questo parametro è facoltativo.
- **--proxy_port (-pq) [port, default: 0]**: La porta proxy. Se si specifica questa opzione, viene richiesto di inserire il nome host o l'IP del proxy (`--proxy_hostname_or_ip`).
- **--proxy_ssh_port (-ps) [port, default: 443]**: La porta proxy SSH. Per impostazione predefinita, viene impostata la porta 443.

e. (Facoltativo) utilizzare la guida ai parametri se sono necessarie ulteriori informazioni su ciascun parametro:

- **--help (-h)**: Restituisce informazioni su ciascun parametro. I parametri sono definiti come obbligatori o facoltativi in base all'implementazione iniziale. I requisiti dei parametri di aggiornamento e ridistribuzione potrebbero variare.

f. Eseguire `setup-mnode` comando.

Configurare le risorse dei controller

1. Individuare l'ID di installazione:
   a. Da un browser, accedere all'interfaccia utente API REST del nodo di gestione:
   b. Accedere a Storage MVIP ed effettuare l'accesso. Questa azione fa sì che il certificato venga accettato per la fase successiva.
   c. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   d. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
   e. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   f. Selezionare **Provalo**.
   g. Selezionare **Esegui**.
   h. Dal corpo della risposta del codice 200, copiare e salvare `id` per l'installazione da utilizzare in un passaggio successivo.

      L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

2. Aggiungere una risorsa vCenter controller per NetApp Hybrid Cloud Control al nodo di gestione risorse

note:

a. Accedere all'interfaccia utente API del servizio mnode sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

```
https://<ManagementNodeIP>/mnode
```

b. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client`.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra.

c. Selezionare **POST /assets/{asset_id}/controller** per aggiungere una sottorisorsa del controller.

> È necessario creare un nuovo ruolo NetApp HCC in vCenter per aggiungere una sottorisorsa del controller. Questo nuovo ruolo di NetApp HCC limiterà la vista dei servizi del nodo di gestione alle risorse solo NetApp. Vedere "Creare un ruolo NetApp HCC in vCenter".

d. Selezionare **Provalo**.

e. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.

f. Inserire i valori del payload richiesti con il tipo `vCenter` E vCenter.

g. Selezionare **Esegui**.

Ulteriori informazioni

- "Volumi persistenti"
- "Aggiungere una risorsa controller al nodo di gestione"
- "Configurare una NIC storage"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Configurazione di un NIC (Network Interface Controller) per lo storage

Se si utilizza una scheda NIC aggiuntiva per lo storage, è possibile accedere al nodo di gestione tramite SSH o utilizzare la console vCenter ed eseguire un comando curl per impostare un'interfaccia di rete con tag o senza tag.

Prima di iniziare

- Conosci il tuo indirizzo IP eth0.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione 11.3 o successivo.

Opzioni di configurazione

Scegli l'opzione più adatta al tuo ambiente:

- Configurare un Network Interface Controller (NIC) per un'interfaccia di rete senza tag
- Configurare un NIC (Network Interface Controller) per lo storage per un'interfaccia di rete con tag

Configurare un Network Interface Controller (NIC) per un'interfaccia di rete senza tag

Fasi

1. Aprire una console SSH o vCenter.
2. Sostituire i valori nel seguente modello di comando ed eseguire il comando:

> I valori sono rappresentati da `$` per ciascuno dei parametri richiesti per la nuova interfaccia di rete dello storage. Il `cluster` l'oggetto nel seguente modello è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` oppure `-k` le opzioni non devono essere utilizzate negli ambienti di produzione.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
                "network": {
                           "$eth1": {
                                    "#default" : false,
                                    "address" : "$storage_IP",
                                    "auto" : true,
                                    "family" : "inet",
                                    "method" : "static",
                                    "mtu" : "9000",
                                    "netmask" : "$subnet_mask",
                                    "status" : "Up"
                                    }
                           },
                "cluster": {
                          "name": "$mnode_host_name"
                          }
             },
    "method": "SetConfig"
}
'
```

Configurare un NIC (Network Interface Controller) per lo storage per un'interfaccia di rete con tag

Fasi

1. Aprire una console SSH o vCenter.
2. Sostituire i valori nel seguente modello di comando ed eseguire il comando:

I valori sono rappresentati da `$` per ciascuno dei parametri richiesti per la nuova interfaccia di rete dello storage. Il `cluster` l'oggetto nel seguente modello è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` oppure `-k` le opzioni non devono essere utilizzate negli ambienti di produzione.

```
curl -u $mnode_user_name:$mnode_password --insecure -X POST \
https://$mnode_IP:442/json-rpc/10.0 \
-H 'Content-Type: application/json' \
-H 'cache-control: no-cache' \
-d ' {
     "params": {
                "network": {
                           "$eth1": {
                                    "#default" : false,
                                    "address" : "$storage_IP",
                                    "auto" : true,
                                    "family" : "inet",
                                    "method" : "static",
                                    "mtu" : "9000",
                                    "netmask" : "$subnet_mask",
                                    "status" : "Up",
                                    "virtualNetworkTag" : "$vlan_id"
                                    }
                            },
                "cluster": {
                          "name": "$mnode_host_name",
                          "cipi": "$eth1.$vlan_id",
                          "sipi": "$eth1.$vlan_id"
                          }
              },
    "method": "SetConfig"
}
'
```

Ulteriori informazioni

- "Aggiungere una risorsa controller al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Ripristinare un nodo di gestione

È possibile ripristinare e ridistribuire manualmente il nodo di gestione per il cluster che esegue il software NetApp Element se il nodo di gestione precedente utilizzava volumi persistenti.

È possibile implementare un nuovo OVA ed eseguire uno script di ridistribuzione per estrarre i dati di configurazione da un nodo di gestione precedentemente installato che esegue la versione 11.3 e successive.

Di cosa hai bisogno

- Il nodo di gestione precedente eseguiva il software NetApp Element versione 11.3 o successiva con "Volumi persistenti" funzionalità attivata.
- Conosci MVIP e SVIP del cluster contenente i volumi persistenti.
- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- L'installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.
- Hai il permesso di scaricare il software dal NetApp Support Site.
- Hai identificato il tipo di immagine del nodo di gestione corretto per la tua piattaforma:

Piattaforma	Tipo di immagine di installazione
Microsoft Hyper-V.	iso
KVM	iso
VMware vSphere	iso, .ova
Citrix XenServer	iso
OpenStack	iso

Fasi

1. Scarica ISO o OVA e implementa la macchina virtuale
2. Configurare la rete
3. Configurare la sincronizzazione dell'ora
4. Configurare il nodo di gestione

Scarica ISO o OVA e implementa la macchina virtuale

1. Scaricare l'OVA o l'ISO per l'installazione dal "Software Element" Sul sito di supporto NetApp.
   a. Selezionare **Download Latest Release** (Scarica ultima versione) e accettare il contratto EULA.
   b. Selezionare l'immagine del nodo di gestione che si desidera scaricare.
2. Se l'OVA è stato scaricato, attenersi alla seguente procedura:
   a. Implementare OVA.
   b. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla VM sulla subnet di storage (ad esempio eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di storage.
3. Se è stato scaricato l'ISO, attenersi alla seguente procedura:
   a. Creare una nuova macchina virtuale a 64 bit dall'hypervisor con la seguente configurazione:
      - Sei CPU virtuali
      - 24 GB DI RAM
      - Disco virtuale da 400 GB, con thin provisioning

- Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
- (Opzionale per lo storage all-flash SolidFire) un'interfaccia di rete virtuale con accesso alla rete di gestione al cluster di storage. Se il cluster di storage si trova su una subnet separata dal nodo di gestione (eth0) e si desidera utilizzare volumi persistenti, aggiungere un secondo controller di interfaccia di rete (NIC) alla macchina virtuale sulla subnet di storage (eth1) o assicurarsi che la rete di gestione possa essere instradata alla rete di storage.

Non accendere la macchina virtuale prima della fase indicata in questa procedura.

b. Collegare l'ISO alla macchina virtuale e avviare l'immagine di installazione .iso.

L'installazione di un nodo di gestione mediante l'immagine potrebbe causare un ritardo di 30 secondi prima della visualizzazione della schermata iniziale.

4. Al termine dell'installazione, accendere la macchina virtuale per il nodo di gestione.

Configurare la rete

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente admin del nodo di gestione.

Per spostarsi tra le opzioni di menu, premere i tasti freccia su o giù. Per spostarsi tra i pulsanti, premere Tab. Per spostarsi dai pulsanti ai campi, premere Tab. Per spostarsi tra i campi, premere i tasti freccia su o giù.

2. Configurare la rete dei nodi di gestione (eth0).

Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di storage, consultare le istruzioni per la configurazione di un'altra scheda di rete: "Configurazione di un NIC (Network Interface Controller) per lo storage".

Configurare la sincronizzazione dell'ora

1. Assicurarsi che il tempo sia sincronizzato tra il nodo di gestione e il cluster di storage utilizzando NTP:

A partire dall'elemento 12.3.1, i passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1, passare a. sottopase (f) per completare la configurazione di time sync.

1. Accedere al nodo di gestione utilizzando SSH o la console fornita dall'hypervisor.
2. Stop NTPD:

```
sudo service ntpd stop
```

3. Modificare il file di configurazione NTP `/etc/ntp.conf`:
   a. Commentare i server predefiniti (`server 0.gentoo.pool.ntp.org`) aggiungendo un `#` davanti a ciascuno.
   b. Aggiungere una nuova riga per ciascun server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati nel cluster di storage in "passo successivo".

```
vi /etc/ntp.conf

#server 0.gentoo.pool.ntp.org
#server 1.gentoo.pool.ntp.org
#server 2.gentoo.pool.ntp.org
#server 3.gentoo.pool.ntp.org
server <insert the hostname or IP address of the default time server>
```

c. Al termine, salvare il file di configurazione.

4. Forzare una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

5. Riavviare NTPD.

```
sudo service ntpd start
```

6. Disattiva la sincronizzazione dell'ora con l'host tramite l'hypervisor (il seguente è un esempio VMware):

> Se si implementa mNode in un ambiente hypervisor diverso da VMware, ad esempio dall'immagine .iso in un ambiente OpenStack, fare riferimento alla documentazione dell'hypervisor per i comandi equivalenti.

a. Disattivare la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

b. Visualizzare e confermare lo stato corrente del servizio:

```
vmware-toolbox-cmd timesync status
```

c. In vSphere, verificare che `Synchronize guest time with host` Nelle opzioni della macchina virtuale, la casella di controllo non è selezionata.

> Non attivare questa opzione se si apportano modifiche future alla macchina virtuale.

> Non modificare l'NTP dopo aver completato la configurazione di Time Sync, in quanto influisce sull'NTP quando si esegue comando di ridistribuzione sul nodo di gestione.

Configurare il nodo di gestione

1. Creare una directory di destinazione temporanea per il contenuto del bundle di servizi di gestione:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Scaricare il bundle di servizi di gestione (versione 2.15.28 o successiva) precedentemente installato sul nodo di gestione esistente e salvarlo in `/sf/etc/mnode/` directory.
3. Estrarre il bundle scaricato utilizzando il seguente comando, sostituendo il valore tra parentesi quadre [ ] (comprese le parentesi quadre) con il nome del file bundle:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle
file]
```

4. Estrarre il file risultante in `/sf/etc/mnode-archive` directory:

```
tar -C /sf/etc/mnode/mnode-archive -xvf
/sf/etc/mnode/services_deploy_bundle.tar.gz
```

5. Creare un file di configurazione per account e volumi:

```
echo '{"trident": true, "mvip": "[mvip IP address]", "account_name":
"[persistent volume account name]"}' | sudo tee /sf/etc/mnode/mnode-
archive/management-services-metadata.json
```

   a. Sostituire il valore tra parentesi [ ] (comprese le parentesi) per ciascuno dei seguenti parametri richiesti:
      - **[mvip IP address]**: L'indirizzo IP virtuale di gestione del cluster di storage. Configurare il nodo di gestione con lo stesso cluster di storage utilizzato durante "Configurazione dei server NTP".
      - **[nome account volume persistente]**: Il nome dell'account associato a tutti i volumi persistenti in questo cluster di storage.

6. Configurare ed eseguire il comando di ridistribuzione del nodo di gestione per connettersi ai volumi persistenti ospitati sul cluster e avviare i servizi con i dati di configurazione del nodo di gestione precedenti:

   Viene richiesto di inserire le password in un prompt sicuro. Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

   a. Sostituire il valore tra parentesi quadre [ ] (comprese le parentesi quadre) con il nome utente dell'account amministratore del nodo di gestione. Probabilmente si tratta del nome utente dell'account utente utilizzato per accedere al nodo di gestione.

È possibile aggiungere il nome utente o consentire allo script di richiedere le informazioni.

b. Eseguire `redeploy-mnode` comando. Al termine della ridistribuzione, lo script visualizza un messaggio di esito positivo.

c. Se si accede alle interfacce web Element (come il nodo di gestione o NetApp Hybrid Cloud Control) utilizzando il FQDN (Fully Qualified Domain Name) del sistema, "riconfigurare l'autenticazione per il nodo di gestione".

Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione ripristinato.

Ulteriori informazioni

- "Volumi persistenti"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Accedere al nodo di gestione

A partire dal software NetApp Element versione 11.3, il nodo di gestione contiene due UI: Un'interfaccia utente per la gestione dei servizi basati SU REST e un'interfaccia utente per nodo per la gestione delle impostazioni di rete e cluster, nonché test e utility del sistema operativo.

Per i cluster che eseguono Element Software versione 11.3 o successiva, è possibile utilizzare una delle due interfacce seguenti:

- Utilizzando l'interfaccia utente del nodo di gestione (`https:// [mNode IP}:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.
- Utilizzando l'interfaccia utente REST API integrata (`https://[mNode IP}/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

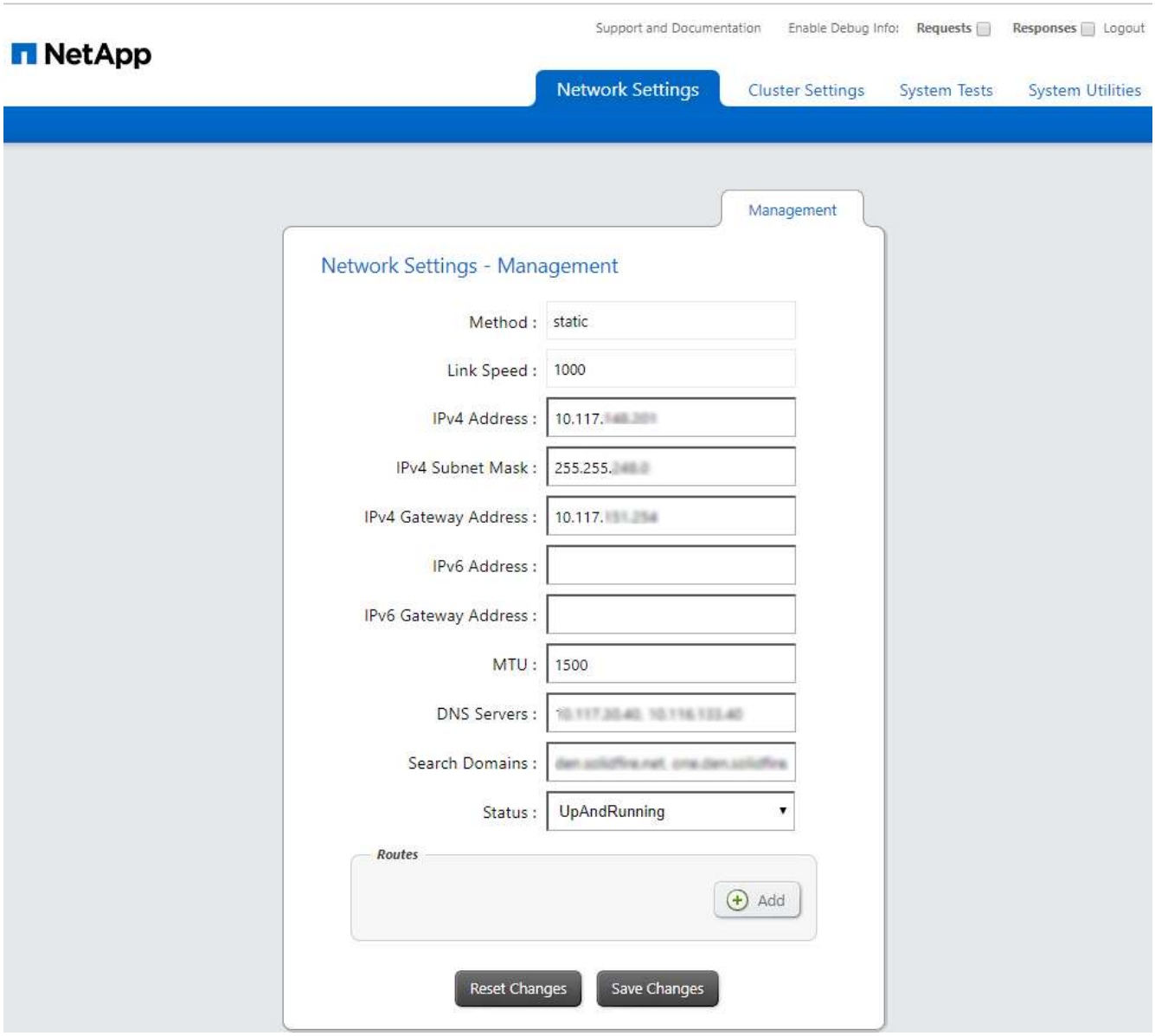
Accedere all'interfaccia utente del nodo di gestione per nodo

Dall'interfaccia utente per nodo, è possibile accedere alle impostazioni di rete e cluster e utilizzare le utility e i test di sistema.

Fasi

1. Accedere all'interfaccia utente per nodo per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da :442

```
https://[IP address]:442
```



2. Inserire il nome utente e la password del nodo di gestione quando richiesto.

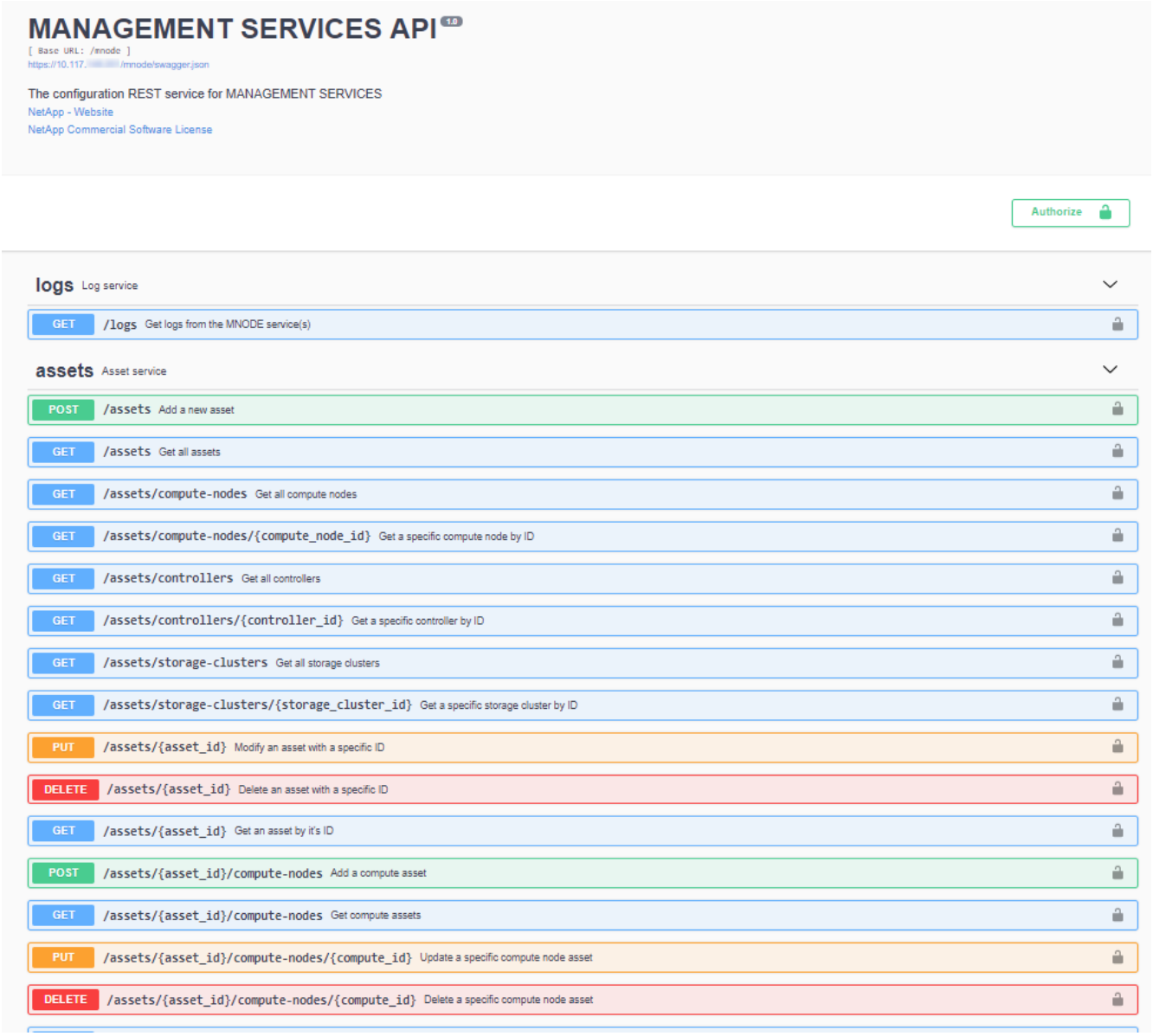
Accedere all'interfaccia utente REST API del nodo di gestione

Dall'interfaccia utente dell'API REST, è possibile accedere a un menu di API correlate al servizio che controllano i servizi di gestione sul nodo di gestione.

Fasi

1. Per accedere all'interfaccia utente API REST per i servizi di gestione, immettere l'indirizzo IP del nodo di gestione seguito da `/mnode`:

```
https://[IP address]/mnode
```



2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per le autorizzazioni per l'utilizzo delle API.

Ulteriori informazioni

- "Abilita il monitoraggio Active IQ e NetApp"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Utilizzare l'interfaccia utente del nodo di gestione

Panoramica dell'interfaccia utente del nodo di gestione

Con l'interfaccia utente del nodo di gestione (`https://<ManagementNodeIP>:442`), è possibile apportare modifiche alle impostazioni di rete e del cluster, eseguire test di sistema o utilizzare le utility di sistema.

Attività che è possibile eseguire con l'interfaccia utente del nodo di gestione:

- "Configurare il monitoraggio degli avvisi"
- "Modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione"
- "Eseguire le utility di sistema dal nodo di gestione"

Trova ulteriori informazioni

- "Accedere al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Configurare il monitoraggio degli avvisi

Gli strumenti di monitoraggio degli avvisi sono configurati per il monitoraggio degli avvisi NetApp HCI. Questi strumenti non sono configurati o utilizzati per lo storage all-flash SolidFire. L'esecuzione degli strumenti per questi cluster comporta il seguente errore 405, che è previsto in base alla configurazione: `webUIParseError : Invalid response from server. 405`

Per ulteriori informazioni sulla configurazione del monitoraggio degli avvisi per NetApp HCI, vedere "Configurare il monitoraggio degli avvisi"

Modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione

È possibile modificare e verificare le impostazioni di rete, cluster e sistema del nodo di gestione.

- Aggiornare le impostazioni di rete del nodo di gestione
- Aggiornare le impostazioni del cluster del nodo di gestione
- Verificare le impostazioni del nodo di gestione

Aggiornare le impostazioni di rete del nodo di gestione

Nella scheda Network Settings (Impostazioni di rete) dell'interfaccia utente del nodo di gestione per nodo, è possibile modificare i campi dell'interfaccia di rete del nodo di gestione.

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Selezionare la scheda **Impostazioni di rete**.
3. Visualizzare o inserire le seguenti informazioni:
   a. **Metodo**: Scegliere uno dei seguenti metodi per configurare l'interfaccia:
      - `loopback`: Consente di definire l'interfaccia di loopback IPv4.
      - `manual`: Consente di definire le interfacce per le quali non viene eseguita alcuna configurazione per impostazione predefinita.
      - `dhop`Consente di ottenere un indirizzo IP tramite DHCP.

- `static`: Consente di definire le interfacce Ethernet con indirizzi IPv4 allocati in modo statico.

b. **Velocità di collegamento**: La velocità negoziata dalla NIC virtuale.

c. **IPv4 Address**: Indirizzo IPv4 per la rete eth0.

d. **IPv4 Subnet Mask**: Suddivisioni di indirizzi della rete IPv4.

e. **IPv4 Gateway Address** (Indirizzo gateway IPv4): Indirizzo di rete del router per l'invio dei pacchetti dalla rete locale.

f. **IPv6 Address**: L'indirizzo IPv6 per la rete eth0.

g. **IPv6 Gateway Address** (Indirizzo gateway IPv6): Indirizzo di rete del router per l'invio dei pacchetti dalla rete locale.

> Le opzioni IPv6 non sono supportate per la versione 11.3 o successive del nodo di gestione.

h. **MTU**: Dimensione massima dei pacchetti che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete per lo storage, il valore deve essere 9000.

i. **Server DNS**: Interfaccia di rete utilizzata per la comunicazione del cluster.

j. **Search Domains** (Cerca domini): Consente di cercare ulteriori indirizzi MAC disponibili per il sistema.

k. **Status**: Valori possibili:

- `UpAndRunning`
- `Down`
- `Up`

l. **Routes**: Route statiche verso host o reti specifici tramite l'interfaccia associata per l'utilizzo da parte dei percorsi.

Aggiornare le impostazioni del cluster del nodo di gestione

Nella scheda Cluster Settings (Impostazioni cluster) dell'interfaccia utente per nodo per il nodo di gestione, è possibile modificare i campi dell'interfaccia cluster quando un nodo si trova negli stati Available (disponibile), PendingActive (PendingActive) e Active (attivo).

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Selezionare la scheda **Cluster Settings** (Impostazioni cluster).
3. Visualizzare o inserire le seguenti informazioni:
   - **Ruolo**: Ruolo del nodo di gestione nel cluster. Valore possibile: `Management`.
   - **Version**: Versione del software Element in esecuzione sul cluster.
   - **Default Interface**: Interfaccia di rete predefinita utilizzata per la comunicazione del nodo di gestione con il cluster che esegue il software Element.

Verificare le impostazioni del nodo di gestione

Dopo aver modificato le impostazioni di gestione e di rete per il nodo di gestione e aver eseguito le modifiche, è possibile eseguire test per convalidare le modifiche apportate.

1. Aprire l'interfaccia utente del nodo di gestione per nodo.

2. Nell'interfaccia utente del nodo di gestione, selezionare **Test di sistema**.
3. Completare una delle seguenti operazioni:
   a. Per verificare che le impostazioni di rete configurate siano valide per il sistema, selezionare **Test Network Config**.
   b. Per verificare la connettività di rete a tutti i nodi del cluster su entrambe le interfacce 1G e 10G utilizzando pacchetti ICMP, selezionare **Test Ping**.
4. Visualizzare o inserire quanto segue:
   - **Hosts**: Specificare un elenco separato da virgole di indirizzi o nomi host dei dispositivi da ping.
   - **Tentativi**: Specificare il numero di volte in cui il sistema deve ripetere il test ping. Predefinito: 5.
   - **Packet Size** (dimensione pacchetto): Specificare il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore al valore MTU massimo specificato nella configurazione di rete.
   - **Timeout msec**: Specificare il numero di millisecondi da attendere per ogni singola risposta ping. Impostazione predefinita: 500 ms.
   - **Total Timeout sec**: Specificare il tempo in secondi in cui il ping deve attendere una risposta di sistema prima di eseguire il successivo tentativo di ping o terminare il processo. Predefinito: 5.
   - **Proibisci frammentazione**: Attiva il flag DF (do not fragment) per i pacchetti ICMP.

Ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Eseguire le utility di sistema dal nodo di gestione

È possibile utilizzare l'interfaccia utente per nodo per il nodo di gestione per creare o eliminare i bundle di supporto del cluster, reimpostare le impostazioni di configurazione del nodo o riavviare la rete.

Fasi

1. Aprire l'interfaccia utente del nodo di gestione per nodo utilizzando le credenziali admin del nodo di gestione.
2. Selezionare **Utilità di sistema**.
3. Selezionare il pulsante dell'utilità che si desidera eseguire:
   a. **Control Power** (alimentazione controllo): Riavvia, spegne e riaccende il nodo. Specificare una delle seguenti opzioni.

      Questa operazione causa la perdita temporanea della connettività di rete.

      - **Azione**: Le opzioni includono `Restart` e. `Halt` (spegnere).
      - **Wakeup Delay** (ritardo di attivazione): Qualsiasi tempo aggiuntivo prima che il nodo torni online.
   b. **Create Cluster Support Bundle**: Crea il bundle di supporto del cluster per assistere le valutazioni diagnostiche del supporto NetApp di uno o più nodi in un cluster. Specificare le seguenti opzioni:
      - **Nome bundle**: Nome univoco per ciascun bundle di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.

- **MVIP**: L'MVIP del cluster. I bundle vengono raccolti da tutti i nodi del cluster. Questo parametro è obbligatorio se il parametro Nodes non è specificato.
- **Nodes**: Gli indirizzi IP dei nodi da cui raccogliere i bundle. Utilizzare nodi o MVIP, ma non entrambi, per specificare i nodi da cui raccogliere i bundle. Questo parametro è obbligatorio se MVIP non è specificato.
- **Username**: Il nome utente dell'amministratore del cluster.
- **Password**: La password di amministrazione del cluster.
- **Allow Incomplete** (Consenti incompleto): Consente di continuare l'esecuzione dello script se non è possibile raccogliere bundle da uno o più nodi.
- **Extra args**: Questo parametro viene inviato a. `sf_make_support_bundle` script. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp.

c. **Delete All Support Bundle** (Elimina tutti i pacchetti di supporto): Elimina tutti i pacchetti di supporto correnti sul nodo di gestione.

d. **Reset Node**: Ripristina il nodo di gestione su una nuova immagine di installazione. In questo modo, tutte le impostazioni, ad eccezione della configurazione di rete, vengono modificate nello stato predefinito. Specificare le seguenti opzioni:
   - **Build**: URL di un'immagine software di elementi remoti in cui il nodo verrà reimpostato.
   - **Opzioni**: Specifiche per l'esecuzione delle operazioni di ripristino. I dettagli sono forniti dal supporto NetApp, se necessario.

   Questa operazione causa la perdita temporanea della connettività di rete.

e. **Restart Networking** (Riavvia rete): Riavvia tutti i servizi di rete sul nodo di gestione.

   Questa operazione causa la perdita temporanea della connettività di rete.

Ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Utilizzare l'API REST del nodo di gestione

Panoramica dell'interfaccia utente REST API del nodo di gestione

Utilizzando l'interfaccia utente REST API integrata (`https://<ManagementNodeIP>/mnode`), è possibile eseguire o comprendere le API relative ai servizi del nodo di gestione, tra cui la configurazione del server proxy, gli aggiornamenti del livello di servizio o la gestione delle risorse.

Attività che è possibile eseguire con le API REST:

Autorizzazione

- "Ottenere l'autorizzazione per utilizzare le API REST"

Configurazione delle risorse

- "Abilita il monitoraggio Active IQ e NetApp"
- "Configurare un server proxy per il nodo di gestione"
- "Configurare NetApp Hybrid Cloud Control per più vCenter"
- "Aggiungere una risorsa controller al nodo di gestione"
- "Creare e gestire le risorse del cluster di storage"

Gestione delle risorse

- "Visualizzare o modificare le risorse dei controller esistenti"
- "Creare e gestire le risorse del cluster di storage"
- "Utilizzare l'API REST per raccogliere i log di sistema degli elementi"
- "Verificare le versioni dei sistemi operativi e dei servizi del nodo di gestione"
- "Recupero dei log dai servizi di gestione"

Trova ulteriori informazioni

- "Accedere al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Ottenere l'autorizzazione per utilizzare le API REST

È necessario autorizzare prima di poter utilizzare le API per i servizi di gestione nell'interfaccia utente REST API. A tale scopo, è necessario ottenere un token di accesso.

Per ottenere un token, fornire le credenziali di amministratore del cluster e un ID client. Ogni token dura circa dieci minuti. Dopo la scadenza di un token, puoi autorizzare di nuovo per un nuovo token di accesso.

La funzionalità di autorizzazione viene impostata durante l'installazione e l'implementazione del nodo di gestione. Il servizio token si basa sul cluster di storage definito durante l'installazione.

Prima di iniziare

- La versione del cluster in uso deve disporre del software NetApp Element 11.3 o versione successiva.
- Si dovrebbe aver implementato un nodo di gestione con versione 11.3 o successiva.

Comando API

```
TOKEN=`curl -k -X POST https://MVIP/auth/connect/token -F client_id=mnode-
client -F grant_type=password -F username=CLUSTER_ADMIN -F
password=CLUSTER_PASSWORD|awk -F':' '{print $2}'|awk -F',' '{print
$1}'|sed s/\"//g`
```

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio immettendo, ad esempio, l'indirizzo IP del nodo di gestione seguito dal nome del servizio `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Selezionare **autorizzare**.

   In alternativa, è possibile selezionare su un'icona a forma di lucchetto accanto a qualsiasi API del servizio.

3. Completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Non inserire un valore per il client secret.
   d. Selezionare **autorizzare** per avviare una sessione.
4. Chiudere la finestra di dialogo **Available Authorisations** (autorizzazioni disponibili).

   Se si tenta di eseguire un comando dopo la scadenza del token, viene visualizzato un `401 Error: UNAUTHORIZED` viene visualizzato il messaggio. Se compare questo, autorizzare di nuovo.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Abilita il monitoraggio Active IQ e NetApp

È possibile attivare il monitoraggio dello storage Active IQ se non è già stato fatto durante l'installazione o l'aggiornamento. Potrebbe essere necessario utilizzare questa procedura se non è stato configurato SolidFire Active IQ durante l'installazione per un sistema di storage all-flash SolidFire.

Il servizio Active IQ Collector inoltra i dati di configurazione e le metriche delle performance del cluster basate su software Element a SolidFire Active IQ per il reporting storico e il monitoraggio delle performance quasi in tempo reale. Il servizio di monitoraggio NetApp consente di inoltrare gli errori del cluster di storage a vCenter per la notifica degli avvisi.

Prima di iniziare

- Alcune funzioni di Active IQ, ad esempio la qualità del servizio (QoS), richiedono l'elemento 11.3 o successivo per funzionare correttamente. Per confermare di disporre della capacità di utilizzare tutte le funzioni di Active IQ, NetApp consiglia quanto segue:
  - Il cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
  - È stato implementato un nodo di gestione con versione 11.3 o successiva.
- Hai accesso a Internet. Il servizio Active IQ Collector non può essere utilizzato da siti oscuri che non

dispongono di connettività esterna.

Fasi

1. Ottenere l'ID risorsa di base per l'installazione:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

      ```
      {
        "installations": [
          {
            "_links": {
              "collection":
      "https://10.111.211.111/inventory/1/installations",
              "self":
      "https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
      91ee-12f111xxc7x0x"
            },
            "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
      ```

      L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

2. Attivare la telemetria:
   a. Accedere all'interfaccia utente API del servizio mnode sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

      ```
      https://<ManagementNodeIP>/mnode
      ```

   b. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.

ii. Immettere l'ID client come `mnode-client`.

iii. Selezionare **autorizzare** per avviare una sessione.

iv. Chiudere la finestra.

c. Configurare la risorsa di base:

i. Selezionare **PUT /assets/{asset_id}**.

ii. Selezionare **Provalo**.

iii. Inserire quanto segue nel payload JSON:

```
{
"telemetry_active": true
"config": {}
}
```

iv. Inserire l'ID di base del passaggio precedente in **asset_ID**.

v. Selezionare **Esegui**.

Il servizio Active IQ viene riavviato automaticamente ogni volta che si modificano le risorse. La modifica delle risorse comporta un breve ritardo prima dell'applicazione delle impostazioni.

3. Se non l'hai già fatto, Aggiungi una risorsa vCenter controller per NetApp Hybrid Cloud Control al nodo di gestione risorse note:

Per i servizi di monitoraggio NetApp è necessaria una risorsa controller.

a. Selezionare **POST /assets/{asset_id}/controller** per aggiungere una sottorisorsa del controller.

b. Selezionare **Provalo**.

c. Inserire l'ID risorsa base principale copiato negli Appunti nel campo **asset_id**.

d. Inserire i valori del payload richiesti con `type` come `vCenter` E vCenter.

```
{
"username": "string",
"password": "string",
"ip": "string",
"type": "vCenter",
"host_name": "string",
"config": {}
}
```

`ip` È l'indirizzo IP di vCenter.

e. Selezionare **Esegui**.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Configurare NetApp Hybrid Cloud Control per più vCenter

È possibile configurare NetApp Hybrid Cloud Control per gestire le risorse di due o più vCenter che non utilizzano Linked Mode.

Questa procedura deve essere utilizzata dopo l'installazione iniziale quando è necessario aggiungere risorse per un'installazione scalata di recente o quando le nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente all'installazione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Fasi

1. "Aggiungere nuovi vCenter come risorse del controller" alla configurazione del nodo di gestione.
2. Aggiornare l'API del servizio di inventario sul nodo di gestione:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

   In alternativa, è possibile attendere 2 minuti per l'aggiornamento dell'inventario nell'interfaccia utente di NetApp Hybrid Cloud Control.

   a. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   b. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   c. Selezionare **Provalo**.
   d. Selezionare **Esegui**.
   e. Dalla risposta, copiare l'ID della risorsa di installazione (`"id"`).
   f. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
   g. Selezionare **Provalo**.
   h. Impostare Refresh su `True`.
   i. Incollare l'ID della risorsa di installazione nel campo **id**.
   j. Selezionare **Esegui**.
3. Aggiorna il browser NetApp Hybrid Cloud Control per vedere le modifiche.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Aggiungere una risorsa controller al nodo di gestione

È possibile aggiungere una risorsa controller alla configurazione del nodo di gestione utilizzando l'interfaccia utente REST API.

Potrebbe essere necessario aggiungere una risorsa se l'installazione è stata scalata di recente e le nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente all'installazione.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.
- Hai creato un nuovo ruolo NetApp HCC in vCenter per limitare la vista dei servizi del nodo di gestione alle risorse solo NetApp. Vedere "Creare un ruolo NetApp HCC in vCenter"

Fasi

1. Ottenere l'ID risorsa di base per l'installazione:
   a. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

```
{
  "installations": [
    {
      "_links": {
        "collection":
"https://10.111.211.111/inventory/1/installations",
        "self":
"https://10.111.217.111/inventory/1/installations/abcd01e2-ab00-1xxx-
91ee-12f111xxc7x0x"
      },
      "id": "abcd01e2-ab00-1xxx-91ee-12f111xxc7x0x",
```

L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
h. Selezionare **Provalo**.
i. Incollare l'ID della risorsa di installazione nel campo **id**.
j. Selezionare **Esegui**.
k. Dalla risposta, copiare e salvare l'ID del controller del cluster (`"controllerId"`) da utilizzare in un passaggio successivo.

2. Per aggiungere una sottorisorsa del controller a una risorsa di base esistente, selezionare:

```
POST /assets/{asset_id}/controllers
```

a. Aprire l'interfaccia utente dell'API REST del servizio mNode sul nodo di gestione:

```
https://<ManagementNodeIP>/mnode
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client`.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra.
c. Selezionare **POST /assets/{asset_id}/controller**.
d. Selezionare **Provalo**.
e. Inserire l'ID risorsa di base principale nel campo **asset_id**.
f. Aggiungere i valori richiesti al payload.
g. Selezionare **Esegui**.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Creare e gestire le risorse del cluster di storage

È possibile aggiungere nuove risorse del cluster di storage al nodo di gestione, modificare le credenziali memorizzate per le risorse del cluster di storage note ed eliminare le risorse del cluster di storage dal nodo di gestione utilizzando l'API REST.

Di cosa hai bisogno

- Assicurarsi che la versione del cluster di storage in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni di gestione delle risorse del cluster di storage

Scegliere una delle seguenti opzioni:

- Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage
- Aggiungere una nuova risorsa di cluster di storage
- Modificare le credenziali memorizzate per una risorsa del cluster di storage
- Eliminare una risorsa del cluster di storage

Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage

È possibile utilizzare L'API REST per ottenere l'ID di installazione e l'ID del cluster di storage. Per aggiungere una nuova risorsa del cluster di storage è necessario l'ID dell'installazione e l'ID del cluster per modificare o eliminare una risorsa specifica del cluster di storage.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di inventario immettendo l'indirizzo IP del nodo di gestione seguito da `/inventory/1/`:

   ```
   https://<ManagementNodeIP>/inventory/1/
   ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **GET /Installations**.
4. Selezionare **Provalo**.
5. Selezionare **Esegui**.

   L'API restituisce un elenco di tutte le installazioni note.

6. Dal corpo di risposta del codice 200, salvare il valore in `id` che si trova nell'elenco delle installazioni. Questo è l'ID dell'installazione. Ad esempio:

```
"installations": [
    {
      "id": "1234a678-12ab-35dc-7b4a-1234a5b6a7ba",
      "name": "my-sf-installation",
      "_links": {
        "collection": "https://localhost/inventory/1/installations",
        "self": "https://localhost/inventory/1/installations/1234a678-
12ab-35dc-7b4a-1234a5b6a7ba"
      }
    }
  ]
```

7. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
9. Selezionare **GET /cluster**.
10. Selezionare **Provalo**.
11. Inserire l'ID di installazione salvato in precedenza in `installationId` parametro.
12. Selezionare **Esegui**.

    L'API restituisce un elenco di tutti i cluster di storage noti in questa installazione.

13. Dal corpo di risposta del codice 200, individuare il cluster di storage corretto e salvare il valore nel cluster `storageId` campo. Questo è l'ID del cluster di storage.

Aggiungere una nuova risorsa di cluster di storage

È possibile utilizzare l'API REST per aggiungere una o più nuove risorse del cluster di storage all'inventario dei nodi di gestione. Quando si aggiunge una nuova risorsa del cluster di storage, questa viene automaticamente registrata con il nodo di gestione.

Di cosa hai bisogno

- È stata copiata la ID cluster storage e ID installazione per qualsiasi cluster di storage che si desidera aggiungere.

- Se si aggiungono più nodi di storage, sono state lette e comprese le limitazioni di "Cluster autorevole" e supporto di più cluster di storage.

> Tutti gli utenti definiti nel cluster autorevole sono definiti come utenti su tutti gli altri cluster legati all'istanza di NetApp Hybrid Cloud Control.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **POST /cluster**.
4. Selezionare **Provalo**.
5. Inserire le informazioni del nuovo cluster di storage nei seguenti parametri nel campo **Request Body** (corpo richiesta):

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Parametro	Tipo	Descrizione
`installationId`	stringa	L'installazione in cui aggiungere il nuovo cluster di storage. Inserire l'ID di installazione salvato in precedenza in questo parametro.
`mvip`	stringa	L'indirizzo IP virtuale di gestione IPv4 (MVIP) del cluster di storage.
`password`	stringa	La password utilizzata per comunicare con il cluster di storage.

Parametro	Tipo	Descrizione
`userId`	stringa	L'ID utente utilizzato per comunicare con il cluster di storage (l'utente deve disporre dei privilegi di amministratore).

6. Selezionare **Esegui**.

   L'API restituisce un oggetto contenente informazioni sulla risorsa del cluster di storage appena aggiunta, ad esempio il nome, la versione e l'indirizzo IP.

Modificare le credenziali memorizzate per una risorsa del cluster di storage

È possibile modificare le credenziali memorizzate che il nodo di gestione utilizza per accedere a un cluster di storage. L'utente scelto deve disporre dell'accesso di amministratore del cluster.

> Assicurarsi di aver seguito i passaggi descritti in Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage prima di continuare.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

   ```
   https://<ManagementNodeIP>/storage/1/
   ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **PUT /cluster/{storageId}**.
4. Selezionare **Provalo**.
5. Incollare l'ID del cluster di storage precedentemente copiato in `storageId` parametro.
6. Modificare uno o entrambi i seguenti parametri nel campo **corpo della richiesta**:

   ```
   {
     "password": "adminadmin",
     "userId": "admin"
   }
   ```

Parametro	Tipo	Descrizione
`password`	stringa	La password utilizzata per comunicare con il cluster di storage.
`userId`	stringa	L'ID utente utilizzato per comunicare con il cluster di storage (l'utente deve disporre dei privilegi di amministratore).

7. Selezionare **Esegui**.

Eliminare una risorsa del cluster di storage

Se il cluster di storage non è più in servizio, è possibile eliminare una risorsa del cluster di storage. Quando si rimuove una risorsa del cluster di storage, questa viene automaticamente annullata dalla registrazione dal nodo di gestione.

Assicurarsi di aver seguito i passaggi descritti in Recuperare l'ID di installazione e l'ID del cluster di una risorsa del cluster di storage prima di continuare.

Fasi

1. Accedere all'interfaccia utente API REST per il servizio di storage immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **DELETE /cluster/{storageId}**.
4. Selezionare **Provalo**.
5. Inserire l'ID del cluster di storage copiato in precedenza in `storageId` parametro.
6. Selezionare **Esegui**.

   All'esito positivo, l'API restituisce una risposta vuota.

Trova ulteriori informazioni

- "Cluster autorevole"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Visualizzare o modificare le risorse dei controller esistenti

È possibile visualizzare informazioni sui controller VMware vCenter esistenti e modificarli nella configurazione del nodo di gestione utilizzando l'API REST. I controller sono istanze di VMware vCenter registrate nel nodo di gestione per l'installazione di NetApp SolidFire.

Prima di iniziare

- Assicurarsi che la versione del cluster in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.

Accedere all'API REST dei servizi di gestione

Fasi

1. Accedere all'interfaccia utente API REST per i servizi di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/vcenter/1/`:

   ```
   https://<ManagementNodeIP>/vcenter/1/
   ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.

Visualizzare le informazioni memorizzate sui controller esistenti

È possibile elencare i controller vCenter esistenti registrati con il nodo di gestione e visualizzare le informazioni memorizzate utilizzando l'API REST.

Fasi

1. Selezionare **GET /compute/controller**.
2. Selezionare **Provalo**.
3. Selezionare **Esegui**.

   L'API restituisce un elenco di tutti i controller vCenter conosciuti, insieme all'indirizzo IP, all'ID del controller, al nome host e all'ID utente utilizzati per comunicare con ciascun controller.

4. Se si desidera lo stato di connessione di un controller specifico, copiare l'ID del controller da `id` del controller negli appunti e vedere Visualizzare lo stato di un controller esistente.

Visualizzare lo stato di un controller esistente

È possibile visualizzare lo stato di uno dei controller vCenter esistenti registrati con il nodo di gestione. L'API restituisce uno stato che indica se NetApp Hybrid Cloud Control è in grado di connettersi al controller vCenter e il motivo di tale stato.

Fasi

1. Selezionare **GET /compute/controller/{controller_id}/status**.
2. Selezionare **Provalo**.
3. Inserire l'ID controller copiato in precedenza in `controller_id` parametro.
4. Selezionare **Esegui**.

   L'API restituisce uno stato di questo particolare controller vCenter, insieme a un motivo per tale stato.

Modificare le proprietà memorizzate di un controller

È possibile modificare il nome utente o la password memorizzati per qualsiasi controller vCenter esistente registrato con il nodo di gestione. Non è possibile modificare l'indirizzo IP memorizzato di un controller vCenter esistente.

Fasi

1. Selezionare **PUT /compute/controller/{controller_id}**.
2. Inserire l'ID del controller di un controller vCenter in `controller_id` parametro.
3. Selezionare **Provalo**.
4. Modificare uno dei seguenti parametri nel campo **corpo della richiesta**:

Parametro	Tipo	Descrizione
`userId`	stringa	Modificare l'ID utente utilizzato per comunicare con il controller vCenter (l'utente deve disporre dei privilegi di amministratore).
`password`	stringa	Modificare la password utilizzata per comunicare con il controller vCenter.

5. Selezionare **Esegui**.

   L'API restituisce informazioni aggiornate sul controller.

Trova ulteriori informazioni

- "Aggiungere una risorsa controller al nodo di gestione"
- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Configurare un server proxy

Se il cluster si trova dietro un server proxy, è necessario configurare le impostazioni del proxy in modo da poter accedere a una rete pubblica.

Un server proxy viene utilizzato per i servizi di raccolta di telemetria e le connessioni di reverse tunnel. È possibile attivare e configurare un server proxy utilizzando l'interfaccia utente API REST se non è già stato configurato un server proxy durante l'installazione o l'aggiornamento. È inoltre possibile modificare le impostazioni del server proxy esistente o disattivare un server proxy.

Il comando per configurare un server proxy viene aggiornato e restituisce le impostazioni proxy correnti per il nodo di gestione. Le impostazioni proxy vengono utilizzate da Active IQ, dal servizio di monitoraggio NetApp e da altre utility software Element installate nel nodo di gestione, incluso il tunnel di supporto inverso per il supporto NetApp.

Prima di iniziare

- È necessario conoscere le informazioni relative all'host e alle credenziali per il server proxy che si sta configurando.
- Assicurarsi che la versione del cluster in uso utilizzi il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver implementato un nodo di gestione con versione 11.3 o successiva.
- (Nodo di gestione 12.0 e versioni successive) hai aggiornato NetApp Hybrid Cloud Control alla versione 2.16 dei servizi di gestione prima di configurare un server proxy.

Fasi

1. Accedere all'interfaccia utente API REST sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode`:

   ```
   https://<ManagementNodeIP>/mnode
   ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **PUT /settings**.
4. Selezionare **Provalo**.
5. Per attivare un server proxy, è necessario impostare `use_proxy` a vero. Immettere l'IP o il nome host e le destinazioni della porta proxy.

   Il nome utente del proxy, la password del proxy e la porta SSH sono opzionali e devono essere omessi se non utilizzati.

   ```
   {
   "proxy_ip_or_hostname": "[IP or name]",
   "use_proxy": [true/false],
   "proxy_username": "[username]",
   "proxy_password": "[password]",
   "proxy_port": [port value],
   "proxy_ssh_port": [port value: default is 443]
   }
   ```

6. Selezionare **Esegui**.

Potrebbe essere necessario riavviare il nodo di gestione a seconda dell'ambiente in uso.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Verificare le versioni dei sistemi operativi e dei servizi del nodo di gestione

È possibile verificare i numeri di versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e dei singoli servizi in esecuzione sul nodo di gestione utilizzando l'API REST nel nodo di gestione.

Di cosa hai bisogno

- Nel cluster è in esecuzione il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Opzioni

- Comandi API
- FASI DELL'INTERFACCIA UTENTE API REST

Comandi API

- Ottenere informazioni sulla versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e del servizio API del nodo di gestione (mnode-api) in esecuzione sul nodo di gestione:

```
curl -X GET "https://<ManagementNodeIP>/mnode/about" -H  "accept:
application/json"
```

- Ottenere informazioni sulla versione dei singoli servizi in esecuzione sul nodo di gestione:

```
curl -X GET "https://<ManagementNodeIP>/mnode/services?status=running"
-H  "accept: */*" -H  "Authorization: ${TOKEN}"
```

Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

```
https://<ManagementNodeIP>/mnode/
```

2. Effettuare una delle seguenti operazioni:
   - Ottenere informazioni sulla versione del sistema operativo del nodo di gestione, del bundle di servizi di gestione e del servizio API del nodo di gestione (mnode-api) in esecuzione sul nodo di gestione:
     i. Selezionare **GET /About**.
     ii. Selezionare **Provalo**.
     iii. Selezionare **Esegui**.

     La versione del bundle dei servizi di gestione (`"mnode_bundle_version"`), versione del sistema operativo del nodo di gestione (`"os_version"`) E la versione API del nodo di gestione (`"version"`) sono indicati nel corpo di risposta.
   - Ottenere informazioni sulla versione dei singoli servizi in esecuzione sul nodo di gestione:
     i. Selezionare **GET /Services**.
     ii. Selezionare **Provalo**.
     iii. Selezionare lo stato **in esecuzione**.
     iv. Selezionare **Esegui**.

     I servizi in esecuzione sul nodo di gestione sono indicati nel corpo della risposta.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Recupero dei log dai servizi di gestione

È possibile recuperare i log dai servizi in esecuzione sul nodo di gestione utilizzando l'API REST. È possibile estrarre i log da tutti i servizi pubblici o specificare servizi specifici e utilizzare i parametri di query per definire meglio i risultati restituiti.

Di cosa hai bisogno

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- È stato implementato un nodo di gestione con versione 11.3 o successiva.

Fasi

1. Aprire l'interfaccia utente API REST sul nodo di gestione.
   - A partire dai servizi di gestione 2.21.61:

     ```
     https://<ManagementNodeIP>/mnode/4/
     ```

   - Per i servizi di gestione 2.20.69 o precedenti:

     ```
     https://<ManagementNodeIP>/mnode
     ```

2. Selezionare **autorizzare** o qualsiasi icona a forma di lucchetto e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Inserire l'ID client come mnode-client se il valore non è già stato compilato.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Selezionare **GET /logs**.
4. Selezionare **Provalo**.
5. Specificare i seguenti parametri:
   - `Lines`: Inserire il numero di righe che si desidera restituire al registro. Questo parametro è un numero intero che per impostazione predefinita è 1000.

     Evitare di richiedere l'intera cronologia del contenuto del registro impostando le righe su 0.

   - `since`: Aggiunge un timestamp ISO-8601 per il punto di inizio dei registri del servizio.

     Utilizzare un ragionevole `since` parametro durante la raccolta di log di intervalli di tempo più ampi.

   - `service-name`: Inserire un nome di servizio.

     Utilizzare `GET /services` comando per elencare i servizi sul nodo di gestione.

   - `stopped`: Impostare su `true` per recuperare i log dai servizi interrotti.
6. Selezionare **Esegui**.
7. Dal corpo della risposta, selezionare **Download** per salvare l'output del log.

Ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Gestire le connessioni di supporto

Avviare una sessione remota di NetApp Support

Se hai bisogno di supporto tecnico per il tuo sistema storage all-flash SolidFire, il supporto NetApp può connetterti in remoto con il tuo sistema. Per avviare una sessione e ottenere l'accesso remoto, il supporto NetApp può aprire una connessione Secure Shell (SSH) inversa al proprio ambiente.

Con il supporto NetApp è possibile aprire una porta TCP per una connessione a tunnel inverso SSH. Questa connessione consente al supporto NetApp di accedere al nodo di gestione.

Prima di iniziare

- Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disattivata per impostazione predefinita nel nodo di gestione. Per attivare la funzionalità di accesso remoto, vedere "Gestire la funzionalità SSH sul nodo di gestione".
- Se il nodo di gestione si trova dietro un server proxy, nel file sshd.config sono necessarie le seguenti porte TCP:

Porta TCP	Descrizione	Direzione di connessione
443	Chiamate API/HTTPS per l'inoltro inverso delle porte all'interfaccia utente Web tramite tunnel di supporto aperto	Nodo di gestione ai nodi di storage
22	Accesso SSH	Nodo di gestione per nodi di storage o da nodi di storage a nodi di gestione

Fasi

- Accedere al nodo di gestione e aprire una sessione terminale.
- Quando richiesto, immettere quanto segue:

```
rst -r sfsupport.solidfire.com -u element -p <port_number>
```

- Per chiudere il tunnel di supporto remoto, immettere quanto segue:

```
rst --killall
```

- (Facoltativo) Disattiva "funzionalità di accesso remoto" di nuovo.

> SSH rimane attivato sul nodo di gestione se non viene disattivato. La configurazione abilitata SSH persiste sul nodo di gestione tramite aggiornamenti e aggiornamenti fino a quando non viene disattivata manualmente.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Gestire la funzionalità SSH sul nodo di gestione

È possibile disattivare, riattivare o determinare lo stato della funzionalità SSH sul nodo di gestione (mNode) utilizzando l'API REST. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive.

A partire da Management Services 2.20.69, è possibile attivare e disattivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

Di cosa hai bisogno

- **NetApp Hybrid Cloud Control Permissions**: Hai le autorizzazioni di amministratore.
- **Cluster Administrator permissions** (autorizzazioni amministratore cluster): Si dispone delle autorizzazioni di amministratore per il cluster di storage.
- **Software Element**: Il cluster esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione**: È stato implementato un nodo di gestione con versione 11.3 o successiva.
- **Aggiornamenti dei servizi di gestione**:
  - Per utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control, è stato aggiornato il "bundle di servizi di gestione" alla versione 2.20.69 o successiva.
  - Per utilizzare l'interfaccia utente API REST, è stato aggiornato il "bundle di servizi di gestione" alla versione 2.17.

Opzioni

- Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control

Dopo di che, è possibile eseguire una delle seguenti attività "autenticare":

- Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API
- Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile farlo utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control.

> Per attivare o disattivare l'accesso al supporto utilizzando SSH per un cluster di storage, è necessario utilizzare "Pagina delle impostazioni del cluster dell'interfaccia utente Element".

Fasi

1. Dalla dashboard, selezionare il menu delle opzioni in alto a destra e selezionare **Configura**.
2. Nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), attivare lo switch per attivare il nodo di gestione SSH.
3. Una volta completata la risoluzione dei problemi, nella schermata **Support Access for Management Node** (accesso supporto per nodo di gestione), impostare lo switch su Disable Management Node SSH (Disattiva SSH nodo di gestione).

Disattivare o attivare la funzionalità SSH sul nodo di gestione utilizzando le API

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disattivazione di SSH non interrompe o disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disattiva SSH e si sceglie di riattivarlo in un secondo momento, è possibile utilizzare la stessa API.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di arricciamento.

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Dall'interfaccia utente API REST, selezionare **PUT /settings/ssh**.
   a. Selezionare **Provalo**.
   b. Impostare il parametro **enabled** su `false` Per disattivare SSH o. `true` Per riattivare la funzionalità SSH precedentemente disattivata.
   c. Selezionare **Esegui**.

Determinare lo stato della funzionalità SSH sul nodo di gestione utilizzando le API

È possibile determinare se la funzionalità SSH è attivata sul nodo di gestione utilizzando un'API di servizio del nodo di gestione. SSH è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive.

Comando API

Per i servizi di gestione 2.18 o versioni successive:

```
curl -k -X PUT
"https://<<ManagementNodeIP>/mnode/2/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Per i servizi di gestione 2.17 o precedenti:

```
curl -X PUT
"https://<ManagementNodeIP>/mnode/settings/ssh?enabled=<false/true>" -H
"accept: application/json" -H  "Authorization: Bearer ${TOKEN}"
```

Puoi trovare il portatore `${TOKEN}` Utilizzato dal comando API quando si "autorizzare". Il portatore `${TOKEN}` è nella risposta di curl..

FASI DELL'INTERFACCIA UTENTE API REST

1. Accedere all'interfaccia utente API REST per il servizio API del nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/`:

   ```
   https://<ManagementNodeIP>/mnode/
   ```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client`.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Dall'interfaccia utente API REST, selezionare **GET /settings/ssh**.
   a. Selezionare **Provalo**.
   b. Selezionare **Esegui**.

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Aggiorna la versione del tuo sistema storage all-flash NetApp SolidFire Element 12,3.x

Panoramica della sequenza di aggiornamento

Puoi mantenere aggiornato il tuo sistema storage SolidFire Element dopo l'implementazione aggiornando in sequenza tutti i componenti dello storage NetApp.

Questi componenti includono servizi di gestione, HealthTools, NetApp Hybrid Cloud Control, software Element, nodo di gestione e (a seconda dell'installazione) il plug-in Element per vCenter Server.

> A partire dal 2023 novembre, non puoi avviare un aggiornamento dei componenti utilizzando il controllo cloud ibrido di NetApp o l'API REST perché i certificati delle chiavi di firma (privati e pubblici) sono scaduti il 5 novembre 2023. Per risolvere questo problema, seguire la soluzione alternativa descritta nell'articolo della Knowledge base "Impossibile avviare gli aggiornamenti di SolidFire e HCI a causa di un errore di caricamento del pacchetto di aggiornamento".

Il sequenza di aggiornamento del sistema Il contenuto descrive le attività necessarie per completare un aggiornamento del sistema storage all-flash SolidFire. Idealmente, queste procedure vengono eseguite come parte di una sequenza di aggiornamento più ampia e non in maniera isolata. Se è necessario un aggiornamento o un aggiornamento basato su componenti, consultare i prerequisiti della procedura per assicurarsi che vengano risolte ulteriori complessità.

Il "Sequenza di aggiornamento di vSphere" L'inclusione del contenuto di Element Plug-in per vCenter Server descrive le fasi aggiuntive di pre e post-aggiornamento necessarie per reinstallare Element Plug-in per vCenter Server.

Di cosa hai bisogno

- Si sta eseguendo il nodo di gestione 11.3 o versione successiva. Le versioni più recenti del nodo di gestione dispongono di un'architettura modulare che fornisce servizi individuali.

  > Per controllare la versione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso. Se non si dispone di 11.3, vedere "Aggiorna il nodo di gestione".

- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326.

  Gli aggiornamenti che utilizzano NetApp Hybrid Cloud Control non sono disponibili nelle versioni precedenti del service bundle.

- Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.

sequenza di aggiornamento del sistema

Per aggiornare il sistema storage all-flash NetApp SolidFire per Element 12.3.x, è possibile utilizzare la seguente sequenza

Fasi

1. "Servizi di gestione degli aggiornamenti da Hybrid Cloud Control".

   Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione.

   Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

2. "(Opzionale) Aggiorna alla versione più recente di HealthTools".

   L'aggiornamento di HealthTools è necessario solo se il nodo di gestione e il software Element in esecuzione sono 11.1 o precedenti. HealthTools non è necessario per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control.

3. "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
4. "Aggiorna il software Element e il firmware dello storage".
5. "(Opzionale) aggiornare solo il firmware dello storage Element".

   È possibile eseguire questa operazione quando un nuovo aggiornamento del firmware dello storage diventa disponibile al di fuori di una release principale.

6. "(Facoltativo) Aggiorna il nodo di gestione".

   L'aggiornamento del sistema operativo del nodo di gestione non è più necessario per aggiornare il software Element sul cluster di storage. Se il nodo di gestione è la versione 11.3 o superiore, è sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control. Se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio la risoluzione dei problemi di protezione, seguire la procedura di aggiornamento del nodo di gestione per lo scenario in uso.

7. "Aggiorna il plug-in Element per vCenter Server".

Trova ulteriori informazioni

- "Plug-in NetApp Element per server vCenter"
- "Documentazione software SolidFire ed Element"

Procedure di aggiornamento del sistema

Servizi di gestione degli aggiornamenti

È possibile aggiornare i servizi di gestione alla versione più recente del bundle dopo aver installato il nodo di gestione 11.3 o successivo.

A partire dalla release del nodo di gestione Element 11.3, la progettazione del nodo di gestione è stata modificata in base a una nuova architettura modulare che fornisce servizi individuali. Questi servizi modulari offrono funzionalità di gestione centrale ed estesa per un sistema storage all-flash SolidFire. I servizi di

gestione includono servizi di telemetria, registrazione e aggiornamento del sistema, il servizio QoSSIOC per Element Plug-in per vCenter Server, NetApp Hybrid Cloud Control e molto altro ancora.

A proposito di questa attività

- Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

> - Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. "Scopri di più".
> - Per le ultime note di rilascio dei servizi di gestione che descrivono i principali servizi, le nuove funzionalità, le correzioni dei bug e le soluzioni alternative per ciascun bundle di servizi, vedere "note di rilascio dei servizi di gestione"

Di cosa hai bisogno

A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare il Contratto di licenza con l'utente finale (EULA) prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare i servizi di gestione:

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di aggiornamento

Puoi aggiornare i servizi di gestione utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control o l'API REST del nodo di gestione:

- Servizi di gestione degli aggiornamenti con Hybrid Cloud Control (Metodo consigliato)
- Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione

Servizi di gestione degli aggiornamenti con Hybrid Cloud Control

Puoi aggiornare i tuoi servizi di gestione NetApp utilizzando NetApp Hybrid Cloud Control.

I bundle di servizi di gestione offrono funzionalità e correzioni avanzate per l'installazione al di fuori delle release principali.

Prima di iniziare

- Si sta eseguendo il nodo di gestione 11.3 o versione successiva.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
  a. Spegnere la VM del nodo di gestione.

b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.

c. Accendere la VM del nodo di gestione.

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nei pacchetti di servizi precedenti.

Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere "Note sulla versione di Management Services".

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina Upgrades (aggiornamenti), selezionare la scheda **Management Services** (servizi di gestione).
5. Seguire le istruzioni riportate nella pagina per scaricare e salvare un pacchetto di aggiornamento dei servizi di gestione sul computer.
6. Selezionare **Sfoglia** per individuare il pacchetto salvato e caricarlo.

   Dopo aver caricato il pacchetto, l'aggiornamento viene avviato automaticamente.

   Una volta avviato l'aggiornamento, lo stato dell'aggiornamento viene visualizzato in questa pagina. Durante l'aggiornamento, potresti perdere la connessione con NetApp Hybrid Cloud Control e devi effettuare nuovamente l'accesso per visualizzare i risultati dell'aggiornamento.

Aggiornare i servizi di gestione utilizzando l'API del nodo di gestione

Gli utenti dovrebbero idealmente eseguire aggiornamenti dei servizi di gestione da NetApp Hybrid Cloud Control. Tuttavia, è possibile caricare, estrarre e distribuire manualmente un aggiornamento del bundle di servizi per i servizi di gestione nel nodo di gestione utilizzando l'API REST. È possibile eseguire ciascun comando dall'interfaccia utente API REST per il nodo di gestione.

Prima di iniziare

- È stato implementato un nodo di gestione software NetApp Element 11.3 o successivo.
- Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione da 11.3 a 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:

  a. Spegnere la VM del nodo di gestione.

  b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.

  c. Accendere la VM del nodo di gestione.

- La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326. Gli aggiornamenti di NetApp Hybrid

Cloud Control non sono disponibili nei pacchetti di servizi precedenti.

> Per un elenco dei servizi disponibili per ciascuna versione del bundle di servizi, vedere "Note sulla versione di Management Services".

Fasi

1. Aprire l'interfaccia utente API REST sul nodo di gestione: `https://<ManagementNodeIP>/mnode`
2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   c. Selezionare **autorizzare** per avviare una sessione.
   d. Chiudere la finestra.
3. Caricare ed estrarre il bundle di servizi sul nodo di gestione utilizzando questo comando: `PUT /services/upload`
4. Implementare i servizi di gestione sul nodo di gestione: `PUT /services/deploy`
5. Monitorare lo stato dell'aggiornamento: `GET /services/update/status`

   Un aggiornamento riuscito restituisce un risultato simile al seguente esempio:

```
{
"current_version": "2.10.29",
"details": "Updated to version 2.17.52",
"status": "success"
}
```

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Effettua l'aggiornamento alla versione più recente di HealthTools

Prima di iniziare un aggiornamento dello storage Element dalla versione 11.1 o precedente, è necessario aggiornare la suite HealthTools. L'aggiornamento di HealthTools è necessario solo se il nodo di gestione e il software Element in esecuzione sono 11.1 o precedenti. HealthTools non sono richiesti per "Esecuzione di upgrade degli elementi utilizzando NetApp Hybrid Cloud Control".

> Il software Element 12.3.2 è la versione finale a cui è possibile eseguire l'aggiornamento utilizzando NetApp HealthTools. Se si utilizza il software Element 11.3 o versioni successive, è necessario utilizzare NetApp Hybrid Cloud Control per aggiornare il software Element. È possibile aggiornare Element versione 11.1 o precedente utilizzando NetApp HealthTools.

Di cosa hai bisogno

- Si sta eseguendo il nodo di gestione 11.0, 11.1 o versione successiva.
- I servizi di gestione sono stati aggiornati almeno alla versione 2.1.326.

  Gli aggiornamenti di NetApp Hybrid Cloud Control non sono disponibili nelle versioni precedenti dei service bundle.

- È stata scaricata l'ultima versione di "HealthTools" e ha copiato il file di installazione nel nodo di gestione.

  È possibile verificare la versione installata localmente di HealthTools eseguendo `sfupdate-healthtools -v` comando.

- Per utilizzare HealthTools con i siti oscuri, è necessario eseguire i seguenti passaggi aggiuntivi:
  - Scaricare un "File JSON" Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
  - Far funzionare il nodo di gestione al sito buio.

A proposito di questa attività

I comandi della suite HealthTools richiedono privilegi di escalation per l'esecuzione. Entrambi i comandi precedano `sudo` oppure eseguire l'escalation dell'utente ai privilegi root.

La versione di HealthTools utilizzata potrebbe essere più aggiornata rispetto all'input e alla risposta di esempio riportati di seguito.

Fasi

1. Eseguire `sfupdate-healthtools <path to install file>` Per installare il nuovo software HealthTools.

   Esempio di input:

   ```
   sfupdate-healthtools /tmp/solidfire-healthtools-2020.03.01.09.tgz
   ```

   Esempio di risposta:

   ```
   Checking key signature for file /tmp/solidfirehealthtools-
   2020.03.01.09/components.tgz
   installing command sfupdate-healthtools
   Restarting on version 2020.03.01.09
   sfupdate-healthtools /sf/bin/sfupdate-healthtools -r 2020.03.01.09
   installing command sfupgradecheck
   installing command sfinstall
   installing command sfresetupgrade
   ```

2. Eseguire `sfupdate-healthtools -v` per verificare che la versione installata sia stata aggiornata.

   Esempio di risposta:

```
Currently installed version of HealthTools:
2020.03.01.09
```

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Prima di aggiornare lo storage Element, è necessario eseguire controlli di integrità per assicurarsi che tutti i nodi di storage nel cluster siano pronti per l'upgrade dello storage Element successivo.

Di cosa hai bisogno

- **Servizi di gestione**: È stato eseguito l'aggiornamento al bundle di servizi di gestione più recente (2.10.27 o versione successiva).

  > Prima di aggiornare il software Element, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente.

- **Nodo di gestione**:si sta eseguendo il nodo di gestione 11.3 o versione successiva.
- **Software Element**: La versione del cluster in uso esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

     ```
     https://<ManagementNodeIP>
     ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di controllo dello stato di salute

È possibile eseguire i controlli dello stato di salute utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control, l'API di NetApp Hybrid Cloud Control o la suite HealthTools:

- Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage (Metodo preferito)
- Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

- Utilizzare HealthTools per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Per ulteriori informazioni sui controlli dello stato dello storage eseguiti dal servizio, consultare:

- Controlli dello stato dello storage eseguiti dal servizio

Utilizza NetApp Hybrid Cloud Control per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

Utilizzando NetApp Hybrid Cloud Control, è possibile verificare che un cluster di storage sia pronto per l'aggiornamento.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare la scheda **Storage**.
5. Selezionare il controllo dello stato di salute per il cluster che si desidera controllare per verificare la disponibilità all'aggiornamento.
6. Nella pagina **Storage Health Check**, selezionare **Run Health Check**.
7. In caso di problemi, procedere come segue:
   a. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.
   b. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
   c. Una volta risolti i problemi del cluster, selezionare **Riesegui controllo stato di salute**.

Una volta completato il controllo dello stato di salute senza errori, il cluster di storage è pronto per l'aggiornamento. Vedere aggiornamento del nodo di storage "istruzioni" per procedere.

Utilizzare l'API per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

È possibile utilizzare REST API per verificare che un cluster di storage sia pronto per l'aggiornamento. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, ad esempio nodi in sospeso, problemi di spazio su disco e guasti del cluster.

Fasi

1. Individuare l'ID del cluster di storage:

   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/mnode
      ```

b. Selezionare **autorizzare** e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra di autorizzazione.
c. Dall'interfaccia utente API REST, selezionare `GET /assets`.
d. Selezionare **Provalo**.
e. Selezionare **Esegui**.
f. Dalla risposta, copiare `"id"` dal `"storage"` sezione del cluster che si intende controllare per verificare la disponibilità all'aggiornamento.

> Non utilizzare `"parent"` Valore in questa sezione perché si tratta dell'ID del nodo di gestione, non dell'ID del cluster di storage.

```
"config": {},
"credentialid": "12bbb2b2-f1be-123b-1234-12c3d4bc123e",
"host_name": "SF_DEMO",
"id": "12cc3a45-e6e7-8d91-a2bb-0bdb3456b789",
"ip": "10.123.12.12",
"parent": "d123ec42-456e-8912-ad3e-4bd56f4a789a",
"sshcredentialid": null,
"ssl_certificate": null
```

2. Eseguire i controlli di integrità sul cluster di storage:
   a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/storage/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Selezionare **POST /Health-checks**.
   d. Selezionare **Provalo**.
   e. Nel campo Parameter (parametro), inserire l'ID del cluster di storage ottenuto nella fase 1.

```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

f. Selezionare **Esegui** per eseguire un controllo dello stato di salute sul cluster di storage specificato.

La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://10.117.149.231/storage/1/health-checks",
    "log": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc/log",
    "self": "https://10.117.149.231/storage/1/health-checks/358f073f-
896e-4751-ab7b-ccbb5f61f9fc"
  },
  "config": {},
  "dateCompleted": null,
  "dateCreated": "2020-02-21T22:11:15.476937+00:00",
  "healthCheckId": "358f073f-896e-4751-ab7b-ccbb5f61f9fc",
  "state": "initializing",
  "status": null,
  "storageId": "c6d124b2-396a-4417-8a47-df10d647f4ab",
  "taskId": "73f4df64-bda5-42c1-9074-b4e7843dbb77"
}
```

a. Copiare il `healthCheckID` ciò fa parte della risposta.

3. Verificare i risultati dei controlli di stato:

a. Selezionare **GET /Health-checks/{healthCheckId}**.

b. Selezionare **Provalo**.

c. Inserire l'ID del controllo di salute nel campo dei parametri.

d. Selezionare **Esegui**.

e. Scorrere fino alla parte inferiore del corpo della risposta.

Se tutti i controlli di integrità hanno esito positivo, il reso è simile al seguente esempio:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Se il `message` la restituzione indica la presenza di problemi relativi allo stato del cluster, procedere come

segue:

a. Selezionare **GET /Health-checks/{healthCheckId}/log**
b. Selezionare **Provalo**.
c. Inserire l'ID del controllo di salute nel campo dei parametri.
d. Selezionare **Esegui**.
e. Esaminare eventuali errori specifici e ottenere i relativi collegamenti agli articoli della Knowledge base.
f. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata.
g. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base.
h. Dopo aver risolto i problemi del cluster, eseguire di nuovo **GET /Health-checks/{healthCheckId}/log**.

Utilizzare HealthTools per eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage

È possibile verificare che il cluster di storage sia pronto per l'aggiornamento utilizzando `sfupgradecheck` comando. Questo comando verifica informazioni quali nodi in sospeso, spazio su disco e guasti del cluster.

Se il nodo di gestione si trova in una sede buia senza connettività esterna, il controllo di preparazione dell'aggiornamento richiede `metadata.json` file scaricato durante "Aggiornamenti di HealthTools" per eseguire correttamente.

A proposito di questa attività

Questa procedura descrive come risolvere i controlli di aggiornamento che producono uno dei seguenti risultati:

- Esecuzione di `sfupgradecheck` il comando viene eseguito correttamente. Il cluster è pronto per l'aggiornamento.
- Controlli all'interno di `sfupgradecheck` errore dello strumento con un messaggio di errore. Il cluster non è pronto per l'aggiornamento e sono necessari ulteriori passaggi.
- Il controllo dell'aggiornamento non riesce e viene visualizzato un messaggio di errore che indica che HealthTools non è aggiornato.
- Il controllo dell'upgrade non riesce perché il nodo di gestione si trova in un sito oscuro.

Fasi

1. Eseguire `sfupgradecheck` comando:

```
sfupgradecheck -u <cluster-user-name> MVIP
```

> Per le password che contengono caratteri speciali, aggiungere una barra rovesciata (`\`) prima di ogni carattere speciale. Ad esempio, `mypass!@1` deve essere inserito come `mypass\!\@`.

Esempio di comando di input con output di esempio in cui non vengono visualizzati errori e si è pronti per l'aggiornamento:

```
sfupgradecheck -u admin 10.117.78.244
```

```
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/
SolidFire-Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnecti
vity
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the
management node
Node ID: 1 Upload speed: 90063.90 KBs/sec
Node ID: 3 Upload speed: 106511.44 KBs/sec
Node ID: 2 Upload speed: 85038.75 KBs/sec
```

2. In caso di errori, sono necessarie ulteriori azioni. Per ulteriori informazioni, consultare le seguenti sottosezioni.

Il cluster non è pronto per l'aggiornamento

Se viene visualizzato un messaggio di errore relativo a uno dei controlli di integrità, attenersi alla seguente procedura:

1. Esaminare `sfupgradecheck` messaggio di errore.

Esempio di risposta:

```
The following tests failed:
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Severity: ERROR
Failed node IDs: 2
Remedy: Remove unneeded files from root drive
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_pending_nodes:
Test Description: Verify no pending nodes in cluster
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltOQAQ/pendingnodes
check_cluster_faults:
Test Description: Report any cluster faults
check_root_disk_space:
Test Description: Verify node root directory has at least 12 GBs of
available disk space
Passed node IDs: 1, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltTQAQ/SolidFire-
Disk-space-error
check_mnode_connectivity:
Test Description: Verify storage nodes can communicate with management
node
Passed node IDs: 1, 2, 3
More information:
https://kb.netapp.com/support/s/article/ka11A0000008ltYQAQ/mNodeconnectivi
ty
check_files:
Test Description: Verify options file exists
Passed node IDs: 1, 2, 3
check_cores:
Test Description: Verify no core or dump files exists
Passed node IDs: 1, 2, 3
check_upload_speed:
Test Description: Measure the upload speed between the storage node and
the management node
Node ID: 1 Upload speed: 86518.82 KBs/sec
Node ID: 3 Upload speed: 84112.79 KBs/sec
Node ID: 2 Upload speed: 93498.94 KBs/sec
```

In questo esempio, il nodo 1 ha poco spazio su disco. Per ulteriori informazioni, consultare "knowledge base" (KB) nel messaggio di errore.

HealthTools non è aggiornato

Se viene visualizzato un messaggio di errore che indica che HealthTools non è la versione più recente, seguire queste istruzioni:

1. Esaminare il messaggio di errore e notare che il controllo dell'aggiornamento non riesce.

   Esempio di risposta:

   ```
   sfupgradecheck failed: HealthTools is out of date:
   installed version: 2018.02.01.200
   latest version: 2020.03.01.09.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/
   Or rerun with the -n option
   ```

2. Seguire le istruzioni descritte nella risposta.

Il nodo di gestione si trova in un sito oscuro

1. Leggere il messaggio e notare che il controllo dell'aggiornamento non riesce:

   Esempio di risposta:

   ```
   sfupgradecheck failed: Unable to verify latest available version of
   healthtools.
   ```

2. Scaricare un "File JSON" Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
3. Eseguire il seguente comando:

   ```
   sfupgradecheck -l --metadata=<path-to-metadata-json>
   ```

4. Per ulteriori informazioni, consultare ulteriori informazioni "Aggiornamenti di HealthTools" informazioni per i siti oscuri.
5. Verificare che la suite HealthTools sia aggiornata eseguendo il seguente comando:

   ```
   sfupgradecheck -u <cluster-user-name> -p <cluster-password> MVIP
   ```

Controlli dello stato dello storage eseguiti dal servizio

I controlli dello stato dello storage effettuano i seguenti controlli per cluster.

Selezionare Nome	Nodo/cluster	Descrizione
check_async_results	Cluster	Verifica che il numero di risultati asincroni nel database sia inferiore a un numero di soglia.
check_cluster_faults	Cluster	Verifica che non vi siano errori del cluster che bloccano l'aggiornamento (come definito nell'origine dell'elemento).
check_upload_speed	Nodo	Misura la velocità di caricamento tra il nodo di storage e il nodo di gestione.
connection_speed_check	Nodo	Verifica che i nodi dispongano di connettività al nodo di gestione che fornisce pacchetti di aggiornamento e stima la velocità di connessione.
check_core	Nodo	Verifica la presenza di un crash dump del kernel e dei file core sul nodo. Il controllo non riesce per eventuali crash in un periodo di tempo recente (soglia 7 giorni).
check_root_disk_space	Nodo	Verifica che il file system root disponga di spazio libero sufficiente per eseguire un aggiornamento.
check_var_log_disk_space	Nodo	Lo verifica `/var/log` lo spazio libero soddisfa una certa soglia percentuale di spazio libero. In caso contrario, il controllo ruota e elimina i registri meno recenti per scendere sotto la soglia. Il controllo non riesce se non riesce a creare spazio libero sufficiente.
check_pending_nodes	Cluster	Verifica che non vi siano nodi in sospeso nel cluster.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiornare il software Element

Per aggiornare il software NetApp Element, è possibile utilizzare l'interfaccia utente per il controllo del cloud ibrido, l'API REST o la suite di tool HealthTools. Alcune operazioni vengono soppresse durante l'aggiornamento di un software Element, ad esempio l'aggiunta e la rimozione di nodi, l'aggiunta e la rimozione di dischi e i comandi associati a iniziatori, gruppi di accesso ai volumi e reti virtuali.

Di cosa hai bisogno

- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **Percorso di aggiornamento valido**: Sono state verificate le informazioni sul percorso di aggiornamento per la versione dell'elemento a cui si sta eseguendo l'aggiornamento e il percorso di aggiornamento è valido.https://kb.netapp.com/Advice_and_Troubleshooting/Data_Storage_Software/Element_Software/What_is_the_upgrade_matrix_for_storage_clusters_running_NetApp_Element_software%3F["KB di NetApp: Matrice di aggiornamento per cluster di storage che eseguono il software NetApp Element"^]
- **System Time Sync**: Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.
- **Nodo di gestione**: Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione**: Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.

> Prima di aggiornare il software Element alla versione 12.3.x, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente Se si sta aggiornando il software Element alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.

- **Cluster Health**: Hai verificato che il cluster è pronto per l'aggiornamento. Vedere "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
- **BMC aggiornato per nodi H610S**: È stata aggiornata la versione BMC per i nodi H610S. Vedere "note di rilascio e istruzioni per l'aggiornamento".
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il software Element:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

     ```
     https://<ManagementNodeIP>
     ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del software Element:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi
- Aggiorna il software Element nei siti connessi utilizzando HealthTools

- Aggiorna il software Element nei siti oscuri utilizzando HealthTools

> Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare lo storage Element

Utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control, è possibile aggiornare un cluster di storage.

> Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, vedere "Articolo della Knowledge base".

> Il processo di aggiornamento richiede circa 30 minuti per nodo per le piattaforme non H610S.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

   ```
   https://<ManagementNodeIP>
   ```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.

   La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**.

5. Scegliere una delle seguenti opzioni ed eseguire la serie di passaggi applicabili al cluster:

Opzione	Fasi
Tutti i cluster che eseguono Element 11.8 e versioni successive	a. Selezionare **Sfoglia** per caricare il pacchetto di aggiornamento scaricato. b. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento. Se ci si allontana dalla finestra del browser, il caricamento del file viene perso. Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato. c. Selezionare **Avvia aggiornamento**. Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere Lo stato dell'aggiornamento cambia. Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina. Una volta completato l'aggiornamento, è possibile scaricare i registri.

Opzione	Fasi
Si sta eseguendo l'aggiornamento di un cluster H610S con una versione di Element precedente alla 11.8.	a. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando e scegliere una delle versioni di aggiornamento disponibili. b. Selezionare **Avvia aggiornamento**. Al termine dell'aggiornamento, l'interfaccia utente richiede di eseguire la fase 2 del processo. c. Completare le fasi aggiuntive richieste (fase 2) in "Articolo della Knowledge base"E confermare nell'interfaccia utente che la fase 2 è stata completata. Una volta completato l'aggiornamento, è possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato dell'aggiornamento, vedere Lo stato dell'aggiornamento cambia.

Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente di Element disponibile.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare **Riprendi**.
In pausa	L'aggiornamento è stato sospeso. Selezionare **Riprendi** per riprendere il processo.

Stato di aggiornamento	Descrizione
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare **Riprendi**. Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.
Completo di follow-up	Solo per l'aggiornamento dei nodi H610S dalla versione Element precedente alla 11.8. Una volta completata la fase 1 del processo di aggiornamento, questo stato richiede di eseguire la fase 2 dell'aggiornamento (vedere la "Articolo della Knowledge base"). Dopo aver completato la fase 2 e aver riconosciuto di averlo completato, lo stato diventa **aggiornato**.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare lo storage degli elementi

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

Fasi

1. Scaricare il pacchetto di aggiornamento dello storage su un dispositivo accessibile al nodo di gestione.

   Accedere al software Element "pagina download" e scaricare l'immagine più recente del nodo di storage.

2. Caricare il pacchetto di aggiornamento dello storage nel nodo di gestione:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/package-repository/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
   d. Selezionare **Provalo**.
   e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
   f. Selezionare **Esegui** per avviare il caricamento.
   g. Dalla risposta, copiare e salvare l'ID del pacchetto (`"id"`) da utilizzare in un passaggio successivo.
3. Verificare lo stato del caricamento.

a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
b. Selezionare **Provalo**.
c. Inserire l'ID del pacchetto copiato nel passaggio precedente in **id**.
d. Selezionare **Esegui** per avviare la richiesta di stato.

   La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID del cluster di storage:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/inventory/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dalla risposta, copiare l'ID della risorsa di installazione (`"id"`).
   g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.
   h. Selezionare **Provalo**.
   i. Incollare l'ID della risorsa di installazione nel campo **id**.
   j. Selezionare **Esegui**.
   k. Dalla risposta, copiare e salvare l'ID del cluster di storage (`"id"`) del cluster che si intende aggiornare per utilizzarlo in un secondo momento.
5. Eseguire l'aggiornamento dello storage:
   a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

      ```
      https://<ManagementNodeIP>/storage/1/
      ```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Selezionare **POST /upgrade**.

d. Selezionare **Provalo**.

e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.

f. Inserire l'ID del cluster di storage nel campo dei parametri.

Il payload dovrebbe essere simile al seguente esempio:

```
{
  "config": {},
  "packageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4",
  "storageId": "884f14a4-5a2a-11e9-9088-6c0b84e211c4"
}
```

g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055`-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
```

```
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```

a. Copiare l'ID dell'aggiornamento (`"upgradeId"`) che fa parte della risposta.

6. Verificare l'avanzamento e i risultati dell'aggiornamento:

   a. Selezionare **GET /upgrades/{upgradeId}**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**.
   d. Selezionare **Esegui**.
   e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. `failedHealthChecks` messaggio nel corpo della risposta.	i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata. ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base. iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare **PUT /upgrades/{upgradeId}**. iv. Selezionare **Provalo**. v. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. vi. Invio `"action":"resume"` nel corpo della richiesta. `{ "action": "resume" }` vii. Selezionare **Esegui**.
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	i. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. ii. Selezionare **Provalo**. iii. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. iv. Invio `"action":"pause"` nel corpo della richiesta. `{ "action": "pause" }` v. Selezionare **Esegui**.

Opzione	Fasi
Se si sta aggiornando un cluster H610S con una versione di Element precedente alla 11.8, viene visualizzato lo stato `finishedNeedsAck` nel corpo di risposta. È necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage H610S.	i. Vedere Aggiornamento dei nodi di storage H610S a Element 12.3.x (fase 2) e completare il processo per ciascun nodo. ii. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. iii. Selezionare **Provalo**. iv. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. v. Invio `"action":"acknowledge"` nel corpo della richiesta. `{ "action": "acknowledge" }` vi. Selezionare **Esegui**.

f. Eseguire l'API **GET /upgrades/{upgradeId}** più volte, in base alle necessità, fino al completamento del processo.

   Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando `percent` il valore è `100` e a. `state` indica `finished`.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.

L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Aggiorna il software Element nei siti connessi utilizzando HealthTools

Fasi

1. Scaricare il pacchetto di aggiornamento dello storage; accedere al software Element "pagina download" e scaricare l'immagine più recente del nodo di storage su un dispositivo che non è il nodo di gestione.

   Per aggiornare il software di storage Element è necessaria l'ultima versione di HealthTools.

2. Copiare il file ISO nel nodo di gestione in una posizione accessibile come /tmp.

   Quando si carica il file ISO, assicurarsi che il nome del file non venga modificato, altrimenti i passaggi successivi non avranno esito positivo.

3. **Opzionale**: Scaricare l'ISO dal nodo di gestione ai nodi del cluster prima dell'aggiornamento.

   Questo passaggio riduce i tempi di aggiornamento pre-organizzando l'ISO sui nodi di storage ed eseguendo ulteriori controlli interni per garantire che il cluster sia in buono stato da aggiornare. L'esecuzione di questa operazione non consente di impostare il cluster in modalità di "upgrade" o di limitare le operazioni del cluster.

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO> --stage
   ```

   Omettere la password dalla riga di comando per consentire `sfinstall` per richiedere le informazioni. Per le password che contengono caratteri speciali, aggiungere una barra rovesciata (`\`) prima di ogni carattere speciale. Ad esempio, `mypass!@1` deve essere inserito come `mypass\!\@`.

   Esempio vedere il seguente esempio di input:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfisodium-11.0.0.345.iso
   --stage
   ```

   L'output dell'esempio mostra questo `sfinstall` tenta di verificare se una versione più recente di `sfinstall` è disponibile:

```
sfinstall 10.117.0.244 -u admin
/tmp/solidfire-rtfisodium-11.0.0.345.iso 2018-10-01 16:52:15:
Newer version of sfinstall available.
This version: 2018.09.01.130, latest version: 2018.06.05.901.
The latest version of the HealthTools can be downloaded from:
https:// mysupport.netapp.com/NOW/cgi-bin/software/
or rerun with --skip-version-check
```

Vedere il seguente estratto di esempio da un'operazione pre-fase di successo:

Al termine della gestione temporanea, viene visualizzato il messaggio `Storage Node Upgrade Staging Successful` dopo l'aggiornamento.

```
flabv0004 ~ # sfinstall -u admin
10.117.0.87 solidfire-rtfi-sodium-patch3-11.3.0.14171.iso --stage
2019-04-03 13:19:58: sfinstall Release Version: 2019.01.01.49 Management
Node Platform:
Ember Revision: 26b042c3e15a Build date: 2019-03-12 18:45
2019-04-03 13:19:58: Checking connectivity to MVIP 10.117.0.87
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.86
2019-04-03 13:19:58: Checking connectivity to node 10.117.0.87
...
2019-04-03 13:19:58: Successfully connected to cluster and all nodes
...
2019-04-03 13:20:00: Do you want to continue? ['Yes', 'No']: Yes
...
2019-04-03 13:20:55: Staging install pack on cluster nodes
2019-04-03 13:20:55: newVersion: 11.3.0.14171
2019-04-03 13:21:01: nodeToStage: nlabp2814, nlabp2815, nlabp2816,
nlabp2813
2019-04-03 13:21:02: Staging Node nlabp2815 mip=[10.117.0.87] nodeID=[2]
(1 of 4 nodes)
2019-04-03 13:21:02: Node Upgrade serving image at
http://10.117.0.204/rtfi/solidfire-rtfisodium-
patch3-11.3.0.14171/filesystem.squashfs
...
2019-04-03 13:25:40: Staging finished. Repeat the upgrade command
without the --stage option to start the upgrade.
```

Gli ISO in più fasi verranno eliminati automaticamente al termine dell'aggiornamento. Tuttavia, se l'aggiornamento non è stato avviato e deve essere ripianificato, gli ISO possono essere disconfigurati manualmente utilizzando il comando:

```
sfinstall <MVIP> -u <cluster_username> --destage
```

Una volta avviato l'aggiornamento, l'opzione di de-stage non è più disponibile.

4. Avviare l'aggiornamento con `sfinstall` E il percorso del file ISO:

   ```
   sfinstall <MVIP> -u <cluster_username> <path-toinstall-file-ISO>
   ```

   Esempio

   Vedere il seguente esempio di comando di input:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   ```

   L'output dell'esempio mostra questo `sfinstall` tenta di verificare se una versione più recente di `sfinstall` è disponibile:

   ```
   sfinstall 10.117.0.244 -u admin /tmp/solidfire-rtfi-sodium-
   11.0.0.345.iso
   2018-10-01 16:52:15: Newer version of sfinstall available.
   This version: 2018.09.01.130, latest version: 2018.06.05.901.
   The latest version of the HealthTools can be downloaded from:
   https://mysupport.netapp.com/NOW/cgi-bin/software/ or rerun with --skip
   -version-check
   ```

   Vedere il seguente estratto di esempio da un aggiornamento riuscito. Gli eventi di aggiornamento possono essere utilizzati per monitorare l'avanzamento dell'aggiornamento.

   ```
   # sfinstall 10.117.0.161 -u admin solidfire-rtfi-sodium-11.0.0.761.iso
   2018-10-11 18:28
   Checking connectivity to MVIP 10.117.0.161
   Checking connectivity to node 10.117.0.23
   Checking connectivity to node 10.117.0.24
   ...
   Successfully connected to cluster and all nodes
   ################################################################
   You are about to start a new upgrade
   10.117.0.161
   10.3.0.161
   solidfire-rtfi-sodium-11.0.0.761.iso
   Nodes:
   10.117.0.23 nlabp1023 SF3010 10.3.0.161
   10.117.0.24 nlabp1025 SF3010 10.3.0.161
   10.117.0.26 nlabp1027 SF3010 10.3.0.161
   10.117.0.28 nlabp1028 SF3010 10.3.0.161
   ################################################################
   ```

```
Do you want to continue? ['Yes', 'No']: yes
...
Watching for new network faults. Existing fault IDs are set([]).
Checking for legacy network interface names that need renaming
Upgrading from 10.3.0.161 to 11.0.0.761 upgrade method=rtfi
Waiting 300 seconds for cluster faults to clear
Waiting for caches to fall below threshold
...
Installing mip=[10.117.0.23] nodeID=[1] (1 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[7] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
Moving primary slice=[12] away from mip[10.117.0.23] nodeID[1] ssid[11]
to new ssid[15]
...
Installing mip=[10.117.114.24] nodeID=[2] (2 of 4 nodes)
Starting to move primaries.
Loading volume list
Moving primary slice=[5] away from mip[10.117.114.24] nodeID[2] ssid[7]
to new ssid[11]
...
Install of solidfire-rtfi-sodium-11.0.0.761 complete.
Removing old software
No staged builds present on nodeID=[1]
No staged builds present on nodeID=[2]
...
Starting light cluster block service check
```

Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Aggiorna il software Element nei siti oscuri utilizzando HealthTools

È possibile utilizzare la suite di strumenti HealthTools per aggiornare il software NetApp Element in un sito buio che non dispone di connettività esterna.

Di cosa hai bisogno

1. Accedere al software Element "pagina download".
2. Selezionare la versione software corretta e scaricare l'immagine più recente del nodo di storage su un computer che non è il nodo di gestione.

   Per aggiornare il software di storage Element è necessaria l'ultima versione di HealthTools.

3. Scarica questo "File JSON" (https://library.netapp.com/ecm/ecm_get_file/ECMLP2840740) Dal NetApp Support Site su un computer che non è il nodo di gestione e rinominarlo in `metadata.json`.
4. Copiare il file ISO nel nodo di gestione in una posizione accessibile come `/tmp`.

È possibile eseguire questa operazione utilizzando, ad esempio, SCP. Quando si carica il file ISO, assicurarsi che il nome del file non venga modificato, altrimenti i passaggi successivi non avranno esito positivo.

Fasi

1. Eseguire `sfupdate-healthtools` comando:

```
sfupdate-healthtools <path-to-healthtools-package>
```

2. Controllare la versione installata:

```
sfupdate-healthtools -v
```

3. Verificare la versione più recente rispetto al file JSON di metadati:

```
sfupdate-healthtools -l --metadata=<path-to-metadata-json>
```

4. Assicurarsi che il cluster sia pronto:

```
sudo sfupgradecheck -u <cluster_username> -p <cluster_password> MVIP
--metadata=<path-to-metadata-json>
```

5. Eseguire `sfinstall` Comando con il percorso del file ISO e del file JSON di metadati:

```
sfinstall -u <cluster_username> <MVIP> <path-toinstall-file-ISO>
--metadata=<path-to-metadata-json-file>
```

Vedere il seguente esempio di comando di input:

```
sfinstall -u admin 10.117.78.244 /tmp/solidfire-rtfi-11.3.0.345.iso
--metadata=/tmp/metadata.json
```

Opzionale è possibile aggiungere `--stage` contrassegna con il `sfinstall` comando per pre-preparare l'aggiornamento in anticipo.

Se si sta aggiornando un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire ulteriori passaggi di aggiornamento (fase 2) per ciascun nodo di storage. Se si esegue Element 11.8 o versioni successive, non sono necessarie ulteriori fasi di aggiornamento (fase 2).

Cosa succede se un aggiornamento non riesce con HealthTools

Se l'aggiornamento del software non riesce, è possibile sospendere l'aggiornamento.

Si consiglia di sospendere un aggiornamento solo con Ctrl-C. In questo modo, il sistema può essere pulito.

Quando `sfinstall` attende la cancellazione dei guasti del cluster e, se un guasto dovesse causare il persistere dei guasti, `sfinstall` non passa al nodo successivo.

Fasi

1. Dovresti smettere `sfinstall` Con Ctrl+C.
2. Contattare il supporto NetApp per assistenza nell'indagine sul guasto.
3. Riprendere l'aggiornamento con lo stesso `sfinstall` comando.
4. Quando un aggiornamento viene messo in pausa utilizzando Ctrl+C, se l'aggiornamento sta aggiornando un nodo, scegliere una delle seguenti opzioni:
   - **Wait**: Consente al nodo in fase di aggiornamento di terminare prima di reimpostare le costanti del cluster.
   - **Continua**: Continua l'aggiornamento, annullando la pausa.
   - **Abort**: Ripristinare le costanti del cluster e interrompere immediatamente l'aggiornamento.

     L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Aggiornamento dei nodi di storage H610S a Element 12.3.x (fase 2)

Se si aggiorna un nodo della serie H610S a Element 12.3.x e il nodo esegue una versione di Element precedente alla 11.8, il processo di aggiornamento prevede due fasi.

La fase 1, che viene eseguita per prima, segue le stesse fasi del processo standard di aggiornamento a Element 12.3.x. Installa Element Software e tutti e 5 gli aggiornamenti del firmware in modo variabile nel cluster, un nodo alla volta. A causa del payload del firmware, il processo richiede circa 1.5 - 2 ore per nodo H610S, incluso un singolo ciclo di avvio a freddo al termine dell'aggiornamento per ciascun nodo.

La fase 2 prevede il completamento delle fasi necessarie per eseguire un arresto completo del nodo e la disconnessione dell'alimentazione per ciascun nodo H610S descritto in un'operazione richiesta "KB". Si stima che questa fase richiede circa un'ora per nodo H610S.

Una volta completata la fase 1, quattro dei cinque aggiornamenti del firmware vengono attivati durante l'avvio a freddo su ciascun nodo H610S; tuttavia, il firmware CPLD (Complex Programmable Logic Device) richiede uno scollegamento completo dell'alimentazione e una riconnessione per l'installazione completa. L'aggiornamento del firmware CPLD protegge da guasti NVDIMM e dall'utilizzo dei metadati durante riavvii o cicli di alimentazione futuri. Il ripristino dell'alimentazione richiede circa un'ora per nodo H610S. Richiede lo spegnimento del nodo, la rimozione dei cavi di alimentazione o la disconnessione dell'alimentazione tramite una Smart PDU, l'attesa di circa 3 minuti e il ricollegamento dell'alimentazione.

Prima di iniziare

- Hai completato la fase 1 del processo di aggiornamento di H610S e hai aggiornato i nodi di storage utilizzando una delle procedure standard di upgrade dello storage Element.

La fase 2 richiede personale on-site.

Fasi

1. (Fase 2) completare il processo di ripristino dell'alimentazione richiesto per ciascun nodo H610S nel cluster:

Se il cluster dispone anche di nodi non H610S, questi nodi non H610S sono esenti dalla fase 2 e non devono essere spenti o scollegati.

1. Contattare il supporto NetApp per assistenza e per pianificare questo aggiornamento.
2. Seguire la procedura di aggiornamento della fase 2 descritta in questa sezione "KB" Necessario per completare un aggiornamento per ciascun nodo H610S.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiornare il firmware dello storage

A partire da Element 12.0 e dalla versione 2.14 dei servizi di gestione, è possibile eseguire aggiornamenti solo firmware sui nodi di storage utilizzando l'interfaccia utente di NetApp Hybrid Cloud Control e l'API REST. Questa procedura non aggiorna il software Element e consente di aggiornare il firmware dello storage al di fuori di una release elemento principale.

Di cosa hai bisogno

- **Privilegi di amministratore**: Si dispone delle autorizzazioni di amministratore del cluster di storage per eseguire l'aggiornamento.
- **System Time Sync**: Hai garantito che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di storage e i nodi. Ciascun nodo deve essere configurato con un server dei nomi DNS nell'interfaccia utente Web per nodo (`https://[IP address]:442`) senza errori del cluster irrisolti correlati all'inclinazione temporale.
- **Porte di sistema**: Se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, si è assicurati che le porte necessarie siano aperte. Vedere "Porte di rete" per ulteriori informazioni.

- **Nodo di gestione**: Per l'interfaccia utente e l'API di NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione**: Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente.

> Per i nodi di storage H610S che eseguono il software Element versione 12.0, applicare D-patch SUST-909 prima di eseguire l'aggiornamento al bundle firmware di storage 2.27. Contattare il supporto NetApp per ottenere la D-patch prima di eseguire l'aggiornamento. Vedere "Note sulla versione di Storage firmware Bundle 2.27".

> Prima di aggiornare il firmware sui nodi di storage, è necessario eseguire l'aggiornamento al bundle di servizi di gestione più recente. Se si sta aggiornando il software Element alla versione 12.2 o successiva, per procedere sono necessari i servizi di gestione 2.14.60 o successiva.

- **Cluster Health**: Sono stati eseguiti controlli di integrità. Vedere "Eseguire i controlli dello stato dello storage Element prima di aggiornare lo storage".
- **Contratto di licenza con l'utente finale (EULA)**: A partire dai servizi di gestione 2.20.69, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage:
  a. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

     ```
     https://<ManagementNodeIP>
     ```

  b. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
  c. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
  d. Viene visualizzato il EULA. Scorrere verso il basso, selezionare **Accetto per aggiornamenti correnti e futuri** e selezionare **Salva**.
- **BMC aggiornato per nodi H610S**: È stata aggiornata la versione BMC per i nodi H610S. Vedere "note di rilascio e istruzioni per l'aggiornamento".

> Per una matrice completa di firmware e firmware del driver per l'hardware, vedere "Versioni del firmware dello storage supportate per i nodi di storage SolidFire"

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del firmware dello storage:

- Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage
- Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage

Utilizza l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dello storage

È possibile utilizzare l'interfaccia utente di NetApp Hybrid Cloud Control per aggiornare il firmware dei nodi di storage nel cluster.

Di cosa hai bisogno

- Se il nodo di gestione non è connesso a Internet "scaricato il pacchetto firmware dello storage".

Per i potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, vedere "Articolo della Knowledge base".

Il processo di aggiornamento richiede circa 30 minuti per nodo di storage. Se si sta aggiornando un cluster di storage Element a un firmware di storage più recente della versione 2.76, i singoli nodi di storage si riavvieranno durante l'aggiornamento solo se è stato scritto un nuovo firmware nel nodo.

Fasi

1. Aprire l'indirizzo IP del nodo di gestione in un browser Web:

```
https://<ManagementNodeIP>
```

2. Accedere a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Upgrade** (Aggiorna) nella parte superiore destra dell'interfaccia.
4. Nella pagina **Upgrades**, selezionare **Storage**.

La scheda **Storage** elenca i cluster di storage che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Upgrade**. Se si utilizzano cluster con Element 12.0 o versioni successive, viene visualizzata la versione corrente del bundle firmware per questi cluster. Se i nodi di un singolo cluster dispongono di versioni firmware diverse o durante il processo di aggiornamento, nella colonna **versione corrente del bundle del firmware** verrà visualizzato **multiplo**. È possibile selezionare **multipli** per accedere alla pagina **nodi** e confrontare le versioni del firmware. Se tutti i cluster eseguono versioni di Element precedenti alla 12.0, non verranno visualizzate informazioni relative ai numeri di versione del bundle del firmware.

Se il cluster è aggiornato e/o non sono disponibili pacchetti di aggiornamento, le schede **Element** e **firmware only** non vengono visualizzate. Queste schede non vengono visualizzate anche quando è in corso un aggiornamento. Se viene visualizzata la scheda **Element**, ma non la scheda **firmware only**, non sono disponibili pacchetti firmware.

5. Selezionare la freccia verso il basso accanto al cluster che si sta aggiornando.
6. Selezionare **Sfoglia** per caricare il pacchetto di aggiornamento scaricato.
7. Attendere il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.

Se ci si allontana dalla finestra del browser, il caricamento del file viene perso.

Una volta caricato e validato il file, viene visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere alcuni minuti. Se in questa fase ci si allontana dalla finestra del browser, il caricamento del file viene preservato.

8. Selezionare **solo firmware** e scegliere una delle versioni di aggiornamento disponibili.
9. Selezionare **Avvia aggiornamento**.

Lo stato dell'aggiornamento viene modificato durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, come la sospensione dell'aggiornamento o se l'aggiornamento restituisce un errore. Vedere Lo stato dell'aggiornamento cambia.

Mentre l'aggiornamento è in corso, è possibile uscire dalla pagina e tornare ad essa in un secondo momento per continuare a monitorare i progressi. La pagina non aggiorna dinamicamente lo stato e la versione corrente se la riga del cluster viene compressa. La riga del cluster deve essere espansa per aggiornare la tabella oppure è possibile aggiornare la pagina.

Una volta completato l'aggiornamento, è possibile scaricare i registri.

Lo stato dell'aggiornamento cambia

Di seguito sono riportati i diversi stati visualizzati nella colonna **Upgrade Status** (Stato aggiornamento) dell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato alla versione più recente disponibile di Element o il firmware è stato aggiornato alla versione più recente.
Impossibile rilevare	Questo stato viene visualizzato quando l'API del servizio di storage restituisce uno stato di aggiornamento non presente nell'elenco degli stati di aggiornamento possibili.
Versioni disponibili	Le versioni più recenti del firmware per elementi e/o storage sono disponibili per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi a schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ogni nodo nel cluster durante l'aggiornamento. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente del server vCenter.
Aggiornamento in pausa	È possibile scegliere di sospendere l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Viene visualizzato un prompt dell'interfaccia utente che richiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di mettere in pausa un aggiornamento, l'operazione di aggiornamento può richiedere fino a due ore. Per riprendere l'aggiornamento, selezionare **Riprendi**.
In pausa	L'aggiornamento è stato sospeso. Selezionare **Riprendi** per riprendere il processo.

Stato di aggiornamento	Descrizione
Errore	Si è verificato un errore durante l'aggiornamento. È possibile scaricare il registro degli errori e inviarlo al supporto NetApp. Dopo aver risolto l'errore, tornare alla pagina e selezionare **Riprendi**. Quando si riprende l'aggiornamento, la barra di avanzamento si sposta indietro per alcuni minuti mentre il sistema esegue il controllo dello stato di salute e verifica lo stato corrente dell'aggiornamento.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

In caso di guasto di un disco o di un nodo durante un aggiornamento, l'interfaccia utente dell'elemento visualizza gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione dei guasti del cluster. La barra di avanzamento nell'interfaccia utente mostra che l'aggiornamento è in attesa della risoluzione degli errori del cluster. In questa fase, la selezione di **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per fornire assistenza durante l'indagine sul guasto.

NetApp Hybrid Cloud Control dispone di un periodo di attesa di tre ore preimpostato, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro tre ore e l'aggiornamento riprende. In questo scenario non è necessario eseguire alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento visualizza **Error** (errore) con un banner rosso. Una volta risolto il problema, è possibile riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere temporaneamente interrotto per intraprendere un'azione correttiva prima della finestra di tre ore. Il supporto utilizzerà l'API per interrompere l'aggiornamento.

> L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe causare la rimozione dei dischi dal nodo. Se i dischi vengono rimossi in modo non corretto, l'aggiunta dei dischi durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe richiedere più tempo per eseguire gli aggiornamenti del firmware o le attività di sincronizzazione post-aggiornamento. Se l'aggiornamento sembra bloccato, contattare il supporto NetApp per assistenza.

Utilizza l'API di controllo del cloud ibrido di NetApp per aggiornare il firmware dello storage

È possibile utilizzare le API per aggiornare i nodi di storage in un cluster alla versione più recente del software Element. È possibile utilizzare uno strumento di automazione a scelta per eseguire le API. Il flusso di lavoro API qui documentato utilizza l'interfaccia utente REST API disponibile sul nodo di gestione come esempio.

Fasi

1. Scaricare il pacchetto di aggiornamento del firmware dello storage su un dispositivo accessibile al nodo di gestione; accedere al software Element "pagina download" e scaricare l'immagine più recente del firmware dello storage.
2. Caricare il pacchetto di aggiornamento del firmware dello storage nel nodo di gestione:
    a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:
   i. Inserire il nome utente e la password del cluster.
   ii. Immettere l'ID client come `mnode-client`.
   iii. Selezionare **autorizzare** per avviare una sessione.
   iv. Chiudere la finestra di autorizzazione.
c. Dall'interfaccia utente API REST, selezionare **POST /packages**.
d. Selezionare **Provalo**.
e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
f. Selezionare **Esegui** per avviare il caricamento.
g. Dalla risposta, copiare e salvare l'ID del pacchetto (`"id"`) da utilizzare in un passaggio successivo.

3. Verificare lo stato del caricamento.
   a. Dall'interfaccia utente API REST, selezionare **GET /packages/{id}/status**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID del pacchetto firmware copiato nella fase precedente in **id**.
   d. Selezionare **Esegui** per avviare la richiesta di stato.

   La risposta indica `state` come `SUCCESS` al termine dell'operazione.

4. Individuare l'ID della risorsa di installazione:
   a. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

   b. Selezionare **autorizzare** e completare le seguenti operazioni:
      i. Inserire il nome utente e la password del cluster.
      ii. Immettere l'ID client come `mnode-client`.
      iii. Selezionare **autorizzare** per avviare una sessione.
      iv. Chiudere la finestra di autorizzazione.
   c. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
   d. Selezionare **Provalo**.
   e. Selezionare **Esegui**.
   f. Dalla risposta, copiare l'ID della risorsa di installazione (`id`).

```
"id": "abcd01e2-xx00-4ccf-11ee-11f111xx9a0b",
"management": {
  "errors": [],
  "inventory": {
    "authoritativeClusterMvip": "10.111.111.111",
    "bundleVersion": "2.14.19",
    "managementIp": "10.111.111.111",
    "version": "1.4.12"
```

g. Dall'interfaccia utente API REST, selezionare **GET /Installations/{id}**.

h. Selezionare **Provalo**.

i. Incollare l'ID della risorsa di installazione nel campo **id**.

j. Selezionare **Esegui**.

k. Dalla risposta, copiare e salvare l'ID del cluster di storage (`"id"`) del cluster che si intende aggiornare per utilizzarlo in un secondo momento.

```
"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",
```

5. Eseguire l'aggiornamento del firmware dello storage:

a. Aprire l'interfaccia utente dell'API REST dello storage sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

b. Selezionare **autorizzare** e completare le seguenti operazioni:

i. Inserire il nome utente e la password del cluster.

ii. Immettere l'ID client come `mnode-client`.

iii. Selezionare **autorizzare** per avviare una sessione.

iv. Chiudere la finestra.

c. Selezionare **POST /upgrade**.

d. Selezionare **Provalo**.

e. Inserire l'ID del pacchetto di aggiornamento nel campo dei parametri.

f. Inserire l'ID del cluster di storage nel campo dei parametri.

g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta deve indicare lo stato come `initializing`:

```
{
  "_links": {
    "collection": "https://localhost:442/storage/upgrades",
    "self": "https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1",
    "log": https://localhost:442/storage/upgrades/3fa85f64-1111-4562-
b3fc-2c963f66abc1/log
  },
  "storageId": "114f14a4-1a1a-11e9-9088-6c0b84e200b4",
  "upgradeId": "334f14a4-1a1a-11e9-1055-6c0b84e2001b4",
  "packageId": "774f14a4-1a1a-11e9-8888-6c0b84e200b4",
  "config": {},
  "state": "initializing",
  "status": {
    "availableActions": [
      "string"
    ],
    "message": "string",
    "nodeDetails": [
      {
        "message": "string",
        "step": "NodePreStart",
        "nodeID": 0,
        "numAttempt": 0
      }
    ],
    "percent": 0,
    "step": "ClusterPreStart",
    "timestamp": "2020-04-21T22:10:57.057Z",
    "failedHealthChecks": [
      {
        "checkID": 0,
        "name": "string",
        "displayName": "string",
        "passed": true,
        "kb": "string",
        "description": "string",
        "remedy": "string",
        "severity": "string",
        "data": {},
        "nodeID": 0
      }
    ]
  },
```

```
  "taskId": "123f14a4-1a1a-11e9-7777-6c0b84e123b2",
  "dateCompleted": "2020-04-21T22:10:57.057Z",
  "dateCreated": "2020-04-21T22:10:57.057Z"
}
```

a. Copiare l'ID dell'aggiornamento (`"upgradeId"`) che fa parte della risposta.

6. Verificare l'avanzamento e i risultati dell'aggiornamento:

   a. Selezionare **GET /upgrades/{upgradeId}**.
   b. Selezionare **Provalo**.
   c. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**.
   d. Selezionare **Esegui**.
   e. In caso di problemi o requisiti speciali durante l'aggiornamento, eseguire una delle seguenti operazioni:

Opzione	Fasi
È necessario correggere i problemi di integrità del cluster dovuti a. `failedHealthChecks` messaggio nel corpo della risposta.	i. Consultare l'articolo della Knowledge base specifico elencato per ciascun problema o eseguire la riparazione specificata. ii. Se viene specificato un KB, completare la procedura descritta nel relativo articolo della Knowledge base. iii. Una volta risolti i problemi del cluster, eseguire nuovamente l'autenticazione, se necessario, e selezionare **PUT /upgrades/{upgradeId}**. iv. Selezionare **Provalo**. v. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. vi. Invio `"action":"resume"` nel corpo della richiesta. `{ "action": "resume" }` vii. Selezionare **Esegui**.

Opzione	Fasi
È necessario sospendere l'aggiornamento perché la finestra di manutenzione si sta chiudendo o per un altro motivo.	i. Se necessario, eseguire nuovamente l'autenticazione e selezionare **PUT /upgrades/{upgradeId}**. ii. Selezionare **Provalo**. iii. Inserire l'ID dell'aggiornamento del passaggio precedente in **upgradeId**. iv. Invio `"action":"pause"` nel corpo della richiesta. `{ "action": "pause" }` v. Selezionare **Esegui**.

f. Eseguire l'API **GET /upgrades/{upgradeId}** più volte, in base alle necessità, fino al completamento del processo.

   Durante l'aggiornamento, il `status` indica `running` se non si riscontrano errori. Man mano che ogni nodo viene aggiornato, il `step` il valore cambia in `NodeFinished`.

L'aggiornamento è stato completato correttamente quando `percent` il valore è `100` e a. `state` indica `finished`.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiornare un nodo di gestione

È possibile aggiornare il nodo di gestione alla versione 12.3.x del nodo di gestione dalla versione 11.0 o successiva.

L'aggiornamento del sistema operativo del nodo di gestione non è più necessario per aggiornare il software Element sul cluster di storage. Se il nodo di gestione è la versione 11.3 o superiore, è sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti degli elementi utilizzando NetApp Hybrid Cloud Control. Se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio la risoluzione dei problemi di protezione, seguire la procedura di aggiornamento del nodo di gestione per lo scenario in uso.

Il plug-in vCenter 4.4 o versione successiva richiede un nodo di gestione 11.3 o versione successiva, creato con architettura modulare e che fornisce singoli servizi.

Opzioni di upgrade

Scegliere una delle seguenti opzioni di aggiornamento del nodo di gestione:

- Il nodo di gestione 12.3.2 contiene una mitigazione della sicurezza per i cluster di storage con la funzione Virtual Volumes (VVol) attivata. Se il cluster di storage si trova già all'elemento 12.3 e la funzione VVols è attivata, eseguire l'aggiornamento alla versione 12.3.2.
- Nel nodo di gestione 12.3 non sono state apportate modifiche aggiuntive alle funzionalità o correzioni di bug. Se si sta già eseguendo il nodo di gestione 12.3, non è necessario aggiornarlo alla versione 12.3.1.

- Se si esegue l'aggiornamento dal nodo di gestione 12.2:Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.2
- Se si esegue l'aggiornamento dal nodo di gestione 12.0:Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.0
- Se si esegue l'aggiornamento dal nodo di gestione 11.3, 11.5, 11.7 o 11.8:Aggiornare un nodo di gestione alla versione 12.3.x dalla 11.3 alla 11.8
- Se si esegue l'aggiornamento dal nodo di gestione 11.0 o 11.1:Aggiornare un nodo di gestione alla versione 12.3.x da 11.1 o 11.0
- Se si esegue l'aggiornamento da un nodo di gestione versione 10.x:Migrazione dal nodo di gestione versione 10.x a 11.x.

Scegliere la seguente opzione se è stato aggiornato in modo **sequenziale** (1) la versione dei servizi di gestione e (2) la versione dello storage Element e si desidera **conservare** il nodo di gestione esistente:

Se non si aggiornano in sequenza i servizi di gestione seguiti dallo storage degli elementi, non è possibile riconfigurare la riautenticazione utilizzando questa procedura. Seguire invece la procedura di aggiornamento appropriata.

- Se si mantiene un nodo di gestione esistente:Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione

Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.2

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 12.2 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- La RAM della VM del nodo di gestione è di 24 GB.
- Il nodo di gestione che si intende aggiornare è la versione 12.0 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control. È possibile accedere a NetApp Hybrid Cloud Control dal seguente indirizzo IP: `https://<ManagementNodeIP>`

- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

> I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
2. Scaricare il "Nodo di gestione ISO" Per il software Element dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

> Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

3. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul NetApp Support Site per il software Element, come nell'esempio seguente:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

4. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

5. Passare alla home directory e smontare il file ISO da `/mnt`:

   ```
   sudo umount /mnt
   ```

6. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

   ```
   sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

7. Sul nodo di gestione che si sta aggiornando, eseguire il comando seguente per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

8. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Se in precedenza era stata disattivata la funzionalità SSH sul nodo di gestione, è necessario "Disattivare nuovamente SSH" sul nodo di gestione ripristinato. Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è attivato sul nodo di gestione per impostazione predefinita.

Aggiornare un nodo di gestione alla versione 12.3.x dalla versione 12.0

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 12.0 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- Il nodo di gestione che si intende aggiornare è la versione 12.0 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud

Control. È possibile accedere a NetApp Hybrid Cloud Control dal seguente indirizzo IP: `https://<ManagementNodeIP>`

- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

> I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
3. Scaricare il "Nodo di gestione ISO" Per il software Element dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

> Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul NetApp Support Site per il software Element, come nell'esempio seguente:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

   ```
   sudo mkdir -p /upgrade
   ```

   ```
   sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso> /mnt
   ```

   ```
   sudo cp -r /mnt/* /upgrade
   ```

6. Passare alla home directory e smontare il file ISO da `/mnt`:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Sul nodo di gestione che si sta aggiornando, eseguire il comando seguente per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

   Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

   Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

   Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione aggiornato.

Aggiornare un nodo di gestione alla versione 12.3.x dalla 11.3 alla 11.8

È possibile eseguire un aggiornamento in-place del nodo di gestione dalla versione 11.3, 11.5, 11.7 o 11.8 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Il nodo di gestione Element 12.3.x è un aggiornamento opzionale. Non è richiesto per le implementazioni esistenti.

Di cosa hai bisogno

- Il nodo di gestione che si intende aggiornare è la versione 11.3, 11.5, 11.7 o 11.8 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

  Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo bundle di servizi di gestione alla versione più recente utilizzando NetApp Hybrid Cloud Control. È possibile accedere a NetApp Hybrid Cloud Control dal seguente indirizzo IP: `https://<ManagementNodeIP>`
- Se si sta aggiornando il nodo di gestione alla versione 12.3.x, per procedere sono necessari i servizi di gestione 2.14.60 o versione successiva.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per "Configurazione di una scheda di rete storage aggiuntiva".

  I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di storage eseguono Element 11.3 o versione successiva.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
3. Scaricare il "Nodo di gestione ISO" Per il software Element dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

   Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul NetApp Support Site per il software Element, come nell'esempio seguente:

   ```
   sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso
   ```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

   ```
   sudo mkdir -p /upgrade
   ```

```
sudo mount <solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso>
/mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Passare alla home directory e smontare il file ISO da `/mnt`:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Nel nodo di gestione 11.3, 11.5, 11.7 o 11.8, eseguire il seguente comando per aggiornare la versione del sistema operativo del nodo di gestione. Lo script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Sul nodo di gestione, eseguire `redeploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:

> Lo script conserva la precedente configurazione dei servizi di gestione, inclusa la configurazione dal servizio di raccolta Active IQ, dai controller (vCenter) o dal proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redeploy-mnode -mu <mnode user>
```

Funzionalità SSH che offre "Accesso alla sessione del NetApp Support Remote Support Tunnel (RST)" è disattivato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza era stata attivata la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "Disattivare nuovamente SSH" sul nodo di gestione aggiornato.

Aggiornare un nodo di gestione alla versione 12.3.x da 11.1 o 11.0

È possibile eseguire un aggiornamento in-place del nodo di gestione da 11.0 o 11.1 alla versione 12.3.x senza dover eseguire il provisioning di una nuova macchina virtuale con nodo di gestione.

Di cosa hai bisogno

- I nodi di storage eseguono Element 11.3 o versione successiva.

  Utilizza gli strumenti HealthTools più recenti per aggiornare il software Element.

- Il nodo di gestione che si intende aggiornare è la versione 11.0 o 11.1 e utilizza la rete IPv4. La versione 12.3.x del nodo di gestione non supporta IPv6.

  Per verificare la versione del nodo di gestione, accedere al nodo di gestione e visualizzare il numero di versione dell'elemento nel banner di accesso.

- Per il nodo di gestione 11.0, la memoria delle macchine virtuali deve essere aumentata manualmente fino a 12 GB.
- È stato configurato un adattatore di rete aggiuntivo (se necessario) seguendo le istruzioni per la configurazione di una scheda di rete storage (eth1) nella guida utente del nodo di gestione del prodotto.

  I volumi persistenti potrebbero richiedere un adattatore di rete aggiuntivo se eth0 non è in grado di essere instradato a SVIP. Configurare un nuovo adattatore di rete sulla rete di storage iSCSI per consentire la configurazione di volumi persistenti.

Fasi

1. Configurare il nodo di gestione VM RAM:
   a. Spegnere la VM del nodo di gestione.
   b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB.
   c. Accendere la VM del nodo di gestione.
2. Accedere alla macchina virtuale del nodo di gestione utilizzando l'accesso a SSH o alla console.
3. Scaricare il "Nodo di gestione ISO" Per il software Element dal sito di supporto NetApp alla macchina virtuale del nodo di gestione.

   Il nome dell'ISO è simile a. `solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso`

4. Verificare l'integrità del download eseguendo md5sum sul file scaricato e confrontare l'output con quello disponibile sul NetApp Support Site per il software Element, come nell'esempio seguente:

```
sudo md5sum -b <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

5. Montare l'immagine ISO del nodo di gestione e copiare il contenuto nel file system utilizzando i seguenti comandi:

```
sudo mkdir -p /upgrade
```

```
sudo mount solidfire-fdva-<Element release>-patchX-XX.X.X.XXXX.iso /mnt
```

```
sudo cp -r /mnt/* /upgrade
```

6. Passare alla home directory e smontare il file ISO da /mnt:

```
sudo umount /mnt
```

7. Eliminare l'ISO per risparmiare spazio sul nodo di gestione:

```
sudo rm <path to iso>/solidfire-fdva-<Element release>-patchX-
XX.X.X.XXXX.iso
```

8. Eseguire uno dei seguenti script con opzioni per aggiornare la versione del sistema operativo del nodo di gestione. Eseguire solo lo script appropriato per la versione in uso. Ogni script conserva tutti i file di configurazione necessari dopo l'aggiornamento, ad esempio le impostazioni di Active IQ Collector e proxy.

   a. Su un nodo di gestione 11.1 (11.1.0.73), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.3.2288
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

   b. Su un nodo di gestione 11.1 (11.1.0.72), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.1.2281
/sf/packages/solidfire-nma-1.4.10/conf /sf/packages/sioc
/sf/packages/nma"
```

c. Su un nodo di gestione 11.0 (11.0.0.781), eseguire il seguente comando:

```
sudo /sf/rtfi/bin/sfrtfi_inplace
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
sf_keep_paths="/sf/packages/solidfire-sioc-4.2.0.2253
/sf/packages/solidfire-nma-1.4.8/conf /sf/packages/sioc
/sf/packages/nma"
```

Al termine del processo di aggiornamento, il nodo di gestione viene riavviato con un nuovo sistema operativo.

> Dopo aver eseguito il comando sudo descritto in questo passaggio, la sessione SSH viene terminata. L'accesso alla console è necessario per il monitoraggio continuo. Se non è disponibile alcun accesso alla console durante l'aggiornamento, riprovare a eseguire l'accesso SSH e verificare la connettività dopo 15 - 30 minuti. Una volta effettuato l'accesso, è possibile confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è stato eseguito correttamente.

9. Nel nodo di gestione 12.3.x, eseguire `upgrade-mnode` script per conservare le impostazioni di configurazione precedenti.

> Se si esegue la migrazione da un nodo di gestione 11.0 o 11.1, lo script copia il Active IQ Collector nel nuovo formato di configurazione.

a. Per un singolo cluster di storage gestito da un nodo di gestione esistente 11.0 o 11.1 con volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account>
```

b. Per un singolo cluster di storage gestito da un nodo di gestione esistente 11.0 o 11.1 senza volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user>
```

c. Per più cluster di storage gestiti da un nodo di gestione esistente 11.0 o 11.1 con volumi persistenti:

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pv <true -
persistent volume> -pva <persistent volume account name - storage
volume account> -pvm <persistent volumes mvip>
```

d. Per più cluster di storage gestiti da un nodo di gestione esistente 11.0 o 11.1 senza volumi persistenti (il `-pvm` Il flag deve fornire uno degli indirizzi MVIP del cluster):

```
sudo /sf/packages/mnode/upgrade-mnode -mu <mnode user> -pvm <mvip for
persistent volumes>
```

10. (Per tutte le installazioni di storage all-flash NetApp SolidFire con plug-in NetApp Element per server vCenter) aggiornare il plug-in vCenter sul nodo di gestione 12.3.x seguendo la procedura descritta nella "Aggiornare il plug-in Element per vCenter Server" argomento.
11. Individuare l'ID risorsa per l'installazione utilizzando l'API del nodo di gestione:
    a. Da un browser, accedere all'interfaccia utente API REST del nodo di gestione:
        i. Accedere a Storage MVIP ed effettuare l'accesso. Questa azione fa sì che il certificato venga accettato per la fase successiva.
    b. Aprire l'interfaccia utente REST API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

    c. Selezionare **autorizzare** e completare le seguenti operazioni:
        i. Inserire il nome utente e la password del cluster.
        ii. Immettere l'ID client come `mnode-client`.
        iii. Selezionare **autorizzare** per avviare una sessione.
        iv. Chiudere la finestra.
    d. Dall'interfaccia utente API REST, selezionare **GET /Installations**.
    e. Selezionare **Provalo**.
    f. Selezionare **Esegui**.
    g. Dal corpo della risposta del codice 200, copiare il `id` per l'installazione.

       L'installazione dispone di una configurazione delle risorse di base creata durante l'installazione o l'aggiornamento.

Migrazione dal nodo di gestione versione 10.x a 11.x.

Se si dispone di un nodo di gestione alla versione 10.x, non è possibile eseguire l'aggiornamento da 10.x a 11.x. È invece possibile utilizzare questa procedura di migrazione per copiare la configurazione da 10.x a un nodo di gestione 11.1 appena distribuito. Se il nodo di gestione è attualmente alla versione 11.0 o superiore, ignorare questa procedura. È necessario il nodo di gestione 11.0 o 11.1 e il "Gli ultimi HealthTools" Per aggiornare il software Element da 10.3 + a 11.x.

Fasi

1. Dall'interfaccia di VMware vSphere, implementare il nodo di gestione 11.1 OVA e accenderlo.
2. Aprire la console VM del nodo di gestione, che consente di visualizzare l'interfaccia utente del terminale (TUI).
3. Utilizzare l'interfaccia telefonica utente per creare un nuovo ID amministratore e assegnare una password.
4. Nel nodo di gestione TUI, accedere al nodo di gestione con il nuovo ID e la nuova password e verificare che funzioni.
5. Dal vCenter o dal nodo di gestione TUI, ottenere l'indirizzo IP del nodo di gestione 11.1 e accedere all'indirizzo IP sulla porta 9443 per aprire l'interfaccia utente del nodo di gestione.

   ```
   https://<mNode 11.1 IP address>:9443
   ```

6. In vSphere, selezionare **Configurazione NetApp Element** > **Impostazioni mNode**. (Nelle versioni precedenti, il menu di primo livello è **Configurazione NetApp SolidFire**).
7. Selezionare **azioni** > **Cancella**.
8. Per confermare, selezionare **Sì**. Il campo mNode Status (Stato mNode) deve riportare non configurato.

   Quando si accede alla scheda **mNode Settings** (Impostazioni mNode) per la prima volta, il campo mNode Status (Stato mNode) potrebbe essere visualizzato come **Not Configured** (non configurato*) anziché come **UP** previsto; potrebbe non essere possibile selezionare **Actions** (azioni) > **Clear** (Cancella). Aggiornare il browser. Il campo mNode Status (Stato mNode) visualizza **UP**.

9. Disconnettersi da vSphere.
10. In un browser Web, aprire l'utility di registrazione del nodo di gestione e selezionare **QoSSIOC Service Management**:

    ```
    https://<mNode 11.1 IP address>:9443
    ```

11. Impostare la nuova password QoSSIOC.

    La password predefinita è `solidfire`. Questa password è necessaria per impostare la nuova password.

12. Selezionare la scheda **vCenter Plug-in Registration**.
13. Selezionare **Aggiorna plug-in**.
14. Inserire i valori richiesti. Al termine, selezionare **UPDATE**.
15. Accedere a vSphere e selezionare **Configurazione NetApp Element** > **Impostazioni mNode**.
16. Selezionare **azioni** > **Configura**.
17. Fornire l'indirizzo IP del nodo di gestione, l'ID utente del nodo di gestione (il nome utente è `admin`), la password impostata nella scheda **QoSSIOC Service Management** dell'utilità di registrazione, nonché l'ID utente e la password di vCenter.

    In vSphere, la scheda **mNode Settings** (Impostazioni mNode) dovrebbe visualizzare lo stato di mNode

come **UP**, che indica che il nodo di gestione 11.1 è registrato in vCenter.

18. Dall'utility di registrazione del nodo di gestione (`https://<mNode 11.1 IP address>:9443`), riavviare il servizio SIOC da **QoSSIOC Service Management**.
19. Attendere un minuto e selezionare la scheda **Configurazione NetApp Element** > **Impostazioni mNode**. Lo stato di mNode dovrebbe essere **UP**.

    Se lo stato è **DOWN**, controllare le autorizzazioni per `/sf/packages/sioc/app.properties`. Il file deve disporre dei permessi di lettura, scrittura ed esecuzione per il proprietario del file. Le autorizzazioni corrette dovrebbero essere visualizzate come segue:

    ```
    -rwx------
    ```

20. Una volta avviato il processo SIOC e visualizzato lo stato di mNode in **UP**, controllare i registri per `sf-hci-nma` sul nodo di gestione. Non dovrebbero essere presenti messaggi di errore.
21. (Solo per il nodo di gestione 11.1) SSH nel nodo di gestione versione 11.1 con privilegi root e avviare il servizio NMA con i seguenti comandi:

    ```
    # systemctl enable /sf/packages/nma/systemd/sf-hci-nma.service
    ```

    ```
    # systemctl start sf-hci-nma21
    ```

22. Eseguire azioni da vCenter per rimuovere un disco, aggiungere un disco o riavviare i nodi. In questo modo vengono attivati gli avvisi relativi allo storage, che devono essere riportati in vCenter. Se funziona, gli avvisi di sistema NMA funzionano come previsto.
23. Se ONTAP Select è configurato in vCenter, configurare gli avvisi ONTAP Select in NMA copiando `.ots.properties` dal nodo di gestione precedente al nodo di gestione versione 11.1 `/sf/packages/nma/conf/.ots.properties` E riavviare il servizio NMA utilizzando il seguente comando:

    ```
    systemctl restart sf-hci-nma
    ```

24. Verificare che ONTAP Select funzioni visualizzando i registri con il seguente comando:

    ```
    journalctl -f | grep -i ots
    ```

25. Configurare Active IQ seguendo questa procedura:
    a. Accedere alla versione 11.1 del nodo di gestione e passare a. `/sf/packages/collector` directory.
    b. Eseguire il seguente comando:

```
sudo ./manage-collector.py --set-username netapp --set-password --set
-mvip <MVIP>
```

c. Inserire la password dell'interfaccia utente del nodo di gestione quando richiesto.

d. Eseguire i seguenti comandi:

```
./manage-collector.py --get-all
```

```
sudo systemctl restart sfcollector
```

e. Verificare `sfcollector` registri per confermare che funziona.

26. In vSphere, la scheda **Configurazione NetApp Element** > **Impostazioni mNode** dovrebbe visualizzare lo stato di mNode come **UP**.
27. Verificare che l'NMA stia segnalando gli avvisi di sistema e gli avvisi ONTAP Select.
28. Se tutto funziona come previsto, chiudere ed eliminare il nodo di gestione 10.x VM.

Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione

È possibile mantenere il nodo di gestione esistente se sono stati aggiornati in sequenza (1) servizi di gestione e (2) storage di elementi. Se si è seguito un ordine di aggiornamento diverso, consultare le procedure per gli aggiornamenti dei nodi di gestione in-place.

Prima di iniziare

- I servizi di gestione sono stati aggiornati alla versione 2.10.29 o successiva.
- Il cluster di storage esegue Element 12.0 o versione successiva.
- Il nodo di gestione è 11.3 o successivo.
- I servizi di gestione sono stati aggiornati in sequenza, seguito dall'aggiornamento dello storage Element. Non è possibile riconfigurare l'autenticazione utilizzando questa procedura a meno che non siano stati completati gli aggiornamenti nella sequenza descritta.

Fasi

1. Aprire l'interfaccia utente REST API del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/mnode
```

2. Selezionare **autorizzare** e completare le seguenti operazioni:
   a. Inserire il nome utente e la password del cluster.
   b. Immettere l'ID client come `mnode-client` se il valore non è già compilato.
   c. Selezionare **autorizzare** per avviare una sessione.
3. Dall'interfaccia utente API REST, selezionare **POST /Services/reconfigure-auth**.
4. Selezionare **Provalo**.

5. Per il parametro **load_images**, selezionare `true`.
6. Selezionare **Esegui**.

   Il corpo della risposta indica che la riconfigurazione è stata eseguita correttamente.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiornare il plug-in Element per vCenter Server

Per gli ambienti vSphere esistenti con un plug-in NetApp Element registrato per VMware vCenter Server, è possibile aggiornare la registrazione del plug-in dopo il primo aggiornamento del pacchetto di servizi di gestione che contiene il servizio plug-in.

È possibile aggiornare la registrazione del plug-in su vCenter Server Virtual Appliance (vCSA) o Windows utilizzando l'utility di registrazione. È necessario modificare la registrazione per il plug-in vCenter su ogni vCenter Server in cui è necessario utilizzare il plug-in.

Management Services 2.22.7 include Element Plug-in per vCenter Server 5.0 che contiene il plug-in remoto. Se si utilizza il plug-in Element, è necessario eseguire l'aggiornamento ai servizi di gestione 2.22.7 o versioni successive per rispettare la direttiva VMware che rimuove il supporto per i plug-in locali. "Scopri di più".

Plug-in Element vCenter 5.0 o versione successiva

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Stai effettuando l'aggiornamento a Element Plug-in per vCenter Server 5,3, 5,2, 5,1 o 5,0.
- Si sta eseguendo l'aggiornamento a 8.0 o 7.0 HTML5 vSphere Web Client.

Il plug-in Element per vCenter 5,0 o versioni successive non è compatibile con vCenter Server 6,7 e 6,5.

Quando si esegue l'aggiornamento da Element Plug-in per vCenter Server 4.x a 5.x, i cluster già configurati con il plug-in vengono persi perché i dati non possono essere copiati da un'istanza di vCenter a un plug-in remoto. È necessario aggiungere nuovamente i cluster al plug-in remoto. Si tratta di un'attività singola durante l'aggiornamento da un plug-in locale a un plug-in remoto.

Plug-in Element vCenter 4.10 o versioni precedenti

Questa procedura di aggiornamento riguarda i seguenti scenari di aggiornamento:

- Si sta eseguendo l'aggiornamento a Element Plug-in per vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 o 4.4.
- Si sta eseguendo l'aggiornamento a un client Web 7.0, 6.7 o 6.5 HTML5 vSphere.

- Il plug-in non è compatibile con VMware vCenter Server 8.0 per Element Plug-in per VMware vCenter Server 4.x.
- Il plug-in non è compatibile con VMware vCenter Server 6.5 per Element Plug-in per VMware vCenter Server 4.6, 4.7 e 4.8.

- Si sta eseguendo l'aggiornamento a 6.7 Flash vSphere Web Client.

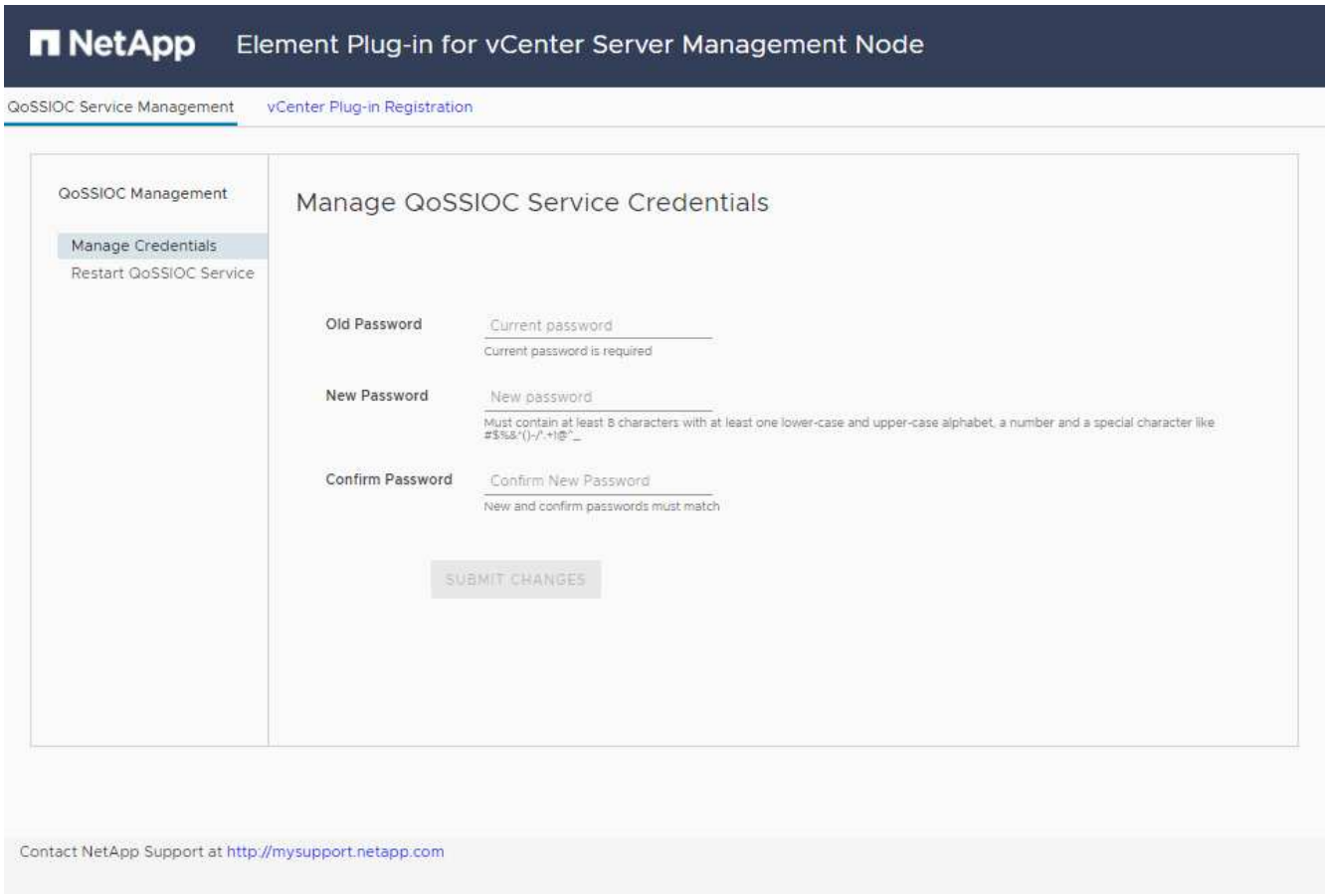
> Il plug-in è compatibile con vSphere Web Client versione 6.7 U2 per Flash, 6.7 U3 (Flash e HTML5) e 7.0 U1. Il plug-in non è compatibile con la versione 6.7 U2 build 13007421 del client Web vSphere HTML5 e con altre build 6.7 U2 rilasciate prima dell'aggiornamento 2a (build 13643870). Per ulteriori informazioni sulle versioni di vSphere supportate, consultare le note sulla versione di "versione del plug-in".

Di cosa hai bisogno

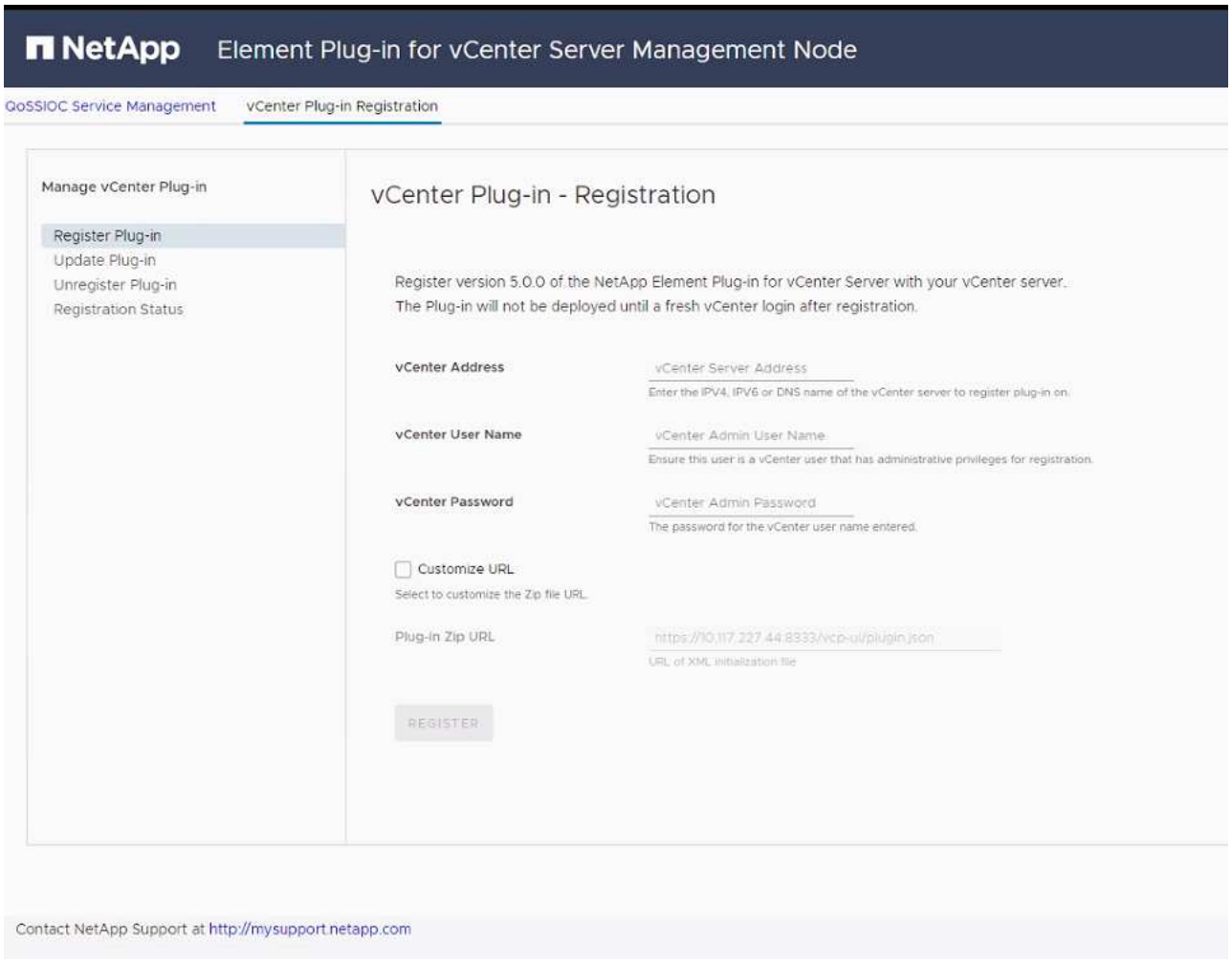
- **Privilegi di amministratore**: Si dispone dei privilegi di amministratore vCenter per installare un plug-in.
- **Aggiornamenti vSphere**: Sono stati eseguiti tutti gli aggiornamenti vCenter necessari prima di aggiornare il plug-in NetApp Element per vCenter Server. Questa procedura presuppone che gli aggiornamenti di vCenter siano già stati completati.
- **VCenter Server**: Il plug-in vCenter versione 4.x o 5.x è registrato con vCenter Server. Dall'utility di registrazione (`https://<ManagementNodeIP>:9443`), selezionare **Registration Status** (Stato registrazione), completare i campi necessari e selezionare **Check Status** (Controlla stato) per verificare che il plug-in vCenter sia già registrato e che il numero di versione dell'installazione corrente.
- **Aggiornamenti dei servizi di gestione**: È stato aggiornato il "bundle di servizi di gestione" alla versione più recente. Gli aggiornamenti del plug-in vCenter vengono distribuiti utilizzando gli aggiornamenti dei servizi di gestione rilasciati al di fuori delle principali release di prodotti per lo storage all-flash NetApp SolidFire.
- **Aggiornamenti del nodo di gestione**:
  - A partire dal plug-in Element vCenter 5.0, viene eseguito un nodo di gestione "aggiornato" alla versione 12.3.x o successiva.
  - Per il plug-in Element vCenter da 4.4 a 4.10, si sta eseguendo un nodo di gestione che lo è stato "aggiornato" alla versione 11.3 o successiva. VCenter Plug-in 4.4 o versione successiva richiede un nodo di gestione 11.3 o versione successiva con un'architettura modulare che fornisce singoli servizi. Il nodo di gestione deve essere acceso con il relativo indirizzo IP o DHCP configurato.
- **Upgrade dello storage Element**:
  - A partire dal plug-in Element vCenter 5.0, si dispone di un cluster che esegue il software NetApp Element 12.3.x o versione successiva.
  - Per il plug-in Element vCenter 4.10 o versione precedente, si dispone di un cluster che esegue il software NetApp Element 11.3 o versione successiva.
- **VSphere Web Client**: Si è disconnessi da vSphere Web Client prima di iniziare qualsiasi aggiornamento del plug-in. Il client Web non riconosce gli aggiornamenti effettuati durante questo processo al plug-in se non si effettua la disconnessione.

Fasi

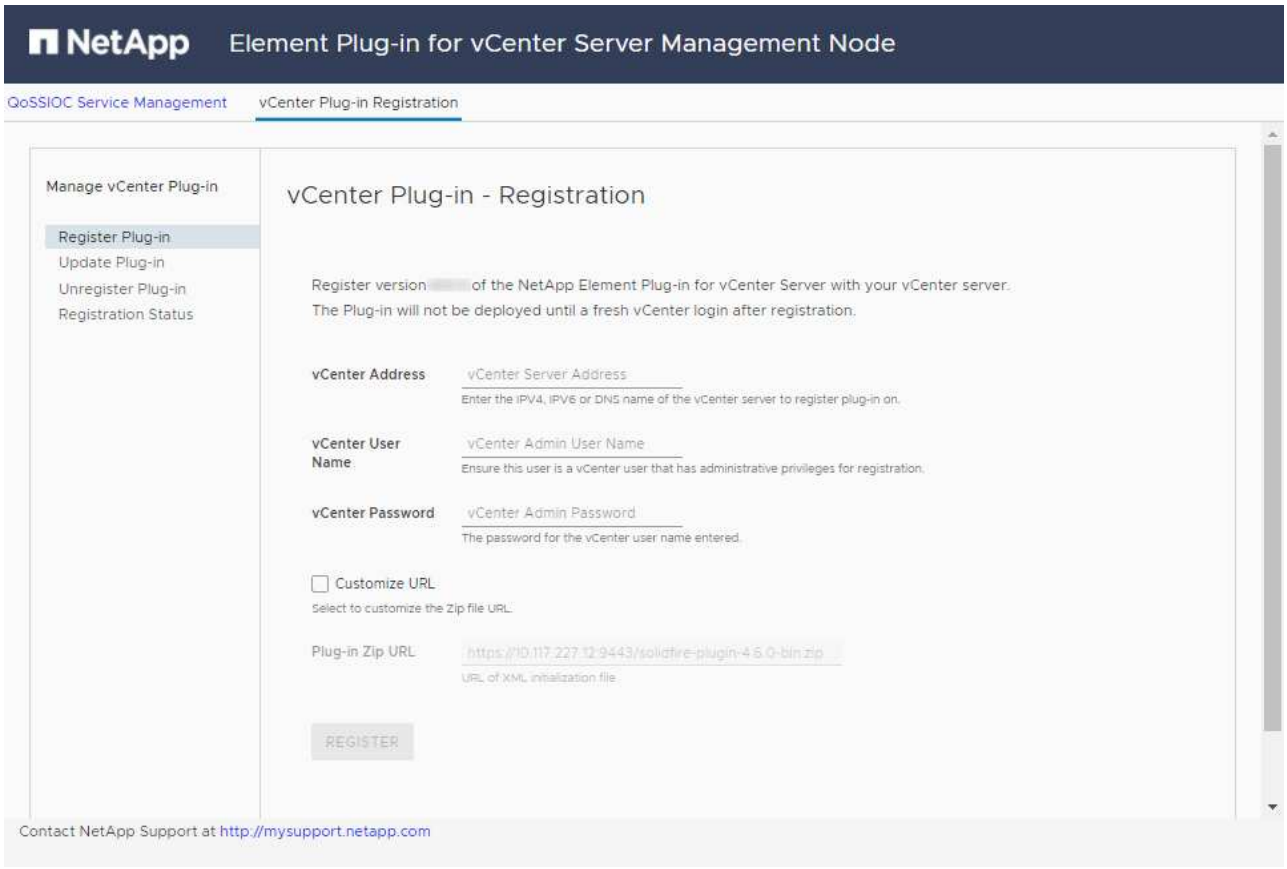
1. Inserire l'indirizzo IP del nodo di gestione in un browser, inclusa la porta TCP per la registrazione: `https://<ManagementNodeIP>:9443`L'interfaccia utente dell'utility di registrazione apre la pagina **Manage QoSSIOC Service Credentials** (Gestisci credenziali servizio QoSSIOC) per il plug-in.



2. Selezionare **vCenter Plug-in Registration**.
   - La pagina di registrazione del plug-in vCenter per il plug-in Element per vCenter Server 5.x:



- La pagina di registrazione del plug-in vCenter per il plug-in Element per vCenter Server 4.10 o versioni precedenti:



3. In **Manage vCenter Plug-in** (Gestisci plug-in vCenter), selezionare **Update Plug-in** (Aggiorna plug-in).
4. Confermare o aggiornare le seguenti informazioni:
   a. L'indirizzo IPv4 o l'FQDN del servizio vCenter su cui si desidera registrare il plug-in.
   b. Il nome utente vCenter Administrator.

      Il nome utente e la password immessi devono essere assegnati a un utente con privilegi di ruolo vCenter Administrator.

   c. La password di vCenter Administrator.
   d. (Per server interni/siti oscuri) a seconda del plug-in Element per la versione di vCenter, un URL personalizzato per il file JSON del plug-in o il plug-in ZIP:
      i. A partire da Element Plug-in per vCenter Server 5.0, un URL personalizzato per il file JSON del plug-in.

         È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito scuro) o se sono state modificate le impostazioni di rete o il nome del file JSON. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito scuro).

      ii. Per Element Plug-in per vCenter Server 4.10 o versioni precedenti, un URL personalizzato per il plug-in ZIP.

È possibile selezionare **Custom URL** (URL personalizzato) per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito scuro) o se sono state modificate le impostazioni di rete o il nome del file ZIP. Per ulteriori procedure di configurazione se si intende personalizzare un URL, vedere la documentazione di Element Plug-in for vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (sito scuro).

5. Selezionare **Aggiorna**.

   Una volta completata la registrazione, nell'interfaccia utente dell'utility di registrazione viene visualizzato un banner.

6. Accedere a vSphere Web Client come vCenter Administrator. Se si è già connessi a vSphere Web Client, è necessario prima disconnettersi, attendere due o tre minuti, quindi eseguire nuovamente l'accesso.

   Questa azione crea un nuovo database e completa l'installazione in vSphere Web Client.

7. In vSphere Web Client, cercare le seguenti attività completate nel task monitor per assicurarsi che l'installazione sia stata completata: `Download plug-in` e. `Deploy plug-in`.
8. Verificare che i punti di estensione del plug-in siano visualizzati nella scheda **Shortcuts** di vSphere Web Client e nel pannello laterale.
   - A partire dal plug-in Element per vCenter Server 5.0, viene visualizzato il punto di estensione del plug-in remoto NetApp Element:

   - Per il plug-in Element per vCenter Server 4.10 o versioni precedenti, vengono visualizzati i punti di estensione per la configurazione e la gestione di NetApp Element:

   Se le icone del plug-in vCenter non sono visibili, vedere "Plug-in Element per vCenter Server" documentazione sulla risoluzione dei problemi del plug-in.

   Dopo aver eseguito l'aggiornamento al plug-in NetApp Element per vCenter Server 4.8 o versioni successive con VMware vCenter Server 6.7U1, se i cluster di storage non sono elencati o viene visualizzato un errore del server nelle sezioni **Clusters** e **QoSSIOC Settings** della configurazione NetApp Element, vedere "Plug-in Element per vCenter Server" documentazione sulla risoluzione di questi errori.

9. Verificare la modifica della versione nella scheda **About** (informazioni su) nel punto di estensione **NetApp Element Configuration** del plug-in.

   Dovrebbero essere visualizzati i seguenti dettagli di versione o dettagli di una versione più recente:

```
NetApp Element Plug-in Version: 5.3
NetApp Element Plug-in Build Number: 9
```

Il plug-in vCenter contiene il contenuto della Guida in linea. Per assicurarsi che la guida contenga i contenuti più recenti, cancellare la cache del browser dopo aver aggiornato il plug-in.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Aggiorna i componenti vSphere per un sistema storage NetApp SolidFire con il plug-in Element per vCenter Server

Quando si aggiornano i componenti VMware vSphere dell'installazione dello storage SolidFire Element, è necessario eseguire alcuni passaggi aggiuntivi per i sistemi con plug-in Element per vCenter Server.

Fasi

1. Per gli aggiornamenti vCSA, "chiaro" Impostazioni QoSSIOC nel plug-in (**Configurazione NetApp Element > Impostazioni QoSSIOC**). Viene visualizzato il campo **QoSSIOC Status** `Not Configured` al termine del processo.
2. Per gli aggiornamenti vCSA e Windows, "annulla registrazione" Il plug-in di vCenter Server a cui è associato mediante l'utility di registrazione.
3. "Aggiornamento di vSphere, inclusi vCenter Server, ESXi, VM e altri componenti VMware".

> È necessario eseguire l'aggiornamento al plug-in NetApp Element per vCenter Server 5.0 o versioni successive per consentire di implementare il plug-in con VMware vCenter 7.0 Update 3 senza applicare una soluzione alternativa.
>
> Con Element Plug-in per vCenter Server 4.x, quando si esegue l'aggiornamento a VMware vCenter Server 7.0 Update 3, il plug-in non viene implementato. Per risolvere questo problema utilizzando Spring Framework 4, vedere "Questo articolo della Knowledge base".

4. "Registrati" Il plug-in Element per vCenter Server con vCenter.
5. "Aggiungere cluster" utilizzando il plug-in.
6. "Configurare le impostazioni QoSSIOC" utilizzando il plug-in.
7. "Abilitare QoSSIOC" per tutti i datastore controllati dal plug-in.

Trova ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Versioni precedenti della documentazione software SolidFire e NetApp Element

La documentazione relativa alle release precedenti è disponibile sul sito NetApp Support.

- "Documentazione di Element 12.2.1"
- "Documentazione di Element 12.2"
- "Documentazione di Element 12.0.1"
- "Documentazione di Element 12.0"
- "Documentazione di Element 11.8.2"
- "Documentazione di Element 11.8.1"
- "Documentazione di Element 11.8"
- "Documentazione di Element 11.7"
- "Documentazione di Element 11.5.1"
- "Documentazione di Element 11.5"
- "Documentazione Element 11,3P1"
- "Documentazione di Element 11.3.2"
- "Documentazione di Element 11.1 e versioni precedenti"

Per ulteriori informazioni

- "Documentazione software SolidFire ed Element"
- "Plug-in NetApp Element per server vCenter"

Note legali

Le note legali forniscono l'accesso a dichiarazioni di copyright, marchi, brevetti e altro ancora.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero 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

Direttiva sulla privacy

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

- "Avviso per Ember OS 12.3"
- "Avviso per HealthTools"
- "Avviso per il nodo di gestione 12.3"
- "Avviso per i servizi di gestione 2.25.42 (plug-in NetApp Element per VMware vCenter Server 5,3.9)"
- "Avviso per i servizi di gestione 2.24.40 (plug-in NetApp Element per VMware vCenter Server 5,2.12)"
- "Avviso per i servizi di gestione 2.23.64 (plug-in NetApp Element per VMware vCenter Server 5.1.12)"
- "Avviso per i servizi di gestione 2.22.7 (plug-in NetApp Element per VMware vCenter Server 5.0.37)"
- "Avviso per i servizi di gestione 2.21.61 (plug-in NetApp Element per VMware vCenter Server 4.10.12)"
- "Avviso per i servizi di gestione 2.20.69 (plug-in NetApp Element per vCenter Server 4.9.14)"
- "Avviso per i servizi di gestione 2.19.48 (plug-in NetApp Element per vCenter Server 4.8.34)"
- "Avviso per i servizi di gestione 2.18.91 (plug-in NetApp Element per vCenter Server 4.7.10)"
- "Avviso per i servizi di gestione 2.17.56 (plug-in NetApp Element per vCenter Server 4.6.32)"
- "Avviso per i servizi di gestione 2.17.52 (plug-in NetApp Element per vCenter Server 4.6.29)"
- "Avviso per i servizi di gestione 2.16 (plug-in NetApp Element per vCenter Server 4.6.29)"

- "Avviso per i servizi di gestione 2.14 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per i servizi di gestione 2.13 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per Storage firmware Bundle 2.146"
- "Avviso per Storage firmware Bundle 2.99.2"
- "Avviso per Storage firmware Bundle 2.76"
- "Avviso per Storage firmware Bundle 2.27"

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.