



Documentazione del software SolidFire ed Element

Element Software

NetApp
November 18, 2025

This PDF was generated from <https://docs.netapp.com/it-it/element-software-128/index.html> on November 18, 2025. Always check docs.netapp.com for the latest.

Sommario

Documentazione del software SolidFire ed Element	1
Note di rilascio	2
Informazioni sulla versione attuale e precedente	2
Software NetApp Element	2
Servizi di gestione	2
Plug-in NetApp Element per vCenter Server	2
Firmware di archiviazione	3
Trova maggiori informazioni	3
Novità nel software Element	3
Elemento 12.8	3
Elemento 12.7	4
Elemento 12.5	6
Trova maggiori informazioni	7
Concetti	8
Panoramica del prodotto	8
Caratteristiche SolidFire	8
Distribuzione di SolidFire	8
Trova maggiori informazioni	8
Architettura e componenti	9
Scopri di più sull'architettura SolidFire	9
Interfacce software SolidFire	10
SolidFire Active IQ	12
Nodo di gestione per il software Element	13
Servizi di gestione per l'archiviazione all-flash SolidFire	13
Nodi	13
Nodo di gestione	14
Nodo di archiviazione	14
Nodo Fibre Channel	14
Stati operativi del nodo	14
Trova maggiori informazioni	15
Cluster	15
Cluster di archiviazione autorevoli	16
Regola dei terzi	16
Capacità bloccata	16
Efficienza di archiviazione	17
Quorum del cluster di archiviazione	17
Sicurezza	17
Crittografia a riposo (hardware)	17
Crittografia a riposo (software)	18
Gestione delle chiavi esterne	18
Autenticazione multifattoriale	18
FIPS 140-2 per HTTPS e crittografia dei dati a riposo	18
Per maggiori informazioni	19

Account e permessi	19
Account amministratore del cluster di archiviazione	19
Account utente	20
Account utente autorevoli del cluster	20
Conti di volume	20
Magazzinaggio	21
Volumi	21
Volumi virtuali (vVols)	21
Gruppi di accesso al volume	23
Iniziatori	23
Protezione dei dati	23
Tipi di replicazione remota	24
Snapshot del volume per la protezione dei dati	26
Cloni di volume	26
Panoramica del processo di backup e ripristino per Element Storage	26
Domini di protezione	27
Domini di protezione personalizzati	27
Doppia elica ad alta disponibilità	28
Prestazioni e qualità del servizio	28
Parametri di qualità del servizio	28
Limiti del valore QoS	29
Prestazioni QoS	29
Criteri QoS	30
Trova maggiori informazioni	30
Requisiti	31
Networking	31
Per maggiori informazioni	31
Configurazione dello switch per cluster che eseguono il software Element	31
Per maggiori informazioni	32
Requisiti delle porte di rete	32
Per maggiori informazioni	36
Provalo	37
Prova le funzionalità di archiviazione utilizzando Element Demo Node	37
Funzionalità supportate:	37
Requisiti VM	38
Requisiti dell'host	38
Scarica il nodo demo dell'elemento	38
Installa Element Demo Node su VMware ESXi	38
Come ottenere supporto	39
Trova maggiori informazioni	39
Installare e mantenere l'hardware	40
Informazioni hardware H410S e H610S	40
Installare nodi di archiviazione della serie H	40
Sostituire un nodo H410S	49
Sostituisci un nodo H610S	53

Sostituire le unità	55
Sostituire un alimentatore	59
Informazioni sull'hardware della serie SF	62
Sostituire un telaio	62
Sostituire le unità per i nodi di archiviazione della serie SF	64
Sostituire un alimentatore	68
Ritorna alle informazioni sull'immagine di fabbrica	69
Configurare l'immagine di ritorno alla fabbrica	69
Opzioni di distribuzione e installazione RTFI	70
Il processo RTFI	71
Menu delle opzioni RTFI	73
Nodi di archiviazione	75
H610S	75
H410S	99
SF38410, SF19210, SF9605 e SF4805	103
Configurare l'archiviazione	108
Scopri come impostare l'archiviazione	108
Trova maggiori informazioni	108
Configurare un cluster con nodi di archiviazione	109
Configurare un nodo di archiviazione	109
Creare un cluster di archiviazione	111
Accedi all'interfaccia utente del software Element	112
Aggiungere unità a un cluster	113
Configurare un cluster con nodi Fibre Channel	114
Configurare un nodo Fibre Channel	114
Crea un nuovo cluster con nodi Fibre Channel	114
Aggiungere nodi Fibre Channel a un cluster	115
Impostare le zone per i nodi Fibre Channel	116
Creare un gruppo di accesso al volume per i client Fibre Channel	116
Determinare quali componenti SolidFire installare	117
Per maggiori informazioni	118
Impostare un nodo di gestione	118
Trova maggiori informazioni	118
Configurare l'accesso all'interfaccia utente Web del nome di dominio completo	118
Configurare l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control	119
Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST	119
Rimuovere l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control	120
Rimuovere l'accesso all'interfaccia utente Web FQDN tramite l'API REST	121
Risoluzione dei problemi	122
Trova maggiori informazioni	122
Cosa c'è dopo?	122
Trova maggiori informazioni	123
Gestisci lo storage con il software Element	124
Gestisci lo storage con il software Element	124
Trova maggiori informazioni	124

Accedi all'interfaccia utente del software Element	124
Trova maggiori informazioni	125
Configurare le opzioni del sistema SolidFire dopo la distribuzione	125
Configurare le opzioni del sistema SolidFire dopo la distribuzione	125
Modificare le credenziali in NetApp HCI e NetApp SolidFire	125
Cambia il certificato SSL predefinito del software Element	129
Cambia la password IPMI predefinita per i nodi	130
Utilizzare le opzioni di base nell'interfaccia utente del software Element	131
Utilizzare le opzioni di base nell'interfaccia utente del software Element	132
Attività API	132
Icone nell'interfaccia Element	133
Fornire feedback	134
Gestire gli account	134
Gestire gli account	134
Lavorare con gli account utilizzando CHAP	135
Gestire gli account utente dell'amministratore del cluster	137
Gestisci LDAP	141
Gestisci il tuo sistema	149
Gestisci il tuo sistema	149
Abilita l'autenticazione a più fattori	150
Configurare le impostazioni del cluster	151
Creare un cluster che supporti le unità FIPS	167
Stabilire una comunicazione sicura	170
Inizia con la gestione delle chiavi esterne	172
Gestire volumi e volumi virtuali	177
Scopri di più sulla gestione dei volumi e dei volumi virtuali	177
Lavorare con i volumi	179
Lavorare con volumi virtuali	188
Lavorare con gruppi di accesso al volume e iniziatori	196
Proteggi i tuoi dati	203
Proteggi i tuoi dati	203
Utilizzare snapshot del volume per la protezione dei dati	204
Eseguire la replica remota tra cluster che eseguono il software NetApp Element	218
Utilizzare la replica SnapMirror tra cluster Element e ONTAP (interfaccia utente Element)	232
Replica tra il software NetApp Element e ONTAP (ONTAP CLI)	243
Eseguire il backup e il ripristino dei volumi	264
Configurare domini di protezione personalizzati	268
Risolvi i problemi del tuo sistema	269
Eventi di sistema	269
Visualizza lo stato delle attività in esecuzione	273
Avvisi di sistema	274
Visualizza l'attività delle prestazioni del nodo	291
Prestazioni di volume	292
sessioni iSCSI	294
Sessioni Fibre Channel	295

Risoluzione dei problemi delle unità	296
Risoluzione dei problemi dei nodi	299
Lavorare con utilità per nodo per nodi di archiviazione	300
Comprendere i livelli di pienezza del cluster	308
Gestisci e monitora lo storage con NetApp Hybrid Cloud Control	310
Aggiungi e gestisci cluster di storage utilizzando NetApp Hybrid Cloud Control	310
Aggiungere un cluster di archiviazione	310
Conferma lo stato del cluster di archiviazione	311
Modifica le credenziali del cluster di archiviazione	311
Rimuovere un cluster di archiviazione	311
Abilita e disabilita la modalità di manutenzione	312
Configurare l'accesso all'interfaccia utente Web del nome di dominio completo	314
Configurare l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control	315
Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST	315
Rimuovere l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control	316
Rimuovere l'accesso all'interfaccia utente Web FQDN tramite l'API REST	317
Risoluzione dei problemi	317
Trova maggiori informazioni	318
Crea e gestisci account utente utilizzando NetApp Hybrid Cloud Control	318
Abilita LDAP	319
Gestire gli account autorevoli del cluster	319
Gestire gli account di volume	321
Crea e gestisci volumi utilizzando NetApp Hybrid Cloud Control	322
Crea un volume	323
Applicare una policy QoS a un volume	324
Modifica un volume	324
Clona volumi	325
Aggiungere volumi a un gruppo di accesso al volume	327
Elimina un volume	327
Ripristina un volume eliminato	328
Elimina un volume eliminato	328
Creare e gestire gruppi di accesso al volume	329
Aggiungi un gruppo di accesso al volume	329
Modifica un gruppo di accesso al volume	329
Elimina un gruppo di accesso al volume	330
Creare e gestire gli iniziatori	330
Creare un iniziatore	331
Aggiungere iniziatori a un gruppo di accesso al volume	332
Cambiare un alias di iniziatore	332
Elimina gli iniziatori	333
Creare e gestire policy QoS del volume	333
Creare una policy QoS	334
Applicare una policy QoS a un volume	334
Modificare l'assegnazione della policy QoS di un volume	335
Modifica una policy QoS	335

Eliminare una policy QoS	336
Monitora il tuo sistema SolidFire con NetApp Hybrid Cloud Control	336
Monitora le risorse di archiviazione sulla dashboard di controllo del cloud ibrido	336
Visualizza il tuo inventario nella pagina Nodi	341
Monitora i volumi sul tuo cluster di archiviazione	343
Raccogliere i registri per la risoluzione dei problemi	344
Gestisci l'archiviazione con Element API	349
Software API Element	349
Scopri come gestire lo storage con Element API	349
Richiedi membri dell'oggetto	353
Membri dell'oggetto di risposta	353
Endpoint della richiesta	354
Autenticazione API	355
Metodi asincroni	355
Attributi	356
Oggetti comuni	357
account	357
authSessionInfo	358
bulkVolumeJob	360
rilegatura (volumi virtuali)	361
certificatoDettagli	362
grappolo	363
ClusterAdmin	365
capacità del cluster	366
clusterConfig	368
clusterInfo	369
clusterPair	371
clusterStats	372
clusterStructure	375
guidare	376
Statistiche di guida	378
errore	381
evento	381
colpa	383
FibreChannelPort	386
fipsErrorNodeReport	387
fipsNodeReport	388
fipsReport	389
groupSnapshot	389
Informazioni hardware	390
host (volumi virtuali)	392
idpConfigInfo	393
iniziatore	394
Autenticazione iSCSI	395
keyProviderKmp	396

keyServerKmpip	396
Configurazione ldap	398
Server di registrazione	399
rete (interfacce vincolate)	400
rete (tutte le interfacce)	404
rete (interfacce Ethernet)	405
rete (interfacce locali)	407
rete (SNMP)	409
interfaccia di rete	410
networkInterfaceStats	410
nodo	411
nodeProtectionDomains	414
nodeStats	414
ontapVersionInfo	416
pendingActiveNode	417
nodo in sospenso	419
protezioneDominio	420
protezioneDomainLevel	421
protezioneDomainResiliency	422
protezioneDominioTolleranza	422
schema di protezioneResilienza	423
schema di protezione Tolleranza	424
protocolloEndpoint	424
Qualità del servizio	425
Politica QoS	426
remoteClusterSnapshotStatus	427
programma	428
sessione (Fibre Channel)	431
sessione (iSCSI)	432
snapMirrorAggregate	435
snapMirrorClusterIdentity	435
snapMirrorEndpoint	436
snapMirrorJobScheduleCronInfo	437
snapMirrorLunInfo	437
snapMirrorNetworkInterface	438
snapMirrorNode	439
snapMirrorPolicy	440
snapMirrorPolicyRule	441
snapMirrorRelationship	442
snapMirrorVolume	445
snapMirrorVolumeInfo	446
snapMirrorVserver	447
snapMirrorVserverAggregateInfo	448
istantanea	449
snmpTrapRecipient	452

contenitore di stoccaggio	452
sincronizzazioneJob	453
attività (volumi virtuali)	456
usmUser	458
rete virtuale	458
volume virtuale	460
volume	461
volumeAccessGroup	465
volumePair	466
volumeStats	468
Metodi comuni	472
OttieniAPI	472
Ottieni risultato asincrono	480
Ottieni statistiche complete	484
Ottieni limiti	484
Ottieni origine	486
Ottieni statistiche grezze	487
ElencoRisultatiAsincroni	488
Metodi API dell'account	491
Aggiungi account	491
OttieniAccountPerID	494
OttieniAccountPerNome	495
Ottieni efficienza dell'account	497
ElencoAccount	498
Modifica Account	501
RimuoviAccount	503
Metodi API dell'amministratore	504
AggiungiClusterAdmin	504
OttieniCurrentClusterAdmin	507
OttieniLoginBanner	508
ListClusterAdmins	509
ModificaClusterAdmin	512
RimuoviClusterAdmin	513
ImpostaLoginBanner	514
Metodi API del cluster	517
Aggiungi nodi	517
ClearClusterFaults	520
CreaPreferenzaInterfacciaCluster	522
DeleteClusterInterfacePreference	523
DisabilitaFunzionalità	524
Abilita funzionalità	525
Ottieni capacità cluster	527
Ottieni soglia completa del cluster	529
OttieniClusterHardwareInfo	535
Ottieni informazioni sul cluster	537

OttieniClusterInterfacePreference	539
OttieniClusterMasterNodeID	540
Ottieni statistiche cluster	541
Ottieni informazioni sulla versione del cluster	542
OttieniStatoFunzionalità	546
Ottieni informazioni sulla sessione di accesso	548
Ottieni informazioni hardware del nodo	550
Ottieni statistiche nodo	551
ListActiveNodes	553
Elenca tutti i nodi	553
ListClusterFaults	555
ListClusterInterfacePreferences	559
ElencoEventi	560
ListNodeStats	563
ElencoISCSISessioni	566
ElencoServizi	568
Elenco nodi in sospeso	570
Elenco nodi attivi in sospeso	572
Modificasoglia completa del cluster	574
ModificaPreferenzaInterfacciaCluster	581
Rimuovi nodi	582
SetLoginSessionInfo	584
Fermare	586
Metodi API per la creazione di cluster	587
CheckProposedCluster	587
Crea cluster	589
OttieniBootstrapConfig	592
Metodi API Drive	596
Aggiungi unità	596
Ottieni informazioni sull'hardware dell'unità	598
Ottieni statistiche di guida	600
ListDrives	603
ListDriveStats	605
Rimuovi unità	607
SecureEraseDrives	609
Metodi API Fibre Channel	610
GetVolumeAccessGroupLunAssignments	610
ListFibreChannelPortInfo	612
ListFibreChannelSessions	616
ListNodeFibreChannelPortInfo	617
ModifyVolumeAccessGroupLunAssignments	619
Metodi API dell'iniziatore	621
CreaIniziatori	622
EliminaIniziatori	626
Iniziatori di elenchi	627

ModificaIniziatori	629
Metodi API LDAP	633
AggiungiLdapClusterAdmin	633
Abilita autenticazione LDAP	635
Disabilita l'autenticazione LDAP	640
OttieniLdapConfiguration	641
TestLdapAuthentication	643
Metodi API di autenticazione a più fattori	645
AddIdpClusterAdmin	645
Crea configurazione Idp	647
DeleteAuthSession	649
DeleteAuthSessionsByClusterAdmin	651
EliminaAuthSessionsByUsername	652
Elimina configurazione Idp	654
Disabilita l'autenticazione Idp	656
Abilita autenticazione Idp	656
Ottieni stato di autenticazione Idp	658
ListActiveAuthSessions	658
ListIdpConfigurations	660
Aggiorna configurazione Idp	661
Metodi API di autenticazione della sessione	664
ListAuthSessionsByClusterAdmin	664
ListAuthSessionsByUsername	666
Metodi API del nodo	668
CheckPingOnVlan	668
CheckProposedNodeAdditions	671
Crea Cluster Support Bundle	674
Crea pacchetto di supporto	677
Elimina tutti i pacchetti di supporto	679
Disabilita modalità manutenzione	680
DisabilitaSsh	683
Abilita modalità di manutenzione	684
AbilitaSsh	687
OttieniClusterConfig	688
Ottieni stato cluster	689
OttieniConfig	691
GetDriveConfig	692
OttieniConfigurazioneHardware	694
Ottieni informazioni sull'hardware	696
OttieniIpmiConfig	698
OttieniIpmiInfo	702
OttieniConfigurazione di rete	706
OttieniInterfaccia di Rete	707
GetNodeActiveTlsCiphers	710
Ottieni report sui drive dei nodi Fips	711

Ottieni certificato SSL nodo	713
GetNodeSupportedTlsCiphers	715
Ottieni informazioni sulla patch	716
Ottieni operazione in sospeso	718
OttieniSshInfo	719
ListDriveHardware	720
ListNetworkInterfaces	723
ListNetworkInterfaceStats	725
ListTests	727
ElencoUtilità	728
RemoveNodeSSLCertificate	729
ResetDrives	730
Reimposta nodo	732
ResetNodeSupplementalTlsCiphers	735
Riavviare la rete	735
Riavvia i servizi	736
ImpostaClusterConfig	738
ImpostaConfig	740
ImpostaConfigurazione di Rete	742
SetNodeSSLCertificate	744
SetNodeSupplementalTlsCiphers	747
Fermare	748
TestConnectEnsemble	750
TestConnectMvip	751
TestConnectSvip	756
Test Drive	761
TestHardwareConfig	762
TestLocateCluster	764
TestLocalConnectivity	765
TestNetworkConfig	768
TestPing	770
TestRemoteConnectivity	774
Metodi API di replicazione	777
Ordine delle operazioni di accoppiamento dei cluster	777
Ordine di accoppiamento dei volumi delle operazioni	778
Modalità di replica supportate per cluster accoppiati	778
CompleteClusterPairing	779
CompleteVolumePairing	780
ListClusterPairs	782
ListActivePairedVolumes	783
Modifica coppia di volumi	786
RimuoviClusterPair	788
RemoveVolumePair	789
StartClusterPairing	790
StartVolumePairing	791

Metodi API di sicurezza	795
AggiungiKeyServerAllProviderKmp	795
CreateKeyProviderKmp	796
CreateKeyServerKmp	798
Crea coppia di chiavi pubbliche e private	801
DeleteKeyProviderKmp	803
DeleteKeyServerKmp	804
Disabilita la crittografia a riposo	805
Abilita crittografia a riposo	806
Ottieni richiesta di firma del certificato del client	808
GetKeyProviderKmp	809
GetKeyServerKmp	811
Ottieni informazioni sulla crittografia software a riposo	812
ListKeyProvidersKmp	814
ListKeyServersKmp	817
ModifyKeyServerKmp	820
RekeySoftwareEncryptionAtRestMasterKey	823
RemoveKeyServerFromProviderKmp	826
SignSshKeys	827
TestKeyProviderKmp	831
TestKeyServerKmp	832
Metodi API SnapMirror	833
AbortSnapMirrorRelationship	833
BreakSnapMirrorRelationship	834
BreakSnapMirrorVolume	835
CreaSnapMirrorEndpoint	837
CreateSnapMirrorEndpointUnmanaged	838
Crea relazioneSnapMirror	838
CreaSnapMirrorVolume	840
DeleteSnapMirrorEndpoints	842
EliminaSnapMirrorRelazioni	842
GetOntapVersionInfo	843
OttieniSnapMirrorClusterIdentity	844
InizializzaSnapMirrorRelationship	845
ListSnapMirrorAggregates	846
ListSnapMirrorEndpoints	847
ListSnapMirrorLuns	848
ListSnapMirrorNetworkInterfaces	848
ListSnapMirrorNodes	849
ListSnapMirrorPolicies	850
ListSnapMirrorSchedules	851
ListSnapMirrorRelationships	852
ListSnapMirrorVolumes	853
ListSnapMirrorVservers	854
ModificaSnapMirrorEndpoint	855

ModifySnapMirrorEndpoint (non gestito)	856
Modificare la relazione SnapMirror	857
Aggiorna relazione SnapMirror	858
QuiesceSnapMirrorRelationship	859
ResumeSnapMirrorRelationship	860
ResyncSnapMirrorRelationship	861
Metodi API di configurazione del sistema	862
DisabilitaBmcColdReset	862
DisabilitaClusterSsh	863
Disabilita Snmp	865
AbilitaBmcColdReset	866
AbilitaClusterSsh	867
AbilitaSnmp	869
OttieniBinAssignmentProperties	870
OttieniClusterSshInfo	873
OttieniStrutturaCluster	874
OttieniFipsReport	875
OttieniLldpConfig	877
OttieniLldpInfo	878
Ottieni report sui drive dei nodi Fips	879
Ottieni informazioni Ntp	880
Ottieni informazioni Nvram	882
OttieniProtectionDomainLayout	883
OttieniHost di registrazione remoti	885
OttieniSnmpACL	886
OttieniSnmpInfo	887
OttieniSnmpState	889
OttieniSnmpTrapInfo	891
Ottieni certificato SSL	892
ListProtectionDomainLevels	894
RimuoviCertificatoSSL	896
ReimpostaConfigurazioneRete	897
ResetSupplementalTlsCiphers	898
ImpostaStrutturaCluster	899
ImpostaLldpConfig	900
ImpostaNtpInfo	901
ImpostaProtezioneDominioLayout	903
Imposta host di registrazione remoti	906
SetSnmpACL	907
ImpostaSnmpInfo	909
ImpostaSnmpTrapInfo	912
SetSSLCertificate	914
SnmpSendTestTraps	916
Disponibilità dell'indirizzo di prova	917
Metodi API di rete multitenant	919

Convenzioni di denominazione delle reti virtuali	919
AggiungiVirtualNetwork	919
Modificare la rete virtuale	922
ElencoRetiVirtuali	926
RimuoviVirtualNetwork	928
Metodi API del volume	929
AnnullaClona	929
AnnullaGruppoClona	930
Clona più volumi	931
CloneVolume	935
CopiaVolume	940
Crea politica QoS	942
Crea volume	944
Crea destinazione di backup	952
Elimina QoSPolicy	953
Elimina volume	954
EliminaVolumi	957
Ottieni destinazione di backup	959
Ottieni statistiche sul volume	961
OttieniQoS predefinito	963
Ottieni la politica QoSPolicy	965
OttieniConteggioVolume	967
OttieniEfficienzaVolume	968
ListActiveVolumes	969
ListBackupTargets	971
ListBulkVolumeJobs	972
ElencoVolumiEliminati	974
ListQoS Policies	977
ListSyncJobs	979
ElencoVolumeQoSHistogrammi	981
ElencoVolumi	983
ListVolumeStats	987
ListVolumesForAccount	989
ListVolumeStatsByAccount	992
ListVolumeStatsByVirtualVolume	993
ListVolumeStatsByVolume	996
ListVolumeStatsByVolumeAccessGroup	998
Modifica destinazione backup	1000
Modifica politica QoS	1002
ModificaVolume	1004
ModificaVolumi	1013
PurgeDeletedVolume	1022
Elimina i volumi eliminati	1023
RimuoviBackupTarget	1025
RipristinaVolumeEliminato	1026

Imposta QoS predefinito	1027
StartBulkVolumeRead	1028
StartBulkVolumeWrite	1031
AggiornaStatoVolumeMassuale	1034
Metodi API del gruppo di accesso al volume	1036
AggiungiIniziatoriAlGruppoAccessoVolume	1036
AggiungiVolumiAlGruppoAccessoVolumi	1039
Crea gruppo di accesso al volume	1040
DeleteVolumeAccessGroup	1043
ListVolumeAccessGroups	1045
RimuoviVolumiDaVolumeAccessGroup	1047
RemoveInitiatorsFromVolumeAccessGroup	1049
ModificaVolumeAccessGroup	1052
GetVolumeAccessGroupEfficiency	1055
Metodi API per snapshot del volume	1057
Panoramica delle istantanee	1057
Crea istantanea di gruppo	1058
Crea programma	1064
Crea istantanea	1077
EliminaSnapshot di Gruppo	1083
EliminaSnapshot	1085
Ottieni pianificazione	1086
ListGroupSnapshots	1088
ListSchedules	1091
ListSnapshots	1093
ModificaSnapshotGruppo	1095
Modifica pianificazione	1099
ModificaSnapshot	1106
RollbackToGroupSnapshot	1110
RollbackToSnapshot	1115
Metodi API del volume virtuale	1118
Crea contenitore di archiviazione	1118
Elimina contenitori di archiviazione	1119
Ottieni efficienza del contenitore di archiviazione	1120
OttieniConteggioVolumeVirtuale	1122
ListProtocolEndpoints	1123
ListStorageContainers	1126
ListVirtualVolumeBindings	1127
ListVirtualVolumeHosts	1129
ListVirtualVolumes	1130
ListVirtualVolumeTasks	1134
ModificaContenitore di archiviazione	1135
Controllo degli accessi	1137
conti	1137
amministratore	1138

ClusterAdmin	1138
unità	1141
nodi	1141
Leggere	1142
segnalazione	1143
repository	1145
volumi	1145
scrivere	1146
Esempi di risposta	1147
OttieniConfig	1147
OttieniClusterHardwareInfo	1150
OttieniLldpInfo	1164
OttieniConfigurazione di rete	1193
GetNodeHardwareInfo (output per iSCSI)	1197
GetNodeHardwareInfo (output per i nodi Fibre Channel)	1199
Ottieni informazioni Nvram	1206
ListActiveNodes	1215
ListActiveVolumes	1218
TestHardwareConfig	1228
Plug-in NetApp Element per vCenter Server	1234
Per maggiori informazioni	1234
Archiviazione del monitor con SolidFire Active IQ	1235
Per maggiori informazioni	1235
Lavorare con il nodo di gestione	1236
Panoramica del nodo di gestione	1236
Installa o ripristina un nodo di gestione	1237
Installa un nodo di gestione	1237
Creare un ruolo NetApp HCC in vCenter	1243
Configurare un controller di interfaccia di rete (NIC) di archiviazione	1249
Recupera un nodo di gestione	1251
Accedi al nodo di gestione	1256
Accedi all'interfaccia utente per nodo di gestione	1256
Accedi all'interfaccia utente dell'API REST del nodo di gestione	1257
Modificare il certificato SSL predefinito del nodo di gestione	1258
Trova maggiori informazioni	1259
Lavorare con l'interfaccia utente del nodo di gestione	1259
Panoramica dell'interfaccia utente del nodo di gestione	1259
Configurare il monitoraggio degli avvisi	1260
Modificare e testare le impostazioni di rete, cluster e sistema del nodo di gestione	1260
Eseguire le utilità di sistema dal nodo di gestione	1262
Lavorare con l'API REST del nodo di gestione	1263
Panoramica dell'interfaccia utente dell'API REST del nodo di gestione	1263
Ottieni l'autorizzazione per utilizzare le API REST	1264
Abilita il monitoraggio Active IQ e NetApp	1265
Configurare NetApp Hybrid Cloud Control per più vCenter	1267

Aggiungere una risorsa controller al nodo di gestione	1268
Creare e gestire risorse di cluster di archiviazione	1270
Visualizza o modifica le risorse del controller esistenti	1275
Configurare un server proxy	1277
Verificare le versioni del sistema operativo e dei servizi del nodo di gestione	1278
Ottenere i log dai servizi di gestione	1279
Gestisci le connessioni di supporto	1281
Accesso ai nodi di archiviazione tramite SSH per la risoluzione dei problemi di base	1281
Avvia una sessione di supporto NetApp remota	1285
Gestire la funzionalità SSH sul nodo di gestione	1286
Aggiorna il tuo sistema di archiviazione all-flash NetApp SolidFire	1290
Panoramica della sequenza di aggiornamento	1290
Sequenza di aggiornamento del sistema	1291
Procedure di aggiornamento del sistema	1292
Eseguire controlli di integrità dell'archiviazione Element prima di aggiornare l'archiviazione	1292
Aggiornare un nodo di gestione	1297
Servizi di gestione degli aggiornamenti	1301
Aggiorna il software Element	1304
Aggiorna il firmware di archiviazione	1315
Aggiorna il plug-in Element per vCenter Server	1325
Aggiorna i tuoi componenti vSphere per un sistema di storage NetApp SolidFire con Element Plug-in per vCenter Server	1332
Trova maggiori informazioni	1333
Versioni precedenti della documentazione del software SolidFire e NetApp Element	1334
Per maggiori informazioni	1334
Note legali	1335
Copyright	1335
Marchi	1335
Brevetti	1335
Politica sulla riservatezza	1335
Open source	1335

Documentazione del software SolidFire ed Element

Note di rilascio

Informazioni sulla versione attuale e precedente

Puoi trovare i link alle note di rilascio più recenti e precedenti per vari componenti dell'ambiente di archiviazione Element.



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

Software NetApp Element

- ["Note sulla versione NetApp Element Software 12.8"](#)
- ["Note sulla versione NetApp Element Software 12.7"](#)
- ["Note sulla versione NetApp Element Software 12.5"](#)
- ["Note sulla versione NetApp Element Software 12.3.2"](#)
- ["Note sulla versione NetApp Element Software 12.3.1"](#)
- ["Note sulla versione NetApp Element Software 12.3"](#)
- ["Note sulla versione NetApp Element Software 12.2.1"](#)
- ["Note sulla versione NetApp Element Software 12.2"](#)
- ["Note sulla versione 12.0.1 NetApp Element Software"](#)
- ["Note sulla versione NetApp Element Software 12.0"](#)
- ["Note sulla versione NetApp Element Software 11.8.2"](#)
- ["Note sulla versione NetApp Element Software 11.8.1"](#)
- ["Note sulla versione NetApp Element Software 11.8"](#)
- ["Note sulla versione NetApp Element Software 11.7"](#)
- ["Note sulla versione NetApp Element Software 11.5.1"](#)
- ["Note sulla versione NetApp Element Software 11.3P1"](#)

Servizi di gestione

- ["Note sulla versione dei servizi di gestione"](#)

Plug-in NetApp Element per vCenter Server

- ["Note sulla versione del plug-in vCenter 5.5"](#) *Nuovo*
- ["Note sulla versione del plug-in vCenter 5.4"](#)
- ["Note sulla versione del plug-in vCenter 5.3"](#)
- ["Note sulla versione del plug-in vCenter 5.2"](#)
- ["Note sulla versione del plug-in vCenter 5.1"](#)
- ["Note sulla versione del plug-in vCenter 5.0"](#)
- ["Note sulla versione del plug-in vCenter 4.10"](#)

- ["Note sulla versione del plug-in vCenter 4.9"](#)
- ["Note sulla versione del plug-in vCenter 4.8"](#)
- ["Note sulla versione del plug-in vCenter 4.7"](#)
- ["Note sulla versione del plug-in vCenter 4.6"](#)
- ["Note sulla versione del plug-in vCenter 4.5"](#)
- ["Note sulla versione del plug-in vCenter 4.4"](#)
- ["Note sulla versione del plug-in vCenter 4.3"](#)

Firmware di archiviazione

- ["Note sulla versione del firmware di archiviazione 2.182.0"](#)**NUOVO**
- ["Note sulla versione del firmware di archiviazione 2.175.0"](#)
- ["Note sulla versione del firmware di archiviazione 2.164.0"](#)
- ["Note sulla versione del pacchetto firmware di archiviazione 2.150"](#)
- ["Note sulla versione del pacchetto firmware di archiviazione 2.146"](#)
- ["Note sulla versione del firmware di archiviazione 2.99.2"](#)
- ["Note sulla versione del pacchetto firmware di archiviazione 2.76"](#)
- ["Note sulla versione 2.27 del pacchetto firmware di archiviazione"](#)
- ["Note sulla versione H610S BMC 3.84.07"](#)
- ["Versioni supportate del firmware e del driver ESXi"](#)**NUOVO**

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Novità nel software Element

NetApp aggiorna periodicamente i software SolidFire ed Element per offrirti nuove funzionalità, miglioramenti e correzioni di bug. Element 12.8 è la versione più recente e include aggiornamenti dei componenti di sistema e di sicurezza, miglioramenti operativi e problemi risolti.



Gli aggiornamenti cumulativi di software e firmware vengono installati come parte di un aggiornamento di Element 12.8 basato sulla versione corrente di Element in esecuzione su un cluster di storage. Ad esempio, se un cluster esegue attualmente Element 12.5, è possibile eseguire l'aggiornamento direttamente a Element 12.8 per ottenere gli aggiornamenti cumulativi sia da Element 12.7 che da Element 12.8. Per i percorsi di aggiornamento supportati, consultare l'articolo della Knowledge Base ["Qual è la matrice di aggiornamento per i cluster di storage che eseguono il software NetApp Element ?"](#).

Elemento 12.8

Scopri di più sulle novità di Element 12.8.

Bilanciamento del carico del volume

L'elemento 12.8 introduce la funzionalità Volume Load Balancing. È possibile utilizzare questa funzionalità per bilanciare i volumi tra i nodi in base al livello IOPS effettivo di ciascun volume anziché in base al minimo IOPS configurato nella policy QoS. È possibile utilizzare la funzionalità Volume Load Balancing solo per bilanciare i volumi. Non è possibile utilizzarlo per bilanciare i volumi virtuali. Per impostazione predefinita, la funzionalità di bilanciamento del carico del volume è disabilitata. È possibile abilitarlo e disabilitarlo utilizzando `VolumeLoadBalanceOnActualIOPS` Parametro API con il ["Abilita funzionalità"](#) E ["Disabilita Funzionalità"](#) Metodi API o utilizzando il ["Bilanciamento del carico del volume"](#) opzione nell'interfaccia utente dell'elemento.

Visualizza le informazioni sull'utilizzo del nodo

Con Element 12.8, è possibile visualizzare le informazioni sull'utilizzo del nodo come `nodeHeat` utilizzando il `getNodeStats` E `listNodeStats` Metodi API. IL `nodeHeat` l'oggetto è un membro del `nodeStats` oggetto e visualizza le informazioni sull'utilizzo del nodo in base al rapporto tra IOPS totali primari o IOPS totali e IOPS configurati, calcolati in media nel tempo.

Inoltre, è possibile visualizzare l'utilizzo del nodo come percentuale di `recentPrimaryTotalHeat` nella visualizzazione Dettagli visualizzazione per un nodo nell'interfaccia utente Elemento.

Visualizza le statistiche I/O per un volume

Con Element 12.8, è possibile visualizzare le statistiche di utilizzo I/O per un volume come `sliceIopsStats` utilizzando il `getVolumeStats` E `listVolumeStatsByVolume` Metodi API. Le statistiche I/O vengono calcolate utilizzando le informazioni IOPS di lettura e scrittura per il volume e misurate su due periodi di tempo: le ultime 24 ore e l'ultima ora. ["Saperne di più"](#).

Algoritmo CHAP per sessione iSCSI

Un iniziatore iSCSI host richiede un elenco di algoritmi CHAP (Challenge-Handshake Authentication Protocol) da utilizzare quando crea una sessione iSCSI con una destinazione iSCSI Element. A partire da Element 12.8, è possibile visualizzare l'algoritmo CHAP supportato che la destinazione Element iSCSI sceglie di utilizzare per una sessione iSCSI.

Aggiorna la versione hardware della VM

Se si esegue un aggiornamento sul posto di un nodo di gestione esistente a Element 12.8, prima di eseguire l'aggiornamento è necessario assicurarsi che la versione hardware della VM sul nodo di gestione sia compatibile con ESXi 6.7 (versione hardware della VM 14) o successiva, a seconda dell'ambiente. ["Saperne di più"](#).

Elemento 12.7

Scopri di più sulle novità di Element 12.7.

Algoritmi CHAP sicuri

Element 12.7 include il supporto per gli algoritmi CHAP (Challenge-Handshake Authentication Protocol) sicuri e conformi allo standard FIPS SHA1, SHA-256 e SHA3-256. ["Saperne di più"](#).

Velocità di sincronizzazione dinamica dei blocchi (bin)

Le operazioni del cluster, come aggiunte, aggiornamenti o manutenzione dei nodi, oppure l'aggiunta di unità e così via, attivano la sincronizzazione dei blocchi (bin) per distribuire i dati dei blocchi ai nodi nuovi o aggiornati

in un layout del cluster. L'utilizzo di una singola velocità lenta come velocità di sincronizzazione predefinita fa sì che queste operazioni richiedano molto tempo e non sfruttano la maggiore potenza di elaborazione dei nodi più grandi. A partire da Element 12.7, la velocità di sincronizzazione viene regolata dinamicamente in base al numero di core sul nodo di archiviazione, consentendo di eseguire queste operazioni in modo notevolmente più rapido.

Ad esempio, quando si aggiungono grandi nodi di archiviazione a 28 core (H610S, SF19210 e SF38410) che eseguono Element 12.7 a un cluster esistente, la velocità di sincronizzazione dei dati si regola automaticamente su 110 Mbps anziché 60 Mbps. Inoltre, quando si esce dalla modalità di manutenzione dei nodi per questi grandi nodi di storage, ad esempio durante un aggiornamento da Element 12.3.x o versione successiva a Element 12.7 utilizzando NetApp Hybrid Cloud Control, la velocità di sincronizzazione per la velocità dei dati dei blocchi modificata si regola automaticamente su 110 Mbps anziché 20 Mbps.

Quando si aggiungono i nodi di storage medi a 16 core (H410S) e i nodi di storage piccoli a 12 core (SF4805) a un cluster Element 12.7, la velocità di sincronizzazione dei dati rimane a 60 Mbps; tuttavia, per la sincronizzazione dei blocchi modificati quando vengono disattivati dalla modalità di manutenzione dei nodi durante gli aggiornamenti da Element 12.3.x a Element 12.7, la velocità di sincronizzazione si regola automaticamente da 20 Mbps a 60 Mbps per i nodi di storage medi e 40 Mbps per i nodi di storage più piccoli.

Quando si rimuovono i nodi di archiviazione, non vi è alcun impatto sulla velocità di sincronizzazione dei blocchi, evitando così ripercussioni sulle prestazioni dell'I/O del client.

Miglioramento della raccolta dei rifiuti

Per i cluster con nodi di archiviazione più grandi, ad esempio un H610S-4, che hanno 1 PB di spazio utilizzato, eseguono carichi di lavoro molto elevati con sovrascritture e hanno un'elevata deduplicazione e compressione, l'operazione di Garbage Collection può ora tenere il passo poiché la dimensione predefinita del filtro Bloom è stata aumentata per i nodi più grandi da 700 GB o più di memoria a 1048576 bit. Questa modifica ha effetto automaticamente dopo l'aggiornamento dei nodi di archiviazione a Element 12.7 e non ha alcun impatto sui nodi più piccoli.

Miglioramento della scala

Con Element 12.7 non è più necessario seguire una sequenza specifica quando si aggiungono più nodi di archiviazione di unità di blocchi e metadati a un cluster esistente. Utilizzando l'interfaccia utente o l'API di Element, puoi semplicemente selezionare tutte le unità disponibili e aggiungerle simultaneamente in blocco. L'elemento 12.7 gestisce automaticamente la sincronizzazione dei dati in modo che tutti i servizi di blocco vengano sincronizzati simultaneamente. Quando i servizi di blocco per ciascun nodo completano la sincronizzazione, l'unità metadati su quel nodo diventa assegnabile ai volumi host. Questo miglioramento della scalabilità riduce significativamente la latenza della risposta di lettura e previene il degrado delle prestazioni durante la sincronizzazione dei dati tra i nuovi nodi di archiviazione aggiunti.

Aggiornamenti del firmware del nodo di archiviazione

Element 12.7 include il bundle firmware di archiviazione versione 2.164.0, che include il supporto per i nuovi componenti di sistema. ["Saperne di più"](#).



Non ci sono nuovi aggiornamenti del firmware nella versione Element 12.7. Tuttavia, in base al pacchetto firmware corrente in esecuzione sui nodi di archiviazione, gli aggiornamenti cumulativi vengono installati quando si esegue l'aggiornamento a Element 12.7.

Documentazione di SolidFire Active IQ

Nell'interfaccia utente SolidFire Active IQ, ora puoi accedere alla pagina Gestione QoS per visualizzare

consigli e informazioni sulla limitazione dei nodi per il tuo cluster. Inoltre, la dashboard del cluster ora visualizza il conteggio totale degli snapshot. Altri miglioramenti recenti includono l'aggiunta di informazioni sui nodi primari e secondari per i volumi attivi e la velocità effettiva media, gli IOPS e la latenza media per gli ultimi 30 minuti sui volumi primari di un nodo.

Ora è possibile accedere alla documentazione SolidFire Active IQ dalla documentazione del software Element. ["Saperne di più"](#).

NetApp Bugs Online contiene problemi risolti e noti

I problemi risolti e noti sono elencati nello strumento NetApp Bugs Online. Puoi consultare questi numeri per il software Element e altri prodotti su ["Bug NetApp online"](#).

Elemento 12.5

Scopri di più sulle novità di Element 12.5.

Accesso migliorato al nodo di archiviazione

Element 12.5 offre un accesso remoto migliorato ai singoli nodi mediante certificati SSH firmati. Per fornire un accesso remoto sicuro ai nodi di archiviazione, è stato creato un nuovo account utente locale con privilegi limitati denominato `sfreadonly` viene ora creato durante l'RTFI di un nodo di archiviazione. IL `sfreadonly` L'account consente l'accesso al backend del nodo di archiviazione per scopi di manutenzione di base o risoluzione dei problemi. Ora puoi configurare il `supportAdmin` tipo di accesso per un utente amministratore del cluster per consentire al supporto NetApp di accedere al cluster in base alle necessità.

Gestibilità migliorata dei domini di protezione personalizzati

Element 12.5 è dotato di una nuova interfaccia utente che consente di visualizzare in modo rapido e semplice i domini di protezione personalizzati esistenti e di configurarne di nuovi.

Nuovi e migliorati guasti, eventi e avvisi del cluster

Element 12.5 migliora la risoluzione dei problemi del sistema con l'introduzione dei nuovi codici di errore del cluster `BmcSelfTestFailed` `E CpuThermalEventThreshold`. L'elemento 12.5 contiene anche miglioramenti di robustezza per gli eventi e gli avvisi del cluster esistenti, come `nodeOffline`, `volumeOffline`, `driveHealthFault`, `networkEvent`, `E cSumEvent`.

Abilita la crittografia software a riposo dall'interfaccia utente Crea cluster

Con l'aggiunta di una nuova casella di controllo nell'interfaccia utente Crea cluster, Element 12.5 offre la possibilità di abilitare la crittografia software a riposo per l'intero cluster per i cluster di archiviazione all-flash SolidFire durante la creazione del cluster.

Aggiornamenti del firmware del nodo di archiviazione

Element 12.5 include aggiornamenti del firmware per i nodi di archiviazione. ["Saperne di più"](#).

Sicurezza migliorata

Element 12.5 contiene la mitigazione che chiude l'esposizione del software Element alla vulnerabilità Apache Log4j. I cluster di storage NetApp SolidFire con la funzionalità Virtual Volumes (VVols) abilitata sono esposti alla vulnerabilità Apache Log4j. Per informazioni sulla soluzione alternativa alla vulnerabilità Apache Log4j nel software NetApp Element, consultare l'[articolo della KB](#).

Se stai utilizzando Element 11.x, 12.0 o 12.2 o se il tuo cluster di archiviazione è già Element 12.3 o 12.3.1 con la funzionalità VVols abilitata, dovresti eseguire l'aggiornamento alla versione 12.5.

Element 12.5 include anche più di 120 soluzioni per le vulnerabilità di sicurezza CVE.

Trova maggiori informazioni

- ["Note sulla versione dei servizi di controllo e gestione del cloud ibrido NetApp"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Centro di documentazione SolidFire ed Element Software per le versioni precedenti"](#)
- ["Documentazione NetApp HCI"](#)
- ["Versioni del firmware di archiviazione supportate per i nodi di archiviazione SolidFire"](#)

Concetti

Apprendi i concetti di base relativi al software Element.

- ["Panoramica del prodotto"](#)
- [Panoramica dell'architettura SolidFire](#)
- [Nodi](#)
- [Cluster](#)
- ["Sicurezza"](#)
- [Account e permessi](#)
- ["Volumi"](#)
- [Protezione dei dati](#)
- [Prestazioni e qualità del servizio](#)

Panoramica del prodotto

Un sistema di archiviazione all-flash SolidFire è composto da componenti hardware discreti (unità e nodi) combinati in un unico pool di risorse di archiviazione. Questo cluster unificato si presenta come un singolo sistema di archiviazione utilizzabile da client esterni ed è gestito tramite il software NetApp Element .

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

Caratteristiche SolidFire

Un sistema Solidfire offre le seguenti caratteristiche:

- Offre storage ad alte prestazioni per la tua infrastruttura cloud privata su larga scala
- Fornisce una scala flessibile che consente di soddisfare le mutevoli esigenze di archiviazione
- Utilizza un'interfaccia software Element per la gestione dell'archiviazione basata su API
- Garantisce le prestazioni utilizzando le politiche di qualità del servizio
- Include il bilanciamento automatico del carico su tutti i nodi del cluster
- Riequilibra automaticamente i cluster quando vengono aggiunti o sottratti nodi

Distribuzione di SolidFire

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

["Panoramica dell'architettura di archiviazione all-flash SolidFire"](#)

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)

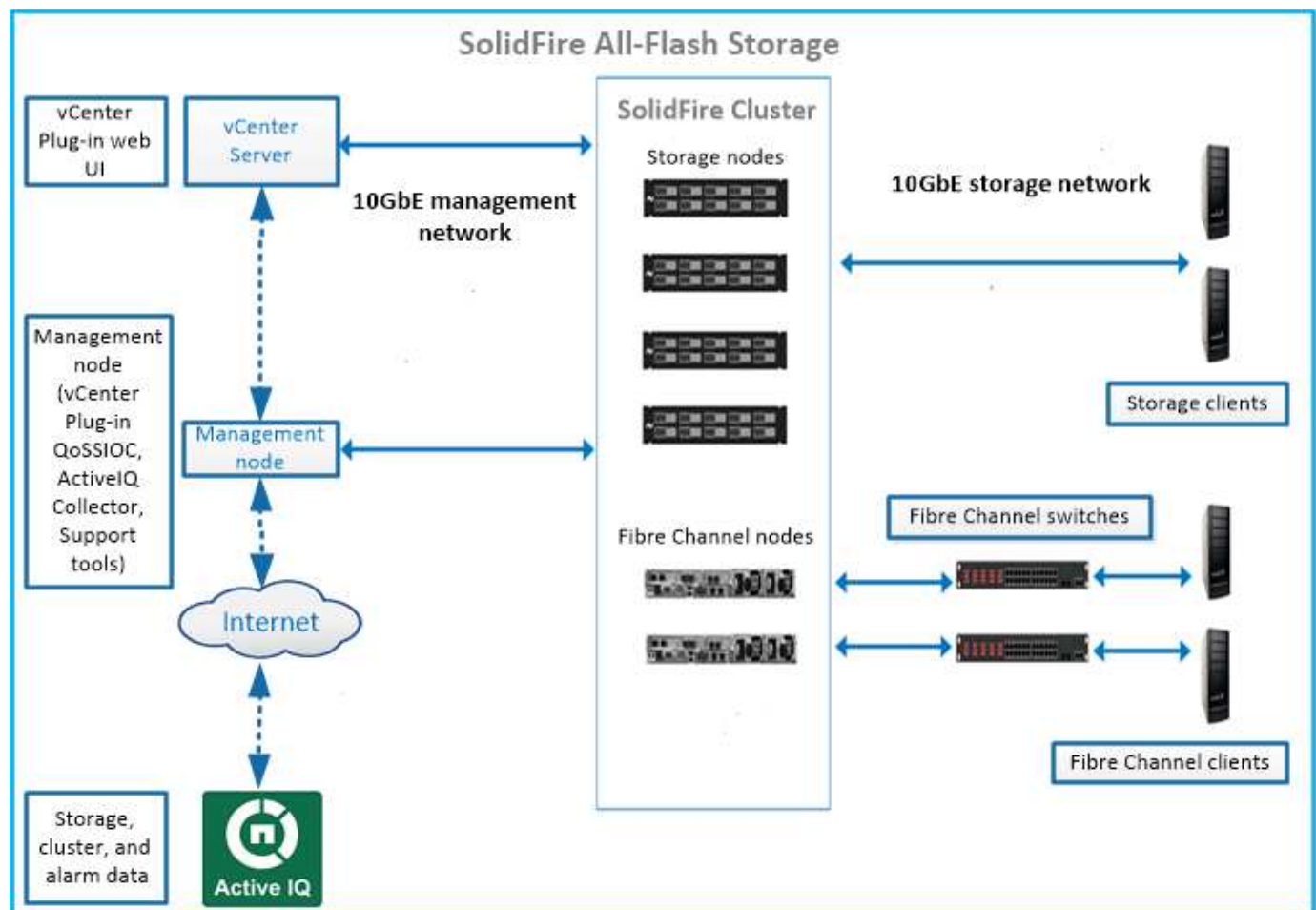
Architettura e componenti

Scopri di più sull'architettura SolidFire

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

Un sistema di archiviazione SolidFire include i seguenti componenti hardware:

- **Cluster:** l'hub del sistema di archiviazione SolidFire, ovvero un insieme di nodi.
- **Nodi:** i componenti hardware raggruppati in un cluster. Esistono due tipi di nodi:
 - Nodi di archiviazione, che sono server contenenti una raccolta di unità
 - Nodi Fibre Channel (FC), che utilizzi per connetterti ai client FC
- **Unità:** utilizzate nei nodi di archiviazione per archiviare i dati per il cluster. Un nodo di archiviazione contiene due tipi di unità:
 - Le unità metadati del volume archiviano informazioni che definiscono i volumi e altri oggetti all'interno di un cluster.
 - Le unità a blocchi memorizzano blocchi di dati per i volumi.



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

- ["Interfacce software SolidFire"](#)
- ["SolidFire Active IQ"](#)
- ["Nodo di gestione per il software Element"](#)
- ["Servizi di gestione"](#)

URL comuni

Ecco gli URL più comuni utilizzati con un sistema di archiviazione all-flash SolidFire :

URL	Descrizione
<code>https://[storage cluster MVIP address]</code>	Accedi all'interfaccia utente del software NetApp Element .
https://activeiq.solidfire.com	Monitora i dati e ricevi avvisi su eventuali colli di bottiglia nelle prestazioni o potenziali problemi di sistema.
<code>https://[management node IP address]</code>	Accedi a NetApp Hybrid Cloud Control per aggiornare l'installazione dello storage e i servizi di gestione.
<code>https://[IP address]:442</code>	Dall'interfaccia utente per nodo, accedi alle impostazioni di rete e cluster e utilizza test e utilità di sistema. "Saperne di più."
<code>https://[management node IP address]/mnode</code>	Utilizzare i servizi di gestione REST API e altre funzionalità dal nodo di gestione. "Saperne di più."
<code>https://[management node IP address]:9443</code>	Registrare il pacchetto vCenter Plug-in in vSphere Web Client. "Saperne di più."

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Interfacce software SolidFire

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

Opzioni

- [Interfaccia utente del software NetApp Element](#)
- [API del software NetApp Element](#)
- [Plug-in NetApp Element per vCenter Server](#)
- [Controllo del cloud ibrido NetApp](#)
- [Interfacce utente dei nodi di gestione](#)
- [Ulteriori utilità e strumenti di integrazione](#)

Interfaccia utente del software NetApp Element

Consente di configurare l'archiviazione Element, monitorare la capacità e le prestazioni del cluster e gestire l'attività di archiviazione in un'infrastruttura multi-tenant. Element è il sistema operativo di archiviazione 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 risorse presentate come un unico sistema di archiviazione ai client esterni. Element Software è responsabile del coordinamento, della scalabilità e della gestione del cluster nel suo complesso. L'interfaccia software è basata sull'API Element.

["Gestisci lo storage con il software Element"](#)

API del software NetApp Element

Consente di utilizzare un set di oggetti, metodi e routine per gestire l'archiviazione degli elementi. L'API Element si basa sul protocollo JSON-RPC su HTTPS. È possibile monitorare le operazioni API nell'interfaccia utente dell'elemento abilitando il registro API; ciò consente di visualizzare i metodi che vengono inviati al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi emessi.

["Gestisci l'archiviazione con l'API Element"](#)

Plug-in NetApp Element per vCenter Server

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

["Plug-in NetApp Element per vCenter Server"](#)

Controllo del cloud ibrido NetApp

Consente di aggiornare i servizi di archiviazione e gestione di Element e di gestire le risorse di archiviazione tramite l'interfaccia NetApp Hybrid Cloud Control.

["Gestisci e monitora lo storage con NetApp Hybrid Cloud Control"](#)

Interfacce utente dei nodi 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 dei test e delle utilità del sistema operativo. Dall'interfaccia utente dell'API REST è possibile accedere a un menu di API correlate ai servizi che controllano le funzionalità del sistema basate sui servizi dal nodo di gestione.

Ulteriori utilità e strumenti di integrazione

Sebbene in genere si gestisca l'archiviazione con NetApp Element, NetApp Element API e NetApp Element Plug-in per vCenter Server, è possibile utilizzare utilità e strumenti di integrazione aggiuntivi per accedere all'archiviazione.

Elemento CLI

["Elemento CLI"](#) consente di controllare un sistema di archiviazione SolidFire tramite un'interfaccia a riga di comando senza dover ricorrere all'API Element.

Strumenti PowerShell per gli elementi

"[Strumenti PowerShell per gli elementi](#)" consentono di utilizzare una raccolta di funzioni di Microsoft Windows PowerShell che utilizzano l'API Element per gestire un sistema di archiviazione SolidFire .

SDK di elementi

"[SDK di elementi](#)" ti consentono di gestire il tuo cluster SolidFire utilizzando questi 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 SolidFire Postman

Consente ai programmatori di utilizzare una raccolta di "[Postino](#)" funzioni che testano le chiamate API dell'elemento.

Adattatore di replicazione dello storage SolidFire

"[Adattatore di replicazione dello storage SolidFire](#)" si integra con VMware Site Recovery Manager (SRM) per abilitare la comunicazione con i cluster di storage SolidFire replicati ed eseguire i flussi di lavoro supportati.

SolidFire vRO

"[SolidFire vRO](#)" fornisce un modo pratico per utilizzare l'API Element per amministrare il sistema di archiviazione SolidFire con VMware vRealize Orchestrator.

Fornitore SolidFire VSS

"[Fornitore SolidFire VSS](#)" integra copie shadow VSS con snapshot e cloni di Element.

Trova maggiori informazioni

- "[Documentazione del software SolidFire ed Element](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"

SolidFire Active IQ

"[SolidFire Active IQ](#)" è uno strumento basato sul Web che fornisce visualizzazioni storiche costantemente aggiornate dei dati dell'intero cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le prestazioni e la capacità del sistema, nonché di rimanere informati sullo stato di salute del cluster.

Puoi trovare le seguenti informazioni sul tuo sistema in SolidFire Active IQ:

- Numero di nodi e stato dei nodi: integri, offline o guasti
- Rappresentazione grafica dell'utilizzo della CPU, della memoria e della limitazione dei nodi

- Dettagli sul nodo, come numero di serie, posizione dello slot nello chassis, modello e versione del software NetApp Element in esecuzione sul nodo di storage
- Informazioni relative alla CPU e allo storage delle macchine virtuali

Per saperne di più su SolidFire Active IQ, vedere ["Documentazione di SolidFire Active IQ"](#) .

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- [Sito di supporto NetApp](#) > [Strumenti per Active IQ](#)

Nodo di gestione per il software Element

IL ["nodo di gestione \(mNode\)"](#) è una macchina virtuale che viene eseguita in parallelo con uno o più cluster di archiviazione basati sul 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 utilità di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi.

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

A partire dalla versione Element 11.3, il nodo di gestione funziona come host di microservizi, consentendo aggiornamenti più rapidi di servizi software selezionati al di fuori delle versioni principali. Questi microservizi o ["servizi di gestione"](#) vengono aggiornati frequentemente come pacchetti di servizi.

Servizi di gestione per l'archiviazione all-flash SolidFire

A partire dalla versione 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 versioni principali.

I servizi di gestione forniscono funzionalità di gestione centralizzata ed estesa per l'archiviazione all-flash SolidFire . Questi servizi includono ["Controllo del cloud ibrido NetApp"](#) , Telemetria del sistema Active IQ , registrazione e aggiornamenti del servizio, nonché il servizio QoSSIOC per Element Plug-in per vCenter.



Scopri di più su ["rilasci di servizi di gestione"](#) .

Nodi

I nodi sono risorse hardware o virtuali raggruppate in un cluster per fornire capacità di elaborazione e di archiviazione a blocchi.

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

- [Nodo di gestione](#)

- [Nodo di archiviazione](#)
- [Nodo Fibre Channel](#)

[Stati dei nodi](#) variano a seconda dell'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 risorse e impostazioni del cluster, eseguire test e utilità di sistema e abilitare l'accesso al supporto NetApp per la risoluzione dei problemi. ["Saperne di più"](#)

Nodo di archiviazione

Un nodo di archiviazione SolidFire è un server contenente una raccolta di unità che comunicano tra loro tramite l'interfaccia di rete Bond10G. Le unità nel nodo contengono spazio di blocchi e metadati per l'archiviazione e la gestione dei dati. Ogni nodo contiene un'immagine di fabbrica del software NetApp Element .

I nodi di archiviazione presentano le seguenti caratteristiche:

- Ogni nodo ha un nome univoco. Se un nome di nodo non viene specificato da un amministratore, il valore predefinito è SF-XXXX, dove XXXX rappresenta quattro caratteri casuali generati dal sistema.
- Ogni nodo ha la propria cache di scrittura NVRAM(non-volatile random access memory) ad alte prestazioni per migliorare le prestazioni complessive del sistema e ridurre la latenza di scrittura.
- Ogni nodo è collegato a due reti, una di archiviazione e una di gestione, ciascuna con due collegamenti indipendenti per garantire ridondanza e prestazioni. Ogni nodo richiede un indirizzo IP su ogni rete.
- È possibile creare un cluster con nuovi nodi di archiviazione oppure aggiungere nodi di archiviazione a un cluster esistente per aumentare la capacità e le prestazioni di archiviazione.
- È possibile aggiungere o rimuovere nodi dal cluster in qualsiasi momento senza interrompere il servizio.

Nodo Fibre Channel

I nodi SolidFire Fibre Channel forniscono connettività a uno switch Fibre Channel, al quale è possibile collegare i client Fibre Channel. I nodi Fibre Channel fungono da convertitore di protocollo tra i protocolli Fibre Channel e iSCSI; ciò consente di aggiungere la connettività Fibre Channel a qualsiasi cluster SolidFire nuovo o esistente.

I nodi Fibre Channel presentano le seguenti caratteristiche:

- Gli switch Fibre Channel gestiscono lo stato della struttura, garantendo 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 delle altre porte.
- In una struttura possono comunicare simultaneamente più coppie di porte.

Stati operativi del nodo

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

- **Disponibile**

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

- **In attesa di**

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

Per accedere al nodo non è richiesta l'autenticazione.

- **In attesa di attivazione**

Il sistema sta installando il software Element compatibile sul nodo. Una volta completato, il nodo passerà allo stato Attivo.

- **Attivo**

Il nodo partecipa a un cluster.

Per modificare il nodo è richiesta l'autenticazione.

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

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Cluster

Un cluster è il fulcro di un sistema di archiviazione SolidFire ed è costituito da un insieme di nodi. Per realizzare l'efficienza di archiviazione SolidFire, è necessario disporre di almeno quattro nodi in un cluster. Un cluster appare sulla rete come un singolo gruppo logico e può quindi essere accessibile 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 nel 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 ampliare 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 di archiviazione (SVIP) consente l'accesso dell'host all'archiviazione 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 fallisce, un altro nodo nel 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 loro rete di gestione. Ciò vale sia per i nodi di archiviazione che per quelli di gestione, ad eccezione del nodo di gestione 11.3 e versioni successive che non supportano 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.

Di più sui cluster

- [Cluster di archiviazione autorevoli](#)
- [Regola dei terzi](#)
- [Capacità bloccata](#)
- [Efficienza di archiviazione](#)
- [Quorum del cluster di archiviazione](#)

Cluster di archiviazione 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 ha un solo cluster di archiviazione, questo è il cluster autorevole. Se il nodo di gestione ha due o più cluster di storage, uno di questi cluster 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 nel `token_url` campo è l'indirizzo IP virtuale di gestione (MVIP) del cluster di archiviazione 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 riuscirà.

Molte funzionalità di NetApp Hybrid Cloud Control sono progettate per funzionare con più cluster di storage, ma l'autenticazione e l'autorizzazione presentano delle limitazioni. La limitazione relativa all'autenticazione e all'autorizzazione è che l'utente del cluster autorevole può eseguire azioni su altri cluster collegati 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 archiviazione, è necessario assicurarsi che gli utenti definiti sui cluster autorevoli siano definiti su tutti gli altri cluster di archiviazione con le stesse autorizzazioni. Puoi gestire gli utenti da ["Interfaccia utente del software Element"](#).

Vedere ["creare e gestire risorse di cluster di archiviazione"](#) per ulteriori informazioni sull'utilizzo delle risorse del cluster di archiviazione del nodo di gestione.

Regola dei terzi

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

Capacità bloccata

Se un nodo appena aggiunto rappresenta più del 50 per cento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Ciò rimarrà vero finché non verrà aggiunta ulteriore capacità di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo si blocca, viene generato un errore di cluster appropriato.

Efficienza di archiviazione

I cluster di storage Netapp SolidFire sfruttano la deduplicazione, la compressione e il thin provisioning per ridurre la quantità di storage fisico necessaria per archiviare un volume.

- **Compressione**

La compressione riduce la quantità di spazio di archiviazione fisico richiesto per un volume combinando i blocchi di dati in gruppi di compressione, ognuno dei quali viene archiviato come un singolo blocco.

- **Deduplicazione**

La deduplicazione riduce la quantità di spazio di archiviazione fisico richiesto per un volume eliminando i blocchi di dati duplicati.

- **Provisioning sottile**

Un volume con thin provisioning o LUN è un volume per il quale non è stato prenotato in anticipo alcuno spazio di archiviazione. Al contrario, lo spazio di archiviazione viene allocato dinamicamente, in base alle necessità. Lo spazio libero viene rilasciato nuovamente nel sistema di archiviazione quando i dati nel volume o LUN vengono eliminati.

Quorum del cluster di archiviazione

Il software Element crea un cluster di archiviazione dai nodi selezionati, che mantiene un database replicato della configurazione del cluster. Per mantenere il quorum necessario alla resilienza del cluster, è necessario che almeno tre nodi partecipino all'insieme del cluster.

Sicurezza

Quando utilizzi il tuo sistema di archiviazione all-flash SolidFire , i tuoi dati sono protetti da protocolli di sicurezza standard del settore.

Crittografia a riposo (hardware)

Tutte le unità nei nodi di archiviazione sono in grado di sfruttare la crittografia AES a 256 bit a livello di unità. Ogni unità ha la propria chiave di crittografia, che viene creata quando l'unità viene inizializzata per la prima volta. Quando si abilita la funzionalità di crittografia, viene creata una password per l'intero cluster e parti della password vengono poi distribuite a tutti i nodi del cluster. Nessun singolo nodo memorizza l'intera password. La password viene quindi utilizzata per proteggere con password tutti gli accessi alle unità. La password è necessaria per sbloccare l'unità e non è più necessaria a meno che non venga rimossa l'alimentazione dall'unità o quest'ultima non sia bloccata.

"[Abilitazione della funzionalità di crittografia hardware a riposo](#)" non influisce sulle prestazioni o sull'efficienza del cluster. Se un'unità o un nodo abilitato alla crittografia viene rimosso dalla configurazione del cluster tramite l'API Element o l'interfaccia utente Element, la crittografia a riposo verrà disabilitata sulle unità. Dopo aver rimosso l'unità, è possibile cancellarla in modo sicuro utilizzando SecureEraseDrives Metodo API. Se un'unità fisica o un nodo viene rimosso forzatamente, i dati rimangono protetti dalla password dell'intero cluster e dalle chiavi di crittografia individuali dell'unità.

Crittografia a riposo (software)

Un altro tipo di crittografia a riposo, la crittografia software a riposo, consente di crittografare tutti i dati scritti su SSD in un cluster di archiviazione. **"Quando abilitato"**, crittografa automaticamente tutti i dati scritti e decrittografa tutti i dati letti nel software. La crittografia software a riposo rispecchia l'implementazione dell'unità auto-crittografante (SED) nell'hardware per garantire la sicurezza dei dati in assenza di SED.



Per i cluster di archiviazione all-flash SolidFire, la crittografia software a riposo deve essere abilitata durante la creazione del cluster e non può essere disabilitata dopo la creazione del cluster.

Sia la crittografia a riposo basata su software che su hardware può essere utilizzata in modo indipendente o in combinazione tra loro.

Gestione delle chiavi esterne

È possibile configurare il software Element in modo che utilizzi un servizio di gestione delle chiavi (KMS) di terze parti conforme a KMIP per gestire le chiavi di crittografia del cluster di archiviazione. Quando si abilita questa funzionalità, la chiave di crittografia della password di accesso all'unità a livello di cluster del cluster di archiviazione viene gestita da un KMS specificato dall'utente.

Element può utilizzare i seguenti servizi di gestione delle chiavi:

- Gemalto SafeNet KeySecure
- SafeNet AT KeySecure
- Controllo chiave HyTrust
- Responsabile della sicurezza dei dati Vormetric
- IBM Security Key Lifecycle Manager

Per ulteriori informazioni sulla configurazione della gestione delle chiavi esterne, vedere ["per iniziare con la gestione delle chiavi esterne"](#) documentazione.

Autenticazione multifattoriale

L'autenticazione a più fattori (MFA) consente di richiedere agli utenti di presentare più tipi di prove per l'autenticazione con l'interfaccia utente Web NetApp Element o con l'interfaccia utente del nodo di storage 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 utenti e il provider di identità esistenti. È possibile configurare Element per integrarlo con un provider di identità SAML 2.0 esistente, in grado di applicare più schemi di autenticazione, ad esempio password e messaggio di testo, password e messaggio di posta elettronica o altri metodi.

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

Per configurare MFA, vedere ["abilitare 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 sia per le comunicazioni HTTPS sia per la crittografia delle unità.

Quando si abilita la modalità operativa FIPS 140-2 sul cluster, il cluster attiva il NetApp Cryptographic Security Module (NCSM) e sfrutta la crittografia certificata FIPS 140-2 Livello 1 per tutte le comunicazioni tramite HTTPS all'interfaccia utente e all'API NetApp Element . Tu usi il `EnableFeature` API Element con `fips` parametro per abilitare la crittografia HTTPS FIPS 140-2. Nei cluster di archiviazione con hardware compatibile con FIPS, è anche possibile abilitare la crittografia delle unità FIPS per i dati inattivi utilizzando `EnableFeature` API Element con `FipsDrives` parametro.

Per ulteriori informazioni sulla preparazione di un nuovo cluster di archiviazione per la crittografia FIPS 140-2, vedere ["Creare un cluster che supporti le unità FIPS"](#) .

Per ulteriori informazioni sull'abilitazione di FIPS 140-2 su un cluster esistente e preparato, vedere ["l'API dell'elemento EnableFeature"](#) .

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Account e permessi

Per amministrare e fornire accesso alle risorse di archiviazione sul tuo sistema, dovrai configurare gli account per le risorse di sistema.

Utilizzando Element Storage puoi creare e gestire i seguenti tipi di account:

- [Account utente amministratore per il cluster di archiviazione](#)
- [Account utente per l'accesso al volume di archiviazione](#)
- [Account utente cluster autorevoli per NetApp Hybrid Cloud Control](#)

Account amministratore del cluster di archiviazione

In un cluster di storage che esegue il software NetApp Element possono esistere due tipi di account amministratore:

- **Account amministratore del cluster primario:** questo account amministratore viene creato quando viene creato il cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo all'utente root in un sistema Linux. Puoi modificare la password per questo account amministratore.
- **Account amministratore del cluster:** è possibile concedere 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 e Element UI all'interno del sistema di archiviazione.



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

Puoi ["gestire gli account degli amministratori del cluster"](#) creando, eliminando e modificando gli account degli amministratori del cluster, cambiando la password degli amministratori 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 sul 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 hai creato un volume virtuale, l'account è il contenitore di archiviazione.

Ecco alcune considerazioni aggiuntive:

- L'account contiene l'autenticazione CHAP necessaria 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 NetApp Element Management.

Account utente autorevoli del cluster

Gli account utente autorevoli del cluster possono eseguire l'autenticazione su 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 altro ancora su tutti i cluster.

Gli account utente autorevoli vengono gestiti tramite l'opzione Gestione utenti nel menu in alto a destra in NetApp Hybrid Cloud Control.

IL "[cluster di archiviazione 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 a NetApp Hybrid Cloud Control. Gli utenti creati su altri cluster di archiviazione *non* possono accedere a Hybrid Cloud Control.

- Se il nodo di gestione ha un solo cluster di archiviazione, questo è il cluster autorevole.
- Se il nodo di gestione ha due o più cluster di storage, uno di questi cluster 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 presentano delle limitazioni necessarie. La limitazione relativa all'autenticazione e all'autorizzazione è che gli utenti del cluster autorevole possono eseguire azioni su altri cluster collegati 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 archiviazione, è necessario assicurarsi che gli utenti definiti sui cluster autorevoli siano definiti su tutti gli altri cluster di archiviazione con le stesse autorizzazioni. È possibile gestire gli utenti da NetApp Hybrid Cloud Control.

Conti di volume

Gli account specifici del volume sono specifici solo del cluster di archiviazione su cui sono stati creati. Questi account consentono di impostare autorizzazioni su volumi specifici nella 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.

Magazzinaggio

Volumi

Il sistema di storage NetApp Element esegue il provisioning dello storage tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel.

Element Storage consente di creare, visualizzare, modificare, eliminare, clonare, eseguire il backup o ripristinare volumi per gli account utente. È inoltre possibile gestire ciascun volume su un cluster e aggiungere o rimuovere volumi nei gruppi di accesso ai volumi.

Volumi persistenti

I volumi persistenti consentono di archiviare i dati di configurazione del nodo di gestione su un cluster di archiviazione specificato, anziché localmente con una macchina virtuale, in modo che i dati possano essere conservati in caso di perdita o rimozione del nodo di gestione. I volumi persistenti sono una configurazione del nodo di gestione facoltativa ma consigliata.

Un'opzione per abilitare i volumi persistenti è inclusa negli script di installazione e aggiornamento quando ["distribuzione di un nuovo nodo di gestione"](#). I volumi persistenti sono volumi su un cluster di archiviazione basato sul software Element che contengono informazioni sulla configurazione del nodo di gestione per la VM del nodo di gestione host che persistono oltre la durata della VM. Se il nodo di gestione viene perso, una VM del nodo di gestione sostitutiva può riconnettersi e recuperare i dati di configurazione per la VM persa.

La funzionalità dei volumi persistenti, se abilitata durante l'installazione o l'aggiornamento, crea automaticamente più volumi. Questi volumi, come qualsiasi volume basato sul software Element, possono essere visualizzati tramite 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 funzionanti 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 (vVols)

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 (vVols) è possibile allocare lo spazio di archiviazione in base ai requisiti delle singole macchine virtuali.

Rilegature

Il cluster NetApp Element sceglie un endpoint di protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint di protocollo e restituisce il binding all'host ESXi. Dopo l'associazione, 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 di protocollo per comunicare con i volumi virtuali. Gli host ESXi associano 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 a 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 di protocollo corrispondente. Ad esempio, un cluster a quattro nodi avrà quattro endpoint di protocollo.

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

contenitori di stoccaggio

I contenitori di archiviazione sono strutture logiche che vengono mappate sugli account NetApp Element e vengono utilizzate per la creazione di report e l'allocazione delle risorse. Raggruppano la capacità di archiviazione grezza o aggregano le capacità di archiviazione che il sistema di archiviazione può fornire ai volumi virtuali. Un datastore VVol creato in vSphere viene mappato su un singolo contenitore di archiviazione. Per impostazione predefinita, un singolo contenitore di archiviazione 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 contenitori di archiviazione.

I contenitori di archiviazione funzionano come account tradizionali e possono contenere sia volumi virtuali che volumi tradizionali. Sono supportati al massimo quattro contenitori di archiviazione per cluster. Per utilizzare la funzionalità VVols è necessario almeno un contenitore di archiviazione. È possibile individuare i contenitori di archiviazione in vCenter durante la creazione di VVol.

Fornitore VASA

Per far sì che vSphere sia a conoscenza 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 fuori banda tra vSphere e il cluster Element. È responsabile dell'esecuzione delle richieste sul cluster Element per conto di vSphere, ad esempio la creazione di VM, la messa a disposizione di VM per vSphere e la pubblicità delle capacità di storage per vSphere.

Il provider VASA viene eseguito come parte del cluster master nel software Element. Il master del cluster è un servizio ad alta disponibilità che esegue il failover su qualsiasi nodo del cluster, se necessario. Se il master del cluster fallisce, il provider VASA si sposta di conseguenza, garantendo un'elevata disponibilità per il provider VASA. Tutte le attività di provisioning e gestione dell'archiviazione utilizzano il provider VASA, che gestisce tutte le modifiche necessarie sul cluster Element.



Per Element 12.5 e versioni precedenti, non registrare più di un provider NetApp Element VASA su una singola istanza di vCenter. Se viene aggiunto un secondo provider NetApp Element VASA, tutti i datastore VVOL diventano inaccessibili.



Il supporto VASA per un massimo di 10 vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con il tuo vCenter. Per installare, seguire le istruzioni nel manifesto VASA39 e scaricare il file .tar.gz da "[Download del software NetApp](#)" sito. Il provider NetApp Element VASA 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 maggiori informazioni

- "[Documentazione del software SolidFire ed Element](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"

Gruppi di accesso al volume

Creando e utilizzando gruppi di accesso al volume, è possibile controllare l'accesso a un set di volumi. Quando si associa un set di volumi e un set di iniziatori a un gruppo di accesso al volume, il gruppo di accesso concede a tali iniziatori l'accesso a quel set di volumi.

I gruppi di accesso ai volumi nello storage NetApp SolidFire consentono agli IQN dell'iniziatore iSCSI o ai 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 alla rete Fibre Channel ai volumi nel gruppo di accesso.

I gruppi di accesso al volume hanno i seguenti limiti:

- Un massimo di 128 iniziatori per gruppo di accesso al volume.
- Massimo 64 gruppi di accesso per volume.
- Un gruppo di accesso può essere composto 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 in un cluster, fungendo da punto di ingresso per la comunicazione tra client e volumi. È possibile utilizzare gli iniziatori per l'accesso basato su CHAP anziché su account ai volumi di archiviazione. Un singolo iniziatore, se aggiunto a un gruppo di accesso al volume, consente ai membri del gruppo di accesso al volume di accedere a tutti i volumi di archiviazione 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, clonazione dei volumi, domini di protezione e alta disponibilità con tecnologia Double Helix.

La protezione dei dati di archiviazione degli elementi include i seguenti concetti:

- [Tipi di replicazione remota](#)
- [Snapshot del volume per la protezione dei dati](#)
- [Cloni di volume](#)
- [Panoramica del processo di backup e ripristino per Element Storage](#)
- [Domini di protezione](#)
- [Domini di protezione personalizzati](#)
- [Doppia elica ad alta disponibilità](#)

Tipi di replicazione 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 tramite SnapMirror](#)

Per maggiori 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 rapida creazione di copie remote dei dati del volume.

È possibile associare un cluster di archiviazione a un massimo di altri quattro cluster di archiviazione. È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in 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 adatta alle seguenti situazioni:

- Replicazione di più sistemi su breve distanza
- Un sito di ripristino di emergenza geograficamente locale rispetto alla fonte
- Applicazioni sensibili al fattore tempo e protezione dei database
- Applicazioni di continuità aziendale 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 le conferme dal cluster di destinazione. Durante la replica asincrona, le scritture vengono riconosciute al client (applicazione) dopo essere state eseguite sul cluster di origine.

La replica asincrona è adatta alle seguenti situazioni:

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

Replica solo snapshot

La protezione dei dati basata solo su snapshot replica i dati modificati in momenti specifici su un cluster remoto. Vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non lo sono.

È possibile impostare la frequenza delle repliche degli snapshot.

La replica snapshot non influisce sulla replica asincrona o sincrona.

Replica tra cluster Element e ONTAP tramite SnapMirror

Grazie alla tecnologia NetApp SnapMirror, è possibile replicare gli snapshot acquisiti tramite 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 replicazione Snapshot 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 mirror, dei dati di lavoro nell'archivio secondario, da cui è possibile continuare a fornire dati in caso di interruzione nel sito primario. I dati vengono rispecchiati a livello di volume.

La relazione tra il volume di origine nell'archiviazione primaria e il volume di destinazione nell'archiviazione secondaria è detta 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 sottoposti a peering. Una relazione peer consente ai cluster e ai 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 per controllare SnapMirror risiede nel software ONTAP; pertanto, tutte le relazioni SnapMirror devono coinvolgere almeno un sistema ONTAP per eseguire il lavoro di coordinamento. Gli utenti gestiscono le relazioni tra Element e i cluster ONTAP principalmente tramite l'interfaccia utente di Element; tuttavia, alcune attività di gestione risiedono in NetApp ONTAP System Manager. Gli utenti possono gestire SnapMirror anche tramite CLI e API, entrambe disponibili in ONTAP ed Element.

Vedere ["TR-4651: Architettura e configurazione NetApp SolidFire SnapMirror"](#) (è richiesto l'accesso)

È necessario abilitare manualmente la funzionalità SnapMirror a livello di cluster utilizzando il software Element. La funzionalità SnapMirror è disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento.

Dopo aver abilitato SnapMirror, è possibile creare relazioni SnapMirror dalla scheda Protezione dati nel software Element.

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

I sistemi che eseguono Element 10.1 e versioni successive includono codice in grado di comunicare direttamente con SnapMirror sui sistemi ONTAP che eseguono 9.3 o versioni successive. 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 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 ONTAP nei volumi

Element in casi d'uso specifici con funzionalità limitate.

Per maggiori informazioni, vedere ["Replica tra NetApp Element Software e ONTAP \(ONTAP CLI\)"](#).

Snapshot del volume per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un momento specifico, che può essere utilizzata in seguito per ripristinare un volume a quel momento specifico.

Sebbene gli snapshot siano simili ai cloni dei volumi, sono semplicemente repliche dei metadati dei volumi, quindi non è possibile montarli o scriverci sopra. La creazione di uno snapshot del volume richiede inoltre solo una piccola quantità di risorse di sistema e spazio, il che rende la creazione di snapshot più rapida della clonazione.

È possibile replicare gli snapshot su un cluster remoto e utilizzarli come copia di backup del volume. Ciò consente di ripristinare un volume a un punto specifico nel tempo utilizzando lo snapshot replicato; è anche possibile creare un clone di un volume da uno snapshot replicato.

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

È possibile acquisire uno snapshot di un singolo volume o di più volumi per la protezione dei dati.

Cloni di volume

Un clone di un singolo volume o di più volumi è una copia dei dati effettuata in un dato momento. Quando si clona un volume, il sistema crea uno snapshot del volume e quindi crea una copia dei dati a cui fa riferimento lo snapshot.

Si tratta di un processo asincrono e la quantità di tempo richiesta dipende dalle dimensioni del volume che si sta clonando e dal carico attuale del cluster.

Il cluster supporta fino a due richieste di clonazione in esecuzione per volume alla volta e fino a otto operazioni di clonazione di volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per essere elaborate in un secondo momento.

Panoramica del processo di backup e ripristino per Element Storage

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 nel modo seguente:

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

Quando si ripristinano volumi da OpenStack Swift o Amazon S3, sono necessarie le informazioni manifest del processo di backup originale. Se si ripristina un volume di cui è stato eseguito il backup su un sistema di archiviazione SolidFire , non sono necessarie informazioni sul manifesto.

Domini di protezione

Un dominio di protezione è un nodo o un insieme di nodi raggruppati insieme in modo tale che una parte o addirittura la totalità di esso possa guastarsi, mantenendo al contempo la disponibilità dei dati. I domini di protezione consentono a un cluster di storage di ripristinare automaticamente la funzionalità in caso di perdita di uno chassis (affinità dello chassis) o di un intero dominio (gruppo di chassis).

È possibile abilitare manualmente il monitoraggio del dominio di protezione utilizzando il punto di estensione NetApp Element Configuration nel plug-in NetApp Element per vCenter Server. È possibile selezionare una soglia del dominio di protezione in base ai domini dei nodi o degli chassis. È anche possibile abilitare il monitoraggio del dominio di protezione tramite l'API Element o l'interfaccia utente Web.

Un layout di dominio di protezione assegna ciascun nodo a uno specifico dominio di protezione.

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

- A livello di nodo, ogni 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 ogni nodo si trova in uno chassis separato, questi due livelli sono funzionalmente identici.

Quando si crea un nuovo cluster, se si utilizzano nodi di archiviazione che risiedono in uno chassis condiviso, potrebbe essere opportuno valutare la progettazione di una protezione contro gli errori a livello di chassis mediante la funzionalità Domini di protezione.

Domini di protezione personalizzati

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

Se non vengono assegnati domini di protezione personalizzati:

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

Quando si configurano domini di protezione personalizzati per un cluster, sono disponibili tre possibili livelli di protezione, che è possibile visualizzare nella dashboard dell'interfaccia utente Web di Element:

- Non protetto: il cluster di archiviazione non è protetto dal guasto di uno dei suoi domini di protezione personalizzati. Per risolvere questo problema, aggiungere ulteriore capacità di archiviazione al cluster o riconfigurare i domini di protezione personalizzati del cluster per proteggere il cluster da possibili perdite di dati.
- Tollerante agli errori: il cluster di archiviazione dispone di capacità libera sufficiente per impedire la perdita di dati dopo il guasto di uno dei suoi domini di protezione personalizzati.
- Resistente agli errori: il cluster di storage ha sufficiente capacità libera per autoripararsi dopo l'errore di uno dei suoi domini di protezione personalizzati. Una volta completato il processo di ripristino, 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 assegnerà i duplicati a domini di protezione personalizzati separati. Se ciò non è possibile, si torna ad assegnare i duplicati a nodi separati. Ogni sottosistema (ad esempio, contenitori, sezioni, provider di endpoint di protocollo ed ensemble) esegue questa operazione in modo indipendente.

Puoi usare l'interfaccia utente dell'elemento per "[configurare domini di protezione personalizzati](#)" oppure puoi utilizzare i seguenti metodi API:

- "[OttieniProtectionDomainLayout](#)" - mostra in quale chassis e in quale dominio di protezione personalizzato si trova ciascun nodo.
- "[ImpostaProtezioneDominioLayout](#)" - consente di assegnare un dominio di protezione personalizzato a ciascun nodo.

Doppia elica ad alta disponibilità

La protezione dei dati Double Helix è un metodo di replicazione che distribuisce almeno due copie ridondanti dei dati su tutte le unità di un sistema. L'approccio "senza RAID" consente a un sistema di assorbire più guasti simultanei su tutti i livelli del sistema di archiviazione e di ripararli rapidamente.

Prestazioni e qualità del servizio

Un cluster di storage SolidFire è in grado di fornire parametri di qualità del servizio (QoS) in base al volume. È possibile garantire le prestazioni del cluster misurate in input e output al secondo (IOPS) utilizzando tre parametri configurabili che definiscono la QoS: IOPS minimi, IOPS massimi e IOPS a raffica.



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

Parametri di qualità del servizio

I parametri IOPS sono definiti nei seguenti modi:

- **IOPS minimi:** il numero minimo di input e output sostenuti al secondo (IOPS) che il cluster di storage fornisce a un volume. Il valore Min IOPS configurato per un volume rappresenta il livello di prestazioni garantito per un volume. Le prestazioni non scendono al di sotto di questo livello.
- **IOPS massimi:** il numero massimo di IOPS sostenuti che il cluster di storage fornisce a un volume. Quando i livelli IOPS del cluster sono estremamente elevati, questo livello di prestazioni IOPS non viene superato.
- **Burst IOPS** - Numero massimo di IOPS consentiti in uno scenario di burst breve. Se un volume è stato eseguito al di sotto del numero massimo di IOPS, vengono accumulati crediti burst. Quando i livelli di prestazioni diventano molto elevati e vengono spinti al massimo, sul volume sono consentiti brevi raffiche di IOPS.

Il software Element utilizza Burst IOPS quando un cluster è in esecuzione in uno stato di basso utilizzo degli IOPS del cluster.

Un singolo volume può accumulare Burst IOPS e utilizzare i crediti per superare i propri Max IOPS fino al livello Burst IOPS per un "periodo di burst" impostato. Un volume può subire un burst fino a 60 secondi se il cluster ha la capacità di gestire il burst. Un volume accumula un secondo di credito burst (fino a un massimo di 60 secondi) per ogni secondo in cui il volume viene eseguito al di sotto del limite Max IOPS.

I burst IOPS sono limitati in due modi:

- Un volume può superare il suo massimo IOPS per un numero di secondi pari al numero di crediti burst accumulati dal volume.
- Quando un volume supera l'impostazione Max IOPS, è limitato dall'impostazione Burst IOPS. Pertanto, il burst IOPS non supera mai l'impostazione burst IOPS 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 IO.

Esempio: le impostazioni dei parametri QoS pari a 100 IOPS minimi, 1000 IOPS massimi e 1500 IOPS burst hanno i seguenti effetti sulla qualità delle prestazioni:

- I carichi di lavoro sono in grado di raggiungere e sostenere un massimo di 1000 IOPS finché non si manifesta sul cluster la condizione di contesa del carico di lavoro per gli IOPS. Gli IOPS vengono quindi ridotti in modo incrementale finché gli IOPS su tutti i volumi rientrano negli intervalli QoS designati e la contesa per le prestazioni viene alleviata.
- Le prestazioni su tutti i volumi sono spinte verso il valore minimo di IOPS pari a 100. I livelli non scendono al di sotto dell'impostazione Min IOPS, ma potrebbero rimanere superiori a 100 IOPS quando la contesa del carico di lavoro viene alleviata.
- Le prestazioni non sono mai superiori a 1000 IOPS, né inferiori a 100 IOPS per un periodo prolungato. Sono consentite prestazioni pari a 1500 IOPS (Burst IOPS), ma solo per i volumi che hanno accumulato crediti burst eseguendo al di sotto del Max IOPS e sono consentite 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 4KB	5 8KB	6 16KB	262 KB
IOPS minimi	50	50	15.000	9.375*	5556*	385*
IOPS massimi	100	15.000	200.000**	125.000	74.074	5128
IOPS a raffica	100	15.000	200.000**	125.000	74,074	5128

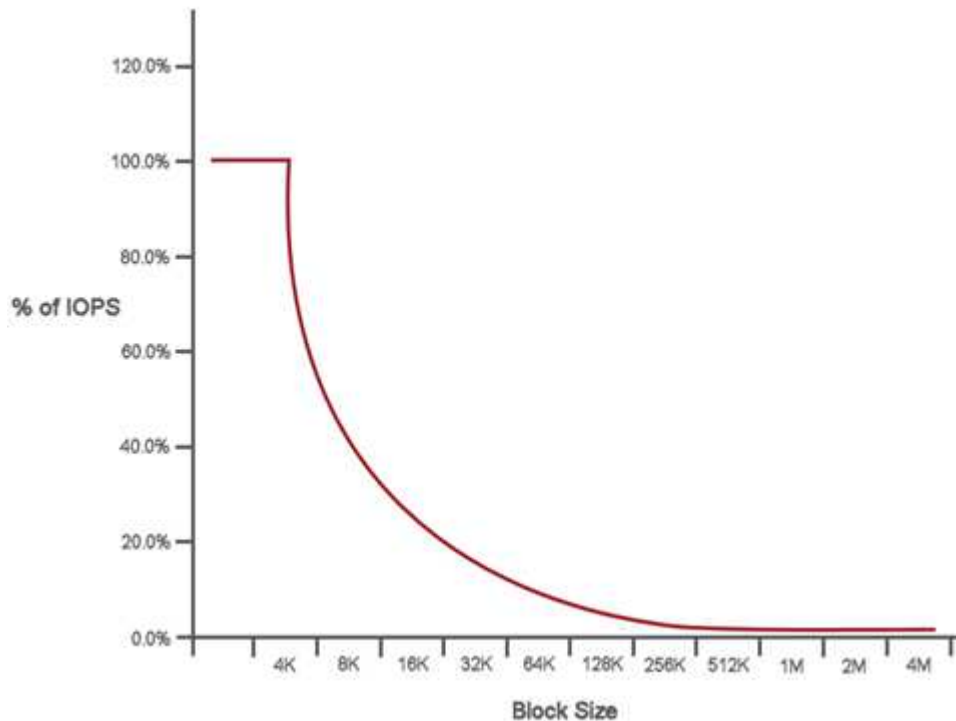
*Queste stime sono approssimative. **I valori Max IOPS e Burst IOPS possono essere impostati fino a 200.000; tuttavia, questa impostazione è consentita solo per superare efficacemente il limite delle prestazioni di un volume. Le prestazioni massime reali di un volume sono limitate dall'utilizzo del cluster e dalle prestazioni per nodo.

Prestazioni QoS

La curva delle prestazioni 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 che riceve normalizzandole 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 al livello necessario per elaborare blocchi di dimensioni maggiori. Con l'aumento della larghezza di banda, il numero di IOPS che il sistema è in grado di raggiungere diminuisce.

La curva delle prestazioni 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 a 8k, la larghezza di banda aumenta a 5000 KBps e gli IOPS diminuiscono a 625. Tenendo conto delle dimensioni dei blocchi, il sistema garantisce che i carichi di lavoro a priorità inferiore che utilizzano dimensioni dei blocchi più elevate, come i backup e le attività dell'hypervisor, non assorbano troppe prestazioni necessarie al traffico a priorità superiore che utilizza dimensioni dei blocchi più piccole.

Criteri QoS

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

Le policy QoS sono ideali per gli ambienti di servizio, ad esempio con server di database, applicazioni o infrastrutture che si riavviano raramente e necessitano di un accesso costante e paritario allo storage. La QoS per volume individuale è ideale per le VM con utilizzo leggero, come desktop virtuali o VM specializzate di tipo chiosco, che possono essere riavviate, accese o spente quotidianamente o più volte al giorno.

QoS e policy QoS non devono essere utilizzati insieme. Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.



Per utilizzare i criteri QoS, il cluster selezionato deve essere Element 10.0 o versione successiva; in caso contrario, le funzioni dei criteri QoS non saranno disponibili.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)

Requisiti

Networking

La configurazione di rete per un sistema SolidFire è composta da requisiti di switch e porte. L'implementazione di queste opzioni dipende dal sistema in uso.

Per maggiori informazioni

- ["Configurazione dello switch per cluster che eseguono il software Element"](#)
- ["Requisiti delle porte di rete"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurazione dello switch per cluster che eseguono il software Element

Il sistema software NetApp Element presenta determinati requisiti di switch e best practice per prestazioni di storage ottimali.

I nodi di storage richiedono switch Ethernet da 10 o 25 GbE, a seconda dell'hardware specifico del nodo, 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

Migliori pratiche: è necessario implementare le seguenti migliori pratiche durante la configurazione degli switch Ethernet per il traffico del cluster:

- Per il traffico non di storage nel cluster, distribuire una coppia di switch da 1 GbE per garantire elevata disponibilità e condivisione del carico.
- Sugli switch della rete di storage, distribuire gli switch a coppie e configurare e utilizzare i frame jumbo (con una dimensione MTU di 9216 byte). Ciò garantisce un'installazione corretta ed elimina gli errori della rete di archiviazione dovuti a pacchetti frammentati.

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

- Gestione
- Archiviazione/Dati

A seconda dei modelli di nodi di storage NetApp H-Series e della configurazione di cablaggio pianificata, è possibile separare fisicamente queste reti utilizzando switch separati oppure separarle logicamente utilizzando VLAN. Tuttavia, per la maggior parte delle distribuzioni, è necessario separare logicamente queste reti

utilizzando le VLAN.

I nodi di archiviazione devono essere in grado di comunicare prima, durante e dopo la distribuzione.

Se si implementano reti di gestione separate per i nodi di archiviazione, assicurarsi che tali reti di gestione dispongano di percorsi di rete tra di loro. A queste reti devono essere assegnati dei gateway e deve esserci un percorso tra i gateway. Assicurarsi che a ogni nuovo nodo sia assegnato un gateway per facilitare la comunicazione tra i nodi e le reti di gestione.

NetApp Element richiede quanto segue:

- Tutte le porte dello switch connesse ai nodi di 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`
 - Sugli switch Mellanox, puoi farlo con `spanning-tree port type edge` comando.
- Gli switch che gestiscono il traffico di archiviazione devono supportare velocità di almeno 10 GbE per porta (sono supportate 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 archiviazione. Per un'installazione corretta, gli host devono essere in grado di inviare pacchetti da 9000 byte end-to-end.
- La latenza di rete di andata e ritorno tra tutti i nodi di archiviazione non deve superare i 2 ms.

Alcuni nodi forniscono 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 nel tuo ambiente.

Per maggiori informazioni

- ["Requisiti di rete e switch NetApp HCI"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Requisiti delle porte di rete

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

Tutte le porte sono TCP, salvo diversa indicazione, e tutte le porte TCP devono supportare la comunicazione handshake a tre vie tra NetApp Support Server, nodo di gestione e nodi che eseguono il software Element. Ad

esempio, l'host su un nodo di gestione sorgente comunica con l'host su un cluster di storage MVIP destinazione tramite la porta TCP 443, e l'host di destinazione comunica di nuovo con l'host di origine tramite una porta qualsiasi.



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 di archiviazione, un indirizzo per nodo
- MVIP: indirizzo IP virtuale di gestione
- SVIP: indirizzo IP virtuale di archiviazione

Fonte	Destinazione	Porta	Descrizione
client iSCSI	Cluster di archiviazione MVIP	443	(Facoltativo) Accesso all'interfaccia utente e all'API
client iSCSI	Cluster di archiviazione SVIP	3260	Comunicazioni iSCSI del client
client iSCSI	Nodo di archiviazione SIP	3260	Comunicazioni iSCSI del client
Nodo di gestione	<code>sfsupport.solidfire.com</code>	22	Tunnel SSH inverso per l'accesso al supporto
Nodo di gestione	Nodo di archiviazione MIP	22	Accesso SSH per supporto
Nodo di gestione	server DNS	53 TCP/UDP	Ricerca DNS
Nodo di gestione	Nodo di archiviazione MIP	442	Accesso tramite interfaccia utente e API al nodo di archiviazione e agli aggiornamenti software Element
Nodo di gestione	Cluster di archiviazione MVIP	442	Accesso tramite interfaccia utente e API al nodo di archiviazione e agli aggiornamenti software Element
Nodo di gestione	<code>monitoring.solidfire.com</code>	443	Reporting del cluster di archiviazione ad Active IQ
Nodo di gestione	Cluster di archiviazione MVIP	443	Accesso tramite interfaccia utente e API al nodo di archiviazione e agli aggiornamenti software Element

Fonte	Destinazione	Porta	Descrizione
Nodo di gestione	repo.netapp.com	443	Fornisce l'accesso ai componenti necessari per installare/aggiornare la distribuzione in locale.
Nodo di gestione	Nodo di archiviazione BMC/IPMI	623 UDP	Porta RMCP. Ciò è necessario per gestire i sistemi abilitati IPMI.
Nodo di gestione	Nodo testimone	9442	Servizio API di configurazione per nodo
Nodo di gestione	Server vCenter	9443	Registrazione del plug-in vCenter. Una volta completata la registrazione, la porta potrà essere chiusa.
server SNMP	Cluster di archiviazione MVIP	161 UDP	Interrogazione SNMP
server SNMP	Nodo di archiviazione MIP	161 UDP	Interrogazione SNMP
Nodo di archiviazione BMC/IPMI	Nodo di gestione	623 UDP	Porta RMCP. Ciò è necessario per gestire i sistemi abilitati IPMI.
Nodo di archiviazione MIP	server DNS	53 TCP/UDP	Ricerca DNS
Nodo di archiviazione MIP	Nodo di gestione	80	Aggiornamenti software Element
Nodo di archiviazione MIP	Punto finale S3/Swift	80	(Facoltativo) Comunicazione HTTP all'endpoint S3/Swift per backup e ripristino
Nodo di archiviazione MIP	server NTP	123 UDP	NTP
Nodo di archiviazione MIP	Nodo di gestione	162 UDP	(Facoltativo) Trappole SNMP
Nodo di archiviazione MIP	server SNMP	162 UDP	(Facoltativo) Trappole SNMP
Nodo di archiviazione MIP	server LDAP	389 TCP/UDP	(Facoltativo) Ricerca LDAP
Nodo di archiviazione MIP	Nodo di gestione	443	Aggiornamenti dello storage degli elementi
Nodo di archiviazione MIP	Cluster di archiviazione remota MVIP	443	Comunicazione di associazione del cluster di replicazione remota
Nodo di archiviazione MIP	Nodo di archiviazione remoto MIP	443	Comunicazione di associazione del cluster di replicazione remota

Fonte	Destinazione	Porta	Descrizione
Nodo di archiviazione MIP	Punto finale S3/Swift	443	(Facoltativo) Comunicazione HTTPS all'endpoint S3/Swift per backup e ripristino
Nodo di archiviazione MIP	Nodo di gestione	514 TCP/UDP 10514 TCP/UDP	Inoltro Syslog
Nodo di archiviazione MIP	Server Syslog	514 TCP/UDP 10514 TCP/UDP	Inoltro Syslog
Nodo di archiviazione MIP	server LDAPS	636 TCP/UDP	Ricerca LDAPS
Nodo di archiviazione MIP	Nodo di archiviazione remoto MIP	2181	Comunicazione intercluster per la replicazione remota
Nodo di archiviazione SIP	Nodo di archiviazione remoto SIP	2181	Comunicazione intercluster per la replicazione remota
Nodo di archiviazione SIP	Nodo di archiviazione SIP	3260	Internodo iSCSI
Nodo di archiviazione SIP	Nodo di archiviazione remoto SIP	dall'4000 al 4020	Trasferimento dati da nodo a nodo di replicazione remota
Amministratore di sistema PC	Nodo di gestione	442	Accesso HTTPS all'interfaccia utente al nodo di gestione
Amministratore di sistema PC	Nodo di archiviazione MIP	442	Accesso API e interfaccia utente HTTPS al nodo di archiviazione
Amministratore di sistema PC	Nodo di gestione	443	Accesso HTTPS all'interfaccia utente e all'API per il nodo di gestione
Amministratore di sistema PC	Cluster di archiviazione MVIP	443	Accesso API e interfaccia utente HTTPS al cluster di archiviazione
Amministratore di sistema PC	Controller di gestione della scheda base del nodo di archiviazione (BMC)/Interfaccia di gestione della piattaforma intelligente (IPMI) serie H410 e H600	443	Accesso HTTPS all'interfaccia utente e all'API per il controllo remoto del nodo

Fonte	Destinazione	Porta	Descrizione
Amministratore di sistema PC	Nodo di archiviazione MIP	443	Creazione di cluster di archiviazione HTTPS, accesso all'interfaccia utente post-distribuzione al cluster di archiviazione
Amministratore di sistema PC	Nodo di archiviazione BMC/IPMI serie H410 e H600	623 UDP	Porta del protocollo di controllo della gestione remota. Ciò è necessario per gestire i sistemi abilitati IPMI.
Amministratore di sistema PC	Nodo testimone	8080	Interfaccia utente web per nodo Witness Node
Server vCenter	Cluster di archiviazione MVIP	443	Accesso all'API del plug-in vCenter
Server vCenter	Plug-in remoto	8333	Servizio plug-in vCenter remoto
Server vCenter	Nodo di gestione	8443	(Facoltativo) Servizio QoSSIOC del plug-in vCenter.
Server vCenter	Cluster di archiviazione MVIP	8444	Accesso al provider vCenter VASA (solo VVols)
Server vCenter	Nodo di gestione	9443	Registrazione del plug-in vCenter. Una volta completata la registrazione, la porta potrà essere chiusa.

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Provalo

Scopri le risorse e gli strumenti che ti aiuteranno a iniziare a usare il software Element.

- ["Lab on Demand per la flessibilità dell'archiviazione cloud privata con Element \(è richiesto l'accesso\)"](#): Questo laboratorio presenta i concetti di scalabilità senza limitazioni, prestazioni garantite del carico di lavoro e automazione dell'infrastruttura di storage applicabili ai sistemi di storage che eseguono il software Element.
- ["Prova le funzionalità di archiviazione utilizzando Element Demo Node"](#): Element Demo Node è una versione per 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 .

Prova le funzionalità di archiviazione utilizzando Element Demo Node

"[Nodo demo elemento](#)" è una versione VMware per macchina virtuale (VM) 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 programmare in base all'API Element senza bisogno di hardware fisico. È confezionato come file OVA per una facile distribuzione VMware.

Funzionalità supportate:

Element Demo Node è concepito esclusivamente per essere utilizzato come strumento di dimostrazione e sviluppo. Prima di utilizzare il nodo demo, tenere presente le seguenti limitazioni funzionali:

- Element Demo Node non supporta il clustering. Funziona solo come cluster a nodo singolo.
- Non supporta gli aggiornamenti Element. Per provare una versione più recente di Element, dovresti installare una nuova VM del nodo demo.
- Non ha lo scopo di dimostrare le prestazioni di archiviazione. Le prestazioni osservate sul nodo demo non sono in alcun modo indicative delle prestazioni 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.
- La funzionalità di configurazione e monitoraggio basata sull'hardware non funziona 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 vVols 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 maggiori dettagli, consultare le ultime Note di rilascio del software Element.

Requisiti VM

- Capacità totale di 240 GB (non è possibile modificare le dimensioni e il numero di dischi virtuali per la VM. Qualsiasi spazio di archiviazione aggiuntivo presentato tramite l'hypervisor viene ignorato dal sistema operativo guest.)
- Disco di root da 60 GB
- Thick provisioned/eager zeroed (un'unità metadati da 30 GB o tre unità a blocchi da 50 GB) o thin provisioned/eager zeroed (**consigliato**) (un'unità metadati da 30 GB o tre unità a blocchi da 50 GB)
- Due vCPU (completamente riservate)
- 16 GB di RAM (completamente riservati)
- HBA singolo per tutti i dischi, LSI Logic parallelo
- Due vNIC, entrambe vmxnet3 (una di gestione, una di archiviazione)

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 le VM Element Demo Node 12.3 e 12.5
- Architettura Intel® multi-core a 64 bit

Scarica il nodo demo dell'elemento

Il software Element Demo Node è un set di file VMware impacchettati in un file .ova.

Installa Element Demo Node su VMware ESXi

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

- [Configurare le interfacce di rete](#)
- [Registra il nodo demo su un server ESXi](#)
- [Avvia il nodo demo su un server ESXi](#)

Configurare le interfacce di rete

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

Registra il nodo demo su un server ESXi

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

Passi

1. Accedi a vSphere Client e seleziona l'host ESXi dal pannello dell'inventario.
2. Selezionare **File > Distribuisci modello OVF**.

Viene avviata la procedura guidata Distribuisci modello OVF.

3. Nella pagina **Seleziona modello**, vai al file OVA scaricato e seleziona **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**, vai alla posizione in cui desideri eseguire il modello e seleziona **Avanti**.
7. Verificare i dettagli e selezionare **Avanti**.
8. Nella pagina **Seleziona archiviazione**, seleziona dove desideri archiviare i file della macchina virtuale, quindi seleziona **Avanti**.
9. Nella pagina **Seleziona reti**, mappa la rete utilizzata nel file OVA alle due reti distinte delle macchine virtuali nel tuo inventario e seleziona **Avanti**.
10. Nella pagina **Pronto per il completamento**, verifica i dettagli sulla macchina virtuale che stai creando, quindi seleziona **Fine**.



Il completamento della distribuzione del nodo demo potrebbe richiedere alcuni minuti.

Avvia il nodo demo su un server ESXi

È necessario avviare la VM del nodo demo per accedere a Element tramite la console VMware ESXi.

Passi

1. Nel vSphere Client, seleziona la VM del nodo demo che hai creato.
2. Selezionare la scheda **Riepilogo** per visualizzare i dettagli su questa VM.
3. Selezionare **Accensione** per avviare la VM.
4. Selezionare **Avvia Web Console**.
5. Utilizzare l'interfaccia utente guidata per configurare il nodo demo. Per maggiori informazioni, vedere ["Configurare un nodo di archiviazione"](#).

Come ottenere supporto

Element Demo Node è disponibile su base volontaria con il massimo impegno. Per supporto, invia le tue domande a ["Forum del nodo dimostrativo dell'elemento"](#).

Trova maggiori informazioni

["Pagina di download del nodo demo Element \(è richiesto l'accesso\)"](#)

Installare e mantenere l'hardware

Informazioni hardware H410S e H610S

Installare nodi di archiviazione della serie H

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



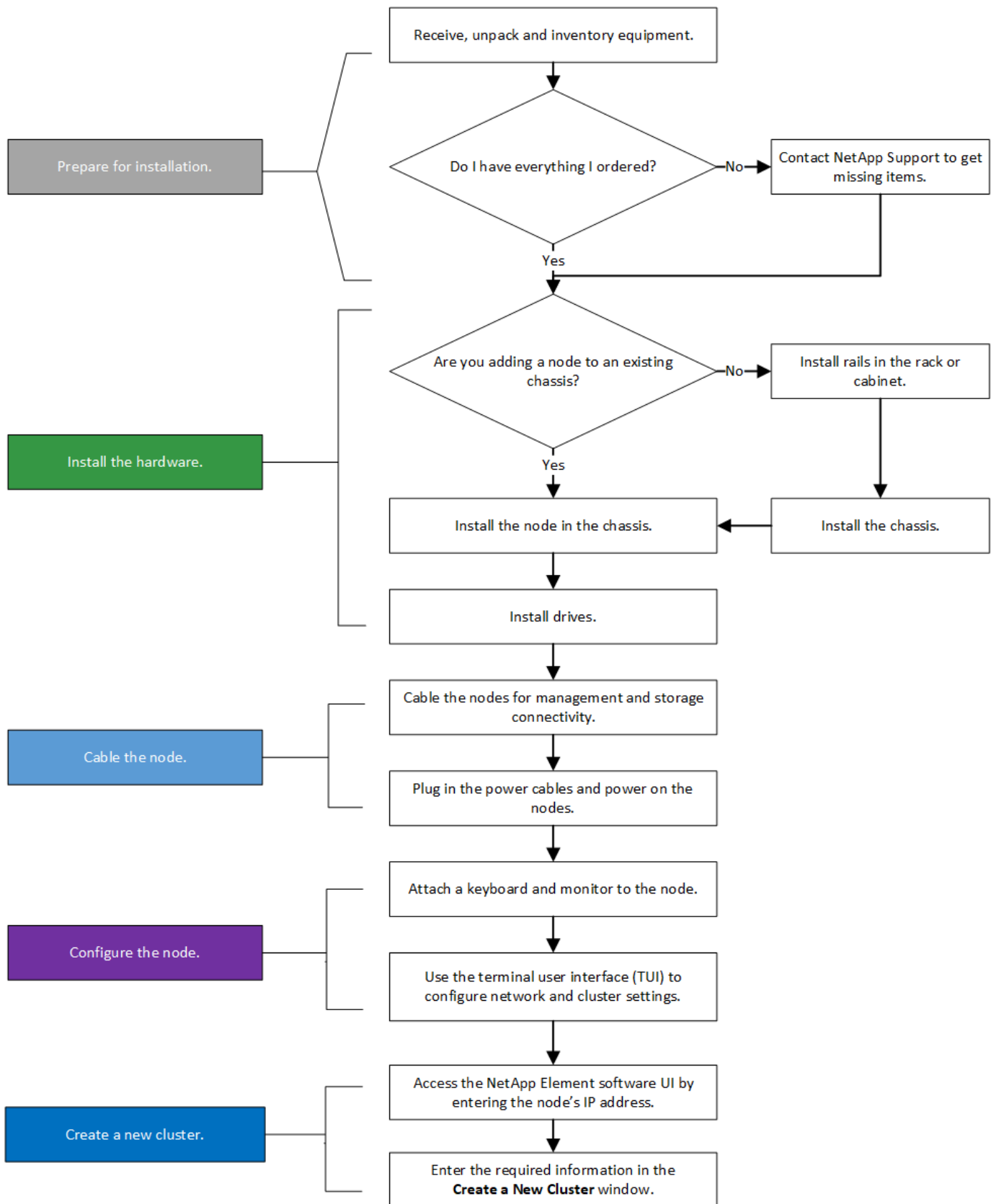
Vedi il ["poster"](#) per una rappresentazione visiva delle istruzioni.

- [Diagrammi di flusso di lavoro](#)
- [Prepararsi per l'installazione](#)
- [Installare le rotaie](#)
- [Installare e cablare i nodi](#)
- [Configurare i nodi](#)
- [Creare un cluster](#)

Diagrammi di flusso di lavoro

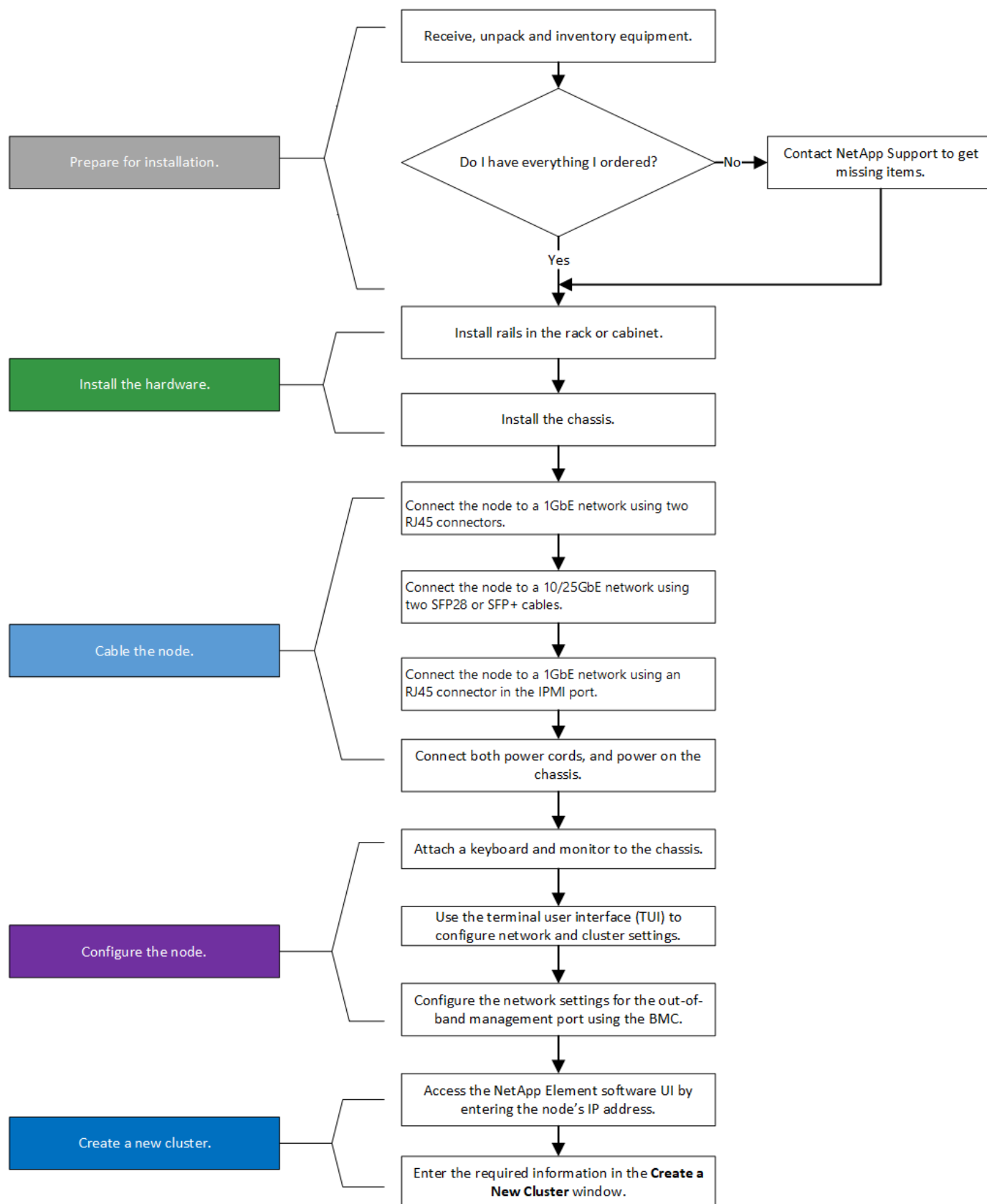
I diagrammi del flusso di lavoro qui riportati forniscono una panoramica generale dei passaggi di installazione. I passaggi variano leggermente a seconda del modello della serie H.

H410S





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



Prepararsi per l'installazione

In preparazione all'installazione, fai un inventario dell'hardware che ti è stato spedito e contatta l'assistenza NetApp se uno qualsiasi degli elementi risulta mancante.

Assicurarsi di avere i seguenti elementi nel luogo 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 transceiver a collegamento diretto SFP28/SFP+
- Cavi CAT5e o superiori con connettore RJ45
- Uno switch tastiera, video, mouse (KVM) per configurare il tuo sistema
- Chiavetta USB (facoltativa)



L'hardware che ti verrà spedito dipenderà da ciò che ordini. Un nuovo ordine da 2U a quattro nodi include lo chassis, la cornice, il kit di guide di scorrimento, le unità, i nodi di archiviazione e i cavi di alimentazione (due per chassis). Se si ordinano i nodi di archiviazione H610S, le unità vengono fornite installate nello chassis.



Durante l'installazione dell'hardware, assicurarsi di rimuovere tutto il materiale di imballaggio e la pellicola dall'unità. Ciò impedirà il surriscaldamento e lo spegnimento dei nodi.

Installare le rotaie

L'ordine hardware che ti è stato spedito include un set di guide di scorrimento. Per completare l'installazione della guida sarà necessario un cacciavite. I passaggi di installazione variano leggermente per ogni modello di nodo.



Installare l'hardware dal basso verso l'alto del rack per evitare che l'apparecchiatura si ribalti. Se il rack include dispositivi di stabilizzazione, installarli prima di installare l'hardware.

- [H410S](#)
- [H610S](#)

H410S

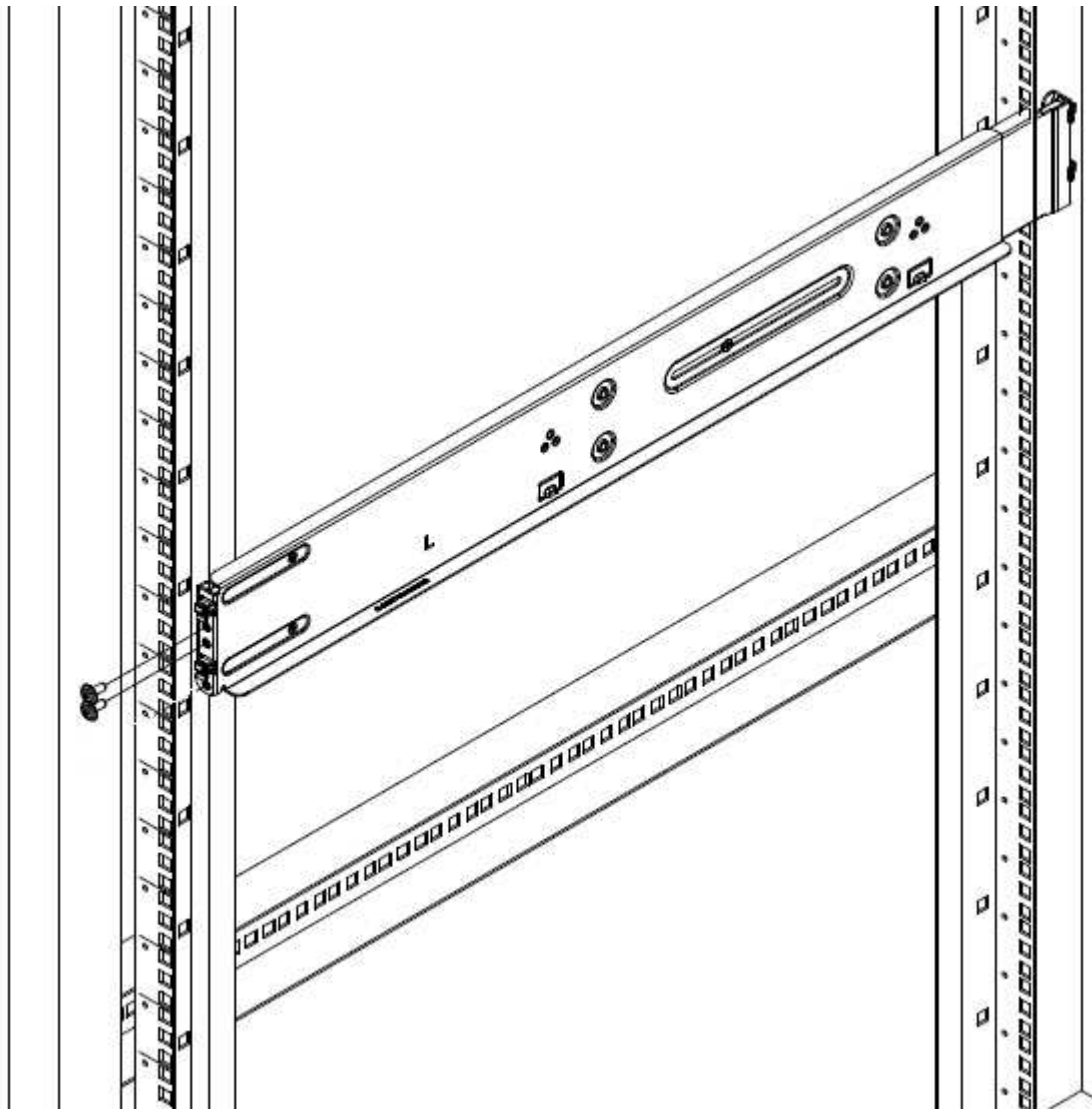
I nodi H410S sono installati in chassis H-Series 2U a quattro nodi, forniti con due set di adattatori. Se si desidera installare il telaio in un rack con fori rotondi, utilizzare gli adattatori adatti per rack con fori rotondi. Le guide per i nodi H410S si adattano a rack con profondità compresa tra 29 e 33,5 pollici. Quando la rotaia è completamente contratta, è lunga 28 pollici e le sezioni anteriore e posteriore della rotaia 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.

Passi

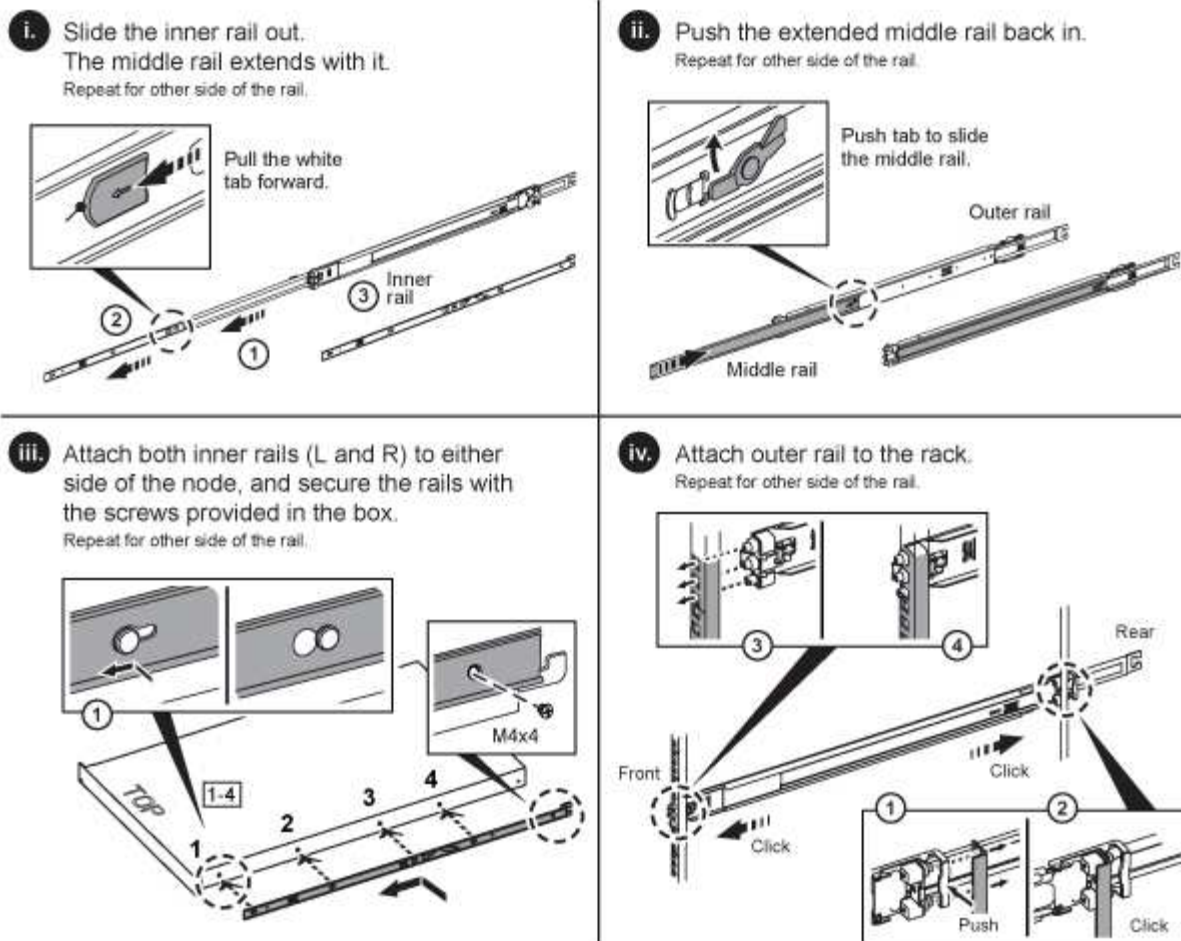
1. Allineare la parte anteriore della guida con i fori sul montante anteriore del rack.
2. Spingere i ganci sulla parte anteriore della guida nei fori sul montante anteriore del rack e poi verso il basso, finché i perni a molla non scattano nei fori del rack.
3. Fissare la guida al rack con le viti. Ecco un'illustrazione del binario sinistro fissato 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 rotaia con i fori appropriati sul montante posteriore, assicurandosi che la parte anteriore e quella posteriore della rotaia siano allo stesso livello.
6. Montare la parte posteriore della guida sul rack e fissarla con le viti.
7. Eseguire tutti i passaggi sopra descritti per l'altro lato del rack.

H610S

Ecco un'illustrazione per l'installazione delle guide per un nodo di archiviazione H610S:



L'H610S è dotato di binari sinistro e destro. 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

Installare il nodo di archiviazione H410S in uno chassis 2U a quattro nodi. Per H610S, installare lo chassis/nodo direttamente sulle guide del rack.



Rimuovere tutto il materiale di imballaggio e la pellicola dall'unità. Ciò impedisce che i nodi si surriscaldino e si spengano.

- [H410S](#)
- [H610S](#)

H410S

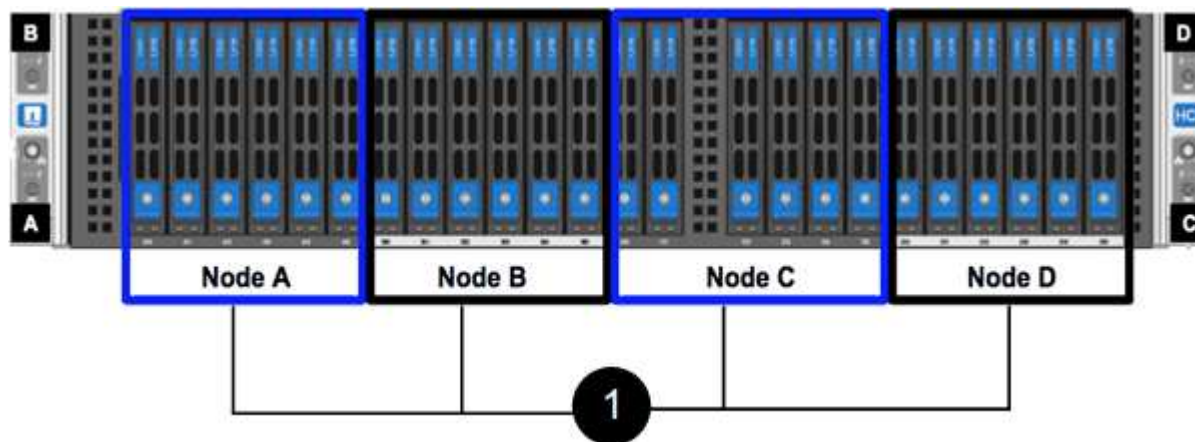
Passi

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



Prestare attenzione quando si solleva l'hardware e lo si installa nel rack. Un telaio vuoto da due unità rack (2U) e quattro nodi pesa 54,45 libbre (24,7 kg) e un nodo pesa 8,0 libbre (3,6 kg).

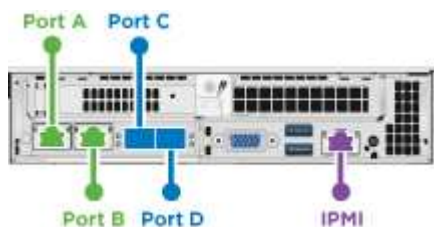
2. Installare le unità.



3. Cablare i nodi.



Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, si possono verificare 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 SFP28/SFP+ o transceiver nelle porte C e D per la connettività di archiviazione.
- (Facoltativo, consigliato) collegare un cavo CAT5e alla porta IPMI per la connettività di gestione fuori banda.

4. Collegare i cavi di alimentazione ai due alimentatori per chassis e inserirli nella PDU da 240 V o nella presa di corrente.

5. Accendere i nodi.



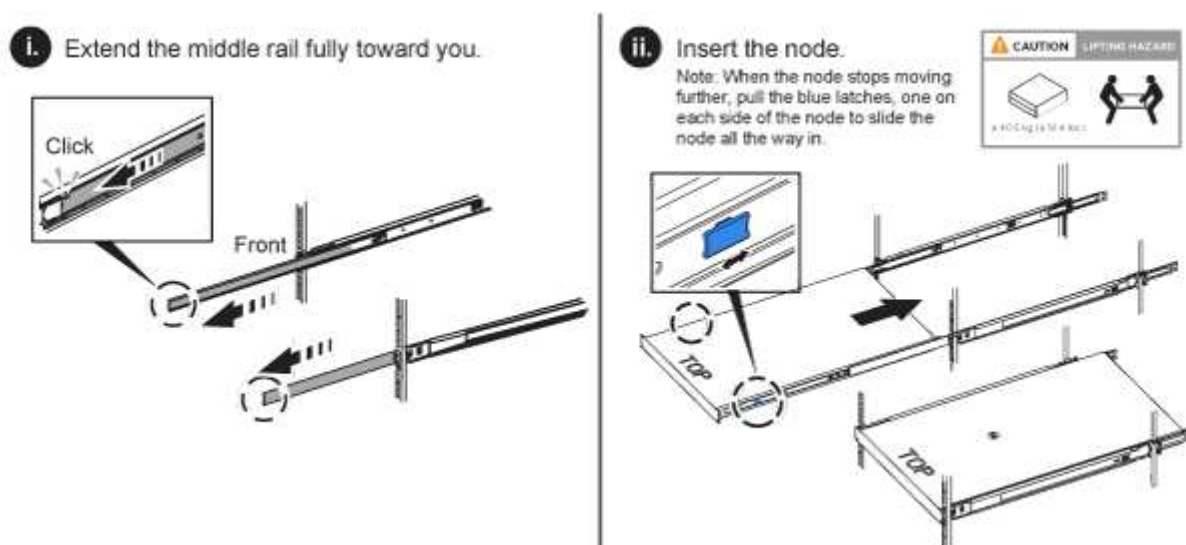
L'avvio del nodo richiede circa sei minuti.



H610S

Passi

1. Installare il telaio H610S. Ecco un'illustrazione per l'installazione del nodo/chassis nel rack:

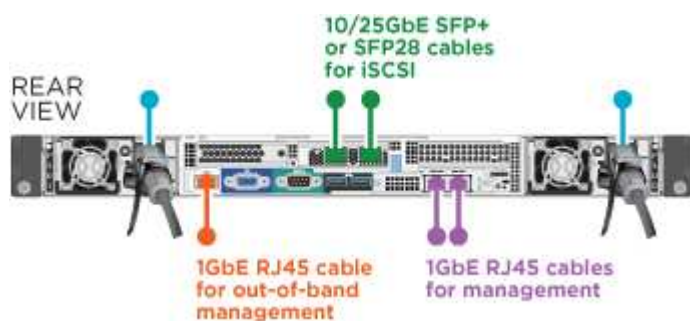


Prestare attenzione quando si solleva l'hardware e lo si installa nel rack. Un telaio H610S pesa 40,5 libbre (18,4 kg).

2. Cablare i nodi.



Se le prese d'aria sul retro del telaio sono bloccate da cavi o etichette, si possono verificare 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 installato e cablato l'hardware, sei pronto per configurare la tua nuova risorsa di archiviazione.

Passi

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



Dovresti ottenere l'indirizzo IP del nodo dalla TUI. Questa informazione è necessaria 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 <inserire collegamento alla sezione Configurazione>.

3. Configurare la gestione fuori banda 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. Accedi utilizzando **root** come nome utente e **calvin** come password.
 - c. Dalla schermata di gestione del nodo, vai su **Impostazioni > Impostazioni di rete** e configura i parametri di rete per la porta di gestione fuori banda.



Vedere ["questo articolo della Knowledge Base \(è richiesto l'accesso\)"](#) .

Creare un cluster

Dopo aver aggiunto il nodo di archiviazione all'installazione e configurato la nuova risorsa di archiviazione, sei pronto per creare un nuovo cluster di archiviazione

Passi

1. Da un client sulla stessa rete del nodo appena configurato, accedi all'interfaccia utente del software NetApp Element immettendo l'indirizzo IP del nodo.
2. Immettere le informazioni richieste nella finestra **Crea un nuovo cluster**. Vedi il ["panoramica della configurazione"](#) per maggiori informazioni.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituire un nodo H410S

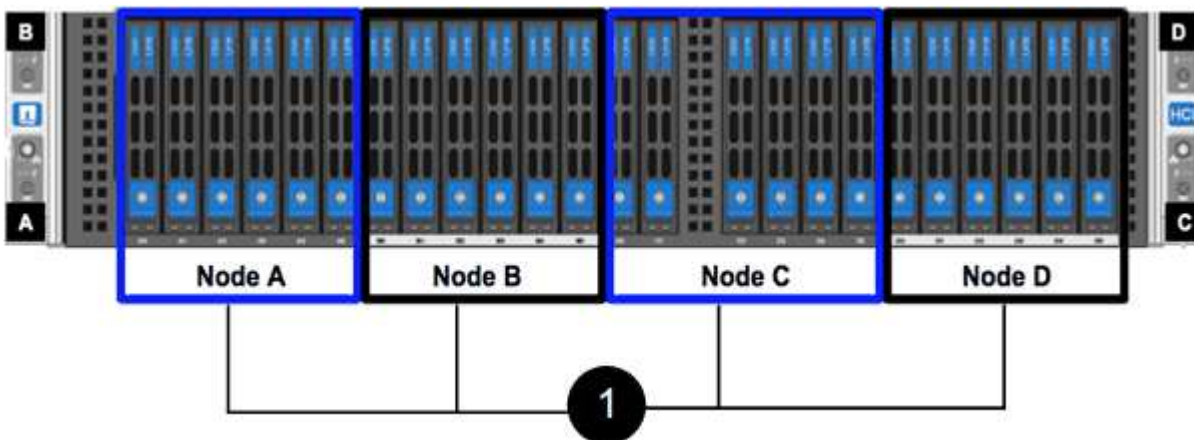
È necessario sostituire un nodo di archiviazione in caso di guasto della CPU, problemi alla scheda Radian, altri problemi alla scheda madre o se non si accende. Le istruzioni si applicano ai nodi di archiviazione H410S.

Gli allarmi nell'interfaccia utente del software NetApp Element ti avvisano quando un nodo di storage si guasta. Dovresti utilizzare l'interfaccia utente Element per ottenere il numero di serie (tag di servizio) del nodo non riuscito. Queste informazioni sono necessarie per individuare il nodo non riuscito nel cluster.

Ecco il retro di un telaio a due unità rack (2U), quattro nodi con quattro nodi di archiviazione:



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



Cosa ti servirà

- Hai verificato che il tuo nodo di archiviazione è difettoso e deve essere sostituito.
- Hai ottenuto un nodo di archiviazione sostitutivo.
- Hai un braccialetto antistatico (ESD) o hai adottato altre misure di protezione antistatiche.
- Hai etichettato ogni cavo collegato al nodo di archiviazione.

Ecco una panoramica generale dei passaggi:

- [Prepararsi a sostituire il nodo](#)
- [Sostituire il nodo nello chassis](#)
- [Aggiungi il nodo al cluster](#)

Prepararsi a sostituire il nodo

Prima di installare il nodo sostitutivo, è necessario rimuovere correttamente il nodo di archiviazione difettoso dal cluster nell'interfaccia utente del software NetApp Element . Puoi farlo senza causare alcuna interruzione del servizio. Dovresti ottenere il numero di serie del nodo di archiviazione difettoso dall'interfaccia utente di Element e confrontarlo con il numero di serie sull'adesivo sul retro del nodo.

Passi

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

Opzione	Passi
Per rimuovere singole unità	a. Fare clic su Azioni per l'unità che si desidera rimuovere. b. Fare clic su Rimuovi.
Per rimuovere più unità	a. Seleziona tutte le unità che vuoi rimuovere e fai clic su Azioni in blocco. b. Fare clic su Rimuovi.

3. Selezionare **Cluster > Nodi**.
4. Annotare il numero di serie (etichetta di servizio) del nodo difettoso. Dovresti abbinarlo al numero di serie sull'adesivo sul retro del nodo.
5. Dopo aver annotato il numero di serie, rimuovere il nodo dal cluster come segue:
 - a. Selezionare il pulsante **Azioni** per il nodo che si desidera rimuovere.
 - b. Seleziona **Rimuovi**.

Sostituire il nodo nello chassis

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

Passi

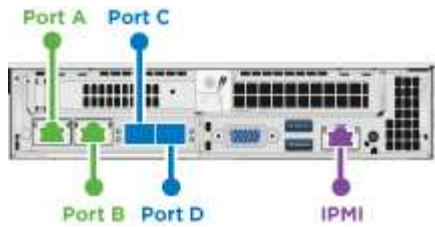
1. Indossare una protezione antistatica prima di procedere.
2. Disimballare il nuovo nodo di archiviazione e posizionarlo su una superficie piana vicino allo chassis.

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

3. Etichettare ogni cavo inserito nella parte posteriore del nodo di archiviazione che si desidera rimuovere.

Dopo aver installato il nuovo nodo di archiviazione, è necessario inserire i cavi nelle porte originali.

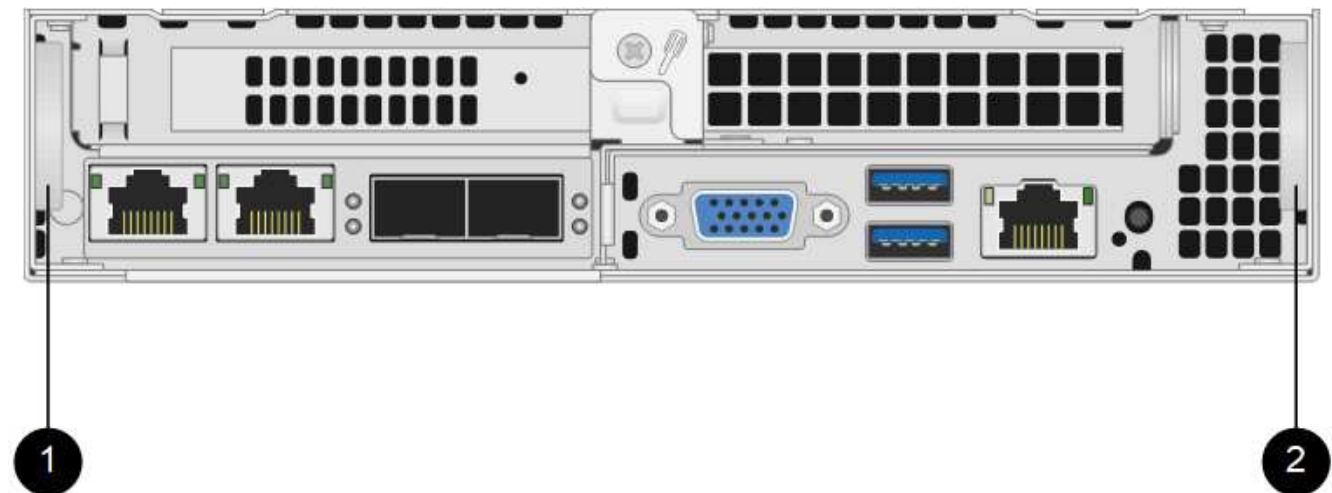
Ecco un'immagine che mostra il retro di un nodo di archiviazione:



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

- Scollegare tutti i cavi dal nodo di archiviazione.
- Tirare verso il basso la maniglia a camma sul lato destro del nodo ed estrarre il nodo utilizzando entrambe le maniglie a camma.

La maniglia della camma che si tira verso il basso ha una freccia che indica la direzione in cui si muove. L'altra maniglia della camma non si muove e serve ad aiutarti a estrarre il nodo.



Articolo	Descrizione
1	Maniglia a camma per aiutarti a estrarre il nodo.
2	Maniglia a camma che si tira verso il basso prima di estrarre il nodo.



Quando lo si estrae dallo chassis, sostenere il nodo con entrambe le mani.

6. Posizionare il nodo su una superficie piana.

È necessario impacchettare il nodo e restituirlo a NetApp.

7. Installare il nodo sostitutivo nello stesso slot dello chassis.



Assicurarsi di non esercitare una forza eccessiva quando si fa scorrere il nodo nello chassis.

8. Spostare le unità dal nodo rimosso e inserirle nel nuovo nodo.

9. Ricollegare i cavi alle porte dalle quali erano stati originariamente scollegati.

Le etichette che avevi sui cavi quando li hai scollegati ti saranno utili.



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

b. Non forzare i cavi nelle porte; potresti danneggiare i cavi, le porte o entrambi.



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.

Aggiungi 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 tramite l'interfaccia utente o l'API di Element prima che possano partecipare al cluster.

La versione del software su 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, secondo necessità.

Passi

1. Selezionare **Cluster > Nodi**.

2. Selezionare **In attesa** per visualizzare l'elenco dei nodi in attesa.

3. Eseguire una delle seguenti operazioni:

- Per aggiungere singoli nodi, seleziona l'icona **Azioni** per il nodo che desideri aggiungere.
- Per aggiungere più nodi, seleziona la casella di controllo dei nodi da aggiungere, quindi **Azioni in blocco**.



Se il nodo che stai 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. Dopo l'aggiornamento, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo sarà in un `pendingActive` stato.

4. Selezionare **Aggiungi**.

Il nodo appare nell'elenco dei nodi attivi.

5. Dall'interfaccia utente di Element, seleziona **Cluster > Unità**.

6. Selezionare **Disponibile** per visualizzare l'elenco delle unità disponibili.
7. Eseguire una delle seguenti operazioni:
 - Per aggiungere singole unità, seleziona l'icona **Azioni** per l'unità che desideri aggiungere, quindi seleziona **Aggiungi**.
 - Per aggiungere più unità, seleziona le caselle di controllo delle unità da aggiungere, seleziona **Azioni in blocco**, quindi seleziona **Aggiungi**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituisci un nodo H610S

Potrebbe essere necessario sostituire lo chassis in caso di guasto della ventola, dell'unità di elaborazione centrale (CPU) o del modulo di memoria dual inline (DIMM), oppure per risolvere problemi di surriscaldamento o problemi con il processo di avvio. Il LED ambra lampeggiante nella parte anteriore del telaio indica la possibile necessità di sostituire il telaio. Prima di procedere, contattare l'assistenza NetApp .



Vedi il ["Articolo della Knowledge Base"](#) per informazioni sui requisiti di installazione per i nodi H610S. I nodi di archiviazione H610S nuovi e di riserva potrebbero avere requisiti di installazione aggiuntivi in base alla versione software Element esistente del cluster di archiviazione. Per ulteriori informazioni, contattare l'assistenza NetApp .



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

Procedure consigliate per l'aggiunta e la rimozione di unità

Per aggiungere unità al cluster, è opportuno seguire queste best practice:

- Aggiungere tutte le unità a blocchi e assicurarsi che la sincronizzazione dei blocchi sia completa prima di aggiungere le unità slice.
- Per Element Software 10.x e versioni successive, aggiungere tutte le unità a blocchi contemporaneamente. Assicuratevi di non eseguire questa operazione su più di tre nodi contemporaneamente.
- Per il software Element 9.x e versioni precedenti, aggiungere tre unità contemporaneamente, consentendo loro di sincronizzarsi completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere l'unità slice e assicurarsi che la sincronizzazione delle slice sia completa prima di rimuovere le unità block.
- Rimuovere contemporaneamente tutte le unità a blocchi da un singolo nodo. Assicuratevi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

Cosa ti servirà

- Hai contattato l'assistenza NetApp . Se si ordina una sostituzione, è necessario aprire un caso con il supporto NetApp .

- Hai ottenuto il nodo sostitutivo.
- Hai un braccialetto antistatico (ESD) o hai adottato altre misure di protezione antistatiche.
- Se devi eseguire il processo di restituzione dell'immagine di fabbrica (RTFI), hai ottenuto la chiave USB. Il supporto NetApp può aiutarti a decidere se è necessario eseguire il processo RTFI.
- Hai una tastiera e un monitor.
- Hai rimosso correttamente il nodo non riuscito dal cluster.
- Se un DIMM è guasto, è necessario rimuovere le unità prima di rimuovere il nodo dal cluster.

Informazioni su questo compito

Gli allarmi nell'interfaccia utente di Element ti avvisano quando un host non funziona. È necessario far corrispondere il numero di serie dell'host non riuscito del VMware vSphere Web Client con il numero di serie sull'adesivo sul retro del nodo.

Passi

1. Individuare l'etichetta di servizio nella parte anteriore del telaio guasto.



2. Verificare che il numero di serie sull'etichetta di servizio corrisponda al numero del caso di supporto NetApp quando è stato ordinato lo chassis sostitutivo.
3. Collegare la tastiera e il monitor al retro dello chassis guasto.
4. Verificare il numero di serie del nodo non riuscito con il supporto NetApp .
5. Spegnerne il telaio.
6. Etichettare le unità nella parte anteriore e i cavi nella parte posteriore con la loro posizione, in modo da poterli riposizionare nelle stesse posizioni dopo la sostituzione. Per il posizionamento delle unità nello chassis, vedere l'immagine seguente:



7. Rimuovere i cavi.
8. Rimuovere il telaio svitando le viti a testa zigrinata sulle alette di montaggio. Dovresti 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.



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

11. Rimuovere gli alimentatori dallo chassis guasto e inserirli nello chassis sostitutivo.
12. Inserire i cavi di alimentazione e i cavi di rete nelle porte originali.
13. I transceiver Small Form-Factor Pluggable (SFP) potrebbero essere inseriti nelle porte 10GbE del nodo sostitutivo. Dovresti rimuoverli prima di cablare le porte 10GbE.



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

14. Accendere il telaio premendo il pulsante di accensione nella parte anteriore. L'avvio del nodo richiede circa cinque minuti e 30 secondi.
15. Eseguire i passaggi di configurazione.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituire le unità

Se un'unità è difettosa o se il suo livello di usura scende al di sotto di una determinata soglia, è necessario sostituirla. Gli allarmi nell'interfaccia utente del software Element ti avvisano quando un'unità si è guastata o sta per guastarsi. È possibile sostituire a caldo un'unità guasta.

Informazioni su questo compito

Questa procedura serve per sostituire le unità nei nodi di archiviazione H410S e H610S. La rimozione di un'unità comporta la disconnessione dell'unità stessa. Tutti i dati presenti sull'unità vengono rimossi e migrati su altre unità del cluster. La migrazione dei dati su altre unità attive nel sistema può richiedere da alcuni minuti a un'ora, a seconda dell'utilizzo della capacità e dell'I/O attivo sul cluster. Per la gestione delle unità durante la rimozione e la sostituzione, è opportuno seguire queste buone pratiche:

- Conservare l'unità nella custodia ESD finché non si è pronti a installarla.
- Aprire il sacchetto ESD manualmente o tagliare la parte superiore con un paio di forbici.
- Indossare sempre un braccialetto antistatico collegato a una superficie non verniciata del telaio.
- Utilizzare sempre entrambe le mani quando si rimuove, si installa o si trasporta un'unità.
- Non forzare mai un'unità nello chassis.
- Per la spedizione delle unità utilizzare sempre imballaggi approvati.
- Non impilare le unità una sopra l'altra.

Procedure consigliate per l'aggiunta e la rimozione di unità

- Aggiungere tutte le unità a blocchi e assicurarsi che la sincronizzazione dei blocchi sia completa prima di aggiungere le unità slice.
- Per Element Software 10.x e versioni successive, aggiungere tutte le unità a blocchi contemporaneamente. Assicuratevi di non eseguire questa operazione su più di tre nodi contemporaneamente.
- Per il software Element 9.x e versioni precedenti, aggiungere tre unità contemporaneamente, consentendo loro di sincronizzarsi completamente prima di aggiungere il gruppo successivo di tre.
- Rimuovere l'unità slice e assicurarsi che la sincronizzazione delle slice sia completa prima di rimuovere le unità block.
- Rimuovere contemporaneamente tutte le unità a blocchi da un singolo nodo. Assicuratevi che la sincronizzazione di tutti i blocchi sia completa prima di passare al nodo successivo.

Passi

1. Rimuovere l'unità dal cluster utilizzando l'interfaccia utente del software NetApp Element :
 - a. Dall'interfaccia utente di Element, selezionare **Cluster > Unità**.
 - b. Selezionare **Non riuscito** per visualizzare l'elenco delle unità non riuscite.
 - c. Prendi nota del numero di slot dell'unità guasta. Queste informazioni sono necessarie per individuare l'unità guasta nello chassis.
 - d. Selezionare **Azioni** per l'unità che si desidera rimuovere.
 - e. Seleziona **Rimuovi**.



Se non c'è abbastanza capacità per rimuovere le unità attive prima di rimuovere un nodo, viene visualizzato un messaggio di errore quando si conferma la rimozione dell'unità. Dopo aver risolto l'errore, è possibile rimuovere fisicamente l'unità dallo chassis.

2. Sostituire l'unità dallo chassis:
 - a. Disimballare l'unità sostitutiva e posizionarla su una superficie piana e priva di elettricità statica, vicino al rack. Conservare il materiale di imballaggio per quando si restituirà l'unità guasta a NetApp. Ecco la vista frontale dei nodi di archiviazione H610S e H410S con le unità:

H610S storage node



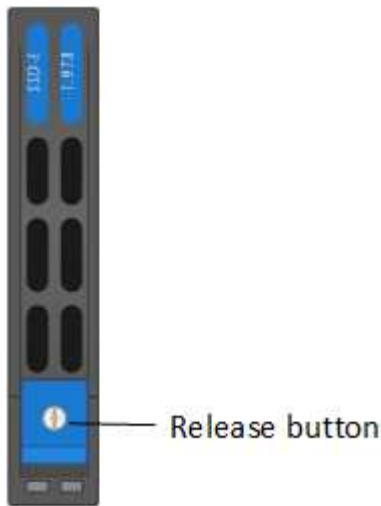
H410S storage nodes in a four-node chassis



- b. **(Solo H410S)** Eseguire i seguenti passaggi:
 - i. Identifica il nodo confrontando il numero di serie (tag di servizio) con il numero annotato nell'interfaccia utente di Element. Il numero di serie si trova su un adesivo sul retro di ogni nodo.

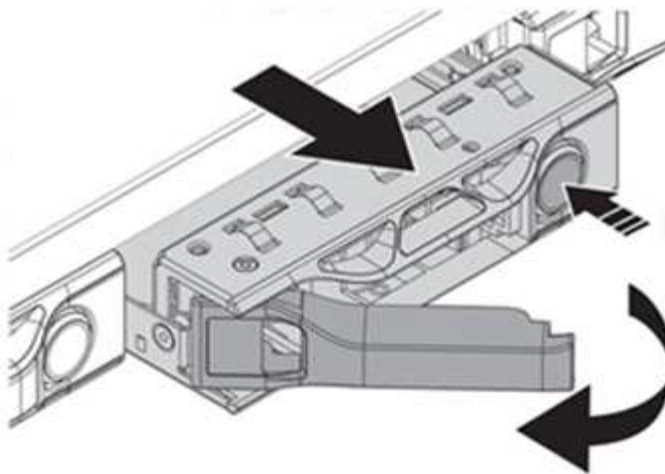
Dopo aver identificato il nodo, è possibile utilizzare le informazioni sullo slot per identificare lo slot in cui si trova l'unità guasta. Le unità sono ordinate alfabeticamente dalla A alla D e dallo 0 al 5.

- ii. Rimuovere la lunetta.
- iii. Premere il pulsante di rilascio sull'unità guasta:



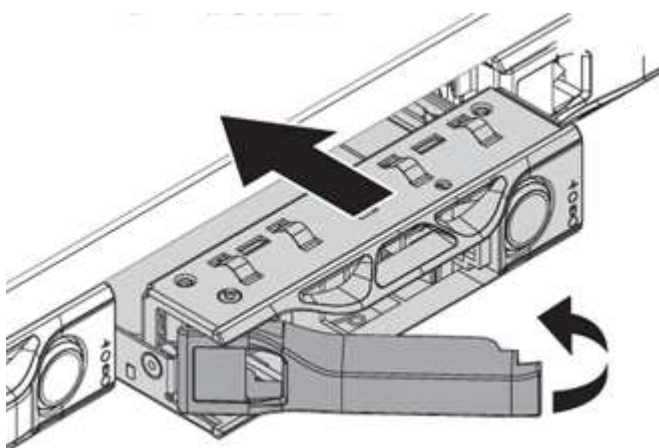
Quando si preme il pulsante di rilascio, la maniglia a camma sulla trasmissione si apre parzialmente e la trasmissione si stacca dal piano centrale.

- i. Aprire la maniglia della camma e far scorrere con cautela l'unità fuori usando entrambe le mani.
 - ii. Posizionare l'unità su una superficie piana e antistatica.
 - iii. Inserire l'unità sostitutiva nello slot fino in fondo nel telaio, utilizzando entrambe le mani.
 - iv. Premere la maniglia della camma verso il basso finché non scatta.
 - v. Reinstallare la lunetta.
 - vi. Informare il supporto NetApp della sostituzione dell'unità. Il supporto NetApp fornirà istruzioni per la restituzione dell'unità guasta.
- c. **(Solo H610S)** Eseguire i seguenti passaggi:
- i. Abbinare il numero di slot dell'unità guasta dall'interfaccia utente di Element con il numero sullo chassis. Il LED sull'unità guasta è illuminato in ambra.
 - ii. Rimuovere la lunetta.
 - iii. Premere il pulsante di rilascio e rimuovere l'unità guasta come mostrato nella seguente illustrazione:



Prima di provare a far scorrere l'unità fuori dallo chassis, assicurarsi che la maniglia del vassoio sia completamente aperta.

- 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. La maniglia del vassoio dell'unità si apre a scatto.



- iii. Inserire l'unità sostitutiva senza esercitare una forza eccessiva. Quando l'unità è completamente inserita, si sente un clic.
- iv. Chiudere con cautela la maniglia del vassoio dell'unità.
- v. Reinstallare la lunetta.
- vi. Informare il supporto NetApp della sostituzione dell'unità. Il supporto NetApp fornirà istruzioni per la restituzione dell'unità guasta.

3. Aggiungere nuovamente l'unità al cluster utilizzando l'interfaccia utente di Element.



Quando si installa una nuova unità in un nodo esistente, l'unità viene automaticamente registrata come **Disponibile** nell'interfaccia utente di Element. È necessario aggiungere l'unità al cluster prima che possa partecipare al cluster.

- a. Dall'interfaccia utente di Element, selezionare **Cluster > Unità**.
- b. Selezionare **Disponibile** per visualizzare l'elenco delle unità disponibili.
- c. Selezionare l'icona Azioni per l'unità che si desidera aggiungere e selezionare **Aggiungi**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituire un alimentatore

Ogni telaio include due alimentatori per la ridondanza di potenza. Se un alimentatore è difettoso, è necessario sostituirlo il prima possibile per garantire che il telaio disponga di una fonte di alimentazione ridondante.

Cosa ti servirà

- Hai stabilito che l'alimentatore è difettoso.
- Hai un alimentatore sostitutivo.
- Hai verificato che il secondo alimentatore sia funzionante.
- Hai un braccialetto antistatico (ESD) o hai preso altre precauzioni antistatiche.

Informazioni su questo compito

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

- Chassis NetApp HCI a due unità rack (2U) e quattro nodi
- Un telaio di archiviazione 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'unità di alimentazione guasta, facendo riferimento ad essa come PS1 o PS2. In uno chassis NetApp HCI 2U a quattro nodi, PS1 si riferisce all'unità nella fila superiore dello chassis e PS2 si riferisce all'unità nella fila inferiore dello chassis. È possibile sostituire l'alimentatore difettoso mentre il telaio è acceso e funzionante, a condizione che l'alimentatore ridondante sia funzionante.



Se si sostituiscono entrambi gli alimentatori in un nodo, è necessario che abbiano lo stesso codice articolo e la stessa potenza. Gli alimentatori non abbinati potrebbero danneggiare il sistema.

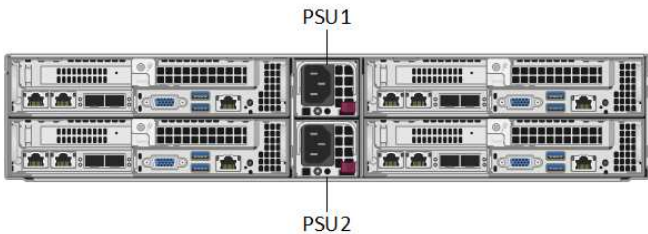
Passi

1. Individuare l'alimentatore difettoso nello chassis. Il LED sull'unità difettosa è di colore ambra.

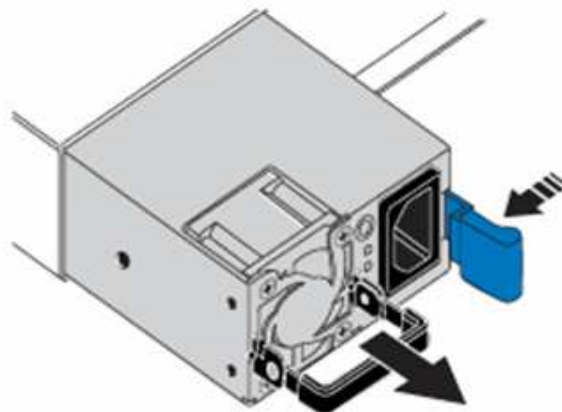
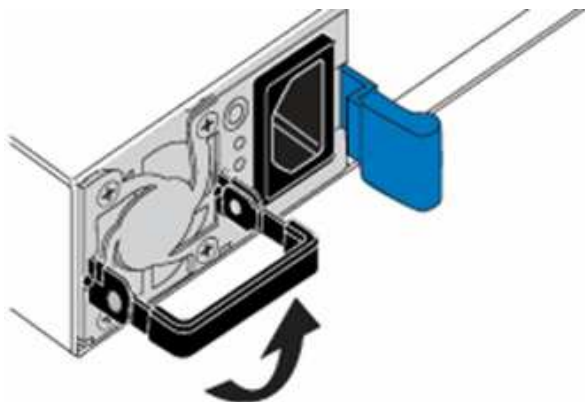


Le unità di alimentazione sono posizionate in modo diverso a seconda del tipo di telaio.

Per individuare la posizione degli alimentatori, vedere le immagini sottostanti:

Modello	Ubicazione delle unità di alimentazione
Chassis di storage NetApp HCI a quattro nodi, 2U	 PSU1 PSU2  I nodi nel tuo chassis potrebbero apparire diversi a seconda del tipo di nodi (di storage o di elaborazione) di cui disponi.
Telaio H610S	 PSU1 PSU0

2. Identificare il nodo corretto utilizzando l'etichetta estraibile blu o il numero di serie. L'etichetta blu estraibile riporta il numero di serie (S/N) e il layout dell'unità. Confermare il numero di serie del nodo da sottoporre a manutenzione.
 - Se si sostituiscono entrambi gli alimentatori, procedere al passaggio 3.
 - Se si sostituisce solo un alimentatore, passare al passaggio 4.
3. Verificare che il nodo sia stato spento o sia pronto per essere spento per l'assistenza. Notare quanto segue:
 - Un nodo che è stato spento non visualizza alcun LED di alimentazione blu sulle unità o sul pulsante di accensione.
 - Un nodo che non è ancora stato spento mostra LED blu sulle unità e sul pulsante di accensione.
 - Un nodo che è stato spento ed è pronto per il servizio visualizza un LED PSU lampeggiante che lampeggia (verde) e spento (nessun colore).
 - Un nodo che non è ancora stato spento mostra LED verdi fissi sugli alimentatori.
4. Scollegare il cavo di alimentazione dall'alimentatore o entrambi i cavi di alimentazione, se si sostituiscono entrambe le unità.
5. Sollevare la maniglia della cappa e premere il fermo blu per far scorrere fuori l'alimentatore.



L'illustrazione è un esempio. La posizione dell'alimentatore 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.

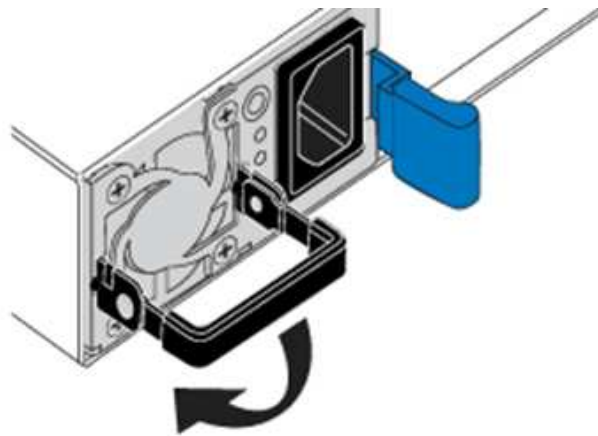
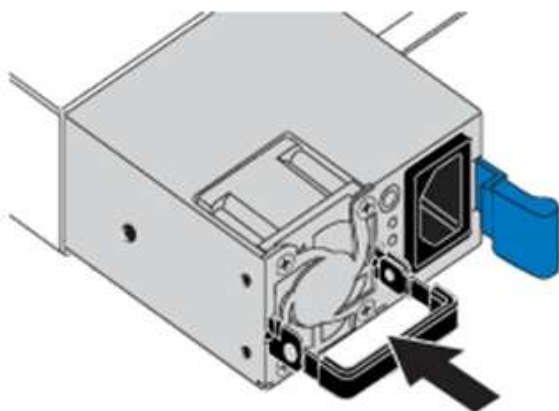
Ripetere i passaggi 3, 4 e 5 se si sostituisce un secondo alimentatore.

6. Individuare l'etichetta sull'alimentatore rimosso dallo chassis. L'etichetta contiene i dettagli del produttore e la potenza in uscita.



Non sostituire l'alimentatore se la potenza in watt dell'alimentatore fornito tramite RMA non corrisponde a quella dell'alimentatore rimosso. Per i passaggi successivi, contattare l'assistenza NetApp.

7. Utilizzando entrambe le mani, allineare i bordi dell'alimentatore con l'apertura nello chassis, spingere delicatamente l'unità nello chassis utilizzando la maniglia a camma finché non si blocca in posizione e riportare la maniglia a camma in posizione verticale.



8. Collegare uno o entrambi i cavi di alimentazione.
9. Se hai sostituito entrambi gli alimentatori, vai nella parte anteriore del nodo e premi il pulsante di accensione per accendere i nodi. Dopo l'accensione, il LED del pulsante di accensione si illumina di blu fisso. I LED blu delle unità e il pulsante di identificazione inizieranno a lampeggiare.
10. Restituisci l'unità difettosa a NetApp seguendo le istruzioni contenute nella scatola che ti è stata spedita.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Informazioni sull'hardware della serie SF

Sostituire un telaio

Potrebbe essere necessario sostituire lo chassis in caso di guasto della ventola, dell'unità di elaborazione centrale (CPU) o del modulo di memoria dual inline (DIMM), oppure per risolvere problemi di surriscaldamento o problemi con il processo di avvio. Errori del cluster nell'interfaccia utente (UI) del software NetApp Element e la luce ambra lampeggiante nella parte anteriore dello chassis sono indicazioni di una possibile necessità di sostituzione dello chassis. Prima di procedere, contattare l'assistenza NetApp .

Cosa ti servirà

- Hai contattato l'assistenza NetApp .

Se si ordina una sostituzione, è necessario aprire un caso con il supporto NetApp .

- Hai ottenuto il telaio sostitutivo.
- Hai un bracciale antistatico (ESD) o hai adottato altre misure di protezione antistatiche.
- Se devi eseguire il processo di restituzione dell'immagine di fabbrica (RTFI), hai ottenuto la chiave USB.

Il supporto NetApp ti aiuterà a decidere se è necessario RTFI. Vedere ["questo articolo della Knowledge Base \(è richiesto l'accesso\)"](#) .

- Hai una tastiera e un monitor.

Informazioni su questo compito

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

- SF2405
- SF4805
- SF9605
- SF9608
- SF19210
- SF38410
- SF-FCN-01
- FC0025

A seconda della versione del software Element, i seguenti nodi non sono supportati:



- A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
- A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608 e nodi FC FC0025 e SF-FCN-01.
- A partire dai nodi di archiviazione Element 12.0, SF3010, SF6010 e SF9010.

Passi

1. Individuare l'etichetta di servizio dello chassis guasto e verificare che il numero di serie corrisponda al numero riportato sulla custodia aperta presso l'assistenza NetApp quando è stato ordinato il componente sostitutivo.

È possibile individuare l'etichetta di servizio nella parte anteriore del telaio.

La figura seguente è un esempio del tag di servizio:



La figura sopra è un esempio. La posizione esatta del tag di servizio potrebbe variare a seconda del modello hardware.

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



I nodi Fibre Channel non hanno unità nella parte anteriore.

6. Rimuovere gli alimentatori e i cavi.
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 il telaio premendo il fermo o svitando la vite a testa zigrinata, a seconda del modello hardware.

Dovresti imballare e restituire lo chassis guasto a NetApp.

9. **Facoltativo:** rimuovere le guide e installare quelle nuove fornite con il telaio sostitutivo.

È possibile scegliere di riutilizzare le rotaie esistenti. Se si riutilizzano le rotaie esistenti, è possibile saltare questo passaggio.

10. Far scorrere il telaio sostitutivo sulle guide.

11. Per i nodi di archiviazione, inserire le unità dallo chassis guasto allo chassis sostitutivo.



Dovresti inserire le unità negli stessi slot in cui si trovavano nello chassis guasto.

12. Installare gli alimentatori.

13. Inserire i cavi di alimentazione e i cavi 1GbE e 10GbE nelle rispettive porte originali.

I transceiver Small Form-Factor Pluggable (SFP) potrebbero essere inseriti nelle porte 10GbE dello chassis sostitutivo. Dovresti rimuoverli prima di cablare le porte 10GbE.

14. Se hai stabilito che non è necessario eseguire il processo RTFI sul nodo, avvia il nodo e attendi che venga visualizzata l'interfaccia utente del terminale (TUI). Procedere al passaggio 16 e consentire al cluster di ricreare automaticamente l'immagine del nodo quando lo si aggiunge tramite l'interfaccia utente.

15. **Facoltativo:** se il supporto NetApp consiglia di ricreare l'immagine del nodo con una chiave USB, eseguire i seguenti passaggi secondari:

- Accendere il telaio. Si avvia con l'immagine della chiave RTFI.
- Al primo prompt, digitare **Y** per creare l'immagine del nodo di archiviazione.
- Al secondo prompt, digitare **N** per i controlli di integrità dell'hardware.

Se lo script RTFI rileva un problema con un componente hardware, visualizza un errore nella console. Se vedi un errore, contatta l'assistenza NetApp . Una volta completato il processo RTFI, il nodo si spegne.

- Rimuovere la chiavetta USB dallo slot USB.

- Avviare il nodo appena creato e attendere che venga visualizzata l'interfaccia utente guidata (TUI).

16. Configurare le informazioni di rete e cluster dalla TUI.

Per ricevere assistenza, puoi contattare il supporto NetApp .

17. Aggiungere il nuovo nodo al cluster utilizzando l'interfaccia utente terminale del cluster.

18. Imballare e restituire il telaio guasto.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituire le unità per i nodi di archiviazione della serie SF

È possibile sostituire a caldo un'unità a stato solido guasta con un'unità sostitutiva.

Cosa ti servirà

- Hai un'unità sostitutiva.
- Hai un braccialetto antistatico (ESD) o hai preso altre precauzioni antistatiche.
- Hai contattato l'assistenza NetApp per verificare che l'SSD debba essere sostituito e per ricevere assistenza sulla corretta procedura di risoluzione.

Quando chiami l'assistenza NetApp, ti serviranno il codice di matricola o il numero di serie. Il supporto collaborerà con te per ottenere un'unità sostitutiva in base al tuo Contratto di Servizio.

Informazioni su questo compito

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

- SF2405
- SF4805
- SF9605
- SF9608
- SF19210
- SF38410

A seconda della versione del software Element, i seguenti nodi non sono supportati:



- A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
- A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608.
- A partire dai nodi di archiviazione Element 12.0, SF3010, SF6010 e SF9010.

La figura seguente mostra il posizionamento delle unità in uno chassis SF9605:



La figura sopra è un esempio. SF9608 ha una disposizione delle unità diversa che include solo otto unità numerate da uno a otto, da sinistra a destra.

Lo slot 0 contiene l'unità metadati per il nodo. Se si sostituisce l'unità nello slot 0, è necessario applicare l'adesivo incluso nella scatola di spedizione sull'unità sostitutiva, in modo da poterla identificare separatamente dalle altre.

Seguire queste buone pratiche durante la gestione delle unità:



- Per evitare le scariche elettrostatiche (ESD), conservare l'unità nell'apposita custodia ESD finché non si è pronti a installarla.
- 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 la busta ESD e tutti i materiali di imballaggio nel caso in cui si debba restituire l'unità in un secondo momento.
- Indossare sempre un braccialetto antistatico collegato a una superficie non verniciata del telaio.
- Utilizzare sempre entrambe le mani quando si rimuove, si installa o si trasporta un'unità.
- Non forzare mai un'unità nello chassis.
- Non impilare le unità una sopra l'altra.
- Per la spedizione delle unità utilizzare sempre imballaggi approvati.

Ecco una panoramica generale dei passaggi:

- [Rimuovere l'unità dal cluster](#)
- [Sostituire l'unità dallo chassis](#)
- [Aggiungere l'unità al cluster](#)

Rimuovere l'unità dal cluster

Il sistema SolidFire segnala un'unità in stato di errore se l'autodiagnosi dell'unità segnala al nodo che si è verificata un'anomalia o se la comunicazione con l'unità si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco delle unità guaste. È necessario rimuovere un'unità guasta dall'elenco delle unità guaste nel software NetApp Element .

Passi

1. Nell'interfaccia utente di Element, seleziona **Cluster > Unità**.
2. Selezionare **Non riuscito** per visualizzare l'elenco delle unità non riuscite.
3. Annotare il numero di slot dell'unità guasta.

Queste informazioni sono necessarie per individuare l'unità guasta nello chassis.

4. Rimuovere l'unità guasta utilizzando uno dei seguenti metodi:

Opzione	Passi
Per rimuovere singole unità	a. Selezionare Azioni per l'unità che si desidera rimuovere. b. Seleziona Rimuovi.
Per rimuovere più unità	a. Seleziona tutte le unità che vuoi rimuovere e seleziona Azioni in blocco. b. Seleziona Rimuovi.

Sostituire l'unità dallo chassis

Dopo aver rimosso un'unità guasta dall'elenco delle unità guaste nell'interfaccia utente di Element, è possibile sostituirla fisicamente dallo chassis.

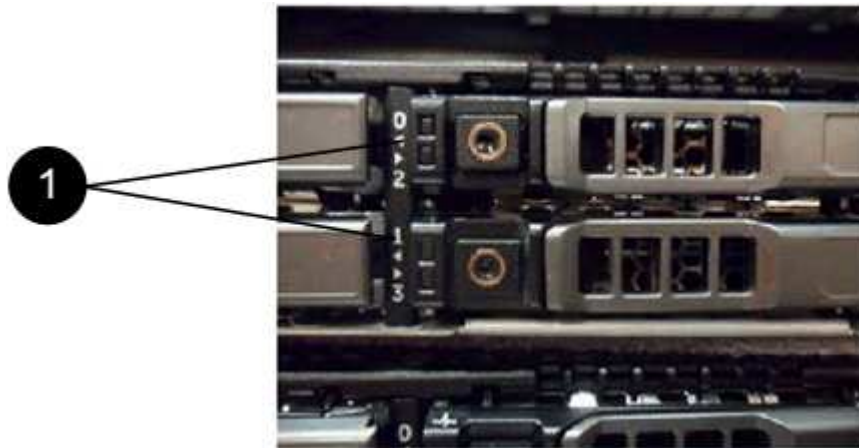
Passi

1. Disimballare l'unità sostitutiva e posizionarla su una superficie piana e priva di elettricità statica, vicino al rack.

Conservare il materiale di imballaggio per quando si restituirà l'unità guasta a NetApp.

2. Abbinare il numero di slot dell'unità guasta dall'interfaccia utente di Element con il numero sullo chassis.

La figura seguente è un esempio per mostrare la numerazione degli slot delle unità:



Articolo	Descrizione
1	Numeri degli slot dell'unità

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

Il fermo si apre con uno scatto.

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 della sostituzione dell'unità.

Il supporto NetApp fornirà istruzioni per la restituzione dell'unità guasta.

Aggiungere l'unità al cluster

Dopo aver installato una nuova unità nello chassis, questa viene registrata come disponibile. È necessario aggiungere l'unità al cluster tramite l'interfaccia utente di Element prima che possa partecipare al cluster.

Passi

1. Nell'interfaccia utente di Element, fare clic su **Cluster > Unità**.

2. Fare clic su **Disponibile** per visualizzare l'elenco delle unità disponibili.
3. Per aggiungere unità, seleziona una delle seguenti opzioni:

Opzione	Passi
Per aggiungere singole unità	a. Selezionare il pulsante Azioni per l'unità che si desidera aggiungere. b. Selezionare Aggiungi.
Per aggiungere più unità	a. Selezionare le caselle di controllo delle unità da aggiungere, quindi selezionare Azioni in blocco. b. Selezionare Aggiungi.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Sostituire un alimentatore

Ogni chassis SolidFire include due alimentatori per la ridondanza di alimentazione. Se un alimentatore si guasta, è necessario sostituirlo il prima possibile per garantire che il telaio disponga di una fonte di alimentazione ridondante.

Cosa ti servirà

- Hai stabilito che è necessario sostituire l'alimentatore.
- Hai un alimentatore sostitutivo.
- Hai verificato che il secondo alimentatore sia funzionante.
- Hai un braccialetto antistatico (ESD) o hai preso altre precauzioni antistatiche.

Informazioni su questo compito

Le istruzioni sono valide se si dispone di uno chassis con un'unità rack (1U) con uno qualsiasi dei seguenti nodi:

- SF2405
- SF4805
- SF9605
- SF9608
- SF19210
- SF38410
- SF-FCN-01
- FC0025

A seconda della versione del software Element, i seguenti nodi non sono supportati:



- A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
- A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608 e nodi FC FC0025 e SF-FCN-01.
- A partire dai nodi di archiviazione Element 12.0, SF3010, SF6010 e SF9010.

Passi

1. Scollegare il cavo di alimentazione dall'alimentatore che si desidera sostituire.
2. Premere il pulsante di rilascio per far scorrere l'alimentatore fuori dallo chassis.



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

3. Utilizzando entrambe le mani, allineare i bordi dell'alimentatore sostitutivo con l'apertura nello chassis e spingere delicatamente l'unità nello chassis.



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

4. Collegare il cavo di alimentazione.
5. Restituisci l'unità guasta a NetApp seguendo le istruzioni contenute nella scatola che ti è stata spedita.

Per ricevere assistenza sulla procedura di sostituzione, è possibile contattare l'assistenza NetApp .

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Ritorna alle informazioni sull'immagine di fabbrica

Configurare l'immagine di ritorno alla fabbrica

I sistemi di storage NetApp SolidFire utilizzano il processo Return To Factory Image (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 del software Element. Ciò include installazioni manuali interne eseguite dagli sviluppatori, installazioni automatiche tramite test 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 di nodo in uso, per risolvere automaticamente eventuali problemi.

Questa guida è rivolta agli integratori che installano, configurano, utilizzano o risolvono problemi relativi all'archiviazione.

- Linux: Hai una certa esperienza con i sistemi Linux.
- Networking: hai familiarità con le reti di server e con l'archiviazione in rete, inclusi indirizzi IP, maschere di rete 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.

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

- [Opzioni di distribuzione e installazione RTFI](#)
- [Eseguire il processo RTFI](#)
- [Menu delle opzioni RTFI](#)

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Opzioni di distribuzione e installazione RTFI

Il processo Return To Factory Image (RTFI) utilizza un supporto avviabile e installabile con un sistema operativo Linux minimalista e completamente autonomo per distribuire il software Element su un nodo. È possibile scaricare l'immagine ISO RTFI specifica per la versione del software Element da ["Sito di supporto NetApp"](#).

Dopo aver scaricato l'immagine ISO RTFI, è possibile distribuirla utilizzando uno dei seguenti metodi comunemente utilizzati:

- **Chiave USB fisica:** è possibile scrivere un'immagine ISO avviabile del software Element su una chiave USB. Per istruzioni, consultare l'articolo della Knowledge Base ["Come creare una chiave RTFI per ricreare l'immagine di un nodo di archiviazione SolidFire"](#). Inserire la chiave USB con l'ISO nel nodo ed eseguire l'avvio dalla chiave USB.
- **Supporti virtuali che utilizzano la porta di gestione del Baseboard Management Controller (BMC):** è possibile utilizzare il BMC per collegarsi dinamicamente all'ISO presente sul sistema client. L'ISO viene reso disponibile al sistema operativo host come unità virtuale (CD o DVD). Per ulteriori informazioni, consultare l'articolo della Knowledge Base ["Come eseguire l'RTFI di un nodo tramite BMC"](#).
- **Avvio di rete tramite Preboot Execution Environment (PXE), Trivial File Transfer Protocol (TFTP) o FTP:** invece di decomprimere manualmente un'immagine ISO, è possibile utilizzare `autoifs` per estrarre automaticamente un'immagine quando il processo RTFI lo richiede. Questo meccanismo di distribuzione richiede una maggiore configurazione iniziale, ma consente una corretta automazione e scalabilità dell'installazione.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Il processo RTFI

È possibile avviare il processo RTFI (Return to Factory Image) interagendo con il nodo tramite i prompt della console di testo che vengono visualizzati 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 tutte le unità su un nodo.
3. Convalida e aggiorna il firmware.
4. Controlla l'hardware.
5. Testa l'hardware.
6. Cancella in modo sicuro tutte le unità selezionate.
7. Partiziona l'unità radice e crea file system.
8. Monta e decompime l'immagine.
9. Configura il nome host, la rete (Dynamic Host Configuration Protocol), la configurazione predefinita del cluster e il bootloader GRUB.
10. Arresta tutti i servizi, raccoglie i registri e riavvia.

Per configurare il nodo dopo il completamento con successo del processo RTFI, vedere ["documentazione per la versione del software Element"](#). Dopo che un nodo ha completato con successo il processo RTFI, passa per impostazione predefinita allo stato *disponibile* (non configurato).

Eseguire il processo RTFI

Per ripristinare il software Element sul nodo SolidFire , utilizzare la seguente procedura.

Per informazioni sulla creazione di una chiave USB o sull'utilizzo del BMC per eseguire il processo RTFI, vedere [Opzioni di distribuzione e installazione RTFI](#) .

Prima di iniziare

Verifica di soddisfare i seguenti requisiti:

- Hai accesso a una console per il nodo SolidFire .
- Il nodo su cui si sta eseguendo il processo RTFI è acceso e connesso a una rete.
- Il nodo su cui si sta eseguendo il processo RTFI non fa parte di un cluster attivo.
- Hai accesso al supporto di installazione avviabile che contiene l'immagine della versione del software Element pertinente alla tua configurazione.

In caso di dubbi prima di eseguire il processo RTFI, contattare l'assistenza NetApp .

Passi

1. Collegare un monitor e una tastiera sul retro del nodo oppure connettersi all'interfaccia utente IP BMC e richiamare la console **iKVM/HTML5** dalla scheda **Controllo remoto** nell'interfaccia utente.
2. Inserire una chiavetta USB con un'immagine appropriata in uno dei due slot USB sul retro del nodo.
3. Accendere o ripristinare l'alimentazione del nodo. Durante l'avvio, selezionare il dispositivo di avvio premendo **F11**:



È necessario premere **F11** più volte in rapida successione perché la schermata del dispositivo di avvio scorre rapidamente.

4. Nel menu di selezione del dispositivo di avvio, evidenziare l'opzione USB.

Le opzioni visualizzate dipendono dalla marca USB utilizzata.



Se non sono elencati dispositivi USB, accedere al BIOS, verificare che l'USB sia elencato nell'ordine di avvio, riavviare e riprovare.

Se il problema persiste, accedi al BIOS, vai alla scheda **Salva ed esci**, seleziona **Ripristina impostazioni predefinite ottimizzate**, accetta e salva le impostazioni e riavvia.

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

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

6. Al prompt iniziale, ti verrà comunicato che il processo rimuoverà tutti i dati dal nodo e che i dati non saranno recuperabili dopo l'inizio del processo. Inserisci **Sì** per iniziare.



Tutti i dati e i dettagli di configurazione vengono cancellati definitivamente dal nodo dopo l'avvio del processo. Se scegli di non procedere, verrai indirizzato al [Menu delle opzioni RTFI](#) .



Se si desidera visualizzare la console durante il processo RTFI, è possibile premere i tasti **ALT+F8** per passare alla modalità dettagliata della console. 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 riceva l'indicazione di eseguire i test dal supporto NetApp .

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

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

Il nodo è ora pronto per essere acceso e configurato. Vedi il "[Documentazione di archiviazione della configurazione del software Element](#)" per configurare il nodo di archiviazione.

Se hai riscontrato un messaggio di errore durante il processo RTFI, vedi [Menu delle opzioni RTFI](#) .

Trova maggiori informazioni

- "[Documentazione del software SolidFire ed Element](#)"
- "[Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element](#)"

Menu delle opzioni RTFI

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



Contattare l'assistenza NetApp prima di utilizzare una qualsiasi delle seguenti opzioni di comando.

Opzione	Descrizione
Riavviare	Esce dal processo RTFI e riavvia il nodo nel suo stato attuale. Non viene eseguita alcuna pulizia.
Spegnimento	Spegne correttamente il nodo nel suo stato attuale. Non viene eseguita alcuna pulizia.

Opzione	Descrizione
Uscita	Esce dal processo RTFI e apre un prompt dei comandi.
Caricare i registri	Raccoglie tutti i log del sistema e carica un singolo archivio di log consolidato su un URL specificato.

Carica i registri

Raccogli tutti i registri del sistema e caricali su un URL specificato secondo la seguente procedura.

Passi

1. Al prompt del menu delle opzioni RTFI, immettere **UploadLogs**.
2. Inserisci le informazioni della directory remota:
 - a. Digitare un URL che includa il protocollo. Per esempio: `ftp://, scp://, http://, or https://`.
 - b. (Facoltativo) Aggiungi un nome utente e una password incorporati. Per esempio:
`scp://user:password@URLaddress.com`.



Per una gamma completa di opzioni di sintassi, vedere ["arricciare"](#) manuale utente.

Il file di registro viene caricato e salvato nella directory specificata come `.tbz2` archivio.

Utilizzare il tunnel di supporto

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

È possibile aprire una porta TCP per una connessione tunnel inversa SSH con il supporto NetApp. 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 disabilitata per impostazione predefinita sul nodo di gestione. Per abilitare 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 richieste le seguenti porte TCP:

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

Passi

- Accedi al tuo nodo di gestione e apri una sessione terminale.
- Al prompt, 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) Disabilita ["funzionalità di accesso remoto"](#) Ancora.



Se non lo si disabilita, SSH rimane abilitato sul nodo di gestione. La configurazione abilitata per SSH persiste sul nodo di gestione attraverso aggiornamenti e upgrade finché non viene disabilitata manualmente.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Nodi di archiviazione

Versioni del firmware supportate per i nodi di archiviazione della serie H e SolidFire .

- [H610S](#)
- [H410S](#)
- [SF38410, SF19210, SF9605 e SF4805](#)

H610S

Numero di modello (parte famiglia): H610S **Numeri di modello completi:** H610S-1, H610S-1-NE, H610S-2, H610S-2-NE, H610S-4, H610S-4-NE e H610S-2F

Firmware del componente gestito da un pacchetto firmware di archiviazione

Durante il periodo 11.x, il software NetApp Element era l'unico modo per rilasciare il firmware. A partire da Element 12.0, è stato introdotto il concetto di **Storage Firmware Bundle** e gli aggiornamenti del firmware sono ora possibili tramite uno Storage Firmware Bundle rilasciato in modo indipendente o incluso come parte di una versione di Element 12.x.



Un trattino (-) nella tabella seguente indica che il componente hardware specifico NON era supportato in quel dato veicolo di rilascio.

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.1 82. 0	20 24 -1 0- 17	3B 14	4.0 1.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,5	2,1 7	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 A0 2Q	11 09 3A 10	11 0B 3A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.1 75. 0	20 23 -0 6- 15	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,5	2,1 7	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 10 (S ED)	Un ità SK Hy ni x PE 80 10 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.1 64. 0	20 22 -1 0- 20	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 10 (S ED)	Un ità SK Hy ni x PE 80 10 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.1 64. 0 tra mi te Ne tA pp El e m en t 12. 7	20 22 -1 0- 20	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	16. 32. 10 10	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 60 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.1 50. 4	20 22 -0 6- 08	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.1 50. 4 tra mi te Ne tA pp El e m en t 12. 5	20 22 -0 6- 08	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 10 (S ED)	Un ità SK Hy ni x PE 80 10 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.1 46. 2	20 22 -0 2- 22	3B 11	3.9 4.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,3	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 60 2Q	ED A5 90 0Q	01 09	01 09	01 08	G D C5 50 2Q	11 09 2A 10	11 0B 2A 10

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.9 9.4 tra mi te Ne tA pp El e m en t 12. 3.2	20 21 -0 9- 16	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.9 9.4 tra mi te Ne tA pp El e m en t 12. 3.1 .16 5	20 21 -1 2- 06	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.9 9.2	20 21 -1 2- 06	3B 06	3.9 1.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.9 9.1 tra mi te Ne tA pp El e m en t 12. 3.1 .10 3	20 21 -0 9- 16	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.9 9 tra mi te Ne tA pp El e m en t 12. 3	20 21 -0 4- 15	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.7 6.8	20 21 -0 2- 03	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
Bu nd le fir m wa re di ar ch ivi azi one 2.2 7.1	20 20 -0 9- 29	3B 03	3.8 4.0 7	12 2	14. 02. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 30 2Q	ED A5 60 0Q	01 08	01 08	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.7 6.8 tra mi te Ne tA pp El e m en t 12. 2.1	20 21 -0 6- 02	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.2 1 tra mi te Ne tA pp El e m en t 12. 2	20 20 -0 9- 29	3B 03	3.8 4.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 30 2Q	ED A5 60 0Q	01 08	01 08	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 2.7 6.8 tra mi te Ne tA pp El e m en t 12. 0.1	20 21 -0 6- 02	3B 06	3.8 6.0 7	12 2	14. 25. 10 20	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	1,1 0	3,1	2,1 6	CX V8 20 2Q	CX V8 50 1Q	ED A5 40 2Q	ED A5 70 0Q	01 09	01 09	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)
St or ag e Fir m wa re Bu nd le 1.2 .17 tra mi te Ne tA pp El e m en t 12. 0	20 20 -0 3- 20	3B 03	3.7 8.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 08	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 8*	20 20 -0 3- 11	3B 03	3.7 8.0 7	12 2	14. 22. 10 02	-	3,1	2,1 6	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-
* Ne tA pp El em ent 11. 7*	20 19 -11 -2 1	3A 10	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 5.1 *	20 20 -0 2- 20	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	01 07	-	-	-
* Ne tA pp El em ent 11. 5*	20 19 -0 9- 26	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	01 07	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 3.2 *	20 20 -0 2- 19	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-
* Ne tA pp El em ent 11. 3.1 *	20 19 -0 8- 19	3A 08	3.7 6.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	Ca ch e NV DI M Fo nt e di en er gi a (B P M) S m art (G en 2)	M od ul o NV DI M Fo nt e di en er gi a (B P M) S m art (G en 1)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M Fo nt e di en er gi a (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)	
* Ne tA pp El em ent 11. 1.1 *	20 20 -0 2- 19	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-
* Ne tA pp El em ent 11. 1*	20 19 -0 4- 25	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-

Ril as cia re il vei co lo	Da ta di ril as ci o	BI O S	B M C	CP LD	Sc he da di ret e CX 4 10/ 25 Gb E	Sc he da di ret e CX 5 10/ 25 Gb E	M od ul o NV DI M Fo M ca ch e NV DI M S m art (G en 1)	Ca ch e NV DI M Fo M ca ch e NV DI M S m art (G en 1)	M od ul o NV DI M Fo M ca ch e NV DI M S m art (G en 2)	Ca ch e NV DI M Fo M ca ch e NV DI M S m art (G en 2)	M od ul o NV DI M Fo M ca ch e NV DI M S m art (G en 1)	Fo nt e di en er gi a NV DI M ca ch e NV DI M ca ch e (P G E M) Ag ig at ec h (G en 1)	M od ul o NV DI M Fo M ca ch e NV DI M ca ch e (P G E M) Ag ig at ec h (G en 2)	Fo nt e di en er gi a NV DI M ca ch e (P G E M) Ag ig at ec h (G en 3)	Fo nt e di en er gi a NV DI M ca ch e (P G E M) Ag ig at ec h (G en 3)	Un ità Sa m su ng P M9 63 (S ED)	Un ità Sa m su ng P M9 63 (N- SE D)	Un ità Sa m su ng P M9 83 (S ED)	Un ità Sa m su ng P M9 83 (N- SE D)	Un ità Ki ox ia C D5 (S ED)	Un ità Ki ox ia C D5 (N- SE D)	Un ità C D5 (FI PS)	Un ità Sa m su ng P M9 A3 (S ED)	Un ità SK Hy ni x PE 80 (S ED)	Un ità SK Hy ni x PE 80 (N- SE D)		
* Ne tA pp El em ent 11. 0.2 *	20 20 -0 2- 19	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	25. 3C	1,4 0	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	01 08	01 08	-	-	-	-	-
* Ne tA pp El em ent 11 *	20 18 -11 -2 9	3A 06	3.7 0.0 7	11 7	14. 22. 10 02	-	2. C	2,0 7	26. 2C	1,3 0	-	-	-	-	-	-	CX V8 20 2Q	CX V8 50 1Q	ED A5 20 2Q	ED A5 20 0Q	-	-	-	-	-	-	-

Firmware del componente non gestito da un bundle di firmware di archiviazione

Il seguente firmware non è gestito da un pacchetto firmware di archiviazione:

Componente	Versione attuale
Scheda di rete da 1/10 GbE	3.2d 0x80000b4b
Dispositivo di avvio	M161225i

H410S

Numero di modello (parte della famiglia): H410S **Numeri di modello completi:** H410S-0, H410S-1, H410S-1-NE e H410S-2

Firmware del componente gestito da un pacchetto firmware di archiviazione

Firmware del componente gestito da un pacchetto firmware di archiviazione.

Rilasciare il veicolo	Data di rilascio	BIOS	BMC	Scheda di rete SMCI Mellanox 10/25 GbE	Cache NVDIMM RMS200	Cache NVDIMM RMS300	Unità Samsung PM863 (SED)	Unità Samsung PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsung PM883 (SED)
Bundle firmware di archiviazione 2.182.0	2024-10-17	NAT3.6	07.02.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Bundle firmware di archiviazione 2.175.0	2023-06-15	NAT3.4	07.02.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Storage Firmware Bundle 2.164.0 tramite NetApp Element 12.7	2022-10-20	NAT3.4	6.98.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Bundle firmware di archiviazione 2.164.0	2022-10-20	NAT3.4	6.98.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q

Rilasciare il veicolo	Data di rilascio	BIOS	BMC	Scheda di rete SMCI Mellanox 10/25 GbE	Cache NVDIMM RMS200	Cache NVDIMM RMS300	Unità Samsung PM863 (SED)	Unità Samsung PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsung PM883 (SED)
Storage Firmware Bundle 2.164.0 tramite NetApp Element 12.7	2022-10-20	NAT3.4	6.98.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Storage Firmware Bundle 2.150.4 tramite NetApp Element 12.5	2022-06-08	NAT3.4	6.98.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7A04Q
Storage Firmware Bundle 2.99 tramite NetApp Element 12.3	2021-04-15	NA2.1	6.84.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
Storage Firmware Bundle 2.76.8 tramite NetApp Element 12.2.1	2021-06-02	NA2.1	6.84.00	14.25.1020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Rilasciare il veicolo	Data di rilascio	BIOS	BMC	Scheda di rete SMC Mellanox 10/25 GbE	Cache NVDIMM RMS200	Cache NVDIMM RMS300	Unità Samsung PM863 (SED)	Unità Samsung PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsung PM883 (SED)
Storage Firmware Bundle 1.2.17 tramite NetApp Element 12.0	2020-03-20	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8.2*	2022-02-22	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8.1*	2021-06-02	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.8*	2020-03-11	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.7*	2019-11-21	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.5.1*	2020-02-19	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.5*	2019-09-26	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.3.2*	2020-02-19	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Rilasciare il veicolo	Data di rilascio	BIOS	BMC	Scheda di rete SMC Mellanox 10/25 GbE	Cache NVDIMM RMS200	Cache NVDIMM RMS300	Unità Samsung PM863 (SED)	Unità Samsung PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsung PM883 (SED)
* NetApp Element 11.3.1*	2019-08-19	NA2.1	3,25	14.21.1000	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.1.1*	2020-02-19	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.1*	2019-04-25	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.0.2*	2020-02-19	NA2.1	3,25	14.17.2020	ae3b8cc	7d8422bc	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q
* NetApp Element 11.0*	2018-11-29	NA2.1	3,25	14.17.2020	ae3b8cc	-	GXT5404Q	GXT5103Q	8ENP7101	8ENP6101	HXT7904Q

Firmware del componente non gestito da un bundle di firmware di archiviazione

Il seguente firmware non è gestito da un pacchetto firmware di archiviazione:

Componente	Versione attuale
CPLD	01.A1.06
Adattatore SAS	16.00.01.00
Unità microcontrollore (MCU)	1,18
Scheda di rete SIOM 1/10 GbE	1,93
Alimentazione elettrica	1,3
Dispositivo di avvio SSDSCKJB240G7	N2010121
Dispositivo di avvio MTFDDAV240TCB1AR	DOMU037

SF38410, SF19210, SF9605 e SF4805

Numeri di modello completi: SF38410, SF19210, SF9605 e SF4805

Firmware del componente gestito da un pacchetto firmware di archiviazione

Durante il periodo 11.x, il software NetApp Element era l'unico modo per rilasciare il firmware. A partire da Element 12.0, è stato introdotto il concetto di **Storage Firmware Bundle** e gli aggiornamenti del firmware sono ora possibili tramite uno Storage Firmware Bundle rilasciato in modo indipendente o incluso come parte di una versione di Element 12.x.



Un trattino (-) nella tabella seguente indica che il componente hardware specifico NON era supportato in quel dato veicolo di rilascio.

Rilasciar e il veicolo	Data di rilascio	NIC	Cache NVDIMM RMS200 (RMS200)	Cache NVDIMM RMS200 (RMS300)	Unità Samsun g PM863 (SED)	Unità Samsun g PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsun g PM883 (SED)
Bundle firmware di archiviaz ione 2.164.0	2022-10- 20	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Storage Firmwar e Bundle 2.164.0 tramite NetApp Element 12.7	2022-10- 20	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Bundle firmware di archiviaz ione 2.150.4	2022-06- 08	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Storage Firmwar e Bundle 2.150.4 tramite NetApp Element 12.5	2022-06- 08	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q

Rilasciar e il veicolo	Data di rilascio	NIC	Cache NVDIMM RMS200 (RMS200)	Cache NVDIMM RMS200 (RMS300)	Unità Samsun g PM863 (SED)	Unità Samsun g PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsun g PM883 (SED)
Bundle firmware di archiviaz ione 2.146.2	2022-02- 22	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7A04 Q
Storage Firmwar e Bundle 2.99.4 tramite NetApp Element 12.3.2	2021-09- 16	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Storage Firmwar e Bundle 2.99.4 tramite NetApp Element 12.3.1.16 5	2021-12- 06	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Bundle firmware di archiviaz ione 2.99.2	2021-08- 03	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Storage Firmwar e Bundle 2.99.1 tramite NetApp Element 12.3.1.10 3	2021-09- 16	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q

Rilasciar e il veicolo	Data di rilascio	NIC	Cache NVDIMM RMS200 (RMS200)	Cache NVDIMM RMS200 (RMS300)	Unità Samsun g PM863 (SED)	Unità Samsun g PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsun g PM883 (SED)
Storage Firmwar e Bundle 2.99 tramite NetApp Element 12.3	2021-04- 15	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Bundle firmware di archiviaz ione 2.76.8	2021-02- 03	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Bundle firmware di archiviaz ione 2.27.1	2020-09- 29	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
Storage Firmwar e Bundle 2.76.8 tramite NetApp Element 12.2.1	2021-06- 02	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q
Storage Firmwar e Bundle 2.21 tramite NetApp Element 12.2	2020-09- 29	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
Storage Firmwar e Bundle 2.76.8 tramite NetApp Element 12.0.1	2021-06- 02	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7904 Q

Rilasciar e il veicolo	Data di rilascio	NIC	Cache NVDIMM RMS200 (RMS200)	Cache NVDIMM RMS200 (RMS300)	Unità Samsun g PM863 (SED)	Unità Samsun g PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsun g PM883 (SED)
Storage Firmwar e Bundle 1.2.17 tramite NetApp Element 12.0	2020-03- 20	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.8.2*	2022-02- 22	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.8.1*	2021-06- 02	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.8*	2020-03- 11	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.7*	2019-11- 21	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.5.1*	2020-02- 19	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.5*	2019-09- 26	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.3.2*	2020-02- 19	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.3.1*	2019-08- 19	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.1.1*	2020-02- 19	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.1*	2019-04- 25	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q
* NetApp Element 11.0.2*	2020-02- 19	7.10.18	ae3b8cc	7d8422bc	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q

Rilasciare il veicolo	Data di rilascio	NIC	Cache NVDIMM RMS200 (RMS200)	Cache NVDIMM RMS200 (RMS300)	Unità Samsung PM863 (SED)	Unità Samsung PM863 (N-SED)	Unità Toshiba Hawk-4 (SED)	Unità Toshiba Hawk-4 (N-SED)	Unità Samsung PM883 (SED)
* NetApp Element 11*	2018-11-29	7.10.18	ae3b8cc	-	GXT5404 Q	GXT5103 Q	8ENP710 1	8ENP610 1	HXT7104 Q

Firmware del componente non gestito da un bundle di firmware di archiviazione

Il seguente firmware non è gestito da un pacchetto firmware di archiviazione:

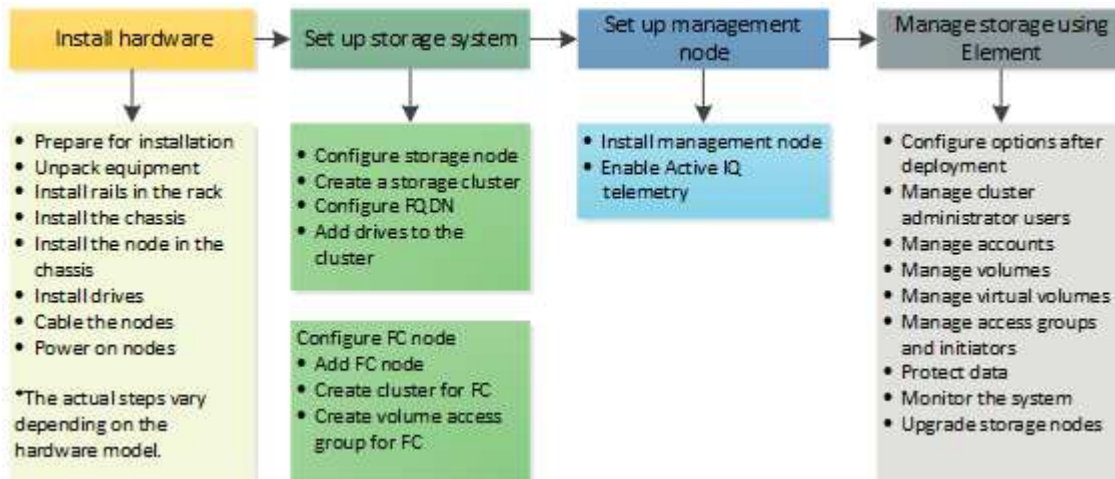
Componente	Versione attuale
BIOS	2.8.0
iDRAC	2.75.75.75
Modulo di identità	N41WC 1.02
Adattatore SAS	16.00.01.00
Alimentazione elettrica	1,3
Dispositivo di avvio	M161225i

Configurare l'archiviazione

Scopri come impostare l'archiviazione

A questo punto dovresti aver installato l'hardware. L'hardware include anche il software Element.

Successivamente, dovrai configurare il sistema di archiviazione per il tuo ambiente. È possibile configurare un cluster con nodi di storage o nodi Fibre Channel e gestirlo tramite il software Element dopo aver installato e cablato i nodi in un'unità rack e averli accesi.



Passaggi per configurare l'archiviazione

1. Seleziona una delle seguenti opzioni:

- ["Configurare il cluster con nodi di archiviazione"](#)

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

- ["Configurare il cluster con nodi Fibre Channel"](#)

È possibile configurare un cluster con nodi Fibre Channel e gestirlo tramite il software Element dopo aver installato e cablato i nodi in un'unità rack e averli accesi. È quindi possibile installare e configurare componenti aggiuntivi nel sistema di archiviazione.

2. ["Determinare quali componenti SolidFire installare"](#)

3. ["Configurare un nodo di gestione e abilitare la telemetria Active IQ"](#)

Trova maggiori informazioni

- ["Scopri i passaggi successivi per utilizzare lo storage"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Configurare un cluster con nodi di archiviazione

Configurare un nodo di archiviazione

È necessario configurare i singoli nodi prima di poterli aggiungere a un cluster. Dopo aver installato e cablato 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.

Esistono due opzioni per configurare i nodi di archiviazione:

- **Interfaccia utente per nodo:** Utilizza 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 tramite DHCP a un cluster. È possibile utilizzare l'indirizzo IP DHCP per configurare inizialmente il nodo nell'interfaccia utente, nell'interfaccia utente terminale 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, aggiungerlo a un cluster o utilizzare il nodo per creare un cluster. È anche 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 loro rete di gestione. Ciò vale sia per i nodi di archiviazione che per quelli di gestione, ad eccezione del nodo di gestione 11.3 e versioni successive che non supportano 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 archiviazione utilizzando l'interfaccia utente per nodo

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

Informazioni su questo compito

- È possibile configurare il nodo in modo che abbia un indirizzo IPv4 o IPv6.
- Per accedere a un nodo è necessario l'indirizzo DHCP visualizzato nell'interfaccia utente terminale (TUI). Non è possibile utilizzare indirizzi DHCP per aggiungere un nodo a un cluster.



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

Passi

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

Devi aggiungere l'estensione : 442 per accedere al nodo; ad esempio, <https://172.25.103.6:442>.

Si apre la scheda **Impostazioni di rete** con la sezione **Bond1G**.

2. Immettere 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 archiviazione 10G.
5. Immettere le impostazioni della rete di archiviazione 10G.
6. Fare clic su **Applica modifiche**.
7. Fare clic su **Impostazioni cluster**.
8. Inserisci il nome host per la rete 10G.
9. Inserisci il nome del cluster.



Questo nome deve essere aggiunto alla configurazione di 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 alle maiuscole e alle minuscole.

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

Configurare un nodo di archiviazione utilizzando TUI

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

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

Passi

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

Il menu principale NetApp Storage della TUI viene visualizzato sul terminale tty1.



Se il nodo non riesce a raggiungere il server di configurazione, l'interfaccia utente terminale visualizza un messaggio di errore. Per risolvere l'errore, controlla la connessione al server di configurazione o la connessione di rete.

2. Selezionare **Rete > Configurazione di rete**.



Per navigare nel menu, premere i tasti freccia Su o Giù. Per passare a un altro pulsante o ai campi dai pulsanti, premere **Tab**. Per navigare tra i campi, utilizzare i tasti freccia Su o Giù.

3. Selezionare **Bond1G (Gestione)** o **Bond10G (Archiviazione)** 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 Aiuto e identificare le opzioni disponibili.

Tutti i nodi di un cluster devono avere nomi di cluster identici. I nomi dei cluster sono sensibili alle maiuscole e alle minuscole. Se sulla rete è in esecuzione un server DHCP con indirizzi IP disponibili, nel campo Indirizzo viene visualizzato l'indirizzo 1GbE.

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

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

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Creare un cluster di archiviazione

È possibile creare un cluster di archiviazione dopo aver configurato tutti i singoli nodi. Quando crei un cluster, viene automaticamente creato un account utente amministratore del cluster. L'amministratore del cluster ha l'autorizzazione per gestire tutti gli attributi del cluster e può creare altri account amministratore del cluster.

Cosa ti servirà

- Hai installato il nodo di gestione.
- Hai configurato tutti i singoli nodi.

Informazioni su questo compito

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



Se si desidera abilitare l'intero cluster ["crittografia software a riposo"](#) per i cluster di archiviazione all-flash SolidFire, è necessario farlo durante la creazione del cluster. A partire da Element 12.5, è necessario abilitare la crittografia software a riposo nell'interfaccia utente di creazione cluster durante la creazione del cluster. Per Element 12.3.x e versioni precedenti, è necessario creare il cluster utilizzando ["Crea cluster"](#) Metodo API e modificare il parametro `enableSoftwareEncryptionAtRest` in `true`. Una volta abilitata la crittografia software a riposo sul cluster, non è possibile disattivarla. Puoi ["abilitare e disabilitare"](#) Crittografia basata su hardware a riposo dopo la creazione del cluster.



Quando si crea un nuovo cluster, tenere presente quanto segue:

- Se si utilizzano nodi di archiviazione che risiedono in uno chassis condiviso, potrebbe essere opportuno valutare la progettazione di una protezione contro i guasti a livello di chassis mediante la funzionalità dei domini di protezione.
- Se uno chassis condiviso non è in uso, è possibile definire un layout di dominio di protezione personalizzato.

Passi

1. In una finestra del browser, inserisci `https://MIP:443`, dove MIP è l'indirizzo IP del nodo di gestione.

2. In Crea un nuovo cluster, inserisci le seguenti informazioni:

- Management VIP: IP virtuale instradabile sulla rete 1GbE o 10GbE per attività di gestione della rete.



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

- VIP iSCSI (archiviazione): IP virtuale sulla rete 10GbE per l'archiviazione e la scoperta iSCSI.



Non è possibile modificare MVIP, SVIP o il nome del cluster dopo aver creato il cluster.

- Nome utente: nome utente dell'amministratore del cluster primario per l'accesso autenticato al cluster. È necessario salvare il nome utente per riferimento futuro.



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

- Password: password per l'accesso autenticato al cluster. È necessario salvare la password per riferimento futuro. La protezione bidirezionale dei dati è abilitata per impostazione predefinita. Non è possibile modificare questa impostazione.

3. Leggere il Contratto di licenza con l'utente finale e selezionare **Accetto**.

4. **Facoltativo**: nell'elenco Nodi, assicurarsi che le caselle di controllo per i nodi che non devono essere inclusi nel cluster non siano selezionate.

5. Selezionare **Crea cluster**.

A seconda del numero di nodi presenti nel cluster, il sistema potrebbe impiegare diversi minuti per creare il cluster. Su una rete configurata correttamente, un piccolo cluster di cinque nodi dovrebbe impiegare meno di un minuto. Dopo aver creato il cluster, la finestra Crea un nuovo cluster viene reindirizzata all'indirizzo URL MVIP del cluster e visualizza l'interfaccia utente dell'elemento.

Per maggiori informazioni

- ["Gestione dello storage con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Accedi all'interfaccia utente del software Element

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

Devi assicurarti che i blocchi popup e le impostazioni NoScript siano disattivati nel tuo browser.

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

Passi

1. Scegli una delle seguenti opzioni:

- IPv6: Invio `https://[IPv6_MVIP_address]` . Per esempio:

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

- **IPv4:** Invio `https://[IPv4 MVIP address]` . Per esempio:

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

2. Per DNS, immettere il nome host.
3. Fare clic su tutti i messaggi del certificato di autenticazione.

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiungere unità 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 tramite l'interfaccia utente o l'API di Element prima che possano partecipare al cluster.

Le unità non vengono visualizzate nell'elenco Unità disponibili quando si verificano le seguenti condizioni:

- Le unità sono in stato Attivo, Rimozione, Cancellazione o Errore.
- Il nodo di cui fa parte l'unità è nello stato In sospeso.

Passi

1. Dall'interfaccia utente di Element, seleziona **Cluster > Unità**.
2. Fare clic su **Disponibile** per visualizzare l'elenco delle unità disponibili.
3. Eseguire una delle seguenti operazioni:
 - Per aggiungere singole unità, fare clic sull'icona **Azioni** relativa all'unità che si desidera aggiungere e fare clic su **Aggiungi**.
 - Per aggiungere più unità, seleziona le caselle di controllo delle unità da aggiungere, fai clic su **Azioni in blocco** e quindi 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 connettere il cluster a una struttura di rete Fibre Channel. I nodi Fibre Channel vengono aggiunti a coppie e funzionano in modalità attivo-attivo (tutti i nodi elaborano attivamente il traffico per il cluster). I cluster che eseguono il software Element 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, è necessario assicurarsi che siano soddisfatte le seguenti condizioni:

- Almeno due nodi Fibre Channel sono collegati agli switch Fibre Channel.
- Tutte le porte SolidFire Fibre Channel devono essere collegate alla struttura Fibre Channel. Le quattro connessioni di rete SolidFire Bond10G devono essere collegate in un gruppo di bond LACP a livello di switch. Ciò consentirà di ottenere le migliori prestazioni complessive dai sistemi Fibre Channel.
- Esaminare e convalidare tutte le best practice per i cluster Fibre Channel incluse in questo articolo della Knowledge Base NetApp .

["Buone pratiche per il cluster SolidFire FC"](#)

I passaggi di configurazione della rete e del cluster sono gli stessi per i nodi Fibre Channel e per i nodi di storage.

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

I WWPN vengono registrati nel sistema quando si crea un nuovo cluster con nodi. Nell'interfaccia utente Element, puoi trovare gli indirizzi WWPN nella colonna WWPN della scheda Porte FC, a cui puoi accedere dalla scheda Cluster.

Trova maggiori informazioni

[Aggiungere nodi Fibre Channel a un cluster](#)

[Crea un nuovo cluster con nodi Fibre Channel](#)

Crea un nuovo cluster con nodi Fibre Channel

È possibile creare un nuovo cluster dopo aver configurato i singoli nodi Fibre Channel. Quando crei un cluster, viene automaticamente creato un account utente amministratore del cluster. L'amministratore del cluster ha l'autorizzazione a gestire tutti gli attributi del cluster e può creare altri account amministratori del cluster.

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

Cosa ti servirà

Hai configurato i singoli nodi Fibre Channel.

Passi

1. In una finestra del browser, immettere l'indirizzo MIP del nodo.
2. In Crea un nuovo cluster, inserisci le seguenti informazioni:
 - Management VIP: IP virtuale instradabile sulla rete 1GbE o 10GbE per attività di gestione della rete.
 - VIP iSCSI (archiviazione): IP virtuale sulla rete 10GbE per l'archiviazione e la scoperta iSCSI.



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

- Nome utente: il nome utente principale dell'amministratore del cluster per l'accesso autenticato al cluster. È necessario salvare il nome utente per riferimento futuro.



Per il nome utente è possibile utilizzare lettere maiuscole e minuscole, caratteri speciali e numeri.

- Password: password per l'accesso autenticato al cluster. È necessario salvare il nome utente per riferimento futuro. La protezione bidirezionale dei dati è abilitata 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. **Facoltativo**: 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 **Crea cluster**.

A seconda del numero di nodi presenti nel cluster, il sistema potrebbe impiegare diversi minuti per creare il cluster. Su una rete configurata correttamente, un piccolo cluster di cinque nodi dovrebbe impiegare meno di un minuto. Dopo aver creato il cluster, la finestra Crea un nuovo cluster viene reindirizzata all'indirizzo URL MVIP del cluster e visualizza l'interfaccia utente Web.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiungere nodi Fibre Channel a un cluster

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

La versione software su ciascun nodo Fibre Channel in 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, secondo necessità.

Passi

1. Selezionare **Cluster > Nodi**.

2. Fare clic su **In attesa** per visualizzare l'elenco dei nodi in attesa.
3. Eseguire una delle seguenti operazioni:
 - Per aggiungere singoli nodi, fare clic sull'icona **Azioni** relativa al nodo che si desidera aggiungere.
 - Per aggiungere più nodi, seleziona la casella di controllo dei nodi da aggiungere, quindi **Azioni in blocco**.



Se il nodo che stai aggiungendo ha una versione di Element diversa da quella in esecuzione sul cluster, il cluster aggiorna in modo asincrono il nodo alla versione di Element in esecuzione sul master del cluster. Dopo l'aggiornamento, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo sarà nello stato pendingActive.

4. Fare clic su **Aggiungi**.

Il nodo appare nell'elenco dei nodi attivi.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Impostare le zone per i nodi Fibre Channel

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

I WWPN vengono registrati nel sistema quando si crea un nuovo cluster con nodi. Nell'interfaccia utente Element, puoi trovare gli indirizzi WWPN nella colonna WWPN della scheda Porte FC, a cui puoi accedere dalla scheda Cluster.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

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

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

È anche possibile aggiungere iniziatori iSCSI a un gruppo di accesso al volume; in questo modo, gli iniziatori avranno accesso agli stessi volumi nel gruppo di accesso al volume.

Passi

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic su **Crea gruppo di accesso**.
3. Immettere un nome per il gruppo di accesso al volume nel campo **Nome**.
4. Selezionare e aggiungere gli iniziatori Fibre Channel dall'elenco **Iniziatori Fibre Channel non associati**.



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

5. **Facoltativo:** selezionare e aggiungere un iniziatore iSCSI dall'elenco **Iniziatori**.
6. Per collegare i volumi al gruppo di accesso, procedere come segue:
 - a. Selezionare un volume dall'elenco **Volumi**.
 - b. Fare clic su **Allega volume**.
7. Fare clic su **Crea gruppo di accesso**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Determinare quali componenti SolidFire installare

Potrebbe essere opportuno verificare quali componenti SolidFire , come il nodo di gestione, Active IQ e NetApp Monitoring Agent (NMA), installare, a seconda delle scelte di configurazione e distribuzione.

Nella tabella seguente sono elencati i componenti aggiuntivi e viene indicato se è necessario installarli.

Componente	Cluster di archiviazione SolidFire autonomo	Cluster NetApp HCI
Nodo di gestione	Raccomandato	Installato di default, obbligatorio
Active IQ	Raccomandato*	Raccomandato*
Agente di monitoraggio NetApp	Non supportato	Raccomandato

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

Passi

1. Determinare quali componenti devono essere installati.
2. Completare l'installazione secondo le ["installare il nodo di gestione"](#) procedura.



Per impostare Active IQ, utilizzare `--telemetry_active` parametro nello script di configurazione per abilitare la raccolta dati per l'analisi da parte di Active IQ.

3. Per informazioni sull'agente di monitoraggio NetApp , vedere questo ["procedura"](#) .

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Impostare un nodo di gestione

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

1. Vedi il ["installare il nodo di gestione"](#) documentazione.



Per impostare Active IQ, utilizzare `--telemetry_active` parametro nello script di configurazione per abilitare la raccolta dati per l'analisi da parte di Active IQ.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurare l'accesso all'interfaccia utente Web del nome di dominio completo

L'archiviazione all-flash SolidFire con software NetApp Element 12.2 o versione successiva consente di accedere alle interfacce Web del cluster di archiviazione 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 archiviazione 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 quali gestori di chiavi e provider di identità per l'autenticazione a più fattori.

Cosa ti servirà

- Questa funzionalità richiede Element 12.2 o versione successiva.
- Per configurare questa funzionalità tramite le API REST NetApp Hybrid Cloud Control sono necessari i servizi di gestione 2.15 o versioni successive.
- Per configurare questa funzionalità tramite l'interfaccia utente di controllo NetApp Hybrid Cloud, è necessario disporre dei servizi di gestione versione 2.19 o successiva.
- Per utilizzare le API REST, è necessario aver distribuito un nodo di gestione che esegue la versione 11.5 o successiva.
- Sono necessari nomi di dominio completi per il nodo di gestione e per ciascun cluster di archiviazione che si risolvano correttamente nell'indirizzo IP del nodo di gestione e in quello di ciascun cluster di

archiviazione.

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

- [Configurare l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control](#)
- [Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST](#)
- [Rimuovere l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control](#)
- [Rimuovere l'accesso all'interfaccia utente Web FQDN tramite l'API REST](#)
- [Risoluzione dei problemi](#)

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

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare l'icona del menu in alto a destra della pagina.
4. Selezionare **Configura**.
5. Nel riquadro **Nomi di dominio completi**, seleziona **Configura**.
6. Nella finestra visualizzata, immettere gli FQDN per il nodo di gestione e per ciascun cluster di archiviazione.
7. Seleziona **Salva**.

Nel riquadro **Nomi di dominio completi** sono elencati tutti i cluster di archiviazione con i relativi MVIP e FQDN.



Nel riquadro **Nomi di dominio completi** vengono elencati solo i cluster di storage connessi con l'FQDN impostato.

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

Passi

1. Assicurarsi che i nodi di archiviazione 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 archiviazione e al nodo di gestione, quindi selezionare **Impostazioni di rete > Rete di gestione**.
 - a. Interfaccia utente per nodo per nodi di archiviazione:
`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 archiviazione utilizzando l'API Element.

- a. Accedi all'API Element e crea la seguente preferenza di interfaccia cluster utilizzando "**CreaPreferenzaInterfacciaCluster**" Metodo API, inserendo l'FQDN MVIP del cluster per il 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. Accedi all'interfaccia utente dell'API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`

Per esempio:

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

- a. Fare clic su **Autorizza** o su qualsiasi icona a forma di lucchetto e immettere il nome utente e la password del cluster.
- b. Inserisci l'ID cliente come `mnode-client`.
- c. Fare clic su **Autorizza** per iniziare la sessione e quindi chiudere la finestra.
- d. Dall'elenco dei server, seleziona `mnode2`.
- e. Fare clic su **OTTIENI /impostazioni**.
- f. Fai clic su **Provalo**.
- g. Fare clic su **Esegui**.
- h. Registrare tutte le impostazioni proxy riportate nel corpo della risposta.
 - i. Fare clic su **METTI/impostazioni**.
 - j. Fai clic su **Provalo**.
- k. Nell'area del corpo della richiesta, immettere il nome di dominio completo del nodo di gestione come valore per `mnode_fqdn` parametro.
- l. Inserisci tutti i valori delle impostazioni proxy registrati in precedenza nei parametri rimanenti nel corpo della richiesta. Se si lasciano vuoti i parametri proxy o non li si include nel corpo della richiesta, le impostazioni proxy esistenti verranno rimosse.
- m. Fare clic su **Esegui**.

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

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

Passi

1. Nel riquadro **Nomi di dominio completi**, seleziona **Modifica**.
2. Nella finestra visualizzata, eliminare il contenuto del campo di testo **FQDN**.
3. Seleziona **Salva**.

La finestra si chiude e il nome di dominio completo non è più elencato nel riquadro **Nomi di dominio completi**.

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

Passi

1. Modificare le impostazioni del cluster di archiviazione utilizzando l'API Element.
 - a. Accedi all'API Element ed elimina la seguente preferenza dell'interfaccia cluster utilizzando DeleteClusterInterfacePreference Metodo API:

▪ Nome: mvip_fqdn

Per 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. Accedi all'interfaccia utente dell'API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da /mnode/2/ . Per esempio:

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

- b. Selezionare **Autorizza** o qualsiasi icona a forma di lucchetto e immettere il nome utente e la password del cluster Element.
- c. Inserisci l'ID cliente come mnode-client .
- d. Selezionare **Autorizza** per iniziare una sessione.
- e. Chiudi la finestra.
- f. Selezionare **METTI /impostazioni**.
- g. Seleziona **Provalo**.
- h. Nell'area del corpo della richiesta, non immettere un valore per mnode_fqdn parametro. Specificare anche se deve essere utilizzato il proxy(true O false) per il use_proxy parametro.

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

- i. Selezionare **Esegui**.

Risoluzione dei problemi

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

Problema	Causa	Risoluzione
• Si verifica un errore del browser quando si tenta di accedere al nodo di gestione o al cluster di archiviazione utilizzando l'FQDN. • Non è possibile accedere al nodo di gestione o al cluster di archiviazione utilizzando un indirizzo IP.	Sia il nome di dominio completo del nodo di gestione che il nome di dominio completo del cluster di archiviazione sono configurati in modo errato.	Utilizzare le istruzioni dell'API REST in questa pagina per rimuovere le impostazioni FQDN del nodo di gestione e del cluster di archiviazione e configurarle nuovamente.
• Si verifica un errore del browser quando si tenta di accedere al nome di dominio completo del cluster di archiviazione. • Non è possibile accedere al nodo di gestione o al cluster di archiviazione utilizzando un indirizzo IP.	Il nome di dominio completo del nodo di gestione è configurato correttamente, ma il nome di dominio completo del cluster di archiviazione non è configurato correttamente.	Utilizzare le istruzioni dell'API REST in questa pagina per rimuovere le impostazioni FQDN del cluster di archiviazione e configurarle nuovamente.
• Si verifica un errore del browser quando si tenta di accedere al nome di dominio completo del nodo di gestione. • È possibile accedere al nodo di gestione e al cluster di archiviazione utilizzando un indirizzo IP.	Il nome di dominio completo del nodo di gestione non è configurato correttamente, ma il nome di dominio completo del cluster di archiviazione è configurato correttamente.	Accedi a NetApp Hybrid Cloud Control per correggere le impostazioni FQDN del nodo di gestione nell'interfaccia utente oppure utilizza le istruzioni dell'API REST in questa pagina per correggere le impostazioni.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Cosa c'è dopo?

Dopo aver configurato il software Element, puoi gestire l'archiviazione completando alcune delle seguenti opzioni:

- ["Accedi all'interfaccia utente del software Element"](#)

- ["Configurare le opzioni del sistema SolidFire dopo la distribuzione"](#)
- ["Gestire gli account"](#)
- ["Gestisci il tuo sistema"](#)
- ["Gestire volumi e volumi virtuali"](#)
- ["Proteggi i tuoi dati"](#)
- ["Risolvi i problemi del tuo sistema"](#)

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci lo storage con il software Element

Gestisci lo storage con il software Element

Utilizza il software Element per configurare l'archiviazione SolidFire , monitorare la capacità e le prestazioni del cluster e gestire l'attività di archiviazione in un'infrastruttura multi-tenant.

Element è il sistema operativo di archiviazione 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 unico sistema di archiviazione ai client esterni. Element Software è responsabile del coordinamento, della scalabilità e della gestione del cluster nel suo complesso.

L'interfaccia software è basata sull'API Element.

- ["Accedi all'interfaccia utente del software Element"](#)
- ["Configurare le opzioni del sistema SolidFire dopo la distribuzione"](#)
- ["Aggiornare i componenti del sistema di archiviazione"](#)
- ["Utilizzare le opzioni di base nell'interfaccia utente del software Element"](#)
- ["Gestire gli account"](#)
- ["Gestisci il tuo sistema"](#)
- ["Gestire volumi e volumi virtuali"](#)
- ["Proteggi i tuoi dati"](#)
- ["Risolvi i problemi del tuo sistema"](#)

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Accedi all'interfaccia utente del software Element

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

Devi assicurarti che i blocchi popup e le impostazioni NoScript siano disattivati nel tuo browser.

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

1. Scegli una delle seguenti opzioni:

- IPv6: immettere `https://[indirizzo IPv6 MVIP]` Ad esempio:

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

- IPv4: immettere `https://[indirizzo IPv4 MVIP]` Ad esempio:

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

2. Per DNS, immettere il nome host.
3. Fare clic su tutti i messaggi del certificato di autenticazione.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Configurare le opzioni del sistema SolidFire dopo la distribuzione

Dopo aver configurato il sistema SolidFire , potresti voler eseguire alcune attività facoltative.

Se modifichi le credenziali nel sistema, potresti voler conoscere l'impatto sugli altri componenti.

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

Trova maggiori informazioni

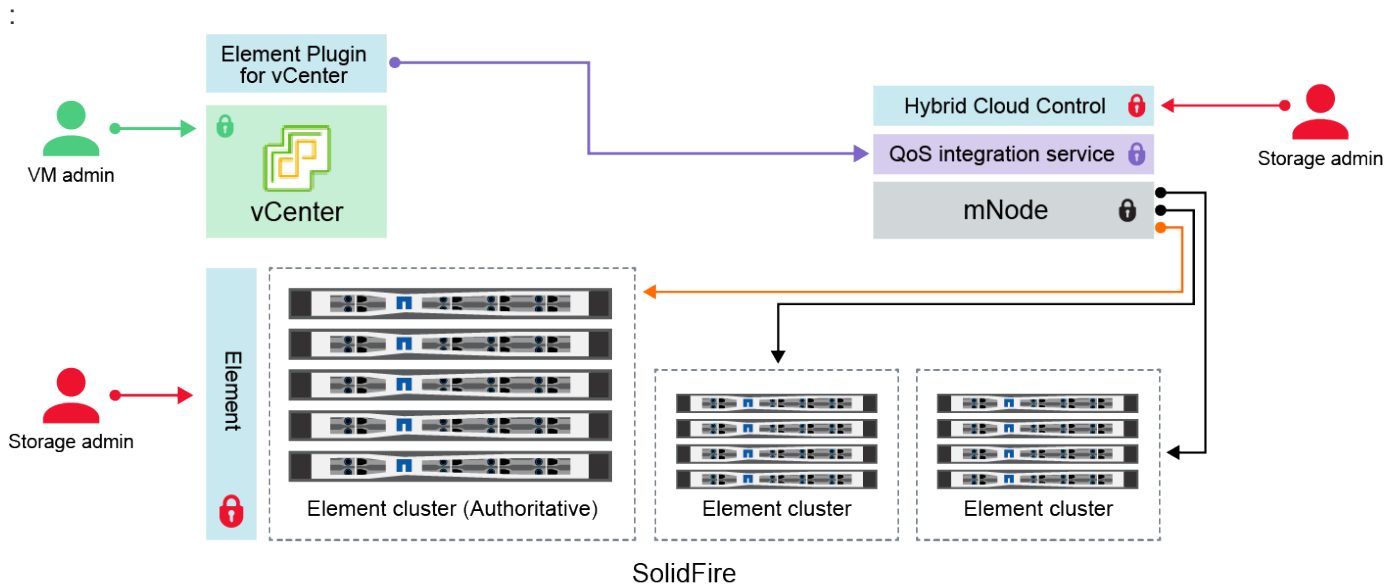
- ["Modificare le credenziali in NetApp HCI e NetApp SolidFire"](#)
- ["Cambia il certificato SSL predefinito del software Element"](#)
- ["Cambia la password IPMI per i nodi"](#)
- ["Abilita l'autenticazione a più fattori"](#)
- ["Inizia con la gestione delle chiavi esterne"](#)
- ["Creare un cluster che supporti le unità 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 rientra solitamente nelle pratiche di sicurezza. Prima di modificare le password, è necessario essere consapevoli dell'impatto sugli altri componenti software nella distribuzione.

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

Interazioni dei componenti NetApp SolidFire



- Administrator uses administrative Element storage credentials to log into Element UI and Hybrid Cloud Control
- Element Plugin for VMware vCenter uses password to communicate with QoS service on mNode
- mNode and services use Element certificates to communicate with authoritative storage cluster
- mNode and services use Element administrative credentials for additional storage clusters
- Administrators use VMware vSphere Single Sign-on credentials to log into vCenter

Tipo di credenziali e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali dell'elemento 	Si applica a: NetApp HCI e SolidFire Gli amministratori utilizzano queste credenziali per accedere a: - Interfaccia utente Element sul cluster di archiviazione 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, noti come <i>cluster autorevole</i> per cui il mnode è stato inizialmente configurato. Per i cluster di storage aggiunti in seguito a Hybrid Cloud Control, mnode memorizza in modo sicuro le credenziali di amministratore. Se vengono modificate le credenziali per i cluster di archiviazione aggiunti successivamente, è necessario aggiornarle anche nel mnode utilizzando l'API mnode.	"Aggiornare le password di amministrazione del cluster di archiviazione." - Aggiornare le credenziali di amministratore del cluster di archiviazione nel mnode utilizzando "API di modifica cluster admin".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali vSphere Single Sign-on 	Si applica 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 in NetApp Deployment Engine come segue: • username@vsphere.local con la password specificata e • administrator@vsphere.local con la password specificata. Quando si utilizza un vCenter esistente per distribuire NetApp HCI, le credenziali di vSphere Single Sign-on vengono gestite dagli amministratori IT VMware.	"Aggiorna le credenziali vCenter ed ESXi".
Credenziali del controller di gestione della scheda madre (BMC) 	Si applica a: solo NetApp HCI Gli amministratori utilizzano queste credenziali per accedere al BMC dei nodi di elaborazione NetApp in una distribuzione NetApp HCI. BMC fornisce funzionalità di monitoraggio hardware di base e di console virtuale. Le credenziali BMC (talvolta denominate <i>IPMI</i>) per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni NetApp HCI. NetApp Hybrid Cloud Control utilizza le credenziali BMC in una capacità di account di servizio per comunicare con il BMC nei nodi di elaborazione durante gli aggiornamenti del firmware dei nodi di elaborazione. Quando si modificano le credenziali BMC, è necessario aggiornare anche le credenziali per i rispettivi nodi di elaborazione sul nodo m per mantenere tutte le funzionalità di Hybrid Cloud Control.	• "Configurare IPMI per ogni nodo su NetApp HCI". • Per i nodi H410C, H610C e H615C, "cambiare la password IPMI predefinita". • Per i nodi H410S e H610S, "cambia la password IPM predefinita". • "Modificare le credenziali BMC sul nodo di gestione".

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali ESXi 	Si applica a: solo NetApp HCI Gli amministratori possono accedere agli host ESXi tramite SSH o tramite la DCUI locale con un account root locale. Nelle distribuzioni NetApp HCI, il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione in NetApp Deployment Engine. Le credenziali root ESXi per ciascun nodo di elaborazione NetApp vengono archiviate in modo sicuro sul mnode nelle distribuzioni 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 elaborazione e i controlli di integrità. Quando le credenziali di root ESXi vengono modificate da un amministratore VMware, le credenziali per i rispettivi nodi di elaborazione devono essere aggiornate sul mnode per mantenere la funzionalità Hybrid Cloud Control.	"Aggiornare le credenziali per gli host vCenter ed ESXi".
Password di integrazione QoS 	Si applica a: NetApp HCI e facoltativo in SolidFire Non utilizzato per accessi interattivi da parte degli amministratori. L'integrazione QoS tra VMware vSphere ed Element Software è abilitata tramite: • Plug-in Element per vCenter Server e • Servizio QoS sul 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 oppure generata automaticamente durante la distribuzione di NetApp HCI. Nessun impatto sugli altri componenti.	"Aggiornare le credenziali QoSSIOC nel plug-in NetApp Element per vCenter Server". La password SIOC del plug-in NetApp Element per vCenter Server è nota anche come <i>password QoSSIOC</i>. Consultare l'articolo della Knowledge Base sul plug-in Element per vCenter Server.

Tipo di credenziale e icona	Utilizzo da parte dell'amministratore	Vedi queste istruzioni
Credenziali di vCenter Service Appliance 	Si applica a: NetApp HCI solo se configurato da NetApp Deployment Engine Gli amministratori possono accedere alle macchine virtuali dell'appliance vCenter Server. Nelle distribuzioni NetApp HCI , il nome utente è "root" e la password è stata specificata durante l'installazione iniziale di quel nodo di elaborazione nel NetApp Deployment Engine. A seconda della versione di VMware vSphere distribuita, anche alcuni amministratori nel dominio vSphere Single Sign-on possono accedere all'appliance. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.
Credenziali di amministratore del nodo di gestione NetApp 	Si applica a: NetApp HCI e facoltativo 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 abilitato per impostazione predefinita. Nelle distribuzioni NetApp HCI , il nome utente e la password venivano specificati dall'utente durante l'installazione iniziale del nodo di elaborazione in NetApp Deployment Engine. Nessun impatto sugli altri componenti.	Non sono necessarie modifiche.

Trova maggiori informazioni

- ["Cambia il certificato SSL predefinito del software Element"](#)
- ["Cambia la password IPMI per i nodi"](#)
- ["Abilita l'autenticazione a più fattori"](#)
- ["Inizia con la gestione delle chiavi esterne"](#)
- ["Creare un cluster che supporti le unità FIPS"](#)

Cambia il certificato SSL predefinito del software Element

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

Quando viene creato un cluster software NetApp Element , il cluster crea un certificato Secure Sockets Layer (SSL) autofirmato univoco e una chiave privata 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 sia i certificati autofirmati sia i certificati emessi e verificati da un'autorità di certificazione (CA) attendibile.

È possibile utilizzare i seguenti metodi API per ottenere maggiori informazioni sul certificato SSL predefinito e

apportare modifiche.

- **OttieniCertificatoSSL**

Puoi usare il "[Metodo GetSSLCertificate](#)" per recuperare informazioni sul certificato SSL attualmente installato, compresi tutti i dettagli del certificato.

- **SetSSLCertificate**

Puoi usare il "[Metodo SetSSLCertificate](#)" per impostare i certificati SSL del cluster e per nodo sul certificato e sulla chiave privata forniti. Il sistema convalida il certificato e la chiave privata per impedire che venga applicato un certificato non valido.

- **RimuoviCertificatoSSL**

IL "[Metodo RemoveSSLCertificate](#)" rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una chiave privata.



Il certificato SSL del cluster viene applicato automaticamente a tutti i nuovi nodi aggiunti al cluster. Qualsiasi nodo rimosso dal cluster torna a essere un certificato autofirmato e tutte le informazioni sui certificati e sulle chiavi definite dall'utente vengono rimosse dal nodo.

Trova maggiori informazioni

- "[Modificare il certificato SSL predefinito del nodo di gestione](#)"
- "[Quali sono i requisiti per l'impostazione di certificati SSL personalizzati in Element Software?](#)"
- "[Documentazione del software SolidFire ed Element](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"

Cambia la password IPMI predefinita per i nodi

È possibile modificare la password predefinita dell'amministratore dell'Intelligent Platform Management Interface (IPMI) non appena si ottiene l'accesso IPMI remoto al nodo. Potrebbe essere opportuno farlo se ci sono aggiornamenti di installazione.

Per i dettagli sulla configurazione dell'accesso IPM per i nodi, vedere "[Configurare IPMI per ogni 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 archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `ADMIN` e password `ADMIN` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, fare clic sulla scheda **Configurazione**.
4. Fare clic su **Utenti**.
5. Seleziona il `ADMIN` utente e fare clic su **Modifica utente**.
6. Selezionare la casella di controllo **Cambia password**.
7. Inserisci una nuova password nei campi **Password** e **Conferma password**.
8. Fare clic su **Modifica**, 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 archiviazione non appena si configura la porta di rete IPMI.

Cosa ti servirà

Dovresti aver configurato l'indirizzo IP IPMI per ciascun nodo di archiviazione.

Passi

1. Aprire un browser Web su un computer in grado di raggiungere la rete IPMI e andare all'indirizzo IP IPMI del nodo.
2. Inserisci il nome utente `root` e password `calvin` nel prompt di accesso.
3. Dopo aver effettuato l'accesso, clicca 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 **Amministratore** dall'elenco.
7. Abilitare la casella di controllo **Cambia password**.
8. Inserisci una nuova password complessa nei campi **Password** e **Conferma password**.
9. Fare clic su **Salva** in fondo alla pagina.
10. Ripetere questa procedura per tutti gli altri nodi H610S con password IPMI predefinite.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

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

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 la fornitura di feedback.

- ["Visualizza l'attività API"](#)
- ["Icone nell'interfaccia Element"](#)
- ["Fornire feedback"](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Attività API

Visualizza l'attività API

Il sistema Element utilizza l'API NetApp Element come base per le sue caratteristiche e funzionalità. L'interfaccia utente Element consente di visualizzare vari tipi di attività API in tempo reale sul sistema mentre si utilizza l'interfaccia. Grazie al registro API, puoi visualizzare l'attività API di sistema avviata dall'utente e in background, nonché le chiamate API effettuate sulla pagina che stai visualizzando.

È possibile utilizzare il registro API per identificare quali metodi API vengono 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 dell'elemento, fare clic su **Registro API**.
2. Per modificare il tipo di attività API visualizzata nella finestra Registro API, procedere come segue:
 - a. Selezionare **Richieste** per visualizzare il traffico delle richieste API.
 - b. Selezionare **Risposte** per visualizzare il traffico di risposta API.
 - c. Filtra i tipi di traffico API selezionando una delle seguenti opzioni:
 - **Avviato dall'utente**: traffico API generato dalle tue attività durante questa sessione dell'interfaccia utente web.
 - **Background Polling**: traffico API generato dall'attività del sistema in background.
 - **Pagina corrente**: traffico API generato dalle attività sulla pagina che stai visualizzando.

Trova maggiori informazioni

- ["Gestione dello storage con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Frequenza di aggiornamento dell'interfaccia influenzata dal carico del cluster

A seconda dei tempi di risposta dell'API, il cluster potrebbe regolare automaticamente l'intervallo di aggiornamento dei dati per determinate parti della pagina del software NetApp Element visualizzata.

L'intervallo di aggiornamento viene ripristinato al valore predefinito quando si ricarica la pagina nel browser. È possibile visualizzare l'intervallo di aggiornamento corrente facendo clic sul nome del cluster nell'angolo in alto a destra della pagina. Si noti che l'intervallo controlla la frequenza con cui vengono effettuate le richieste API, non la rapidità con cui i dati vengono restituiti dal server.

Quando un cluster è sottoposto a un carico elevato, potrebbe mettere in coda le richieste API dall'interfaccia utente di Element. In rare circostanze, quando la risposta del sistema subisce un ritardo significativo, ad esempio a causa di una connessione di rete lenta combinata con un cluster occupato, è possibile che si venga disconnessi dall'interfaccia utente di Element se il sistema non risponde alle richieste API in coda con sufficiente rapidità. Se vieni reindirizzato alla schermata di disconnessione, puoi effettuare nuovamente l'accesso dopo aver ignorato la richiesta iniziale di autenticazione del browser. Una volta tornati alla pagina di panoramica, potrebbero venirti richieste le credenziali del cluster se non sono state salvate dal tuo browser.

Icone nell'interfaccia Element

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 rapido riferimento:

Icona	Descrizione
	Azioni
	Backup su
	Clona o copia
	Elimina o elimina
	Modificare
	Filtro
	Paio

	Aggiorna
	Ripristinare
	Ripristina da
	Ripristino
	Istantanea

Fornire feedback

Puoi contribuire a migliorare l'interfaccia utente web del software Element e risolvere eventuali problemi dell'interfaccia utente utilizzando il modulo di feedback accessibile in tutta l'interfaccia utente.

1. Da qualsiasi pagina dell'interfaccia utente di Element, fare clic sul pulsante **Feedback**.
2. Inserisci le informazioni rilevanti nei campi Riepilogo e Descrizione.
3. Allega eventuali screenshot utili.
4. Inserisci un nome e un indirizzo email.
5. Seleziona la casella di controllo per includere i dati relativi al tuo ambiente attuale.
6. Fare clic su **Invia**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestire gli account

Gestire gli account

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

- ["Lavorare con gli account utilizzando CHAP"](#)
- ["Gestire gli account utente dell'amministratore del cluster"](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Lavorare con gli account utilizzando CHAP

Nei sistemi di archiviazione SolidFire, i tenant possono utilizzare gli account per consentire ai client di connettersi ai volumi su un cluster. Un account contiene l'autenticazione CHAP (Challenge-Handshake Authentication Protocol) necessaria per accedere ai volumi a esso 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.

Algoritmi CHAP

A partire da Element 12.7, sono supportati gli algoritmi CHAP sicuri conformi a FIPS SHA1, SHA-256 e SHA3-256. Quando un iniziatore iSCSI host crea una sessione iSCSI con un target iSCSI Element, richiede un elenco di algoritmi CHAP da utilizzare. La destinazione Element iSCSI sceglie il primo algoritmo supportato dall'elenco richiesto dall'iniziatore iSCSI host. Per confermare che la destinazione Element iSCSI scelga l'algoritmo più sicuro, è necessario configurare l'iniziatore iSCSI host per inviare un elenco di algoritmi ordinati dal più sicuro, ad esempio SHA3-256, al meno sicuro, ad esempio SHA1 o MD5. Quando gli algoritmi SHA non vengono richiesti dall'iniziatore iSCSI host, la destinazione iSCSI Element sceglie MD5, presupponendo che l'elenco degli algoritmi proposti dall'host contenga MD5. Potrebbe essere necessario aggiornare la configurazione dell'iniziatore iSCSI dell'host per abilitare il supporto per gli algoritmi sicuri.

Durante un aggiornamento a Element 12.7 o versione successiva, se è già stata aggiornata la configurazione dell'iniziatore iSCSI host per inviare una richiesta di sessione con un elenco che include algoritmi SHA, quando i nodi di archiviazione si riavviano, i nuovi algoritmi sicuri vengono attivati e vengono stabilite sessioni iSCSI nuove o riconnesse utilizzando il protocollo più sicuro. Durante l'aggiornamento, tutte le sessioni iSCSI esistenti passano da MD5 a SHA. Se non si aggiorna la configurazione dell'iniziatore iSCSI host per richiedere SHA, le sessioni iSCSI esistenti continueranno a utilizzare MD5. In un secondo momento, dopo aver aggiornato gli algoritmi CHAP dell'iniziatore iSCSI host, le sessioni iSCSI dovrebbero passare gradualmente da MD5 a SHA nel tempo, in base alle attività di manutenzione che determinano la riconnessione delle sessioni iSCSI.

Ad esempio, l'iniziatore iSCSI host predefinito in Red Hat Enterprise Linux (RHEL) 8.3 ha `node.session.auth.chap_algs = SHA3-256, SHA256, SHA1, MD5` impostazione commentata, il che fa sì che l'iniziatore iSCSI utilizzi solo MD5. Rimuovendo il commento da questa impostazione sull'host e riavviando l'iniziatore iSCSI, le sessioni iSCSI da quell'host inizieranno a utilizzare SHA3-256.

Se necessario, è possibile utilizzare il ["ElencoISCSISessioni"](#) Metodo API per visualizzare gli algoritmi CHAP utilizzati per ogni sessione.

Creare un account

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

Ogni nome di account nel sistema deve essere univoco.

1. Selezionare **Gestione > Account**.

2. Fare clic su **Crea account**.
3. Inserisci 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.

- **Segreto dell'iniziatore** per l'autenticazione della sessione del nodo CHAP.
- **Segreto di destinazione** per l'autenticazione della sessione del nodo CHAP.

5. Fare clic su **Crea account**.

Visualizza i dettagli dell'account

È possibile visualizzare l'attività di performance per singoli account in formato grafico.

Le informazioni del grafico forniscono informazioni su I/O e produttività per l'account. I livelli di attività media e massima vengono mostrati in incrementi di periodi di segnalazione 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 per un account.
3. Fare clic su **Visualizza dettagli**.

Ecco alcuni dettagli:

- **Stato**: Lo stato dell'account. Valori possibili:
 - attivo: un account attivo.
 - bloccato: Un account bloccato.
 - rimosso: un account che è stato eliminato e ripulito.
- **Volumi attivi**: numero di volumi attivi assegnati all'account.
- **Compressione**: punteggio di efficienza della compressione per i volumi assegnati all'account.
- **Deduplicazione**: punteggio di efficienza della deduplicazione per i volumi assegnati all'account.
- **Thin Provisioning**: punteggio di efficienza del thin provisioning per i volumi assegnati all'account.
- **Efficienza complessiva**: punteggio di efficienza complessiva per i volumi assegnati all'account.

Modifica un account

È possibile modificare un account per cambiarne lo stato, cambiare i segreti CHAP o modificare 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 imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettere sempre le sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali 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 per un account.
3. Nel menu che si apre, seleziona **Modifica**.
4. **Facoltativo:** modifica il **Nome utente**.
5. **Facoltativo:** fare clic sull'elenco a discesa **Stato** e selezionare uno stato diverso.



Modificando lo stato in **bloccato**, tutte le connessioni iSCSI all'account vengono interrotte e l'account non è più accessibile. I volumi associati all'account vengono mantenuti; tuttavia, i volumi non sono rilevabili tramite iSCSI.

6. **Facoltativo:** in **Impostazioni CHAP**, modifica le credenziali **Segreto iniziatore** e **Segreto destinazione** utilizzate per l'autenticazione della sessione del nodo.



Se non modifichi le credenziali **Impostazioni CHAP**, queste rimarranno invariate. Se si lasciano vuoti i campi delle credenziali, il sistema genera nuove password.

7. Fare clic su **Salva modifiche**.

Elimina un account

Puoi eliminare un account quando non ti serve più.

Eliminare e ripulire 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 relativa all'account che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestire gli account utente dell'amministratore del cluster

È possibile gestire gli account degli amministratori del cluster per un sistema di archiviazione SolidFire creando, eliminando e modificando gli account degli amministratori del cluster, cambiando la password degli amministratori del cluster e configurando le impostazioni LDAP per gestire l'accesso al sistema per gli utenti.

Tipi di account amministratore del cluster di archiviazione

In un cluster di storage che esegue il software NetApp Element possono esistere due tipi di account amministratore: l'account amministratore del cluster primario e un account amministratore del cluster.

- **Account amministratore del cluster primario**

Questo account amministratore viene creato quando viene creato il cluster. Questo account è l'account amministrativo principale con il livello di accesso più elevato al cluster. Questo account è analogo all'utente root in un sistema Linux. Puoi modificare la password per questo account amministratore.

- **Account amministratore del cluster**

È possibile concedere a un account amministratore del cluster un intervallo limitato di accessi amministrativi 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 e Element UI all'interno del sistema di archiviazione.



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

Visualizza i dettagli dell'amministratore del cluster

1. Per creare un account amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
 - a. Fare clic su **Utenti > Amministratori cluster**.
2. Nella pagina Amministratori cluster della scheda Utenti, è possibile visualizzare le seguenti informazioni.
 - **ID**: Numero sequenziale assegnato all'account dell'amministratore del cluster.
 - **Nome utente**: il nome assegnato all'account dell'amministratore del cluster al momento della sua creazione.
 - **Accesso**: le autorizzazioni utente assegnate all'account utente. Valori possibili:
 - Leggere
 - segnalazione
 - nodi
 - unità
 - volumi
 - conti
 - amministratori del cluster
 - amministratore
 - supportoAdmin



Tutte le autorizzazioni sono disponibili per il tipo di accesso amministratore.

Sono disponibili tipi di accesso tramite l'API che non sono disponibili nell'interfaccia utente di Element.

+

- **Tipo:** Tipo di amministratore del cluster. Valori possibili:
 - Grappolo
 - Ldap
- **Attributi:** se l'account dell'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 del software NetApp Element](#)".

Crea un account amministratore del cluster

È possibile creare nuovi account di amministratore del cluster con autorizzazioni per consentire o limitare l'accesso ad aree specifiche del sistema di archiviazione. Quando si impostano le autorizzazioni dell'account amministratore del cluster, il sistema concede diritti di sola lettura per tutte 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.

"Abilita l'autenticazione LDAP con l'interfaccia utente Element"

In seguito è possibile modificare i privilegi dell'account amministratore del cluster per la creazione di report, nodi, unità, volumi, account e accesso 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.

In seguito è anche possibile rimuovere 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 amministratore del cluster a livello di cluster (non LDAP), eseguire le seguenti operazioni:
 - a. Fare clic su **Utenti > Amministratori cluster**.
 - b. Fare clic su **Crea amministratore cluster**.
 - c. Selezionare il tipo di utente **Cluster**.
 - d. Inserisci un nome utente e una password per l'account e conferma la password.
 - e. Seleziona 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 **Crea amministratore cluster**.
2. Per creare un account amministratore del cluster nella directory LDAP, eseguire le seguenti azioni:
 - a. Fare clic su **Cluster > LDAP**.
 - b. Assicurarsi che l'autenticazione LDAP sia abilitata.
 - c. Fare clic su **Test 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 seguito.
 - d. Fare clic su **Utenti > Amministratori cluster**.

- e. Fare clic su **Crea amministratore cluster**.
- f. Selezionare il tipo di utente LDAP.
- g. Nel campo Nome distinto, seguire l'esempio nella casella di testo per immettere un nome distinto completo per l'utente o il gruppo. In alternativa, incollalo dal nome distinto che hai copiato in precedenza.

Se il nome distinto fa parte di un gruppo, qualsiasi utente membro di quel gruppo sul server LDAP avrà le autorizzazioni di questo account amministratore.

Per aggiungere utenti o gruppi LDAP Cluster Admin, il formato generale del nome utente è "LDAP:<Nome distinto completo>".

- a. Seleziona 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 **Crea amministratore cluster**.

Modifica le autorizzazioni dell'amministratore del cluster

È possibile modificare i privilegi dell'account amministratore del cluster per la creazione di report, nodi, unità, volumi, account e accesso 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 Azioni relativa all'amministratore del cluster che si desidera modificare.
3. Fare clic su **Modifica**.
4. Seleziona le autorizzazioni utente da applicare all'account.
5. Fare clic su **Salva modifiche**.

Cambiare le password per gli account degli amministratori del cluster

È possibile utilizzare l'interfaccia utente di Element per modificare le password degli amministratori del cluster.

1. Fare clic su **Utenti > Amministratori cluster**.
2. Fare clic sull'icona Azioni relativa all'amministratore del cluster che si desidera modificare.
3. Fare clic su **Modifica**.
4. Nel campo Cambia password, inserisci una nuova password e confermalà.
5. Fare clic su **Salva modifiche**.

Informazioni correlate

- ["Scopri i tipi di accesso disponibili per le API Element"](#)
- ["Abilita l'autenticazione LDAP con l'interfaccia utente Element"](#)
- ["Disabilitare LDAP"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci LDAP

È possibile configurare il protocollo LDAP (Lightweight Directory Access Protocol) per abilitare la funzionalità di accesso sicura 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 sia indirizzi IPv4 che IPv6.

L'abilitazione di LDAP prevede i seguenti passaggi generali, descritti in dettaglio:

1. **Completare i passaggi di preconfigurazione per il supporto LDAP.** Verificare di disporre di tutti i dettagli necessari per configurare l'autenticazione LDAP.
2. **Abilita l'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 API GetLdapConfiguration o controllando la configurazione LDAP tramite l'interfaccia utente dell'elemento.
4. **Testare l'autenticazione LDAP** (con `readonly` utente). Verificare che la configurazione LDAP sia corretta eseguendo il metodo API TestLdapAuthentication oppure utilizzando l'interfaccia utente dell'elemento. Per questo test iniziale, utilizzare il nome utente "sAMAccountName" del `readonly` utente. Ciò convaliderà che il cluster è configurato correttamente per l'autenticazione LDAP e convaliderà anche che `readonly` le credenziali e l'accesso sono corretti. Se questo passaggio non riesce, ripetere i passaggi da 1 a 3.
5. **Testa l'autenticazione LDAP** (con un account utente che desideri aggiungere). Ripetere la procedura descritta al punto 4 con un account utente che si desidera aggiungere come amministratore del cluster Element. Copia il `distinguished` nome (DN) o l'utente (o il gruppo). Questo DN verrà utilizzato nel passaggio 6.
6. **Aggiungere l'amministratore del cluster LDAP** (copiare e incollare il DN dal passaggio 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, incolla il DN completo che hai copiato nel passaggio 5. Ciò garantisce che il DN sia formattato correttamente.
7. **Testare l'accesso dell'amministratore del cluster.** Accedere al cluster utilizzando l'utente amministratore del cluster LDAP appena creato. Se hai aggiunto un gruppo LDAP, puoi accedere come qualsiasi utente di quel gruppo.

Completare i passaggi di preconfigurazione per il supporto LDAP

Prima di abilitare il supporto LDAP in Element, è necessario configurare un server Windows Active Directory ed eseguire altre attività di preconfigurazione.

Passi

1. Configurare un server Windows Active Directory.
2. **Facoltativo:** abilitare il supporto LDAPS.
3. Crea utenti e gruppi.
4. Creare un account di servizio di sola lettura (ad esempio "sfreadonly") da utilizzare per la ricerca nella directory LDAP.

Abilita l'autenticazione LDAP con l'interfaccia utente Element

È possibile configurare l'integrazione del sistema di archiviazione con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso degli utenti al sistema di archiviazione.

È possibile configurare LDAP tramite l'interfaccia utente Element o tramite 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 utilizza `SearchAndBind` come tipo di autenticazione. Nell'esempio viene utilizzato un singolo server Active Directory Windows Server 2012 R2.

Passi

1. Fare clic su **Cluster > LDAP**.
2. Fare clic su **Sì** per abilitare l'autenticazione LDAP.
3. Fare clic su **Aggiungi un server**.
4. Inserisci **Nome host/Indirizzo IP**.



È anche possibile immettere un numero di porta personalizzato facoltativo.

Ad esempio, per aggiungere un numero di porta personalizzato, immettere <nome host o indirizzo IP>:<numero di porta>

5. **Facoltativo:** seleziona **Usa protocollo LDAPS**.
6. Inserisci le informazioni richieste in **Impostazioni generali**.

LDAP Servers

Host Name/IP Address	192.168.9.99	Remove
☐ Use LDAPS Protocol		

[Add a Server](#)

General Settings

Auth Type	Search and Bind	▼
Search Bind DN	msmyth@thesmyths.ca	
Search Bind Password	e.g. password	☐ Show password
User Search Base DN	OU=Home users,DC=thesmyths,DC=ca	
User Search Filter	(&(objectClass=person))((sAMAccountName=%USER	
Group Search Type	Active Directory	▼
Group Search Base DN	OU=Home users,DC=thesmyths,DC=ca	

[Save Changes](#)

7. Fare clic su **Abilita LDAP**.
8. Fare clic su **Test autenticazione utente** se si desidera testare l'accesso al server per un utente.
9. Copiare il nome distinto e le informazioni sul gruppo utente che vengono visualizzate per utilizzarle in seguito durante la creazione degli amministratori del cluster.
10. Fare clic su **Salva modifiche** per salvare le nuove impostazioni.
11. Per creare un utente in questo gruppo in modo che chiunque possa accedere, completa quanto segue:
 - a. Fare clic su **Utente > Visualizza**.

Create a New Cluster Admin



Select User Type

☐ Cluster ☒ LDAP

Enter User Details

Distinguished Name

CN=StorageAdmins,OU=Home
users,DC=thesmyths,DC=ca

Select User Permissions

☐ Reporting	☐ Volumes
☐ Nodes	☐ Accounts
☐ Drives	☐ Cluster Admin

Accept the Following End User License Agreement

- Per il nuovo utente, fare clic su **LDAP** per Tipo utente e incollare il gruppo copiato nel campo Nome distinto.
- Selezionare le autorizzazioni, in genere tutte le autorizzazioni.
- Scorri verso il basso fino al Contratto di licenza con l'utente finale e fai clic su **Accetto**.
- Fare clic su **Crea amministratore cluster**.

Ora hai un utente con il valore di un gruppo Active Directory.

Per testarlo, disconnettiti dall'interfaccia utente di Element e accedi nuovamente come utente di quel gruppo.

Abilita l'autenticazione LDAP con l'API Element

È possibile configurare l'integrazione del sistema di archiviazione con un server LDAP esistente. Ciò consente agli amministratori LDAP di gestire centralmente l'accesso degli utenti al sistema di archiviazione.

È possibile configurare LDAP tramite l'interfaccia utente Element o tramite l'API Element. Questa procedura descrive come configurare LDAP utilizzando l'API Element.

Per sfruttare l'autenticazione LDAP su un cluster SolidFire , abilitare prima l'autenticazione LDAP sul cluster utilizzando EnableLdapAuthentication Metodo API.

Passi

- 1. Abilitare prima l'autenticazione LDAP sul cluster utilizzando EnableLdapAuthentication Metodo API.
- 2. Inserisci 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	Stabilisce che il cluster utilizzerà l'account di servizio di sola lettura per cercare prima l'utente da autenticare e successivamente associare tale utente se trovato e autenticato.
groupSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifica la posizione nell'albero LDAP da cui iniziare la ricerca dei gruppi. Per questo esempio abbiamo utilizzato la radice del nostro albero. Se l'albero LDAP è molto grande, potrebbe essere opportuno impostarlo su un sottoalbero più granulare per ridurre i tempi di ricerca.
userSearchBaseDN: dc=prodtest,dc=solidfire,dc=net	Specifica la posizione nell'albero LDAP da cui iniziare la ricerca degli utenti. Per questo esempio abbiamo utilizzato la radice del nostro albero. Se l'albero LDAP è molto grande, potrebbe essere opportuno impostarlo su un sottoalbero più granulare per ridurre i tempi di ricerca.

Parametri utilizzati	Descrizione
groupSearchType: ActiveDirectory	Utilizza il server Windows Active Directory come server LDAP.
<pre>userSearchFilter: " (& (objectClass=person) (sAMAccountName=%USERNAME%)) "</pre> Per utilizzare userPrincipalName (indirizzo email per l'accesso) puoi modificare userSearchFilter in: <pre>" (& (objectClass=person) (userPrincipalName=%USERNAME%)) "</pre> In alternativa, per cercare sia userPrincipalName che sAMAccountName, è possibile utilizzare il seguente userSearchFilter: <pre>" (& (objectClass=person) (</pre>	(sAMAccountName=%USERNAME%)(userPrincipalName=%USERNAME%))" ----
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
Questo è il nome distinto dell'utente di sola lettura che verrà utilizzato per cercare nella directory LDAP. Per Active Directory è solitamente più semplice utilizzare userPrincipalName (formato indirizzo email) per l'utente.	cercaBindPassword

Per testarlo, disconnettiti dall'interfaccia utente di Element e accedi nuovamente come utente di quel gruppo.

Visualizza i dettagli LDAP

Visualizzare le informazioni LDAP nella pagina LDAP nella scheda Cluster.



Per visualizzare queste impostazioni di configurazione LDAP è necessario abilitare LDAP.

1. Per visualizzare i dettagli LDAP con l'interfaccia utente Element, fare clic su **Cluster > LDAP**.
 - **Nome host/Indirizzo IP:** Indirizzo di un server di directory LDAP o LDAPS.

- **Tipo di autenticazione:** metodo di autenticazione dell'utente. Valori possibili:
 - Legame diretto
 - Cerca e collega
- **DN di binding di ricerca:** un DN completamente qualificato con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente (richiede l'accesso a livello di binding alla directory LDAP).
- **Cerca password di associazione:** password utilizzata per autenticare l'accesso al server LDAP.
- **DN base ricerca utente:** il DN base dell'albero utilizzato per avviare la ricerca utente. Il sistema esegue la ricerca nel sottoalbero dalla posizione specificata.
- **Filtro di ricerca utente:** inserisci quanto segue utilizzando il tuo nome di dominio:

```
( & (objectClass=person) ( | (sAMAccountName=%USERNAME%) (userPrincipalName=%USERN
AME%) ) )
```

- **Tipo di ricerca di gruppo:** tipo di ricerca che controlla il filtro di ricerca di gruppo predefinito utilizzato. Valori possibili:
 - Active Directory: appartenenza nidificata di tutti i gruppi LDAP di un utente.
 - Nessun gruppo: nessun supporto di gruppo.
 - Membro DN: gruppi in stile Membro DN (livello singolo).
- **DN base ricerca gruppo:** il DN base dell'albero utilizzato per avviare la ricerca di gruppo. Il sistema esegue la ricerca nel sottoalbero dalla posizione specificata.
- **Test di autenticazione utente:** dopo aver configurato LDAP, utilizzare questa opzione per testare l'autenticazione del nome utente e della password per il server LDAP. Inserisci un account già esistente per testarlo. Vengono visualizzate le informazioni sul nome distinto e sul gruppo utente, che è possibile copiare per un utilizzo successivo durante la creazione degli amministratori del cluster.

Testare la configurazione LDAP

Dopo aver configurato LDAP, dovresti testarlo utilizzando l'interfaccia utente Element o l'API Element `TestLdapAuthentication` metodo.

Passi

1. Per testare la configurazione LDAP con Element UI, procedere come segue:
 - a. Fare clic su **Cluster > LDAP**.
 - b. Fare clic su **Test autenticazione LDAP**.
 - c. Risolvi eventuali problemi utilizzando le informazioni nella tabella sottostante:

Messaggio di errore	Descrizione
xLDAPUserNotFound	• L'utente sottoposto a test non è stato trovato nella configurazione <code>userSearchBaseDN</code> sottoalbero. • IL <code>userSearchFilter</code> è configurato in modo errato.

Messaggio di errore	Descrizione
<code>xLDAPBindFailed (Error: Invalid credentials)</code>	- Il nome utente testato è un utente LDAP valido, ma la password fornita non è corretta. - Il nome utente testato è un utente LDAP valido, ma l'account è attualmente disabilitato.
<code>xLDAPSearchBindFailed (Error: Can't contact LDAP server)</code>	L'URI del server LDAP non è corretto.
<code>xLDAPSearchBindFailed (Error: Invalid credentials)</code>	Il nome utente o la password di sola lettura non sono configurati correttamente.
<code>xLDAPSearchFailed (Error: No such object)</code>	IL <code>userSearchBaseDN</code> non è una posizione valida all'interno dell'albero LDAP.
<code>xLDAPSearchFailed (Error: Referral)</code>	- IL <code>userSearchBaseDN</code> non è una posizione valida all'interno dell'albero LDAP. - IL <code>userSearchBaseDN</code> E <code>groupSearchBaseDN</code> si trovano in una OU annidata. Ciò può causare problemi di autorizzazione. La soluzione alternativa è quella di includere l'OU nelle voci DN di base dell'utente e del gruppo (ad esempio: <code>ou=storage, cn=company, cn=com</code>)

2. Per testare la configurazione LDAP con l'API Element, procedere come segue:

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 dei gruppi di 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"
  }
}
```

Disabilitare LDAP

È possibile disattivare l'integrazione LDAP tramite l'interfaccia utente di Element.

Prima di iniziare, è opportuno annotare tutte le impostazioni di configurazione, poiché disabilitando LDAP tutte le impostazioni vengono cancellate.

Passi

1. Fare clic su **Cluster > LDAP**.
2. Fare clic su **No**.
3. Fare clic su **Disabilita LDAP**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci il tuo sistema

Gestisci il tuo sistema

Puoi gestire il tuo sistema nell'interfaccia utente Element. Ciò include l'abilitazione dell'autenticazione a più fattori, la gestione delle impostazioni del cluster, il supporto degli standard federali di elaborazione delle informazioni (FIPS) e l'utilizzo della gestione delle chiavi esterne.

- ["Abilita l'autenticazione a più fattori"](#)
- ["Configurare le impostazioni del cluster"](#)
- ["Creare un cluster che supporti le unità FIPS"](#)
- ["Inizia con la gestione delle chiavi esterne"](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Abilita l'autenticazione a più fattori

Configurare l'autenticazione a più fattori

L'autenticazione a più fattori (MFA) utilizza un Identity Provider (IdP) di terze parti tramite Security Assertion Markup Language (SAML) per gestire le sessioni utente. L'MFA consente agli amministratori di configurare ulteriori fattori di autenticazione, a seconda delle necessità, come password e messaggio di testo oppure password e messaggio di posta elettronica.

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 possono essere trovati in ["Riferimento API dell'elemento"](#).

1. Creare una nuova configurazione dell'Identity Provider (IdP) 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 dall'IdP di terze parti. Questi metadati devono essere convalidati per garantire che siano formattati correttamente in JSON. Sono disponibili numerose applicazioni di formattazione JSON che puoi utilizzare, ad esempio: <https://freeformatter.com/json-escape.html>.

2. Recupera i metadati del cluster tramite `spMetadataUrl` per copiarli 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 l'IdP al fine di stabilire una relazione di trust.

3. Configurare le asserzioni SAML sull'IdP di terze parti in modo da includere l'attributo "NameID" per identificare in modo univoco un utente per la registrazione degli audit e per il corretto funzionamento di Single Logout.
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 dell'attributo SAML per ottenere l'effetto desiderato, come mostrato negli esempi seguenti:

- `email=bob@company.com` — dove l'IdP è configurato per rilasciare un indirizzo email negli attributi SAML.
- `group=cluster-administrator` - dove l'IdP è configurato per rilasciare una proprietà di gruppo a cui tutti gli utenti dovrebbero avere accesso. Si noti che l'abbinamento Nome/Valore dell'attributo SAML è sensibile alle maiuscole e alle minuscole per motivi di sicurezza.

5. Abilitare MFA per il cluster chiamando il seguente metodo API: `EnableIdpAuthentication`

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Informazioni aggiuntive per l'autenticazione a più fattori

È opportuno tenere presente le seguenti avvertenze in relazione all'autenticazione a più fattori.

- Per aggiornare i certificati IdP non più validi, è necessario utilizzare un utente non amministratore IdP per chiamare il seguente metodo API: `UpdateIdpConfiguration`
- L'MFA non è compatibile con i certificati di lunghezza inferiore a 2048 bit. Per impostazione predefinita, sul cluster viene creato un certificato SSL a 2048 bit. Dovresti evitare di impostare un certificato di dimensioni inferiori quando chiami il metodo API: `SetSSLCertificate`



Se il cluster utilizza un certificato inferiore a 2048 bit prima dell'aggiornamento, il certificato del cluster deve essere aggiornato con un certificato da 2048 bit o superiore dopo l'aggiornamento a Element 12.0 o versione successiva.

- 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). Se è necessario creare utenti dotati di queste capacità, aggiungere utenti amministratori del cluster LDAP o utenti amministratori del cluster locale.

Trova maggiori informazioni

- ["Gestione dello storage con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurare le impostazioni del cluster

Abilitare e disabilitare la crittografia a riposo per un cluster

Con i cluster SolidFire è possibile crittografare tutti i dati inattivi archiviati sulle unità del cluster. È possibile abilitare la protezione a livello di cluster delle unità auto-crittografanti (SED) utilizzando ["crittografia a riposo basata su hardware o software"](#).

È possibile abilitare la crittografia hardware a riposo tramite l'interfaccia utente o l'API di Element. L'abilitazione della funzionalità di crittografia hardware a riposo non influisce sulle prestazioni o sull'efficienza del cluster. È possibile abilitare la crittografia software a riposo solo tramite l'API Element.

La crittografia basata su hardware a riposo non è abilitata per impostazione predefinita durante la creazione del cluster e può essere abilitata e disabilitata dall'interfaccia utente di Element.



Per i cluster di archiviazione all-flash SolidFire, la crittografia software a riposo deve essere abilitata durante la creazione del cluster e non può essere disabilitata dopo la creazione del cluster.

Cosa ti servirà

- Si dispone dei privilegi di amministratore del cluster per abilitare o modificare le impostazioni di crittografia.
- Per la crittografia a riposo basata su hardware, è necessario assicurarsi che il cluster sia in uno stato di integrità prima di modificare le impostazioni di crittografia.
- Se si disabilita la crittografia, è necessario che due nodi partecipino a un cluster per accedere alla chiave per disabilitare la crittografia su un'unità.

Controllare lo stato di crittografia a riposo

Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo sul cluster, utilizzare ["Ottieni informazioni sul cluster"](#) metodo. Puoi usare il ["Ottieni informazioni sulla crittografia software a riposo"](#) metodo per ottenere le informazioni che il cluster utilizza per crittografare i dati a riposo.



La dashboard dell'interfaccia utente del software Element su <https://<MVIP>/> attualmente mostra solo lo stato di crittografia a riposo per la crittografia basata su hardware.

Opzioni

- [Abilita la crittografia basata su hardware a riposo](#)
- [Abilita la crittografia basata su software a riposo](#)
- [Disabilitare la crittografia basata su hardware a riposo](#)

Abilita la crittografia basata su hardware a riposo



Per abilitare la crittografia a riposo utilizzando una configurazione di gestione delle chiavi esterna, è necessario abilitare la crittografia a riposo tramite ["API"](#). L'abilitazione tramite il pulsante Element UI esistente ripristinerà l'utilizzo delle chiavi generate internamente.

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster > Impostazioni**.
2. Selezionare **Abilita crittografia a riposo**.

Abilita la crittografia basata su software a riposo



La crittografia software a riposo non può essere disabilitata dopo essere stata abilitata sul cluster.

1. Durante la creazione del cluster, eseguire il comando ["metodo di creazione del cluster"](#) con `enableSoftwareEncryptionAtRest` impostato su `true`.

Disabilitare la crittografia basata su hardware a riposo

1. Dall'interfaccia utente dell'elemento, seleziona **Cluster > Impostazioni**.
2. Selezionare **Disabilita crittografia a riposo**.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Imposta la soglia di riempimento del cluster

È possibile modificare il livello al quale il sistema genera un avviso di riempimento del cluster di blocchi seguendo i passaggi indicati di seguito. Inoltre, è possibile utilizzare il metodo API `ModifyClusterFullThreshold` per modificare il livello in cui il sistema genera un avviso di blocco o di metadati.

Cosa ti servirà

È necessario disporre dei privilegi di amministratore del cluster.

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Nella sezione Impostazioni complete del cluster, immettere una percentuale in **Genera un avviso quando rimane _% di capacità prima che Helix non riesca a riprendersi da un errore del nodo**.
3. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

["Come vengono calcolate le soglie di blockSpace per Element"](#)

Abilita e disabilita il bilanciamento del carico del volume

A partire da Element 12.8, è possibile utilizzare Volume Load Balancing per bilanciare i volumi tra i nodi in base agli IOPS effettivi di ciascun volume anziché agli IOPS minimi configurati nella policy QoS. È possibile abilitare e disabilitare il bilanciamento del carico del volume, disabilitato per impostazione predefinita, tramite l'interfaccia utente o l'API di Element.

Passi

1. Selezionare **Cluster > Impostazioni**.
2. Nella sezione Cluster Specific, modifica lo stato per Volume Load Balancing:

Abilita il bilanciamento del carico del volume

Selezionare **Abilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

Disabilita il bilanciamento del carico del volume:

Selezionare **Disabilita bilanciamento del carico su IOPS effettivi** e confermare la selezione.

3. Facoltativamente, selezionare **Reporting > Panoramica** per confermare la modifica dello stato per il saldo sugli IOPS effettivi. Potrebbe essere necessario scorrere verso il basso le informazioni sullo stato del cluster per visualizzarne lo stato.

Trova maggiori informazioni

- ["Abilita il bilanciamento del carico del volume tramite l'API"](#)
- ["Disabilitare il bilanciamento del carico del volume tramite l'API"](#)
- ["Creare e gestire policy QoS del volume"](#)

Abilita e disabilita 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 > Impostazioni**.
2. Nella sezione Abilita/Disabilita accesso supporto, inserisci la durata (in ore) per cui desideri consentire l'accesso al supporto.
3. Fare clic su **Abilita accesso supporto**.
4. **Facoltativo:** per disattivare l'accesso al supporto, fare clic su **Disattiva accesso al supporto**.

Gestisci il banner Termini di utilizzo

È possibile abilitare, modificare o configurare un banner contenente un messaggio per l'utente.

Opzioni

[Abilita il banner Termini di utilizzo](#) [Modifica il banner dei Termini di utilizzo](#) [Disattiva il banner Termini di utilizzo](#)

Abilita il banner Termini di utilizzo

È possibile abilitare un banner con i Termini di utilizzo che viene visualizzato quando un utente accede all'interfaccia utente di Element. Quando l'utente clicca sul banner, viene visualizzata una finestra di dialogo di testo contenente il messaggio configurato per il cluster. Il banner può essere rimosso in qualsiasi momento.

Per abilitare 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**, immettere il testo da visualizzare nella finestra di dialogo Termini di utilizzo.



Non superare i 4096 caratteri.

3. Fare clic su **Abilita**.

Modifica il banner dei Termini di utilizzo

Puoi modificare il testo che un utente vede quando seleziona il banner di accesso ai Termini di utilizzo.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che la funzione Termini di utilizzo sia abilitata.

Passi

1. Fare clic su **Utenti > Termini di utilizzo**.
2. Nella finestra di dialogo **Termini di utilizzo**, modifica il testo che desideri visualizzare.



Non superare i 4096 caratteri.

3. Fare clic su **Salva modifiche**.

Disattiva il banner Termini di utilizzo

Puoi disattivare il banner Termini di utilizzo. Con il banner disabilitato, all'utente non viene più richiesto di accettare i termini di utilizzo quando utilizza Element UI.

Cosa ti servirà

- Per configurare i Termini di utilizzo è necessario disporre dei privilegi di amministratore del cluster.
- Assicurati che i Termini di utilizzo siano abilitati.

Passi

1. Fare clic su **Utenti > Termini di utilizzo**.
2. Fare clic su **Disabilita**.

Imposta il protocollo di tempo di rete

Configurare i server Network Time Protocol affinché il cluster esegua le query

È possibile istruire ciascun nodo di un cluster a interrogare un server NTP (Network Time Protocol) per gli aggiornamenti. Il cluster contatta solo i server configurati e richiede loro informazioni NTP.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

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, a seconda della posizione fisica del cluster SolidFire, non è sempre possibile stabilire una connessione a questo sito.

L'utilizzo dell'FQDN dipende dal fatto che le impostazioni DNS del singolo nodo di archiviazione siano corrette e operative. Per farlo, configura i server DNS su ogni nodo di archiviazione e assicurati che le porte siano aperte consultando la pagina Requisiti delle porte di rete.

È possibile inserire fino a cinque server NTP diversi.



È possibile utilizzare sia indirizzi IPv4 che IPv6.

Cosa ti servirà

Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.

Passi

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 > Impostazioni**.
4. In Impostazioni Network Time Protocol, seleziona **No**, che utilizza la configurazione NTP standard.

5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- ["Configurare il cluster per ascoltare le trasmissioni NTP"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Configurare il cluster per ascoltare le trasmissioni NTP

Utilizzando la modalità broadcast, è possibile istruire ciascun nodo di un cluster ad ascoltare sulla rete i messaggi broadcast NTP (Network Time Protocol) provenienti da un server specifico.

L'NTP viene utilizzato per sincronizzare gli orologi su una rete. La connessione a un server NTP interno o esterno dovrebbe essere parte della configurazione iniziale del cluster.

Cosa ti servirà

- Per configurare questa impostazione è necessario disporre dei privilegi di amministratore del cluster.
- È necessario configurare un server NTP sulla rete come server broadcast.

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Inserire nell'elenco dei server il server o i server NTP che utilizzano la modalità broadcast.
3. In Impostazioni Network Time Protocol, seleziona **Sì** per utilizzare un client broadcast.
4. Per impostare il client broadcast, nel campo **Server**, immettere il server NTP configurato in modalità broadcast.
5. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- ["Configurare i server Network Time Protocol affinché il cluster esegua le query"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci SNMP

Scopri di più su 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 USM (User-based Security Model) SNMP e configurare trap per monitorare il cluster SolidFire. È inoltre possibile visualizzare e accedere ai file della base dati di gestione.



È possibile utilizzare sia indirizzi IPv4 che 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 abilitare o disabilitare SNMP. Dopo aver abilitato SNMP, puoi scegliere quale versione utilizzare. Se si utilizza la versione 2, è possibile aggiungere richiedenti, mentre se si utilizza la versione 3, è possibile impostare utenti USM.

- **Impostazioni trap SNMP**

Puoi identificare le trappole che vuoi catturare. È possibile impostare l'host, la porta e la stringa della community per ciascun destinatario della trap.

Configurare un richiedente SNMP

Quando è abilitata la versione 2 di SNMP, è possibile abilitare o disabilitare un richiedente e configurare i richiedenti per ricevere richieste SNMP autorizzate.

1. Fare clic sul **Cluster > SNMP**.
2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 2**.
4. Nella sezione **Richiedenti**, immettere le informazioni **Stringa della community** e **Rete**.



Per impostazione predefinita, la stringa della community è public e la rete è localhost. È possibile modificare queste impostazioni predefinite.

5. **Facoltativo:** per aggiungere un altro richiedente, fare clic su **Aggiungi un richiedente** e immettere le informazioni **Stringa della community** e **Rete**.
6. Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- [Configurare le trappole SNMP](#)
- [Visualizzare i dati degli oggetti gestiti utilizzando i file della base di informazioni di gestione](#)

Configurare un utente USM SNMP

Quando si abilita SNMP versione 3, è necessario configurare un utente USM per ricevere richieste SNMP autorizzate.

1. Fare clic su **Cluster > SNMP**.
2. In **Impostazioni SNMP generali**, fare clic su **Sì** per abilitare SNMP.
3. Dall'elenco **Versione**, seleziona **Versione 3**.

4. Nella sezione **Utenti USM**, immettere il nome, la password e la passphrase.
5. **Facoltativo:** per aggiungere un altro utente USM, fare clic su **Aggiungi un utente USM** e immettere nome, password e passphrase.
6. Fare clic su **Salva modifiche**.

Configurare le trappole SNMP

Gli amministratori di sistema possono utilizzare trap SNMP, note anche come notifiche, per monitorare lo stato di salute del cluster SolidFire .

Quando le trap SNMP sono abilitate, il cluster SolidFire genera trap associate alle voci del registro eventi e agli avvisi di sistema. Per ricevere le notifiche SNMP, è necessario scegliere le trappole da generare e identificare i destinatari delle informazioni sulle trappole. Per impostazione predefinita, non vengono generate trappole.

1. Fare clic su **Cluster > SNMP**.
2. Selezionare uno o più tipi di trap nella sezione **Impostazioni trap SNMP** che il sistema deve generare:
 - Cluster Fault Traps
 - Cluster Resolved Fault Traps
 - Trappole per eventi cluster
3. Nella sezione **Destinatari trap**, immettere le informazioni relative all'host, alla porta e alla stringa di community per un destinatario.
4. **Facoltativo:** per aggiungere un altro destinatario della trappola, fare clic su **Aggiungi un destinatario della trappola** e immettere le informazioni relative a host, porta e stringa della community.
5. Fare clic su **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 di volume
- Volumi per statistiche di conto
- Statistiche del nodo
- Altri dati come report, errori ed eventi di sistema

Il sistema supporta anche l'accesso al file MIB contenente i punti di accesso di livello superiore (OIDs) ai prodotti della serie SF.

Passi

1. Fare clic su **Cluster > SNMP**.
2. In **SNMP MIB**, fare clic sul file MIB che si desidera scaricare.
3. Nella finestra di download visualizzata, apri o salva il file MIB.

Gestisci unità

Ogni nodo contiene una o più unità fisiche utilizzate per archiviare una parte dei dati del cluster. Il cluster utilizza la capacità e le prestazioni dell'unità dopo che questa è stata aggiunta correttamente a un cluster. È possibile utilizzare l'interfaccia utente di Element per gestire le unità.

Dettagli delle unità

La pagina Unità nella scheda Cluster fornisce un elenco delle unità attive nel cluster. È possibile filtrare la pagina selezionando tra le 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 unità non assegnate a un cluster ed elencate nella scheda Disponibili dopo la creazione di un nuovo cluster SolidFire .

Nell'elenco delle unità attive compaiono i seguenti elementi.

- **ID unità**

Numero sequenziale assegnato all'unità.

- **ID nodo**

Numero di nodo assegnato quando il nodo viene aggiunto al cluster.

- **Nome nodo**

Il nome del nodo che ospita l'unità.

- **Fessura**

Il numero dello slot in cui si trova fisicamente l'unità.

- **Capacità**

La dimensione dell'unità, in GB.

- **Seriale**

Il numero di serie dell'unità.

- **Usura rimanente**

L'indicatore del livello di usura.

Il sistema di archiviazione segnala la quantità approssimativa di usura disponibile su ciascuna unità a stato solido (SSD) per la scrittura e la cancellazione dei dati. Un'unità che ha consumato il 5 percento dei cicli di scrittura e cancellazione previsti segnala un'usura residua del 95 percento. Il sistema non aggiorna automaticamente le informazioni sull'usura dell'unità; è possibile aggiornare o chiudere e ricaricare la pagina per aggiornare le informazioni.

- **Tipo**

Il tipo di unità. Il tipo può essere blocco o metadati.

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestisci nodi

Gestisci nodi

È possibile gestire lo storage SolidFire e i nodi Fibre Channel dalla pagina Nodi della scheda Cluster.

Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo si blocca, viene generato un errore di cluster appropriato.

Trova maggiori informazioni

[Aggiungere un nodo a un cluster](#)

Aggiungere un nodo a un cluster

È possibile aggiungere nodi a un cluster quando è necessario più spazio di archiviazione o dopo la creazione del cluster. I nodi richiedono una configurazione iniziale quando vengono accesi per la prima volta. Dopo aver configurato il nodo, questo viene visualizzato nell'elenco dei nodi in sospeso ed è possibile aggiungerlo a un cluster.

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

È possibile aggiungere nodi di capacità più piccole o più grandi 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 disporre di spazio sufficiente per spostare i dati nel caso in cui uno dei nodi più grandi dovesse guastarsi. È possibile aggiungere capacità di nodi più piccole a un cluster di nodi più grande per migliorare le prestazioni.



Se un nodo appena aggiunto rappresenta più del 50 percento della capacità totale del cluster, parte della capacità di questo nodo viene resa inutilizzabile ("bloccata"), in modo da rispettare la regola sulla capacità. Questa situazione rimane invariata finché non viene aggiunto altro spazio di archiviazione. Se viene aggiunto un nodo molto grande che non rispetta la regola della capacità, il nodo precedentemente bloccato non sarà più bloccato, mentre il nodo appena aggiunto diventerà bloccato. Per evitare che ciò accada, la capacità dovrebbe essere sempre aggiunta in coppia. Quando un nodo diventa inutilizzabile, viene generato l'errore cluster strandedCapacity.

["Video NetApp : Scalabilità in base alle tue esigenze: espansione di un cluster SolidFire"](#)

È possibile aggiungere nodi agli appliance NetApp HCI .

Passi

1. Selezionare **Cluster > Nodi**.
2. Fare clic su **In attesa** per visualizzare l'elenco dei nodi in attesa.

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 Attivi in sospeso.

SolidFire installa la versione software Element del cluster sui nodi in sospeso quando li aggiungi a un cluster. Potrebbero volerci alcuni minuti.

3. Eseguire una delle seguenti operazioni:
 - Per aggiungere singoli nodi, fare clic sull'icona **Azioni** relativa al nodo che si desidera aggiungere.
 - Per aggiungere più nodi, seleziona la casella di controllo dei nodi da aggiungere, quindi **Azioni in blocco**. **Nota:** se il nodo che stai 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. Dopo l'aggiornamento, il nodo si aggiunge automaticamente al cluster. Durante questo processo asincrono, il nodo sarà nello stato pendingActive.
4. Fare clic su **Aggiungi**.

Il nodo appare nell'elenco dei nodi attivi.

Trova maggiori informazioni

[Versionamento e compatibilità dei nodi](#)

Versionamento e compatibilità dei nodi

La compatibilità dei nodi si basa sulla versione del software Element installata su un nodo. I cluster di storage basati sul software Element creano automaticamente un'immagine di un nodo nella versione del software Element sul cluster se il nodo e il cluster non hanno versioni compatibili.

L'elenco seguente descrive i livelli di significatività della versione software che compongono il numero di versione del software Element:

- **Maggiore**

Il primo numero indica la versione del 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 è possibile creare un cluster con nodi con versioni principali miste.

- **Minore**

Il secondo numero indica funzionalità software minori o miglioramenti alle funzionalità software esistenti che sono stati aggiunti a una versione principale. Questo componente viene incrementato all'interno di un componente di versione principale per indicare che questa versione incrementale non è compatibile con nessun'altra versione incrementale del software Element con un componente secondario 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 del software Element

rappresentata dai componenti major.minor. Ad esempio, 11.0.1 è compatibile con 11.0.2 e 11.0.2 è compatibile con 11.0.3.

Per garantire la compatibilità, i numeri di versione principale e secondaria devono corrispondere. Per garantire la compatibilità, i micronumeri non devono necessariamente corrispondere.

Capacità del cluster in un ambiente di nodi misti

È possibile combinare diversi tipi di nodi in un cluster. Le serie SF 2405, 3010, 4805, 6010, 9605, 9010, 19210, 38410 e la serie H possono coesistere in un cluster.

La serie H è composta dai nodi H610S-1, H610S-2, H610S-4 e H410S. Questi nodi supportano sia 10GbE che 25GbE.

È meglio non mescolare nodi crittografati e non crittografati. In un cluster con nodi misti, nessun nodo può essere più grande del 33 per cento 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 un SF-Series 9605. La soglia di capacità del cluster viene calcolata in base alla potenziale perdita del nodo più grande in questa situazione.

A seconda della versione del software Element, i seguenti nodi di archiviazione della serie SF non sono supportati:

A partire da...	Nodo di archiviazione non supportato...
Elemento 12.8	• SF4805 • SF9605 • SF19210 • SF38410
Elemento 12.7	• SF2405 • SF9608
Elemento 12.0	• SF3010 • SF6010 • SF9010

Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x.

Visualizza i dettagli del nodo

È possibile visualizzare i dettagli dei singoli nodi, ad esempio tag di servizio, dettagli dell'unità e grafici per l'utilizzo e statistiche dell'unità. La pagina Nodi della scheda Cluster fornisce la colonna Versione in cui è possibile visualizzare la versione software di ciascun nodo.

Passi

1. Fare clic su **Cluster > Nodi**.

2. Per visualizzare i dettagli di un nodo specifico, fare clic sull'icona **Azioni** per un nodo.
3. Fare clic su **Visualizza dettagli**.
4. Esaminare i dettagli del nodo:
 - **ID nodo**: ID generato dal sistema per il nodo.
 - **Nome nodo**: il nome host del nodo.
 - **Ruolo del nodo**: il ruolo che il nodo ha nel cluster. Valori possibili:
 - Cluster Master: il nodo che esegue attività amministrative a livello di cluster e contiene MVIP e SVIP.
 - Nodo ensemble: un nodo che partecipa al cluster. A seconda della dimensione del cluster, sono presenti 3 o 5 nodi ensemble.
 - Fibre Channel: un nodo del cluster.
 - **Tipo di nodo**: il tipo di modello del nodo.
 - **Unità attive**: numero di unità attive nel nodo.
 - **Utilizzo del nodo**: percentuale di utilizzo del nodo in base a nodeHeat. Il valore visualizzato è recentPrimaryTotalHeat in percentuale. Disponibile a partire da Element 12.8.
 - **IP di gestione**: indirizzo IP di gestione (MIP) assegnato al nodo per le attività di amministrazione di rete da 1 GbE o 10 GbE.
 - **IP del cluster**: l'indirizzo IP del cluster (CIP) assegnato al nodo utilizzato per la comunicazione tra i nodi nello stesso cluster.
 - **IP di archiviazione**: l'indirizzo IP di archiviazione (SIP) assegnato al nodo utilizzato per la scoperta della rete iSCSI e per tutto il traffico dati della rete.
 - **ID VLAN di gestione**: ID virtuale per la rete locale di gestione.
 - **ID VLAN di archiviazione**: ID virtuale per la rete locale di archiviazione.
 - **Versione**: la versione del software in esecuzione su ciascun nodo.
 - **Porta di replicazione**: la porta utilizzata sui nodi per la replica remota.
 - **Tag di servizio**: il numero univoco del tag di servizio assegnato al nodo.
 - **Dominio di protezione personalizzato**: il dominio di protezione personalizzato assegnato al nodo.

Visualizza i dettagli delle porte Fibre Channel

È possibile visualizzare i dettagli delle porte Fibre Channel, come lo stato, il nome e l'indirizzo della porta, dalla pagina Porte FC.

Visualizza le informazioni sulle porte Fibre Channel connesse al cluster.

Passi

1. Fare clic su **Cluster > Porte FC**.
2. Per filtrare le informazioni in questa pagina, clicca su **Filtra**.
3. Esamina i dettagli:
 - **ID nodo**: il nodo che ospita la sessione per la connessione.
 - **Nome nodo**: Nome del nodo generato dal sistema.
 - **Slot**: Numero dello slot in cui si trova la porta Fibre Channel.

- **Porta HBA:** porta fisica sull'adattatore bus host (HBA) Fibre Channel.
- **WWNN:** Nome del nodo mondiale.
- **WWPN:** Nome della porta mondiale di destinazione.
- **Switch WWN:** Nome mondiale dello switch Fibre Channel.
- **Stato del porto:** Stato attuale del porto.
- **nPort ID:** ID della porta del nodo sulla struttura Fibre Channel.
- **Velocità:** la velocità Fibre Channel negoziata. I valori possibili sono i seguenti:
 - 4Gbps
 - 8Gbps
 - 16Gbps

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestire reti virtuali

Gestire reti virtuali

La rete virtuale nello storage SolidFire consente di connettere a un unico cluster il traffico tra più client che si trovano su reti logiche separate. Le connessioni al cluster sono separate nello stack di rete tramite l'uso del tagging VLAN.

Trova maggiori informazioni

- [Aggiungi una rete virtuale](#)
- [Abilita il routing e l'inoltro virtuali](#)
- [Modifica una rete virtuale](#)
- [Modifica VLAN VRF](#)
- [Elimina una rete virtuale](#)

Aggiungi una rete virtuale

È possibile aggiungere una nuova rete virtuale a una configurazione cluster per abilitare una connessione di ambiente multi-tenant a un cluster che esegue il software Element.

Cosa ti servirà

- Identificare il blocco di indirizzi IP che verrà assegnato alle reti virtuali sui nodi del cluster.
- Identificare un indirizzo IP di rete di storage (SVIP) che verrà utilizzato come endpoint per tutto il traffico di storage NetApp Element .



Per questa configurazione è necessario considerare i seguenti criteri:

- Le VLAN che non sono abilitate per VRF richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP.

- Le VLAN abilitate per VRF non richiedono che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.
- L'SVIP predefinito non richiede che gli iniziatori si trovino nella stessa subnet dell'SVIP e il routing è supportato.

Quando si aggiunge una rete virtuale, viene creata un'interfaccia per ciascun nodo e ciascuno richiede un indirizzo IP di rete virtuale. Il numero di indirizzi IP specificato durante la creazione di una nuova rete virtuale deve essere uguale o maggiore del numero di nodi nel cluster. Gli indirizzi di rete virtuale vengono forniti in blocco e assegnati automaticamente ai singoli nodi. Non è necessario assegnare manualmente gli indirizzi di rete virtuale ai nodi del cluster.

Passi

1. Fare clic su **Cluster > Rete**.
2. Fare clic su **Crea VLAN**.
3. Nella finestra di dialogo **Crea una nuova VLAN**, immettere i valori nei seguenti campi:
 - **Nome VLAN**
 - **Tag VLAN**
 - **SVIP**
 - **Maschera di rete**
 - (Facoltativo) **Descrizione**
4. Immettere l'indirizzo **IP iniziale** per l'intervallo di indirizzi IP in **Blocchi di indirizzi IP**.
5. Immettere la **Dimensione** dell'intervallo IP come numero di indirizzi IP da includere nel blocco.
6. Fare clic su **Aggiungi un blocco** per aggiungere un blocco non continuo di indirizzi IP per questa VLAN.
7. Fare clic su **Crea VLAN**.

Visualizza i dettagli della rete virtuale

Passi

1. Fare clic su **Cluster > Rete**.
2. Esamina i dettagli.
 - **ID**: ID univoco della rete VLAN, assegnato dal sistema.
 - **Nome**: Nome univoco assegnato dall'utente per la rete VLAN.
 - **Tag VLAN**: tag VLAN assegnato al momento della creazione della rete virtuale.
 - **SVIP**: Indirizzo IP virtuale di archiviazione assegnato alla rete virtuale.
 - **Netmask**: Maschera di rete per questa rete virtuale.
 - **Gateway**: Indirizzo IP univoco di un gateway di rete virtuale. VRF deve essere abilitato.
 - **VRF abilitato**: Indica se il routing e l'inoltro virtuali sono abilitati o meno.
 - **IP utilizzati**: intervallo di indirizzi IP di rete virtuale utilizzati per la rete virtuale.

Abilita il routing e l'inoltro virtuali

È possibile abilitare il routing e l'inoltro virtuali (VRF), che consente a più istanze di una tabella di routing di esistere in un router e di funzionare simultaneamente. Questa funzionalità è disponibile solo per le reti di archiviazione.

È possibile abilitare 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 > Rete**.
2. Per abilitare VRF su una nuova VLAN, selezionare **Crea VLAN**.
 - a. Inserire le informazioni rilevanti per il nuovo VRF/VLAN. Vedere Aggiunta di una rete virtuale.
 - b. Selezionare la casella di controllo **Abilita VRF**.
 - c. **Facoltativo**: Inserisci un gateway.
3. Fare clic su **Crea VLAN**.

Trova maggiori informazioni

[Aggiungi una rete virtuale](#)

Modifica una rete virtuale

È possibile modificare gli attributi VLAN, come il nome 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 sessioni iSCSI, di replica remota o di altra rete, la modifica potrebbe non riuscire.

Quando si gestisce la dimensione degli intervalli di indirizzi IP VLAN, è necessario 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 indirizzi IP, dall'intervallo di indirizzi IP iniziale o da un blocco IP, utilizzati dai nodi del cluster, l'operazione potrebbe non riuscire.
- Non è possibile riassegnare specifici indirizzi IP in uso ad altri nodi del cluster.

È possibile aggiungere un blocco di indirizzi IP utilizzando la seguente procedura:

1. Selezionare **Cluster > Rete**.
2. Selezionare l'icona Azioni per la VLAN che si desidera modificare.
3. Selezionare **Modifica**.
4. Nella finestra di dialogo **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 **Salva modifiche**.

Collegamento agli articoli della Knowledge Base sulla 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 di IP duplicato dopo l'aggiunta di un nodo di archiviazione nella VLAN sul cluster Element"](#)

- ["Come determinare quali IP VLAN sono in uso e a quali nodi sono assegnati tali IP in Element"](#)

Modifica VLAN VRF

È possibile modificare gli attributi VLAN VRF, come il nome VLAN, la netmask, il gateway e i blocchi di indirizzi IP.

1. Fare clic su **Cluster > Rete**.
2. Fare clic sull'icona Azioni per la VLAN che si desidera modificare.
3. Fare clic su **Modifica**.
4. Immettere i nuovi attributi per la VLAN VRF nella finestra di dialogo **Modifica VLAN**.
5. Fare clic su **Salva modifiche**.

Elimina una rete virtuale

È possibile rimuovere un oggetto di rete virtuale. Prima di rimuovere una rete virtuale, è necessario aggiungere i blocchi di indirizzi a un'altra rete virtuale.

1. Fare clic su **Cluster > Rete**.
2. Fare clic sull'icona Azioni relativa alla VLAN che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Trova maggiori informazioni

[Modifica una rete virtuale](#)

Creare un cluster che supporti le unità FIPS

Prepara il cluster Element per la funzionalità delle unità FIPS

La sicurezza sta diventando sempre più critica per l'implementazione di soluzioni in molti ambienti dei clienti. Gli standard federali per l'elaborazione delle informazioni (FIPS) sono standard per la sicurezza e l'interoperabilità informatica. La crittografia certificata FIPS 140-2 per i dati inattivi è un componente della soluzione di sicurezza complessiva.

Per preparare l'abilitazione della funzionalità delle unità FIPS, è opportuno evitare di mischiare nodi in cui alcuni sono compatibili con le unità FIPS e altri no.

Un cluster è considerato conforme alle unità FIPS in base alle seguenti condizioni:

- Tutte le unità sono certificate FIPS.
- Tutti i nodi sono nodi unità FIPS.
- La crittografia a riposo (EAR) è abilitata.
- La funzionalità delle unità FIPS è abilitata. Tutte le unità e i nodi devono essere compatibili con FIPS e la crittografia a riposo deve essere abilitata per abilitare la funzionalità unità FIPS.

Abilita la crittografia a riposo

È possibile abilitare e disabilitare la crittografia a livello di cluster quando è inattivo. Questa funzione non è abilitata per impostazione predefinita. Per supportare le unità FIPS, è necessario abilitare la crittografia a riposo.

1. Nell'interfaccia utente del software NetApp Element , fare clic su **Cluster > Impostazioni**.
2. Fare clic su **Abilita crittografia a riposo**.

Trova maggiori informazioni

- [Abilitare e disabilitare la crittografia per un cluster](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Identificare se i nodi sono pronti per la funzionalità delle unità FIPS

È necessario verificare se tutti i nodi nel 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:

- Nessuno: il nodo non è in grado di supportare la funzionalità delle unità FIPS.
- Parziale: il nodo supporta FIPS, ma non tutte le unità sono FIPS.
- Pronto: il nodo è compatibile con FIPS e tutte le unità sono unità FIPS oppure non è presente alcuna unità.

Passi

1. Utilizzando l'API Element, verificare se i nodi e le unità nel cluster di archiviazione sono compatibili con le unità FIPS immettendo:

```
GetFipsReport
```

2. Esaminare i risultati, annotando tutti i nodi che non visualizzano lo stato Pronto.
3. Per tutti i nodi che non visualizzano lo stato Pronto, verificare se l'unità è in grado di supportare la funzionalità delle unità FIPS:
 - Utilizzando l'API Element, immettere: `GetHardwareList`
 - Prendere nota del valore di **DriveEncryptionCapabilityType**. Se è "fips", l'hardware può supportare la funzionalità delle unità FIPS.

Vedi i dettagli su `GetFipsReport` O `ListDriveHardware` nel ["Riferimento API dell'elemento"](#).

4. Se l'unità non supporta la funzionalità unità FIPS, sostituire l'hardware con hardware FIPS (nodo o unità).

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Abilita la funzionalità delle unità FIPS

È possibile abilitare la funzionalità delle unità FIPS utilizzando il software NetApp Element EnableFeature Metodo API.

La crittografia a riposo deve essere abilitata sul cluster e tutti i nodi e le unità devono essere compatibili con FIPS, come indicato quando GetFipsReport visualizza lo stato Pronto per tutti i nodi.

Fare un passo

1. Utilizzando l'API Element, abilitare FIPS su tutte le unità immettendo:

```
EnableFeature params: FipsDrives
```

Trova maggiori informazioni

- ["Gestisci l'archiviazione con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Controllare lo stato dell'unità FIPS

È possibile verificare se la funzionalità delle unità FIPS è abilitata sul cluster utilizzando il software NetApp Element GetFeatureStatus Metodo API che mostra se lo stato FIPS Drives Enabled è vero o falso.

1. Utilizzando l'API Element, verificare la funzionalità delle unità FIPS sul cluster immettendo:

```
GetFeatureStatus
```

2. Esaminare i risultati del GetFeatureStatus Chiamata API. Se il valore Unità FIPS abilitate è Vero, la funzionalità Unità FIPS è abilitata.

```
{ "enabled": true,  
  "feature": "FipsDrives"  
}
```

Trova maggiori informazioni

- ["Gestisci l'archiviazione con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Risolvere i problemi della funzionalità dell'unità FIPS

Utilizzando l'interfaccia utente del software NetApp Element , è possibile visualizzare avvisi per informazioni su guasti o errori del cluster nel sistema correlati alla funzionalità delle unità FIPS.

1. Utilizzando l'interfaccia utente di Element, seleziona **Reporting > Avvisi**.
2. Cercare guasti del cluster, tra cui:
 - Unità FIPS non corrispondenti
 - FIPS non rispetta la conformità
3. Per suggerimenti sulla risoluzione, vedere le informazioni sul codice di errore del cluster.

Trova maggiori informazioni

- [Codici di errore del cluster](#)
- ["Gestisci l'archiviazione con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Stabilire una comunicazione sicura

Abilita FIPS 140-2 per HTTPS sul tuo cluster

È possibile utilizzare il metodo API EnableFeature per abilitare la modalità operativa FIPS 140-2 per le comunicazioni HTTPS.

Con il software NetApp Element , puoi scegliere di abilitare la modalità operativa Federal Information Processing Standards (FIPS) 140-2 sul tuo cluster. L'abilitazione di questa modalità attiva il NetApp Cryptographic Security Module (NCSM) e sfrutta la crittografia certificata FIPS 140-2 Livello 1 per tutte le comunicazioni tramite HTTPS all'interfaccia utente e all'API NetApp Element .



Dopo aver abilitato la modalità FIPS 140-2, non è più possibile disattivarla. Quando la modalità FIPS 140-2 è abilitata, ogni nodo del cluster si riavvia ed esegue un autotest per verificare che NCSM sia correttamente abilitato e funzioni nella modalità certificata FIPS 140-2. Ciò provoca un'interruzione sia delle connessioni di gestione che di archiviazione sul cluster. È opportuno pianificare attentamente e abilitare questa modalità solo se l'ambiente in uso necessita del meccanismo di crittografia offerto.

Per ulteriori informazioni, consultare le informazioni sull'API Element.

Di seguito è riportato un esempio di richiesta API per abilitare FIPS:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "fips"
  },
  "id": 1
}
```

Dopo aver abilitato questa modalità operativa, tutte le comunicazioni HTTPS utilizzano i cifrari approvati FIPS 140-2.

Trova maggiori informazioni

- [Cifrari SSL](#)
- ["Gestisci l'archiviazione con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Cifrari SSL

I cifrari SSL sono algoritmi di crittografia utilizzati dagli host per stabilire una comunicazione sicura. Esistono cifrari standard supportati dal software Element e cifrari non standard quando è abilitata la modalità FIPS 140-2.

Gli elenchi seguenti forniscono i cifrari Secure Socket Layer (SSL) standard supportati dal software Element e i cifrari SSL supportati quando è abilitata la modalità FIPS 140-2:

• FIPS 140-2 disabilitato

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 maggiori informazioni

[Abilita FIPS 140-2 per HTTPS sul tuo cluster](#)

Inizia con la gestione delle chiavi esterne

Inizia con la gestione delle chiavi esterne

La gestione delle chiavi esterne (EKM) garantisce una gestione sicura delle chiavi di

autenticazione (AK) in combinazione con un server di chiavi esterne (EKS) esterno al cluster. Gli AK vengono utilizzati per bloccare e sbloccare le unità auto-crittografanti (SED) quando ["crittografia a riposo"](#) è abilitato sul cluster. L'EKS garantisce la generazione e l'archiviazione sicura degli AK. Il cluster utilizza il protocollo KMIP (Key Management Interoperability Protocol), un protocollo standard definito da OASIS, per comunicare con l'EKS.

- ["Impostare la gestione esterna"](#)
- ["Crittografia software di reimpostazione della chiave principale a riposo"](#)
- ["Recupera le chiavi di autenticazione inaccessibili o non valide"](#)
- ["Comandi API di gestione delle chiavi esterne"](#)

Trova maggiori informazioni

- ["API CreateCluster che può essere utilizzata per abilitare la crittografia del software a riposo"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Impostare la gestione delle chiavi esterne

È possibile seguire questi passaggi e utilizzare i metodi API Element elencati per configurare la funzionalità di gestione delle chiavi esterne.

Cosa ti servirà

- Se si sta configurando la gestione delle chiavi esterne in combinazione con la crittografia software a riposo, è stata abilitata la crittografia software a riposo utilizzando ["Crea cluster"](#) metodo su un nuovo cluster che non contiene volumi.

Passi

1. Stabilire una relazione di fiducia con l'External Key Server (EKS).
 - a. Creare una coppia di chiavi pubblica/privata per il cluster Element che verrà utilizzata per stabilire una relazione di trust con il server delle chiavi chiamando il seguente metodo API: ["Crea coppia di chiavi pubbliche e private"](#)
 - b. Ottieni la richiesta di firma del certificato (CSR) che l'autorità di certificazione deve firmare. Il CSR consente al server delle chiavi di verificare che il cluster Element che accederà alle chiavi sia autenticato come cluster Element. Chiamare il seguente metodo API: ["Ottieni richiesta di firma del certificato del client"](#)
 - c. Utilizzare EKS/Autorità di certificazione per firmare il CSR recuperato. Per ulteriori informazioni, consultare la documentazione di terze parti.
2. Creare un server e un provider sul cluster per comunicare con EKS. Un fornitore di chiavi definisce dove ottenere una chiave, mentre un server definisce gli attributi specifici dell'EKS con cui verrà comunicata.
 - a. Crea un fornitore di chiavi in cui risiederanno i dettagli del server delle chiavi chiamando il seguente metodo API: ["CreateKeyProviderKmip"](#)
 - b. Creare un server di chiavi che fornisca il certificato firmato e il certificato di chiave pubblica dell'Autorità di certificazione chiamando i seguenti metodi API: ["CreateKeyServerKmip"](#) ["TestKeyServerKmip"](#)

Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

- c. Aggiungere il server delle chiavi al contenitore del provider delle chiavi chiamando i seguenti metodi API: ["AggiungiKeyServerAlProviderKmp"](#) ["TestKeyProviderKmp"](#)

Se il test fallisce, verifica la connettività e la configurazione del server. Quindi ripetere il test.

3. Come passaggio successivo per la crittografia a riposo, eseguire una delle seguenti operazioni:

- a. (Per la crittografia hardware a riposo) Abilita ["crittografia hardware a riposo"](#) fornendo l'ID del fornitore di chiavi che contiene il server di chiavi utilizzato per memorizzare le chiavi chiamando il ["Abilita crittografia a riposo"](#) Metodo API.



È necessario abilitare la crittografia a riposo tramite ["API"](#). Abilitando la crittografia a riposo tramite il pulsante Element UI esistente, la funzionalità tornerà a utilizzare chiavi generate internamente.

- b. (Per la crittografia software a riposo) Per ["crittografia software a riposo"](#) per utilizzare il fornitore di chiavi appena creato, passare l'ID del fornitore di chiavi al ["RekeySoftwareEncryptionAtRestMasterKey"](#) Metodo API.

Trova maggiori informazioni

- ["Abilitare e disabilitare la crittografia per un cluster"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Crittografia software di reimpostazione della chiave principale a riposo

È possibile utilizzare l'API Element per rigenerare una chiave esistente. Questo processo crea una nuova chiave master sostitutiva per il server di gestione delle chiavi esterno. Le chiavi principali vengono sempre sostituite da nuove chiavi principali e non vengono mai duplicate o sovrascritte.

Potrebbe essere necessario rinominare la chiave come parte di una delle seguenti procedure:

- Creare una nuova chiave come parte di un passaggio dalla gestione delle chiavi interne alla gestione delle chiavi esterne.
- Crea una nuova chiave come reazione o come protezione contro un evento correlato alla sicurezza.



Questo processo è asincrono e restituisce una risposta prima che l'operazione di reimpostazione delle chiavi sia completata. Puoi usare il ["Ottieni risultato asincrono"](#) metodo per interrogare il sistema per vedere quando il processo è stato completato.

Cosa ti servirà

- Hai abilitato la crittografia software a riposo utilizzando ["Crea cluster"](#) metodo su un nuovo cluster che non contiene volumi e non ha I/O. Utilizzare il collegamento: `../api/reference_element_api_getsoftwareencryptionatrestinfo.html[GetSoftwareEncryptionAtRestInfo]` per confermare che lo stato è `enabled` prima di procedere.
- Hai ["ha stabilito un rapporto di fiducia"](#) tra il cluster SolidFire e un External Key Server (EKS). Esegui il ["TestKeyProviderKmp"](#) metodo per verificare che sia stata stabilita una connessione con il fornitore della chiave.

Passi

1. Esegui il ["ListKeyProvidersKnip"](#) comando e copia l'ID del fornitore della chiave(`keyProviderID`).
2. Esegui il ["RekeySoftwareEncryptionAtRestMasterKey"](#) con il `keyManagementType` parametro come `external` E `keyProviderID` come numero ID del fornitore della chiave dal passaggio precedente:

```
{
  "method": "rekeysoftwareencryptionatrestmasterkey",
  "params": {
    "keyManagementType": "external",
    "keyProviderID": "<ID number>"
  }
}
```

3. Copia il `asyncHandle` valore dal `RekeySoftwareEncryptionAtRestMasterKey` risposta al comando.
4. Esegui il ["Ottieni risultato asincrono"](#) comando con il `asyncHandle` valore del passaggio precedente per confermare la modifica nella configurazione. Dalla risposta al comando dovresti vedere che la vecchia configurazione della chiave principale è stata aggiornata con le nuove informazioni sulla chiave. Copiare l'ID del nuovo fornitore 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. Esegui il `GetSoftwareEncryptionatRestInfo` comando per confermare i nuovi dettagli della 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 maggiori informazioni

- ["Gestisci l'archiviazione con l'API Element"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Recupera le chiavi di autenticazione inaccessibili o non valide

Occasionalmente può verificarsi un errore che richiede l'intervento dell'utente. In caso di errore, verrà generato un errore del cluster (denominato codice di errore del cluster). Qui vengono descritti i due casi più probabili.

Il cluster non è in grado di sbloccare le unità a causa di un errore del cluster `KmipServerFault`.

Ciò 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 i passaggi di ripristino indicati nei codici di errore del cluster (se presenti).

Potrebbe essere impostato un errore `sliceServiceUnhealthy` perché le unità dei metadati sono state contrassegnate come non riuscite e impostate sullo stato "Disponibile".

Passaggi per la cancellazione:

1. Aggiungere nuovamente le unità.
2. Dopo 3 o 4 minuti, verificare che il `sliceServiceUnhealthy` il guasto è stato risolto.

Vedere ["codici di errore del cluster"](#) per maggiori informazioni.

Comandi API di gestione delle chiavi esterne

Elenco di tutte le API disponibili per la gestione e la configurazione di EKM.

Utilizzato per stabilire una relazione di fiducia tra il cluster e i server esterni di proprietà del cliente:

- Crea coppia di chiavi pubbliche e private
- Ottieni richiesta di firma del certificato del client

Utilizzato per definire i dettagli specifici dei server esterni di proprietà del cliente:

- CreateKeyServerKmp
- ModifyKeyServerKmp
- DeleteKeyServerKmp
- GetKeyServerKmp
- ListKeyServersKmp
- TestKeyServerKmp

Utilizzato per creare e gestire i fornitori di chiavi che gestiscono server di chiavi esterni:

- CreateKeyProviderKmp
- DeleteKeyProviderKmp
- AggiungiKeyServerAlProviderKmp
- RemoveKeyServerFromProviderKmp
- GetKeyProviderKmp
- ListKeyProvidersKmp
- RekeySoftwareEncryptionAtRestMasterKey
- TestKeyProviderKmp

Per informazioni sui metodi API, vedere ["Informazioni di riferimento API"](#).

Gestire volumi e volumi virtuali

Scopri di più sulla gestione dei volumi e dei volumi virtuali

È possibile gestire i dati in un cluster che esegue il software Element dalla scheda Gestione nell'interfaccia utente di 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 criteri di qualità del servizio (QoS).

Lavorare con i volumi

Il sistema SolidFire fornisce spazio di archiviazione tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel. Dalla pagina Volumi nella scheda Gestione, è possibile creare, modificare, clonare ed eliminare volumi su un nodo. È anche possibile visualizzare statistiche sulla larghezza di banda del volume e sull'utilizzo di I/O.

Lavorare con volumi virtuali

È possibile visualizzare informazioni ed eseguire attività per volumi virtuali e relativi contenitori di archiviazione, endpoint di protocollo, associazioni e host utilizzando l'interfaccia utente di Element.

Il sistema di archiviazione software NetApp Element viene fornito con la funzionalità Virtual Volumes (VVols) disabilitata. È necessario eseguire un'attività una tantum di abilitazione manuale della funzionalità vSphere VVol tramite l'interfaccia utente di Element.

Dopo aver abilitato la funzionalità VVol, nell'interfaccia utente viene visualizzata la scheda VVols, che offre opzioni di monitoraggio e gestione limitate relative a VVols. Inoltre, un componente software lato storage noto come VASA Provider funge da servizio di storage awareness per vSphere. La maggior parte dei comandi VVol, come la creazione, la clonazione e la modifica di VVol, vengono avviati da un vCenter Server o da un host ESXi e tradotti dal provider VASA nelle API Element per il sistema di archiviazione software Element. I comandi per creare, eliminare e gestire contenitori di archiviazione ed eliminare volumi virtuali possono essere avviati tramite l'interfaccia utente di Element.

La maggior parte delle configurazioni necessarie per utilizzare la funzionalità Virtual Volumes con i sistemi di storage software Element vengono eseguite in vSphere. Consultare la *Guida alla configurazione di VMware vSphere Virtual Volumes for SolidFire Storage* per registrare il provider VASA in vCenter, creare e gestire datastore VVol e gestire l'archiviazione in base ai criteri.



Per Element 12.5 e versioni precedenti, non registrare più di un provider NetApp Element VASA su una singola istanza di vCenter. Se viene aggiunto un secondo provider NetApp Element VASA, tutti i datastore VVOL diventano inaccessibili.



Il supporto VASA per più vCenter è disponibile come patch di aggiornamento se hai già registrato un provider VASA con il tuo vCenter. Per installare, scaricare il file VASA39 .tar.gz dal ["Download del software NetApp"](#) sito e seguire le istruzioni riportate nel manifesto. Il provider NetApp Element VASA 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.

Lavorare con gruppi di accesso al volume e iniziatori

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 dell'iniziatore iSCSI o i WWPN Fibre Channel in una raccolta 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 all'account.
- Autenticazione CHAP a livello di iniziatore: è possibile assegnare segreti e target CHAP univoci per iniziatori specifici senza essere vincolati a un singolo CHAP per un singolo account. Questa autenticazione CHAP a livello di iniziatore sostituisce le credenziali a livello di account.

Facoltativamente, con CHAP per iniziatore, è possibile applicare l'autorizzazione dell'iniziatore e

l'autenticazione CHAP per iniziatore. Queste opzioni possono essere definite per ogni iniziatore e un gruppo di accesso può contenere un mix di iniziatori con opzioni diverse.

Ogni WWPN aggiunto a un gruppo di accesso abilita l'accesso alla rete Fibre Channel ai volumi nel gruppo di accesso.



I gruppi di accesso al volume hanno i seguenti limiti:

- In un gruppo di accesso sono consentiti al massimo 64 IQN o WWPN.
- Un gruppo di accesso può essere composto 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.

["Scopri come lavorare con i gruppi di accesso al volume e gli iniziatori"](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Lavorare con i volumi

Gestire le politiche di qualità del servizio

Un criterio 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 Criteri QoS nella scheda Gestione.



Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.

["Video NetApp : Criteri di qualità del servizio SolidFire"](#)

Vedere ["Prestazioni e qualità del servizio"](#) .

- Creare una policy QoS
- Modifica una policy QoS
- Eliminare una policy QoS

Creare una policy QoS

È possibile creare criteri QoS e applicarli durante la creazione dei volumi.

1. Selezionare **Gestione > Criteri QoS**.
2. Fare clic su **Crea criterio QoS**.
3. Inserisci il **Nome della polizza**.

4. Immettere i valori **MIN IOPS**, **MAX IOPS** e **Burst IOPS**.
5. Fare clic su **Crea criterio QoS**.

Modifica una policy QoS

È possibile modificare il nome di un criterio QoS esistente o modificare i valori associati al criterio. La modifica di una policy QoS influisce su tutti i volumi associati alla policy.

1. Selezionare **Gestione > Criteri QoS**.
2. Fare clic sull'icona Azioni per il criterio QoS che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica criterio QoS**, modificare le seguenti proprietà come richiesto:
 - Nome della polizza
 - IOPS minimi
 - IOPS massimi
 - IOPS a raffica
5. Fare clic su **Salva modifiche**.

Eliminare una policy QoS

È possibile eliminare un criterio QoS se non è più necessario. Quando si elimina un criterio QoS, tutti i volumi associati al criterio mantengono le impostazioni QoS ma non vengono più associati al criterio.



Se invece si sta tentando di dissociare un volume da una policy QoS, è possibile modificare le impostazioni QoS per quel volume in personalizzate.

1. Selezionare **Gestione > Criteri QoS**.
2. Fare clic sull'icona Azioni per il criterio QoS che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.

Trova maggiori informazioni

- ["Rimuovere l'associazione della policy QoS di un volume"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Gestire i volumi

Il sistema SolidFire fornisce spazio di archiviazione tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel.

Dalla pagina Volumi nella scheda Gestione, è possibile creare, modificare, clonare ed eliminare volumi su un nodo.

Crea 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 **Gestione > Volumi**.
2. Fare clic su **Crea volume**.
3. Nella finestra di dialogo **Crea un nuovo volume**, immettere il **Nome del volume**.
4. Inserisci la dimensione totale 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

5. Selezionare una **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 **Crea account**, immettere un nuovo nome account e fare clic su **Crea**. L'account viene creato e associato al nuovo volume.



Se ci sono più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico ti mostrerà i possibili valori tra cui scegliere.

7. Per impostare la **Qualità del servizio**, procedere in uno dei seguenti modi:
 - a. In **Criterio** è possibile selezionare un criterio QoS esistente, se disponibile.
 - b. In **Impostazioni personalizzate**, imposta i valori minimi, massimi e burst personalizzati per IOPS oppure utilizza i valori QoS predefiniti.

I volumi con un valore Max o Burst IOPS superiore a 20.000 IOPS potrebbero richiedere un'elevata profondità di coda o più sessioni per raggiungere questo livello di IOPS su un singolo volume.

8. Fare clic su **Crea volume**.

Visualizza i dettagli del volume

1. Selezionare **Gestione > Volumi**.
2. Esamina i dettagli.
 - **ID**: ID generato dal sistema per il volume.
 - **Nome**: il nome assegnato al volume al momento della sua creazione.
 - **Account**: 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.
 - **Accesso**: tipo di accesso assegnato al volume al momento della sua creazione. Valori possibili:
 - Lettura/Scrittura: sono accettate tutte le letture e le scritture.

- Sola lettura: sono consentite tutte le attività di lettura; non sono consentite le attività di scrittura.
- Bloccato: è consentito solo l'accesso dell'amministratore.
- ReplicationTarget: designato come volume di destinazione in una coppia di volumi replicati.
- **Utilizzato**: percentuale di spazio utilizzato nel volume.
- **Dimensione**: la dimensione totale (in GB) del volume.
- **ID nodo primario**: il nodo primario per questo volume.
- **ID nodo secondario**: elenco dei nodi secondari per questo volume. Possono assumere più valori durante gli stati transitori, come il cambio dei nodi secondari, ma solitamente avranno un singolo valore.
- **QoS Throttle**: identifica se il volume è stato limitato a causa dell'elevato carico sul nodo di archiviazione primario.
- **Criterio QoS**: nome e collegamento al criterio QoS definito dall'utente.
- **MIN IOPS**: numero minimo di IOPS garantiti per il volume.
- **IOPS massimi**: numero massimo di IOPS consentiti per il volume.
- **Burst IOPS**: il numero massimo di IOPS consentiti in un breve periodo di tempo per il volume. Predefinito = 15.000.
- **Snapshot**: numero di snapshot creati per il volume.
- **Attributi**: attributi assegnati al volume come coppia chiave/valore tramite un metodo API.
- **512e**: Indica se 512e è abilitato su un volume. Valori possibili:
 - SÌ
 - NO
- **Creato il**: data e ora in cui è stato creato il volume.

Visualizza i dettagli dei singoli volumi

È possibile visualizzare le statistiche sulle prestazioni per singoli volumi.

1. Selezionare **Reporting > Prestazioni volume**.
2. Nell'elenco dei volumi, fare clic sull'icona Azioni per un volume.
3. Fare clic su **Visualizza dettagli**.

Nella parte inferiore della pagina viene visualizzata una barra contenente informazioni generali sul volume.

4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi altri dettagli**.

Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Modifica volumi attivi

È possibile modificare gli attributi del volume, quali i valori QoS, le dimensioni del volume e l'unità di misura in cui vengono calcolati i valori dei byte. È anche possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

È possibile ridimensionare un volume quando c'è spazio sufficiente sul cluster nelle seguenti condizioni:

- Condizioni operative normali.
- Vengono segnalati errori o guasti del volume.
- Il volume è in fase di clonazione.
- Il volume è in fase di risincronizzazione.

Passi

1. Selezionare **Gestione > Volumi**.
2. Nella finestra **Attiva**, fare clic sull'icona Azioni per il volume che si desidera modificare.
3. Fare clic su **Modifica**.
4. **Facoltativo**: modifica la dimensione totale del volume.
 - È possibile aumentare, ma non diminuire, la dimensione del volume. È possibile ridimensionare un solo volume in un'unica operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.
 - Se si desidera modificare le dimensioni del volume per la replica, è necessario innanzitutto aumentare le dimensioni del volume assegnato come destinazione della replica. Quindi puoi ridimensionare il volume sorgente. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

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

5. **Facoltativo**: seleziona un livello di accesso all'account diverso tra i seguenti:
 - Solo lettura
 - Lettura/scrittura
 - Bloccato
 - Obiettivo di replicazione
6. **Facoltativo**: seleziona l'account che deve avere accesso al volume.

Se l'account non esiste, fare clic sul collegamento **Crea account**, immettere un nuovo nome account e fare clic su **Crea**. L'account viene creato e associato al volume.



Se ci sono più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico ti mostrerà i possibili valori tra cui scegliere.

7. **Facoltativo**: per modificare la selezione in **Qualità del servizio**, procedere in uno dei seguenti modi:
 - a. In **Criterio** è possibile selezionare un criterio QoS esistente, se disponibile.
 - b. In **Impostazioni personalizzate**, imposta i valori minimi, massimi e burst personalizzati per IOPS oppure utilizza i valori QoS predefiniti.



Se si utilizzano criteri QoS su un volume, è possibile impostare un QoS personalizzato per rimuovere l'affiliazione del criterio QoS al volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.



Quando si modificano i valori IOPS, è necessario incrementarli 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 di grandi blocchi, limitando comunque gli IOPS sostenuti per un volume.

8. Fare clic su **Salva modifiche**.

Elimina un volume

È possibile eliminare uno o più volumi da un cluster di archiviazione Element.

Il sistema non elimina immediatamente un volume eliminato; il volume rimane disponibile per circa otto ore. Se si ripristina un volume prima che il sistema lo elimini, il volume torna online e le connessioni iSCSI vengono ripristinate.

Se un volume utilizzato per creare uno snapshot viene eliminato, gli snapshot associati diventano inattivi. Quando i volumi di origine eliminati vengono eliminati, anche gli snapshot inattivi associati vengono rimossi 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.

Passi

1. Selezionare **Gestione > Volumi**.
2. Per eliminare un singolo volume, procedere come segue:
 - a. Fare clic sull'icona Azioni relativa al volume che si desidera eliminare.
 - b. Nel menu che si apre, fare clic su **Elimina**.
 - c. Conferma l'azione.

Il sistema sposta il volume nell'area **Eliminati** nella pagina **Volumi**.

3. Per eliminare più volumi, procedere come segue:
 - a. Nell'elenco dei volumi, seleziona la casella accanto ai volumi che desideri eliminare.
 - b. Fare clic su **Azioni in blocco**.
 - c. Nel menu che si apre, fare clic su **Elimina**.
 - d. Conferma l'azione.

Il sistema sposta i volumi nell'area **Eliminati** nella pagina **Volumi**.

Ripristina un volume eliminato

È possibile ripristinare un volume nel sistema se è stato eliminato ma non ancora ripulito. Il sistema elimina automaticamente un volume circa otto ore dopo la sua eliminazione. Se il sistema ha eliminato il volume, non è possibile ripristinarlo.

1. Selezionare **Gestione > Volumi**.

2. Fare clic sulla scheda **Eliminati** per visualizzare l'elenco dei volumi eliminati.
3. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
4. Nel menu che si apre, fare clic su **Ripristina**.
5. Conferma l'azione.

Il volume viene inserito nell'elenco dei volumi **Attivi** e le connessioni iSCSI al volume vengono ripristinate.

Svuota un volume

Quando un volume viene eliminato, viene rimosso definitivamente dal sistema. Tutti i dati nel volume andranno persi.

Il sistema elimina automaticamente i volumi eliminati otto ore dopo l'eliminazione. Tuttavia, se si desidera eliminare un volume prima dell'orario programmato, è possibile farlo.

1. Selezionare **Gestione > Volumi**.
2. Fare clic sul pulsante **Eliminato**.
3. Eseguire i passaggi per eliminare un singolo volume o più volumi.

Opzione	Passi
Svuotare un singolo volume	a. Fare clic sull'icona Azioni relativa al volume che si desidera eliminare. b. Fare clic su Elimina. c. Conferma l'azione.
Svuota più volumi	a. Selezionare i volumi che si desidera eliminare. b. Fare clic su Azioni in blocco. c. Nel menu che si apre, seleziona Elimina. d. Conferma l'azione.

Clonare un volume

È possibile creare un clone di un singolo volume o di più volumi per realizzare una copia dei dati in un dato momento. Quando si clona un volume, il sistema crea uno snapshot del volume e quindi crea una copia dei dati a cui fa riferimento lo snapshot. Si tratta di un processo asincrono e la quantità di tempo richiesta dipende dalle dimensioni del volume che si sta clonando e dal carico attuale del cluster.

Il cluster supporta fino a due richieste di clonazione in esecuzione per volume alla volta e fino a otto operazioni di clonazione di volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per essere elaborate in un secondo momento.



I sistemi operativi differiscono nel modo in cui gestiscono i volumi clonati. VMware ESXi tratterà un volume clonato come una copia del volume o un volume snapshot. Il volume sarà un dispositivo disponibile da utilizzare per creare un nuovo datastore. Per ulteriori informazioni sul montaggio di volumi clone e sulla gestione di LUN snapshot, consultare la documentazione VMware su ["montaggio di una copia del datastore VMFS"](#) e ["gestione di datastore VMFS duplicati"](#).



Prima di troncare un volume clonato clonandolo in una dimensione più piccola, assicurarsi di preparare le partizioni in modo che si adattino al volume più piccolo.

Passi

1. Selezionare **Gestione > Volumi**.
2. Per clonare un singolo volume, procedere come segue:
 - a. Nell'elenco dei volumi nella pagina **Attivi**, fare clic sull'icona Azioni per il volume che si desidera clonare.
 - b. Nel menu che si apre, fare clic su **Clona**.
 - c. Nella finestra **Clona volume**, immettere un nome per il volume appena clonato.
 - d. Selezionare una dimensione e una misura per il volume utilizzando la casella di selezione e l'elenco **Dimensione 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

- e. Selezionare il tipo di accesso per il volume appena clonato.
- f. Selezionare un account da associare al volume appena clonato dall'elenco **Account**.



Puoi creare un account durante questa fase cliccando sul link **Crea account**, inserendo un nome account e cliccando su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'account all'elenco **Account**.

3. Per clonare più volumi, procedere come segue:
 - a. Nell'elenco dei volumi nella pagina **Attivi**, seleziona la casella accanto ai volumi che desideri clonare.
 - b. Fare clic su **Azioni in blocco**.
 - c. Nel menu che si apre, seleziona **Clona**.
 - d. Nella finestra di dialogo **Clona più volumi**, immettere un prefisso per i volumi clonati nel campo **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**.



Aumentando la dimensione del volume di un clone si ottiene un nuovo volume con spazio libero aggiuntivo alla fine del volume. A seconda di come si utilizza il volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per sfruttarlo.

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Assegnare LUN ai volumi Fibre Channel

È possibile modificare l'assegnazione LUN per un volume Fibre Channel in un gruppo di accesso al volume. È anche possibile effettuare assegnazioni LUN del volume Fibre Channel quando si crea un gruppo di accesso al volume.

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 rilevarlo.

1. Selezionare **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. In **Assegna ID LUN** nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Assegnazioni LUN**.
5. Per ogni volume nell'elenco a cui si desidera assegnare un LUN, immettere un nuovo valore nel campo **LUN** corrispondente.
6. Fare clic su **Salva modifiche**.

Applicare una policy QoS ai volumi

È possibile applicare in blocco una policy QoS esistente a uno o più volumi.

Deve esistere la policy QoS che si desidera applicare in blocco.

1. Selezionare **Gestione > Volumi**.
2. Nell'elenco dei volumi, seleziona la casella accanto ai volumi a cui desideri applicare la policy QoS.
3. Fare clic su **Azioni in blocco**.
4. Nel menu visualizzato, fare clic su **Applica criterio QoS**.
5. Selezionare il criterio QoS dall'elenco a discesa.
6. Fare clic su **Applica**.

Trova maggiori informazioni

[Politiche di qualità del servizio](#)

Rimuovere l'associazione della policy QoS di un volume

È possibile rimuovere un'associazione di criteri QoS da un volume selezionando le impostazioni QoS personalizzate.

Il volume che si desidera modificare deve essere associato a una policy QoS.

1. Selezionare **Gestione > Volumi**.
2. Fare clic sull'icona Azioni per un volume che contiene un criterio QoS che si desidera modificare.
3. Fare clic su **Modifica**.
4. Nel menu visualizzato in **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 **Salva modifiche**.

Trova maggiori informazioni

[Eliminare una policy QoS](#)

Lavorare con volumi virtuali

Abilita volumi virtuali

È necessario abilitare manualmente la funzionalità vSphere Virtual Volumes (VVols) tramite il software NetApp Element . Il sistema software Element è dotato di funzionalità VVols disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento. L'abilitazione della funzionalità VVols è un'attività di configurazione che deve essere eseguita una sola volta.

Cosa ti servirà

- 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 VVols.
- Se si utilizza Element 11.3 o versione successiva, il cluster deve essere connesso a un ambiente ESXi 6.0 aggiornamento 3 o versione successiva.



L'abilitazione della funzionalità vSphere Virtual Volumes modifica in modo permanente la configurazione del software Element. È opportuno abilitare la funzionalità VVols solo se il cluster è connesso a un ambiente compatibile con VMware ESXi VVols. È possibile disattivare la funzionalità VVols e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica, eliminando così tutti i dati presenti sul sistema.

Passi

1. Selezionare **Cluster > Impostazioni**.
2. Trova le impostazioni specifiche del cluster per i volumi virtuali.
3. Fare clic su **Abilita volumi virtuali**.
4. Fare clic su **Sì** per confermare la modifica alla configurazione dei volumi virtuali.

La scheda **VVols** viene visualizzata nell'interfaccia utente di Element.



Quando la funzionalità VVols è abilitata, 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 **Cluster > Impostazioni**. Utilizzerai questo URL per registrare il provider VASA in vCenter.
6. Creare un contenitore di archiviazione in **VVols > Contenitori di archiviazione**.



È necessario creare almeno un contenitore di archiviazione affinché le VM possano essere fornite a un datastore VVol.

7. Selezionare **VVols > Endpoint protocollo**.

8. Verificare che sia stato creato un endpoint del protocollo per ciascun nodo del cluster.



In vSphere sono necessarie ulteriori attività di configurazione. Consultare la *Guida alla configurazione di VMware vSphere Virtual Volumes for SolidFire Storage* per registrare il provider VASA in vCenter, creare e gestire datastore VVol e gestire l'archiviazione in base ai criteri.

Trova maggiori informazioni

["Guida alla configurazione di VMware vSphere Virtual Volumes per SolidFire Storage"](#)

Visualizza i dettagli del volume virtuale

È possibile esaminare 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 prestazioni per ciascun volume virtuale, inclusi input, output, throughput, latenza, profondità della coda e informazioni sul volume.

Cosa ti servirà

- Dovresti aver abilitato la funzionalità VVols nell'interfaccia utente Element per il cluster.
- Dovresti aver creato un contenitore di archiviazione associato.
- Dovresti aver configurato il tuo cluster vSphere per utilizzare la funzionalità VVols del software Element.
- Dovresti aver creato almeno una VM in vSphere.

Passi

1. Fare clic su **VVols > Volumi virtuali**.

Vengono visualizzate le informazioni per tutti i volumi virtuali attivi.

2. Fare clic sull'icona **Azioni** per il volume virtuale che si desidera esaminare.
3. Nel menu visualizzato, seleziona **Visualizza dettagli**.

Dettagli

La pagina Volumi virtuali della scheda VVols fornisce informazioni su ciascun volume virtuale attivo nel cluster, ad esempio ID volume, ID snapshot, ID volume virtuale padre e ID volume virtuale.

- **ID volume:** ID del volume sottostante.
- **ID snapshot:** ID dello snapshot del volume sottostante. Il valore è 0 se il volume virtuale non rappresenta uno snapshot SolidFire .
- **ID volume virtuale padre:** ID del volume virtuale padre. Se l'ID è composto da soli zeri, il volume virtuale è indipendente e non ha alcun collegamento con un elemento padre.
- **ID volume virtuale:** UUID del volume virtuale.
- **Nome:** il nome assegnato al volume virtuale.
- **Contenitore di archiviazione:** il contenitore di archiviazione che possiede il volume virtuale.
- **Tipo di sistema operativo guest:** sistema operativo associato al volume virtuale.

- **Tipo di volume virtuale:** il tipo di volume virtuale: Configurazione, Dati, Memoria, Swap o Altro.
- **Accesso:** autorizzazioni di lettura-scrittura assegnate al volume virtuale.
- **Dimensione:** la dimensione del volume virtuale in GB o GiB.
- **Snapshot:** numero di snapshot associati. Fare clic sul numero per collegarsi ai dettagli dello snapshot.
- **IOPS minimi:** impostazione QoS IOPS minima del volume virtuale.
- **IOPS massimi:** impostazione QoS IOPS massima del volume virtuale.
- **Burst IOPS:** impostazione QoS burst massima del volume virtuale.
- **VMW_VmID:** le informazioni nei campi preceduti da "VMW_" sono definite da VMware.
- **Ora di creazione:** ora in cui è stata completata l'attività di creazione del volume virtuale.

Dettagli individuali del volume virtuale

La pagina Volumi virtuali nella scheda VVols fornisce le seguenti informazioni sui volumi virtuali quando si seleziona un singolo volume virtuale e ne si visualizzano i dettagli.

- **VMW_XXX:** Le informazioni nei campi preceduti da "VMW_" sono definite da VMware.
- **ID volume virtuale padre:** ID del volume virtuale padre. Se l'ID è composto da soli zeri, il volume virtuale è indipendente e non ha alcun collegamento con un elemento padre.
- **ID volume virtuale:** UUID del volume virtuale.
- **Tipo di volume virtuale:** il tipo di volume virtuale: Configurazione, Dati, Memoria, Swap o Altro.
- **ID volume:** ID del volume sottostante.
- **Accesso:** 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.
- **Dimensione totale del volume:** 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 Blocchi:** numero totale di blocchi da 4 KiB senza dati dopo il completamento dell'ultimo ciclo di operazioni di garbage collection.
- **Snapshot:** numero di snapshot associati. Fare clic sul numero per collegarsi ai dettagli dello snapshot.
- **IOPS minimi:** impostazione QoS IOPS minima del volume virtuale.
- **IOPS massimi:** impostazione QoS IOPS massima del volume virtuale.
- **Burst IOPS:** impostazione QoS burst massima del volume virtuale.
- **Abilita 512:** poiché i volumi virtuali utilizzano sempre l'emulazione della dimensione del blocco da 512 byte, il valore è sempre sì.
- **Volumi accoppiati:** indica se un volume è accoppiato.
- **Ora di creazione:** ora in cui è stata completata l'attività di creazione del volume virtuale.
- **Dimensione blocchi:** dimensione dei blocchi sul volume.
- **Scritture non allineate:** per i volumi 512e, il numero di operazioni di scrittura che non si sono svolte su un limite di settore di 4k. Un numero elevato di scritture non allineate potrebbe indicare un allineamento non corretto 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 non corretto 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 nel formato NAA IEEE Registered Extended.
- **Attributi:** Elenco di coppie nome-valore nel formato oggetto JSON.

Elimina un volume virtuale

Sebbene i volumi virtuali debbano sempre essere eliminati dal VMware Management Layer, la funzionalità per eliminare i volumi virtuali è abilitata dall'interfaccia utente di Element. È opportuno eliminare un volume virtuale dall'interfaccia utente di Element solo quando assolutamente necessario, ad esempio quando vSphere non riesce a pulire i volumi virtuali sullo storage SolidFire .

1. Selezionare **VVols > Volumi virtuali**.
2. Fare clic sull'icona Azioni relativa al volume virtuale che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.



È necessario eliminare un volume virtuale dal VMware Management Layer per garantire che il volume virtuale sia correttamente scollegato prima dell'eliminazione. È opportuno eliminare un volume virtuale dall'interfaccia utente di Element solo quando 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 verrà eliminato immediatamente.

4. Conferma l'azione.
5. Aggiornare l'elenco dei volumi virtuali per confermare che il volume virtuale è stato rimosso.
6. **Facoltativo:** selezionare **Segnalazione > Registro eventi** per confermare che la cancellazione è avvenuta correttamente.

Gestire i contenitori di stoccaggio

Un contenitore di archiviazione è una rappresentazione del datastore vSphere creata su un cluster che esegue il software Element.

I contenitori di archiviazione vengono creati e associati agli account NetApp Element . Un contenitore di archiviazione creato su Element Storage viene visualizzato come un datastore vSphere in vCenter ed ESXi. I contenitori di archiviazione non allocano alcuno spazio nell'archiviazione Element. Vengono semplicemente utilizzati per associare logicamente volumi virtuali.

Sono supportati al massimo quattro contenitori di archiviazione per cluster. Per abilitare la funzionalità VVols è necessario almeno un contenitore di archiviazione.

Creare un contenitore di archiviazione

È possibile creare contenitori di archiviazione nell'interfaccia utente di Element e individuarli in vCenter. È

necessario creare almeno un contenitore di archiviazione per iniziare il provisioning delle macchine virtuali supportate da VVol.

Prima di iniziare, abilitare la funzionalità VVols nell'interfaccia utente di Element per il cluster.

Passi

1. Selezionare **VVols > Contenitori di archiviazione**.
2. Fare clic sul pulsante **Crea contenitori di archiviazione**.
3. Immettere le informazioni sul contenitore di archiviazione nella finestra di dialogo **Crea un nuovo contenitore di archiviazione**:
 - a. Immettere un nome per il contenitore di archiviazione.
 - b. Configurare i segreti dell'iniziatore e della destinazione per CHAP.
4. Verificare che il nuovo contenitore di archiviazione appaia nell'elenco nella sotto-scheda **Contenitori di archiviazione**.



Lasciare vuoti i campi Impostazioni CHAP per generare automaticamente i segreti.



Poiché un ID account NetApp Element viene creato automaticamente e assegnato al contenitore di archiviazione, non è necessario creare manualmente un account.

Visualizza i dettagli del contenitore di stoccaggio

Nella pagina Contenitori di archiviazione della scheda VVols, è possibile visualizzare le informazioni relative a tutti i contenitori di archiviazione attivi nel cluster.

- **ID account:** ID dell'account NetApp Element associato al contenitore di archiviazione.
- **Nome:** Nome del contenitore di archiviazione.
- **Stato:** Stato del contenitore di archiviazione. Valori possibili:
 - Attivo: il contenitore di stoccaggio è in uso.
 - Bloccato: il contenitore di stoccaggio è bloccato.
- **Tipo PE:** tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile per il software Element).
- **ID contenitore di archiviazione:** UUID del contenitore di archiviazione del volume virtuale.
- **Volumi virtuali attivi:** numero di volumi virtuali attivi associati al contenitore di archiviazione.

Visualizza i dettagli dei singoli contenitori di stoccaggio

È possibile visualizzare le informazioni relative a un singolo contenitore di archiviazione selezionandolo dalla pagina Contenitori di archiviazione nella scheda VVols.

- **ID account:** ID dell'account NetApp Element associato al contenitore di archiviazione.
- **Nome:** Nome del contenitore di archiviazione.
- **Stato:** Stato del contenitore di archiviazione. Valori possibili:
 - Attivo: il contenitore di stoccaggio è in uso.
 - Bloccato: il contenitore di stoccaggio è bloccato.

- **Segreto dell'iniziatore CHAP:** Il segreto CHAP esclusivo dell'iniziatore.
- **Segreto del bersaglio CHAP:** Il segreto CHAP univoco per il bersaglio.
- **ID contenitore di archiviazione:** UUID del contenitore di archiviazione del volume virtuale.
- **Tipo di endpoint del protocollo:** indica il tipo di endpoint del protocollo (SCSI è l'unico protocollo disponibile).

Modifica un contenitore di archiviazione

È possibile modificare l'autenticazione CHAP del contenitore di archiviazione nell'interfaccia utente dell'elemento.

1. Selezionare **VVols > Contenitori di archiviazione**.
2. Fare clic sull'icona **Azioni** relativa al contenitore di archiviazione che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. In Impostazioni CHAP, modifica le credenziali Segreto iniziatore e Segreto destinazione utilizzate per l'autenticazione.



Se non modifichi le credenziali delle impostazioni CHAP, queste rimarranno invariate. Se si lasciano vuoti i campi delle credenziali, il sistema genera automaticamente nuovi segreti.

5. Fare clic su **Salva modifiche**.

Elimina un contenitore di archiviazione

È possibile eliminare i contenitori di archiviazione dall'interfaccia utente dell'elemento.

Cosa ti servirà

Assicurarsi che tutte le macchine virtuali siano state rimosse dal datastore VVol.

Passi

1. Selezionare **VVols > Contenitori di archiviazione**.
2. Fare clic sull'icona **Azioni** relativa al contenitore di archiviazione che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.
4. Conferma l'azione.
5. Aggiornare l'elenco dei contenitori di archiviazione nella sotto-scheda **Contenitori di archiviazione** per confermare che il contenitore di archiviazione è stato rimosso.

Endpoint del protocollo

Scopri di più sugli endpoint del protocollo

Gli endpoint del protocollo sono punti di accesso utilizzati da un host per indirizzare lo storage su un cluster che esegue il software NetApp Element . Gli endpoint del protocollo non possono essere eliminati 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 che esegue il software Element crea automaticamente un endpoint di protocollo per ogni nodo di archiviazione nel cluster. Ad esempio, un cluster di storage a sei nodi ha sei endpoint di protocollo mappati su

ciascun host ESXi. Gli endpoint del protocollo vengono gestiti dinamicamente dal software Element e vengono creati, spostati o rimossi in base alle necessità, senza alcun intervento. Gli endpoint del protocollo sono l'obiettivo del multi-pathing e fungono da proxy I/O per le LUN sussidiarie. Ogni endpoint del protocollo utilizza un indirizzo SCSI disponibile, proprio come una destinazione iSCSI standard. Gli endpoint del protocollo vengono visualizzati come un dispositivo di archiviazione a blocco singolo (512 byte) nel client vSphere, ma questo dispositivo di archiviazione non è disponibile per essere formattato o utilizzato come archiviazione.

iSCSI è l'unico protocollo supportato. Il protocollo Fibre Channel non è supportato.

Dettagli degli endpoint del protocollo

La pagina Endpoint del protocollo nella scheda VVols fornisce informazioni sugli endpoint del protocollo.

- **ID fornitore principale**

ID del fornitore dell'endpoint del protocollo primario.

- **ID fornitore secondario**

ID del provider dell'endpoint del protocollo secondario.

- **ID endpoint protocollo**

L'UUID dell'endpoint del protocollo.

- **Stato dell'endpoint del protocollo**

Lo stato dell'endpoint del protocollo. I valori possibili sono i seguenti:

- Attivo: l'endpoint del protocollo è in uso.
- Inizio: l'endpoint del protocollo è in fase di avvio.
- Failover: l'endpoint del protocollo ha subito un failover.
- Riservato: l'endpoint del protocollo è riservato.

- **Tipo di fornitore**

Il tipo di provider dell'endpoint del protocollo. I valori possibili sono i seguenti:

- Primario
- Secondario

- **ID dispositivo SCSI NAA**

Identificatore univoco globale del dispositivo SCSI per l'endpoint del protocollo nel formato NAA IEEE Registered Extended.

Rilegature

Scopri di più sulle 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 di protocollo ottimale, crea un binding che associa l'host ESXi e il volume virtuale all'endpoint di protocollo e restituisce il binding all'host ESXi. Dopo l'associazione, l'host ESXi può eseguire operazioni di I/O con il volume virtuale associato.

Dettagli degli attacchi

La pagina Associazioni nella scheda VVols fornisce informazioni di associazione su ciascun volume virtuale.

Vengono visualizzate le seguenti informazioni:

- **ID host**

L'UUID dell'host ESXi che ospita i volumi virtuali ed è noto al cluster.

- **ID endpoint protocollo**

ID endpoint del protocollo che corrispondono a ciascun nodo nel cluster SolidFire .

- **Endpoint del protocollo nell'ID banda**

ID del dispositivo SCSI NAA dell'endpoint del protocollo.

- **Tipo di endpoint del protocollo**

Il tipo di endpoint del protocollo.

- **ID associazione VVol**

L'UUID di associazione del volume virtuale.

- **ID VVol**

Identificatore univoco universale (UUID) del volume virtuale.

- **ID secondario VVol**

ID secondario del volume virtuale che è un ID LUN SCSI di secondo livello.

Dettagli dell'host

La pagina Host nella scheda VVols fornisce informazioni sugli host VMware ESXi che ospitano volumi virtuali.

Vengono visualizzate le seguenti informazioni:

- **ID host**

L'UUID dell'host ESXi che ospita i volumi virtuali ed è noto al cluster.

- **Indirizzo host**

L'indirizzo IP o il nome DNS dell'host ESXi.

- **Legami**

ID di associazione per tutti i volumi virtuali associati dall'host ESXi.

- **ID cluster ESX**

ID del cluster host vSphere o GUID di vCenter.

- **Iniziatori IQN**

IQN dell'iniziatore per l'host del volume virtuale.

- * ID endpoint del protocollo SolidFire *

Gli endpoint del protocollo attualmente visibili all'host ESXi.

Lavorare con gruppi di accesso al volume e iniziatori

Creare un gruppo di accesso al volume

È possibile creare gruppi di accesso al volume mappando gli iniziatori a una raccolta di volumi per un accesso protetto. È quindi possibile concedere l'accesso ai volumi nel gruppo con un segreto di avvio CHAP dell'account e un segreto di destinazione.

Se si utilizza CHAP basato sull'iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso al volume, garantendo maggiore sicurezza. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

Passi

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic su **Crea gruppo di accesso**.
3. Immettere 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. In Aggiungi iniziatori, seleziona un iniziatore Fibre Channel esistente dall'elenco Iniziatori Fibre Channel non associati. b. Fare clic su Aggiungi iniziatore FC.  È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento Crea iniziatore, inserendo un nome per l'iniziatore e facendo clic su Crea. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco Iniziatori. Un esempio del formato è il seguente: <pre>5f:47:ac:c0:5c:74:d4:02</pre>
Aggiunta di un iniziatore iSCSI	In Aggiungi iniziatori, seleziona un iniziatore esistente dall'elenco Iniziatori. Nota: puoi creare un iniziatore durante questo passaggio cliccando sul link Crea iniziatore, immettendo un nome per l'iniziatore e cliccando su Crea. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco Iniziatori. Un esempio del formato è il seguente: <pre>iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b</pre>  È possibile trovare l'IQN dell'iniziatore per ciascun volume selezionando Visualizza dettagli nel menu Azioni per il volume nell'elenco Gestione > Volumi > Attivi. Quando si modifica un iniziatore, è possibile impostare l'attributo requiredCHAP su True, consentendo di impostare il segreto dell'iniziatore di destinazione. Per maggiori dettagli, vedere le informazioni API sul metodo API ModifyInitiator. "Gestisci l'archiviazione con l'API Element"

5. **Facoltativo:** aggiungere altri iniziatori secondo necessità.

6. In Aggiungi volumi, seleziona un volume dall'elenco **Volumi**.

Il volume viene visualizzato nell'elenco **Volumi allegati**.

7. **Facoltativo:** aggiungere altri volumi secondo necessità.

8. Fare clic su **Crea gruppo di accesso**.

Trova maggiori informazioni

[Aggiungere volumi a un gruppo di accesso](#)

Visualizza i dettagli del gruppo di accesso individuale

È possibile visualizzare i dettagli di un singolo gruppo di accesso, ad esempio volumi e iniziatori collegati, in formato grafico.

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona Azioni per un gruppo di accesso.
3. Fare clic su **Visualizza dettagli**.

Dettagli del gruppo di accesso al volume

La pagina Gruppi di accesso nella scheda Gestione fornisce informazioni sui gruppi di accesso al volume.

Vengono visualizzate le seguenti informazioni:

- **ID**: ID generato dal sistema per il gruppo di accesso.
- **Nome**: il nome assegnato al gruppo di accesso al momento della sua creazione.
- **Volumi attivi**: numero di volumi attivi nel gruppo di accesso.
- **Compressione**: punteggio di efficienza della compressione per il gruppo di accesso.
- **Deduplicazione**: punteggio di efficienza della deduplicazione per il gruppo di accesso.
- **Thin Provisioning**: punteggio di efficienza del thin provisioning per il gruppo di accesso.
- **Efficienza complessiva**: punteggio di efficienza complessiva per il gruppo di accesso.
- **Iniziatori**: numero di iniziatori connessi al gruppo di accesso.

Aggiungere volumi a un gruppo di accesso

È possibile aggiungere volumi a un gruppo di accesso ai volumi. Ogni volume può appartenere a più di un gruppo di accesso al volume; è possibile visualizzare i gruppi a cui appartiene ogni volume nella pagina Volumi **Attivi**.

È possibile utilizzare questa procedura anche per aggiungere volumi a un gruppo di accesso al volume Fibre Channel.

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso a cui si desidera aggiungere volumi.
3. Fare clic sul pulsante **Modifica**.
4. In Aggiungi volumi, seleziona un volume dall'elenco **Volumi**.

È possibile aggiungere altri volumi ripetendo questo passaggio.

5. Fare clic su **Salva modifiche**.

Rimuovere volumi da un gruppo di accesso

Quando si rimuove un volume da un gruppo di accesso, il gruppo non ha più accesso a quel 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 imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettersi sempre dalle sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali modifiche alle impostazioni dell'iniziatore e del cluster.

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona Azioni per il gruppo di accesso da cui si desidera rimuovere i volumi.
3. Fare clic su **Modifica**.
4. In Aggiungi volumi nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Volumi collegati**.
5. Selezionare il volume che si desidera rimuovere dall'elenco e fare clic sull'icona **x** per rimuovere il volume dall'elenco.

È possibile rimuovere altri volumi ripetendo questo passaggio.

6. Fare clic su **Salva modifiche**.

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnare loro degli alias.

È anche possibile assegnare attributi CHAP basati sull'iniziatore utilizzando una chiamata API. Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare `CreateInitiator` Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP. L'accesso dell'iniziatore 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 maggiori dettagli, consultare le informazioni di riferimento dell'API. "[Gestisci l'archiviazione con l'API Element](#)"

Passi

1. Fare clic su **Gestione > Iniziatori**.
2. Fare clic su **Crea iniziatore**.
3. Eseguire i passaggi per creare un singolo iniziatore o più iniziatori:

Opzione	Passi
Creare un singolo iniziatore	a. Fare clic su Crea un singolo iniziatore. b. Inserire l'IQN o il WWPN dell'iniziatore nel campo IQN/WWPN. c. Inserisci un nome descrittivo per l'iniziatore nel campo Alias. d. Fare clic su Crea iniziatore.

Opzione	Passi
Crea più iniziatori	- Fare clic su Crea iniziatori in blocco. - Inserire un elenco di IQN o WWPN nella casella di testo. - Fare clic su Aggiungi iniziatori. - Selezionare un iniziatore dall'elenco risultante e fare clic sull'icona Aggiungi corrispondente nella colonna Alias per aggiungere un alias per l'iniziatore. - Fare clic sul segno di spunta per confermare il nuovo alias. - Fare clic su Crea iniziatori.

Modifica un iniziatore

È possibile modificare l'alias di un iniziatore esistente o aggiungerne uno nuovo se non ne esiste già uno.

Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare ModifyInitiator Chiamata API per rimuovere e aggiungere l'accesso e gli attributi CHAP.

Vedere ["Gestisci l'archiviazione con l'API Element"](#).

Passi

1. Fare clic su **Gestione > Iniziatori**.
2. Fare clic sull'icona Azioni relativa all'iniziatore che si desidera modificare.
3. Fare clic su **Modifica**.
4. Immettere un nuovo alias per l'iniziatore nel campo **Alias**.
5. Fare clic su **Salva modifiche**.

Aggiungere un singolo iniziatore a un gruppo di accesso al volume

È possibile aggiungere un iniziatore a un gruppo di accesso al 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 Azioni e selezionando quindi **Visualizza dettagli** per il volume nell'elenco dei volumi attivi.

Se si utilizza CHAP basato sull'iniziatore, è possibile aggiungere credenziali CHAP per un singolo iniziatore in un gruppo di accesso al volume, garantendo maggiore sicurezza. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

Passi

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera modificare.
3. Fare clic su **Modifica**.

4. Per aggiungere un iniziatore Fibre Channel al gruppo di accesso al volume, procedere come segue:
 - a. In **Aggiungi iniziatori**, seleziona un iniziatore Fibre Channel esistente dall'elenco **Iniziatori Fibre Channel non associati**.
 - b. Fare clic su **Aggiungi iniziatore FC**.



È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento **Crea iniziatore**, inserendo un nome per l'iniziatore e facendo clic su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco **Iniziatori**.

Un esempio del formato è il seguente:

```
5f:47:ac:c0:5c:74:d4:02
```

5. Per aggiungere un iniziatore iSCSI al gruppo di accesso al volume, in **Aggiungi iniziatori**, seleziona un iniziatore esistente dall'elenco **Iniziatori**.



È possibile creare un iniziatore durante questo passaggio facendo clic sul collegamento **Crea iniziatore**, inserendo un nome per l'iniziatore e facendo clic su **Crea**. Dopo averlo creato, il sistema aggiunge automaticamente l'iniziatore all'elenco **Iniziatori**.

Il formato accettato di un IQN di avvio è il seguente: `iqn.aaaa-mm`, in cui `y` e `m` sono cifre, seguite da testo che deve contenere solo cifre, caratteri alfabetici minuscoli, un punto (`.`), due punti (`:`) o un trattino (`-`).

Un esempio del formato è il seguente:

```
iqn.2010-01.com.solidfire:c2r9.fc0.2100000e1e09bb8b
```



È possibile trovare l'IQN dell'iniziatore per ciascun volume nella pagina **Gestione > Volumi** Volumi attivi facendo clic sull'icona Azioni e selezionando quindi **Visualizza dettagli** per il volume.

6. Fare clic su **Salva modifiche**.

Aggiungere più iniziatori a un gruppo di accesso al volume

È possibile aggiungere più iniziatori a un gruppo di accesso al volume esistente per consentire l'accesso ai volumi nel gruppo di accesso al volume con o senza la necessità dell'autenticazione CHAP.

Quando si aggiungono 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 Azioni e quindi su **Visualizza dettagli** per il volume nell'elenco dei volumi attivi.

È possibile aggiungere più iniziatori a un gruppo di accesso al volume esistente per abilitare l'accesso ai volumi e assegnare credenziali CHAP univoche per ciascun iniziatore all'interno di tale gruppo di accesso al

volume. Ciò consente di applicare questa opzione ai gruppi di accesso al volume già esistenti.

È possibile assegnare attributi CHAP basati sull'iniziatore utilizzando una chiamata API. Per aggiungere un nome account CHAP e credenziali per ogni iniziatore, è necessario utilizzare la chiamata API ModifyInitiator per rimuovere e aggiungere l'accesso e gli attributi CHAP.

Per i dettagli, vedere ["Gestisci l'archiviazione con l'API Element"](#).

Passi

1. Fare clic su **Gestione > Iniziatori**.
2. Seleziona gli iniziatori che desideri aggiungere a un gruppo di accesso.
3. Fare clic sul pulsante **Azioni in blocco**.
4. Fare clic su **Aggiungi al gruppo di accesso al volume**.
5. Nella finestra di dialogo Aggiungi al gruppo di accesso al volume, selezionare un gruppo di accesso dall'elenco **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 potrà più accedere ai volumi in quel gruppo di accesso al volume. L'accesso normale 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 imprevista dell'accesso degli iniziatori ai volumi. Per verificare che l'accesso al volume non venga perso inaspettatamente, disconnettersi sempre dalle sessioni iSCSI che saranno interessate da una modifica dell'account o del gruppo di accesso e verificare che gli iniziatori possano riconnettersi ai volumi dopo aver completato eventuali modifiche alle impostazioni dell'iniziatore e del cluster.

Passi

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera rimuovere.
3. Nel menu che si apre, seleziona **Modifica**.
4. In Aggiungi iniziatori nella finestra di dialogo **Modifica gruppo di accesso al volume**, fare clic sulla freccia nell'elenco **Iniziatori**.
5. Selezionare l'icona x per ogni iniziatore che si desidera rimuovere dal gruppo di accesso.
6. Fare clic su **Salva modifiche**.

Elimina 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. Dopo aver eliminato il gruppo di accesso, l'accesso del gruppo ai volumi viene interrotto.

1. Fare clic su **Gestione > Gruppi di accesso**.
2. Fare clic sull'icona **Azioni** per il gruppo di accesso che si desidera eliminare.

3. Nel menu che si apre, fare clic su **Elimina**.
4. Per eliminare anche gli iniziatori associati a questo gruppo di accesso, selezionare la casella di controllo **Elimina iniziatori in questo gruppo di accesso**.
5. Conferma l'azione.

Elimina un iniziatore

È possibile eliminare un iniziatore quando non è più necessario. Quando si elimina un iniziatore, il sistema lo rimuove da tutti i gruppi di accesso al volume associati. Tutte le connessioni che utilizzano l'iniziatore rimangono valide finché la connessione non viene reimpostata.

Passi

1. Fare clic su **Gestione > Iniziatori**.
2. Eseguire i passaggi per eliminare un singolo iniziatore o più iniziatori:

Opzione	Passi
Elimina singolo iniziatore	a. Fare clic sull'icona Azioni relativa all'iniziatore che si desidera eliminare. b. Fare clic su Elimina. c. Conferma l'azione.
Elimina più iniziatori	a. Seleziona le caselle di controllo accanto agli iniziatori che desideri eliminare. b. Fare clic sul pulsante Azioni in blocco. c. Nel menu che appare, seleziona Elimina. d. Conferma l'azione.

Proteggi i tuoi dati

Proteggi i tuoi dati

Il software NetApp Element consente di proteggere i dati in vari modi, grazie a funzionalità quali snapshot per singoli volumi o gruppi di volumi, replica tra cluster e volumi in esecuzione su Element e replica su sistemi ONTAP .

- **Istantanee**

La protezione dei dati basata solo su snapshot replica i dati modificati in momenti specifici su un cluster remoto. Vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non lo sono.

[Utilizzare snapshot del volume per la protezione dei dati](#)

- **Replica remota tra cluster e volumi in esecuzione su Element**

È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in 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 utilizzando la tecnologia SnapMirror ***

Grazie alla tecnologia NetApp SnapMirror , è possibile replicare gli snapshot acquisiti tramite Element su ONTAP per scopi di disaster recovery. In una relazione SnapMirror , Element è un endpoint e ONTAP è l'altro.

[Utilizzare la replica SnapMirror tra i cluster Element e ONTAP](#)

- **Esegui 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 negli archivi di oggetti SolidFire, S3 o Swift](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Utilizzare snapshot del volume per la protezione dei dati

Utilizzare snapshot del volume per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un dato momento. È possibile acquisire uno snapshot di un volume e utilizzarlo in un secondo momento se è necessario riportare un volume allo stato in cui si trovava al momento della creazione dello snapshot.

Gli snapshot sono simili ai cloni di volume. Tuttavia, gli snapshot sono semplicemente repliche dei metadati del volume, quindi non è possibile montarli o scriverci sopra. La creazione di uno snapshot del volume richiede inoltre solo una piccola quantità di risorse di sistema e spazio, il che rende la creazione di snapshot più rapida della clonazione.

È possibile acquisire un'istantanea di un singolo volume o di un set di volumi.

Facoltativamente, replicare gli snapshot su un cluster remoto e utilizzarli come copia di backup del volume. Ciò consente di ripristinare un volume a un punto specifico nel tempo utilizzando lo snapshot replicato. In alternativa, è possibile creare un clone di un volume da uno snapshot replicato.

Trova maggiori informazioni

- [Utilizzare snapshot di volumi individuali per la protezione dei dati](#)
- [Utilizzo di snapshot di gruppo per attività di protezione dei dati](#)
- [Pianificazione di uno snapshot](#)

Utilizzare snapshot di volumi individuali per la protezione dei dati

Utilizzare snapshot di volumi individuali per la protezione dei dati

Uno snapshot del volume è una copia di un volume effettuata in un dato momento. Per lo snapshot è possibile utilizzare un singolo volume anziché un gruppo di volumi.

Trova maggiori informazioni

- [Crea uno snapshot del volume](#)
- [Modifica la conservazione degli snapshot](#)
- [Eliminazione di uno snapshot](#)
- [Clonazione di un volume da uno snapshot](#)
- [Ripristino di un volume in uno snapshot](#)
- [Backup di uno snapshot del volume in un archivio oggetti Amazon S3](#)
- [Backup di uno snapshot del volume in un archivio oggetti OpenStack Swift](#)
- [Backup di uno snapshot del volume su un cluster SolidFire](#)

Crea uno snapshot del volume

È possibile creare uno snapshot di un volume attivo per preservare l'immagine del volume in qualsiasi momento. È possibile creare fino a 32 snapshot per un singolo volume.

1. Fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera utilizzare per lo snapshot.
3. Nel menu che si apre, seleziona **Snapshot**.
4. Nella finestra di dialogo **Crea snapshot del volume**, immettere il nome del nuovo snapshot.
5. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando associato** per garantire che lo snapshot venga acquisito nella replica quando il volume padre viene associato.
6. Per impostare la conservazione per lo snapshot, selezionare una delle seguenti opzioni:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
7. Per acquisire un singolo snapshot immediato, procedere come segue:
 - a. Fare clic su **Scatta istantanea ora**.
 - b. Fare clic su **Crea snapshot**.
8. Per pianificare l'esecuzione dello snapshot in un momento futuro, procedere come segue:
 - a. Fare clic su **Crea pianificazione snapshot**.
 - b. Inserisci un **Nome nuovo programma**.
 - c. Selezionare un **Tipo di pianificazione** dall'elenco.
 - d. **Facoltativo:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.

e. Fare clic su **Crea pianificazione**.

Trova maggiori informazioni

[Pianifica uno snapshot](#)

Modifica la conservazione degli snapshot

È possibile modificare il periodo di conservazione di uno snapshot per controllare quando e se il sistema elimina gli snapshot. Il periodo di conservazione specificato inizia quando si immette 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 in base all'ora di creazione dello snapshot). È possibile specificare intervalli in minuti, ore e giorni.

Passi

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot che si desidera modificare.
3. Nel menu che si apre, fare clic su **Modifica**.
4. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando associato** per garantire che lo snapshot venga acquisito nella replica quando il volume padre è associato.
5. **Facoltativo:** seleziona un'opzione di conservazione per lo snapshot:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per selezionare un periodo di tempo durante il quale il sistema conserverà lo snapshot.
6. Fare clic su **Salva modifiche**.

Elimina uno snapshot

È possibile eliminare uno snapshot del volume da un cluster di archiviazione 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 è in fase di sincronizzazione con il cluster di destinazione quando lo elimini, la replica di sincronizzazione viene completata e lo snapshot viene eliminato dal cluster di origine. Lo snapshot non viene eliminato dal cluster di destinazione.

È anche possibile eliminare gli snapshot replicati sulla destinazione dal cluster di destinazione. Lo snapshot eliminato viene conservato in un elenco di snapshot eliminati sulla destinazione finché il sistema non rileva che lo snapshot è stato eliminato sul cluster di origine. Quando la destinazione rileva che hai eliminato lo snapshot di origine, interrompe la replica dello snapshot.

Quando si elimina uno snapshot dal cluster di origine, lo snapshot del cluster di destinazione non viene influenzato (vale anche il contrario).

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot che si desidera eliminare.
3. Nel menu che appare, seleziona **Elimina**.

4. Conferma l'azione.

Clonare un volume da uno snapshot

È possibile creare un nuovo volume da uno snapshot di un volume. Quando si esegue questa operazione, il sistema utilizza le informazioni dello snapshot per clonare un nuovo volume utilizzando i dati contenuti nel volume al momento della creazione dello snapshot. Questo processo memorizza le informazioni su altri snapshot del volume nel volume appena creato.

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** per lo snapshot che si desidera utilizzare per il clone del volume.
3. Nel menu visualizzato, fare clic su **Clona volume da snapshot**.
4. Immettere un **Nome volume** nella finestra di dialogo **Clona volume da snapshot**.
5. Selezionare una **Dimensione totale** e le unità di misura per il nuovo volume.
6. Selezionare un tipo di **Accesso** per il volume.
7. Selezionare un **Account** dall'elenco da associare al nuovo volume.
8. Fare clic su **Avvia clonazione**.

Ripristinare un volume a uno snapshot

È possibile ripristinare un volume a uno snapshot precedente in qualsiasi momento. In questo modo vengono annullate tutte le modifiche apportate al volume dalla creazione dello snapshot.

Passi

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** per lo snapshot che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, seleziona **Rollback Volume To Snapshot**.
4. **Facoltativo:** per salvare lo stato corrente del volume prima di tornare allo snapshot:
 - a. Nella finestra di dialogo **Rollback a snapshot**, seleziona **Salva lo stato corrente del volume come snapshot**.
 - b. Inserisci un nome per il nuovo snapshot.
5. Fare clic su **Rollback Snapshot**.

Eseguire il backup di uno snapshot del volume

Eseguire il backup di uno snapshot del volume

È possibile utilizzare la funzionalità di backup integrata per eseguire il backup di uno snapshot del volume. È possibile eseguire il backup degli snapshot da un cluster SolidFire a un archivio oggetti esterno o a un altro cluster SolidFire. Quando si esegue il backup di uno snapshot in un archivio oggetti esterno, è necessario disporre di una connessione all'archivio oggetti che consenta operazioni di lettura/scrittura.

- "Eseguire il backup di uno snapshot del volume in un archivio oggetti Amazon S3"
- "Eseguire il backup di uno snapshot del volume in un archivio oggetti OpenStack Swift"
- "Eseguire il backup di uno snapshot del volume su un cluster SolidFire"

Eseguire il backup di uno snapshot del volume in un archivio oggetti Amazon S3

È possibile eseguire il backup degli snapshot SolidFire su archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **S3**.
5. Selezionare un'opzione in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
7. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
8. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
9. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
10. **Facoltativo**: inserisci un'etichetta da aggiungere al prefisso nel campo **Etichetta**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di uno snapshot del volume in un archivio oggetti OpenStack Swift

È possibile eseguire il backup degli snapshot SolidFire in archivi di oggetti secondari compatibili con OpenStack Swift.

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sull'icona **Azioni** relativa allo snapshot di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **Swift**.
5. Selezionare un'opzione in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Inserisci un **URL** da utilizzare per accedere all'archivio oggetti.
7. Inserisci un **Nome utente** per l'account.
8. Inserisci la **Chiave di autenticazione** per l'account.
9. Immettere il **Contenitore** in cui archiviare il backup.
10. **Facoltativo**: Inserisci un **tag**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di uno snapshot del volume su un cluster SolidFire

È possibile eseguire il backup di snapshot di volumi residenti su un cluster SolidFire su un cluster SolidFire remoto.

Assicurarsi che i cluster di origine e di destinazione siano accoppiati.

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona **Azioni** per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **Ripristina da**.
4. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare * SolidFire*.
5. Selezionare un formato dati in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copia la chiave dalla casella **Chiave di scrittura volume in blocco** negli appunti.
8. Nel cluster di origine, fare clic su **Protezione dati > Snapshot**.
9. Fare clic sull'icona Azioni relativa allo snapshot che si desidera utilizzare per il backup.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare * SolidFire*.
12. Selezionare lo stesso formato dati selezionato in precedenza nel campo **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.
14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Nel campo **Chiave di scrittura volume di massa**, incollare la chiave generata in precedenza sul cluster di destinazione.
17. Fare clic su **Inizia a leggere**.

Utilizzare snapshot di gruppo per la protezione dei dati

Utilizzo di snapshot di gruppo per attività di protezione dei dati

È possibile creare uno snapshot di gruppo di un set correlato di volumi per conservare una copia puntuale dei metadati per ciascun volume. È possibile utilizzare lo snapshot del gruppo in futuro come backup o rollback per ripristinare lo stato del gruppo di volumi a uno stato precedente.

Trova maggiori informazioni

- [Crea uno snapshot di gruppo](#)
- [Modifica istantanee di gruppo](#)
- [Modifica i membri dello snapshot del gruppo](#)
- [Eliminare uno snapshot di gruppo](#)
- [Ripristina i volumi in uno snapshot di gruppo](#)
- [Clona più volumi](#)
- [Clona più volumi da uno snapshot di gruppo](#)

Dettagli dello snapshot del gruppo

La pagina Snapshot di gruppo nella scheda Protezione dati fornisce informazioni sugli snapshot di gruppo.

- **ID**

ID generato dal sistema per lo snapshot del gruppo.

- **UUID**

ID univoco dello snapshot del gruppo.

- **Nome**

Nome definito dall'utente per l'istantanea del gruppo.

- **Crea tempo**

Ora in cui è stato creato lo snapshot del gruppo.

- **Stato**

Lo stato attuale dello snapshot. Valori possibili:

- Preparazione: lo snapshot è in fase di preparazione per l'uso e non è ancora scrivibile.
- Fatto: la preparazione di questo snapshot è terminata ed è ora utilizzabile.
- Attivo: lo snapshot è il ramo attivo.

- **# Volumi**

Il numero di volumi nel gruppo.

- **Conservare fino a**

Giorno e ora in cui lo snapshot verrà eliminato.

- **Replica remota**

Indica se lo snapshot è abilitato o meno per la replica su un cluster SolidFire remoto. Valori possibili:

- Abilitato: lo snapshot è abilitato per la replica remota.

- Disabilitato: lo snapshot non è abilitato per la replica remota.

Creazione di uno snapshot di gruppo

È possibile creare uno snapshot di un gruppo di volumi e anche creare una pianificazione di snapshot di gruppo per automatizzare gli snapshot di gruppo. Un singolo snapshot di gruppo può eseguire snapshot costanti di un massimo di 32 volumi contemporaneamente.

Passi

1. Fare clic su **Gestione > Volumi**.
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 **Snapshot di gruppo**.
5. Immettere un nuovo nome per lo snapshot di gruppo nella finestra di dialogo Crea snapshot di gruppo dei volumi.
6. **Facoltativo:** selezionare la casella di controllo **Includi ciascun membro dello snapshot di gruppo nella replica quando associato** per garantire che ogni snapshot venga acquisito nella replica quando il volume padre viene associato.
7. Seleziona un'opzione di conservazione per lo snapshot del gruppo:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
8. Per acquisire un singolo snapshot immediato, procedere come segue:
 - a. Fare clic su **Acquisisci istantanea di gruppo ora**.
 - b. Fare clic su **Crea snapshot di gruppo**.
9. Per pianificare l'esecuzione dello snapshot in un momento futuro, procedere come segue:
 - a. Fare clic su **Crea pianificazione snapshot di gruppo**.
 - b. Inserisci un **Nome nuovo programma**.
 - c. Selezionare un **Tipo di pianificazione** dall'elenco.
 - d. **Facoltativo:** selezionare la casella di controllo **Pianificazione ricorrente** per ripetere periodicamente lo snapshot pianificato.
 - e. Fare clic su **Crea pianificazione**.

Modifica degli snapshot di gruppo

È possibile modificare le impostazioni di replica e conservazione per gli snapshot di gruppo esistenti.

1. Fare clic su **Protezione dati > Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per l'istantanea del gruppo che si desidera modificare.
3. Nel menu che si apre, seleziona **Modifica**.
4. **Facoltativo:** per modificare l'impostazione di replica per lo snapshot del gruppo:

- a. Fare clic su **Modifica** accanto a **Replica corrente**.
 - b. Selezionare la casella di controllo **Includi ciascun membro dello snapshot di gruppo nella replica quando abbinato** per garantire che ogni snapshot venga acquisito nella replica quando il volume padre viene abbinato.
5. **Facoltativo:** per modificare l'impostazione di conservazione per lo snapshot del gruppo, seleziona una delle seguenti opzioni:
- a. Fare clic su **Modifica** accanto a **Conservazione corrente**.
 - b. Seleziona un'opzione di conservazione per lo snapshot del gruppo:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
6. Fare clic su **Salva modifiche**.

Eliminazione di uno snapshot di gruppo

È possibile eliminare uno snapshot di gruppo dal sistema. Quando elimini lo snapshot del gruppo, puoi scegliere se tutti gli snapshot associati al gruppo devono essere eliminati o conservati come snapshot individuali.

Se si elimina un volume o uno snapshot che fa parte di uno snapshot di gruppo, non sarà più possibile eseguire il rollback allo snapshot di gruppo. Tuttavia, è possibile ripristinare ogni volume singolarmente.

1. Fare clic su **Protezione dati > Snapshot di gruppo**.
2. Fare clic sull'icona Azioni relativa allo snapshot che si desidera eliminare.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Selezionare una delle seguenti opzioni nella finestra di dialogo di conferma:
 - Fare clic su **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 i membri dello snapshot del gruppo come snapshot individuali** per eliminare lo snapshot del gruppo ma conservare tutti gli snapshot dei membri.
5. Conferma l'azione.

Ripristina i volumi in uno snapshot di gruppo

È possibile ripristinare un gruppo di volumi in qualsiasi momento trasformandolo 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 del gruppo. Il rollback ripristina anche le dimensioni del volume a quelle registrate nello snapshot originale. Se il sistema ha eliminato un volume, al momento dell'eliminazione sono stati eliminati anche tutti gli snapshot di quel volume; il sistema non ripristina nessuno snapshot del volume eliminato.

1. Fare clic su **Protezione dati > Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per lo snapshot di gruppo che si desidera utilizzare per il rollback del volume.
3. Nel menu visualizzato, selezionare **Esegui rollback dei volumi nello snapshot di gruppo**.

4. **Facoltativo:** per salvare lo stato corrente dei volumi prima di tornare allo snapshot:
 - a. Nella finestra di dialogo **Rollback a snapshot**, selezionare **Salva lo stato corrente dei volumi come snapshot di gruppo**.
 - b. Inserisci un nome per il nuovo snapshot.
5. Fare clic su **Ripristina snapshot gruppo**.

Modifica dei membri dello snapshot del gruppo

È possibile modificare le impostazioni di conservazione per i membri di uno snapshot di gruppo esistente.

1. Fare clic su **Protezione dati > Snapshot**.
2. Fare clic sulla scheda **Membri**.
3. Fare clic sull'icona Azioni relativa al membro dello snapshot di gruppo che si desidera modificare.
4. Nel menu che si apre, seleziona **Modifica**.
5. Per modificare l'impostazione di replica per lo snapshot, selezionare una delle seguenti opzioni:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
6. Fare clic su **Salva modifiche**.

Clona più volumi

È possibile creare più cloni di volume in un'unica operazione per creare una copia puntuale dei dati su un gruppo di volumi.

Quando si clona un volume, il sistema crea uno snapshot del volume e poi 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 una quantità di tempo variabile a seconda delle dimensioni e del numero dei volumi da clonare.

Le dimensioni del volume e il carico attuale del cluster influiscono sul tempo necessario per completare un'operazione di clonazione.

Passi

1. Fare clic su **Gestione > Volumi**.
2. Fare clic sulla scheda **Attivo**.
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 **Clona** nel menu visualizzato.
6. Immettere un **Nuovo prefisso nome volume** nella finestra di dialogo **Clona più volumi**.

Il prefisso viene applicato a tutti i volumi del gruppo.

7. **Facoltativo:** seleziona un account diverso a cui apparterrà il clone.

Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

8. **Facoltativo:** 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 in un dato momento. 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 nel sistema.

Le dimensioni del volume e il carico attuale del cluster influiscono sul tempo necessario per completare un'operazione di clonazione.

1. Fare clic su **Protezione dati > Snapshot di gruppo**.
2. Fare clic sull'icona Azioni per lo snapshot di gruppo che si desidera utilizzare per i cloni del volume.
3. Nel menu visualizzato, selezionare **Clona volumi da snapshot di gruppo**.
4. Immettere un **Nuovo prefisso nome volume** nella finestra di dialogo **Clona volumi da snapshot di gruppo**.

Il prefisso viene applicato a tutti i volumi creati dallo snapshot del gruppo.

5. **Facoltativo:** seleziona un account diverso a cui apparterrà il clone.

Se non si seleziona un account, il sistema assegna i nuovi volumi all'account del volume corrente.

6. **Facoltativo:** 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 uno snapshot

Pianifica uno snapshot

È possibile proteggere i dati su un volume o un gruppo di volumi pianificando l'esecuzione di snapshot del volume a intervalli specifici. È possibile pianificare l'esecuzione automatica di snapshot di singoli volumi o di snapshot di gruppo.

Quando si configura una pianificazione degli snapshot, è possibile scegliere tra intervalli di tempo basati sui giorni della settimana o sui giorni del mese. È anche possibile specificare i giorni, le ore e i minuti prima che venga eseguito lo snapshot successivo. Se il volume viene replicato, è possibile archiviare gli snapshot risultanti su un sistema di archiviazione remoto.

Trova maggiori informazioni

- [Creare una pianificazione snapshot](#)
- [Modificare una pianificazione di snapshot](#)

- [Elimina una pianificazione snapshot](#)
- [Copia una pianificazione snapshot](#)

Dettagli della pianificazione degli snapshot

Nella pagina Protezione dati > Pianificazioni, è possibile visualizzare le seguenti informazioni nell'elenco delle pianificazioni degli snapshot.

- **ID**

ID generato dal sistema per lo snapshot.

- **Tipo**

Il tipo di programma. Attualmente l'unico tipo supportato è Snapshot.

- **Nome**

Nome assegnato alla pianificazione al momento della sua creazione. I nomi delle pianificazioni snapshot possono avere una lunghezza massima di 223 caratteri e contenere caratteri az, 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**

Indica se la pianificazione deve essere eseguita una sola volta o a intervalli regolari.

- **Messo in pausa manualmente**

Indica se la pianificazione è stata sospesa manualmente o meno.

- **ID volume**

ID del volume che la pianificazione utilizzerà quando verrà eseguita.

- **Ultima corsa**

L'ultima volta che è stato eseguito il programma.

- **Stato dell'ultima esecuzione**

L'esito dell'ultima esecuzione programmata. Valori possibili:

- Successo
- Fallimento

Creare una pianificazione snapshot

È possibile pianificare l'esecuzione automatica di uno snapshot di uno o più volumi a intervalli specificati.

Quando si configura una pianificazione degli snapshot, è possibile scegliere tra intervalli di tempo basati sui giorni della settimana o sui giorni del mese. È anche possibile creare una pianificazione ricorrente e specificare i giorni, le ore e i minuti prima che venga eseguito lo snapshot successivo.

Se si pianifica l'esecuzione di uno snapshot in un intervallo di tempo non divisibile per 5 minuti, lo snapshot verrà eseguito nel successivo intervallo di tempo divisibile per 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.

A partire da Element 12.5, è possibile abilitare la creazione seriale e scegliere di conservare gli snapshot in base al metodo First-In-First-Out (FIFO) dall'interfaccia utente.

- L'opzione **Abilita creazione seriale** specifica che viene replicato solo uno snapshot alla volta. La creazione di un nuovo snapshot non riesce quando è ancora in corso la replica di uno snapshot precedente. Se la casella di controllo non è selezionata, è consentita la creazione di uno snapshot quando è ancora in corso un'altra replica dello snapshot.
- L'opzione **FIFO** aggiunge la possibilità di conservare un numero coerente degli snapshot più recenti. Quando la casella di controllo è selezionata, gli snapshot vengono conservati secondo il metodo FIFO. Una volta che la coda di snapshot FIFO raggiunge la sua profondità massima, lo snapshot FIFO più vecchio viene scartato quando viene inserito un nuovo snapshot FIFO.

Passi

1. Selezionare **Protezione dati > Pianificazioni**.
2. Seleziona **Crea pianificazione**.
3. Nel campo **ID volume CSV**, immettere un singolo ID volume o un elenco di ID volume separati da virgole da includere nell'operazione di snapshot.
4. Inserisci un nuovo nome per la pianificazione.
5. Selezionare un tipo di pianificazione e impostare la pianificazione tra le opzioni fornite.
6. **Facoltativo:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione degli snapshot indefinitamente.
7. **Facoltativo:** inserisci un nome per il nuovo snapshot nel campo **Nome nuovo snapshot**.

Se si lascia vuoto il campo, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.

8. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per garantire che gli snapshot vengano acquisiti nella replica quando il volume padre è accoppiato.
9. **Facoltativo:** selezionare la casella di controllo **Abilita creazione seriale** per garantire che venga replicato solo uno snapshot alla volta.
10. Per impostare la conservazione per lo snapshot, selezionare una delle seguenti opzioni:
 - **Facoltativo:** selezionare la casella di controllo **FIFO (First In First out)** per conservare un numero coerente degli snapshot più recenti.
 - Selezionare **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Selezionare **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per scegliere il periodo di tempo durante il quale il sistema deve conservare lo snapshot.
11. Seleziona **Crea pianificazione**.

Modificare una pianificazione di snapshot

È possibile modificare le pianificazioni degli snapshot esistenti. Dopo la modifica, la prossima volta che la pianificazione verrà eseguita, utilizzerà gli attributi aggiornati. Tutti gli snapshot creati dalla pianificazione originale rimangono sul sistema di archiviazione.

Passi

1. Fare clic su **Protezione dati > Pianificazioni**.
2. Fare clic sull'icona **Azioni** relativa alla pianificazione che si desidera modificare.
3. Nel menu che si apre, fare clic su **Modifica**.
4. Nel campo **ID volume CSV**, modificare l'ID del singolo volume o l'elenco separato da virgole degli ID del volume attualmente inclusi nell'operazione di snapshot.
5. Per mettere in pausa o riprendere la pianificazione, seleziona una delle seguenti opzioni:
 - Per mettere in pausa una pianificazione attiva, selezionare **Sì** dall'elenco **Metti in pausa manualmente la pianificazione**.
 - Per riprendere una pianificazione sospesa, selezionare **No** dall'elenco **Sospendi manualmente la pianificazione**.
6. Se lo si desidera, immettere un nome diverso per la pianificazione nel campo **Nuovo nome pianificazione**.
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. **Facoltativo:** selezionare **Pianificazione ricorrente** per ripetere la pianificazione degli snapshot indefinitamente.
9. **Facoltativo:** immettere o modificare il nome del nuovo snapshot nel campo **Nome nuovo snapshot**.

Se si lascia vuoto il campo, il sistema utilizza come nome l'ora e la data di creazione dello snapshot.
10. **Facoltativo:** selezionare la casella di controllo **Includi snapshot nella replica quando accoppiato** per garantire che gli snapshot vengano acquisiti nella replica quando il volume padre è accoppiato.
11. Per modificare l'impostazione di conservazione, selezionare una delle seguenti opzioni:
 - Fare clic su **Conserva per sempre** per conservare lo snapshot sul sistema a tempo indeterminato.
 - Fare clic su **Imposta periodo di conservazione** e utilizzare le caselle di selezione della data per selezionare un periodo di tempo durante il quale il sistema conserverà lo snapshot.
12. Fare clic su **Salva modifiche**.

Copia una pianificazione snapshot

È possibile copiare una pianificazione e mantenerne gli attributi correnti.

1. Fare clic su **Protezione dati > Pianificazioni**.
2. Fare clic sull'icona **Azioni** relativa alla pianificazione che si desidera copiare.
3. Nel menu che si apre, fare clic su **Crea una copia**.

Viene visualizzata la finestra di dialogo **Crea pianificazione**, compilata con gli attributi correnti della pianificazione.

4. **Facoltativo:** inserisci un nome e gli attributi aggiornati per la nuova pianificazione.
5. Fare clic su **Crea pianificazione**.

Elimina una pianificazione snapshot

È possibile eliminare una pianificazione snapshot. Dopo aver eliminato la pianificazione, non verranno eseguiti più snapshot pianificati. Tutti gli snapshot creati dalla pianificazione rimangono nel sistema di archiviazione.

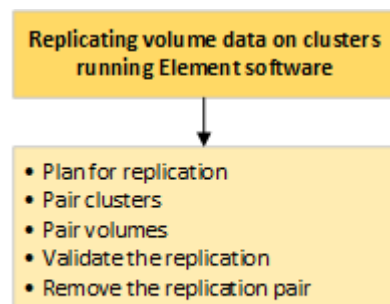
1. Fare clic su **Protezione dati > Pianificazioni**.
2. Fare clic sull'icona **Azioni** relativa alla pianificazione che si desidera eliminare.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Conferma l'azione.

Eseguire la replica remota tra cluster che eseguono il software NetApp Element

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 rapida creazione di copie remote dei dati del volume. È possibile associare un cluster di archiviazione a un massimo di altri quattro cluster di archiviazione. È possibile replicare i dati del volume in modo sincrono o asincrono da entrambi i cluster in una coppia di cluster per scenari di failover e failback.

Il processo di replicazione comprende i seguenti passaggi:



- "Pianifica l'associazione di cluster e volumi per la replica in tempo reale"
- "Cluster di coppie per la replicazione"
- "Volumi di coppia"
- "Convalida la replica del volume"
- "Elimina una relazione di volume dopo la replica"
- "Gestire le relazioni di volume"

Pianifica l'associazione di cluster e volumi per la replica in tempo reale

Per la replica remota in tempo reale è necessario associare due cluster di storage che

eseguono il software Element, associare i volumi su ciascun cluster e convalidare la replica. Una volta completata la replica, è necessario eliminare la relazione del volume.

Cosa ti servirà

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.
- Tutti gli indirizzi IP dei nodi sulle reti di gestione e di archiviazione per i cluster accoppiati vengono instradati l'uno verso l'altro.
- L'MTU di tutti i nodi accoppiati deve essere lo stesso e supportato end-to-end tra i cluster.
- Entrambi i cluster di archiviazione devono avere nomi di cluster, MVIP, SVIP e tutti gli indirizzi IP dei nodi univoci.
- La differenza tra le versioni del software Element sui cluster non è maggiore di una versione principale. Se la differenza è maggiore, è necessario aggiornare uno dei cluster per eseguire la replica dei dati.



Gli apparecchi WAN Accelerator non sono stati qualificati da NetApp per l'uso durante la replica dei dati. Questi dispositivi possono interferire con la compressione e la deduplicazione se distribuiti tra due cluster che replicano i dati. Assicuratevi di valutare attentamente gli effetti di qualsiasi dispositivo WAN Accelerator prima di distribuirlo in un ambiente di produzione.

Trova maggiori informazioni

- [Cluster di coppie per la replicazione](#)
- [Volumi di coppia](#)
- [Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati](#)

Cluster di coppie per la replicazione

Cluster di coppie per la replicazione

Per utilizzare la funzionalità di replica in tempo reale, è necessario innanzitutto associare due cluster. Dopo aver associato e connesso due cluster, è possibile configurare i volumi attivi su un cluster in modo che vengano replicati continuamente su un secondo cluster, garantendo una protezione continua dei dati (CDP).

Cosa ti servirà

- È necessario disporre dei privilegi di amministratore del cluster per uno o entrambi i cluster da associare.
- Tutti i MIP e i SIP 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, MVIP, SVIP e tutti gli indirizzi IP dei nodi univoci.
- La differenza tra le versioni del software Element sui cluster non è maggiore di una versione principale. Se la differenza è maggiore, è necessario aggiornare uno dei cluster per eseguire la replica dei dati.



L'associazione dei cluster richiede la piena connettività tra i nodi sulla rete di gestione. La replica richiede la connettività tra i singoli nodi sulla rete del cluster di archiviazione.

È possibile associare un cluster a un massimo di altri quattro cluster per replicare i volumi. È anche possibile associare tra loro i cluster all'interno del gruppo di cluster.

Accoppiare i cluster utilizzando MVIP o una chiave di associazione

È possibile associare un cluster di origine e uno di destinazione utilizzando l'MVIP del cluster di destinazione se è presente l'accesso dell'amministratore del cluster a entrambi i cluster. Se l'accesso dell'amministratore del cluster è disponibile solo su un cluster in una coppia di cluster, è possibile utilizzare una chiave di associazione sul cluster di destinazione per completare l'associazione del cluster.

1. Selezionare uno dei seguenti metodi per associare i cluster:
 - ["Cluster di coppie tramite MVIP"](#): Utilizzare questo metodo se l'amministratore del cluster ha accesso a entrambi i cluster. Questo metodo utilizza l'MVIP del cluster remoto per accoppiare due cluster.
 - ["Accoppia i cluster utilizzando una chiave di associazione"](#): Utilizzare questo metodo se l'amministratore del cluster ha accesso solo a uno dei cluster. Questo metodo genera una chiave di associazione che può essere utilizzata sul cluster di destinazione per completare l'associazione del cluster.

Trova maggiori informazioni

[Requisiti delle porte di rete](#)

Cluster di coppie tramite 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 l'accesso come 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 che i cluster possano essere associati.

1. Nel cluster locale, selezionare **Protezione dati > Coppie cluster**.
2. Fare clic su **Cluster di coppie**.
3. Fare clic su **Avvia associazione** e quindi su **Sì** per indicare che si ha accesso al cluster remoto.
4. Immettere l'indirizzo MVIP del cluster remoto.
5. Fare clic su **Completa associazione sul cluster remoto**.

Nella finestra **Autenticazione richiesta**, immettere il nome utente e la password dell'amministratore del cluster remoto.

6. Nel cluster remoto, selezionare **Protezione dati > Coppie cluster**.
7. Fare clic su **Cluster di coppie**.
8. Fare clic su **Completa associazione**.
9. Fare clic sul pulsante **Completa associazione**.

Trova maggiori informazioni

- [Accoppia i cluster utilizzando una chiave di associazione](#)
- ["Accoppiamento di cluster tramite MVIP \(video\)"](#)

Accoppia i cluster utilizzando una chiave di associazione

Se si dispone dell'accesso come amministratore del cluster a un cluster locale ma non a

quello remoto, è possibile associare i cluster utilizzando una chiave di associazione. Una chiave di associazione viene generata su un cluster locale e quindi inviata in modo sicuro a un amministratore del cluster in un sito remoto per stabilire una connessione e completare l'associazione del cluster per la replica in tempo reale.

1. Nel cluster locale, selezionare **Protezione dati > Coppie cluster**.
2. Fare clic su **Cluster di coppie**.
3. Fare clic su **Avvia associazione** e poi su **No** per indicare che non si ha accesso al cluster remoto.
4. Fare clic su **Genera chiave**.



Questa azione genera una chiave di testo per l'associazione e crea una coppia di cluster non configurata sul cluster locale. Se non si completa la procedura, sarà necessario eliminare manualmente la coppia di cluster.

5. Copia la chiave di associazione del cluster negli appunti.
6. Rendere la chiave di associazione accessibile all'amministratore del cluster nel sito remoto del cluster.



La chiave di associazione del cluster contiene una versione dell'MVIP, del nome utente, della password e delle informazioni del database per consentire le connessioni del volume per la replica remota. Questa chiave deve essere trattata in modo sicuro e non conservata in un modo che possa consentire l'accesso accidentale o non protetto al nome utente o alla password.



Non modificare nessuno dei caratteri nella chiave di associazione. La chiave diventa non valida se viene modificata.

7. Nel cluster remoto, selezionare **Protezione dati > Coppie cluster**.
8. Fare clic su **Cluster di coppie**.
9. Fare clic su **Completa associazione** e immettere la chiave di associazione nel campo **Chiave di associazione** (il metodo consigliato è incollare).
10. Fare clic su **Completa associazione**.

Trova maggiori informazioni

- [Cluster di coppie tramite MVIP](#)
- ["Associazione di cluster tramite una chiave di associazione cluster \(video\)"](#)

Convalida la connessione della coppia di cluster

Una volta completata l'associazione dei cluster, potrebbe essere opportuno verificare la connessione della coppia di cluster per garantire il successo della replica.

1. Nel cluster locale, selezionare **Protezione dati > Coppie cluster**.
2. Nella finestra **Coppie di cluster**, verificare che la coppia di cluster sia connessa.
3. **Facoltativo:** tornare al cluster locale e alla finestra **Coppie di cluster** e verificare che la coppia di cluster sia connessa.

Volumi di coppia

Volumi di coppia

Dopo aver stabilito una connessione tra i cluster in una coppia di cluster, è possibile associare un volume su un cluster con un volume sull'altro cluster nella coppia. Quando viene stabilita una relazione di associazione di volumi, è necessario identificare quale volume è la destinazione della replica.

È possibile associare due volumi per la replica in tempo reale archiviati su cluster di archiviazione diversi in una coppia di cluster connessi. Dopo aver associato due cluster, è possibile configurare i volumi attivi su un cluster in modo che vengano replicati continuamente su un secondo cluster, garantendo una protezione continua dei dati (CDP). È anche possibile assegnare uno dei due volumi come origine o destinazione della replica.

Gli abbinamenti di volume sono sempre uno a uno. Dopo che un volume fa parte di un abbinamento con un volume su un altro cluster, non è possibile abbinarlo nuovamente a nessun altro volume.

Cosa ti servirà

- Hai stabilito una connessione tra i cluster in una coppia di cluster.
- Si dispone dei privilegi di amministratore del cluster per uno o entrambi i cluster associati.

Passi

1. [Crea 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 replicazione ai volumi accoppiati](#)

Crea un volume di destinazione con accesso in lettura o scrittura

Il processo di replicazione 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 **Gestione > Volumi**.
2. Fare clic su **Crea volume**.
3. Nella finestra di dialogo Crea un nuovo volume, immettere il nome del volume.
4. Immettere la dimensione totale del volume, selezionare una dimensione di blocco per il volume e selezionare l'account che deve avere accesso al volume.
5. Fare clic su **Crea volume**.
6. Nella finestra Attiva, fare clic sull'icona Azioni per il volume.
7. Fare clic su **Modifica**.
8. Modificare il livello di accesso dell'account in Destinazione replica.
9. Fare clic su **Salva modifiche**.

Associare i volumi utilizzando un ID volume o una chiave di associazione

Abbinare i volumi utilizzando un ID volume

È possibile associare un volume a un altro volume su un cluster remoto se si dispone dell'accesso come amministratore del cluster a entrambi i cluster su cui si desidera associare i volumi. Questo metodo utilizza l'ID del volume sul cluster remoto per avviare una connessione.

Cosa ti servirà

- Assicurarsi che i cluster contenenti i volumi siano accoppiati.
- Creare un nuovo volume sul cluster remoto.



Dopo il processo di associazione è possibile assegnare un'origine e una destinazione di replicazione. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione della dimensione del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

- Conoscere l'ID del volume di destinazione.

Passi

1. Selezionare **Gestione > Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera associare.
3. Fare clic su **Associa**.
4. Nella finestra di dialogo **Volume di associazione**, selezionare **Avvia associazione**.
5. Selezionare **Lo voglio** per indicare che si ha accesso al cluster remoto.
6. Selezionare una **Modalità di replicazione** dall'elenco:
 - **In tempo reale (asincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.
 - **In tempo reale (sincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
 - **Solo snapshot**: vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.
7. Selezionare un cluster remoto dall'elenco.
8. Scegli un ID volume remoto.
9. Fare clic su **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 dell'elemento del cluster remoto, selezionare **Completa associazione**.
11. Confermare i dettagli in **Conferma associazione volume**.
12. Fare clic su **Completa associazione**.

Dopo aver confermato l'associazione, i due cluster avviano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Stato volume** della finestra **Coppie di volumi**. La coppia di volumi viene visualizzata `PausedMisconfigured` finché non vengono assegnate la coppia di volumi sorgente e destinazione.

Dopo aver completato correttamente l'associazione, si consiglia di aggiornare la tabella Volumi per rimuovere l'opzione **Associa** dall'elenco **Azioni** per il volume associato. Se non si aggiorna la tabella, l'opzione **Coppia** rimane disponibile per la selezione. Se si seleziona nuovamente l'opzione **Associa**, si apre una nuova scheda e poiché il volume è già associato, il sistema segnala un `StartVolumePairing Failed: xVolumeAlreadyPaired` messaggio di errore nella finestra **Volume coppia** della pagina Element UI.

Trova maggiori informazioni

- [Messaggi di associazione del volume](#)
- [Avvisi di associazione del volume](#)
- [Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati](#)

Abbinare i volumi utilizzando una chiave di associazione

Se si dispone dell'accesso come amministratore del cluster solo al cluster di origine (non si dispone delle credenziali di amministratore del cluster per un cluster remoto), è possibile associare un volume a un altro volume su un cluster remoto utilizzando una chiave di associazione.

Cosa ti servirà

- Assicurarsi che i cluster contenenti i volumi siano accoppiati.
- Assicurarsi che sul cluster remoto sia presente un volume da utilizzare per l'associazione.



Dopo il processo di associazione è possibile assegnare un'origine e una destinazione di replicazione. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È necessario creare un volume di destinazione che non contenga dati e che abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione della dimensione del blocco per i volumi (512e o 4k) e configurazione QoS. Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

Passi

1. Selezionare **Gestione > Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che si desidera associare.
3. Fare clic su **Associa**.
4. Nella finestra di dialogo **Volume di associazione**, selezionare **Avvia associazione**.
5. Selezionare **Non** per indicare che non si ha accesso al cluster remoto.
6. Selezionare una **Modalità di replicazione** dall'elenco:
 - **In tempo reale (asincrono)**: le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.

- **In tempo reale (sincrono):** le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
- **Solo snapshot:** vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.

7. Fare clic su **Genera chiave**.



Questa azione genera una chiave di testo per l'associazione e crea una coppia di volumi non configurati sul cluster locale. Se non si completa la procedura, sarà necessario eliminare manualmente la coppia di volumi.

8. Copia la chiave di associazione negli appunti del tuo computer.

9. Rendere la chiave di associazione accessibile all'amministratore del cluster nel sito remoto del cluster.



La chiave di associazione del volume deve essere trattata in modo sicuro e non utilizzata in un modo che possa consentire un accesso accidentale o non protetto.



Non modificare nessuno dei caratteri nella chiave di associazione. La chiave diventa non valida se viene modificata.

10. Nell'interfaccia utente dell'elemento del cluster remoto, selezionare **Gestione > Volumi**.

11. Fare clic sull'icona Azioni per il volume che si desidera associare.

12. Fare clic su **Associa**.

13. Nella finestra di dialogo **Volume di associazione**, selezionare **Completa associazione**.

14. Incolla la chiave di associazione dall'altro cluster nella casella **Chiave di associazione**.

15. Fare clic su **Completa associazione**.

Dopo aver confermato l'associazione, i due cluster avviano il processo di connessione dei volumi per l'associazione. Durante il processo di associazione, è possibile visualizzare i messaggi nella colonna **Stato volume** della finestra **Coppie di volumi**. La coppia di volumi viene visualizzata `PausedMisconfigured` finché non vengono assegnate la coppia di volumi sorgente e destinazione.

Dopo aver completato correttamente l'associazione, si consiglia di aggiornare la tabella Volumi per rimuovere l'opzione **Associa** dall'elenco **Azioni** per il volume associato. Se non si aggiorna la tabella, l'opzione **Coppia** rimane disponibile per la selezione. Se si seleziona nuovamente l'opzione **Associa**, si apre una nuova scheda e poiché il volume è già associato, il sistema segnala un `StartVolumePairing Failed: xVolumeAlreadyPaired` messaggio di errore nella finestra **Volume coppia** della pagina Element UI.

Trova maggiori informazioni

- [Messaggi di associazione del volume](#)
- [Avvisi di associazione del volume](#)
- [Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati](#)

Assegnare un'origine e una destinazione di replicazione ai volumi accoppiati

Dopo aver associato i volumi, è necessario assegnare un volume di origine e il relativo

volume di destinazione della replica. Un'origine o una destinazione di replicazione può essere uno qualsiasi dei volumi di una coppia di volumi. È possibile utilizzare questa procedura anche 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 sia più disponibile.

Cosa ti servirà

Hai accesso ai cluster contenenti i volumi di origine e di destinazione.

Passi

1. Preparare il volume sorgente:

- Dal cluster che contiene il volume che si desidera assegnare come origine, selezionare **Gestione > Volumi**.
- Fare clic sull'icona **Azioni** per il volume che si desidera assegnare come origine e fare clic su **Modifica**.
- Nell'elenco a discesa **Accesso**, selezionare **Lettura/Scrittura**.



Se si inverte l'assegnazione di origine e destinazione, questa azione farà sì che la coppia di volumi visualizzi il seguente messaggio finché non verrà assegnata una nuova destinazione di replica: `PausedMisconfigured`

La modifica dell'accesso interrompe la replicazione del volume e causa l'interruzione della trasmissione dei dati. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

- Fare clic su **Salva modifiche**.

2. Preparare il volume di destinazione:

- Dal cluster che contiene il volume che si desidera assegnare come destinazione, selezionare **Gestione > Volumi**.
- Fare clic sull'icona Azioni per il volume che si desidera assegnare come destinazione e fare clic su **Modifica**.
- Nell'elenco a discesa **Accesso**, selezionare **Destinazione replica**.



Se si assegna un volume esistente come destinazione di replica, i dati su quel volume verranno sovrascritti. Dovresti utilizzare un nuovo volume di destinazione che non contenga dati e abbia le stesse caratteristiche del volume di origine, come dimensioni, impostazione 512e e configurazione QoS. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.

- Fare clic su **Salva modifiche**.

Trova maggiori informazioni

- [Abbinare i volumi utilizzando un ID volume](#)
- [Abbinare i volumi utilizzando una chiave di associazione](#)

Convalida la replica del volume

Dopo aver replicato un volume, è necessario assicurarsi che i volumi di origine e di destinazione siano attivi. Quando sono in stato attivo, i volumi vengono accoppiati, i dati

vengono inviati dal volume di origine a quello di destinazione e i dati sono sincronizzati.

1. Da entrambi i cluster, selezionare **Protezione dati > Coppie di volumi**.
2. Verificare che lo stato del volume sia Attivo.

Trova maggiori informazioni

[Avvisi di associazione del volume](#)

Elimina una relazione di volume dopo la replica

Una volta completata la replica e non più necessaria la relazione tra coppie di volumi, è possibile eliminare la relazione tra volumi.

1. Selezionare **Protezione dati > Coppie di volumi**.
2. Fare clic sull'icona **Azioni** relativa alla coppia di volumi che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Gestire le relazioni di volume

Sospendi la replicazione

È possibile sospendere manualmente la replicazione se è necessario interrompere l'elaborazione I/O per un breve periodo. Potrebbe essere necessario sospendere la replicazione in caso di aumento dell'elaborazione I/O e se si desidera ridurre il carico di elaborazione.

1. Selezionare **Protezione dati > Coppie di volumi**.
2. Fare clic sull'icona Azioni per la coppia di volumi.
3. Fare clic su **Modifica**.
4. Nel riquadro **Modifica coppia di volumi**, sospendere manualmente il processo di replica.



La sospensione o la ripresa manuale della replicazione del volume determina l'interruzione o la ripresa della trasmissione dei dati. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Salva modifiche**.

Cambia la modalità di replicazione

È possibile modificare le proprietà della coppia di volumi per cambiare la modalità di replica della relazione tra coppie di volumi.

1. Selezionare **Protezione dati > Coppie di volumi**.
2. Fare clic sull'icona Azioni per la coppia di volumi.
3. Fare clic su **Modifica**.
4. Nel riquadro **Modifica coppia di volumi**, seleziona una nuova modalità di replica:

- **In tempo reale (asincrono):** le scritture vengono riconosciute al client dopo essere state eseguite sul cluster di origine.
- **In tempo reale (sincrono):** le scritture vengono riconosciute al client dopo essere state eseguite sia sul cluster di origine che su quello di destinazione.
- **Solo snapshot:** vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate. **Attenzione:** La modifica della modalità di replicazione modifica immediatamente la modalità. Assicuratevi di aver coordinato queste modifiche in entrambi i siti.

5. Fare clic su **Salva modifiche**.

Elimina coppie di volumi

È possibile eliminare una coppia di volumi se si desidera rimuovere un'associazione di coppia tra due volumi.

1. Selezionare **Protezione dati > Coppie di volumi**.
2. Fare clic sull'icona Azioni relativa alla coppia di volumi che si desidera eliminare.
3. Fare clic su **Elimina**.
4. Conferma il messaggio.

Elimina una coppia di cluster

È possibile eliminare una coppia di cluster dall'interfaccia utente dell'elemento di uno qualsiasi dei cluster nella coppia.

1. Fare clic su **Protezione dati > Coppie cluster**.
2. Fare clic sull'icona Azioni per una coppia di cluster.
3. Nel menu che si apre, fare clic su **Elimina**.
4. Conferma l'azione.
5. Ripetere i passaggi dal secondo cluster nell'associazione di cluster.

Dettagli della coppia di cluster

La pagina Coppie di cluster nella scheda Protezione dati fornisce informazioni sui cluster che sono stati associati o che sono in fase di associazione. Il sistema visualizza messaggi di associazione e di avanzamento nella colonna Stato.

- **ID**

Un ID generato dal sistema assegnato a ciascuna coppia di cluster.

- **Nome del cluster remoto**

Il nome dell'altro cluster nella coppia.

- **MVIP remoto**

L'indirizzo IP virtuale di gestione dell'altro cluster nella coppia.

- **Stato**

Stato di replicazione del cluster remoto

- **Replica dei volumi**

Numero di volumi contenuti nel cluster che vengono accoppiati per la replica.

- **UUID**

Un ID univoco assegnato a ciascun cluster nella coppia.

Coppie di volumi

Dettagli della coppia di volumi

La pagina Coppie di volumi nella scheda Protezione dati fornisce informazioni sui volumi che sono stati associati o sono in fase di associazione. Il sistema visualizza messaggi di associazione e di avanzamento nella colonna Stato volume.

- **ID**

ID generato dal sistema per il volume.

- **Nome**

Nome dato al volume al momento della sua creazione. I nomi dei volumi possono contenere fino a 223 caratteri e contenere az, 0-9 e trattino (-).

- **Account**

Nome dell'account assegnato al volume.

- **Stato del volume**

Stato di replicazione del volume

- **Stato dell'istantanea**

Stato del volume snapshot.

- **Modalità**

Metodo di replicazione della scrittura del client. I valori possibili sono i seguenti:

- Asincrono
- Solo snapshot
- Sincronizzazione

- **Direzione**

La direzione dei dati del volume:

- Icona del volume sorgente (➡) indica che i dati vengono scritti su una destinazione esterna al cluster.

- Icona del volume di destinazione (🔍) indica che i dati vengono scritti sul volume locale da una fonte esterna.

- **Ritardo asincrono**

Intervallo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è abbinato, 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 del volume remoto**

Nome assegnato al volume remoto al momento della sua creazione.

Messaggi di associazione del volume

È possibile visualizzare i messaggi di associazione del volume durante il processo di associazione iniziale dalla pagina Coppie di volumi nella scheda Protezione dati. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia nella vista elenco dei volumi di replica.

- **PausaDisconnesso**

Timeout della replica di origine o delle RPC di sincronizzazione. La connessione al cluster remoto è stata persa. Controllare le connessioni di rete al cluster.

- **Ripresa della connessione**

La sincronizzazione della replica remota è ora attiva. Avvio del processo di sincronizzazione e attesa dei dati.

- **Ripresa di RRSync**

Viene creata una singola copia elicoidale dei metadati del volume nel cluster associato.

- **Ripresa della sincronizzazione locale**

Viene eseguita una copia a doppia elica dei metadati del volume nel cluster associato.

- **Ripresa del trasferimento dati**

Il trasferimento dei dati è ripreso.

- **Attivo**

I volumi vengono accoppiati e i dati vengono inviati dal volume di origine a quello di destinazione, sincronizzandoli.

- **Oziare**

Non si verifica alcuna attività di replicazione.

Avvisi di associazione del volume

La pagina Coppie di volumi nella scheda Protezione dati fornisce questi messaggi dopo aver associato i volumi. Questi messaggi possono essere visualizzati sia sull'estremità di origine che su quella di destinazione della coppia (salvo diversa indicazione) nella vista elenco dei volumi di replica.

- **PausedClusterFull**

Poiché il cluster di destinazione è pieno, la replicazione di origine e il trasferimento di dati in blocco non possono procedere. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedExceededMaxSnapshotCount**

Il volume di destinazione ha già il numero massimo di snapshot e non può replicare snapshot aggiuntivi.

- **PausaManuale**

Il volume locale è stato messo in pausa manualmente. È necessario riattivarla prima che la replicazione riprenda.

- **PausedManualRemote**

Il volume remoto è in modalità di pausa manuale. È necessario un intervento manuale per riattivare il volume remoto prima che la replica riprenda.

- **PausaNon configurato correttamente**

In attesa di una sorgente e di una destinazione attive. Per riprendere la replicazione è necessario un intervento manuale.

- **QoS in pausa**

La QoS di destinazione non è riuscita a sostenere l'I/O in entrata. La replicazione riprende automaticamente. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedSlowLink**

È stato rilevato un collegamento lento e la replica è stata interrotta. La replicazione riprende automaticamente. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **PausedVolumeSizeMismatch**

Il volume di destinazione non ha le stesse dimensioni del volume di origine.

- **PausedXCopy**

Un comando SCSI XCOPY viene inviato a un volume sorgente. Il comando deve essere completato prima che la replicazione possa riprendere. Il messaggio viene visualizzato solo sul lato sorgente della coppia.

- **ArrestatoNon configurato correttamente**

È stato rilevato un errore di configurazione permanente. Il volume remoto è stato eliminato o disaccoppiato. Non è possibile alcuna azione correttiva; è necessario stabilire un nuovo abbinamento.

Utilizzare la replica SnapMirror tra cluster Element e ONTAP (interfaccia utente Element)

Utilizzare la replica SnapMirror tra cluster Element e ONTAP (interfaccia utente Element)

È possibile creare relazioni SnapMirror dalla scheda Protezione dati nell'interfaccia utente NetApp Element . Per visualizzarlo nell'interfaccia utente, è necessario abilitare la funzionalità SnapMirror .

IPv6 non è supportato per la replica SnapMirror tra il software NetApp Element e i cluster ONTAP .

["Video NetApp : SnapMirror per NetApp HCI e Element Software"](#)

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare copie Snapshot con i sistemi NetApp ONTAP . Il motivo principale per cui si utilizza questa tecnologia è il ripristino di emergenza di NetApp HCI su ONTAP. Gli endpoint includono ONTAP, ONTAP Select e Cloud Volumes ONTAP. Vedere TR-4641 Protezione dei dati NetApp HCI .

["Rapporto tecnico NetApp 4641: Protezione dei dati NetApp HCI"](#)

Trova maggiori informazioni

- ["Creazione del tuo Data Fabric con NetApp HCI, ONTAP e Converged Infrastructure"](#)
- ["Replica tra NetApp Element Software e ONTAP \(ONTAP CLI\)"](#)

Panoramica SnapMirror

I sistemi che eseguono il software NetApp Element supportano la funzionalità SnapMirror per copiare e ripristinare snapshot con i sistemi NetApp ONTAP .

I sistemi che eseguono Element possono comunicare direttamente con SnapMirror sui sistemi ONTAP 9.3 o versioni successive. L'API 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 SnapMirror tra il software Element e i sistemi ONTAP .

È possibile replicare i volumi originati ONTAP nei volumi Element in casi d'uso specifici con funzionalità limitate. Per maggiori informazioni, vedere ["Replica tra il software Element e ONTAP \(ONTAP CLI\)"](#).

Abilita SnapMirror sul cluster

È necessario abilitare manualmente la funzionalità SnapMirror a livello di cluster tramite l'interfaccia utente NetApp Element . Il sistema è dotato di funzionalità SnapMirror disabilitata per impostazione predefinita e non viene abilitata automaticamente come parte di una nuova installazione o di un aggiornamento. L'abilitazione della funzionalità SnapMirror è un'operazione di configurazione che va eseguita una sola volta.

SnapMirror può essere abilitato solo per i cluster che eseguono il software Element utilizzato insieme ai volumi su un sistema NetApp ONTAP . È necessario abilitare la funzionalità SnapMirror solo se il cluster è connesso

per l'uso con volumi NetApp ONTAP .

Cosa ti servirà

Il cluster di storage deve eseguire il software NetApp Element .

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Trova le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Abilita SnapMirror**.



L'abilitazione della funzionalità SnapMirror modifica in modo permanente la configurazione del software Element. È possibile disattivare la funzionalità SnapMirror e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica.

4. Fare clic su **Sì** per confermare la modifica alla configurazione SnapMirror .

Abilita SnapMirror sul volume

È necessario abilitare SnapMirror sul volume nell'interfaccia utente di Element. Ciò consente la replica dei dati su volumi ONTAP specificati. Si tratta dell'autorizzazione concessa dall'amministratore del cluster che esegue il software NetApp Element affinché SnapMirror controlli un volume.

Cosa ti servirà

- Hai abilitato SnapMirror nell'interfaccia utente Element per il cluster.
- È disponibile un endpoint SnapMirror .
- Il volume deve avere una dimensione di blocco di 512e.
- Il volume non partecipa alla replica remota.
- Il tipo di accesso al volume non è Destinazione replica.



È possibile impostare questa proprietà anche durante la creazione o la clonazione di un volume.

Passi

1. Fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona **Azioni** per il volume per cui si desidera abilitare SnapMirror .
3. Nel menu che si apre, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica volume**, selezionare la casella di controllo **Abilita SnapMirror**.
5. Fare clic su **Salva modifiche**.

Crea un endpoint SnapMirror

Prima di poter creare una relazione, è necessario creare un endpoint SnapMirror nell'interfaccia utente NetApp Element .

Un endpoint SnapMirror è un cluster ONTAP che funge da destinazione di replica per un cluster che esegue il software Element. Prima di creare una relazione SnapMirror , è necessario creare un endpoint SnapMirror .

È possibile creare e gestire fino a quattro endpoint SnapMirror su un cluster di archiviazione 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 tramite l'API Element.

Per i dettagli sui metodi API, vedere ["Gestisci l'archiviazione con l'API Element"](#).

Cosa ti servirà

- Dovresti aver abilitato SnapMirror nell'interfaccia utente di Element per il cluster di archiviazione.
- Conosci le credenziali ONTAP per l'endpoint.

Passi

1. Fare clic su **Protezione dati** > *Endpoint SnapMirror*.
2. Fare clic su **Crea endpoint**.
3. Nella finestra di dialogo **Crea un nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster del sistema ONTAP .
4. Immettere le credenziali di amministratore ONTAP associate all'endpoint.
5. Esaminare i dettagli aggiuntivi:
 - LIF: elenca le interfacce logiche intercluster ONTAP utilizzate per comunicare con Element.
 - Stato: mostra lo stato corrente dell'endpoint SnapMirror . I valori possibili sono: connesso, disconnesso e non gestito.
6. Fare clic su **Crea endpoint**.

Crea una relazione SnapMirror

È necessario creare una relazione SnapMirror nell'interfaccia utente NetApp Element .



Se un volume non è ancora abilitato per SnapMirror e si sceglie di creare una relazione dall'interfaccia utente dell'elemento, SnapMirror viene automaticamente abilitato su quel volume.

Cosa ti servirà

SnapMirror è abilitato sul volume.

Passi

1. Fare clic su **Gestione** > **Volumi**.
2. Fare clic sull'icona **Azioni** per il volume che deve far parte della relazione.
3. Fare clic su *Crea una relazione SnapMirror*.
4. Nella finestra di dialogo **Crea una relazione SnapMirror***, **seleziona 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 la **Macchina virtuale di archiviazione** per questa relazione.
- b. Selezionare **Aggregato** dall'elenco a discesa.
- c. Nel campo **Suffisso nome volume**, immettere un suffisso.



Il sistema rileva il nome del volume di origine e lo copia nel campo **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 **Usa volume esistente**.
 - a. Selezionare la **Macchina virtuale di archiviazione** per questa relazione.
 - b. Selezionare il volume di destinazione per questa nuova relazione.
8. Nella sezione **Dettagli relazione**, seleziona una policy. Se il criterio selezionato ha regole di mantenimento, la tabella Regole visualizza le regole e le etichette associate.
9. **Facoltativo**: seleziona una pianificazione.

Ciò determina la frequenza con cui la relazione crea copie.

10. **Facoltativo**: Nel campo **Limita larghezza di banda a**, immettere la quantità massima di larghezza di banda che può essere utilizzata dai trasferimenti di dati associati a questa relazione.
11. Esaminare i dettagli aggiuntivi:
 - **Stato**: Stato attuale della relazione del volume di destinazione. I valori possibili sono:
 - 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 SnapMirror.
 - interrotto: il volume di destinazione è in lettura/scrittura e sono presenti snapshot.
 - **Stato**: Stato attuale della relazione. I valori possibili sono idle, transferring, checking, quiescing, quiesced, queued, preparing, finalizing, aborting e breaking.
 - **Tempo di ritardo**: quantità di tempo in secondi per cui il sistema di destinazione è in ritardo rispetto al sistema di origine. Il tempo di ritardo non deve essere superiore all'intervallo di pianificazione del trasferimento.
 - **Limite di larghezza di banda**: la quantità massima di larghezza di banda che può essere consumata dai trasferimenti di dati associati a questa relazione.
 - **Ultimo trasferimento**: timestamp dell'ultimo snapshot trasferito. Clicca per ulteriori informazioni.
 - **Nome policy**: il nome della policy ONTAP SnapMirror per la relazione.
 - **Tipo di policy**: tipo di policy ONTAP SnapMirror selezionata per la relazione. I valori possibili sono:
 - specchio asincrono
 - specchio_vault
 - **Nome pianificazione**: Nome della pianificazione preesistente sul sistema ONTAP selezionato per questa relazione.
12. Per non inizializzare in questo momento, assicurarsi che la casella di controllo **Inizializza** non sia selezionata.



L'inizializzazione può richiedere molto tempo. Potrebbe essere opportuno eseguirlo durante le ore non di punta. L'inizializzazione esegue un trasferimento di base; crea una copia snapshot del volume di origine, quindi trasferisce tale copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione. È possibile inizializzare manualmente oppure utilizzare una pianificazione per avviare il processo di inizializzazione (e gli aggiornamenti successivi) in base alla pianificazione.

13. Fare clic su **Crea relazione**.

14. Fare clic su **Protezione dati** > *Relazioni SnapMirror * per visualizzare questa nuova relazione SnapMirror

Azioni di relazione SnapMirror

È possibile configurare una relazione dalla pagina Relazioni SnapMirror della scheda Protezione dati. Qui vengono descritte le opzioni dell'icona Azioni.

- **Modifica:** modifica la policy utilizzata o la pianificazione per la relazione.
- **Elimina:** elimina la relazione SnapMirror . Questa funzione non elimina il volume di destinazione.
- **Inizializza:** esegue il primo trasferimento iniziale di dati di base per stabilire una nuova relazione.
- **Aggiorna:** esegue un aggiornamento su richiesta della relazione, replicando tutti i nuovi dati e le copie Snapshot inclusi dall'ultimo aggiornamento alla destinazione.
- **Quiesce:** impedisce ulteriori aggiornamenti per una relazione.
- **Riprendi:** Riprende una relazione sospesa.
- **Break:** imposta il volume di destinazione in lettura-scrittura e interrompe tutti i trasferimenti correnti e futuri. Verificare che i client non stiano utilizzando il volume sorgente originale, perché l'operazione di risincronizzazione inversa rende il volume sorgente originale di sola lettura.
- **Risincronizzazione:** ripristina una relazione interrotta nella stessa direzione prima che si verificasse l'interruzione.
- **Risincronizzazione inversa:** automatizza i passaggi necessari per creare e inizializzare una nuova relazione nella direzione opposta. Ciò è possibile solo se la relazione esistente è in uno stato di interruzione. Questa operazione non eliminerà la relazione corrente. Il volume di origine originale torna alla copia Snapshot comune più recente e si risincronizza con la destinazione. Tutte le modifiche apportate al volume sorgente originale dall'ultimo aggiornamento SnapMirror riuscito andranno perse. Tutte le modifiche apportate o i nuovi dati scritti nel volume di destinazione corrente vengono rispediti al volume di origine originale.
- **Annulla:** annulla un trasferimento in corso. Se viene emesso un aggiornamento SnapMirror per una relazione interrotta, la relazione continua con l'ultimo trasferimento dall'ultimo checkpoint di riavvio creato prima dell'interruzione.

Etichette SnapMirror

Etichette SnapMirror

Un'etichetta SnapMirror funge da marcatore 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 SnapMirror . Il ruolo della relazione è quello di far rispettare le regole durante il trasferimento dei dati selezionando lo

snapshot etichettato corrispondente, copiandolo nel volume di destinazione e assicurando che venga conservato il numero corretto di copie. Si riferisce alla politica per determinare il conteggio dei dati da conservare e il periodo di conservazione. La policy 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 viene applicata allo snapshot, allo snapshot di gruppo o alla pianificazione selezionati.

Aggiungi etichette SnapMirror agli snapshot

Le etichette SnapMirror specificano i criteri di conservazione degli snapshot sull'endpoint SnapMirror . È possibile aggiungere etichette agli snapshot e agli snapshot di gruppo.

È possibile visualizzare le etichette disponibili da una finestra di dialogo di relazione SnapMirror esistente o da NetApp ONTAP System Manager.



Quando si aggiunge un'etichetta a uno snapshot di gruppo, tutte le etichette esistenti nei singoli snapshot vengono sovrascritte.

Cosa ti servirà

- SnapMirror è abilitato sul cluster.
- L'etichetta che vuoi aggiungere esiste già in ONTAP.

Passi

1. Fare clic sulla pagina **Protezione dati > Snapshot o Snapshot di gruppo**.
2. Fare clic sull'icona **Azioni** per lo snapshot o lo snapshot di gruppo a cui si desidera aggiungere un'etichetta SnapMirror .
3. Nella finestra di dialogo **Modifica istantanea**, immettere il testo nel campo *Etichetta SnapMirror *. L'etichetta deve corrispondere a un'etichetta di regola nel criterio applicato alla relazione SnapMirror .
4. Fare clic su **Salva modifiche**.

Aggiungere etichette SnapMirror alle pianificazioni degli snapshot

È possibile aggiungere etichette SnapMirror alle pianificazioni degli snapshot per garantire che venga applicata una policy SnapMirror . È possibile visualizzare le etichette disponibili da una finestra di dialogo di relazione SnapMirror esistente o da NetApp ONTAP System Manager.

Cosa ti servirà

- SnapMirror deve essere abilitato a livello di cluster.
- L'etichetta che vuoi aggiungere esiste già in ONTAP.

Passi

1. Fare clic su **Protezione dati > Pianificazioni**.
2. Aggiungere un'etichetta SnapMirror a una pianificazione in uno dei seguenti modi:

Opzione	Passi
Creazione di un nuovo programma	a. Seleziona Crea pianificazione . b. Inserisci tutti gli altri dettagli rilevanti. c. Seleziona Crea pianificazione .
Modifica della pianificazione esistente	a. Fare clic sull'icona Azioni per la pianificazione a cui si desidera aggiungere un'etichetta e selezionare Modifica . b. Nella finestra di dialogo visualizzata, immettere il testo nel campo *Etichetta SnapMirror *. c. Selezionare Salva modifiche .

Trova maggiori informazioni

[Creare una pianificazione snapshot](#)

Ripristino di emergenza tramite SnapMirror

Ripristino di emergenza tramite 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 ed eseguire il failover sul volume di destinazione.



Se il cluster originale è completamente guasto o non esiste più, contattare l'assistenza NetApp per ulteriore assistenza.

Eseguire un failover da un cluster Element

È possibile eseguire un failover dal cluster Element per rendere il volume di destinazione accessibile in lettura/scrittura agli host sul lato di destinazione. Prima di eseguire un failover dal cluster Element, è necessario interrompere la relazione SnapMirror .

Utilizzare l'interfaccia utente NetApp Element per eseguire il failover. Se l'interfaccia utente dell'elemento non è disponibile, è possibile utilizzare anche ONTAP System Manager o ONTAP CLI per emettere il comando di interruzione della relazione.

Cosa ti servirà

- Esiste una relazione SnapMirror e sul volume di destinazione è presente almeno uno snapshot valido.
- È necessario effettuare il failover sul volume di destinazione a causa di un'interruzione imprevista o di un evento pianificato nel sito principale.

Passi

1. Nell'interfaccia utente dell'elemento, fare clic su **Protezione dati** > *Relazioni SnapMirror *.
2. Trova la relazione con il volume di origine di cui vuoi eseguire il failover.
3. Fare clic sull'icona **Azioni**.

4. Fare clic su **Interruzione**.
5. Conferma l'azione.

Il volume sul cluster di destinazione ora ha accesso in lettura/scrittura e può essere montato sugli host dell'applicazione per riprendere i carichi di lavoro di produzione. A seguito di questa azione, tutte le repliche SnapMirror vengono interrotte. La relazione mostra uno stato di rottura.

Eseguire un failback su Element

Scopri come eseguire un failback su Element

Una volta mitigato il problema sul lato primario, è necessario risincronizzare il volume di origine ed eseguire il failback sul software NetApp Element . I passaggi da eseguire variano a seconda che il volume di origine esista ancora o che sia necessario eseguire il failback su un volume appena creato.

Scenari di failback SnapMirror

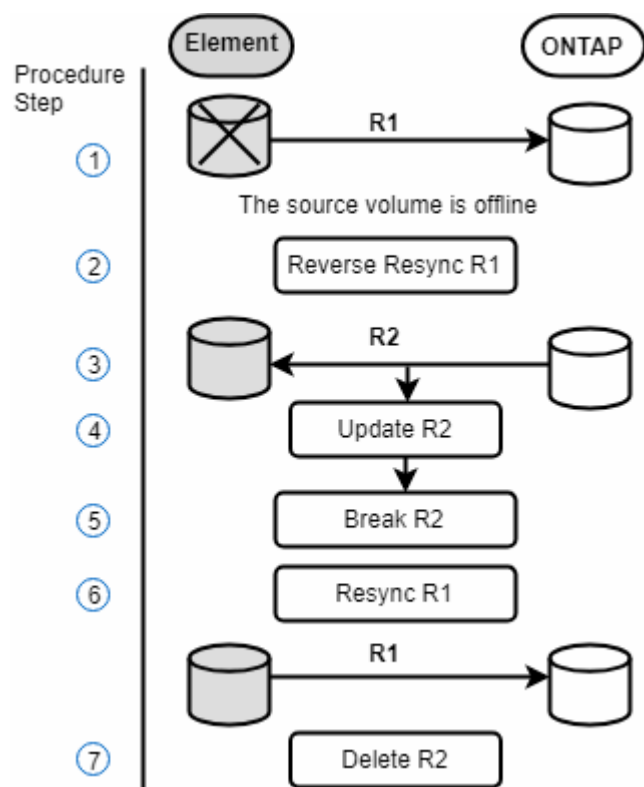
La funzionalità di disaster recovery SnapMirror è illustrata in due scenari di failback. Questi presuppongono che la relazione originale sia stata interrotta (interrotta).

I passaggi delle procedure corrispondenti sono aggiunti a titolo di riferimento.

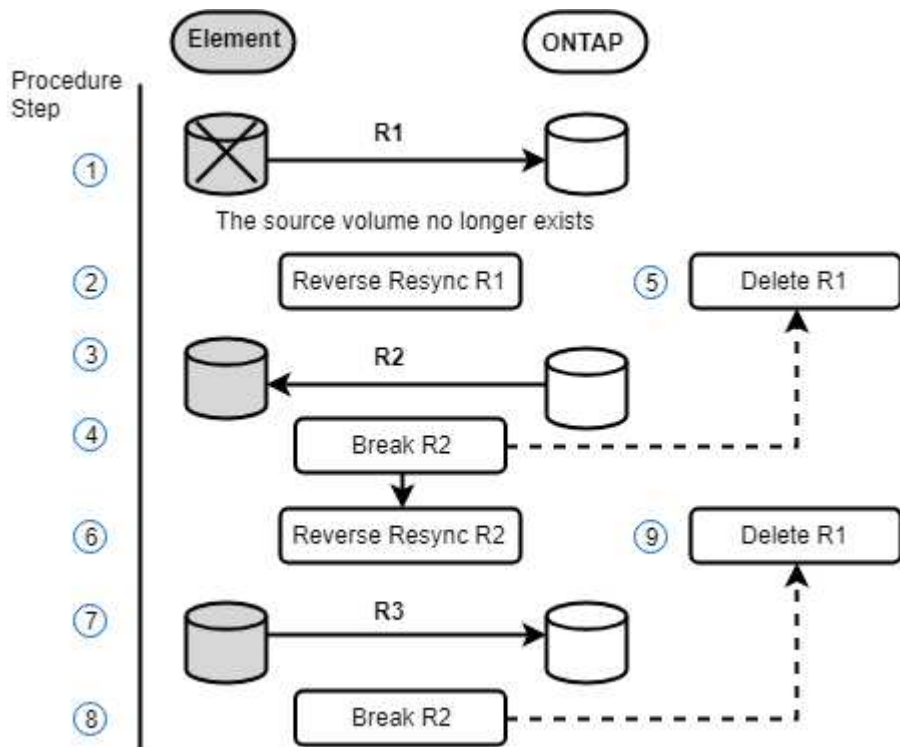


Negli esempi qui riportati, R1 = la relazione originale in cui il cluster che esegue il software NetApp Element è il volume di origine originale (Element) e ONTAP è il volume di destinazione originale (ONTAP). R2 e R3 rappresentano le relazioni inverse create tramite l'operazione di risincronizzazione inversa.

L'immagine seguente mostra lo scenario di failback quando il volume di origine esiste ancora:



L'immagine seguente mostra lo scenario di failback quando il volume di origine non esiste più:



Trova maggiori 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 SnapMirror](#)

Eseguire un failback quando il volume di origine esiste ancora

È possibile risincronizzare il volume di origine originale ed eseguire il failback utilizzando l'interfaccia utente NetApp Element . Questa procedura si applica agli scenari in cui il volume sorgente originale esiste ancora.

1. Nell'interfaccia utente dell'elemento, individua la relazione che hai interrotto per eseguire il failover.
2. Fare clic sull'icona Azioni e quindi su **Risincronizzazione inversa**.
3. Conferma l'azione.



L'operazione di risincronizzazione inversa crea una nuova relazione in cui i ruoli dei volumi di origine e di destinazione originali vengono invertiti (ciò determina due relazioni poiché la relazione originale persiste). Tutti i nuovi dati dal volume di destinazione originale vengono trasferiti al volume di origine originale come parte dell'operazione di risincronizzazione inversa. È possibile continuare ad accedere e scrivere dati sul volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host dal volume di origine ed eseguire un aggiornamento SnapMirror prima di reindirizzare al volume primario originale.

4. Fare clic sull'icona Azioni della relazione inversa appena creata e fare clic su **Aggiorna**.

Ora che hai completato la risincronizzazione inversa e verificato che non ci sono sessioni attive connesse al volume sul lato di destinazione e che i dati più recenti si trovano sul volume primario originale, puoi eseguire i seguenti passaggi per completare il failback e riattivare il volume primario originale:

5. Fare clic sull'icona Azioni della relazione inversa e fare clic su **Interrompi**.
6. Fare clic sull'icona Azioni della relazione originale e fare clic su **Risincronizza**.



Ora è possibile montare il volume primario originale per riprendere i carichi di lavoro di produzione sul volume primario originale. La replica SnapMirror originale riprende in base ai criteri e alla pianificazione configurati per la relazione.

7. Dopo aver confermato che lo stato della relazione originale è “snapmirrored”, fare clic sull'icona Azioni della relazione inversa e fare clic su **Elimina**.

Trova maggiori informazioni

[Scenari di failback SnapMirror](#)

Eseguire un failback quando il volume di origine non esiste più

È possibile risincronizzare il volume di origine originale ed eseguire il failback utilizzando l'interfaccia utente NetApp Element . Questa sezione si applica agli scenari in cui il volume sorgente originale è andato perso ma il cluster originale è ancora intatto. Per istruzioni su come ripristinare un nuovo cluster, consultare la documentazione sul sito di supporto NetApp .

Cosa ti servirà

- Si è verificata un'interruzione della relazione di replica tra i volumi Element e ONTAP .
- Il volume Element è irrimediabilmente perso.
- Il nome del volume originale risulta NON TROVATO.

Passi

1. Nell'interfaccia utente dell'elemento, individua la relazione che hai interrotto per eseguire il failover.

Migliore pratica: prendi nota della politica SnapMirror e pianifica i dettagli della relazione interrotta originariamente. Queste informazioni saranno necessarie per ricreare la relazione.

2. Fare clic sull'icona **Azioni** e quindi su **Risincronizzazione inversa**.
3. Conferma 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 (ciò determina due relazioni poiché la relazione originale persiste). Poiché il volume originale non esiste più, il sistema crea un nuovo volume Element con lo stesso nome e le stesse dimensioni del volume di origine originale. Al nuovo volume viene assegnata una policy QoS predefinita denominata sm-recovery ed è associato a un account predefinito denominato sm-recovery. Sarà necessario modificare manualmente l'account e la policy QoS per tutti i volumi creati da SnapMirror per sostituire i volumi di origine originali che sono stati 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 dati sul volume attivo sul lato di destinazione, ma sarà necessario disconnettere tutti gli host dal volume attivo ed eseguire un aggiornamento 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 passaggi seguenti 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 **Interrompi**.
5. Fare clic sull'icona **Azioni** della relazione originale, in cui il volume di origine non esiste, e fare clic su **Elimina**.
6. Fare clic sull'icona **Azioni** della relazione inversa, che è stata interrotta nel passaggio 4, e fare clic su **Risincronizzazione inversa**.
7. In questo modo si invertono l'origine e la destinazione e si ottiene una relazione con lo stesso volume di origine e lo stesso volume di destinazione della relazione originale.
8. Fare clic sull'icona **Azioni** e su **Modifica** per aggiornare questa relazione con le impostazioni di pianificazione e i criteri QoS originali di cui si è preso nota.
9. Ora è possibile eliminare in sicurezza la relazione inversa che hai risincronizzato al passaggio 6.

Trova maggiori informazioni

[Scenari di failback 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 archiviazione ONTAP può fungere da origine e Element da destinazione.

- Esistono due scenari:
 - Non esiste alcuna relazione precedente di disaster recovery. Seguire tutti i passaggi di questa procedura.
 - Esiste una precedente relazione di disaster recovery, ma non tra i volumi utilizzati per questa mitigazione. In questo caso, seguire solo i passaggi 3 e 4 riportati di seguito.

Cosa ti servirà

- Il nodo di destinazione dell'elemento deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror.

È necessario specificare il percorso di destinazione dell'elemento nel formato `hostip:/lun/<id_number>`, dove `lun` è la stringa effettiva "lun" e `id_number` è l'ID del volume dell'elemento.

Passi

1. Utilizzando ONTAP, creare la relazione con il cluster Element:

```
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 ONTAP `snapmirror show`.

Per informazioni sulla creazione di una relazione di replica, consultare la documentazione ONTAP e per la sintassi completa dei comandi, consultare la pagina `man ONTAP`.

3. Utilizzando il `ElementCreateVolume` API, crea il volume di destinazione e imposta la modalità di accesso al volume di destinazione su SnapMirror:

Crea 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 replicazione utilizzando ONTAP `snapmirror initialize` comando:

```
snapmirror initialize -source-path hostip:/lun/name
-destination-path SVM:volume|cluster://SVM/volume
```

Replica tra il software NetApp Element e ONTAP (ONTAP CLI)

Panoramica della replica tra il software NetApp Element e ONTAP (ONTAP CLI)

È possibile garantire la continuità aziendale su un sistema Element utilizzando

SnapMirror per replicare copie snapshot di un volume Element su una destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP e quindi riattivare il sistema Element quando il servizio viene ripristinato.

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un nodo ONTAP su un sistema Element. Potresti aver creato una LUN durante un'interruzione nel sito Element oppure potresti utilizzare una LUN per migrare i dati da ONTAP al software Element.

Dovresti utilizzare il backup Element to ONTAP se si verificano le seguenti condizioni:

- È meglio utilizzare le best practice, non esplorare tutte le opzioni disponibili.
- Si desidera utilizzare l'interfaccia della riga di comando (CLI) ONTAP , non System Manager o uno strumento di scripting automatizzato.
- Si utilizza iSCSI per fornire dati ai client.

Se hai bisogno di ulteriori informazioni sulla configurazione o concettuali SnapMirror , vedi ["Panoramica sulla protezione dei dati"](#) .

Informazioni sulla replica tra Element e ONTAP

A partire da ONTAP 9.3, è possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element in una destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un nodo ONTAP su un sistema Element. Potresti aver creato una LUN durante un'interruzione nel sito Element oppure potresti utilizzare una LUN per migrare i dati da ONTAP al software Element.

Tipi di rapporto di protezione dei dati

SnapMirror offre due tipi di rapporto di protezione dei dati. Per ogni tipo, SnapMirror crea una copia snapshot del volume sorgente dell'elemento prima di inizializzare o aggiornare la relazione:

- In una relazione di protezione dei dati di *disaster recovery (DR)*, il volume di destinazione contiene solo la copia snapshot creata da SnapMirror, dalla quale è possibile continuare a fornire dati in caso di catastrofe nel sito primario.
- In una relazione di protezione dei dati con *conservazione a lungo termine*, il volume di destinazione contiene copie snapshot point-in-time create dal software Element, nonché la copia snapshot creata da SnapMirror. Ad esempio, potresti voler conservare copie mensili degli snapshot creati in un arco di tempo di 20 anni.

Politiche predefinite

La prima volta che si richiama SnapMirror, viene eseguito un *trasferimento di base* dal volume di origine al volume di destinazione. La policy *SnapMirror* definisce il contenuto della baseline e tutti gli aggiornamenti.

Quando si crea una relazione di protezione dei dati, è possibile utilizzare una policy predefinita o personalizzata. Il *tipo di policy* determina quali copie snapshot includere e quante copie conservare.

La tabella seguente mostra le policy predefinite. Utilizzare il *MirrorLatest* politica per creare una relazione DR tradizionale. Utilizzare il *MirrorAndVault* O *Unified7year* policy per creare una relazione di replica unificata, in cui DR e conservazione a lungo termine sono configurati sullo stesso volume di destinazione.

Politica	Tipo di polizza	Aggiorna il comportamento
MirrorLatest	specchio asincrono	Trasferisci la copia snapshot creata da SnapMirror.
MirrorAndVault	specchio-volta	Trasferisci la copia snapshot creata da SnapMirror e tutte le copie snapshot meno recenti create dall'ultimo aggiornamento, a condizione che abbiano etichette SnapMirror "giornaliera" o "settimanali".
Unified7year	specchio-volta	Trasferisci la copia snapshot creata da SnapMirror e tutte le copie snapshot meno recenti create dall'ultimo aggiornamento, a condizione che abbiano le etichette SnapMirror "giornaliera", "settimanale" o "mensile".



Per informazioni di base complete sulle policy SnapMirror , inclusa una guida su quale policy utilizzare, vedere ["Panoramica sulla protezione dei dati"](#) .

Informazioni sulle etichette SnapMirror

Ogni policy con tipo di policy "mirror-vault" deve avere una regola che specifica quali copie snapshot replicare. La regola "daily", ad esempio, indica che devono essere replicate solo le copie snapshot a cui è stata assegnata l'etichetta SnapMirror "daily". L'etichetta SnapMirror viene assegnata quando si configurano le copie snapshot di Element.

Replica da un cluster di origine Element a un cluster di destinazione ONTAP

È possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element su un sistema di destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

Un volume Element è più o meno equivalente a un LUN ONTAP . SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP . SnapMirror replica i dati su una LUN esistente se la LUN soddisfa i requisiti per la replica da Element a ONTAP .

Le regole di replicazione sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume Element.
- Non è possibile replicare i dati da un volume ONTAP a più volumi Element.

Replica da un cluster di origine ONTAP a un cluster di destinazione Element

A partire da ONTAP 9.4, è possibile replicare copie snapshot di una LUN creata su un sistema ONTAP su un volume Element:

- Se esiste già una relazione SnapMirror tra un'origine Element e una destinazione ONTAP , un LUN creato mentre si forniscono dati dalla destinazione viene replicato automaticamente quando l'origine viene riattivata.
- In caso contrario, è necessario creare e inizializzare una relazione SnapMirror tra il cluster di origine ONTAP e il cluster di destinazione Element.

Le regole di replicazione sono le seguenti:

- La relazione di replicazione deve avere una policy di tipo “async-mirror”.

I criteri di tipo “mirror-vault” non sono supportati.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Prerequisiti

Prima di configurare una relazione di protezione dei dati tra Element e ONTAP, è necessario aver completato le seguenti attività:

- Il cluster Element deve eseguire il software NetApp Element versione 10.1 o successiva.
- Il cluster ONTAP deve eseguire ONTAP 9.3 o versione successiva.
- SnapMirror deve essere concesso in licenza sul cluster ONTAP .
- È necessario aver configurato volumi sui cluster Element e ONTAP sufficientemente grandi da gestire i trasferimenti di dati previsti.
- Se si utilizza il tipo di criterio “mirror-vault”, è necessario che sia stata configurata un’etichetta SnapMirror per le copie snapshot dell’elemento da replicare.



Puoi eseguire questa attività solo in ["Interfaccia utente web del software Element"](#) o utilizzando il ["Metodi API"](#) .

- È necessario assicurarsi che la porta 5010 sia disponibile.
- Se si prevede di dover spostare un volume di destinazione, è necessario assicurarsi che esista una connettività full-mesh tra l’origine e la destinazione. Ogni nodo del cluster di origine Element deve essere in grado di comunicare con ogni nodo del cluster di destinazione ONTAP .

Dettagli di supporto

La tabella seguente mostra i dettagli del supporto per il backup da Element a ONTAP .

Risorsa o funzionalità	Dettagli di supporto

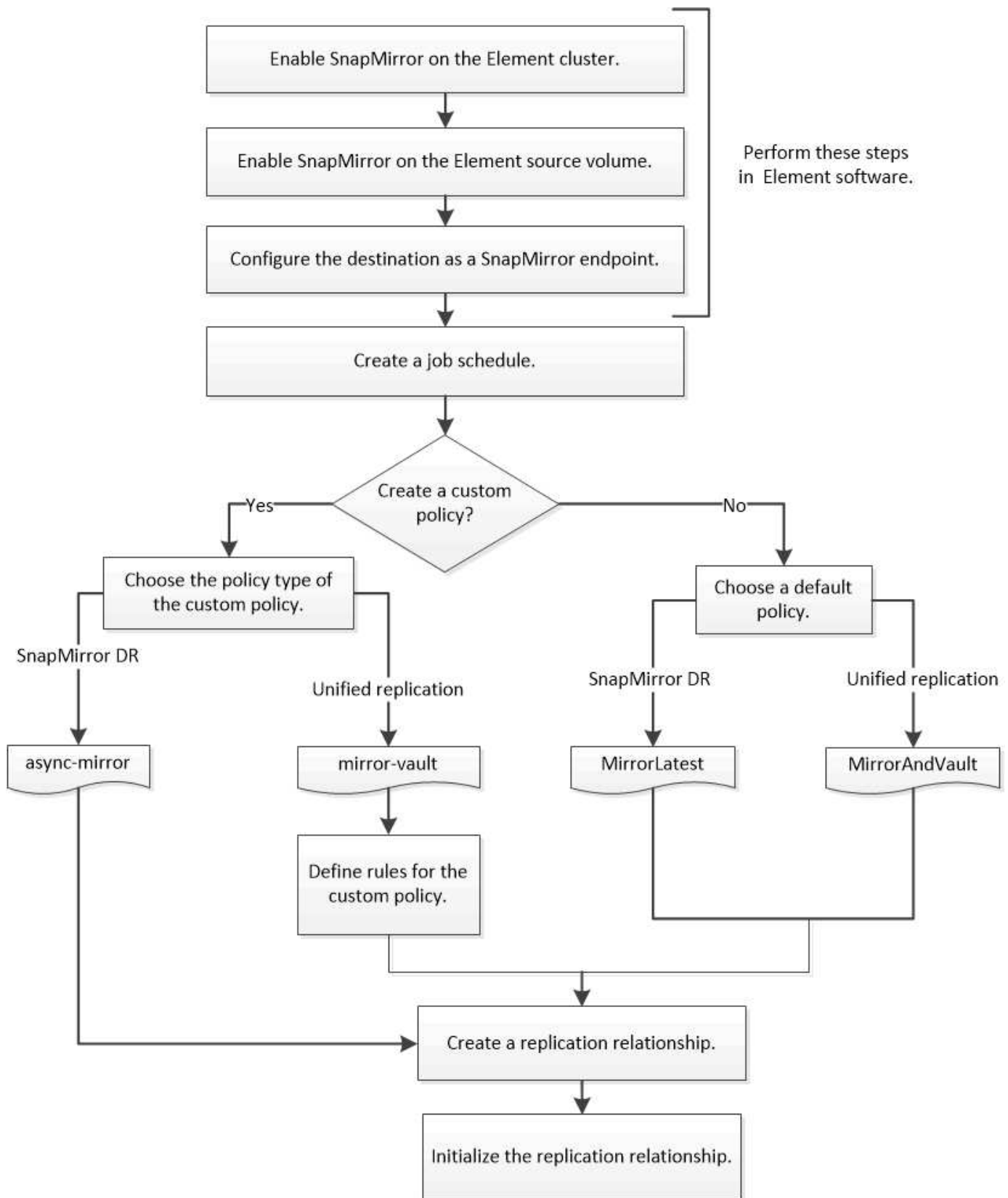
SnapMirror	• La funzione di ripristino SnapMirror non è supportata. • IL <code>MirrorAllSnapshots</code> E <code>XDPDefault</code> le policy non sono supportate. • Il tipo di criterio “vault” non è supportato. • La regola definita dal sistema “all_source_snapshots” non è supportata. • Il tipo di policy “mirror-vault” è supportato solo per la replica dal software Element a ONTAP. Utilizzare “async-mirror” per la replica da ONTAP al software Element. • IL <code>-schedule</code> E <code>-prefix</code> opzioni per <code>snapmirror policy add-rule</code> non sono supportati. • IL <code>-preserve</code> E <code>-quick-resync</code> opzioni per <code>snapmirror resync</code> non sono supportati. • L'efficienza di archiviazione non viene preservata. • Le distribuzioni di protezione dei dati a cascata e a fan-out non sono supportate.
ONTAP	• ONTAP Select è supportato a partire da ONTAP 9.4 ed Element 10.3. • Cloud Volumes ONTAP è supportato a partire da ONTAP 9.5 ed Element 11.0.
Elemento	• Il limite di dimensione del volume è 8 TiB. • La dimensione del blocco del volume deve essere 512 byte. Non è supportata una dimensione di blocco di 4K byte. • La dimensione del volume deve essere un multiplo di 1 MiB. • Gli attributi del volume non vengono conservati. • Il numero massimo di copie snapshot da replicare è 30.
Rete	• È consentita una singola connessione TCP per trasferimento. • Il nodo Elemento deve essere specificato come indirizzo IP. La ricerca del nome host DNS non è supportata. • Gli spazi IP non sono supportati.
SnapLock	I volumi SnapLock non sono supportati.
FlexGroup	I volumi FlexGroup non sono supportati.
SVM DR	I volumi ONTAP in una configurazione SVM DR non sono supportati.
MetroCluster	I volumi ONTAP in una configurazione MetroCluster non sono supportati.

Flusso di lavoro per la replica tra Element e ONTAP

Sia che si replichino dati da Element a ONTAP o da ONTAP a Element, è necessario

configurare una pianificazione dei processi, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare una policy predefinita o personalizzata.

Il flusso di lavoro presuppone che siano state completate le attività prerequisito elencate in ["Prerequisiti"](#) . Per informazioni di base complete sulle policy SnapMirror , inclusa una guida su quale policy utilizzare, vedere ["Panoramica sulla protezione dei dati"](#) .



Abilita SnapMirror nel software Element

Abilita SnapMirror sul cluster Element

È necessario abilitare SnapMirror sul cluster Element prima di poter creare una relazione

di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element o utilizzando ["Metodo API"](#).

Prima di iniziare

- Il cluster Element deve eseguire il software NetApp Element versione 10.1 o successiva.
- SnapMirror può essere abilitato solo per i cluster Element utilizzati con volumi NetApp ONTAP .

Informazioni su questo compito

Il sistema Element è dotato di SnapMirror disabilitato per impostazione predefinita. SnapMirror non viene abilitato automaticamente come parte di una nuova installazione o di un aggiornamento.



Una volta abilitato, SnapMirror non può essere disabilitato. È possibile disattivare la funzionalità SnapMirror e ripristinare le impostazioni predefinite solo restituendo il cluster all'immagine di fabbrica.

Passi

1. Fare clic su **Cluster > Impostazioni**.
2. Trova le impostazioni specifiche del cluster per SnapMirror.
3. Fare clic su **Abilita SnapMirror**.

Abilita SnapMirror sul volume sorgente dell'elemento

È necessario abilitare SnapMirror sul volume di origine Element prima di poter creare una relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software Element o utilizzando ["ModificaVolume"](#) E ["ModificaVolumi"](#) Metodi API.

Prima di iniziare

- È necessario aver abilitato SnapMirror sul cluster Element.
- La dimensione del blocco del volume deve essere di 512 byte.
- Il volume non deve partecipare alla replica remota di Element.
- Il tipo di accesso al volume non deve essere "Replication Target".

Informazioni su questo compito

La procedura seguente presuppone che il volume esista già. È anche possibile abilitare SnapMirror quando si crea o si clona un volume.

Passi

1. Selezionare **Gestione > Volumi**.
2. Seleziona il  pulsante per il volume.
3. Nel menu a discesa, seleziona **Modifica**.
4. Nella finestra di dialogo **Modifica volume**, seleziona **Abilita SnapMirror**.
5. Selezionare **Salva modifiche**.

Crea un endpoint SnapMirror

È necessario creare un endpoint SnapMirror prima di poter creare una relazione di replica. È possibile eseguire questa attività solo nell'interfaccia utente Web del software

Element o utilizzando ["Metodi API SnapMirror"](#).

Prima di iniziare

È necessario aver abilitato SnapMirror sul cluster Element.

Passi

1. Fare clic su **Protezione dati** > *Endpoint SnapMirror*.
2. Fare clic su **Crea endpoint**.
3. Nella finestra di dialogo **Crea un nuovo endpoint**, immettere l'indirizzo IP di gestione del cluster ONTAP .
4. Immettere l'ID utente e la password dell'amministratore del cluster ONTAP .
5. Fare clic su **Crea endpoint**.

Configurare una relazione di replicazione

Creare una pianificazione di processi di replicazione

Sia che si replichino dati da Element a ONTAP o da ONTAP a Element, è necessario configurare una pianificazione dei processi, specificare una policy e creare e inizializzare la relazione. È possibile utilizzare una policy predefinita o personalizzata.

Puoi usare il `job schedule cron create` comando per creare una pianificazione di processi di replicazione. La pianificazione dei lavori determina quando SnapMirror aggiorna automaticamente la relazione di protezione dei dati a cui è assegnata la pianificazione.

Informazioni su questo compito

Quando si crea una relazione di protezione dei dati, si assegna una pianificazione dei lavori. Se non si assegna una pianificazione dei lavori, è necessario aggiornare manualmente la relazione.

Fare un passo

1. Crea una pianificazione di lavoro:

```
job schedule cron create -name job_name -month month -dayofweek day_of_week
-day day_of_month -hour hour -minute minute
```

Per `-month`, `-dayofweek`, E `-hour`, puoi specificare `all` per eseguire il lavoro rispettivamente ogni mese, giorno della settimana e ora.

A partire da ONTAP 9.10.1, è possibile includere il Vserver nella pianificazione dei lavori:

```
job schedule cron create -name job_name -vserver Vserver_name -month month
-dayofweek day_of_week -day day_of_month -hour hour -minute minute
```

L'esempio seguente crea una pianificazione di lavoro denominata `my_weekly` che si svolge il sabato alle 3:00 del mattino:

```
cluster_dst:> job schedule cron create -name my_weekly -dayofweek
"Saturday" -hour 3 -minute 0
```

Creare una politica di replica personalizzata

Quando si crea una relazione di replica, è possibile utilizzare un criterio predefinito o personalizzato. Per una policy di replica unificata personalizzata, è necessario definire una o più *regole* che stabiliscano quali copie snapshot vengono trasferite durante l'inizializzazione e l'aggiornamento.

È possibile creare una policy di replica personalizzata se la policy predefinita per una relazione non è adatta. Ad esempio, potresti voler comprimere i dati in un trasferimento di rete o modificare il numero di tentativi effettuati SnapMirror per trasferire copie di snapshot.

Informazioni su questo compito

Il *tipo di policy* della policy di replica determina il tipo di relazione supportata. La tabella seguente mostra i tipi di polizza disponibili.

Tipo di polizza	Tipo di relazione
specchio asincrono	SnapMirror DR
specchio-volta	Replica unificata

Fare un passo

1. Crea una policy di replica personalizzata:

```
snapmirror policy create -vserver SVM -policy policy -type async-  
mirror|mirror-vault -comment comment -tries transfer_tries -transfer-priority  
low|normal -is-network-compression-enabled true|false
```

Per la sintassi completa dei comandi, vedere la pagina `man`.

A partire da ONTAP 9.5, è possibile specificare la pianificazione per la creazione di una pianificazione di copia snapshot comune per le relazioni sincrone SnapMirror utilizzando `-common-snapshot-schedule` parametro. Per impostazione predefinita, la pianificazione comune della copia degli snapshot per le relazioni sincrone SnapMirror è di un'ora. È possibile specificare un valore compreso tra 30 minuti e due ore per la pianificazione della copia degli snapshot per le relazioni sincrone SnapMirror .

L'esempio seguente crea un criterio di replica personalizzato per SnapMirror DR che abilita la compressione di rete per i trasferimenti di dati:

```
cluster_dst::> snapmirror policy create -vserver svml -policy  
DR_compressed -type async-mirror -comment "DR with network compression  
enabled" -is-network-compression-enabled true
```

L'esempio seguente crea un criterio di replica personalizzato per la replica unificata:

```
cluster_dst::> snapmirror policy create -vserver svm1 -policy my_unified
-type mirror-vault
```

Dopo aver finito

Per i tipi di policy “mirror-vault”, è necessario definire regole che determinino quali copie snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento.

Utilizzare il `snapmirror policy show` comando per verificare che il criterio SnapMirror sia stato creato. Per la sintassi completa dei comandi, vedere la pagina man.

Definire una regola per una policy

Per le policy personalizzate con tipo di policy “mirror-vault”, è necessario definire almeno una regola che determini quali copie snapshot vengono trasferite durante l’inizializzazione e l’aggiornamento. È anche possibile definire regole per policy predefinite con il tipo di policy “mirror-vault”.

Informazioni su questo compito

Ogni policy con tipo di policy “mirror-vault” deve avere una regola che specifica quali copie snapshot replicare. La regola “bi-monthly”, ad esempio, indica che devono essere replicate solo le copie snapshot a cui è stata assegnata l’etichetta SnapMirror “bi-monthly”. L’etichetta SnapMirror viene assegnata quando si configurano le copie snapshot di Element.

Ogni tipo di policy è associato a una o più regole definite dal sistema. Queste regole vengono assegnate automaticamente a una policy quando ne specifichi il tipo. La tabella seguente mostra le regole definite dal sistema.

Regola definita dal sistema	Utilizzato nei tipi di policy	Risultato
sm_creato	specchio asincrono, specchio-vault	Una copia snapshot creata da SnapMirror viene trasferita durante l’inizializzazione e l’aggiornamento.
quotidiano	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “daily” vengono trasferite durante l’inizializzazione e l’aggiornamento.
settimanale	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “weekly” vengono trasferite durante l’inizializzazione e l’aggiornamento.
mensile	specchio-volta	Le nuove copie snapshot sulla sorgente con etichetta SnapMirror “mensile” vengono trasferite durante l’inizializzazione e l’aggiornamento.

È possibile specificare regole aggiuntive in base alle esigenze, per policy predefinite o personalizzate. Per esempio:

- Per impostazione predefinita `MirrorAndVault` policy, potresti creare una regola denominata “bi-monthly” per abbinare le copie snapshot sulla sorgente con l’etichetta `SnapMirror` “bi-monthly”.
- Per una policy personalizzata con il tipo di policy “mirror-vault”, è possibile creare una regola denominata “bi-weekly” per abbinare le copie snapshot sull’origine con l’etichetta `SnapMirror` “bi-weekly”.

Fare un passo

1. Definisci una regola per una policy:

```
snapmirror policy add-rule -vserver SVM -policy policy_for_rule -snapmirror  
-label snapmirror-label -keep retention_count
```

Per la sintassi completa dei comandi, vedere la pagina man.

L’esempio seguente aggiunge una regola con l’etichetta `SnapMirror` `bi-monthly` al valore predefinito `MirrorAndVault` politica:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy  
MirrorAndVault -snapmirror-label bi-monthly -keep 6
```

L’esempio seguente aggiunge una regola con l’etichetta `SnapMirror` `bi-weekly` all’usanza `my_snapvault` politica:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy  
my_snapvault -snapmirror-label bi-weekly -keep 26
```

L’esempio seguente aggiunge una regola con l’etichetta `SnapMirror` `app_consistent` all’usanza `Sync` politica:

```
cluster_dst::> snapmirror policy add-rule -vserver svml -policy Sync  
-snapmirror-label app_consistent -keep 1
```

È quindi possibile replicare copie snapshot dal cluster di origine che corrispondono a questa etichetta `SnapMirror` :

```
cluster_src::> snapshot create -vserver vs1 -volume vol1 -snapshot  
snapshot1 -snapmirror-label app_consistent
```

Creare una relazione di replicazione

Crea una relazione da una sorgente Element a una destinazione ONTAP

La relazione tra il volume di origine nell’archiviazione primaria e il volume di destinazione

nell'archiviazione secondaria è chiamata *relazione di protezione dei dati*. Puoi usare il `snapmirror create` comando per creare una relazione di protezione dei dati da una sorgente Element a una destinazione ONTAP , o da una sorgente ONTAP a una destinazione Element.

È possibile utilizzare SnapMirror per replicare copie snapshot di un volume Element su un sistema di destinazione ONTAP . In caso di disastro presso il sito Element, è possibile fornire dati ai client dal sistema ONTAP , quindi riattivare il volume sorgente Element quando il servizio viene ripristinato.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .
- Se si utilizza il tipo di criterio “mirror-vault”, è necessario che sia stata configurata un’etichetta SnapMirror per le copie snapshot dell’elemento da replicare.



Puoi eseguire questa attività solo in ["Interfaccia utente web del software Element"](#) o utilizzando il ["Metodi API"](#) .

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>` , dove “lun” è la stringa effettiva “lun” e `name` è il nome del volume Element.

Un volume Element è più o meno equivalente a un LUN ONTAP . SnapMirror crea un LUN con il nome del volume Element quando viene inizializzata una relazione di protezione dei dati tra il software Element e ONTAP . SnapMirror replica i dati su una LUN esistente se la LUN soddisfa i requisiti per la replica dal software Element a ONTAP.

Le regole di replicazione sono le seguenti:

- Un volume ONTAP può contenere dati provenienti da un solo volume Element.
- Non è possibile replicare i dati da un volume ONTAP a più volumi Element.

In ONTAP 9.3 e versioni precedenti, un volume di destinazione può contenere fino a 251 copie snapshot. In ONTAP 9.4 e versioni successive, un volume di destinazione può contenere fino a 1019 copie snapshot.

Fare un passo

1. Dal cluster di destinazione, creare una relazione di replica da un'origine Element a una destinazione ONTAP :

```
snapmirror create -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume> -type XDP -schedule schedule -policy  
<policy>
```

Per la sintassi completa dei comandi, vedere la pagina [man](#).

L'esempio seguente crea una relazione SnapMirror DR utilizzando l'impostazione predefinita `MirrorLatest` politica:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorLatest
```

L'esempio seguente crea una relazione di replica unificata utilizzando l'impostazione predefinita MirrorAndVault politica:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy MirrorAndVault
```

L'esempio seguente crea una relazione di replica unificata utilizzando Unified7year politica:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy Unified7year
```

L'esempio seguente crea una relazione di replica unificata utilizzando il metodo personalizzato my_unified politica:

```
cluster_dst:> snapmirror create -source-path 10.0.0.11:/lun/0005
-destination-path svm_backup:volA_dst -type XDP -schedule my_daily
-policy my_unified
```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Creare una relazione da una sorgente ONTAP a una destinazione Element

A partire da ONTAP 9.4, è possibile utilizzare SnapMirror per replicare copie snapshot di una LUN creata su una sorgente ONTAP su una destinazione Element. Potresti utilizzare la LUN per migrare i dati da ONTAP al software Element.

Prima di iniziare

- Il nodo di destinazione dell'elemento deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .

Informazioni su questo compito

È necessario specificare il percorso di destinazione dell'elemento nel modulo `<hostip:>/lun/<name>` , dove "lun" è la stringa effettiva "lun" e name è il nome del volume Element.

Le regole di replicazione sono le seguenti:

- La relazione di replicazione deve avere una policy di tipo “async-mirror”.

È possibile utilizzare una policy predefinita o personalizzata.

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Fare un passo

1. Creare una relazione di replica da una sorgente ONTAP a una destinazione Element:

```
snapmirror create -source-path <SVM:volume>|<cluster://SVM/volume>
-destination-path <hostip:>/lun/<name> -type XDP -schedule schedule -policy
<policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente crea una relazione SnapMirror DR utilizzando l'impostazione predefinita MirrorLatest politica:

```
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
```

L'esempio seguente crea una relazione SnapMirror DR utilizzando il valore personalizzato my_mirror politica:

```
cluster_dst::> snapmirror create -source-path svm_1:volA_dst
-destination-path 10.0.0.11:/lun/0005 -type XDP -schedule my_daily
-policy my_mirror
```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Inizializzare una relazione di replicazione

Per tutti i tipi di relazione, l'inizializzazione esegue un *trasferimento di base*: crea una copia snapshot del volume di origine, quindi trasferisce tale copia e tutti i blocchi di dati a cui fa riferimento al volume di destinazione.

Prima di iniziare

- Il nodo Element contenente il volume da replicare deve essere reso accessibile a ONTAP.
- Il volume Element deve essere stato abilitato per la replica SnapMirror .
- Se si utilizza il tipo di criterio “mirror-vault”, è necessario che sia stata configurata un'etichetta SnapMirror per le copie snapshot dell'elemento da replicare.



Puoi eseguire questa attività solo in ["Interfaccia utente web del software Element"](#) o utilizzando il ["Metodi API"](#).

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>`, dove "lun" è la stringa effettiva "lun" e *name* è il nome del volume Element.

L'inizializzazione può richiedere molto tempo. Potrebbe essere opportuno effettuare il trasferimento di base nelle ore non di punta.

Se per qualsiasi motivo l'inizializzazione di una relazione da una sorgente ONTAP a una destinazione Element non riesce, continuerà a non riuscire anche dopo aver corretto il problema (ad esempio, un nome LUN non valido). La soluzione alternativa è la seguente:



1. Elimina la relazione.
2. Eliminare il volume di destinazione dell'elemento.
3. Crea un nuovo volume di destinazione Element.
4. Crea e inicializza una nuova relazione dall'origine ONTAP al volume di destinazione Element.

Fare un passo

1. Inizializzare una relazione di replicazione:

```
snapmirror initialize -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume|cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente inicializza la relazione tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al volume di destinazione volA_dst SU svm_backup:

```
cluster_dst:> snapmirror initialize -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Fornire dati da un volume di destinazione SnapMirror DR

Rendere scrivibile il volume di destinazione

Quando un disastro disabilita il sito primario per una relazione SnapMirror DR, è possibile fornire dati dal volume di destinazione con un'interruzione minima. È possibile riattivare il volume di origine quando il servizio viene ripristinato nel sito primario.

È necessario rendere scrivibile il volume di destinazione prima di poter fornire dati dal volume ai client. Puoi usare il `snapmirror quiesce` comando per interrompere i trasferimenti programmati verso la destinazione, il `snapmirror abort` comando per interrompere i trasferimenti in corso e il `snapmirror break` comando per rendere scrivibile la destinazione.

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo <hostip:>/lun/<name> , dove "lun" è la stringa effettiva "lun" e name è il nome del volume Element.

Passi

1. Interrompere i trasferimenti programmati verso la destinazione:

```
snapmirror quiesce -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti pianificati tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al volume di destinazione volA_dst SU svm_backup :

```
cluster_dst::> snapmirror quiesce -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

2. Interrompere i trasferimenti in corso verso la destinazione:

```
snapmirror abort -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti in corso tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al volume di destinazione volA_dst SU svm_backup :

```
cluster_dst::> snapmirror abort -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

3. Interrompere la relazione SnapMirror DR:

```
snapmirror break -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe la relazione tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al volume di destinazione volA_dst SU svm_backup e il volume di destinazione volA_dst SU svm_backup :

```
cluster_dst::> snapmirror break -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Configurare il volume di destinazione per l'accesso ai dati

Dopo aver reso scrivibile il volume di destinazione, è necessario configurarlo per

l'accesso ai dati. Gli host SAN possono accedere ai dati dal volume di destinazione finché il volume di origine non viene riattivato.

1. Mappare l'Element LUN sul gruppo di iniziatori appropriato.
2. Creare sessioni iSCSI dagli iniziatori host SAN ai LIF SAN.
3. Sul client SAN, eseguire una nuova scansione dell'archiviazione per rilevare la LUN connessa.

Riattivare il volume sorgente originale

È possibile ristabilire la relazione di protezione dei dati originale tra i volumi di origine e di destinazione quando non è più necessario fornire dati dalla destinazione.

Informazioni su questo compito

La procedura seguente presuppone che la linea di base nel volume sorgente originale sia intatta. Se la linea di base non è intatta, è necessario creare e inizializzare la relazione tra il volume da cui si stanno fornendo i dati e il volume di origine originale prima di eseguire la procedura.

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>`, dove "lun" è la stringa effettiva "lun" e name è il nome del volume Element.

A partire da ONTAP 9.4, le copie snapshot di una LUN create durante la distribuzione dei dati dalla destinazione ONTAP vengono replicate automaticamente quando l'origine dell'elemento viene riattivata.

Le regole di replicazione sono le seguenti:

- Sono supportati solo i LUN iSCSI.
- Non è possibile replicare più di una LUN da un volume ONTAP a un volume Element.
- Non è possibile replicare una LUN da un volume ONTAP a più volumi Element.

Passi

1. Elimina la relazione di protezione dei dati originale:

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente elimina la relazione tra il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, volA_dst SU svm_backup:

```
cluster_dst::> snapmirror delete -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

2. Invertire la relazione originale di protezione dei dati:

```
snapmirror resync -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.

Sebbene la risincronizzazione non richieda un trasferimento della linea di base, può richiedere molto tempo. Potresti voler eseguire la risincronizzazione nelle ore non di punta.

L'esempio seguente inverte la relazione tra il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, volA_dst SU svm_backup :

```
cluster_dst:> snapmirror resync -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

3. Aggiorna la relazione invertita:

```
snapmirror update -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.



Il comando fallisce se non esiste una copia snapshot comune sull'origine e sulla destinazione. Utilizzo `snapmirror initialize` per reinizializzare la relazione.

L'esempio seguente aggiorna la relazione tra il volume da cui si stanno fornendo i dati, volA_dst SU svm_backup e il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror update -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

4. Interrompere i trasferimenti programmati per la relazione invertita:

```
snapmirror quiesce -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti pianificati tra il volume da cui si stanno fornendo i dati, volA_dst SU svm_backup e il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror quiesce -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

5. Interrompere i trasferimenti in corso per la relazione invertita:

```
snapmirror abort -source-path <SVM:volume>|<cluster://SVM/volume> -destination  
-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe i trasferimenti in corso tra il volume da cui si stanno fornendo i dati, volA_dst SU svm_backup e il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror abort -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

6. Interrompi la relazione inversa:

```
snapmirror break -source-path <SVM:volume>|<cluster://SVM/volume> -destination  
-path <hostip:>/lun/<name>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente interrompe la relazione tra il volume da cui si stanno fornendo i dati, volA_dst SU svm_backup e il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11:

```
cluster_dst:> snapmirror break -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005
```

7. Eliminare la relazione di protezione dei dati invertita:

```
snapmirror delete -source-path <SVM:volume>|<cluster://SVM/volume>  
-destination-path <hostip:>/lun/<name> -policy <policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente elimina la relazione invertita tra il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11 e il volume da cui vengono forniti i dati, volA_dst SU svm_backup :

```
cluster_src:> snapmirror delete -source-path svm_backup:volA_dst  
-destination-path 10.0.0.11:/lun/0005 -policy MirrorLatest
```

8. Ripristinare il rapporto originale di protezione dei dati:

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente ristabilisce la relazione tra il volume sorgente originale, 0005 all'indirizzo IP 10.0.0.11 e il volume di destinazione originale, volA_dst SU svm_backup :

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Dopo aver finito

Utilizzare il `snapmirror show` comando per verificare che la relazione SnapMirror sia stata creata. Per la sintassi completa dei comandi, vedere la pagina man.

Aggiornare manualmente una relazione di replicazione

Potrebbe essere necessario aggiornare manualmente una relazione di replica se un aggiornamento non riesce a causa di un errore di rete.

Informazioni su questo compito

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>`, dove "lun" è la stringa effettiva "lun" e name è il nome del volume Element.

Passi

1. Aggiornare manualmente una relazione di replicazione:

```
snapmirror update -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume>
```

Per la sintassi completa dei comandi, vedere la pagina man.



Il comando fallisce se non esiste una copia snapshot comune sull'origine e sulla destinazione. Utilizzo `snapmirror initialize` per reinizializzare la relazione.

L'esempio seguente aggiorna la relazione tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al volume di destinazione volA_dst SU svm_backup:

```
cluster_src::> snapmirror update -source-path 10.0.0.11:/lun/0005  
-destination-path svm_backup:volA_dst
```

Risincronizzare una relazione di replicazione

È necessario risincronizzare una relazione di replica dopo aver reso scrivibile un volume di destinazione, dopo che un aggiornamento non riesce perché non esiste una copia Snapshot comune sui volumi di origine e di destinazione oppure se si desidera modificare i criteri di replica per la relazione.

Informazioni su questo compito

Sebbene la risincronizzazione non richieda un trasferimento della linea di base, può richiedere molto tempo. Potresti voler eseguire la risincronizzazione nelle ore non di punta.

È necessario specificare il percorso sorgente dell'elemento nel modulo `<hostip:>/lun/<name>`, dove "lun" è la stringa effettiva "lun" e name è il nome del volume Element.

Fare un passo

1. Risincronizzare i volumi di origine e di destinazione:

```
snapmirror resync -source-path <hostip:>/lun/<name> -destination-path  
<SVM:volume>|<cluster://SVM/volume> -type XDP -policy <policy>
```

Per la sintassi completa dei comandi, vedere la pagina man.

L'esempio seguente risincronizza la relazione tra il volume di origine 0005 all'indirizzo IP 10.0.0.11 e al

volume di destinazione volA_dst SU svm_backup :

```
cluster_dst:> snapmirror resync -source-path 10.0.0.11:/lun/0005  
-policy MirrorLatest -destination-path svm_backup:volA_dst
```

Eseguire il backup e il ripristino dei volumi

Eseguire il backup e il 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 si ripristinano volumi da OpenStack Swift o Amazon S3, sono necessarie le informazioni manifest del processo di backup originale. Se si ripristina un volume di cui è stato eseguito il backup su un sistema di archiviazione SolidFire , non sono necessarie informazioni sul manifesto.

Trova maggiori informazioni

- [Eseguire il backup di un volume in un archivio oggetti Amazon S3](#)
- [Eseguire il backup di un volume in un archivio oggetti OpenStack Swift](#)
- [Eseguire il backup di un volume su un cluster di archiviazione SolidFire](#)
- [Ripristina un volume dal backup su un archivio oggetti Amazon S3](#)
- [Ripristina un volume dal backup su un archivio oggetti OpenStack Swift](#)
- [Ripristinare un volume dal backup su un cluster di archiviazione SolidFire](#)

Eseguire il backup di un volume in un archivio oggetti Amazon S3

È possibile eseguire il backup dei volumi su archivi di oggetti esterni compatibili con Amazon S3.

1. Fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona Azioni per il volume di cui si desidera eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **S3**.
5. Selezionare un'opzione in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
7. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
8. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
9. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
10. Inserisci un'etichetta da aggiungere al prefisso nel campo **Etichetta**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di un volume in un archivio oggetti OpenStack Swift

È possibile eseguire il backup dei volumi su archivi di oggetti esterni compatibili con OpenStack Swift.

1. Fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona Azioni relativa al volume di cui eseguire il backup.
3. Nel menu visualizzato, fare clic su **Backup su**.
4. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare **Swift**.
5. Selezionare un formato dati in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Immettere un URL da utilizzare per accedere all'archivio oggetti nel campo **URL**.
7. Inserisci un nome utente per l'account nel campo **Nome utente**.
8. Inserisci la chiave di autenticazione per l'account nel campo **Chiave di autenticazione**.
9. Immettere il contenitore in cui archiviare il backup nel campo **Contenitore**.
10. **Facoltativo**: inserisci un'etichetta con il nome da aggiungere al prefisso nel campo **Etichetta con il nome**.
11. Fare clic su **Inizia a leggere**.

Eseguire il backup di un volume su un cluster di archiviazione SolidFire

È possibile eseguire il backup dei volumi residenti in un cluster su un cluster remoto per i cluster di archiviazione che eseguono il software Element.

Assicurarsi che i cluster di origine e di destinazione siano accoppiati.

Vedere "[Cluster di coppie per la replicazione](#)".

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, **Gestione > Volumi**.
2. Fare clic sull'icona Azioni per il volume di destinazione.
3. Nel menu visualizzato, fare clic su **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 di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copia la chiave dalla casella **Chiave di scrittura volume in blocco** negli appunti.
8. Nel cluster di origine, vai a **Gestione > Volumi**.

9. Fare clic sull'icona Azioni relativa al volume di cui eseguire il backup.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, in **Backup su**, selezionare * SolidFire*.
12. Seleziona la stessa opzione selezionata in precedenza nel campo **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.
14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Nel campo **Chiave di scrittura volume di massa**, incollare la chiave generata in precedenza sul cluster di destinazione.
17. Fare clic su **Inizia a leggere**.

Ripristina un volume dal backup su un archivio oggetti Amazon S3

È possibile ripristinare un volume da un backup su un archivio oggetti Amazon S3.

1. Fare clic su **Segnalazione > Registro eventi**.
2. Individua l'evento di backup che ha creato il backup che devi ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.
4. Copia le informazioni del manifesto negli appunti.
5. Fare clic su **Gestione > Volumi**.
6. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Ripristina da**.
8. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **S3**.
9. Selezionare l'opzione corrispondente al backup in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
10. Immettere un nome host da utilizzare per accedere all'archivio oggetti nel campo **Nome host**.
11. Immettere un ID chiave di accesso per l'account nel campo **ID chiave di accesso**.
12. Inserisci la chiave di accesso segreta per l'account nel campo **Chiave di accesso segreta**.
13. Immettere il bucket S3 in cui archiviare il backup nel campo **Bucket S3**.
14. Incolla le informazioni del manifesto nel campo **Manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristina un volume dal backup su un archivio oggetti OpenStack Swift

È possibile ripristinare un volume da un backup su un archivio oggetti OpenStack Swift.

1. Fare clic su **Segnalazione > Registro eventi**.
2. Individua l'evento di backup che ha creato il backup che devi ripristinare.
3. Nella colonna **Dettagli** dell'evento, fare clic su **Mostra dettagli**.

4. Copia le informazioni del manifesto negli appunti.
5. Fare clic su **Gestione > Volumi**.
6. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
7. Nel menu visualizzato, fare clic su **Ripristina da**.
8. Nella finestra di dialogo **Ripristino integrato**, in **Ripristina da**, selezionare **Swift**.
9. Selezionare l'opzione corrispondente al backup in **Formato dati**:
 - **Nativo**: formato compresso leggibile solo dai sistemi di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
10. Immettere un URL da utilizzare per accedere all'archivio oggetti nel campo **URL**.
11. Inserisci un nome utente per l'account nel campo **Nome utente**.
12. Inserisci la chiave di autenticazione per l'account nel campo **Chiave di autenticazione**.
13. Immettere il nome del contenitore in cui è archiviato il backup nel campo **Contenitore**.
14. Incolla le informazioni del manifesto nel campo **Manifesto**.
15. Fare clic su **Avvia scrittura**.

Ripristinare un volume dal backup su un cluster di archiviazione SolidFire

È possibile ripristinare un volume da un backup su un cluster di archiviazione SolidFire .

Quando si esegue il backup o il ripristino da un cluster a un altro, il sistema genera una chiave da utilizzare come autenticazione tra i cluster. Questa chiave di scrittura del volume di massa consente al cluster di origine di autenticarsi con il cluster di destinazione, garantendo un certo livello di sicurezza durante la scrittura sul volume di destinazione. Come parte del processo di backup o ripristino, è necessario generare una chiave di scrittura del volume di massa dal volume di destinazione prima di avviare l'operazione.

1. Nel cluster di destinazione, fare clic su **Gestione > Volumi**.
2. Fare clic sull'icona Azioni per il volume che si desidera ripristinare.
3. Nel menu visualizzato, fare clic su **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 di archiviazione SolidFire .
 - **Non compresso**: formato non compresso compatibile con altri sistemi.
6. Fare clic su **Genera chiave**.
7. Copiare le informazioni **Bulk Volume Write Key** negli appunti.
8. Nel cluster di origine, fare clic su **Gestione > Volumi**.
9. Fare clic sull'icona Azioni per il volume che si desidera utilizzare per il ripristino.
10. Nel menu visualizzato, fare clic su **Backup su**.
11. Nella finestra di dialogo **Backup integrato**, selezionare * SolidFire* in **Backup su**.
12. Selezionare l'opzione corrispondente al backup in **Formato dati**.
13. Immettere l'indirizzo IP virtuale di gestione del cluster del volume di destinazione nel campo **MVIP cluster remoto**.

14. Immettere il nome utente del cluster remoto nel campo **Nome utente del cluster remoto**.
15. Immettere la password del cluster remoto nel campo **Password cluster remoto**.
16. Incolla la chiave dagli appunti nel campo **Chiave di scrittura volume in blocco**.
17. Fare clic su **Inizia a leggere**.

Configurare domini di protezione personalizzati

Per i cluster Element che contengono più di due nodi di archiviazione, è possibile configurare domini di protezione personalizzati per ciascun nodo. Quando si configurano domini di protezione personalizzati, è necessario assegnare tutti i nodi del cluster a un dominio.



Quando si assegnano domini di protezione, inizia una sincronizzazione dei dati tra i nodi e alcune operazioni del cluster non sono disponibili finché la sincronizzazione dei dati non viene completata. Dopo aver configurato un dominio di protezione personalizzato per un cluster, quando si aggiunge un nuovo nodo di archiviazione, non è possibile aggiungere unità per il nuovo nodo finché non si assegna un dominio di protezione per il nodo e non si consente il completamento della sincronizzazione dei dati. Visita il ["Documentazione sui domini di protezione"](#) per saperne di più sui domini di protezione.



Affinché uno schema di dominio di protezione personalizzato sia utile per un cluster, tutti i nodi di archiviazione all'interno di ogni chassis devono essere assegnati allo stesso dominio di protezione personalizzato. Per ottenere questo risultato, è necessario creare tutti i domini di protezione personalizzati necessari (lo schema di dominio di protezione personalizzato più piccolo possibile è di tre domini). Come buona pratica, configura un numero uguale di nodi per dominio e prova a garantire che ogni nodo assegnato a un dominio specifico sia dello stesso tipo.

Passi

1. Fare clic su **Cluster > Nodi**.
2. Fare clic su **Configura domini di protezione**.

Nella finestra **Configura domini di protezione personalizzati**, è possibile visualizzare i domini di protezione attualmente configurati (se presenti), nonché le assegnazioni dei domini di protezione per i singoli nodi.

3. Inserisci un nome per il nuovo dominio di protezione personalizzato e fai clic su **Crea**.

Ripetere questo passaggio per tutti i nuovi domini di protezione che si desidera creare.

4. Per ogni nodo nell'elenco **Assegna nodi**, fare clic sul menu a discesa nella colonna **Dominio di protezione** e selezionare un dominio di protezione da assegnare a quel nodo.



Prima di applicare le modifiche, assicurati di comprendere il layout del nodo e dello chassis, lo schema del dominio di protezione personalizzato configurato e gli effetti dello schema sulla protezione dei dati. Se si applica uno schema di dominio di protezione e si hanno immediatamente necessità di apportare modifiche, potrebbe volerci del tempo prima che sia possibile farlo a causa della sincronizzazione dei dati che avviene una volta applicata una configurazione.

5. Fare clic su **Configura domini di protezione**.

Risultato

A seconda delle dimensioni del cluster, la sincronizzazione dei dati tra i domini potrebbe richiedere del tempo. Una volta completata la sincronizzazione dei dati, è possibile visualizzare le assegnazioni personalizzate del dominio di protezione nella pagina **Cluster > Nodi** e la dashboard dell'interfaccia utente Web di Element mostra lo stato di protezione del cluster nel riquadro **Stato del dominio di protezione personalizzato**.

Possibili errori

Ecco alcuni errori che potresti visualizzare dopo aver applicato una configurazione personalizzata del dominio di protezione:

Errore	Descrizione	Risoluzione
Errore di SetProtectionDomainLayout: ProtectionDomainLayout renderebbe inutilizzabile NodeID {9}. Non è possibile utilizzare contemporaneamente nomi predefiniti e non predefiniti.	A un nodo non è assegnato alcun dominio di protezione.	Assegnare un dominio di protezione al nodo.
Errore SetProtectionDomainLayout: il tipo di dominio di protezione 'personalizzato' divide il tipo di dominio di protezione 'chassis'.	A un nodo in uno chassis multi-nodo viene assegnato un dominio di protezione diverso dagli altri nodi nello chassis.	Assicurarsi che a tutti i nodi nello chassis sia assegnato lo stesso dominio di protezione.

Trova maggiori informazioni

- ["Domini di protezione personalizzati"](#)
- ["Gestisci l'archiviazione con l'API Element"](#)

Risolvi i problemi del tuo sistema

Eventi di sistema

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 del cluster.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting > Registro eventi**.

Per ogni evento vengono visualizzate le seguenti informazioni:

Articolo	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 del servizio	Il servizio che ha segnalato l'evento (se applicabile).
Nodo	Il nodo che ha segnalato l'evento (se applicabile).
ID unità	L'unità che ha segnalato l'evento (se applicabile).
Ora dell'evento	L'ora in cui si è verificato l'evento.

Trova maggiori informazioni

[Tipi di eventi](#)

Tipi di eventi

Il sistema segnala diversi tipi di eventi; ogni evento è un'operazione completata dal sistema. 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 compaiono nel registro eventi:

- **apiEvent**

Eventi avviati da un utente tramite un'API o un'interfaccia utente Web che modificano le impostazioni.

- **binAssegnazioniEvento**

Eventi correlati all'assegnazione dei contenitori di dati. I contenitori sono essenzialmente contenitori 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 di blocco.

- **bsKillEvent**

Eventi di sistema correlati alla cessazione del servizio di blocco.

- **bulkOpEvent**

Eventi correlati alle operazioni eseguite su un intero volume, come un backup, un ripristino, uno snapshot o una clonazione.

- **cloneEvent**

Eventi correlati alla clonazione del volume.

- **clusterMasterEvent**

Eventi che si verificano durante l'inizializzazione del cluster o in seguito a modifiche della configurazione del cluster, come l'aggiunta o la rimozione di nodi.

- **cSumEvent**

Eventi correlati al rilevamento di una mancata corrispondenza del checksum durante la convalida del checksum end-to-end.

I servizi che rilevano una mancata corrispondenza del checksum vengono automaticamente arrestati e non riavviati dopo aver generato questo evento.

- **dataEvent**

Eventi correlati alla lettura e alla scrittura dei dati.

- **dbEvent**

Eventi correlati al database globale gestito dai nodi ensemble nel cluster.

- **driveEvent**

Eventi correlati alle operazioni di azionamento.

- **encryptionAtRestEvent**

Eventi correlati al processo di crittografia su un cluster.

- **eventoensemble**

Eventi correlati all'aumento o alla diminuzione del numero di nodi in un ensemble.

- **fibreChannelEvent**

Eventi relativi alla configurazione e alle connessioni ai nodi.

- **gcEvent**

Gli eventi correlati ai processi vengono eseguiti ogni 60 minuti per recuperare spazio di archiviazione sulle unità a blocchi. Questo processo è noto anche come garbage collection.

- **ieEvent**

Errore interno del sistema.

- **installEvent**

Eventi di installazione automatica del software. Il software viene installato automaticamente su un nodo in sospeso.

- **iSCSIEvent**

Eventi correlati a problemi iSCSI nel sistema.

- **limitEvent**

Eventi correlati al numero di volumi o volumi virtuali in un account o nel cluster che si avvicinano al massimo consentito.

- **maintenanceModeEvent**

Eventi correlati alla modalità di manutenzione del nodo, come la disabilitazione del nodo.

- **evento_di_rete**

Eventi correlati alla segnalazione degli errori di rete per ciascuna interfaccia fisica della scheda di interfaccia di rete (NIC).

Questi eventi vengono attivati quando un conteggio di errori per un'interfaccia supera la soglia predefinita di 1000 durante un intervallo di monitoraggio di 10 minuti. Questi eventi si applicano agli errori di rete quali mancate risposte ricevute, errori di controllo di ridondanza ciclico (CRC), errori di lunghezza, errori di overrun ed errori di frame.

- **piattaformaHardwareEvent**

Eventi correlati a problemi rilevati sui dispositivi hardware.

- **eventoClusterremoto**

Eventi correlati all'associazione di cluster remoti.

- **schedulerEvent**

Eventi correlati agli snapshot pianificati.

- **servizioEvento**

Eventi relativi allo stato del servizio di sistema.

- **sliceEvent**

Eventi correlati a Slice Server, come la rimozione di un'unità o di un volume di metadati.

Esistono tre tipi di eventi di riassegnazione delle sezioni, che includono informazioni sul servizio a cui è assegnato un volume:

- flipping: cambiare il servizio primario in un nuovo servizio primario

```
sliceID oldPrimaryServiceID->newPrimaryServiceID
```

- spostamento: modifica del servizio secondario in un nuovo servizio secondario

```
sliceID {oldSecondaryServiceID(s)}->{newSecondaryServiceID(s)}
```

- potatura: rimozione di un volume da un insieme di servizi

```
sliceID {oldSecondaryServiceID(s)}
```

- **snmpTrapEvent**

Eventi correlati alle trappole SNMP.

- **statEvent**

Eventi relativi alle statistiche di sistema.

- **tsEvento**

Eventi relativi al servizio di trasporto del sistema.

- **eccezione inaspettata**

Eventi correlati a eccezioni di sistema impreviste.

- **ureEvent**

Eventi correlati a errori di lettura irrecuperabili che si verificano durante la lettura dal dispositivo di archiviazione.

- **vasaProviderEvent**

Eventi correlati a un provider VASA (vSphere APIs for Storage Awareness).

Visualizza lo stato delle attività in esecuzione

È possibile visualizzare nell'interfaccia utente Web lo stato di avanzamento e di completamento delle attività in esecuzione segnalate dai metodi API ListSyncJobs e ListBulkVolumeJobs. È possibile accedere alla pagina Attività in esecuzione dalla scheda Report dell'interfaccia utente dell'elemento.

Se il numero di attività è elevato, il sistema potrebbe metterle in coda ed eseguirle in batch. Nella pagina Attività in esecuzione vengono visualizzati i servizi attualmente sincronizzati. Una volta completata, un'attività viene sostituita dalla successiva attività di sincronizzazione in coda. Le attività di sincronizzazione potrebbero continuare ad apparire nella pagina Attività in esecuzione finché non ci saranno più attività da completare.



È possibile visualizzare i dati di sincronizzazione della replica per i volumi sottoposti a replica nella pagina Attività in esecuzione del cluster contenente il volume di destinazione.

Avvisi di sistema

Visualizza gli avvisi di sistema

È possibile visualizzare avvisi per informazioni su guasti o errori del cluster nel sistema. Gli avvisi possono essere informazioni, avvertenze o errori e sono un buon indicatore del funzionamento del cluster. La maggior parte degli errori si risolve automaticamente.

È possibile utilizzare il metodo API ListClusterFaults per automatizzare il monitoraggio degli avvisi. Ciò ti consente di essere informato su tutti gli avvisi che si verificano.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting > Avvisi**.

Il sistema aggiorna gli avvisi sulla pagina ogni 30 secondi.

Per ogni evento vengono visualizzate le seguenti informazioni:

Articolo	Descrizione
ID	ID univoco associato a un avviso cluster.
Gravità	Il grado di importanza dell'allerta. Valori possibili: • Attenzione: un problema minore che potrebbe presto richiedere attenzione. Gli aggiornamenti del sistema sono ancora consentiti. • errore: un errore che potrebbe causare un degrado delle prestazioni o la perdita di alta disponibilità (HA). In genere, gli errori non dovrebbero compromettere il servizio. • critico: un guasto grave che influisce sul servizio. Il sistema non è in grado di soddisfare le richieste API o I/O del client. Operare in questo stato potrebbe comportare una potenziale perdita di dati. • bestPractice: non viene utilizzata una delle best practice consigliate per la configurazione del sistema.
Tipo	Il componente interessato dal guasto. Può essere un nodo, un'unità, un cluster, un servizio o un volume.
Nodo	ID del nodo a cui si riferisce questo errore. Incluso per errori di nodo e unità, altrimenti impostato su - (trattino).
ID unità	ID dell'unità a cui si riferisce questo errore. Incluso per guasti dell'unità, altrimenti impostato su - (trattino).

Codice di errore	Un codice descrittivo che indica la causa del guasto.
Dettagli	Una descrizione del guasto con dettagli aggiuntivi.
Data	Data e ora in cui è stato registrato l'errore.

2. Fare clic su **Mostra dettagli** per visualizzare le informazioni relative a un singolo 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 sull'avviso, inclusa la data in cui è stato risolto, vengono spostate nell'area Risolti.

Trova maggiori informazioni

- [Codici di errore del cluster](#)
- ["Gestisci l'archiviazione con l'API Element"](#)

Codici di errore del cluster

Il sistema segnala un errore o uno stato che potrebbe essere di interesse generando un codice di errore, che viene elencato nella pagina Avvisi. Questi codici aiutano a determinare quale componente del sistema ha ricevuto l'avviso e perché è stato generato.

L'elenco seguente descrive i diversi tipi di codici:

- **errore di servizio di autenticazione**

Il servizio di autenticazione su uno o più nodi del cluster non funziona come previsto.

Per ricevere assistenza, contattare il supporto NetApp .

- **disponibileIndirizzi IP di rete virtualeBasso**

Il numero di indirizzi di rete virtuali nel blocco di indirizzi IP è basso.

Per risolvere questo errore, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuali.

- **blockClusterFull**

Non c'è abbastanza spazio di archiviazione a blocchi libero per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di riempimento del cluster, vedere il metodo API `GetClusterFullThreshold`. Questo errore del cluster indica una delle seguenti condizioni:

- `stage3Low` (Avviso): è stata superata la soglia definita dall'utente. Regola le impostazioni del Cluster completo o aggiungi altri nodi.
- `stage4Critical` (Errore): non c'è abbastanza spazio per il ripristino da un errore di 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
- `stage5CompletelyConsumed` (Critical)1; Non sono consentite scritture o nuove connessioni iSCSI. Le

attuali connessioni iSCSI saranno mantenute. Le scritture non riusciranno finché non verrà aggiunta ulteriore capacità al cluster.

Per risolvere questo errore, eliminare o ripulire i volumi oppure aggiungere un altro nodo di archiviazione al cluster di archiviazione.

- **blocchiDegradato**

I dati del blocco non vengono più replicati completamente a causa di un errore.

Gravità	Descrizione
Avvertimento	Sono accessibili solo due copie complete dei dati del blocco.
Errore	È accessibile solo una singola copia completa dei dati del blocco.
Critico	Non sono accessibili copie complete dei dati del blocco.

Nota: lo stato di avviso può verificarsi solo su un sistema Triple Helix.

Per risolvere questo errore, ripristinare tutti i nodi offline o bloccare i servizi oppure contattare il supporto NetApp per ricevere assistenza.

- **blockServiceTooFull**

Un servizio di blocco sta utilizzando troppo spazio.

Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **blockServiceNon integro**

È stato rilevato un servizio di blocco non funzionante:

- Gravità = Avvertenza: non viene intrapresa alcuna azione. Questo periodo di avviso scadrà tra `cTimeUntilBSIsKilledMSec=330000` millisecondi.
- Gravità = Errore: il sistema sta automaticamente dismettendo i dati e replicandoli nuovamente su altre unità funzionanti.
- Gravità = Critica: sono presenti servizi di blocco non riusciti su diversi nodi, superiori o uguali al conteggio delle repliche (2 per la doppia elica). I dati non sono disponibili e la sincronizzazione del cestino non verrà completata.

Verificare la presenza di problemi di connettività di rete ed errori hardware. Si verificheranno altri guasti se specifici componenti hardware non funzionano. L'errore verrà risolto quando il servizio di blocco sarà accessibile o quando il servizio sarà stato dismesso.

- **BmcSelfTestFailed**

Il Baseboard Management Controller (BMC) non ha superato l'autotest.

Per ricevere assistenza, contattare l'assistenza NetApp .

Durante un aggiornamento a Element 12.5 o versione successiva, il `BmcSelfTestFailed` l'errore non viene generato per un nodo che ha un BMC preesistente non riuscito o quando il BMC di un nodo non funziona durante l'aggiornamento. I BMC che non superano gli autotest durante l'aggiornamento emetteranno un `BmcSelfTestFailed` avviso di errore dopo che l'intero cluster ha completato l'aggiornamento.

- **clockSkewExceedsFaultThreshold**

Lo sfasamento temporale tra il master del cluster e il nodo che presenta un token supera la soglia consigliata. Il cluster di archiviazione non è in grado di correggere automaticamente lo sfasamento temporale tra i nodi.

Per risolvere questo errore, utilizzare i server NTP interni alla rete anziché quelli predefiniti di installazione. Se si utilizza un server NTP interno, contattare il supporto NetApp per ricevere assistenza.

- **clusterNonPuòSincronizzarsi**

Si è verificata una condizione di spazio insufficiente e i dati sulle unità di archiviazione a blocchi offline non possono essere sincronizzati con le unità ancora attive.

Per risolvere questo problema, aggiungere altro spazio di archiviazione.

- **clusterFull**

Non c'è più spazio di archiviazione libero nel cluster di archiviazione.

Per risolvere questo problema, aggiungere altro spazio di archiviazione.

- **clusterIOPSAreOverProvisioned**

Gli IOPS del cluster sono sovradimensionati. La somma di tutti gli IOPS QoS minimi è maggiore degli IOPS previsti del cluster. Non è possibile mantenere la QoS minima per tutti i volumi contemporaneamente.

Per risolvere questo problema, ridurre le impostazioni minime QoS IOPS per i volumi.

- **SogliaEventoTermicoCpu**

Il numero di eventi termici della CPU su una o più CPU supera la soglia configurata.

Se non vengono rilevati nuovi eventi termici della CPU entro dieci minuti, l'avviso si risolverà automaticamente.

- **disableDriveSecurityFailed**

Il cluster non è configurato per abilitare la sicurezza dell'unità (crittografia a riposo), ma almeno un'unità ha la sicurezza abilitata, il che significa che la disabilitazione della sicurezza dell'unità su tali unità non è riuscita. Questo errore viene registrato con gravità "Warning".

Per risolvere questo errore, controllare i dettagli dell'errore per scoprire il motivo per cui non è stato possibile disattivare la sicurezza dell'unità. Le possibili ragioni sono:

- Non è stato possibile acquisire la chiave di crittografia. Verificare il problema con l'accesso alla chiave o al server delle chiavi esterno.
- L'operazione di disattivazione sull'unità non è riuscita. Verificare se è possibile che sia stata acquisita la chiave sbagliata.

Se nessuna di queste cause è la causa del guasto, potrebbe essere necessario sostituire l'unità.

È possibile tentare di ripristinare un'unità che non disattiva correttamente la sicurezza anche quando viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere l'unità/le unità dal sistema spostandola su Disponibile, eseguire una cancellazione sicura sull'unità e spostarla nuovamente su Attiva.

- **ClusterPair disconnesso**

Una coppia di cluster è disconnessa o configurata in modo errato.

Controllare la connettività di rete tra i cluster.

- **nodoremoto disconnesso**

Un nodo remoto è disconnesso o configurato in modo errato.

Controllare la connettività di rete tra i nodi.

- **disconnectedSnapMirrorEndpoint**

Un endpoint remoto SnapMirror è disconnesso o configurato in modo errato.

Verificare la connettività di rete tra il cluster e lo SnapMirrorEndpoint remoto.

- **unità disponibile**

Nel cluster sono disponibili una o più unità. In generale, tutti i cluster dovrebbero avere tutte le unità aggiunte e nessuna nello stato disponibile. Se questo errore si verifica inaspettatamente, contattare l'assistenza NetApp .

Per risolvere questo errore, aggiungere tutte le unità disponibili al cluster di archiviazione.

- **driveFailed**

Il cluster restituisce questo errore quando una o più unità si guastano, indicando una delle seguenti condizioni:

- Il gestore dell'unità non riesce ad accedere all'unità.
- Il servizio slice o block ha avuto esito negativo troppe volte, presumibilmente a causa di errori di lettura o scrittura dell'unità, e non può essere riavviato.
- L'unità è mancante.
- Il servizio master per il nodo non è accessibile (tutte le unità nel nodo sono considerate mancanti/guaste).
- L'unità è bloccata e non è possibile acquisire la chiave di autenticazione per l'unità.
- L'unità è bloccata e l'operazione di sblocco non riesce.

Per risolvere questo problema:

- Controllare la connettività di rete per il nodo.
- Sostituire l'unità.
- Assicurarsi che la chiave di autenticazione sia disponibile.

- **driveHealthFault**

Un'unità non ha superato il controllo di integrità SMART e, di conseguenza, le sue funzionalità risultano ridotte. Per questo errore esiste un livello di gravità critico:

- L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> non ha superato il controllo di integrità generale SMART.

Per risolvere questo errore, sostituire l'unità.

- **driveWearFault**

La durata residua di un'unità è scesa al di sotto delle soglie, ma l'unità continua a funzionare. Esistono due possibili livelli di gravità per questo errore: Critico e Avvertenza:

- L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> presenta livelli di usura critici.
- L'unità con numero di serie: <numero di serie> nello slot: <slot nodo><slot unità> ha basse riserve di usura.

Per risolvere questo problema, sostituire l'unità al più presto.

- **duplicateClusterMasterCandidates**

È stato rilevato più di un candidato master del cluster di archiviazione.

Per ricevere assistenza, contattare il supporto NetApp .

- **enableDriveSecurityFailed**

Il cluster è configurato per richiedere la sicurezza dell'unità (crittografia a riposo), ma la sicurezza dell'unità non può essere abilitata su almeno un'unità. Questo errore viene registrato con gravità "Warning".

Per risolvere questo errore, controllare i dettagli dell'errore per scoprire il motivo per cui non è stato possibile abilitare la sicurezza dell'unità. Le possibili ragioni sono:

- Non è stato possibile acquisire la chiave di crittografia. Verificare il problema con l'accesso alla chiave o al server delle chiavi esterno.
- L'operazione di abilitazione sull'unità non è riuscita. Verificare se è possibile che sia stata acquisita la chiave sbagliata. Se nessuna di queste cause è la causa del guasto, potrebbe essere necessario sostituire l'unità.

È possibile tentare di ripristinare un'unità che non abilita correttamente la sicurezza anche quando viene fornita la chiave di autenticazione corretta. Per eseguire questa operazione, rimuovere l'unità/le unità dal sistema spostandola su Disponibile, eseguire una cancellazione sicura sull'unità e spostarla nuovamente su Attiva.

- **ensembleDegraded**

Si è verificata un'interruzione della connettività di rete o dell'alimentazione su uno o più nodi dell'ensemble.

Per risolvere questo errore, ripristinare la connettività di rete o l'alimentazione.

- **eccezione**

Un guasto segnalato che non è un guasto di routine. Questi errori non vengono cancellati

automaticamente dalla coda degli errori.

Per ricevere assistenza, contattare il supporto NetApp .

- **SpazioTroppoPienofallito**

Un servizio a blocchi non risponde alle richieste di scrittura dei dati. Ciò fa sì che il servizio slice esaurisca lo spazio per archiviare le scritture non riuscite.

Per risolvere questo errore, ripristinare la funzionalità dei servizi a blocchi per consentire alle scritture di continuare normalmente e allo spazio non riuscito di essere svuotato dal servizio slice.

- **sensore ventola**

Un sensore della ventola è guasto o mancante.

Per risolvere questo errore, sostituire l'hardware guasto.

- **fibreChannelAccessDegraded**

Un nodo Fibre Channel non risponde agli altri nodi nel cluster di storage tramite il proprio IP di storage per un certo periodo di tempo. In questo stato, il nodo verrà considerato non reattivo e genererà un errore del cluster.

Controllare la connettività di rete.

- **fibreChannelAccessUnavailable**

Tutti i nodi Fibre Channel non rispondono. Vengono visualizzati gli ID dei nodi.

Controllare la connettività di rete.

- **fibreChannelActiveIxl**

Il conteggio di IxL Nexus si sta avvicinando al limite supportato di 8000 sessioni attive per nodo Fibre Channel.

- Il limite ottimale è 5500.
- Il limite di attenzione è 7500.
- Il limite massimo (non applicato) è 8192.

Per risolvere questo errore, ridurre il conteggio IxL Nexus al di sotto del limite ottimale di 5500.

- **fibreChannelConfig**

Questo errore del cluster indica una delle seguenti condizioni:

- C'è una porta Fibre Channel inaspettata su uno slot PCI.
- Esiste un modello HBA Fibre Channel inaspettato.
- Si è verificato un problema con il firmware di un HBA Fibre Channel.
- Una porta Fibre Channel non è online.
- Si verifica un problema persistente durante la configurazione del passthrough Fibre Channel.

Per ricevere assistenza, contattare il supporto NetApp .

- **fibreChannelIOPS**

Il conteggio totale degli IOPS si sta avvicinando al limite degli IOPS per i nodi Fibre Channel nel cluster. I limiti sono:

- FC0025: limite di 450K IOPS con dimensione del blocco di 4K per nodo Fibre Channel.
- FCN001: limite OPS di 625K con dimensione del blocco di 4K per nodo Fibre Channel.

Per risolvere questo errore, bilanciare il carico su tutti i nodi Fibre Channel disponibili.

- **fibreChannelStaticIxl**

Il conteggio Ixl Nexus si sta avvicinando al limite supportato di 16.000 sessioni statiche per nodo Fibre Channel.

- Il limite ottimale è 11000.
- Il limite di attenzione è 15000.
- Il limite massimo (applicato) è 16384.

Per risolvere questo errore, ridurre il conteggio Ixl Nexus al di sotto del limite ottimale di 11000.

- **fileSystemCapacityLow**

Lo spazio su uno dei file system non è sufficiente.

Per risolvere questo errore, aggiungere più capacità al file system.

- **fileSystemIsReadOnly**

Un file system è passato alla modalità di sola lettura.

Per ricevere assistenza, contattare il supporto NetApp .

- **fipsDrivesMismatch**

Un'unità non FIPS è stata fisicamente inserita in un nodo di archiviazione compatibile con FIPS oppure un'unità FIPS è stata fisicamente inserita in un nodo di archiviazione non FIPS. Viene generato un singolo errore per nodo e vengono elencate tutte le unità interessate.

Per risolvere questo errore, rimuovere o sostituire l'unità o le unità non corrispondenti in questione.

- **fipsDrivesOutOfCompliance**

Il sistema ha rilevato che la crittografia a riposo è stata disabilitata dopo l'abilitazione della funzionalità Unità FIPS. Questo errore viene generato anche quando la funzionalità Unità FIPS è abilitata e nel cluster di archiviazione è presente un'unità o un nodo non FIPS.

Per risolvere questo errore, abilitare la crittografia a riposo o rimuovere l'hardware non FIPS dal cluster di archiviazione.

- **fipsSelfTestFailure**

Il sottosistema FIPS ha rilevato un errore durante l'autotest.

Per ricevere assistenza, contattare il supporto NetApp .

- **hardwareConfigMismatch**

Questo errore del cluster indica una delle seguenti condizioni:

- La configurazione non corrisponde alla definizione del nodo.
- La dimensione dell'unità per questo tipo di nodo non è corretta.
- È stata rilevata un'unità non supportata. Un possibile motivo è che la versione Element installata non riconosce questa unità. Si consiglia di aggiornare il software Element su questo nodo.
- C'è una mancata corrispondenza del firmware dell'unità.
- Lo stato di capacità di crittografia dell'unità non corrisponde al nodo.

Per ricevere assistenza, contattare il supporto NetApp .

- **idPCertificateExpiration**

Il certificato SSL del fornitore di servizi del cluster per l'utilizzo con un fornitore di identità (IdP) di terze parti sta per scadere o è già scaduto. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	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, aggiorna il certificato SSL prima che scada. Utilizzare il metodo API `UpdateIdpConfiguration` con `refreshCertificateExpirationTime=true` per fornire il certificato SSL aggiornato.

- **inconsistentBondModes**

Mancano le modalità di legame sul dispositivo VLAN. Questo errore visualizzerà la modalità di legame prevista e la modalità di legame attualmente in uso.

- **incoerenteMtus**

Questo errore del cluster indica una delle seguenti condizioni:

- Mancata corrispondenza Bond1G: sono state rilevate MTU incoerenti sulle interfacce Bond1G.
- Mancata corrispondenza Bond10G: sono stati rilevati MTU incoerenti 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.

- **SubnetMasks incoerenti**

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 di collegamento non è corretto.

- **invalidConfiguredFibreChannelNodeCount**

Una delle due connessioni previste del nodo Fibre Channel è degradata. Questo errore si verifica quando è connesso un solo nodo Fibre Channel.

Per risolvere questo errore, controllare la connettività di rete del cluster e il cablaggio di rete, nonché verificare la presenza di servizi non funzionanti. Se non ci sono problemi di rete o di servizio, contattare l'assistenza NetApp per la sostituzione del nodo Fibre Channel.

- **irqBalanceFailed**

Si è verificata un'eccezione durante il tentativo di bilanciare gli interrupt.

Per ricevere assistenza, contattare il supporto NetApp .

- **kmipCertificateFault**

- Il certificato della Root Certification Authority (CA) sta per scadere.

Per risolvere questo errore, acquisire un nuovo certificato dalla CA radice con data di scadenza di almeno 30 giorni e utilizzare `ModifyKeyServerKmp` per fornire il certificato CA radice aggiornato.

- Il certificato client sta per scadere.

Per risolvere questo errore, creare un nuovo CSR utilizzando `GetClientCertificateSigningRequest`, farlo firmare assicurandosi che la nuova data di scadenza sia di almeno 30 giorni e utilizzare `ModifyKeyServerKmp` per sostituire il certificato client KMIP in scadenza con il nuovo certificato.

- Il certificato dell'autorità di certificazione radice (CA) è scaduto.

Per risolvere questo errore, acquisire un nuovo certificato dalla CA radice con data di scadenza di almeno 30 giorni e utilizzare `ModifyKeyServerKmp` per fornire il certificato CA radice aggiornato.

- Il certificato client è scaduto.

Per risolvere questo errore, creare un nuovo CSR utilizzando `GetClientCertificateSigningRequest`, farlo firmare assicurandosi che la nuova data di scadenza sia di almeno 30 giorni e utilizzare `ModifyKeyServerKmp` per sostituire il certificato client KMIP scaduto con il nuovo certificato.

- Errore del certificato dell'autorità di certificazione radice (CA).

Per risolvere questo errore, verificare che sia stato fornito il certificato corretto e, se necessario, riacquisire il certificato dalla CA radice. Utilizzare `ModifyKeyServerKmp` per installare il certificato client KMIP corretto.

- Errore del certificato client.

Per risolvere questo errore, verificare che sia installato il certificato client KMIP corretto. La CA radice del certificato client deve essere installata sull'EKS. Utilizzare `ModifyKeyServerKmp` per installare il certificato client KMIP corretto.

- **kmipServerFault**

- Errore di connessione

Per risolvere questo errore, verificare che il server delle chiavi esterne sia attivo e raggiungibile tramite la rete. Utilizza TestKeyServerKimp e TestKeyProviderKimp per testare la tua connessione.

- Errore di autenticazione

Per risolvere questo errore, verificare che vengano utilizzati i certificati client KMIP e CA radice corretti e che la chiave privata e il certificato client KMIP corrispondano.

- Errore del server

Per risolvere questo errore, controlla i dettagli dell'errore. Potrebbe essere necessario risolvere il problema sul server chiavi esterno in base all'errore restituito.

- **sogliaEccMemoria**

Sono stati rilevati numerosi errori ECC correggibili o non correggibili. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Evento	Gravità	Descrizione
Un singolo DIMM cErrorCount raggiunge cDimmCorrectableErrWarnThreshold.	Avvertimento	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <Slot DIMM>
Un singolo DIMM cErrorCount rimane al di sopra di cDimmCorrectableErrWarnThreshold finché non scade cErrorFaultTimer per il DIMM.	Errore	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <DIMM>
Un controller di memoria segnala cErrorCount al di sopra di cMemCtrlCorrectableErrWarnThreshold e viene specificato cMemCtrlCorrectableErrWarnDuration.	Avvertimento	Errori di memoria ECC correggibili oltre la soglia sul controller di memoria: <Processore> <Controller di memoria>
Un controller di memoria segnala cErrorCount al di sopra di cMemCtrlCorrectableErrWarnThreshold finché non scade cErrorFaultTimer per il controller di memoria.	Errore	Errori di memoria ECC correggibili oltre la soglia su DIMM: <Processore> <DIMM>

Un singolo DIMM segnala un uErrorCount superiore a zero, ma inferiore a cDimmUncorrectableErrFaultThreshold.	Avvertimento	Errore/i di memoria ECC non correggibile rilevato/i su DIMM: <Processore> <Slot DIMM>
Un singolo DIMM segnala un uErrorCount di almeno cDimmUncorrectableErrFaultThreshold.	Errore	Errore/i di memoria ECC non correggibile rilevato/i su DIMM: <Processore> <Slot DIMM>
Un controller di memoria segnala un uErrorCount superiore a zero, ma inferiore a cMemCtrlrUncorrectableErrFaultThreshold.	Avvertimento	Errore/i di memoria ECC non correggibile/i rilevato/i sul controller di memoria: <Processore> <Controller di memoria>
Un controller di memoria segnala un uErrorCount di almeno cMemCtrlrUncorrectableErrFaultThreshold.	Errore	Errore/i di memoria ECC non correggibile/i rilevato/i sul controller di memoria: <Processore> <Controller di memoria>

Per risolvere questo errore, contattare il supporto NetApp per ricevere assistenza.

• soglia di utilizzo della memoria

L'utilizzo della memoria è superiore alla norma. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:



Per informazioni più dettagliate sul tipo di errore, consultare la sezione **Dettagli** nell'errore.

Gravità	Descrizione
Avvertimento	La memoria di sistema è insufficiente.
Errore	La memoria di sistema è molto bassa.
Critico	La memoria di sistema è completamente consumata.

Per risolvere questo errore, contattare il supporto NetApp per ricevere assistenza.

• metadataClusterFull

Non c'è abbastanza spazio libero per l'archiviazione dei metadati per supportare la perdita di un singolo nodo. Per informazioni dettagliate sui livelli di riempimento del cluster, vedere il metodo API GetClusterFullThreshold. Questo errore del cluster indica una delle seguenti condizioni:

- stage3Low (Avviso): è stata superata la soglia definita dall'utente. Regola le impostazioni del Cluster

completo o aggiungi altri nodi.

- **stage4Critical (Errore):** non c'è abbastanza spazio per il ripristino da un errore di 1 nodo. Non è consentita la creazione di volumi, snapshot e cloni.
- **stage5CompletelyConsumed (Critical)1;** Non sono consentite scritture o nuove connessioni iSCSI. Le attuali connessioni iSCSI saranno mantenute. Le scritture non riusciranno finché non verrà aggiunta ulteriore capacità al cluster. Elimina o ripulisci i dati oppure aggiungi altri nodi.

Per risolvere questo errore, eliminare o ripulire i volumi oppure aggiungere un altro nodo di archiviazione al cluster di archiviazione.

• **mtuCheckFailure**

Un dispositivo di rete non è configurato per la dimensione MTU corretta.

Per risolvere questo errore, assicurarsi che tutte le interfacce di rete e le porte dello switch siano configurate per frame jumbo (MTU fino a 9000 byte di dimensione).

• **Configurazione di rete**

Questo errore del cluster indica una delle seguenti condizioni:

- Non è presente un'interfaccia prevista.
- È presente un'interfaccia duplicata.
- Un'interfaccia configurata non è attiva.
- È necessario riavviare la rete.

Per ricevere assistenza, contattare il supporto NetApp .

• **nessunIndirizzoIPdiReteVirtualeDisponibile**

Non ci sono indirizzi di rete virtuali disponibili nel blocco di indirizzi IP.

- **virtualNetworkID # TAG(###)** non ha indirizzi IP di archiviazione disponibili. Non è possibile aggiungere nodi aggiuntivi al cluster.

Per risolvere questo errore, aggiungere altri indirizzi IP al blocco di indirizzi di rete virtuali.

• **nodeHardwareFault (l'interfaccia di rete <nome> è inattiva o il cavo è scollegato)**

Un'interfaccia di rete è inattiva oppure il cavo è scollegato.

Per risolvere questo errore, verificare la connettività di rete del nodo o dei nodi.

• **nodeHardwareFault (Lo stato di capacità di crittografia dell'unità non corrisponde allo stato di capacità di crittografia del nodo per l'unità nello slot <slot del nodo><slot dell'unità>)**

Un'unità non corrisponde alle capacità di crittografia del nodo di archiviazione in cui è installata.

• **nodeHardwareFault (<tipo di unità> dimensione dell'unità <dimensione effettiva> errata per l'unità nello slot <slot del nodo><slot dell'unità> per questo tipo di nodo - prevista <dimensione prevista>)**

Un nodo di archiviazione contiene un'unità di dimensioni errate per questo nodo.

• **nodeHardwareFault (Unità non supportata rilevata nello slot <slot nodo><slot unità>; le statistiche dell'unità e le informazioni sullo stato non saranno disponibili)**

Un nodo di archiviazione contiene un'unità che non supporta.

- **nodeHardwareFault** (L'unità nello slot <slot nodo><slot unità> dovrebbe utilizzare la versione firmware <versione prevista>, ma utilizza la versione non supportata <versione effettiva>)

Un nodo di archiviazione contiene un'unità che esegue una versione del firmware non supportata.

- **nodeMaintenanceMode**

Un nodo è stato messo in modalità manutenzione. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	Indica che il nodo è ancora in modalità di manutenzione.
Errore	Indica che la modalità di manutenzione non è riuscita a essere disattivata, molto probabilmente a causa di standby attivi o non riusciti.

Per risolvere questo errore, disattivare la modalità di manutenzione una volta completata la manutenzione. Se l'errore persiste, contattare il supporto NetApp per ricevere assistenza.

- **nodoOffline**

Il software Element non riesce a 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 la distribuzione dei nodi di archiviazione; i client potrebbero riscontrare problemi di prestazioni se LACP non è abilitato e configurato correttamente.

- **ntpServerUnreachable**

Il cluster di archiviazione non riesce a 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 l'ora del cluster di archiviazione e l'ora specificata del server NTP è troppo grande. Il cluster di archiviazione non può correggere automaticamente la differenza.

Per risolvere questo errore, utilizzare i server NTP interni alla rete anziché quelli predefiniti di installazione. Se si utilizzano server NTP interni e il problema persiste, contattare il supporto NetApp per ricevere assistenza.

- **nvrnDeviceStatus**

Un dispositivo NVRAM presenta un errore, è in errore o è guasto. Questo guasto ha le seguenti gravità:

Gravità	Descrizione
Avvertimento	È stato rilevato un avviso dall'hardware. Questa condizione può essere transitoria, come ad esempio un avviso di temperatura. • Errore di durata nvm • Stato di durata nvm • Stato della fonte energetica a vita • Stato della temperatura della fonte energetica • warningThresholdExceeded
Errore	L'hardware ha rilevato uno stato di errore o critico. Il master del cluster tenta di rimuovere l'unità slice dal funzionamento (ciò genera un evento di rimozione dell'unità). Se i servizi di slice secondari non sono disponibili, l'unità non verrà rimossa. Errori restituiti oltre agli errori di livello 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 l'unità slice dal funzionamento (ciò genera un evento di rimozione dell'unità). Se i servizi di slice secondari non sono disponibili, l'unità non verrà rimossa. • persistenzapersa • armStatusSaveNArmed • csaveStatusError

Sostituire qualsiasi componente hardware guasto nel nodo. Se il problema persiste, contattare l'assistenza NetApp per ricevere assistenza.

• **ErroreAlimentazione**

Questo errore del cluster indica una delle seguenti condizioni:

- Non è presente un alimentatore.
- Si è verificato un guasto all'alimentatore.
- Un ingresso di alimentazione è mancante o fuori portata.

Per risolvere questo errore, verificare che a tutti i nodi venga fornita alimentazione ridondante. Per ricevere assistenza, contattare il supporto NetApp .

- **Spaziotroppopieno**

La capacità complessiva fornita dal cluster è troppo piena.

Per risolvere questo errore, aggiungere altro spazio fornito oppure eliminare e ripulire i volumi.

- **remoteRepAsyncDelayExceeded**

È stato superato il ritardo asincrono configurato per la replica. Controllare la connettività di rete tra i cluster.

- **remoteRepClusterFull**

I volumi hanno sospeso la replica remota perché il cluster di archiviazione di destinazione è troppo pieno.

Per risolvere questo errore, liberare spazio sul cluster di archiviazione di destinazione.

- **remoteRepSnapshotClusterFull**

I volumi hanno sospeso la replica remota degli snapshot perché il cluster di archiviazione di destinazione è troppo pieno.

Per risolvere questo errore, liberare spazio sul cluster di archiviazione di destinazione.

- **remoteRepSnapshotsExceededLimit**

I volumi hanno sospeso la replica remota degli snapshot perché il volume del cluster di archiviazione di destinazione ha superato il limite di snapshot.

Per risolvere questo errore, aumentare il limite degli snapshot sul cluster di archiviazione di destinazione.

- **scheduleActionError**

Una o più attività programmate sono state eseguite, ma non sono riuscite.

L'errore viene cancellato se l'attività pianificata viene eseguita nuovamente e ha esito positivo, se l'attività pianificata viene eliminata o se l'attività viene sospesa e ripresa.

- **sensorReadingFailed**

Un sensore non è riuscito a comunicare con il Baseboard Management Controller (BMC).

Per ricevere assistenza, contattare il supporto NetApp .

- **servizioNonInEsecuzione**

Un servizio richiesto non è in esecuzione.

Per ricevere assistenza, contattare il supporto NetApp .

- **sliceServiceTooFull**

A un servizio slice è assegnata una capacità provisionata troppo bassa.

Per risolvere questo errore, aggiungere ulteriore capacità fornita.

- **sliceServiceNon sano**

Il sistema ha rilevato che un servizio slice non è integro e lo sta disattivando automaticamente.

- Gravità = Avvertenza: non viene intrapresa alcuna azione. Questo periodo di preavviso scadrà tra 6 minuti.
- Gravità = Errore: il sistema sta automaticamente dismettendo i dati e replicandoli nuovamente su altre unità funzionanti.

Verificare la presenza di problemi di connettività di rete ed errori hardware. Si verificheranno altri guasti se specifici componenti hardware non funzionano. L'errore verrà risolto quando il servizio slice sarà accessibile o quando il servizio sarà stato dismesso.

• **sshAbilitato**

Il servizio SSH è abilitato su uno o più nodi nel cluster di archiviazione.

Per risolvere questo errore, disabilitare il servizio SSH sul nodo o sui nodi appropriati oppure contattare il supporto NetApp per ricevere assistenza.

• **ScadenzaCertificatoSsl**

Il certificato SSL associato a questo nodo è prossimo alla scadenza o è scaduto. Questo errore utilizza i seguenti livelli di gravità in base all'urgenza:

Gravità	Descrizione
Avvertimento	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, rinnovare il certificato SSL. Se necessario, contattare il supporto NetApp per ricevere assistenza.

• **capacità bloccata**

Un singolo nodo rappresenta più della metà della capacità del cluster di archiviazione.

Per mantenere la ridondanza dei dati, il sistema riduce la capacità del nodo più grande, in modo che parte della sua capacità di blocco rimanga bloccata (non utilizzata).

Per risolvere questo errore, aggiungere più unità ai nodi di archiviazione esistenti oppure aggiungere nodi di archiviazione al cluster.

• **Sensore di temperatura**

Un sensore di temperatura segnala temperature più alte del normale. Questo errore può essere attivato insieme agli errori powerSupplyError o fanSensor.

Per risolvere questo problema, verificare che non vi siano ostruzioni al flusso d'aria in prossimità del cluster di archiviazione. Se necessario, contattare il supporto NetApp per ricevere assistenza.

• **aggiornamento**

È in corso un aggiornamento da più di 24 ore.

Per risolvere questo errore, riprendere l'aggiornamento o contattare il supporto NetApp per ricevere assistenza.

- **Servizio non responsivo**

Un servizio non risponde più.

Per ricevere assistenza, contattare il supporto NetApp .

- **virtualNetworkConfig**

Questo errore del cluster indica una delle seguenti condizioni:

- Non è presente alcuna interfaccia.
- C'è uno spazio dei nomi errato su un'interfaccia.
- La netmask è errata.
- L'indirizzo IP è errato.
- Un'interfaccia non è attiva e funzionante.
- C'è un'interfaccia superflua su un nodo.

Per ricevere assistenza, contattare il supporto NetApp .

- **volumiDegradati**

I volumi secondari non hanno terminato la replicazione e la sincronizzazione. Il messaggio scompare al termine della sincronizzazione.

- **volumiOffline**

Uno o più volumi nel cluster di archiviazione sono offline. Sarà presente anche l'errore **volumeDegraded**.

Per ricevere assistenza, contattare il supporto NetApp .

Visualizza l'attività delle prestazioni del nodo

È possibile visualizzare l'attività prestazionale di ciascun nodo in formato grafico. Queste informazioni forniscono statistiche in tempo reale sulla CPU e sulle operazioni di I/O di lettura/scrittura al secondo (IOPS) per ogni unità del nodo. Il grafico di utilizzo viene aggiornato ogni cinque secondi, mentre il grafico delle statistiche dell'unità viene aggiornato ogni dieci secondi.

1. Fare clic su **Cluster > Nodi**.
2. Fare clic su **Azioni** per il nodo che si desidera visualizzare.
3. Fare clic su **Visualizza dettagli**.



È possibile visualizzare punti specifici nel tempo sui grafici a linee e a barre posizionando il cursore sulla linea o sulla barra.

Prestazioni di volume

Visualizza le prestazioni del volume

È possibile visualizzare informazioni dettagliate sulle prestazioni di tutti i volumi nel cluster. È possibile ordinare le informazioni in base all'ID del volume o in base a una qualsiasi delle colonne relative alle prestazioni. È anche possibile filtrare 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 **Aggiorna ogni** e scegliendo un valore diverso. L'intervallo di aggiornamento predefinito è di 10 secondi se il cluster ha meno di 1000 volumi; in caso contrario, il valore predefinito è di 60 secondi. Se si sceglie il valore Mai, l'aggiornamento automatico della pagina è disabilitato.

Puoi riattivare l'aggiornamento automatico cliccando su **Attiva aggiornamento automatico**.

1. Nell'interfaccia utente di Element, seleziona **Reporting > Volume Performance**.
2. Nell'elenco dei volumi, fare clic sull'icona Azioni per un volume.
3. Fare clic su **Visualizza dettagli**.

Nella parte inferiore della pagina viene visualizzata una barra contenente informazioni generali sul volume.

4. Per visualizzare informazioni più dettagliate sul volume, fare clic su **Vedi altri dettagli**.

Il sistema visualizza informazioni dettagliate e grafici delle prestazioni per il volume.

Trova maggiori informazioni

[Dettagli sulle prestazioni del volume](#)

Dettagli sulle prestazioni del volume

È possibile visualizzare le statistiche sulle prestazioni dei volumi dalla pagina Prestazioni volume della scheda Report nell'interfaccia utente dell'elemento.

L'elenco seguente descrive i dettagli a tua disposizione:

- **ID**

ID generato dal sistema per il volume.

- **Nome**

Nome dato al volume al momento della sua creazione.

- **Account**

Nome dell'account assegnato al volume.

- **Gruppi di accesso**

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 massimo
- >100 = Il client sta utilizzando il burst

- **IOPS totali**

Numero totale di IOPS (lettura e scrittura) attualmente eseguiti sul volume.

- **Leggi IOPS**

Numero totale di IOPS di lettura attualmente eseguiti sul volume.

- **Scrivi IOPS**

Numero totale di IOPS di scrittura attualmente eseguiti sul volume.

- **Rendimento totale**

Quantità totale di throughput (lettura e scrittura) attualmente in esecuzione sul volume.

- **Velocità di lettura**

Quantità totale di throughput di lettura attualmente in esecuzione sul volume.

- **Capacità di scrittura**

Quantità totale di velocità di scrittura attualmente eseguita sul volume.

- **Latenza totale**

Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura e scrittura su un volume.

- **Latenza di lettura**

Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.

- **Latenza di scrittura**

Tempo medio, in microsecondi, impiegato per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.

- **Profondità della coda**

Numero di operazioni di lettura e scrittura in sospeso sul volume.

- **Dimensione media IO**

Dimensione media in byte delle recenti operazioni di I/O sul volume negli ultimi 500 millisecondi.

sessioni iSCSI

Visualizza 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 > Sessioni iSCSI**.
2. Per visualizzare i campi dei criteri di filtro, fare clic su **Filtro**.

Trova maggiori informazioni

[Dettagli della sessione iSCSI](#)

Dettagli della sessione iSCSI

È possibile visualizzare informazioni sulle sessioni iSCSI connesse al cluster.

L'elenco seguente descrive le informazioni che è possibile trovare sulle sessioni iSCSI:

- **Nodo**

Il nodo che ospita la partizione dei metadati primaria per il volume.

- **Account**

Nome dell'account proprietario del volume. Se il valore è vuoto, viene visualizzato un trattino (-).

- **Volume**

Il nome del volume identificato sul nodo.

- **ID volume**

ID del volume associato al Target IQN.

- **ID iniziatore**

Un ID generato dal sistema per l'iniziatore.

- **Alias dell'iniziatore**

Un nome facoltativo per l'iniziatore che ne facilita la ricerca quando l'elenco è lungo.

- **IP Iniziatore**

L'indirizzo IP dell'endpoint che avvia la sessione.

- **Iniziatore IQN**

L'IQN dell'endpoint che avvia la sessione.

- **IP di destinazione**

L'indirizzo IP del nodo che ospita il volume.

- **Obiettivo IQN**

L'IQN del volume.

- **CAP**

L'algoritmo CHAP per una sessione iSCSI. Se non viene utilizzato un algoritmo CHAP, viene visualizzato un trattino (-). Disponibile a partire da Element 12.8.

- **Creata il**

Data in cui è stata istituita la sessione.

Sessioni Fibre Channel

Visualizza le sessioni Fibre Channel

È possibile visualizzare le sessioni Fibre Channel (FC) connesse al cluster. È possibile filtrare le informazioni per includere solo le connessioni che si desidera visualizzare nella finestra.

1. Nell'interfaccia utente dell'elemento, seleziona **Reporting > Sessioni FC**.
2. Per visualizzare i campi dei criteri di filtro, fare clic su **Filtro**.

Trova maggiori informazioni

[Dettagli della sessione Fibre Channel](#)

Dettagli della sessione Fibre Channel

È possibile trovare informazioni sulle sessioni Fibre Channel (FC) attive connesse al cluster.

L'elenco seguente descrive le informazioni che è possibile trovare 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**

Un ID generato dal sistema per l'iniziatore.

- **Iniziatore WWPN**

Nome della porta mondiale di avvio.

- **Alias dell'iniziatore**

Un nome facoltativo per l'iniziatore che ne facilita la ricerca quando l'elenco è lungo.

- **Obiettivo WWP**

Nome della porta di destinazione mondiale.

- **Gruppo di accesso al volume**

Nome del gruppo di accesso al volume a cui appartiene la sessione.

- **ID gruppo di accesso al volume**

ID generato dal sistema per il gruppo di accesso.

Risoluzione dei problemi delle unità

Risoluzione dei problemi delle unità

È possibile sostituire un'unità a stato solido (SSD) guasta con un'unità sostitutiva. Gli SSD per i nodi di archiviazione SolidFire sono sostituibili a caldo. Se sospetti che un SSD sia guasto, contatta l'assistenza NetApp per verificare il guasto e ricevere istruzioni sulla procedura di risoluzione corretta. Il supporto NetApp collabora anche con te per ottenere un'unità sostitutiva in base al tuo contratto di servizio.

In questo caso, "How-swappable" significa che è possibile rimuovere un'unità guasta da un nodo attivo e sostituirla con una nuova unità SSD di NetApp. Si sconsiglia di rimuovere unità non guaste da un cluster attivo.

È consigliabile tenere a disposizione in loco i pezzi di ricambio suggeriti dal supporto NetApp per consentire la sostituzione immediata dell'unità in caso di guasto.



A scopo di test, se si simula un guasto dell'unità estraendo un'unità da un nodo, è necessario attendere 30 secondi prima di reinserire l'unità nello slot.

In caso di guasto di un'unità, Double Helix ridistribuisce i dati sull'unità tra i nodi rimanenti del cluster. I guasti di più unità sullo stesso nodo non rappresentano un problema, poiché il software Element protegge da due copie di dati residenti sullo stesso nodo. Un'unità guasta provoca i seguenti eventi:

- I dati vengono trasferiti dall'unità.
- La capacità complessiva del cluster è ridotta dalla capacità dell'unità.
- La protezione dei dati Double Helix garantisce che siano presenti due copie valide dei dati.



I sistemi di archiviazione SolidFire non supportano la rimozione di un'unità se ciò comporta una quantità di spazio di archiviazione insufficiente per la migrazione dei dati.

Per maggiori informazioni

- [Rimuovere le unità non riuscite dal cluster](#)
- [Risoluzione dei problemi di base dell'unità MDSS](#)
- [Rimuovere le unità MDSS](#)
- ["Sostituzione delle unità per i nodi di archiviazione SolidFire"](#)

- ["Sostituzione delle unità per i nodi di archiviazione della serie H600S"](#)
- ["Informazioni hardware H410S e H610S"](#)
- ["Informazioni sull'hardware della serie SF"](#)

Rimuovere le unità non riuscite dal cluster

Il sistema SolidFire segnala un'unità in stato di errore se l'autodiagnosi dell'unità segnala al nodo un errore o se la comunicazione con l'unità si interrompe per cinque minuti e mezzo o più. Il sistema visualizza un elenco delle unità guaste. È necessario rimuovere un'unità guasta dall'elenco delle unità guaste nel software NetApp Element .

Le unità nell'elenco **Avvisi** vengono visualizzate come **blockServiceUnhealthy** quando un nodo è offline. Quando si riavvia il nodo, se il nodo e le sue unità tornano online entro cinque minuti e mezzo, le unità si aggiornano automaticamente e continuano a essere attive nel cluster.

1. Nell'interfaccia utente di Element, seleziona **Cluster > Unità**.
2. Fare clic su **Non riuscito** per visualizzare l'elenco delle unità non riuscite.
3. Annotare il numero di slot dell'unità guasta.

Queste informazioni sono necessarie per individuare l'unità guasta nello chassis.

4. Rimuovere le unità danneggiate utilizzando uno dei seguenti metodi:

Opzione	Passi
Per rimuovere singole unità	a. Fare clic su Azioni per l'unità che si desidera rimuovere. b. Fare clic su Rimuovi.
Per rimuovere più unità	a. Seleziona tutte le unità che vuoi rimuovere e fai clic su Azioni in blocco. b. Fare clic su Rimuovi.

Risoluzione dei problemi di base dell'unità MDSS

È possibile ripristinare le unità metadati (o slice) aggiungendole nuovamente al cluster nel caso in cui una o entrambe le unità metadati si guastino. È possibile eseguire l'operazione di ripristino nell'interfaccia utente NetApp Element se la funzionalità MDSS è già abilitata sul nodo.

Se una o entrambe le unità di metadati in un nodo subiscono un errore, il servizio di suddivisione verrà arrestato e i dati di entrambe le unità verranno sottoposti a backup su unità diverse nel nodo.

Gli scenari seguenti delineano possibili scenari di errore e forniscono consigli di base per correggere il problema:

L'unità slice di sistema non funziona

- In questo scenario, lo slot 2 viene verificato e riportato allo stato disponibile.
- L'unità slice di sistema deve essere ripopolata prima che il servizio slice possa essere riattivato.
- È necessario sostituire l'unità slice di sistema; quando l'unità slice di sistema diventa disponibile, aggiungere contemporaneamente l'unità e l'unità slot 2.



Non è possibile aggiungere l'unità nello slot 2 da sola come unità metadati. È necessario aggiungere entrambe le unità al nodo contemporaneamente.

Lo slot 2 non funziona

- In questo scenario, l'unità slice di sistema viene verificata e riportata allo stato disponibile.
- Dovresti sostituire lo slot 2 con uno di riserva; quando lo slot 2 diventa disponibile, aggiungi contemporaneamente l'unità slice di sistema e l'unità dello slot 2.

L'unità slice di sistema e lo slot 2 non funzionano

- Dovresti sostituire sia l'unità slice di sistema sia lo slot 2 con un'unità di riserva. Quando entrambe le unità diventano disponibili, aggiungere contemporaneamente l'unità slice di sistema e l'unità slot 2.

Ordine delle operazioni

- Sostituire l'unità hardware guasta con un'unità di riserva (sostituire entrambe le unità se entrambe sono guaste).
- Aggiungere nuovamente le unità al cluster quando sono state ripopolate e sono disponibili.

Verificare le operazioni

- Verificare che le unità nello slot 0 (o interno) e nello slot 2 siano identificate come unità metadati nell'elenco Unità attive.
- Verificare che il bilanciamento delle sezioni sia stato completato (non ci siano ulteriori messaggi di spostamento delle sezioni nel registro eventi per almeno 30 minuti).

Per maggiori informazioni

[Aggiungi unità MDSS](#)

Aggiungi unità MDSS

È possibile aggiungere una seconda unità metadati su un nodo SolidFire convertendo l'unità a blocchi nello slot 2 in un'unità slice. Ciò si ottiene abilitando la funzionalità Multi-Drive Slice Service (MDSS). Per abilitare questa funzionalità, è necessario contattare l'assistenza NetApp .

Per riportare un'unità slice in uno stato disponibile potrebbe essere necessario sostituire un'unità guasta con una nuova o di riserva. È necessario aggiungere l'unità slice di sistema contemporaneamente all'unità per lo slot 2. Se si tenta di aggiungere solo l'unità slice dello slot 2 o prima di aggiungere l'unità slice di sistema, il sistema genererà un errore.

1. Fare clic su **Cluster > Unità**.

2. Fare clic su **Disponibile** per visualizzare l'elenco delle unità disponibili.
3. Selezionare le unità slice da aggiungere.
4. Fare clic su **Azioni in blocco**.
5. Fare clic su **Aggiungi**.
6. Verificare nella scheda **Unità attive** che le unità siano state aggiunte.

Rimuovere le unità MDSS

È possibile rimuovere le unità MDSS (Multi-Drive Slice Service). Questa procedura si applica solo se il nodo ha più unità slice.



Se l'unità slice di sistema e l'unità slot 2 si guastano, il sistema arresta i servizi slice e rimuove le unità. Se non si verificano guasti e si rimuovono le unità, è necessario rimuovere entrambe le unità contemporaneamente.

1. Fare clic su **Cluster > Unità**.
2. Nella scheda Unità **Disponibili**, fare clic sulla casella di controllo per le unità slice da rimuovere.
3. Fare clic su **Azioni in blocco**.
4. Fare clic su **Rimuovi**.
5. Conferma l'azione.

Risoluzione dei problemi dei nodi

Rimuovere i nodi da un cluster

È possibile rimuovere nodi da un cluster per manutenzione o sostituzione. È consigliabile utilizzare l'interfaccia utente o l'API NetApp Element per rimuovere i nodi prima di metterli offline.

Di seguito è riportata una panoramica della procedura per rimuovere i nodi di archiviazione:

- Assicurarsi che nel cluster vi sia 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 che il sistema migrerà i dati dalle unità del nodo ad altre unità nel cluster. Il tempo impiegato da questo processo dipende dalla quantità di dati da migrare.

- Rimuovere il nodo dal cluster.

Prima di spegnere o accendere un nodo, tenere a mente le seguenti considerazioni:

- Lo spegnimento di nodi e cluster comporta dei rischi se non eseguito correttamente.

Lo spegnimento di un nodo deve essere effettuato sotto la supervisione del supporto NetApp .

- Se un nodo è rimasto inattivo per più di 5,5 minuti a causa di qualsiasi tipo di condizione di arresto, la protezione dei dati Double Helix avvia l'attività di scrittura di singoli blocchi replicati su un altro nodo per replicare i dati. In questo caso, contattare l'assistenza NetApp per ricevere assistenza nell'analisi del nodo non riuscito.

- Per riavviare o spegnere un nodo in modo sicuro, è possibile utilizzare il comando Shutdown API.
- Se un nodo è inattivo o spento, è necessario contattare l'assistenza NetApp prima di riportarlo online.
- Dopo che un nodo è stato riportato online, è necessario aggiungere nuovamente le unità al cluster, a seconda di quanto tempo è stato fuori servizio.

Per maggiori informazioni

["Sostituzione di uno chassis SolidFire guasto"](#)

["Sostituzione di un nodo della serie H600S guasto"](#)

Spegnere un cluster

Per spegnere un intero cluster, eseguire la seguente procedura.

Passi

1. (Facoltativo) Contattare l'assistenza NetApp per ricevere assistenza nel completamento dei passaggi preliminari.
2. Verificare che tutti gli I/O siano stati arrestati.
3. Disconnettere tutte le sessioni iSCSI:
 - a. Passare all'indirizzo IP virtuale di gestione (MVIP) sul cluster per aprire l'interfaccia utente di Element.
 - b. Notare i nodi elencati nell'elenco Nodi.
 - c. Eseguire il metodo API Shutdown con l'opzione halt specificata su ciascun ID nodo nel cluster.

Quando si riavvia il cluster, è necessario seguire alcuni passaggi per verificare che tutti i nodi siano online:



1. Verificare che tutti i livelli di gravità critica e `volumesOffline` gli errori del cluster sono stati risolti.
2. Attendere dai 10 ai 15 minuti affinché il cluster si depositi.
3. Iniziare a richiamare gli host per accedere ai dati.

Se si desidera concedere più tempo per accendere i nodi e verificare che siano integri dopo la manutenzione, contattare l'assistenza tecnica per ricevere assistenza su come ritardare la sincronizzazione dei dati ed evitare una sincronizzazione bin non necessaria.

Trova maggiori informazioni

["Come arrestare e riaccendere correttamente un cluster di storage NetApp Solidfire/HCI"](#)

Lavorare con utilità per nodo per nodi di archiviazione

Lavorare con utilità per nodo per nodi di archiviazione

È possibile utilizzare le utilità 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 utilità per nodo forniscono informazioni e strumenti specifici che possono aiutare a risolvere i problemi di

rete tra i nodi o con il nodo di gestione.

Trova maggiori informazioni

- [Accedi alle impostazioni per nodo tramite 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 utilità di sistema utilizzando l'interfaccia utente per nodo](#)

Accedi alle impostazioni per nodo tramite l'interfaccia utente per nodo

È possibile accedere alle impostazioni di rete, alle impostazioni del cluster, ai test e alle utilità di sistema nell'interfaccia utente per nodo dopo aver immesso l'IP del nodo di gestione ed eseguito l'autenticazione.

Se si desidera modificare le impostazioni di un nodo in stato Attivo che fa parte di un cluster, è necessario accedere come utente amministratore del cluster.



Dovresti configurare o modificare un nodo alla volta. Prima di apportare modifiche a un altro nodo, è necessario assicurarsi che le impostazioni di rete specificate abbiano l'effetto previsto e che la rete sia stabile e funzioni correttamente.

1. Aprire l'interfaccia utente per nodo utilizzando uno dei seguenti metodi:

- Inserisci l'indirizzo IP di gestione seguito da :442 in una finestra del browser ed effettua l'accesso utilizzando un nome utente e una password amministratore.
- Nell'interfaccia utente dell'elemento, seleziona **Cluster > Nodi** e fai clic sul collegamento all'indirizzo IP di gestione per il nodo che desideri configurare o modificare. Nella finestra del browser che si apre, puoi 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 archiviazione per fornire al nodo un nuovo set di attributi di rete.

È possibile visualizzare le impostazioni di rete per un nodo di archiviazione nella pagina **Impostazioni di rete** quando si accede al nodo (https://<node_IP>:442/hcc/node/network-settings). È possibile selezionare le impostazioni **Bond1G** (gestione) o **Bond10G** (archiviazione). L'elenco seguente descrive le impostazioni che è possibile modificare quando un nodo di archiviazione è nello stato Disponibile, In sospeso o Attivo:

- **Metodo**

Metodo utilizzato per configurare l'interfaccia. Metodi possibili:

- loopback: utilizzato per definire l'interfaccia loopback IPv4.
- manuale: utilizzato per definire le interfacce per le quali non viene effettuata alcuna configurazione di default.
- dhcp: utilizzato per ottenere un indirizzo IP tramite DHCP.
- statico: utilizzato per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.

- **Velocità di collegamento**

La velocità negoziata dalla NIC virtuale.

- **Indirizzo IPv4**

L'indirizzo IPv4 per la rete eth0.

- **Maschera di sottorete IPv4**

Suddivisioni degli indirizzi della rete IPv4.

- **Indirizzo gateway IPv4**

Indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.

- **Indirizzo IPv6**

L'indirizzo IPv6 per la rete eth0.

- **Indirizzo gateway IPv6**

Indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.

- **MTU**

Dimensione massima del pacchetto che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete di archiviazione, il valore dovrebbe essere 9000.

- **Server DNS**

Interfaccia di rete utilizzata per la comunicazione del cluster.

- **Cerca domini**

Cerca altri indirizzi MAC disponibili nel sistema.

- **Modalità legame**

Può essere una delle seguenti modalità:

- AttivoPassivo (predefinito)
- CAMICE
- LACP

- **Stato**

Valori possibili:

- In funzione
- Giù
- Su

- **Tag Rete Virtuale**

Tag assegnato al momento della creazione della rete virtuale.

- **Percorsi**

Percorsi statici verso host o reti specifici tramite l'interfaccia associata per la quale i percorsi sono configurati.

Dettagli delle impostazioni del cluster dall'interfaccia utente per nodo

È possibile verificare le impostazioni del cluster per un nodo di archiviazione dopo la configurazione del cluster e modificare il nome host del nodo.

L'elenco seguente descrive le impostazioni del cluster per un nodo di archiviazione indicato dalla pagina **Impostazioni cluster** dell'interfaccia utente per nodo (https://<node_IP>:442/hcc/node/cluster-settings).

- **Ruolo**

Ruolo del nodo nel cluster. Valori possibili:

- Archiviazione: nodo di archiviazione o Fibre Channel.
- Gestione: il nodo è un nodo di gestione.

- **Nome host**

Nome del nodo.

- **Grappolo**

Nome del cluster.

- **Appartenenza al Cluster**

Stato del nodo. Valori possibili:

- Disponibile: il nodo non ha alcun nome di cluster associato e non fa ancora parte di un cluster.
- In attesa: 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 un software compatibile sul nodo. Una volta completato, il nodo passerà allo stato Attivo.
- Attivo: il nodo partecipa a un cluster. Per modificare il nodo è richiesta l'autenticazione.

- **Versione**

Versione del software Element in esecuzione sul nodo.

- **Insieme**

Nodi che fanno parte dell'insieme del 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. L'impostazione predefinita è Bond1G, ma è possibile utilizzare anche Bond10G.

- **Interfaccia di archiviazione**

Interfaccia di rete di archiviazione tramite Bond10G.

- **Capacità di crittografia**

Indica se il nodo supporta o meno la crittografia dell'unità.

Eseguire test di sistema utilizzando l'interfaccia utente per nodo

È possibile testare le modifiche alle impostazioni di rete dopo averle inserite nella configurazione di rete. È possibile eseguire i test per verificare che il nodo di archiviazione sia stabile e possa essere messo online senza problemi.

Hai effettuato l'accesso all'interfaccia utente per nodo del nodo di archiviazione.

1. Fare clic su **Test di sistema**.
2. Fare clic su **Esegui test** accanto al test che si desidera eseguire oppure selezionare **Esegui tutti i test**.



L'esecuzione di tutte le operazioni di test può richiedere molto tempo e dovrebbe essere effettuata solo su indicazione del supporto NetApp .

- **Test Ensemble Connesso**

Testa e verifica la connettività a un insieme di database. Per impostazione predefinita, il test utilizza l'ensemble per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un insieme diverso per testare la connettività.

- **Test di connessione Mvip**

Esegue il ping dell'indirizzo IP virtuale di gestione (MVIP) specificato e quindi esegue una semplice chiamata API all'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**

Esegue il ping dell'indirizzo IP virtuale di archiviazione specificato (SVIP) utilizzando pacchetti ICMP (Internet Control Message Protocol) che corrispondono alla dimensione MTU (Maximum Transmission

Unit) impostata sulla scheda di rete. Si connette quindi allo SVIP come iniziatore iSCSI. Per impostazione predefinita, il test utilizza l'SVIP per il cluster a cui è associato il nodo.

- **Test della configurazione hardware**

Verifica che tutte le configurazioni hardware siano corrette, convalida che le versioni del firmware siano corrette e conferma che tutte le unità siano installate e funzionino correttamente. Si tratta dello stesso test di fabbrica.



Questo test richiede molte risorse e deve essere eseguito solo se richiesto dal supporto NetApp.

- **Test di connettività locale**

Verifica la connettività con tutti gli altri nodi del cluster eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test verrà visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

- **Test Localizza Cluster**

Convalida che il nodo possa individuare il cluster specificato nella configurazione del cluster.

- **Configurazione di rete di prova**

Verifica che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate sul sistema. Questo test non è destinato a rilevare guasti hardware quando un nodo partecipa attivamente a un cluster.

- **Ping di prova**

Esegue il ping di un elenco specificato di host oppure, se non ne viene specificato nessuno, crea dinamicamente un elenco di tutti i nodi registrati nel cluster ed esegue il ping di ciascuno per una semplice connettività.

- **Test di connettività remota**

Verifica la connettività a tutti i nodi nei cluster accoppiati in remoto eseguendo il ping dell'IP del cluster (CIP) su ciascun nodo. Questo test verrà visualizzato su un nodo solo se il nodo fa parte di un cluster attivo.

Eseguire le utilità di sistema utilizzando l'interfaccia utente per nodo

È possibile utilizzare l'interfaccia utente per nodo del nodo di archiviazione per creare o eliminare bundle di supporto, reimpostare le impostazioni di configurazione per le unità e riavviare i servizi di rete o cluster.

Hai effettuato l'accesso all'interfaccia utente per nodo del nodo di archiviazione.

1. Fare clic su **Utilità di sistema**.
2. Fare clic sul pulsante relativo all'utilità di sistema che si desidera eseguire.

- **Controllo del potere**

Riavvia, spegne e riaccende il nodo o lo spegne.



Questa operazione provoca una perdita temporanea della connettività di rete.

Specificare i seguenti parametri:

- Azione: le opzioni includono Riavvia e Arresta (spegnimento).
- Ritardo di riattivazione: qualsiasi tempo aggiuntivo prima che il nodo torni online.

◦ **Raccogli i log dei nodi**

Crea un bundle di supporto nella directory /tmp/bundles del nodo.

Specificare i seguenti parametri:

- Nome bundle: nome univoco per ogni bundle di supporto creato. Se non viene specificato alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
- Argomenti aggiuntivi: questo parametro viene fornito allo script sf_make_support_bundle. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp .
- Timeout Sec: specifica il numero di secondi di attesa per ogni singola risposta ping.

◦ **Elimina i registri dei nodi**

Elimina tutti i bundle di supporto correnti sul nodo creati utilizzando **Create Cluster Support Bundle** o il metodo API CreateSupportBundle.

◦ **Reimposta unità**

Inizializza le unità e rimuove tutti i dati attualmente presenti sull'unità. 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 reimpostare.

◦ **Reimposta 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.

◦ **Reimposta nodo**

Ripristina le impostazioni di fabbrica di un nodo. Durante questa operazione tutti i dati vengono rimossi, ma le impostazioni di rete del nodo vengono conservate. I nodi possono essere reimpostati solo se non sono assegnati a un cluster e sono nello stato Disponibile.



Quando si utilizza questa opzione, tutti i dati, i pacchetti (aggiornamenti software), le configurazioni e i file di registro vengono eliminati dal nodo.

◦ **Riavvia la rete**

Riavvia tutti i servizi di rete su un nodo.



Questa operazione può causare la perdita temporanea della connettività di rete.

◦ **Riavvia i servizi**

Riavvia i servizi software Element su un nodo.



Questa operazione può causare l'interruzione temporanea del servizio del nodo. Questa operazione deve essere eseguita solo su indicazione 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 utilità 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 VMware vCenter ed evitare di definire le stesse risorse di archiviazione e di elaborazione o istanze vCenter in più nodi di gestione.

Vedere "[documentazione del nodo di gestione](#)" per maggiori informazioni.

Comprendere i livelli di pienezza del cluster

Il cluster che esegue il software Element genera errori del cluster per avvisare l'amministratore dello storage quando la capacità del cluster sta esaurendo. Esistono tre livelli di riempimento del cluster, tutti visualizzati nell'interfaccia utente NetApp Element : avviso, errore e critico.

Il sistema utilizza il codice di errore BlockClusterFull per avvisare che lo spazio di archiviazione dei blocchi del cluster è pieno. È possibile visualizzare i livelli di gravità del riempimento del cluster dalla scheda Avvisi dell'interfaccia utente dell'elemento.

L'elenco seguente include informazioni sui livelli di gravità di BlockClusterFull:

• Avvertimento

Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità del blocco del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al tre per cento al di sotto del livello di errore e può essere regolato tramite l'interfaccia utente e l'API di Element. È necessario aggiungere ulteriore capacità o liberarne altra il prima possibile.

• Errore

Quando il cluster si trova in questo stato, se un nodo viene perso, non ci sarà capacità sufficiente nel cluster per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot sono tutti bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per nessun cluster. È necessario aggiungere ulteriore capacità o liberare capacità immediatamente.

- **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 stabilire nuove connessioni iSCSI con il cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente altra capacità.

Il sistema utilizza il codice di errore MetadataClusterFull per avvisare che lo spazio di archiviazione dei metadati del cluster è pieno. È possibile visualizzare la quantità di spazio disponibile per i metadati del cluster nella sezione Capacità del cluster nella pagina Panoramica della scheda Report nell'interfaccia utente dell'elemento.

L'elenco seguente include informazioni sui livelli di gravità MetadataClusterFull:

- **Avvertimento**

Si tratta di un avviso configurabile dal cliente che viene visualizzato quando la capacità dei metadati del cluster si avvicina al livello di gravità dell'errore. Per impostazione predefinita, questo livello è impostato al tre per cento al di sotto del livello di errore e può essere regolato tramite l'API Element. È necessario aggiungere ulteriore capacità o liberarne altra il prima possibile.

- **Errore**

Quando il cluster si trova in questo stato, se un nodo viene perso, non ci sarà capacità sufficiente nel cluster per ricostruire la protezione dei dati Double Helix. La creazione di nuovi volumi, i cloni e gli snapshot sono tutti bloccati mentre il cluster si trova in questo stato. Questo non è uno stato sicuro o consigliato per nessun cluster. È necessario aggiungere ulteriore capacità o liberare capacità immediatamente.

- **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 stabilire nuove connessioni iSCSI con il cluster. Una volta raggiunta questa fase, è necessario liberare o aggiungere immediatamente altra capacità.



Quanto segue si applica alle soglie dei cluster a due nodi:

- L'errore di completezza dei metadati è inferiore del 20% al livello critico.
- L'errore di riempimento del blocco è pari a 1 unità di blocco (inclusa la capacità bloccata) al di sotto del livello critico, ovvero la capacità è pari a due unità di blocco al di sotto del livello critico.

Gestisci e monitora lo storage con NetApp Hybrid Cloud Control

Aggiungi e gestisci cluster di storage utilizzando NetApp Hybrid Cloud Control

È possibile aggiungere cluster di storage all'inventario delle risorse del nodo di gestione in modo che possano essere gestiti tramite NetApp Hybrid Cloud Control (HCC). Il primo cluster di archiviazione aggiunto durante la configurazione del sistema è quello predefinito ["cluster di archiviazione autorevole"](#), ma è possibile aggiungere cluster aggiuntivi utilizzando l'interfaccia utente HCC.

Dopo aver aggiunto un cluster di archiviazione, è possibile monitorarne le prestazioni, modificare le credenziali del cluster di archiviazione per la risorsa gestita o rimuovere un cluster di archiviazione dall'inventario delle risorse del nodo di gestione se non è più necessario gestirlo tramite HCC.

Cosa ti servirà

- **Autorizzazioni di amministratore del cluster:** hai le autorizzazioni come amministratore sul ["cluster di archiviazione autorevole"](#). Il cluster autorevole è il primo cluster aggiunto all'inventario dei nodi di gestione durante la configurazione del sistema.
- **Software Element:** la versione del cluster di storage esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione:** hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.
- **Servizi di gestione:** Hai aggiornato il tuo pacchetto di servizi di gestione alla versione 2.17 o successiva.

Opzioni

- [Aggiungere un cluster di archiviazione](#)
- [Conferma lo stato del cluster di archiviazione](#)
- [Modifica le credenziali del cluster di archiviazione](#)
- [Rimuovere un cluster di archiviazione](#)
- [Abilita e disabilita la modalità di manutenzione](#)

Aggiungere un cluster di archiviazione

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 tramite l'interfaccia utente HCC.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore autorevole del cluster di storage.
2. Dalla Dashboard, seleziona il menu delle opzioni in alto a destra e seleziona **Configura**.
3. Nel riquadro **Cluster di archiviazione**, selezionare **Dettagli cluster di archiviazione**.
4. Selezionare **Aggiungi cluster di archiviazione**.
5. Inserisci le seguenti informazioni:

- Indirizzo IP virtuale di gestione del cluster di archiviazione



È possibile aggiungere solo cluster di archiviazione remoti che non sono attualmente gestiti da un nodo di gestione.

- Nome utente e password del cluster di archiviazione

6. Selezionare **Aggiungi**.



Dopo aver aggiunto il cluster di archiviazione, l'inventario del cluster potrebbe impiegare fino a 2 minuti per aggiornarsi e visualizzare la nuova aggiunta. Potrebbe essere necessario aggiornare la pagina nel browser per visualizzare le modifiche.

Conferma lo stato del cluster di archiviazione

È possibile monitorare lo stato di connessione delle risorse dei cluster di storage tramite l'interfaccia utente di controllo NetApp Hybrid Cloud.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore autorevole del cluster di storage.
2. Dalla Dashboard, seleziona il menu delle opzioni in alto a destra e seleziona **Configura**.
3. Esaminare lo stato dei cluster di archiviazione nell'inventario.
4. Dal riquadro **Cluster di archiviazione**, selezionare **Dettagli cluster di archiviazione** per ulteriori dettagli.

Modifica le credenziali del cluster di archiviazione

È possibile modificare il nome utente e la password dell'amministratore del cluster di storage tramite l'interfaccia utente di controllo NetApp Hybrid Cloud.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore autorevole del cluster di storage.
2. Dalla Dashboard, seleziona il menu delle opzioni in alto a destra e seleziona **Configura**.
3. Nel riquadro **Cluster di archiviazione**, selezionare **Dettagli cluster di archiviazione**.
4. Selezionare il menu **Azioni** per il cluster e selezionare **Modifica credenziali cluster**.
5. Aggiornare il nome utente e la password del cluster di archiviazione.
6. Seleziona **Salva**.

Rimuovere un cluster di archiviazione

La rimozione di un cluster di storage da NetApp Hybrid Cloud Control comporta la rimozione del cluster dall'inventario dei nodi di gestione. Dopo aver rimosso un cluster di archiviazione, il cluster non può più essere gestito da HCC ed è possibile accedervi solo navigando direttamente al suo indirizzo IP di gestione.



Non è possibile rimuovere il cluster autorevole dall'inventario. Per determinare il cluster autorevole, vai su **Gestione utenti > Utenti**. Il cluster autorevole è elencato accanto all'intestazione **Utenti**.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore autorevole del cluster di storage.
2. Dalla Dashboard, seleziona il menu delle opzioni in alto a destra e seleziona **Configura**.
3. Nel riquadro **Cluster di archiviazione**, selezionare **Dettagli cluster di archiviazione**.
4. Selezionare il menu **Azioni** per il cluster e selezionare **Rimuovi cluster di archiviazione**.



Selezionando **Sì** il cluster verrà rimosso dall'installazione.

5. Selezionare **Sì**.

Abilita e disabilita la modalità di manutenzione

Se è necessario portare offline un nodo di archiviazione per interventi di manutenzione, ad esempio aggiornamenti software o riparazioni dell'host, è possibile ridurre al minimo l'impatto di I/O sul resto del cluster di archiviazione **abilitazione** modalità di manutenzione per quel nodo. Quando tu **disabilitare** modalità di manutenzione, il nodo viene monitorato per garantire che determinati criteri siano soddisfatti prima che il nodo possa uscire dalla modalità di manutenzione.

Cosa ti servirà

- **Software Element:** la versione del cluster di storage esegue il software NetApp Element 12.2 o versione successiva.
- **Nodo di gestione:** hai distribuito un nodo di gestione che esegue la versione 12.2 o successiva.
- **Servizi di gestione:** Hai aggiornato il tuo pacchetto di servizi di gestione alla versione 2.19 o successiva.
- Puoi effettuare l'accesso a livello di amministratore.

Abilita la modalità di manutenzione

È possibile utilizzare la seguente procedura per abilitare la modalità di manutenzione per un nodo del cluster di archiviazione.



Solo un nodo alla volta può essere in modalità manutenzione.

Passi

1. Aprire l'indirizzo IP del nodo di gestione in un browser web. Per esempio:

```
https://[management node IP address]
```

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire .

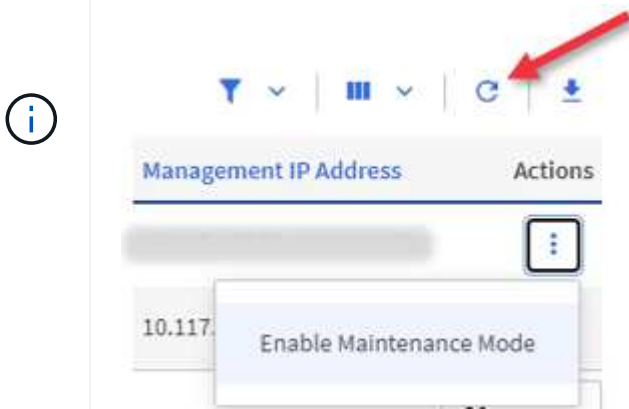


Le opzioni della funzionalità modalità manutenzione sono disabilitate a livello di sola lettura.

3. Nella casella di navigazione blu a sinistra, seleziona l'installazione all-flash SolidFire .
4. Nel riquadro di navigazione a sinistra, seleziona **Nodi**.
5. Per visualizzare le informazioni sull'inventario di archiviazione, selezionare **Archiviazione**.

6. Abilita la modalità di manutenzione su un nodo di archiviazione:

La tabella dei nodi di archiviazione viene aggiornata automaticamente ogni due minuti per le azioni non avviate dall'utente. Prima di un'azione, per assicurarti di avere lo stato più aggiornato, puoi aggiornare la tabella dei nodi utilizzando l'icona di aggiornamento situata nella parte superiore destra della tabella dei nodi.



- a. In **Azioni**, seleziona **Abilita modalità di manutenzione**.

Mentre la **Modalità di manutenzione** è abilitata, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi sullo stesso cluster.

Una volta completata l'**abilitazione della modalità di manutenzione**, nella colonna **Stato nodo** viene visualizzata un'icona a forma di chiave inglese e il testo "**Modalità di manutenzione**" per il nodo in modalità di manutenzione.

Disabilita la modalità di manutenzione

Dopo che un nodo è stato messo correttamente in modalità di manutenzione, per quel nodo è disponibile l'azione **Disabilita modalità di manutenzione**. Le azioni sugli altri nodi non saranno disponibili finché la modalità di manutenzione non verrà disabilitata correttamente sul nodo sottoposto a manutenzione.

Passi

1. Per il nodo in modalità di manutenzione, in **Azioni**, selezionare **Disabilita modalità di manutenzione**.

Quando la **Modalità di manutenzione** è disabilitata, le azioni della modalità di manutenzione non sono disponibili per il nodo selezionato e per tutti gli altri nodi sullo stesso cluster.

Dopo aver completato la **Disattivazione della modalità di manutenzione**, la colonna **Stato nodo** visualizza **Attivo**.

Quando un nodo è in modalità di manutenzione, non accetta nuovi dati. Di conseguenza, la disattivazione della modalità di manutenzione potrebbe richiedere più tempo, perché il nodo deve sincronizzare nuovamente i propri dati prima di poter uscire dalla modalità di manutenzione. Quanto più a lungo si rimane in modalità manutenzione, tanto più tempo sarà necessario per disattivarla.

Risoluzione dei problemi

Se si verificano errori durante l'abilitazione o la disabilitazione della modalità di manutenzione, viene visualizzato un banner di errore nella parte superiore della tabella dei nodi. Per maggiori informazioni sull'errore, puoi selezionare il link **Mostra dettagli** presente nel banner per visualizzare i risultati restituiti dall'API.

Trova maggiori informazioni

- ["Creare e gestire risorse di cluster di archiviazione"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Configurare l'accesso all'interfaccia utente Web del nome di dominio completo

L'archiviazione all-flash SolidFire con software NetApp Element 12.2 o versione successiva consente di accedere alle interfacce Web del cluster di archiviazione 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 archiviazione 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 quali gestori di chiavi e provider di identità per l'autenticazione a più fattori.

Cosa ti servirà

- Questa funzionalità richiede Element 12.2 o versione successiva.
- Per configurare questa funzionalità tramite le API REST NetApp Hybrid Cloud Control sono necessari i servizi di gestione 2.15 o versioni successive.
- Per configurare questa funzionalità tramite l'interfaccia utente di controllo NetApp Hybrid Cloud, è necessario disporre dei servizi di gestione versione 2.19 o successiva.
- Per utilizzare le API REST, è necessario aver distribuito un nodo di gestione che esegue la versione 11.5 o successiva.
- Sono necessari nomi di dominio completi per il nodo di gestione e per ciascun cluster di archiviazione che si risolvano correttamente nell'indirizzo IP del nodo di gestione e in quello di ciascun cluster di archiviazione.

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

- [Configurare l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control](#)
- [Configurare l'accesso all'interfaccia utente Web FQDN utilizzando l'API REST](#)
- [Rimuovere l'accesso all'interfaccia utente Web FQDN tramite NetApp Hybrid Cloud Control](#)
- [Rimuovere l'accesso all'interfaccia utente Web FQDN tramite l'API REST](#)
- [Risoluzione dei problemi](#)

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

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare l'icona del menu in alto a destra della pagina.
4. Selezionare **Configura**.
5. Nel riquadro **Nomi di dominio completi**, seleziona **Configura**.
6. Nella finestra visualizzata, immettere gli FQDN per il nodo di gestione e per ciascun cluster di archiviazione.
7. Seleziona **Salva**.

Nel riquadro **Nomi di dominio completi** sono elencati tutti i cluster di archiviazione con i relativi MVIP e FQDN.



Nel riquadro **Nomi di dominio completi** vengono elencati solo i cluster di storage connessi con l'FQDN impostato.

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

Passi

1. Assicurarsi che i nodi di archiviazione 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 archiviazione e al nodo di gestione, quindi selezionare **Impostazioni di rete > Rete di gestione**.
 - a. Interfaccia utente per nodo per nodi di archiviazione:
`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 archiviazione utilizzando l'API Element.
 - a. Accedi all'API Element e crea la seguente preferenza di interfaccia cluster utilizzando "**CreaPreferenzaInterfacciaCluster**" Metodo API, inserendo l'FQDN MVIP del cluster per il 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. Accedi all'interfaccia utente dell'API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/2/`

Per esempio:

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

- a. Fare clic su **Autorizza** o su qualsiasi icona a forma di lucchetto e immettere il nome utente e la password del cluster.
- b. Inserisci l'ID cliente come `mnode-client`.
- c. Fare clic su **Autorizza** per iniziare la sessione e quindi chiudere la finestra.
- d. Dall'elenco dei server, seleziona `mnode2`.
- e. Fare clic su **OTTIENI /impostazioni**.
- f. Fai clic su **Provalo**.
- g. Fare clic su **Esegui**.
- h. Registrare tutte le impostazioni proxy riportate nel corpo della risposta.
- i. Fare clic su **METTI/impostazioni**.
- j. Fai clic su **Provalo**.
- k. Nell'area del corpo della richiesta, immettere il nome di dominio completo del nodo di gestione come valore per `mnode_fqdn` parametro.
- l. Inserisci tutti i valori delle impostazioni proxy registrati in precedenza nei parametri rimanenti nel corpo della richiesta. Se si lasciano vuoti i parametri proxy o non li si include nel corpo della richiesta, le impostazioni proxy esistenti verranno rimosse.
- m. Fare clic su **Esegui**.

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

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

Passi

1. Nel riquadro **Nomi di dominio completi**, seleziona **Modifica**.
2. Nella finestra visualizzata, eliminare il contenuto del campo di testo **FQDN**.
3. Seleziona **Salva**.

La finestra si chiude e il nome di dominio completo non è più elencato nel riquadro **Nomi di dominio completi**.

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

Passi

1. Modificare le impostazioni del cluster di archiviazione utilizzando l'API Element.
 - a. Accedi all'API Element ed elimina la seguente preferenza dell'interfaccia cluster utilizzando DeleteClusterInterfacePreference Metodo API:

- Nome: mvip_fqdn

Per 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. Accedi all'interfaccia utente dell'API REST per il nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da /mnode/2/ . Per esempio:

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

- b. Selezionare **Autorizza** o qualsiasi icona a forma di lucchetto e immettere il nome utente e la password del cluster Element.
 - c. Inserisci l'ID cliente come mnode-client .
 - d. Selezionare **Autorizza** per iniziare una sessione.
 - e. Chiudi la finestra.
 - f. Selezionare **METTI /impostazioni**.
 - g. Seleziona **Provalo**.
 - h. Nell'area del corpo della richiesta, non immettere un valore per mnode_fqdn parametro. Specificare anche se deve essere utilizzato il proxy(true O false) per il use_proxy parametro.

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

- i. Selezionare **Esegui**.

Risoluzione dei problemi

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

Problema	Causa	Risoluzione
• Si verifica un errore del browser quando si tenta di accedere al nodo di gestione o al cluster di archiviazione utilizzando l'FQDN. • Non è possibile accedere al nodo di gestione o al cluster di archiviazione utilizzando un indirizzo IP.	Sia il nome di dominio completo del nodo di gestione che il nome di dominio completo del cluster di archiviazione sono configurati in modo errato.	Utilizzare le istruzioni dell'API REST in questa pagina per rimuovere le impostazioni FQDN del nodo di gestione e del cluster di archiviazione e configurarle nuovamente.
• Si verifica un errore del browser quando si tenta di accedere al nome di dominio completo del cluster di archiviazione. • Non è possibile accedere al nodo di gestione o al cluster di archiviazione utilizzando un indirizzo IP.	Il nome di dominio completo del nodo di gestione è configurato correttamente, ma il nome di dominio completo del cluster di archiviazione non è configurato correttamente.	Utilizzare le istruzioni dell'API REST in questa pagina per rimuovere le impostazioni FQDN del cluster di archiviazione e configurarle nuovamente
• Si verifica un errore del browser quando si tenta di accedere al nome di dominio completo del nodo di gestione. • È possibile accedere al nodo di gestione e al cluster di archiviazione utilizzando un indirizzo IP.	Il nome di dominio completo del nodo di gestione non è configurato correttamente, ma il nome di dominio completo del cluster di archiviazione è configurato correttamente.	Accedi a NetApp Hybrid Cloud Control per correggere le impostazioni FQDN del nodo di gestione nell'interfaccia utente oppure utilizza le istruzioni dell'API REST in questa pagina per correggere le impostazioni.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Crea e gestisci account utente utilizzando NetApp Hybrid Cloud Control

Nei sistemi di storage basati su Element, è possibile creare utenti cluster autorevoli per abilitare l'accesso a NetApp Hybrid Cloud Control, a seconda delle autorizzazioni che si desidera concedere agli utenti "Amministratore" o "Sola lettura". Oltre agli utenti del cluster, esistono anche account di volume, che consentono ai client di connettersi ai volumi su un nodo di archiviazione.

Gestisci i seguenti tipi di account:

- [Gestire gli account autorevoli del cluster](#)

- [Gestire gli account di volume](#)

Abilita LDAP

Per utilizzare LDAP per qualsiasi account utente, è necessario prima abilitare LDAP.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona l'icona Opzioni in alto a destra e seleziona **Gestione utenti**.
3. Dalla pagina Utenti, seleziona **Configura LDAP**.
4. Definisci la tua configurazione LDAP.
5. Selezionare il tipo di autenticazione tra Cerca e associa o Assegna direttamente.
6. Prima di salvare le modifiche, seleziona **Test LDAP Log In** nella parte superiore della pagina, inserisci il nome utente e la password di un utente che sai esistere e seleziona **Test**.
7. Seleziona **Salva**.

Gestire gli account autorevoli del cluster

"Account utente autorevoli" sono gestiti dall'opzione Gestione utenti nel menu in alto a destra in NetApp Hybrid Cloud Control. Questi tipi di account consentono di eseguire l'autenticazione su 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 altro ancora su tutti i cluster.

Crea un account cluster autorevole

È possibile creare un account utilizzando NetApp Hybrid Cloud Control.

Questo account può essere utilizzato per accedere a Hybrid Cloud Control, all'interfaccia utente per nodo del cluster e al cluster di storage nel software NetApp Element .

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona l'icona Opzioni in alto a destra e seleziona **Gestione utenti**.
3. Seleziona **Crea utente**.
4. Selezionare il tipo di autenticazione cluster o LDAP.
5. Completa una delle seguenti operazioni:
 - Se hai selezionato LDAP, inserisci il DN.



Per utilizzare LDAP, è necessario prima abilitare LDAP o LDAPS. Vedere [Abilita LDAP](#) .

- Se hai selezionato Cluster come Tipo di autenticazione, inserisci un nome e una password per il nuovo account.
6. Selezionare le autorizzazioni Amministratore o Sola lettura.



Per visualizzare le autorizzazioni del software NetApp Element , selezionare **Mostra autorizzazioni legacy**. Se si seleziona un sottoinsieme di queste autorizzazioni, all'account vengono assegnate autorizzazioni di sola lettura. Se selezioni 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 amministrazione dell'organizzazione DN nel server LDAP. Tutti gli account figlio di quel gruppo ereditano tali autorizzazioni.

7. Seleziona la casella che indica "Ho letto e accetto il Contratto di licenza con l'utente finale NetApp ".
8. Seleziona **Crea utente**.

Modifica un account cluster autorevole

È possibile modificare le autorizzazioni o la password di un account utente utilizzando NetApp Hybrid Cloud Control.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona l'icona in alto a destra e seleziona **Gestione utenti**.
3. Facoltativamente, filtrare l'elenco degli account utente selezionando **Cluster, LDAP o Idp**.

Se hai configurato gli utenti sul cluster di archiviazione con LDAP, tali account mostrano il tipo di utente "LDAP". Se hai configurato gli utenti sul cluster di archiviazione con Idp, tali account mostreranno il tipo di utente "Idp".

4. Nella colonna **Azioni** della tabella, espandi il menu dell'account e seleziona **Modifica**.
5. Apportare le modifiche necessarie.
6. Seleziona **Salva**.
7. Disconnettersi da NetApp Hybrid Cloud Control.



Potrebbero essere necessari fino a 2 minuti affinché l'interfaccia utente di controllo NetApp Hybrid Cloud aggiorni l'inventario. Per aggiornare manualmente l'inventario, accedi al servizio di inventario dell'interfaccia utente dell'API REST `https://[management node IP]/inventory/1/` e correre `GET /installations/{id}` per il cluster.

8. Accedi a NetApp Hybrid Cloud Control.

Elimina un account utente autorevole

Puoi eliminare uno o più account quando non ti servono più. È possibile eliminare un account utente LDAP.

Non è possibile eliminare l'account utente amministratore principale per il cluster autorevole.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona l'icona in alto a destra e seleziona **Gestione utenti**.

3. Nella colonna **Azioni** della tabella Utenti, espandi il menu per l'account e seleziona **Elimina**.
4. Confermare l'eliminazione selezionando **Sì**.

Gestire gli account di volume

"Conti di volume" sono gestiti all'interno della tabella NetApp Hybrid Cloud Control Volumes. Questi account sono specifici solo del cluster di archiviazione su cui sono stati creati. Questi tipi di account consentono di impostare autorizzazioni sui volumi in rete, ma non hanno alcun effetto al di fuori di tali volumi.

Un account volume contiene l'autenticazione CHAP necessaria per accedere ai volumi ad esso assegnati.

Crea un account di volume

Crea un account specifico per questo volume.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona **Archiviazione > Volumi**.
3. Selezionare la scheda **Account**.
4. Selezionare il pulsante **Crea account**.
5. Inserisci un nome per il nuovo account.
6. Nella sezione Impostazioni CHAP, immettere le seguenti informazioni:
 - Segreto dell'iniziatore per l'autenticazione della sessione del nodo CHAP
 - Segreto di destinazione per l'autenticazione della sessione del nodo CHAP



Per generare automaticamente una delle due password, lasciare vuoti i campi delle credenziali.

7. Seleziona **Crea account**.

Modifica un account di volume

È possibile modificare le informazioni CHAP e stabilire se un account è attivo o bloccato.



L'eliminazione o il blocco di un account associato al nodo di gestione rende il nodo di gestione inaccessibile.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona **Archiviazione > Volumi**.
3. Selezionare la scheda **Account**.
4. Nella colonna **Azioni** della tabella, espandi il menu dell'account e seleziona **Modifica**.
5. Apportare le modifiche necessarie.
6. Confermare le modifiche selezionando **Sì**.

Elimina un account di volume

Elimina un account di cui non hai più bisogno.

Prima di eliminare un account volume, eliminare e ripulire tutti i volumi associati all'account.



L'eliminazione o il blocco di un account associato al nodo di gestione rende il 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 elimini questi account, potresti rendere inutilizzabile il tuo nodo di gestione.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, seleziona **Archiviazione > Volumi**.
3. Selezionare la scheda **Account**.
4. Nella colonna **Azioni** della tabella, espandi il menu dell'account e seleziona **Elimina**.
5. Confermare l'eliminazione selezionando **Sì**.

Trova maggiori informazioni

- ["Scopri di più sugli account"](#)
- ["Lavorare con gli account utilizzando CHAP"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Crea e gestisci 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.

È possibile gestire i volumi in NetApp Hybrid Cloud Control nei seguenti modi:

- [Crea un volume](#)
- [Applicare una policy QoS a un volume](#)
- [Modifica un volume](#)
- [Clona volumi](#)
- [Aggiungere volumi a un gruppo di accesso al volume](#)
- [Elimina un volume](#)

- [Ripristina un volume eliminato](#)
- [Elimina un volume eliminato](#)

Crea un volume

È possibile creare un volume di archiviazione utilizzando NetApp Hybrid Cloud Control.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare la scheda **Volumi > Panoramica**.

OVERVIEW ACCESS GROUPS ACCOUNTS INITIATORS QOS POLICIES													
VOLUMES Overview													
Active Deleted Create Volume Actions													
☐	ID ↑	Name	Account	Access Groups	Access	Used	Size	Snapshots	QoS Policy	Min IOPS	Max IOPS	Burst IOPS	ISCSI Sessions Actions
☐	1	NetApp-HCI-Datastore-01	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	4%	2.15 TB	0		50	15000	15000	2 ⋮
☐	2	NetApp-HCI-Datastore-02	NetApp-HCI	NetApp-HCI-6ee7b8e7...	Read/Write	0%	2.15 TB	0		50	15000	15000	2 ⋮
☐	3	NetApp-HCI-credential...			Read/Write	0%	5.37 GB	0		1000	2000	4000	1 ⋮
☐	4	NetApp-HCI-mnode-api			Read/Write	0%	53.69 GB	0		1000	2000	4000	1 ⋮
☐	5	NetApp-HCI-hci-monitor			Read/Write	0%	1.07 GB	0		1000	2000	4000	1 ⋮

4. Selezionare **Crea volume**.
5. Inserisci un nome per il nuovo volume.
6. Inserisci la dimensione totale 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**, seleziona l'account che deve avere accesso al volume.

Se non esiste un account, seleziona **Crea nuovo account**, inserisci un nuovo nome account e seleziona **Crea account**. L'account viene creato e associato al nuovo volume nell'elenco **Account**.



Se ci sono più di 50 account, l'elenco non viene visualizzato. Inizia a digitare e la funzione di completamento automatico ti mostrerà i valori tra cui scegliere.

9. Per configurare la qualità del servizio per il volume, procedere in uno dei seguenti modi:
 - In **Impostazioni qualità del servizio**, imposta valori minimi, massimi e burst personalizzati per IOPS oppure utilizza i valori QoS predefiniti.
 - Selezionare un criterio QoS esistente attivando l'opzione **Assegna criterio di qualità del servizio** e scegliendo un criterio QoS esistente dall'elenco risultante.
 - Crea e assegna una nuova policy QoS abilitando l'opzione **Assegna policy di qualità del servizio** e selezionando **Crea nuova policy QoS**. Nella finestra visualizzata, immettere un nome per la policy QoS, quindi immettere i valori QoS. Al termine, seleziona **Crea policy sulla qualità del servizio**.

I volumi con un valore Max o Burst IOPS superiore a 20.000 IOPS potrebbero richiedere un'elevata profondità di coda o più sessioni per raggiungere questo livello di IOPS su un singolo volume.

10. Selezionare **Crea volume**.

Applicare una policy QoS a un volume

È possibile applicare una policy QoS ai volumi di storage esistenti utilizzando NetApp Hybrid Cloud Control. Se invece è necessario impostare valori QoS personalizzati per un volume, è possibile [Modifica un volume](#). Per creare una nuova policy QoS, vedere ["Creare e gestire policy QoS del volume"](#).

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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 **Azioni** nella parte superiore della tabella dei volumi e selezionare **Applica criterio QoS**.
6. Nella finestra visualizzata, seleziona un criterio QoS dall'elenco e seleziona **Applica criterio QoS**.



Se si utilizzano criteri QoS su un volume, è possibile impostare un QoS personalizzato per rimuovere l'affiliazione del criterio QoS al volume. I valori QoS personalizzati sostituiscono i valori dei criteri QoS per le impostazioni QoS del volume.

Modifica un volume

Utilizzando NetApp Hybrid Cloud Control, è possibile modificare gli attributi del volume, quali i valori QoS, le dimensioni del volume e l'unità di misura con cui vengono calcolati i valori dei byte. È anche possibile modificare l'accesso all'account per l'utilizzo della replica o per limitare l'accesso al volume.

Informazioni su questo compito

È possibile ridimensionare un volume quando c'è spazio sufficiente sul cluster nelle seguenti condizioni:

- Condizioni operative normali.
- Vengono segnalati errori o guasti del volume.
- Il volume è in fase di clonazione.
- Il volume è in fase di risincronizzazione.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi > Panoramica**.
4. Nella colonna **Azioni** della tabella dei volumi, espandere il menu per il volume e selezionare **Modifica**.
5. Apportare le modifiche necessarie:

a. Modifica la dimensione totale del volume.



È possibile aumentare, ma non diminuire, la dimensione del volume. È possibile ridimensionare un solo volume in un'unica operazione di ridimensionamento. Le operazioni di garbage collection e gli aggiornamenti software non interrompono l'operazione di ridimensionamento.



Se si desidera modificare le dimensioni del volume per la replica, aumentare innanzitutto le dimensioni del volume assegnato come destinazione della replica. Quindi puoi ridimensionare il volume sorgente. Il volume di destinazione può essere maggiore o uguale al volume di origine, ma non può essere minore.



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. Seleziona un livello di accesso all'account diverso:

- Solo lettura
- Lettura/scrittura
- Bloccato
- Obiettivo di replicazione

c. Selezionare l'account che deve avere accesso al volume.

Inizia a digitare e la funzione di completamento automatico ti mostrerà i possibili valori tra cui scegliere.

Se non esiste un account, seleziona **Crea nuovo account**, inserisci un nuovo nome account e seleziona **Crea**. L'account viene creato e associato al volume esistente.

d. Modifica la qualità del servizio eseguendo una delle seguenti operazioni:

- i. Seleziona una policy esistente.
- ii. In Impostazioni personalizzate, imposta i valori minimo, massimo e burst per IOPS oppure utilizza i valori predefiniti.



Se si utilizzano criteri QoS su un volume, è possibile impostare un QoS personalizzato per rimuovere l'affiliazione del criterio QoS al volume. La QoS personalizzata sovrascriverà i valori dei criteri QoS per le impostazioni QoS del volume.



Quando si modificano i valori IOPS, è necessario incrementarli 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 di grandi dimensioni, limitando comunque gli IOPS sostenuti per un volume.

6. Seleziona **Salva**.

Clona volumi

È possibile creare un clone di un singolo volume di archiviazione o clonare un gruppo di volumi per creare una

copia dei dati in un dato momento. Quando si clona un volume, il sistema crea uno snapshot del volume e quindi crea 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 non provisioning deve essere uguale o superiore alla dimensione del volume.

Informazioni su questo compito

Il cluster supporta fino a due richieste di clonazione in esecuzione per volume alla volta e fino a 8 operazioni di clonazione di volumi attivi alla volta. Le richieste che superano questi limiti vengono messe in coda per essere elaborate in un secondo momento.

La clonazione del volume è un processo asincrono e la quantità di tempo richiesta dipende dalle dimensioni del volume che si sta clonando e dal carico attuale del cluster.



I volumi clonati non ereditano l'appartenenza al gruppo di accesso al volume dal volume di origine.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare la scheda **Volumi > Panoramica**.
4. Seleziona ogni volume che vuoi clonare.
5. Selezionare l'elenco a discesa **Azioni** nella parte superiore della tabella dei volumi e selezionare **Clona**.
6. Nella finestra visualizzata, procedi come segue:
 - a. Immettere un prefisso per il nome del volume (facoltativo).
 - b. Selezionare il tipo di accesso dall'elenco **Accesso**.
 - c. Selezionare un account da associare al nuovo clone del volume (per impostazione predefinita, è selezionato **Copia dal volume**, che utilizzerà lo stesso account utilizzato dal volume originale).
 - d. Se non esiste un account, seleziona **Crea nuovo account**, inserisci un nuovo nome account e seleziona **Crea account**. L'account viene creato e associato al volume.



Utilizzare le migliori pratiche di denominazione descrittiva. Ciò è particolarmente importante se nel tuo ambiente vengono utilizzati più cluster o vCenter Server.



Aumentando la dimensione del volume di un clone si ottiene un nuovo volume con spazio libero aggiuntivo alla fine del volume. A seconda di come si utilizza il volume, potrebbe essere necessario estendere le partizioni o creare nuove partizioni nello spazio libero per poterlo utilizzare.

- a. Selezionare **Clona volumi**.



Il tempo necessario per completare un'operazione di clonazione è influenzato dalle dimensioni del volume e dal carico attuale del cluster. Aggiornare la pagina se il volume clonato non appare 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.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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 dei volumi e selezionare **Aggiungi al gruppo di accesso**.
6. Nella finestra visualizzata, seleziona un gruppo di accesso al volume dall'elenco **Gruppo di accesso al volume**.
7. Selezionare **Aggiungi volume**.

Elimina un volume

È possibile eliminare uno o più volumi da un cluster di archiviazione Element.

Informazioni su questo compito

Il sistema non elimina immediatamente i volumi eliminati; questi rimangono disponibili per circa otto ore. Dopo otto ore vengono eliminati e non sono più disponibili. Se si ripristina un volume prima che il sistema lo elimini, il volume torna online e le connessioni iSCSI vengono ripristinate.

Se un volume utilizzato per creare uno snapshot viene eliminato, gli snapshot associati diventano inattivi. Quando i volumi di origine eliminati vengono eliminati, anche gli snapshot inattivi associati vengono rimossi 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 elimini questi volumi, potresti rendere inutilizzabile il tuo nodo di gestione.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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 dei volumi e selezionare **Elimina**.
6. Nella finestra visualizzata, confermare l'azione selezionando **Sì**.

Ripristina un volume eliminato

Dopo aver eliminato un volume di archiviazione, è ancora possibile ripristinarlo se lo si fa entro otto ore dall'eliminazione.

Il sistema non elimina immediatamente i volumi eliminati; questi rimangono disponibili per circa otto ore. Dopo otto ore vengono eliminati e non sono più disponibili. Se si ripristina un volume prima che il sistema lo elimini, il volume torna online e le connessioni iSCSI vengono ripristinate.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi > Panoramica**.
4. Seleziona **Eliminato**.
5. Nella colonna **Azioni** della tabella Volumi, espandere il menu per il volume e selezionare **Ripristina**.
6. Confermare il processo selezionando **Sì**.

Elimina un volume eliminato

Una volta eliminati, i volumi di archiviazione rimangono disponibili per circa otto ore. Dopo otto ore vengono eliminati automaticamente e non sono più disponibili. Se non vuoi aspettare le otto ore, puoi eliminare

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi > Panoramica**.
4. Seleziona **Eliminato**.
5. Selezionare uno o più volumi da eliminare.
6. Eseguire una delle seguenti operazioni:
 - Se hai selezionato più volumi, seleziona il filtro rapido **Elimina** nella parte superiore della tabella.
 - Se hai selezionato un singolo volume, nella colonna **Azioni** della tabella Volumi, espandi il menu per il volume e seleziona **Elimina**.
7. Nella colonna **Azioni** della tabella Volumi, espandere il menu per il volume e selezionare **Elimina**.
8. Confermare il processo selezionando **Sì**.

Trova maggiori informazioni

- ["Scopri di più sui volumi"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Creare e gestire gruppi di accesso al volume

È possibile creare nuovi gruppi di accesso al volume, apportare modifiche al nome, agli iniziatori associati o ai volumi associati dei gruppi di accesso oppure eliminare gruppi di accesso al volume esistenti utilizzando NetApp Hybrid Cloud Control.

Cosa ti servirà

- Disponi delle credenziali di amministratore per questo sistema di archiviazione all-flash SolidFire .
- Hai aggiornato i tuoi servizi di gestione almeno alla versione 2.15.28. La gestione dello storage NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti del pacchetto di servizi.
- Assicurarsi di disporre di uno schema di denominazione logico per i gruppi di accesso al volume.

Aggiungi un gruppo di accesso al volume

È possibile aggiungere un gruppo di accesso al volume a un cluster di storage utilizzando NetApp Hybrid Cloud Control.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi**.
4. Selezionare la scheda **Gruppi di accesso**.
5. Selezionare il pulsante **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 **Iniziatori**, seleziona 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 bisogno di autenticazione.

8. (Facoltativo) Nella sezione **Volumi**, seleziona uno o più volumi da includere in questo gruppo di accesso al volume.
9. Selezionare **Crea gruppo di accesso**.

Modifica un gruppo di accesso al volume

È possibile modificare le proprietà di un gruppo di accesso al volume esistente utilizzando NetApp Hybrid Cloud Control. È possibile apportare modifiche al nome, agli iniziatori associati o ai volumi associati di un gruppo di accesso.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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, espandi il menu delle opzioni per il gruppo di accesso che devi modificare.
6. Nel menu delle opzioni, seleziona **Modifica**.
7. Apportare le modifiche necessarie al nome, agli iniziatori associati o ai volumi associati.
8. Conferma le modifiche selezionando **Salva**.
9. Nella tabella **Gruppi di accesso**, verificare che il gruppo di accesso rifletta le modifiche.

Elimina un gruppo di accesso al volume

È possibile rimuovere un gruppo di accesso al volume utilizzando NetApp Hybrid Cloud Control e contemporaneamente rimuovere dal sistema gli iniziatori associati a questo gruppo di accesso.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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, espandi il menu delle opzioni per il gruppo di accesso che devi eliminare.
6. Nel menu delle opzioni, seleziona **Elimina**.
7. Se non si desidera eliminare gli iniziatori associati al gruppo di accesso, deselezionare la casella di controllo **Elimina iniziatori in questo gruppo di accesso**.
8. Confermare l'operazione di eliminazione selezionando **Sì**.

Trova maggiori informazioni

- ["Scopri di più sui gruppi di accesso al volume"](#)
- ["Aggiungi l'iniziatore a un gruppo di accesso al volume"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Creare e gestire gli iniziatori

Puoi usare **"iniziatori"** per l'accesso ai volumi basato su CHAP anziché su account. È possibile creare ed eliminare iniziatori e assegnare loro alias intuitivi per semplificare l'amministrazione e l'accesso al volume. Quando si aggiunge un iniziatore a un gruppo di accesso al volume, tale iniziatore consente l'accesso a tutti i volumi nel gruppo.

Cosa ti servirà

- Hai le credenziali di amministratore del cluster.
- Hai aggiornato i tuoi servizi di gestione almeno alla versione 2.17. La gestione dell'iniziatore NetApp Hybrid Cloud Control non è disponibile nelle versioni precedenti del pacchetto di servizi.

Opzioni

- [Creare un iniziatore](#)
- [Aggiungere iniziatori a un gruppo di accesso al volume](#)
- [Cambiare un alias di iniziatore](#)
- [Elimina gli iniziatori](#)

Creare un iniziatore

È possibile creare iniziatori iSCSI o Fibre Channel e, facoltativamente, assegnare loro degli alias.

Informazioni su questo compito

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(-). 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` O `AabBCCdd11223344` . Un esempio del formato è il seguente:

```
5f:47:ac:c0:5c:74:d4:02
```

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi**.
4. Selezionare la scheda **Iniziatori**.
5. Selezionare il pulsante **Crea iniziatori**.

Opzione	Passi
Creare uno o più iniziatori	a. Inserire l'IQN o il WWPN dell'iniziatore nel campo IQN/WWPN. b. Inserisci un nome descrittivo per l'iniziatore nel campo Alias. c. (Facoltativo) Selezionare Aggiungi iniziatore per aprire nuovi campi iniziatore oppure utilizzare l'opzione di creazione in blocco. d. Seleziona Crea iniziatori.

Opzione	Passi
Creazione in blocco di iniziatori	- Seleziona Aggiungi IQN/WWPN in blocco. - Inserire un elenco di IQN o WWPN nella casella di testo. Ogni IQN o WWPN deve essere separato da virgole o spazi oppure deve trovarsi su una riga a sé stante. - Selezionare Aggiungi IQN/WWPN. (Facoltativo) Aggiungere alias univoci a ciascun iniziatore. - Rimuovere dall'elenco qualsiasi iniziatore che potrebbe già essere presente nell'installazione. - Seleziona Crea iniziatori.

Aggiungere iniziatori a un gruppo di accesso al volume

È possibile aggiungere 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 quel gruppo di accesso al volume.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi**.
4. Selezionare la scheda **Iniziatori**.
5. Seleziona uno o più iniziatori che desideri aggiungere.
6. Selezionare **Azioni > Aggiungi al gruppo di accesso**.
7. Selezionare il gruppo di accesso.
8. Conferma le modifiche selezionando **Aggiungi iniziatore**.

Cambiare un alias di iniziatore

È possibile modificare l'alias di un iniziatore esistente o aggiungerne uno nuovo se non ne esiste già uno.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione 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 oppure aggiungerne uno nuovo.
8. Seleziona **Salva**.

Elimina gli iniziatori

È possibile eliminare uno o più iniziatori. Quando si elimina un iniziatore, il sistema lo rimuove da tutti i gruppi di accesso al volume associati. Tutte le connessioni che utilizzano l'iniziatore rimangono valide finché la connessione non viene reimpostata.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il nome del tuo cluster di archiviazione nel menu di navigazione a sinistra.
3. Selezionare **Volumi**.
4. Selezionare la scheda **Iniziatori**.
5. Elimina uno o più iniziatori:
 - a. Seleziona uno o più iniziatori che desideri eliminare.
 - b. Selezionare **Azioni > Elimina**.
 - c. Confermare l'operazione di eliminazione e selezionare **Sì**.

Trova maggiori informazioni

- ["Scopri di più sugli iniziatori"](#)
- ["Scopri di più sui gruppi di accesso al volume"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Creare e gestire policy QoS del volume

Una policy QoS (Quality of Service) consente di creare e salvare un'impostazione standardizzata della qualità del servizio che può essere applicata a molti volumi. Per utilizzare i criteri QoS, il cluster selezionato deve essere Element 10.0 o versione successiva; in caso contrario, le funzioni dei criteri QoS non saranno disponibili.



Per ulteriori informazioni sull'utilizzo, consultare il contenuto dei concetti di archiviazione all-flash SolidFire ["Criteri QoS"](#) invece del volume individuale ["Qualità del servizio"](#).

Utilizzando NetApp Hybrid Cloud Control, è possibile creare e gestire policy QoS completando le seguenti attività:

- [Creare una policy QoS](#)
- [Applicare una policy QoS a un volume](#)
- [Modificare l'assegnazione della policy QoS di un volume](#)
- [Modifica una policy QoS](#)

- [Eliminare una policy QoS](#)

Creare una policy QoS

È possibile creare criteri QoS e applicarli ai volumi che devono avere prestazioni equivalenti.



Se si utilizzano criteri QoS, non utilizzare QoS personalizzati su un volume. La QoS personalizzata sovrascriverà e regolerà i valori dei criteri QoS per le impostazioni QoS del volume.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il menu per il tuo cluster di archiviazione.
3. Selezionare **Archiviazione > Volumi**.
4. Selezionare la scheda **Criteri QoS**.
5. Selezionare **Crea criterio**.
6. Inserisci il **Nome della polizza**.



Utilizzare le migliori pratiche di denominazione descrittiva. Ciò è particolarmente importante se nel tuo ambiente vengono utilizzati più cluster o vCenter Server.

7. Immettere i valori IOPS minimi, IOPS massimi e IOPS burst.
8. Selezionare **Crea criterio QoS**.

Per il criterio viene generato un ID di sistema e il criterio viene visualizzato nella pagina Criteri QoS con i valori QoS assegnati.

Applicare una policy QoS a un volume

È possibile assegnare una policy QoS esistente a un volume utilizzando NetApp Hybrid Cloud Control.

Cosa ti servirà

La politica QoS che si desidera assegnare è stata [creato](#).

Informazioni su questo compito

Questa attività descrive come assegnare un criterio QoS a un singolo volume modificandone le impostazioni. L'ultima versione di NetApp Hybrid Cloud Control non dispone di un'opzione di assegnazione in blocco per più di un volume. Finché la funzionalità di assegnazione in blocco non verrà fornita in una versione futura, è possibile utilizzare l'interfaccia utente Web di Element o l'interfaccia utente del plug-in vCenter per assegnare in blocco i criteri QoS.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il menu per il tuo cluster di archiviazione.
3. Selezionare **Archiviazione > Volumi**.

4. Selezionare il menu **Azioni** accanto al volume che si intende modificare.
5. Nel menu che si apre, seleziona **Modifica**.
6. Nella finestra di dialogo, abilitare **Assegna criterio QoS** e selezionare il criterio QoS dall'elenco a discesa da applicare al volume selezionato.



L'assegnazione di QoS sovrascriverà tutti i valori QoS dei singoli volumi applicati in precedenza.

7. Seleziona **Salva**.

Modificare l'assegnazione della policy QoS di un volume

È possibile rimuovere l'assegnazione di un criterio QoS da un volume oppure selezionare un criterio QoS diverso o un QoS personalizzato.

Cosa ti servirà

Il volume che vuoi modificare è **assegnato** una politica QoS.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il menu per il tuo cluster di archiviazione.
3. Selezionare **Archiviazione > Volumi**.
4. Selezionare il menu **Azioni** accanto al volume che si intende modificare.
5. Nel menu che si apre, seleziona **Modifica**.
6. Nella finestra di dialogo, effettuare una delle seguenti operazioni:
 - Disabilitare **Assegna criterio QoS** e modificare i valori **Min IOPS**, **Max IOPS** e **Burst IOPS** per la QoS del singolo volume.



Quando i criteri QoS sono disabilitati, il volume utilizza i valori QoS IOPS predefiniti, salvo diversa modifica.

- Selezionare un criterio QoS diverso dall'elenco a discesa da applicare al volume selezionato.
7. Seleziona **Salva**.

Modifica una policy QoS

È possibile modificare il nome di un criterio QoS esistente o modificare i valori associati al criterio. La modifica dei valori delle prestazioni della policy QoS influisce sulla QoS per tutti i volumi associati alla policy.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il menu per il tuo cluster di archiviazione.
3. Selezionare **Archiviazione > Volumi**.
4. Selezionare la scheda **Criteri QoS**.

5. Selezionare il menu **Azioni** accanto alla policy QoS che si intende modificare.
6. Selezionare **Modifica**.
7. Nella finestra di dialogo **Modifica criterio QoS**, modifica una o più delle seguenti opzioni:
 - **Nome**: nome definito dall'utente per la policy QoS.
 - **MIN IOPS**: numero minimo di IOPS garantiti per il volume. Predefinito = 50.
 - **IOPS massimi**: numero massimo di IOPS consentiti per il volume. Predefinito = 15.000.
 - **Burst IOPS**: il numero massimo di IOPS consentiti in un breve periodo di tempo per il volume. Predefinito = 15.000.
8. Seleziona **Salva**.



È possibile selezionare il collegamento nella colonna **Volumi attivi** per una policy per visualizzare un elenco filtrato dei volumi assegnati a tale policy.

Eliminare una policy QoS

È possibile eliminare un criterio QoS se non è più necessario. Quando si elimina un criterio QoS, tutti i volumi a cui è assegnato il criterio mantengono i valori QoS precedentemente definiti dal criterio, ma come QoS del volume individuale. Qualsiasi associazione con la policy QoS eliminata viene rimossa.

Passi

1. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
2. Dalla Dashboard, espandi il menu per il tuo cluster di archiviazione.
3. Selezionare **Archiviazione > Volumi**.
4. Selezionare la scheda **Criteri QoS**.
5. Selezionare il menu **Azioni** accanto alla policy QoS che si intende modificare.
6. Seleziona **Elimina**.
7. Conferma l'azione.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Monitora il tuo sistema SolidFire con NetApp Hybrid Cloud Control

Monitora le risorse di archiviazione sulla dashboard di controllo del cloud ibrido

Con la NetApp Hybrid Cloud Control Dashboard puoi visualizzare tutte le tue risorse di storage a colpo d'occhio. Inoltre, è possibile monitorare la capacità e le prestazioni di archiviazione.



Quando si avvia per la prima volta una nuova sessione di NetApp Hybrid Cloud Control, potrebbe verificarsi un ritardo nel caricamento della vista Dashboard NetApp Hybrid Cloud Control quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia a seconda del numero di cluster gestiti attivamente dal nodo di gestione. Nei lanci successivi i tempi di caricamento saranno più rapidi.

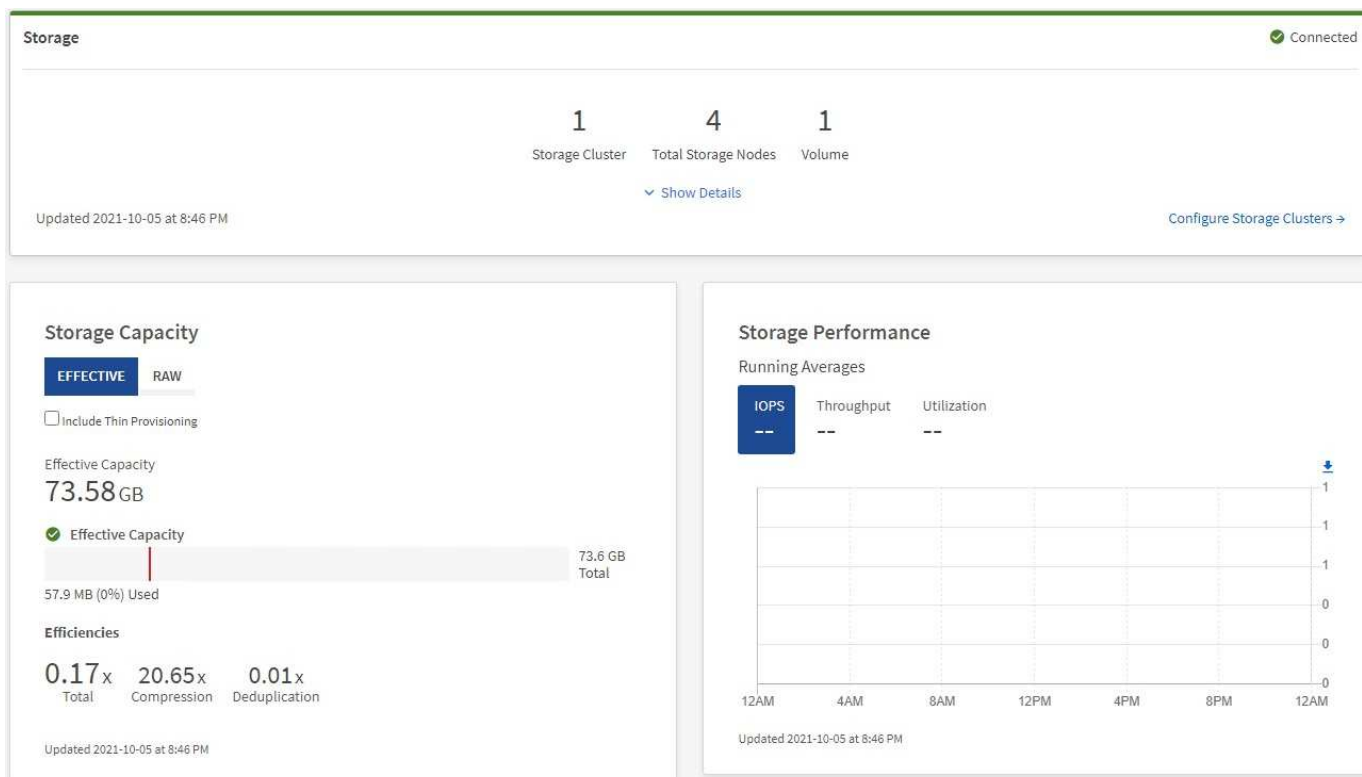
- [Accedi alla dashboard NetApp HCC](#)
- [Monitorare le risorse di archiviazione](#)
- [Monitorare la capacità di archiviazione](#)
- [Monitorare le prestazioni di archiviazione](#)

Accedi alla dashboard NetApp HCC

1. Aprire l'indirizzo IP del nodo di gestione in un browser web. Per esempio:

```
https://[management node IP address]
```

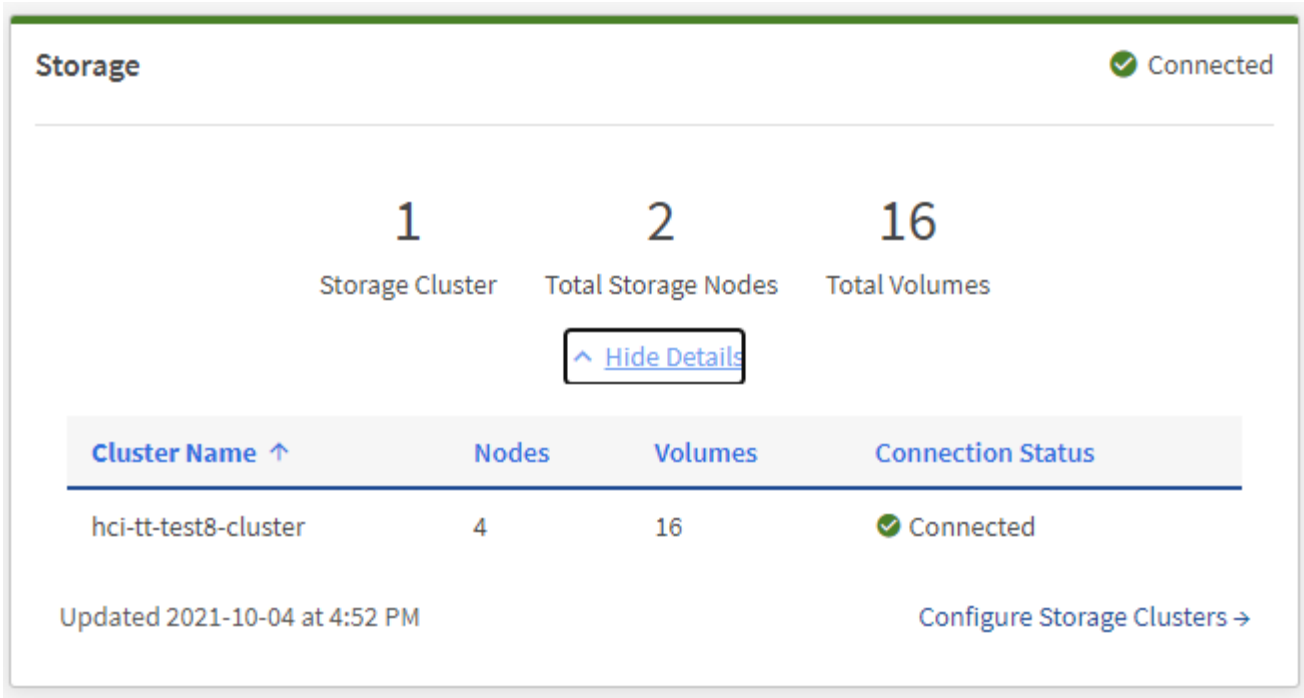
2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire .
3. Visualizza la dashboard di controllo del cloud ibrido.



Monitorare le risorse di archiviazione

Utilizzare il riquadro **Archiviazione** per visualizzare l'ambiente di archiviazione complessivo. È possibile monitorare il numero di cluster di archiviazione, nodi di archiviazione e volumi totali.

Per visualizzare i dettagli, nel riquadro Archiviazione, seleziona **Mostra dettagli**.



Il numero totale di nodi di archiviazione non include i nodi di controllo dei cluster di archiviazione a due nodi. I nodi testimone sono inclusi nel numero di nodi nella sezione dei dettagli per quel cluster.



Per visualizzare i dati più recenti del cluster di archiviazione, utilizzare la pagina Cluster di archiviazione, in cui il polling avviene con maggiore frequenza rispetto alla Dashboard.

Monitorare la capacità di archiviazione

Monitorare la capacità di archiviazione del tuo ambiente è fondamentale. Utilizzando il riquadro Capacità di archiviazione, è possibile determinare i guadagni in termini di efficienza della capacità di archiviazione con o senza funzionalità di compressione, deduplicazione e thin provisioning abilitate.

Puoi visualizzare lo spazio di archiviazione fisico totale disponibile nel tuo cluster nella scheda **RAW** e le informazioni sullo spazio di archiviazione fornito nella scheda **EFFECTIVE**.



Passi

1. Selezionare la scheda **RAW** per visualizzare lo spazio di archiviazione fisico totale utilizzato e disponibile nel cluster.

Osserva le linee verticali per determinare se la capacità utilizzata è inferiore al totale o alle soglie di avviso, errore o critico. Passa il mouse sulle linee per vedere i dettagli.



È possibile impostare la soglia per l'avviso, che per impostazione predefinita è pari al 3% al di sotto della soglia di errore. Le soglie di errore e critiche sono preimpostate e non configurabili per impostazione predefinita. La soglia di errore indica che nel cluster rimane meno di un nodo di capacità. Per i passaggi sull'impostazione della soglia, vedere ["Impostazione della soglia completa del cluster"](#).



Per i dettagli sulle soglie del cluster correlate all'API Element, vedere ["getClusterFullThreshold"](#) nella documentazione API del software Element. Per visualizzare i dettagli sulla capacità dei blocchi e dei metadati, vedere ["Comprensione dei livelli di pienezza del cluster"](#) nella *documentazione del software Element*.

2. Selezionare la scheda **EFFETTIVO** per visualizzare informazioni sullo spazio di archiviazione totale assegnato agli host connessi e per visualizzare le valutazioni di efficienza.
 - a. Facoltativamente, seleziona **Includi Thin Provisioning** per visualizzare i tassi di efficienza del thin provisioning nel grafico a barre della capacità effettiva.
 - b. **Grafico a barre della capacità effettiva:** osserva le linee verticali per determinare se la capacità utilizzata è inferiore al totale o inferiore alle soglie di avviso, errore o critico. Simile alla scheda Raw, puoi passare il mouse sulle linee verticali per vedere i dettagli.
 - c. **Efficienza:** esamina queste valutazioni per determinare i guadagni in termini di efficienza della capacità di archiviazione con le funzionalità di compressione, deduplicazione e thin provisioning abilitate. Ad esempio, se la compressione viene visualizzata come "1,3x", significa che l'efficienza di archiviazione con la compressione abilitata è 1,3 volte più efficiente rispetto a quando non è abilitata.



L'efficienza totale è uguale a $(\text{maxUsedSpace} * \text{fattore di efficienza}) / 2$, dove $\text{efficiencyFactor} = (\text{thinProvisioningFactor} * \text{deDuplicationFactor} * \text{compressionFactor})$. Se l'opzione Thin Provisioning non è selezionata, non viene inclusa nell'efficienza totale.

- d. Se la capacità di archiviazione effettiva si avvicina a una soglia di errore o critica, valutare la possibilità di cancellare i dati dal sistema.
3. Per ulteriori analisi e contesto storico, vedere ["Dettagli NetApp SolidFire Active IQ"](#).

Monitorare le prestazioni di archiviazione

È possibile verificare quanti IOPS o throughput è possibile ottenere da un cluster senza superare le prestazioni utili di tale risorsa utilizzando il riquadro Prestazioni di archiviazione. Le prestazioni di archiviazione rappresentano il punto in cui si ottiene il massimo utilizzo prima che la latenza diventi un problema.

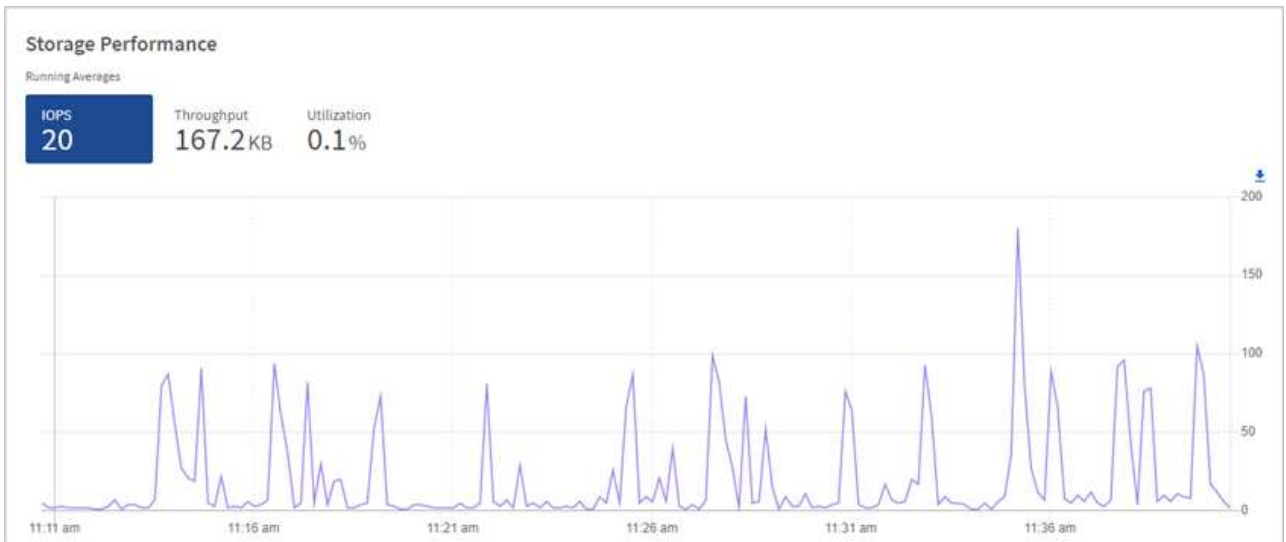
Il riquadro Prestazioni di archiviazione consente di identificare se le prestazioni stanno raggiungendo un punto in cui potrebbero peggiorare in caso di aumento dei carichi di lavoro.

Le informazioni in questo riquadro si aggiornano ogni 10 secondi e mostrano una media di tutti i punti sul grafico.

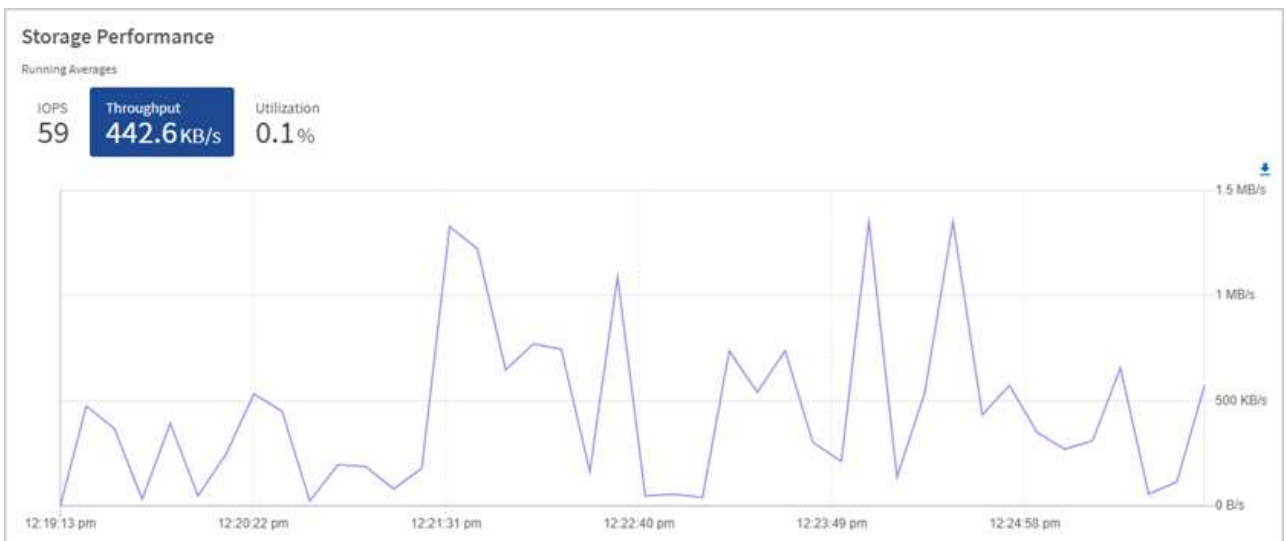
Per i dettagli sul metodo API Element associato, vedere ["Ottieni statistiche cluster"](#) metodo nella

Passi

1. Visualizza il riquadro Prestazioni di archiviazione. Per maggiori dettagli, passa il mouse sui punti del grafico.
 - a. Scheda **IOPS**: visualizza le operazioni correnti al secondo. Cercare tendenze nei dati o picchi. Ad esempio, se noti che il numero massimo di IOPS è 160K e che 100K di questi sono IOPS gratuiti o disponibili, potresti valutare l'aggiunta di altri carichi di lavoro a questo cluster. D'altro canto, se vedi che sono disponibili solo 140K, potresti prendere in considerazione l'idea di scaricare i carichi di lavoro o espandere il tuo sistema.



- b. Scheda **Rendimento**: monitora modelli o picchi nel rendimento. Monitorare anche i valori di throughput costantemente elevati, che potrebbero indicare che ci si sta avvicinando alle massime prestazioni utili della risorsa.



- c. Scheda **Utilizzo**: monitora l'utilizzo degli IOPS in relazione al totale degli IOPS disponibili sommati a livello di cluster.



2. Per un'analisi più approfondita, esaminare le prestazioni di storage utilizzando il plug-in NetApp Element per vCenter Server.

["Prestazioni mostrate nel plug-in NetApp Element per vCenter Server"](#).

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Visualizza il tuo inventario nella pagina Nodi

Puoi visualizzare le risorse di archiviazione nel tuo sistema e determinarne gli indirizzi IP, i nomi e le versioni del software.

È possibile visualizzare le informazioni di archiviazione per i sistemi a più nodi. Se ["domini di protezione personalizzati"](#) sono assegnati, è possibile vedere quali domini di protezione sono assegnati a nodi specifici.

Passi

1. Aprire l'indirizzo IP del nodo di gestione in un browser web. Per esempio:

```
https://[management node IP address]
```

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire .
3. Nella barra di navigazione a sinistra, seleziona **Nodi**.

Nodes

Only NetApp HCI Nodes are displayed on this page.

STORAGE		COMPUTE	
Cluster 1		1 of 1	Two-node
Hostname	Node Model	Element Version	Management IP Address
stg01	H410S-0	12.0.0.318	- VLAN 1184
stg02	H410S-0	12.0.0.318	- VLAN 1184

1 - 2 of 2 results

Witness Nodes

Hostname	Management IP Address	Storage (iSCSI) IP Address
wit01		
wit02		



Quando si avvia per la prima volta una nuova sessione NetApp Hybrid Cloud Control, potrebbe verificarsi un ritardo nel caricamento della pagina dei nodi NetApp Hybrid Cloud Control quando il nodo di gestione gestisce molti cluster. Il tempo di caricamento varia a seconda del numero di cluster gestiti attivamente dal nodo di gestione. Nei lanci successivi i tempi di caricamento saranno più rapidi.

4. Nella scheda **Archiviazione** della pagina Nodi, rivedere le seguenti informazioni:

- Cluster a due nodi: nella scheda Archiviazione viene visualizzata un'etichetta "a due nodi" e vengono elencati i nodi testimone associati.
- Cluster a tre nodi: vengono elencati i nodi di archiviazione e i nodi testimone associati. Nei cluster a tre nodi è presente un nodo testimone distribuito in standby per mantenere un'elevata disponibilità in caso di guasto del nodo.
- Cluster con quattro o più nodi: vengono visualizzate le informazioni per i cluster con quattro o più nodi. I nodi testimone non sono applicabili. Se si è iniziato con due o tre nodi di archiviazione e si sono aggiunti altri nodi, i nodi testimone continueranno a essere visualizzati. In caso contrario, la tabella Nodi testimone non verrà visualizzata.
- Versione del bundle del firmware: a partire dalla versione 2.14 dei servizi di gestione, se si dispone di cluster che eseguono Element 12.0 o versioni successive, è possibile visualizzare la versione del bundle del firmware per tali cluster. Se i nodi di un cluster hanno versioni firmware diverse, nella colonna **Versione bundle firmware** è possibile visualizzare **Multiple**.
- 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 nel cluster. Se i domini di protezione personalizzati non sono abilitati, questa colonna non viene visualizzata.

5. È possibile manipolare le informazioni contenute in queste pagine in diversi modi:

- Per filtrare l'elenco degli elementi nei risultati, selezionare l'icona **Filtro** e selezionare i filtri. È anche possibile inserire del testo per il filtro.
- Per mostrare o nascondere le colonne, seleziona l'icona **Mostra/Nascondi colonne**.

c. Per scaricare la tabella, seleziona l'icona **Download**.



Per visualizzare il numero di storage, consultare la dashboard di NetApp Hybrid Cloud Control (HCC). Vedere "[Monitora le risorse di archiviazione con la dashboard HCC](#)".

Trova maggiori informazioni

- "[Plug-in NetApp Element per vCenter Server](#)"
- "[Documentazione del software SolidFire ed Element](#)"

Monitora i volumi sul tuo cluster di archiviazione

Il sistema SolidFire fornisce spazio di archiviazione tramite volumi. I volumi sono dispositivi a blocchi a cui accedono tramite la rete i client iSCSI o Fibre Channel. È possibile monitorare i dettagli sui gruppi di accesso, gli account, gli iniziatori, la capacità utilizzata, lo stato di protezione dei dati Snapshot, il numero di sessioni iSCSI e la policy di qualità del servizio (QoS) associata al volume.

È anche possibile visualizzare i dettagli sui volumi attivi ed eliminati.

Con questa vista, potresti voler monitorare prima la colonna Capacità utilizzata.

È possibile accedere a queste informazioni solo se si dispone dei privilegi amministrativi NetApp Hybrid Cloud Control.

Passi

1. Aprire l'indirizzo IP del nodo di gestione in un browser web. Per esempio:

```
https://[management node IP address]
```

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage all-flash SolidFire.
3. Nella casella di navigazione blu a sinistra, seleziona l'installazione dell'archiviazione all-flash SolidFire.
4. Nella barra di navigazione a sinistra, seleziona il cluster e seleziona **Archiviazione > Volumi**.

OVERVIEW

ACCESS GROUPS

ACCOUNTS

INITIATORS

QOS POLICIES

VOLUMES

Overview

Active

Deleted

Create Volume

Actions

ID ↑

Name

Account

Access Groups

Access

Used

Size

Snapshots

QoS Policy

Min IOPS

Max IOPS

Burst IOPS

iSCSI Sessions

Actions

1

NetApp-HCI-Datastore-01

NetApp-HCI

NetApp-HCI-6ee7b8e7...

Read/Write

4%

2.15 TB

0

50

15000

15000

2

2

NetApp-HCI-Datastore-02

NetApp-HCI

NetApp-HCI-6ee7b8e7...

Read/Write

0%

2.15 TB

0

50

15000

15000

2

3

NetApp-HCI-credential...

Read/Write

0%

5.37 GB

0

1000

2000

4000

1

4

NetApp-HCI-mnode-api

Read/Write

0%

53.69 GB

0

1000

2000

4000

1

5

NetApp-HCI-hci-monitor

Read/Write

0%

1.07 GB

0

1000

2000

4000

1

5. Nella pagina Volumi, utilizzare le seguenti opzioni:



- a. Filtra i risultati selezionando l'icona **Filtro**.
 - b. Nascondi o mostra le colonne selezionando l'icona **Nascondi/Mostra**.
 - c. Aggiorna i dati selezionando l'icona **Aggiorna**.
 - d. Scarica 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. Attenzione - Giallo
 - b. Errore - Arancione
 - c. Critico - Rosso
7. Dalla vista Volumi, seleziona 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 una raccolta di volumi per l'accesso protetto.

Vedi informazioni su ["gruppi di accesso al volume"](#).
 - b. **Account**: puoi 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.

Vedi informazioni su ["Account utente del sistema di archiviazione all-flash SolidFire"](#).
 - c. **Iniziatori**: è possibile visualizzare l'IQN dell'iniziatore iSCSI o i WWPN Fibre Channel per il volume. Ogni IQN aggiunto a un gruppo di accesso può accedere a ciascun volume nel gruppo senza richiedere l'autenticazione CHAP. Ogni WWPN aggiunto a un gruppo di accesso consente l'accesso alla rete Fibre Channel ai volumi nel gruppo di accesso.
 - d. **Criteri QoS**: è possibile visualizzare i criteri QoS applicati al volume. Una policy QoS applica impostazioni standardizzate per IOPS minimi, IOPS massimi e IOPS burst a più volumi.

Vedi informazioni su ["politiche di prestazioni e QoS"](#).

Trova maggiori informazioni

- ["Documentazione SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Raccogliere i registri per la risoluzione dei problemi

In caso di problemi con l'installazione dell'archiviazione all-flash SolidFire , è possibile raccogliere i log da inviare al supporto NetApp per agevolare la diagnosi. Per raccogliere i log su un sistema Element è possibile utilizzare NetApp Hybrid Cloud Control o l'API REST.

Cosa ti servirà

- Assicurati che la versione del cluster di storage esegua il software NetApp Element 11.3 o versione

successiva.

- Assicurarsi di aver distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Opzioni di raccolta dei log

Scegli una delle seguenti opzioni:

- [Utilizzare NetApp Hybrid Cloud Control per raccogliere i log](#)
- [Utilizzare l'API REST per raccogliere i log](#)

Utilizzare NetApp Hybrid Cloud Control per raccogliere i log

È possibile accedere all'area di raccolta dei log dalla dashboard di controllo del cloud ibrido NetApp .

Passi

1. Aprire l'indirizzo IP del nodo di gestione in un browser web. Per esempio:

```
https://[management node IP address]
```

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage Element.
3. Dalla Dashboard, seleziona il menu in alto a destra.
4. Seleziona **Raccogli registri**.

Se hai già raccolto i log in precedenza, puoi scaricare il pacchetto di log esistente oppure iniziare una nuova raccolta di log.

5. Selezionare un intervallo di date nel menu a discesa **Intervallo di date** per specificare quali date devono essere incluse nei registri.

Se si specifica una data di inizio personalizzata, è possibile selezionare la data di inizio dell'intervallo di date. I registri saranno raccolti da quella data fino al momento attuale.

6. Nella sezione **Raccolta log**, seleziona i tipi di file di log che il pacchetto di log deve includere.

Per i registri di archiviazione, è possibile espandere l'elenco dei nodi di archiviazione e selezionare singoli nodi da cui raccogliere i registri (o tutti i nodi nell'elenco).

7. Selezionare **Raccogli registri** per avviare la raccolta dei registri.

La raccolta dei registri viene eseguita in background e la pagina ne mostra l'avanzamento.



A seconda dei registri raccolti, la barra di avanzamento potrebbe rimanere a una certa percentuale per diversi minuti oppure avanzare molto lentamente in alcuni punti.

8. Selezionare **Scarica registri** per scaricare il pacchetto di registri.

Il pacchetto di log è in un formato di file UNIX compresso .tgz.

Utilizzare l'API REST per raccogliere i log

È possibile utilizzare l'API REST per raccogliere i log degli elementi.

Passi

1. Individuare l'ID del cluster di archiviazione:

a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

```
https://[management node IP]/logs/1/
```

b. Seleziona **Autorizza** e completa quanto segue:

- i. Immettere il nome utente e la password del cluster.
- ii. Inserisci l'ID cliente come `mnode-client` se il valore non è già compilato.
- iii. Selezionare **Autorizza** per iniziare una sessione.

2. Raccogli i log da Element:

a. Selezionare **POST /bundle**.

b. Seleziona **Provalo**.

c. Modificare i valori dei seguenti parametri nel campo **Corpo della richiesta** a seconda del tipo di log che si desidera raccogliere e per quale intervallo di tempo:

Parametro	Tipo	Descrizione
<code>modifiedSince</code>	Stringa di data	Includi solo i log modificati dopo questa data e ora. Ad esempio, il valore "2020-07-14T20:19:00.000Z" definisce la data di inizio del 14 luglio 2020 alle 20:19 UTC.
<code>mnodeLogs</code>	Booleano	Imposta questo parametro su <code>true</code> per includere i log dei nodi di gestione.
<code>storageCrashDumps</code>	Booleano	Imposta questo parametro su <code>true</code> per includere i log di debug degli arresti anomali del nodo di archiviazione.
<code>storageLogs</code>	Booleano	Imposta questo parametro su <code>true</code> per includere i log dei nodi di archiviazione.

Parametro	Tipo	Descrizione
storageNodeIds	matrice UUID	Se <code>storageLogs</code> è impostato su <code>true</code> , popolare questo parametro con gli ID dei nodi del cluster di archiviazione per limitare la raccolta dei log a quei nodi di archiviazione specifici. Utilizzare il GET <code>https://[management node IP]/logs/1/bundle/options</code> endpoint per visualizzare tutti i possibili ID nodo che puoi utilizzare.

- d. Selezionare **Esegui** per iniziare la raccolta dei registri. La risposta dovrebbe restituire una risposta simile alla seguente:

```
{
  "_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. Controlla lo stato dell'attività di raccolta dei log:

- Selezionare **GET /bundle**.
- Seleziona **Provalo**.
- Selezionare **Esegui** per restituire lo stato dell'attività di raccolta.
- Scorrere fino alla fine del corpo della risposta.

Dovresti vedere un `percentComplete` attributo che descrive in dettaglio 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.

- Copia il nome del file alla fine del `downloadLink` attributo.

4. Scarica il pacchetto di log raccolti:

- Selezionare **GET /bundle/{filename}**.
- Seleziona **Provalo**.
- Incolla il nome del file copiato in precedenza nel `filename` campo di testo del parametro.
- Selezionare **Esegui**.

Dopo l'esecuzione, nell'area del corpo della risposta viene visualizzato un collegamento per il download.

- Seleziona **Scarica file** e salva il file risultante sul tuo computer.

Il pacchetto di log è in un formato di file UNIX compresso .tgz.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Gestisci l'archiviazione con Element API

Software API Element

Scopri come gestire lo storage con Element API

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 scambio 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. Attualmente l'API 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 formato form.



L'interfaccia utente web di Element utilizza i metodi API descritti in questo documento. È possibile monitorare le operazioni API nell'interfaccia utente abilitando il registro API; ciò consente di visualizzare i metodi che vengono inviati al sistema. È possibile abilitare sia le richieste che le risposte per vedere come il sistema risponde ai metodi emessi.

Salvo diversa indicazione, tutte le stringhe di data nelle risposte API sono in formato UTC+0.



Quando il cluster di archiviazione è molto carico o si inviano numerose richieste API consecutive senza alcun ritardo intermedio, un metodo potrebbe non funzionare e restituire l'errore "xDBVersionMismatch". In tal caso, riprovare la chiamata al metodo.

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 documenta gli oggetti comunemente utilizzati; gli oggetti utilizzati solo all'interno di un singolo metodo sono documentati con quel metodo anziché in questa sezione.

["Scopri gli oggetti comuni"](#)

Metodi comuni

I metodi comuni sono metodi utilizzati per recuperare informazioni sul cluster di archiviazione, sull'API stessa o sulle operazioni API in corso.

["Scopri i metodi comuni"](#)

Metodi API dell'account

I metodi di account consentono di aggiungere, rimuovere, visualizzare e modificare le informazioni sull'account e sulla sicurezza.

["Scopri di più sui metodi API dell'account"](#)

Metodi API dell'amministratore

È possibile utilizzare i metodi API dell'amministratore per creare, modificare, visualizzare e rimuovere gli amministratori del cluster di archiviazione e assegnare livelli di accesso e privilegi a coloro che hanno accesso a un cluster di archiviazione.

["Scopri i metodi API dell'amministratore"](#)

Metodi API del cluster

I metodi API del cluster software Element consentono di gestire la configurazione e la topologia del cluster di archiviazione e dei nodi che appartengono a un cluster di archiviazione.

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 nello stato "in sospeso", ovvero sono stati configurati ma non ancora aggiunti al cluster.

["Scopri i metodi API del cluster"](#)

Metodi API per la creazione di cluster

È possibile utilizzare questi metodi API per creare un cluster di archiviazione. Tutti questi metodi devono essere utilizzati sull'endpoint API su un singolo nodo.

["Scopri i metodi API per la creazione di cluster"](#)

Metodi API Drive

È possibile utilizzare i metodi API delle unità per aggiungere e gestire le unità disponibili per un cluster di archiviazione. Quando si aggiunge un nodo di archiviazione al cluster di archiviazione o si installano nuove unità in un nodo di archiviazione esistente, le unità sono disponibili per essere aggiunte al cluster di archiviazione.

["Scopri di più sui metodi API di unità"](#)

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.

["Scopri i metodi API Fibre Channel"](#)

Metodi API dell'iniziatore

I metodi di avvio consentono di aggiungere, rimuovere, visualizzare e modificare gli oggetti di avvio iSCSI, che gestiscono la comunicazione tra il sistema di archiviazione e i client di archiviazione esterni.

["Scopri i metodi API dell'iniziatore"](#)

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 archiviazione.

["Scopri i metodi API LDAP"](#)

Metodi API di autenticazione a più fattori

È possibile utilizzare l'autenticazione a più fattori (MFA) per gestire le sessioni utente tramite un Identity Provider (IdP) di terze parti tramite Security Assertion Markup Language (SAML).

["Scopri i metodi API di autenticazione a più fattori"](#)

Metodi API di autenticazione della sessione

È possibile utilizzare l'autenticazione basata sulla sessione per gestire le sessioni utente.

["Scopri i metodi API di autenticazione della sessione"](#)

Metodi API del nodo

È possibile utilizzare i metodi API dei nodi per configurare singoli nodi. Questi metodi operano su singoli nodi che devono essere configurati, sono configurati ma non partecipano ancora a un cluster o partecipano attivamente a un cluster. I metodi API dei nodi consentono di visualizzare e modificare le impostazioni per i singoli nodi e per la rete cluster utilizzata per comunicare con il nodo. È necessario eseguire questi metodi sui singoli nodi; non è possibile eseguire metodi API per nodo sull'indirizzo del cluster.

["Scopri i metodi API del nodo"](#)

Metodi API di replicazione

I metodi API di replicazione consentono di connettere 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 continuamente su un secondo cluster per garantire il ripristino dei dati. Associando i volumi per la replica, puoi proteggere i tuoi dati da eventi che potrebbero renderli inaccessibili.

["Scopri i metodi API di replicazione"](#)

Metodi API di sicurezza

È possibile integrare il software Element con servizi esterni correlati alla sicurezza, come un server di gestione delle chiavi esterno. Questi metodi relativi alla sicurezza consentono di configurare le funzionalità di sicurezza di Element, come la gestione delle chiavi esterne per la crittografia a riposo.

["Scopri i metodi API di sicurezza"](#)

Metodi API SnapMirror

I metodi API SnapMirror vengono utilizzati dall'interfaccia utente Web di Element per gestire gli snapshot replicati con sistemi ONTAP remoti. Questi metodi sono pensati per essere utilizzati solo dall'interfaccia utente web di Element. Se hai bisogno dell'accesso API alla funzionalità SnapMirror, utilizza le API ONTAP. Non sono forniti esempi di richiesta e restituzione per i metodi API SnapMirror.

["Scopri di più sui metodi API SnapMirror"](#)

Metodi API di configurazione del sistema

I metodi API di configurazione del sistema consentono di ottenere e impostare valori di configurazione che si applicano a tutti i nodi del cluster.

["Scopri i metodi API di configurazione del sistema"](#)

Metodi API di rete multitenant

La rete multi-tenant nei cluster di storage Element consente al traffico tra più client che si trovano su reti logiche separate di essere connesso a un cluster di storage Element senza routing di livello 3.

Le connessioni al cluster di storage sono separate nello stack di rete tramite l'uso del tagging VLAN.

Prerequisiti per la configurazione di una rete virtuale multitenant

- È necessario aver identificato il blocco di indirizzi IP di rete client da assegnare alle reti virtuali sui nodi di archiviazione.
- È necessario aver identificato un indirizzo IP della rete di archiviazione client (SVIP) da utilizzare come endpoint per tutto il traffico di archiviazione.

Ordine delle operazioni di rete virtuale

1. Utilizzare il metodo AddVirtualNetwork per effettuare il provisioning in blocco degli indirizzi IP immessi.

Dopo aver aggiunto una rete virtuale, il cluster esegue automaticamente i seguenti passaggi:

- Ogni nodo di archiviazione crea un'interfaccia di rete virtuale.
 - A ciascun nodo di archiviazione viene assegnato un indirizzo VLAN a cui è possibile effettuare il routing tramite l'SVIP virtuale.
 - Gli indirizzi IP 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 client all'SVIP virtuale.

["Scopri i metodi API di rete multitenant"](#)

Metodi API del volume

I metodi API del volume del software Element consentono di gestire i volumi che risiedono su un nodo di archiviazione. Con questi metodi è possibile creare, modificare, clonare ed eliminare volumi. È anche possibile utilizzare i metodi API del volume per raccogliere e visualizzare le misurazioni dei dati per un volume.

["Scopri i metodi API del volume"](#)

Metodi API del gruppo di accesso al volume

I metodi dei gruppi di accesso al volume consentono di aggiungere, rimuovere, visualizzare e modificare i gruppi di accesso al volume, ovvero raccolte di volumi a cui gli utenti possono accedere tramite iniziatori iSCSI o Fibre Channel.

["Scopri i metodi API del gruppo di accesso al volume"](#)

Metodi API per snapshot del volume

I metodi API per gli snapshot dei volumi del software Element consentono di gestire gli snapshot dei volumi. È possibile creare, modificare, clonare ed eliminare snapshot di volume utilizzando i metodi API degli snapshot di volume.

["Scopri i metodi API per gli snapshot del volume"](#)

Metodi API del volume virtuale

I metodi API del volume virtuale 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 contenitori di archiviazione di volumi virtuali. Sebbene non sia possibile utilizzare questi metodi per operare su volumi normali, è possibile utilizzare i metodi API dei volumi normali per elencare le informazioni sui VVol.

["Scopri i metodi API del volume virtuale"](#)

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Richiedi membri dell'oggetto

Ogni richiesta API del software Element è composta dalle seguenti parti di base:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
metodo	Nome del metodo da richiamare.	corda	Nessuno	Sì
parametri	Oggetto contenente i parametri del metodo richiamato. Sono obbligatori i parametri denominati. I parametri posizionali (passati come array) non sono consentiti.	Oggetto JSON	{}	NO
id	Identificatore utilizzato per abbinare la richiesta alla risposta, restituito nel risultato.	stringa o intero	{}	NO

Membri dell'oggetto di risposta

Ogni corpo di risposta dell'API del software Element è costituito dalle seguenti parti di base:

Nome	Descrizione	Tipo
risultato	L'oggetto restituito dal metodo. Il sistema restituisce un oggetto con membri denominati corrispondenti al valore di ritorno 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	Un identificatore utilizzato per abbinare la richiesta alla risposta, come fornito nella richiesta.	stringa o intero
parametri non utilizzati	Un messaggio di avviso indica che almeno un parametro errato è stato passato al metodo API e non è stato utilizzato.	Oggetto

Endpoint della richiesta

Esistono tre tipi di endpoint di richiesta utilizzati nell'API (cluster di archiviazione, creazione di cluster di archiviazione e per nodo). Dovresti sempre utilizzare l'endpoint più recente supportato dalla tua 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 archiviazione è `https://<mvip>/json-rpc/<api-version>`, Dove:

- `<mvip>` è l'indirizzo IP virtuale di gestione per il cluster di archiviazione.
- `<api-version>` è la versione dell'API che stai utilizzando.

Metodi API di creazione di cluster e bootstrap

L'endpoint HTTPS per la creazione di un cluster di archiviazione e l'accesso alle richieste API bootstrap è `https://<nodeIP>/json-rpc/<api-version>`, Dove:

- `<nodeIP>` è l'indirizzo IP del nodo che stai aggiungendo al cluster.
- `<api-version>` è la versione dell'API che stai utilizzando.

Metodi API per nodo

L'endpoint HTTPS per le richieste API dei singoli nodi di archiviazione è `https://<nodeIP>:442/json-rpc/<api-version>`, Dove:

- `<nodeIP>` è l'indirizzo IP di gestione del nodo di archiviazione; 442 è la porta su cui è in esecuzione il server HTTPS.
- `<api-version>` è la versione dell'API che stai utilizzando.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Autenticazione API

È possibile autenticarsi con il sistema quando si utilizza l'API includendo un'intestazione di autenticazione HTTP di base 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 tramite TLS.

Utilizzare l'account amministratore del cluster per l'autenticazione API.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Metodi asincroni

Alcuni metodi API sono asincroni, il che significa che l'operazione che eseguono potrebbe non essere completata quando il metodo ritorna. I metodi asincroni restituiscono un handle che è possibile interrogare per visualizzare lo stato dell'operazione; le informazioni sullo 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'unità al cluster.
- `BulkVolume`: Il sistema sta eseguendo un'operazione di copia tra volumi, ad esempio un backup o un ripristino.
- `Clone`: Il sistema sta clonando un volume.
- `DriveRemoval`: Il sistema sta copiando i dati da un'unità in preparazione alla rimozione dal cluster.
- `RtfiPendingNode`: Il sistema sta installando un software compatibile su un nodo prima di aggiungerlo al cluster.

Quando si utilizzano metodi asincroni o si ottiene lo stato di un'operazione asincrona in esecuzione, tenere presente i seguenti punti:

- I metodi asincroni sono indicati nella documentazione del singolo metodo.
- I metodi asincroni restituiscono un “asyncHandle”, ovvero un handle noto al metodo API emittente. È possibile utilizzare l’handle per interrogare lo stato o il risultato dell’operazione asincrona.
- È possibile ottenere il risultato dei singoli metodi asincroni con il metodo GetAsyncResult. Quando si utilizza GetAsyncResult per interrogare un’operazione completata, il sistema restituisce il risultato e lo elimina automaticamente dal sistema. Quando si utilizza GetAsyncResult per interrogare 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 maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Attributi

Molte delle richieste e delle risposte API utilizzano sia oggetti che tipi semplici. Gli oggetti sono una raccolta di coppie chiave-valore, in cui il valore è un tipo semplice o eventualmente 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 di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON

Richiedi esempio

Il seguente esempio di richiesta utilizza il metodo AddClusterAdmin:

```

{
  "method": "AddClusterAdmin",
  "params": {
    "username": "joeadmin",
    "password": "68!5Aru268)$",
    "access": [
      "volume",
      "reporting"
    ],
    "attributes": {
      "name1": "value1",
      "name2": "value2",
      "name3": "value3"
    }
  }
}

```

Oggetti comuni

account

IL `account` l'oggetto contiene informazioni su un account. Questo oggetto include solo informazioni "configurate" sull'account, non informazioni di runtime o di utilizzo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>accountID</code>	ID account univoco per l'account.	intero
<code>attributes</code>	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
<code>enableChap</code>	Specifica se le credenziali dell'account CHAP possono essere utilizzate da un iniziatore per accedere ai volumi.	booleano
<code>initiatorSecret</code>	Il segreto dell'iniziatore CHAP.	corda

Nome	Descrizione	Tipo
status	Lo stato attuale dell'account. Valori possibili: • attivo: un account attivo. • bloccato: Un account bloccato. • rimosso: un account che è stato eliminato e ripulito.	corda
storageContainerID	ID univoco del contenitore di archiviazione del volume virtuale associato a questo account.	UUID
targetSecret	Il segreto CHAP di destinazione.	corda
username	Il nome utente per l'account.	corda
volumes	Un elenco di ID volume per i volumi di proprietà di questo account.	array di interi

Trova maggiori informazioni

- [Aggiungi account](#)
- [OttieniAccountPerID](#)
- [OttieniAccountPerNome](#)
- [ElencoAccount](#)

authSessionInfo

IL `authSessionInfo` l'oggetto contiene informazioni su una sessione di autenticazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accessGroupList	Elenco dei gruppi di accesso per l'utente.	matrice di stringhe

Nome	Descrizione	Tipo
authMethod	Tipo di autorizzazione di cui dispone l'utente amministratore del cluster. Valori possibili: • LDAP - autenticato tramite LDAP. • Cluster: autenticato tramite nome utente e password memorizzati nel database del cluster. • IdP - autenticato tramite un Identity Provider di terze parti.	corda
clusterAdminIDs	Elenco degli AdminID del cluster associati a questa sessione. Per le sessioni correlate a LDAP o a un Identity Provider (IdP) di terze parti, questo sarà un elenco aggregato di Cluster AdminID corrispondenti associati a questa sessione.	array di interi
finalTimeout	Ora in cui la sessione diventa non valida. Viene impostata al momento della creazione della sessione e non può essere modificata.	corda
idpConfigVersion	Versione della configurazione IdP al momento della creazione della sessione.	intero
lastAccessTimeout	Ora in cui la sessione diventa non valida a causa di inattività. Viene impostato su un nuovo valore quando si accede alla sessione per utilizzarla, fino al momento in cui la sessione diventa non valida a causa del raggiungimento di finalTimeout.	corda
sessionCreationTime	Ora in cui viene creata la sessione.	corda
sessionID	UUID per questa sessione.	UUID

Nome	Descrizione	Tipo
username	Nome utente associato a questa sessione. Per le sessioni relative a LDAP, questo sarà il DN LDAP dell'utente. Per le sessioni relative a un IdP di terze parti, si tratterà di una coppia nome-valore arbitraria che verrà utilizzata per le operazioni di audit all'interno della sessione. Non corrisponderà necessariamente al nome di un amministratore del cluster. Ad esempio, un SAML Subject NameID, ma questo sarà determinato dalla configurazione dell'IdP e dal contenuto risultante dell'asserzione SAML.	corda

bulkVolumeJob

IL `bulkVolumeJob` L'oggetto 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
attributes	Attributo JSON del lavoro di volume in blocco.	Oggetto JSON
bulkVolumeID	ID del processo di volume di massa interno.	intero
createTime	Timestamp creato per il lavoro di volume in blocco nel formato UTC+0.	Stringa di data ISO 8601
elapsedTime	Numero di secondi trascorsi dall'inizio del processo.	corda
format	Formato dell'operazione di volume in blocco. Valori possibili: • nativo • non compresso	corda

Nome	Descrizione	Tipo
key	Chiave univoca creata dalla sessione di volume in blocco.	corda
percentComplete	La percentuale completata riportata dall'operazione.	intero
remainingTime	Tempo rimanente stimato in secondi.	intero
srcVolumeID	ID del volume di origine.	intero
status	Lo stato dell'operazione. Valori possibili: • preparazione • corsa • completare • fallito	corda
script	Il nome dello script, se ne è stato fornito uno.	corda
snapshotID	ID dello snapshot se uno snapshot è presente nell'origine del processo di volume in blocco.	intero
type	Il tipo di operazione in blocco. Valori possibili: • Leggere • scrivere	corda

rilegatura (volumi virtuali)

L'oggetto di associazione 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	scsiNAADeviceID dell'endpoint del protocollo.	corda
protocolEndpointType	Il tipo di endpoint del protocollo. SCSI è l'unico valore restituito per il tipo di endpoint del protocollo.	corda
virtualVolumeBindingID	ID univoco dell'oggetto di associazione del volume virtuale.	intero
virtualVolumeHostID	ID univoco dell'host del volume virtuale.	UUID
virtualVolumeID	ID univoco del volume virtuale.	UUID
virtualVolumeSecondaryID	ID secondario del volume virtuale.	corda

Trova maggiori informazioni

- [ListVirtualVolumeBindings](#)
- [protocolloEndpoint](#)

certificatoDettagli

IL `certificateDetails` L'oggetto contiene le informazioni decodificate su un certificato di sicurezza.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
issuer	Il nome dell'emittente.	corda
modulus	Il modulo della chiave pubblica.	corda
notAfter	La data di scadenza del certificato.	Stringa ISO 8601
notBefore	La data di inizio del certificato.	Stringa ISO 8601

Nome	Descrizione	Tipo
serial	Il numero di serie del certificato.	corda
sha1Fingerprint	Il digest della versione codificata DER del certificato.	corda
subject	Il nome del soggetto.	corda

grappolo

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.	corda
grappolo	Nome univoco del cluster.	corda
crittografiaCapace	Indica se il nodo supporta la crittografia dell'unità.	booleano
insieme	I nodi che partecipano al cluster.	matrice di stringhe
Configurazione dell'unità fips	Indica se il nodo supporta unità certificate FIPS 140-2.	booleano
mipi	Interfaccia di rete utilizzata per la gestione dei nodi.	corda
nome	Il nome del cluster.	corda
ID nodo	L'ID del nodo nel cluster.	corda
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 archiviazione.	corda

Nome	Descrizione	Tipo
stato	Lo stato attuale del nodo. Valori possibili: • Disponibile: il nodo non è stato configurato con un nome cluster. • In sospeso: il nodo è in sospeso per un cluster denominato specifico e può essere aggiunto. • Attivo: il nodo è un membro attivo di un cluster e non può essere aggiunto a un altro cluster. • PendingActive: il nodo è attualmente in fase di ripristino nell'immagine software di fabbrica e non è ancora un membro attivo di un cluster. Una volta completato, passerà allo stato Attivo.	corda
versione	La versione del software in esecuzione sul nodo.	corda

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati in ogni possibile stato del nodo.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
cipi	NO	NO	NO
grappolo	SÌ	Sì	NO
crittografiaCapace	NO	NO	NO
insieme	NO	NO	NO
mipi	SÌ	Sì	NO
nome	SÌ	Sì	Sì
ID nodo	NO	NO	NO
pendingNodeID	NO	NO	NO

ruolo	NO	NO	NO
sipi	NO	NO	NO
stato	NO	NO	NO
versione	NO	NO	NO

Trova maggiori informazioni

[OttieniClusterConfig](#)

ClusterAdmin

L'oggetto clusterAdmin contiene informazioni sull'utente amministratore del cluster corrente. 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 questo amministratore del cluster può utilizzare.	matrice di stringhe
Metodo di autenticazione	Tipo di autorizzazione di cui dispone l'utente amministratore del cluster. Valori possibili: • LDAP • Grappolo • Locale	corda
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
ID amministratore cluster	ID amministratore del cluster per questo utente amministratore del cluster.	intero
nome utente	Nome utente per questo amministratore del cluster.	corda

Trova maggiori informazioni

[OttieniCurrentClusterAdmin](#)

capacità del cluster

L'oggetto `clusterCapacity` contiene misurazioni della 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
<code>activeBlockSpace</code>	La quantità di spazio sulle unità a blocchi. Ciò include informazioni aggiuntive, come voci di metadati e spazio, che possono essere ripulite.	intero
<code>sessioni attive</code>	Numero di sessioni iSCSI attive che comunicano con il cluster.	intero
<code>IOPS medi</code>	IOPS medi per il cluster dalla mezzanotte del Tempo Coordinato Universale (UTC).	intero
<code>clusterRecentIOSize</code>	La dimensione media degli IOPS su tutti i volumi nel cluster.	intero
<code>IOPS correnti</code>	IOPS medi per tutti i volumi nel cluster negli ultimi 5 secondi.	intero
<code>IOPS massimi</code>	Capacità IOPS massima stimata del cluster attuale.	intero

Nome	Descrizione	Tipo
maxOverProvisionableSpace	La quantità massima di spazio disponibile. Questo è un valore calcolato. Non è possibile creare nuovi volumi se lo spazio attualmente fornito più le dimensioni del nuovo volume superano questo numero. Il valore viene calcolato come segue: $\text{maxOverProvisionableSpace} = \text{maxProvisionedSpace} * \text{maxMetadataOverProvisionFactor}$	intero
maxProvisionedSpace	Quantità totale di spazio provisionabile se tutti i volumi sono riempiti al 100% (nessun metadati con provisioning sottile).	intero
maxUsedMetadataSpace	Numero di byte sulle unità di volume utilizzate per archiviare i metadati.	intero
maxUsedSpace	Quantità totale di spazio su tutte le unità a blocchi attive.	intero
nonZeroBlock	Numero totale di blocchi da 4 KiB contenenti dati dopo il completamento dell'ultima operazione di garbage collection.	intero
peakActiveSessions	Numero massimo di connessioni iSCSI dalla mezzanotte UTC.	intero
picco IOPS	Il valore più alto per currentIOPS dalla mezzanotte UTC.	intero
spazio fornito	Quantità totale di spazio fornito in tutti i volumi del cluster.	intero
marca temporale	Data e ora, in formato UTC+0, in cui è stato prelevato il campione di capacità del cluster.	Stringa ISO 8601
totalOps	Numero totale di operazioni di I/O eseguite durante il ciclo di vita del cluster.	intero

Nome	Descrizione	Tipo
blocchi unici	Numero totale di blocchi memorizzati sulle unità a blocchi. Il valore include i blocchi replicati.	intero
uniqueBlocksUsedSpace	La quantità totale di dati che gli uniqueBlocks occupano sulle unità a blocchi. Per informazioni sulla relazione tra questo numero e il valore uniqueBlocks, vedere il metodo GetclusterCapacity.	intero
usedMetadataSpace	Numero totale di byte sulle unità di volume utilizzate per archiviare i metadati.	intero
usedMetadataSpaceInSnapshots	Numero di byte sulle unità di volume utilizzate per archiviare dati univoci negli snapshot. Questo numero fornisce una stima della quantità di spazio dei metadati che verrebbe recuperata eliminando tutti gli snapshot dal sistema.	intero
spazio usato	Quantità totale di spazio utilizzato da tutte le unità a blocchi nel sistema.	intero
zeroBlocks	Numero totale di blocchi vuoti da 4 KiB senza dati dopo il completamento dell'ultimo ciclo di operazioni di garbage collection.	intero

Trova maggiori informazioni

[Ottieni capacità cluster](#)

clusterConfig

IL `clusterConfig` L'oggetto restituisce le informazioni che il nodo utilizza per comunicare con il cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>cipi</code>	Interfaccia di rete utilizzata per la comunicazione del cluster.	corda
<code>cluster</code>	Nome univoco del cluster.	corda
<code>encryptionCapable</code>	Specifica se il nodo supporta la crittografia.	booleano
<code>ensemble</code>	Nodi che partecipano al cluster.	matrice di stringhe
<code>fipsDriveConfiguration</code>	Specifica se il nodo supporta unità certificate FIPS 140-2.	booleano
<code>hasLocalAdmin</code>	Specifica se il cluster ha un amministratore locale.	booleano
<code>mipi</code>	Interfaccia di rete utilizzata per la gestione dei nodi.	corda
<code>name</code>	Identificatore univoco per il cluster.	corda
<code>nodeID</code>	Identificatore univoco per il nodo.	intero
<code>pendingNodeID</code>	Identificatore univoco per il nodo in sospeso.	intero
<code>role</code>	Identifica il ruolo del nodo.	corda
<code>sipi</code>	Interfaccia di rete utilizzata per l'archiviazione.	corda
<code>state</code>	Indica lo stato del nodo.	corda
<code>version</code>	Indica la versione del nodo.	corda

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 di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
schema di protezione predefinito	Lo schema di protezione utilizzato per impostazione predefinita per i nuovi volumi, a meno che non venga fornito uno schema di protezione con Crea volume chiamata al metodo. Questo schema di protezione deve essere sempre presente nell'insieme degli schemi di protezione abilitati.	corda
Schemi di protezione abilitati	Un elenco di tutti gli schemi di protezione abilitati su questo cluster di archiviazione.	matrice di stringhe
crittografiaAtRestState	Lo stato della funzionalità di crittografia a riposo. Valori possibili: • Abilitazione: la crittografia a riposo è abilitata. • Abilitato: la crittografia a riposo è abilitata. • Disabilitazione: la crittografia a riposo è disabilitata. • Disabilitato: la crittografia a riposo è disabilitata.	corda
insieme	I nodi che partecipano al cluster.	matrice di stringhe
mvip	L'indirizzo IP mobile (virtuale) per il cluster sulla rete di gestione.	corda
Interfaccia mvip	L'interfaccia fisica associata all'indirizzo MVIP.	corda
mvipNodeID	Il nodo che contiene l'indirizzo MVIP master.	intero
mvipVlanTag	Identificatore VLAN per l'indirizzo MVIP.	corda
nome	Il nome univoco del cluster.	corda

Nome	Descrizione	Tipo
numero di rep	Numero di repliche di ciascun dato da archiviare nel cluster. Il valore valido è "2".	intero
softwareEncryptionAtRestState	Stato di crittografia a riposo basato su software.	corda
Schemi di protezione supportati	Un elenco di tutti gli schemi di protezione supportati su questo cluster di archiviazione.	matrice di stringhe
svip	Indirizzo IP mobile (virtuale) per il cluster sulla rete di archiviazione (iSCSI).	corda
svipInterface	L'interfaccia fisica associata all'indirizzo SVIP master.	corda
svipNodeID	Il nodo che contiene l'indirizzo SVIP master.	intero
svipVlanTag	Identificatore VLAN per l'indirizzo SVIP master.	corda
ID univoco	ID univoco per il cluster.	corda
uuid	Identificatore univoco del cluster.	UUID
volumeLoadBalanceOnActualIOPS	Lo stato del bilanciamento delle sezioni è basato sugli IOPS effettivi anziché sulla funzionalità Min IOPS. Disponibile a partire da Element 12.8.	corda

Trova maggiori informazioni

- ["Ottieni informazioni sul cluster"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

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 nella coppia.	corda
clusterPairID	Un ID univoco assegnato a ciascun cluster nella coppia.	intero
clusterPairUUID	Identificatore univoco universale per la coppia di cluster.	corda
UUID	Identificatore univoco per il 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.	corda
stato	Lo stato della connessione tra i cluster accoppiati. Valori possibili: • Non configurato • Collegato • Non configurato correttamente • Disconnesso	corda
versione	La versione Element dell'altro cluster nella coppia.	corda

Trova maggiori informazioni

[ListClusterPairs](#)

clusterStats

L'oggetto clusterStats contiene dati statistici per un cluster. Molte delle statistiche relative al volume contenute nell'oggetto vengono calcolate come media 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
IOPS effettivi	IOPS effettivi correnti per l'intero cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
dimensione media dell'IOP	Dimensione media in byte delle recenti operazioni di I/O sul cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
clientQueueDepth	Numero di operazioni di lettura e scrittura in sospeso sul cluster.	N / A	intero
Utilizzo del cluster	Percentuale degli IOPS massimi del cluster attualmente utilizzati. Questo viene calcolato come $\text{clusterUtilization} = \text{normalizedIOPS} / \text{maxIOPS}$ (da <code>GetClusterCapacity</code>).	N / A	galleggiante
latenzaUSec	Tempo medio, in microsecondi, impiegato per completare le operazioni su un cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
IOPS normalizzati	Numero medio di IOPS per l'intero cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
Leggi byte	Numero totale di byte cumulativi letti dal cluster dalla sua creazione.	Monotonicamente crescente	intero
readBytesLastSample	Numero totale di byte letti dal cluster durante l'ultimo periodo di campionamento.	Punto nel tempo	intero

Nome	Descrizione	Calcolo	Tipo
readLatencyUsec	Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura sul cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
readLatencyUsecTotal	Tempo totale impiegato per eseguire operazioni di lettura dalla creazione del cluster.	Monotonicamente crescente	intero
readOps	Il totale cumulativo delle operazioni di lettura sul cluster dalla sua creazione.	Monotonicamente crescente	intero
readOpsLastSample	Numero totale di operazioni di lettura durante l'ultimo periodo di campionamento.	Punto nel tempo	intero
samplePeriodMsec	La lunghezza del periodo di campionamento, in millisecondi.	N / A	intero
serviziConteggio	Numero di servizi in esecuzione sul cluster. Se uguale a servicesTotal, indica che sono state raccolte statistiche valide da tutti i nodi.	Punto nel tempo	intero
serviziTotale	Numero totale di servizi previsti in esecuzione sul cluster.	N / A	intero
marca temporale	L'ora corrente nel formato UTC+0.	N / A	Stringa di data ISO 8601
Lecture non allineate	Il totale cumulativo delle operazioni di lettura non allineate su un cluster dalla creazione del cluster.	Monotonicamente crescente	intero

Nome	Descrizione	Calcolo	Tipo
non allineatoScrive	Il totale cumulativo delle operazioni di scrittura non allineate su un cluster dalla creazione del cluster.	Monotonicamente crescente	intero
scriviBytes	Il totale cumulativo dei byte scritti nel cluster dalla sua creazione.	Monotonicamente crescente	intero
writeBytesLastSample	Numero totale di byte scritti nel cluster durante l'ultimo periodo di campionamento.	Monotonicamente crescente	intero
writeLatencyUsec	Tempo medio, in microsecondi, impiegato per completare le operazioni di scrittura su un cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
writeLatencyUsecTotal	Tempo totale impiegato per eseguire operazioni di scrittura dalla creazione del cluster.	Monotonicamente crescente	intero
writeOps	Il totale cumulativo delle operazioni di scrittura sul cluster dalla sua creazione.	Monotonicamente crescente	intero
writeOpsLastSample	Numero totale di operazioni di scrittura durante l'ultimo periodo di campionamento.	Punto nel tempo	intero

Trova maggiori informazioni

[Ottieni statistiche cluster](#)

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 archiviazione che si sta ricostruendo.

Membri dell'oggetto

Questo oggetto contiene le informazioni di ritorno combinate dai seguenti metodi:

- [Ottieni informazioni sul cluster](#)
- [ElencoAccount](#)
- [Iniziatori di elenchi](#)
- [ElencoVolumi](#)(con includeVirtualVolumes=false)
- [ListVolumeAccessGroups](#)
- [ListStorageContainers](#)
- [ListQoS Policies](#)
- [OttieniSnmpInfo](#)
- [Ottieni informazioni Ntp](#)
- [ElencoRetiVirtuali](#)
- [ListClusterAdmins](#)
- [ListSchedules](#)
- [ListSnapMirrorEndpoints](#)
- [OttieniStatoFunzionalità](#)
- [OttieniLdapConfiguration](#)
- [OttieniHost di registrazione remoti](#)
- [OttieniQoS predefinito](#)
- [GetVolumeAccessGroupLunAssignments](#)

Trova maggiori informazioni

- [OttieniStrutturaCluster](#)
- [ImpostaStrutturaCluster](#)

guidare

L'oggetto unità contiene informazioni sulle singole unità nei nodi attivi del cluster. Questo oggetto contiene dettagli 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 il `ListDrives` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Elenco di coppie nome-valore nel formato oggetto JSON. Questo oggetto è sempre nullo e non è modificabile.	Oggetto JSON
capacità	Capacità totale dell'unità, in byte.	intero
telaioSlot	Per le piattaforme HCI, questo valore è la lettera del nodo e il numero dello slot nello chassis del server in cui si trova questa unità. Per le piattaforme di archiviazione, il numero di slot è una rappresentazione stringa dell'intero "slot".	corda
driveFailureDetail	Se lo stato di un'unità è "Non riuscito", questo campo fornisce maggiori dettagli sul motivo per cui l'unità è stata contrassegnata come non riuscita.	corda
ID unità	L'ID di questa unità.	intero
driveSecurityFaultReason	Se l'abilitazione o la disabilitazione della sicurezza dell'unità non è riuscita, indicarne il motivo. Se il valore è "none", non si è verificato alcun errore.	corda
ID chiave	KeyID utilizzato dal fornitore della chiave per acquisire la chiave di autenticazione per sbloccare questa unità.	UUID
ID fornitore di chiavi	Identifica il fornitore della chiave di autenticazione per sbloccare questa unità.	intero
ID nodo	L'ID del nodo che contiene questa unità.	intero
segmentFileSize	Dimensione del file del segmento dell'unità, in byte.	intero
seriale	Il numero di serie dell'unità.	corda

Nome	Descrizione	Tipo
fessura	Numero di slot nello chassis del server in cui si trova questa unità oppure -1 se per l'unità metadati interna viene utilizzato un dispositivo SATADimm.	intero
stato	Lo stato dell'unità. Valori possibili: • disponibile: Un'unità disponibile. • attivo: Un'unità attiva. • cancellazione: un'unità è in fase di cancellazione sicura. Tutti i dati presenti su quell'unità verranno rimossi definitivamente. • failed: Un'unità che ha subito un guasto. Tutti i dati precedentemente presenti sull'unità sono stati migrati su altre unità del cluster. • rimozione: un'unità è in fase di rimozione. Tutti i dati precedentemente presenti sull'unità vengono migrati su altre unità del cluster.	corda
tipo	Il tipo di unità. Valori possibili: • volume: memorizza i metadati del volume. • blocco: memorizza i dati del blocco. • sconosciuto: il tipo di unità non è ancora attivo e deve ancora essere determinato.	corda
Capacità utilizzabile	Capacità utilizzabile dell'unità, in byte.	intero

Trova maggiori informazioni

[ListDrives](#)

Statistiche di guida

L'oggetto driveStats contiene misurazioni di attività di alto livello per una singola unità. È

possibile recuperare informazioni di misurazione con il metodo API `GetDriveStats`.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
sessioni attive	Numero di sessioni iSCSI che attualmente utilizzano questa unità (presente solo per le unità metadati).	intero
ID unità	ID univoco dell'unità nel cluster.	intero
failedDieCount	Numero di elementi hardware dell'unità guasti.	intero
iosInProgress	Numero di I/O in corso su questa unità.	intero
lifeRemainingPercent	Indicatore di usura del supporto di trasmissione.	intero
durataReadBytes	Numero totale di byte letti da questa unità per tutta la sua durata.	intero
durataWriteBytes	Numero totale di byte scritti su questa unità per tutta la sua durata.	intero
powerOnHours	Numero di ore in cui questa unità è rimasta accesa.	intero
legge	Numero di chiamate <code>read()</code> al secondo su questa unità.	intero
Leggi byte	Byte totali letti dall'unità a causa delle operazioni del client.	intero
lettureCombinare	Numero di chiamate <code>read()</code> a settori adiacenti che potrebbero essere combinate in una lettura più grande.	intero
readMsec	Numero di millisecondi impiegati per la lettura.	intero

Nome	Descrizione	Tipo
readOps	Totale delle operazioni di lettura sull'unità dovute alle operazioni del client.	intero
Settori riallocati	Numero di settori danneggiati sostituiti in questa unità.	intero
reserveCapacityPercent	La capacità di riserva disponibile dell'unità.	intero
marca temporale	L'ora corrente nel formato UTC+0.	Stringa di data ISO 8601
capacità totale	Capacità totale dell'unità, in byte.	intero
Errori non correggibili	Il valore degli errori non correggibili segnalati dal sistema di monitoraggio SMART (Self-Monitoring, Analysis and Reporting Technology) nell'unità.	intero
Capacità utilizzata	Capacità utilizzata dell'unità, in byte.	intero
Memoria usata	Quantità di memoria attualmente utilizzata dal nodo che ospita questa unità.	intero
scrive	Numero di chiamate write() al secondo su questa unità.	intero
scriviBytes	Numero totale di byte scritti sull'unità a causa dell'attività del client.	intero
scriveCombinato	Numero di chiamate write() a settori adiacenti che potrebbero essere combinate in una scrittura più grande.	intero
scrivereMsec	Numero di millisecondi impiegati per scrivere.	intero
writeOps	Totale delle operazioni di scrittura sull'unità dovute all'attività del client.	intero

Trova maggiori informazioni

[Ottieni statistiche di guida](#)

errore

L'oggetto errore 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 il 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 il codice 500.	intero
nome	Identificatore univoco per l'errore specifico che si è verificato. Ogni metodo restituisce un set documentato di errori, ma è necessario essere preparati a gestire anche errori non riconosciuti.	corda
messaggio	Una descrizione dell'errore, eventualmente con ulteriori dettagli.	corda

evento

L'oggetto evento contiene i dettagli degli eventi che si verificano durante una chiamata al metodo API o mentre il sistema esegue un'operazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
dettagli	Ulteriori informazioni sull'evento.	Oggetto JSON
ID unità	L'ID dell'unità che segnala l'errore. 0 se non applicabile.	intero

Nome	Descrizione	Tipo
driveID	Un elenco degli ID delle unità che segnalano l'errore. Un elenco vuoto se non applicabile.	array di interi
ID evento	ID univoco associato a ciascun evento.	intero
eventInfoType	Il tipo di guasto.	corda
messaggio	Una descrizione in formato stringa dell'evento che si è verificato.	corda
ID nodo	L'ID nodo del nodo che segnala l'errore. 0 se non applicabile.	intero
ID servizio	ServiceID del servizio che segnala l'errore. 0 se non applicabile.	intero
gravità	Gravità segnalata dall'evento.	intero
tempo di pubblicazione	Ora in cui il registro eventi del cluster ha ricevuto l'evento, nel formato UTC+0.	Stringa di data ISO 8601
tempo di segnalazione	Ora in cui si è verificato l'evento sul cluster, nel formato UTC+0.	Stringa di data 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 eventi

L'elenco seguente descrive i possibili tipi di evento che il membro `eventInfoType` può contenere:

- `apiEvent`: eventi avviati tramite l'API o l'interfaccia utente Web che modificano le impostazioni.
- `binAssignmentsEvent`: Eventi correlati all'assegnazione di dati a contenitori 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 terminazioni dei servizi di blocco.
- `bulkOpEvent`: eventi che operano su un intero volume, ad esempio un backup, un ripristino, uno snapshot o un clone del 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 dell'ensemble.
- `driveEvent`: Eventi relativi alle operazioni di azionamento.
- `encryptionAtRestEvent`: Eventi relativi alla crittografia dei dati memorizzati.
- `ensembleEvent`: eventi correlati all'aumento o alla diminuzione delle dimensioni dell'ensemble.
- `fibreChannelEvent`: eventi relativi alla configurazione o alle connessioni dei nodi Fibre Channel.
- `gcEvent`: Eventi relativi alla garbage collection. Questi processi vengono eseguiti ogni 60 minuti per recuperare spazio di archiviazione sulle unità a blocchi.
- `ieEvent`: Eventi correlati a errori interni del sistema.
- `installEvent`: eventi relativi all'installazione automatica del software sui nodi di archiviazione in sospenso.
- `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 avvicinano al massimo consentito.
- `networkEvent`: Eventi correlati al networking virtuale.
- `platformHardwareEvent`: Eventi correlati ai problemi rilevati sui dispositivi hardware.
- `remoteClusterEvent`: Eventi correlati all'associazione di cluster remoti.
- `schedulerEvent`: Eventi correlati agli snapshot pianificati.
- `serviceEvent`: Eventi relativi allo stato del servizio di sistema.
- `statEvent`: Eventi relativi alle statistiche di sistema.
- `sliceEvent`: Eventi relativi all'archiviazione dei metadati.
- `snmpTrapEvent`: Eventi correlati alle trap SNMP.
- `tsEvent`: eventi del servizio di trasporto del sistema.
- `unexpectedException`: eventi correlati a errori imprevisti.
- `vasaProviderEvent`: eventi correlati a un provider VMware VASA.

Trova maggiori informazioni

[ElencoEventi](#)

colpa

L'oggetto `fault` contiene informazioni sui guasti 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
blocchiAggiornamento	L'errore blocca un aggiornamento. Valori possibili: • vero: l'errore blocca un aggiornamento. • false: l'errore non blocca l'aggiornamento.	booleano
clusterFaultID	ID univoco associato a ciascun errore del cluster.	intero
codice	Codice di errore per lo specifico errore rilevato. Per ulteriori dettagli, vedere Codici di errore del cluster.	corda
dati	Ulteriori informazioni specifiche sul guasto.	Oggetto JSON
data	L'ora corrente nel formato UTC+0.	Stringa ISO 8601
dettagli	Descrizione del guasto con dettagli aggiuntivi.	corda
ID unità	Il primo ID unità nell'elenco driveIDs. Se l'elenco driveIDs è vuoto (il che significa che non sono stati restituiti errori relativi alle unità), questo valore è 0.	intero
driveID	Un elenco di valori driveID per le unità a cui si riferisce questo errore. Incluso per guasti relativi alle unità. Se non ce n'è nessuno, si tratta di un array vuoto.	array di interi
nodeHardwareFaultID	Identificatore assegnato a un guasto hardware sul cluster.	intero
ID nodo	ID del nodo a cui si riferisce questo errore. Incluso per guasti di nodi e unità, altrimenti impostato su 0.	intero

Nome	Descrizione	Tipo
risolto	Lo stato risolto del guasto. Valori possibili: • vero: l'errore non viene più rilevato. • falso: il guasto è ancora presente.	booleano
Data di risoluzione	Data e ora in cui il guasto è stato risolto.	Stringa ISO 8601
ID servizio	Il servizio associato al guasto. Questo valore è "0" (zero) se l'errore non è associato a un servizio.	intero
gravità	La gravità del guasto. Valori possibili: • Attenzione: un problema minore. Il cluster è funzionante e gli aggiornamenti sono consentiti a questo livello di gravità. • errore: un errore che in genere non dovrebbe influire sul servizio (tranne un possibile degrado delle prestazioni o la perdita di HA). Alcune funzionalità potrebbero essere disabilitate. • critico: un guasto grave che compromette il servizio. Il sistema non è in grado di soddisfare le richieste API o l'I/O del client e rischia la perdita di dati. • bestPractice: guasti causati da una configurazione di sistema non ottimale.	corda

Nome	Descrizione	Tipo
tipo	Il tipo di guasto. Valori possibili: • nodo: un guasto che interessa un intero nodo. • unità: guasto che interessa una singola unità. • cluster: un guasto che interessa l'intero cluster. • servizio: un guasto che interessa un servizio sul cluster. • volume: Un guasto che colpisce un singolo volume.	corda

Trova maggiori informazioni

- [ListClusterFaults](#)
- ["Codici di errore del cluster"](#)

FibreChannelPort

L'oggetto `fibreChannelPort` contiene informazioni sulle singole porte di un nodo o di un intero nodo nel cluster. È possibile recuperare queste informazioni utilizzando il `ListNodeFibreChannelPortInfo` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
firmware	La versione del firmware installato sulla porta Fibre Channel.	intero
hbaPort	ID della singola porta dell'adattatore bus host (HBA).	intero
modello	Modello dell'HBA sulla porta.	corda
nPortID	ID univoco del nodo porta.	corda
Slot pci	Lo slot contenente la scheda PCI nello chassis del nodo Fibre Channel.	intero

Nome	Descrizione	Tipo
seriale	Il numero di serie sulla porta Fibre Channel.	corda
velocità	La velocità dell'HBA sulla porta.	corda
stato	Valori possibili: • Sconosciuto • Non presente • In linea • Fuori linea • Bloccato • Bypassato • Diagnostica • Collegamento in basso • Errore • Loopback • Eliminato	corda
switchWwn	Nome mondiale della porta dello switch Fibre Channel.	corda
wwnn	Nome del nodo HBA a livello mondiale.	corda
wwpn	Nome della porta mondiale assegnato alla porta fisica dell'HBA.	corda

Trova maggiori informazioni

[ListNodeFibreChannelPortInfo](#)

fipsErrorNodeReport

L'oggetto `fipsErrorNodeReport` contiene informazioni di errore per ciascun nodo che non risponde con informazioni sul supporto FIPS 140-2 quando lo si interroga con `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID nodo	L'ID del nodo che non ha risposto.	intero
errore	Un 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 archiviazione. È possibile recuperare queste informazioni utilizzando il `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID nodo	L'ID del nodo che segnala le informazioni.	intero
fipsDrives	Indica se la crittografia dell'unità FIPS 140-2 è abilitata o meno per questo nodo. Valori possibili: - Nessuno: questo nodo non è in grado di crittografare le unità FIPS. - Parziale: il nodo è in grado di crittografare le unità FIPS, ma non tutte le unità presenti sono compatibili con FIPS. - Pronto: il nodo è in grado di crittografare le unità FIPS e tutte le unità presenti sono compatibili con FIPS oppure non sono presenti unità.	FipsDrivesStatusType
httpsAbilitato	Indica se la crittografia HTTPS FIPS 140-2 è abilitata o meno per questo nodo. Valori possibili: - vero: abilitato - falso: disabilitato	booleano

fipsReport

L'oggetto `fipsReport` contiene informazioni sul supporto FIPS 140-2 per tutti i nodi nel cluster di archiviazione. È possibile recuperare queste informazioni utilizzando il `GetFipsReport` metodo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>nod</code>	Un report sullo stato del supporto FIPS 140-2 per ciascun nodo nel cluster di storage.	<code>fipsNodeReport</code>
<code>ErrorNodes</code>	Informazioni di errore per ciascun nodo che non ha risposto con lo stato di supporto FIPS 140-2.	<code>fipsErrorNodeReport</code>

groupSnapshot

L'oggetto `groupSnapshot` contiene informazioni su uno snapshot per un gruppo di volumi. Puoi usare il `ListGroupSnapshots` Metodo API per recuperare informazioni sullo snapshot del gruppo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>attributi</code>	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
<code>createTime</code>	Giorno e ora in formato UTC+0 in cui è stato creato lo snapshot del gruppo.	Stringa di data ISO 8601
<code>enableReplication</code>	Identifica se lo snapshot è abilitato per la replica remota.	booleano
<code>ID istantanea gruppo</code>	ID univoco dello snapshot del gruppo.	intero
<code>groupSnapshotUUID</code>	L'UUID dello snapshot del gruppo.	corda

Nome	Descrizione	Tipo
membri	Una matrice di oggetti contenente informazioni su ciascun membro dello snapshot del gruppo.	istantanea vetto
nome	Il nome dello snapshot del gruppo oppure, se non ne è stato specificato alcuno, il giorno e l'ora in formato UTC in cui è stato creato lo snapshot.	stringa o stringa di data ISO 8601
Stati remoti	Un array contenente l'identificatore universale e lo stato di replica di ogni snapshot remoto sul cluster di destinazione, così come visualizzato dal cluster di origine.	remoteClusterSnapshotStatus vetto
stato	Stato attuale 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 per l'uso e non è ancora scrivibile. • RemoteSyncing: questo snapshot viene replicato da un cluster remoto. • Fatto: la preparazione o la replica di questo snapshot sono state completate e ora è utilizzabile. • Attivo: questo snapshot è il ramo attivo. • Clonazione: questo snapshot è coinvolto in un'operazione CopyVolume.	corda

Trova maggiori informazioni

[ListGroupSnapshots](#)

Informazioni hardware

L'oggetto `hardwareInfo` contiene informazioni dettagliate sull'hardware e sullo stato di ciascun nodo nel cluster. È possibile recuperare queste informazioni con il `GetHardwareInfo` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
boardSerial	Numero di serie della scheda DMI.	corda
autobus	Informazioni sul bus multimediale della scheda madre.	Oggetto JSON
telaioSeriale	Il numero di serie del telaio.	corda
driveHardware	Un elenco di informazioni per ciascuna unità nel nodo.	Matrice di oggetti JSON
FibreChannelPorts	Un elenco delle porte Fibre Channel sul nodo.	array di interi
configurazione hardware	Informazioni sulla configurazione delle periferiche della scheda madre.	Oggetto JSON
kernelCrashDumpState	Configurazione del crash dump del kernel del sistema operativo.	corda
memoria	Informazioni sul firmware e sull'hardware della memoria di sistema.	Oggetto JSON
rete	Descrizioni dell'hardware di ciascuna interfaccia di rete del nodo.	Oggetto JSON
interfacce di rete	Lo stato delle interfacce di rete del nodo.	Oggetto JSON
NodoSlot	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 di archiviazione, questo valore è nullo.	corda
nvrाम	Statistiche NVRAM per il nodo.	Oggetto JSON
origine	Il fornitore della scheda madre.	corda

Nome	Descrizione	Tipo
piattaforma	Descrizione della piattaforma del telaio.	Oggetto JSON
seriale	Il numero di serie del prodotto.	corda
magazzinaggio	Informazioni sul controller di archiviazione.	Oggetto JSON
Memoria di sistema	Informazioni sull'utilizzo della memoria e sulle prestazioni del sistema operativo.	Oggetto JSON
sistema	Il tipo di chassis del nodo.	Oggetto JSON
uuid	L'ID univoco del nodo.	UUID

Trova maggiori informazioni

[Ottieni informazioni sull'hardware](#)

host (volumi virtuali)

L'oggetto host contiene informazioni su un host di volume virtuale. Puoi usare il `ListVirtualVolumeHosts` metodo per ottenere queste informazioni per tutti gli host del volume virtuale.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
legature	Un elenco di oggetti che descrivono i binding per l'host del volume virtuale.	array di interi
ID cluster	ID univoco del cluster a cui è associato questo host.	UUID
indirizzo host	L'indirizzo IP o il nome DNS dell'host del volume virtuale.	corda
nomi iniziatori	Un elenco di IQN di avvio per l'host del volume virtuale.	matrice di stringhe

Nome	Descrizione	Tipo
virtualVolumeHostID	ID univoco di questo host del volume virtuale.	UUID
visibleProtocolEndpointIDs	Un elenco di ID degli endpoint del protocollo visibili su questo host.	matrice UUID

Trova maggiori informazioni

[ListVirtualVolumeHosts](#)

idpConfigInfo

L'oggetto idpConfigInfo contiene dettagli di configurazione e integrazione relativi a un Identity Provider (IdP) di terze parti.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
abilitato	Specifica se questa configurazione IdP di terze parti è abilitata.	booleano
idpConfigurationID	UUID per la configurazione dell'IdP di terze parti.	UUID
idpMetadata	Metadati per i dettagli di configurazione e integrazione per l'accesso singolo SAML 2.0.	corda
Nome idp	Nome per il recupero del provider IdP per l'accesso singolo SAML 2.0.	corda
serviceProviderCertificate	Un certificato PKCS#10 X.509 codificato in Base64 in formato PEM da utilizzare per la comunicazione con questo IdP.	corda
spMetadataUrl	URL per il recupero dei metadati del fornitore di servizi (SP) dal cluster da fornire all'IdP per stabilire una relazione di trust.	corda

iniziatore

L'oggetto iniziatore contiene informazioni su un iniziatore iSCSI o Fibre Channel. Un oggetto iniziatore può contenere identificatori IQN o WWPN. Puoi usare il `ListInitiators` metodo per ottenere un elenco di tutti gli iniziatori noti sul sistema. Gli oggetti iniziatori vengono utilizzati per configurare l'accesso dell'iniziatore SCSI a un set di volumi tramite gruppi di accesso al volume. Un iniziatore può essere membro di un solo gruppo di accesso al 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 specifica alcuna rete virtuale, 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.	corda
attributi	Un set di attributi JSON assegnati a questo iniziatore. Vuoto se non sono assegnati attributi.	Oggetto JSON
chapUsername	Il nome utente CHAP univoco per questo iniziatore.	corda
ID iniziatore	Identificatore numerico dell'iniziatore.	intero
NomelIniziatore	Il nome dell'iniziatore, nel formato IQN o WWPN.	corda
iniziatoreSegreto	Il segreto CHAP utilizzato per autenticare l'iniziatore.	corda
requireChap	Vero se CHAP è richiesto per questo iniziatore.	booleano
targetSecret	Il segreto CHAP utilizzato per autenticare la destinazione (quando si utilizza l'autenticazione CHAP reciproca).	corda

Nome	Descrizione	Tipo
ID di rete virtuali	Elenco degli identificatori di rete virtuale associati a questo iniziatore. Se ne vengono definiti uno o più, questo iniziatore potrà accedere solo alle reti virtuali specificate. Se non sono definite reti virtuali, questo iniziatore può accedere a tutte le reti.	intero
volumeAccessGroups	Un elenco di ID di gruppi di accesso al volume a cui appartiene questo iniziatore.	array di interi

Trova maggiori informazioni

[Iniziatori di elenchi](#)

Autenticazione iSCSI

L'oggetto `ISCSIAuthentication` contiene informazioni di autenticazione su una sessione iSCSI.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
Metodo di autenticazione	Metodo di autenticazione utilizzato durante l'accesso alla sessione iSCSI, ad esempio CHAP o Nessuno.	corda
chapAlgorithm	L'algoritmo CHAP utilizzato, ad esempio MD5, SHA1*, SHA-256* o SHA3-256*	corda
chapUsername	Nome utente CHAP specificato dall'iniziatore durante l'accesso a una sessione iSCSI.	corda
direzione	La direzione dell'autenticazione, ad esempio unidirezionale (solo l'iniziatore) o bidirezionale (sia l'iniziatore che la destinazione).	corda

- Disponibile a partire da Element 12.7.

keyProviderKmip

L'oggetto `keyProviderKmip` descrive un fornitore di chiavi KMIP (Key Management Interoperability Protocol). Un fornitore di chiavi è sia un meccanismo che una posizione 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
ID fornitore di chiavi	L'ID del fornitore della chiave KMIP. Si tratta di un valore univoco assegnato dal cluster durante la creazione del fornitore di chiavi e non può essere modificato.	intero
<code>keyProviderIsActive</code>	Vero se il fornitore della chiave KMIP è attivo. Un provider è considerato attivo se sono presenti chiavi in sospeso che sono state create ma non ancora eliminate e che pertanto si presume siano ancora in uso.	booleano
Nome del fornitore di chiavi	Il nome del fornitore della chiave KMIP.	corda
<code>keyServerIDs</code>	Un ID del server chiave associato a questo provider. Il server deve essere aggiunto prima che questo provider possa diventare attivo. Il server non può essere rimosso finché questo provider è attivo. Per ogni provider è supportato un solo ID server.	array di interi
<code>kmipCapabilities</code>	Le capacità di questo fornitore di chiavi KMIP, inclusi i dettagli sulla libreria sottostante, la conformità FIPS, il fornitore SSL, ecc.	corda

keyServerKmip

L'oggetto `keyServerKmip` descrive un server di chiavi KMIP (Key Management Interoperability Protocol), ovvero una posizione per il recupero delle chiavi di autenticazione da utilizzare con funzionalità del cluster come la crittografia a riposo.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID fornitore di chiavi	Se questo server di chiavi KMIP è assegnato a un provider, questo membro contiene l'ID del provider di chiavi KMIP a cui è assegnato. Altrimenti questo membro è nullo.	intero
ID del server chiave	L'ID del server delle chiavi KMIP. Si tratta di un valore univoco assegnato dal cluster durante la creazione del server chiave. Questo valore non può essere modificato.	intero
kmipAssignedProviderIsActive	Se questo server di chiavi KMIP è assegnato a un provider (keyProviderID non è nullo), questo membro indica se il provider è attivo (fornendo chiavi attualmente in uso). Altrimenti, questo membro è nullo.	booleano
kmipCaCertificate	Il certificato della chiave pubblica della CA radice del server delle chiavi esterno. Viene utilizzato per verificare il certificato presentato dal server delle 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 radice di tutte le CA.	corda
kmipClientCertificate	Un certificato PKCS#10 X.509 codificato Base64 in formato PEM utilizzato dal client KMIP di Element Storage.	corda
kmipKeyServerHostnames	I nomi host o gli indirizzi IP associati a questo server di chiavi KMIP.	matrice di stringhe

Nome	Descrizione	Tipo
kmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda
kmipKeyServerPort	Il numero di porta associato a questo server di chiavi KMIP (in genere 5696).	intero

Configurazione ldap

L'oggetto `LdapConfiguration` contiene informazioni sulla configurazione LDAP sul sistema di archiviazione. È possibile recuperare le informazioni LDAP con `GetLdapConfiguration` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
tipo di autorizzazione	Identifica quale metodo di autenticazione utente utilizzare. Valori possibili: • Collegamento diretto • Cerca e associa	corda
abilitato	Identifica se il sistema è configurato o meno per LDAP. Valori possibili: • VERO • falso	booleano
groupSearchBaseDN	Il DN di base dell'albero da cui iniziare la ricerca del gruppo (da qui il sistema eseguirà una ricerca nel sottoalbero).	corda
groupSearchCustomFilter	Filtro di ricerca personalizzato utilizzato.	corda

Nome	Descrizione	Tipo
groupSearchType	Controlla il filtro di ricerca del gruppo predefinito utilizzato. Valori possibili: • NoGroups: nessun supporto di gruppo. • ActiveDirectory: appartenenza nidificata di tutti i gruppi AD di un utente. • MemberDN: gruppi di stile MemberDN (livello singolo).	corda
searchBindDN	Un DN completamente qualificato con cui effettuare l'accesso per eseguire una ricerca LDAP per l'utente (richiede l'accesso in lettura alla directory LDAP).	corda
serverURIs	Un elenco separato da virgole di URI del server LDAP (ad esempio, ldap://1.2.3.4 E ldaps://1.2.3.4:123.)	corda
ModelloDNutente	Una stringa utilizzata per formare un DN utente completamente qualificato.	corda
userSearchBaseDN	Il DN di base dell'albero utilizzato per avviare la ricerca (da qui verrà effettuata una ricerca nel sottoalbero).	corda
filtroricercautente	Filtro LDAP utilizzato.	corda

Trova maggiori informazioni

[OttieniLdapConfiguration](#)

Server di registrazione

L'oggetto `loggingServer` contiene informazioni su tutti gli host di registrazione configurati per il cluster di archiviazione. Puoi usare `GetRemoteLoggingHosts` per determinare quali sono gli host di registrazione correnti e quindi utilizzare `SetRemoteLoggingHosts` per impostare l'elenco desiderato di host di registrazione attuali e nuovi.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ospite	Indirizzo IP del server di registro.	corda
porta	Numero di porta utilizzato per comunicare con il server di registro.	intero

rete (interfacce vincolate)

L'oggetto rete (interfacce vincolate) contiene informazioni di configurazione per le interfacce di rete vincolate su un nodo di archiviazione. Puoi usare il `GetConfig` E `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
indirizzo	L'indirizzo IPv4 assegnato a questa interfaccia sul nodo.	corda
addressV6	L'indirizzo di gestione IPv6 assegnato all'interfaccia Bond1G sul nodo.	corda
ritardo di discesa del legame	Tempo di attesa, in millisecondi, prima di disabilitare uno slave dopo che è stato rilevato un errore di collegamento.	corda
bond-fail_over_mac	La configurazione dell'indirizzo MAC dell'interfaccia di rete.	corda
bond-miimon	Frequenza, in millisecondi, con cui viene verificato lo stato del collegamento MII per individuare eventuali guasti.	corda

modalità di legame	La modalità di legame. Valori possibili: • AttivoPassivo (predefinito) • CAMICE • LACP (consigliato)	corda
bond-primary_reselect	Specifica quando lo slave di legame primario viene scelto come slave attivo. Valori possibili: • Sempre • Meglio • Fallimento	corda
schiaivi-vincolati	Elenco delle interfacce slave per il bond.	corda
tasso_lacp_obbligazione	Quando Bond Mode è LACP, il tasso può cambiare in uno dei seguenti: • LACP Fast (predefinito) • LACP lento	corda
ritardo di assunzione del legame	Tempo di attesa, in millisecondi, prima di abilitare uno slave dopo che è stato rilevato un collegamento.	corda
server dei nomi DNS	Elenco di indirizzi utilizzati per i servizi di nomi di dominio, separati da virgola o spazio.	corda
ricerca dns	Un elenco di domini di ricerca DNS separati da spazi o virgole.	corda
famiglia	Famiglia di indirizzi per cui l'interfaccia è configurata. Attualmente è supportato "inet" per IPv4.	corda
porta d'accesso	Indirizzo di rete del router IPv4 utilizzato per inviare il traffico dalla rete locale.	corda

gatewayV6	Indirizzo di rete del router IPv6 utilizzato per inviare il traffico dalla rete Bond1G locale.	corda
ipV6PrefixLength	Lunghezza del prefisso di subnet per percorsi statici di tipo "net" per il traffico IPv6 sulla rete Bond1G.	corda
indirizzo MAC	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	corda
macAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	corda
metodo	Metodo utilizzato per configurare l'interfaccia. Valori possibili: • Loopback: utilizzato per definire l'interfaccia loopback IPv4. • manuale: utilizzato per definire le interfacce che non vengono configurate automaticamente. • dhcp: può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • statico: utilizzato per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.	corda
MTU	La dimensione massima del pacchetto (in byte) che l'interfaccia può trasmettere. Deve essere maggiore o uguale a 1500; è supportato fino a 9000.	corda
maschera di rete	La maschera di bit che specifica la subnet per l'interfaccia.	corda
rete	Indica dove inizia l'intervallo di indirizzi IP in base alla netmask.	corda
percorsi	Matrice di stringhe di routing separate da virgole da applicare alla tabella di routing.	matrice di stringhe

stato	Lo stato dell'interfaccia. Valori possibili: • Giù: l'interfaccia è inattiva. • Su: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: l'interfaccia è pronta e il collegamento è stato stabilito.	corda
Regole di percorso simmetriche	Le regole di routing simmetriche configurate sul nodo.	matrice di stringhe
attivo e funzionante	Indica se l'interfaccia è pronta e ha un collegamento.	booleano
virtualNetworkTag	Identificatore di rete virtuale dell'interfaccia (tag VLAN).	corda

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati in ogni possibile stato del nodo.

Nome del membro	Stato disponibile	Stato in sospeso	Stato attivo
indirizzo	Sì	Sì	NO
addressV6	Sì	Sì	NO
ritardo di discesa del legame	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 di legame	Sì	Sì	Sì
bond-primary_reselect	Configurato dal sistema	N / A	N / A
schiavi-vincolati	Configurato dal sistema	N / A	N / A
tasso_lacp_obbligazione	Sì	Sì	Sì
ritardo di assunzione del legame	Configurato dal sistema	N / A	N / A

server dei nomi DNS	Sì	Sì	Sì
ricerca dns	Sì	Sì	Sì
famiglia	NO	NO	NO
porta d'accesso	Sì	Sì	Sì
gatewayV6	Sì	Sì	Sì
ipV6PrefixLength	Sì	Sì	Sì
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
maschera di rete	Sì	Sì	Sì
rete	NO	NO	NO
percorsi	Sì	Sì	Sì
stato	Sì	Sì	Sì
Regole di percorso simmetriche	Configurato dal sistema	N / A	N / A
attivo e funzionante	Configurato dal sistema	N / A	N / A
virtualNetworkTag	Sì	Sì	Sì

Trova maggiori informazioni

- [OttieniConfig](#)
- [OttieniConfigurazione di rete](#)

rete (tutte le interfacce)

L'oggetto rete (tutte le interfacce) raccoglie informazioni sulla configurazione dell'interfaccia di rete per un nodo di archiviazione. Puoi usare il `GetConfig` E `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di

archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
Bond10G	Informazioni di configurazione per l'interfaccia bonded Bond10G.	rete (interfacce vincolate)
Bond1G	Informazioni di configurazione per l'interfaccia bonded Bond1G.	rete (interfacce vincolate)
eth0-5	Un oggetto per ogni interfaccia Ethernet nel nodo di archiviazione, 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 loopback.	rete (interfacce locali)

Trova maggiori informazioni

- [OttieniConfig](#)
- [OttieniConfigurazione di rete](#)

rete (interfacce Ethernet)

L'oggetto rete (interfacce Ethernet) contiene informazioni di configurazione per singole interfacce Ethernet. Puoi usare il `GetConfig` E `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
padrone del legame	Specifica a quale interfaccia collegata questa interfaccia fisica è associata come slave collegato.	corda

famiglia	Famiglia di indirizzi per cui l'interfaccia è configurata. Attualmente è supportato "inet" per IPv4.	corda
indirizzo MAC	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	corda
macAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	corda
metodo	Metodo utilizzato per configurare l'interfaccia. Valori possibili: • loopback: utilizzato per definire l'interfaccia loopback IPv4. • manuale: utilizzato per definire le interfacce che non vengono configurate automaticamente. • dhcp: può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • statico: utilizzato per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.	corda
stato	Lo stato dell'interfaccia. Valori possibili: • Giù: l'interfaccia è inattiva. • Su: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: l'interfaccia è pronta e il collegamento è stato stabilito.	corda
attivo e funzionante	Indica se l'interfaccia è pronta e ha un collegamento.	booleano

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati in ogni possibile stato del nodo.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
padrone del legame	NO	NO	NO

famiglia	NO	NO	NO
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
attivo e funzionante	Configurato dal sistema	N / A	N / A

Trova maggiori informazioni

- [OttieniConfig](#)
- [OttieniConfigurazione di rete](#)

rete (interfacce locali)

L'oggetto rete (interfacce locali) contiene informazioni di configurazione per le interfacce di rete locali, come l'interfaccia loopback, su un nodo di archiviazione. Puoi usare il `GetConfig` E `GetNetworkConfig` metodi per ottenere queste informazioni per un nodo di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
famiglia	Famiglia di indirizzi per cui l'interfaccia è configurata. Attualmente è supportato "inet" per IPv4.	corda
indirizzo MAC	L'indirizzo MAC effettivo assegnato all'interfaccia e osservato dalla rete.	corda
macAddressPermanent	L'indirizzo MAC immutabile assegnato dal produttore all'interfaccia.	corda

metodo	Metodo utilizzato per configurare l'interfaccia. Valori possibili: • loopback: utilizzato per definire l'interfaccia loopback IPv4. • manuale: utilizzato per definire le interfacce che non vengono configurate automaticamente. • dhcp: può essere utilizzato per ottenere un indirizzo IP tramite DHCP. • statico: utilizzato per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.	corda
stato	Lo stato dell'interfaccia. Valori possibili: • Giù: l'interfaccia è inattiva. • Su: L'interfaccia è pronta, ma non ha alcun collegamento. • UpAndRunning: l'interfaccia è pronta e il collegamento è stato stabilito.	corda
attivo e funzionante	Indica se l'interfaccia è pronta e ha un collegamento.	booleano

Modificabilità dei membri e stati dei nodi

Questa tabella indica se i parametri dell'oggetto possono essere modificati in ogni possibile stato del nodo.

Nome del parametro	Stato disponibile	Stato in sospeso	Stato attivo
famiglia	NO	NO	NO
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
attivo e funzionante	Configurato dal sistema	N / A	N / A

Trova maggiori informazioni

- [OttieniConfig](#)
- [OttieniConfigurazione di rete](#)

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	Tipo di accesso consentito per le richieste di informazioni SNMP. Valori possibili: • ro: Accesso di sola lettura. • rw: accesso in lettura-scrittura. • rosys: accesso in sola lettura a un set limitato di informazioni di sistema.	corda
sidro	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	La stringa della community SNMP.	corda
rete	Questo membro, insieme al membro cidr, controlla a quale rete si applicano la stringa di accesso e la stringa di comunità. 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".	corda

Trova maggiori informazioni

[OttieniSnmplInfo](#)

interfaccia di rete

L'oggetto `networkInterface` contiene informazioni di configurazione per singole interfacce di rete su un nodo di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>indirizzo</code>	L'indirizzo di gestione IPv4 dell'interfaccia.	corda
<code>addressV6</code>	Indirizzo di gestione IPv6 dell'interfaccia.	corda
<code>trasmissione</code>	L'indirizzo di broadcast dell'interfaccia.	corda
<code>indirizzo MAC</code>	L'indirizzo MAC dell'interfaccia.	corda
<code>MTU</code>	Unità di trasferimento massima, in byte, dell'interfaccia.	intero
<code>nome</code>	Il nome dell'interfaccia.	corda
<code>spazio dei nomi</code>	Se a questa interfaccia è assegnato o meno uno spazio dei nomi di rete virtuale.	booleano
<code>maschera di rete</code>	La maschera di sottorete dell'interfaccia.	corda
<code>stato</code>	Lo stato operativo dell'interfaccia.	corda
<code>tipo</code>	Il tipo di interfaccia (bond master, bond slave, ecc.).	corda
<code>virtualNetworkTag</code>	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 singole interfacce di rete su un nodo di archiviazione. Puoi usare il `ListNetworkInterfaceStats` Metodo API per elencare queste informazioni per le interfacce di rete su un nodo di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
collisioni	Numero di collisioni rilevate.	intero
nome	Nome dell'interfaccia di rete.	corda
rxBytes	Numero totale di byte ricevuti.	intero
Errori rxCrc	Numero di pacchetti ricevuti che presentavano un errore CRC.	intero
rxDropped	Numero di pacchetti ricevuti che sono stati eliminati.	intero
Errori rx	Numero di pacchetti errati o malformati ricevuti.	intero
Errori rxFifo	Numero di errori di superamento FIFO nei dati ricevuti.	intero
rxFrameErrors	Numero di pacchetti ricevuti con errori di allineamento dei frame.	intero
Errori di lunghezza rx	Numero di pacchetti ricevuti con un errore di lunghezza.	intero
rxMissedErrors	Numero di pacchetti persi dal ricevitore.	intero
rxOverErrors	Numero di errori di overflow del buffer ad anello del ricevitore per questa interfaccia.	intero
Pacchetti rx	Numero totale di pacchetti ricevuti.	intero
txByte	Numero totale di byte trasmessi.	intero
txCarrierErrors	Numero di errori di portante per il lato di trasmissione.	intero
txErrors	Numero di errori nella trasmissione dei pacchetti.	intero
txFifoErrors	Numero di errori di superamento FIFO sul lato trasmissione.	intero
txPackets	Numero totale di pacchetti trasmessi.	intero

nodo

L'oggetto nodo contiene informazioni su ciascun nodo nel cluster. È possibile recuperare queste informazioni utilizzando il `ListActiveNodes` E `ListAllNodes` metodi.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
IDServizioAssociato	ID del servizio Fibre Channel per il nodo. "0" se il nodo non è un nodo Fibre Channel.	intero
IDServizioMasterassociato	ID del servizio master per il nodo.	intero
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
Nometelaio	Identifica in modo univoco uno chassis; identico per tutti i nodi in un singolo chassis.	corda
cip	L'indirizzo IP del cluster assegnato al nodo.	corda
cipi	Interfaccia di rete utilizzata per la comunicazione del cluster.	corda
customProtectionDomainName	Identifica in modo univoco un dominio di protezione personalizzato. Questo nome è identico per tutti i nodi di archiviazione all'interno di tutti gli chassis in un dato dominio di protezione personalizzato.	corda
GruppoPortaTargetChannelFibre	Il gruppo target associato a questo nodo. "null" se il nodo non è un nodo Fibre Channel.	intero
Modalità di manutenzione	Indica in quale modalità si trova un nodo per manutenzione.	n / a
mip	L'indirizzo IP utilizzato per la gestione dei nodi.	corda
mipi	Interfaccia di rete utilizzata per la gestione dei nodi.	corda
nome	Nome host per il nodo.	corda
ID nodo	NodeID per questo nodo.	intero

Nome	Descrizione	Tipo
NodoSlot	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 di archiviazione, questo valore è nullo.	corda
informazioni sulla piattaforma	Informazioni hardware per il nodo. Membri: • chassisType: la piattaforma hardware del nodo. • cpuModel: modello di CPU della piattaforma hardware. • nodeMemoryGB: quantità di memoria installata nella piattaforma fisica in GB. • nodeType: il nome del modello del nodo. • platformConfigVersion: la versione del software configurata per questo hardware del nodo.	Oggetto JSON
ruolo	Il ruolo del nodo nel cluster. Valori possibili: • Gestione • Magazzinaggio • Calcolare • Testimone	
sorso	L'indirizzo IP di archiviazione assegnato al nodo.	corda
sipi	Interfaccia di rete utilizzata per il traffico di archiviazione.	corda
versione software	Restituisce la versione corrente del software Element in esecuzione sul nodo.	corda
uuid	L'identificatore univoco universale associato a questo nodo.	corda

Nome	Descrizione	Tipo
reti virtuali	Oggetto contenente indirizzi IP e ID di reti virtuali.	rete virtuale vettore

Trova maggiori informazioni

- [ListActiveNodes](#)
- [Elenca tutti i nodi](#)

nodeProtectionDomains

L'oggetto nodeProtectionDomains contiene informazioni sull'identità 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 nodo	Identificatore univoco per il nodo.	intero
protezioneDomini	Elenco dei domini di protezione di cui il nodo è membro.	"protezioneDominio"

nodeStats

L'oggetto nodeStats contiene misurazioni di attività di alto livello per un nodo. Puoi usare il `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
contare	Numero totale di campioni nell'oggetto nodeStats.	intero
processore	Utilizzo della CPU, in %.	intero
CPU totale	Valore di utilizzo della CPU in aumento monotono.	intero
cBytesIn	Byte nell'interfaccia del cluster.	intero

Nome	Descrizione	Tipo
cBytesOut	Byte in uscita sull'interfaccia del cluster.	intero
sBytesIn	Byte nell'interfaccia di archiviazione.	intero
sBytesOut	Byte in uscita sull'interfaccia di archiviazione.	intero
mBytesIn	Byte nell'interfaccia di gestione.	intero
mBytesOut	Byte in uscita sull'interfaccia di gestione.	intero
cluster di utilizzo della rete	Utilizzo dell'interfaccia di rete (in %) per l'interfaccia di rete del cluster.	intero
Utilizzo della rete Archiviazione	Utilizzo dell'interfaccia di rete (in %) per l'interfaccia di rete di archiviazione.	intero
nodoCalore	Informazioni sull'utilizzo dei nodi. Disponibile a partire da Element 12.8. Membri: • primaryTotalHeat: IOPS totali del nodo primario / IOPS configurati del nodo calcolati in media su 24 ore • recentPrimaryTotalHeat: IOPS totali del nodo primario / IOPS configurati dal nodo calcolati in media in un'ora • recentTotalHeat: IOPS totali del nodo / IOPS configurati dal nodo calcolati in media in un'ora • totalHeat: IOPS totali del nodo / IOPS configurati del nodo calcolati in media su 24 ore	Oggetto JSON
readLatencyUsecTotal	Valore monotono crescente del tempo totale impiegato per eseguire operazioni di lettura sul nodo.	intero

Nome	Descrizione	Tipo
readOps	Valore monotono crescente delle operazioni di lettura totali su un nodo.	intero
ssLoadHistogram	Dati dell'istogramma che illustrano il carico del servizio slice nel tempo.	Oggetto JSON
marca temporale	L'ora corrente nel formato UTC+0.	Stringa di data ISO 8601
Memoria usata	Utilizzo totale della memoria in byte.	intero
writeLatencyUsecTotal	Valore monotono crescente del tempo totale impiegato per eseguire operazioni di scrittura sul nodo.	intero
writeOps	Valore monotono crescente del totale delle operazioni di scrittura su un nodo.	intero

Trova maggiori informazioni

- [Ottieni statistiche nodo](#)
- [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
clientAPIMajorVersion	Versione principale dell'API ONTAP utilizzata dal client Element API.	corda

Nome	Descrizione	Tipo
clientAPIMinorVersion	Versione secondaria dell'API ONTAP utilizzata dal client Element API.	corda
ontapAPIMajorVersion	L'attuale versione principale dell'API supportata dal sistema ONTAP .	corda
ontapAPIMinorVersion	L'attuale versione secondaria dell'API supportata dal sistema ONTAP .	corda
ontapVersion	Versione software corrente in esecuzione sul cluster ONTAP .	corda

pendingActiveNode

L'oggetto `pendingActiveNode` contiene informazioni su un nodo che si trova attualmente nello stato `pendingActive`, tra gli stati `pending` e `active`. Si tratta di nodi che al momento vengono restituiti all'immagine software di fabbrica. Utilizzare il `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	Una chiave univoca che consente al nodo di unirsi automaticamente al cluster dopo l'installazione corretta del software.	corda
IDNodoassegnato	L'ID nodo assegnato al nodo.	corda
asyncHandle	L'handle del metodo asincrono che è possibile utilizzare per interrogare lo stato dell'operazione.	intero
cip	L'indirizzo IP del cluster assegnato al nodo.	corda
mip	L'indirizzo IP di gestione assegnato al nodo.	corda

Nome	Descrizione	Tipo
NodoSlot	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 di archiviazione, questo valore è nullo.	corda
pendingActiveNodeID	ID del nodo in sospeso.	intero
informazioni sulla piattaforma	Informazioni hardware per il nodo. Membri: • chassisType: la piattaforma hardware del nodo. • cpuModel: modello di CPU della piattaforma hardware. • nodeMemoryGB: quantità di memoria installata nella piattaforma fisica in GB. • nodeType: il nome del modello del nodo. • platformConfigVersion: la versione del software configurata per questo hardware del nodo.	Oggetto JSON
ruolo	Il ruolo del nodo nel cluster. Valori possibili: • Gestione • Magazzinaggio • Calcolare • Testimone	
sorso	L'indirizzo IP di archiviazione (iSCSI) assegnato al nodo.	corda
versione software	La versione corrente del software Element in esecuzione sul nodo.	corda

Trova maggiori informazioni

[Elenco nodi attivi in sospeso](#)

nodo in sospeso

L'oggetto `pendingNode` contiene informazioni su un nodo che può essere aggiunto a un cluster. Utilizzare il `ListPendingNodes` Metodo API per restituire un elenco di queste informazioni per tutti i nodi in sospeso. È possibile aggiungere uno qualsiasi dei nodi elencati a un cluster utilizzando `AddNodes` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>cipi</code>	L'indirizzo IP del cluster assegnato al nodo.	corda
<code>activeNodeKey</code>	Una chiave univoca che consente al nodo di unirsi automaticamente al cluster dopo l'installazione corretta del software.	corda
<code>IDNodoassegnato</code>	L'ID nodo assegnato al nodo.	corda
<code>asyncHandle</code>	L'handle del metodo asincrono che è possibile utilizzare per interrogare lo stato dell'operazione.	intero
<code>Nometelaio</code>	Identifica in modo univoco uno chassis; identico per tutti i nodi in un singolo chassis.	corda
<code>cip</code>	L'indirizzo IP del cluster assegnato al nodo.	corda
<code>mip</code>	L'indirizzo IP di gestione assegnato al nodo.	corda
<code>NodoSlot</code>	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 di archiviazione, questo valore è nullo.	corda
<code>pendingActiveNodeID</code>	ID del nodo in sospeso.	intero

Nome	Descrizione	Tipo
informazioni sulla piattaforma	Informazioni hardware per il nodo. Membri: • chassisType: la piattaforma hardware del nodo. • cpuModel: modello di CPU della piattaforma hardware. • nodeMemoryGB: quantità di memoria installata nella piattaforma fisica in GB. • nodeType: il nome del modello del nodo. • platformConfigVersion: la versione del software configurata per questo hardware del nodo.	Oggetto JSON
ruolo	Il ruolo del nodo nel cluster. Valori possibili: • Gestione • Magazzinaggio • Calcolare • Testimone	
sorso	L'indirizzo IP di archiviazione (iSCSI) assegnato al nodo.	corda
versione software	La versione corrente del software Element in esecuzione sul nodo.	corda

Trova maggiori informazioni

- [Aggiungi nodi](#)
- [Elenco nodi in sospeso](#)

protezioneDominio

L'oggetto protectionDomain contiene i dettagli sul nome e sul 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.	corda
protectionDomainType	Il tipo di dominio di protezione. Valori possibili: • chassis: tutti i nodi di archiviazione in un unico chassis. • personalizzato: tutti i nodi di archiviazione in un singolo dominio di protezione definito dal cliente.	corda

protezioneDomainLevel

L'oggetto protectionDomainLevel contiene informazioni sui livelli di tolleranza e resilienza correnti del cluster di archiviazione. I livelli di tolleranza indicano la capacità del cluster di continuare a leggere e scrivere dati in caso di errore, mentre i livelli di resilienza indicano la capacità del cluster di ripristinarsi automaticamente da uno o più errori 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 a cui sono associate tolleranza e resilienza. Valori possibili: • nodo: qualsiasi nodo individuale. • chassis: qualsiasi singolo nodo o tutti i nodi di archiviazione in un singolo chassis. • personalizzato: tutti i nodi di archiviazione in un singolo dominio di protezione definito dal cliente.	corda
resilienza	L'attuale resilienza di questo cluster dal punto di vista di questo tipo di dominio di protezione.	protezioneDomainResiliency

Nome	Descrizione	Tipo
tolleranza	L'attuale tolleranza di questo cluster dal punto di vista di questo tipo di dominio di protezione.	protezioneDominioTolleranza

protezioneDomainResiliency

L'oggetto `protectionDomainResiliency` contiene lo stato di resilienza di questo cluster di archiviazione. La resilienza indica la capacità del cluster di storage di ripristinarsi 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 è considerato ripristinato quando può continuare a leggere e scrivere dati nonostante 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
schema di protezioneResilienze	Un elenco di oggetti (uno per ogni schema di protezione) contenente informazioni sulla resilienza ai guasti per il tipo di dominio di protezione associato.	schema di protezioneResilienzavettore
singleFailureThresholdBytesForBlockData	Numero massimo di byte che possono essere archiviati nel cluster di archiviazione prima di perdere la capacità di ripristinare automaticamente uno stato di tolleranza del nodo.	intero
GuastisostenibiliPerInsieme	Numero previsto di guasti simultanei che possono verificarsi senza perdere la capacità di ripristinare automaticamente uno stato di tolleranza del nodo per il quorum dell'ensemble.	intero

protezioneDominioTolleranza

L'oggetto `protectionDomainTolerance` contiene informazioni sulla capacità del cluster di archiviazione di continuare a leggere e scrivere dati in caso di uno o più guasti, 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
Scheme di protezione Tolleranze	Un elenco di oggetti (uno per ogni schema di protezione) contenente informazioni sulla tolleranza ai guasti per il tipo di dominio di protezione associato.	schema di protezione Tolleranza vettore
GuastisostenibiliPerInsieme	Numero di guasti simultanei all'interno del tipo di dominio di protezione associato che possono verificarsi senza perdere il quorum dell'ensemble.	intero

schema di protezioneResilienza

L'oggetto `protectionSchemeResiliency` contiene informazioni sulla possibilità per un cluster di archiviazione, per uno schema di protezione specifico, di ripristinarsi automaticamente da uno o più errori all'interno del `protectionDomainType` associato. Un cluster di storage è considerato ripristinato quando può continuare a leggere e scrivere dati nonostante 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
schema di protezione	L'attuale schema di protezione di questo cluster di archiviazione. L'unico valore possibile è <code>doubleHelix</code> .	corda
GuastisostenibiliPerBlocchiDati	Numero previsto di guasti simultanei che possono verificarsi senza perdere la capacità di ripristinare automaticamente uno stato di tolleranza del nodo per i dati.	intero

Nome	Descrizione	Tipo
GuastisostenibiliPerMetadati	Numero previsto di guasti simultanei che possono verificarsi senza perdere la capacità di ripristinare automaticamente uno stato di tolleranza del nodo per i metadati.	intero

schema di protezione Tolleranza

L'oggetto `protectionSchemeTolerance` contiene informazioni sulla possibilità per un cluster di archiviazione, per uno schema di protezione specifico, di continuare a leggere e scrivere dati dopo errori.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
schema di protezione	L'attuale schema di protezione di questo cluster di archiviazione. L'unico valore possibile è <code>doubleHelix</code> .	corda
GuastisostenibiliPerBlocchiDati	Numero attuale di guasti simultanei che possono verificarsi senza perdere la disponibilità dei dati di blocco per lo schema di protezione associato.	intero
GuastisostenibiliPerMetadati	Numero attuale di guasti simultanei che possono verificarsi senza perdere la disponibilità dei metadati per lo schema di protezione associato.	intero

protocolloEndpoint

L'oggetto `protocolEndpoint` contiene gli attributi di un endpoint di 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
ID fornitore primario	ID dell'oggetto provider dell'endpoint del protocollo primario per l'endpoint del protocollo.	intero
protocolloEndpointID	ID univoco dell'endpoint del protocollo.	UUID
protocolloEndpointState	Lo stato dell'endpoint del protocollo. Valori possibili: • Attivo: l'endpoint del protocollo è in uso. • Inizio: l'endpoint del protocollo è in fase di avvio. • Failover: l'endpoint del protocollo ha subito un failover. • Riservato: l'endpoint del protocollo è riservato.	corda
tipo di fornitore	Il tipo di provider dell'endpoint del protocollo. Valori possibili: • Primario • Secondario	corda
scsiNAADeviceID	Identificatore univoco globale del dispositivo SCSI per l'endpoint del protocollo nel formato NAA IEEE Registered Extended.	corda
ID fornitore secondario	ID dell'oggetto provider dell'endpoint del protocollo secondario per l'endpoint del protocollo.	intero

Trova maggiori informazioni

[ListProtocolEndpoints](#)

Qualità del servizio

L'oggetto QoS contiene informazioni sulle impostazioni della qualità del servizio (QoS) 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 "picco" di IOPS di 4 KB consentito per brevi periodi di tempo. Consente picchi di attività I/O superiori al normale valore maxIOPS.	intero
Tempo di raffica	È consentita la durata del burstIOPS. Il valore restituito è espresso 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 dimensioni I/O in byte. I valori rappresentano il costo di esecuzione di un IOP a una dimensione I/O specifica. La curva è calcolata in relazione a un'operazione da 4096 byte impostata a 100 IOPS.	Oggetto JSON
IOPS massimi	Il massimo IOPS desiderato di 4 KB consentito per un periodo di tempo prolungato.	intero
minIOPS	Il minimo desiderato di 4 KB IOPS da garantire. Gli IOPS consentiti scenderanno al di sotto di questo livello solo se tutti i volumi sono stati limitati al loro valore minIOPS e la capacità di prestazioni è ancora insufficiente.	intero

Trova maggiori informazioni

[OttieniQoS predefinito](#)

Politica QoSP

L'oggetto QoSPolicy contiene informazioni su una policy QoS su 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 QoSPolicy assegnato automaticamente dal cluster di archiviazione.	intero
nome	Il nome della policy QoS. Ad esempio: oro, platino o argento.	corda
qualità	Le impostazioni QoS rappresentate da questa policy.	Qualità del servizio
volumeID	Elenco dei volumi associati a questa politica.	array di interi

Trova maggiori informazioni

[Ottieni la politica QoSPolicy](#)

remoteClusterSnapshotStatus

IL `remoteClusterSnapshotStatus` L'oggetto contiene l'UUID e lo stato di uno snapshot archiviato su un cluster di archiviazione remoto. Puoi ottenere queste informazioni con il `ListSnapshots` O `ListGroupSnapshots` Metodi API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
stato remoto	Lo stato di replica dello snapshot remoto sul cluster di destinazione così come viene visualizzato dal cluster di origine. Valori possibili: • Presente: lo snapshot esiste su un cluster remoto. • NotPresent: lo snapshot non esiste su un cluster remoto. • Sincronizzazione: questo è un cluster di destinazione e sta attualmente replicando lo snapshot. • Eliminato: questo è un cluster di destinazione. Lo snapshot è stato eliminato, ma è ancora presente sulla sorgente.	corda
volumePairUUID	Identificatore universale della coppia di volumi.	UUID

programma

L'oggetto pianificazione contiene informazioni su una pianificazione creata per creare autonomamente uno snapshot di un volume. È possibile recuperare le informazioni sulla pianificazione per tutte le pianificazioni con `ListSchedules` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
attributi	Indica la frequenza con cui si verifica la pianificazione. Valori possibili: • Giorno della settimana • Giorno del mese • Intervallo di tempo	Oggetto JSON
ha un errore	Indica se la pianificazione presenta errori. Valori possibili: • VERO • falso	booleano

Nome	Descrizione	Tipo
ore	Mostra le ore che trascorreranno prima che venga creato lo snapshot successivo. I valori possibili sono compresi tra 0 e 24.	intero
ultimoStatoEsecuzione	Indica lo stato dell'ultimo snapshot pianificato. Valori possibili: • Successo • Fallito	corda
lastRunTimeStart	Indica l'ultima volta in cui è iniziata la pianificazione.	Stringa di data ISO 8601
minuti	Mostra i minuti che trascorreranno prima che venga creato lo snapshot successivo. I valori possibili sono compresi tra 0 e 59.	intero
giorni del mese	Indica i giorni del mese in cui verrà effettuato uno snapshot.	vettore
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 la prossima volta che lo scheduler sarà attivo. Se impostato su true, la pianificazione verrà eseguita la volta successiva che lo scheduler sarà attivo, dopodiché questo valore verrà reimpostato su false. Valori possibili: • VERO • falso	booleano

Nome	Descrizione	Tipo
IDprogramma	L'ID univoco della pianificazione.	intero
informazioni sulla pianificazione	Include il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume da cui è stato creato lo snapshot. Valori validi: • <code>enableRemoteReplication</code>: Indica se lo snapshot deve essere incluso nella replica remota. (booleano) • <code>ensureSerialCreation</code>: specifica se è consentita la creazione di un nuovo snapshot se è in corso una replica di snapshot precedente. (booleano) • <code>name</code>: Nome dello snapshot da utilizzare. (corda) • <code>retention</code>: La quantità di tempo per cui viene conservato lo snapshot. A seconda dell'ora, viene visualizzato in uno dei seguenti formati: ◦ <code>fifo</code>: Lo snapshot viene conservato secondo il principio FIFO (First-In-First-Out). Se vuoto, lo snapshot viene conservato per sempre. (corda) ◦ <code>HH:mm:ss</code> • <code>volumeID</code>: ID del volume da includere nello snapshot. (numero intero) • <code>volumes</code>: Elenco degli ID volume da includere nello snapshot del gruppo. (array di interi)	Oggetto JSON
Nome programma	Il nome univoco assegnato alla pianificazione.	corda
tipo di programma	Al momento sono supportati solo i tipi di snapshot pianificati.	corda

Nome	Descrizione	Tipo
snapMirrorLabel	snapMirrorLabel da applicare allo Snapshot o allo Snapshot di gruppo creato, contenuto in scheduleInfo. Se non impostato, questo valore è nullo.	corda
data di inizio	Indica la data in cui è iniziata o inizierà la prima volta la programmazione; formattata in ora UTC.	Stringa di data ISO 8601
da eliminare	Indica se la pianificazione è contrassegnata per l'eliminazione. Valori possibili: • VERO • falso	booleano
giorni feriali	Indica i giorni della settimana in cui verrà effettuato uno snapshot.	vettore

Trova maggiori informazioni

[ListSchedules](#)

sessione (Fibre Channel)

L'oggetto sessione contiene informazioni su ciascuna sessione Fibre Channel visibile al cluster e sulle porte di destinazione su cui è visibile. È possibile recuperare queste informazioni con il `ListFibreChannelSessions` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
iniziatoreWWPN	Il nome della porta mondiale (WWPN) dell'iniziatore che ha effettuato l'accesso alla porta di destinazione.	corda
ID nodo	Il nodo proprietario della sessione Fibre Channel.	intero

Nome	Descrizione	Tipo
iniziatore	Informazioni sull'iniziatore del server di questa sessione Fibre Channel. Membri: • alias: il nome descrittivo assegnato all'iniziatore. • attributi: Gli attributi di questo iniziatore. • initiatorID: ID di questo iniziatore. • initiatorName: il nome di questo iniziatore. • volumeAccessGroups: elenco dei gruppi di accesso al volume associati a questo iniziatore.	Oggetto JSON
ID servizio	ID del servizio della porta di destinazione coinvolta in questa sessione.	intero
targetWWPN	Il WWPN della porta di destinazione coinvolta in questa sessione.	corda
volumeAccessGroupID	ID del gruppo di accesso al volume a cui appartiene l'initiatorWWPN. Se non si trova in un gruppo di accesso al volume, questo valore è nullo.	intero

Trova maggiori informazioni

[ListFibreChannelSessions](#)

sessione (iSCSI)

L'oggetto sessione (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	ID account dell'account utilizzato per l'autenticazione CHAP, se presente.	intero
nome utente	Nome dell'account utilizzato per l'autenticazione CHAP, se presente.	corda
autenticazione	Informazioni di autenticazione per questa sessione iSCSI.	Autenticazione iSCSI
createTime	Ora di creazione della sessione iSCSI, nel formato UTC+0.	Stringa di data ISO 8601
ID unità	Il driveID associato al servizio di trasporto che ospita la sessione.	intero
driveID	Un elenco degli ID delle unità che segnalano l'errore. Un elenco vuoto se non applicabile.	array di interi
iniziatore	Informazioni sull'iniziatore del server di questa sessione iSCSI. Membri: • alias: il nome descrittivo assegnato all'iniziatore. • attributi: Gli attributi di questo iniziatore. • initiatorID: ID di questo iniziatore. • initiatorName: il nome di questo iniziatore. • volumeAccessGroups: elenco dei gruppi di accesso al volume associati a questo iniziatore.	Oggetto JSON
iniziatoreIP	L'indirizzo IP e il numero di porta dell'iniziatore del server iSCSI.	corda
NomeIniziatore	Nome qualificato iSCSI (IQN) dell'iniziatore del server iSCSI.	corda
NomePortaIniziatore	L'initiatorName combinato con l'initiatorSessionID identifica la porta dell'iniziatore.	corda

Nome	Descrizione	Tipo
IDSessioneIniziatore	Un ID a 48 bit fornito dall'iniziatore che identifica la sessione iSCSI come appartenente a quell'iniziatore.	intero
msSinceLastIscsiPDU	Tempo, in millisecondi, trascorso dall'ultima ricezione dell'iSCSI PDU per questa sessione.	intero
msSinceLastScsiCommand	Tempo, in millisecondi, trascorso dall'ultimo comando SCSI ricevuto per questa sessione.	intero
ID nodo	Il nodeID associato al servizio di trasporto che ospita la sessione.	intero
ID servizio	ServiceID del servizio di trasporto che ospita la sessione.	intero
ID sessione	ID della sessione iSCSI.	intero
IP di destinazione	L'indirizzo IP e il numero di porta della destinazione di archiviazione iSCSI.	corda
NomeDestinazione	L'IQN della destinazione iSCSI.	corda
NomePortaDestinazione	Il tag targetName combinato con il tag del gruppo del portale di destinazione identifica la porta di destinazione.	corda
ID di rete virtuale	ID della rete virtuale associato alla sessione.	intero
ID volume	L'ID volume del volume associato alla sessione, se presente.	intero
volumeIstanza	Identifica l'oggetto volume associato alla sessione iSCSI, se presente.	intero

Trova maggiori informazioni

[Elenco iSCSI Sessioni](#)

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
NomeAggregato	Il nome dell'aggregato.	corda
NomeNodo	Nome del nodo ONTAP proprietario di questo aggregato.	corda
dimensioneDisponibile	Numero di byte disponibili rimanenti nell'aggregato.	intero
dimensioneTotale	La dimensione totale (in byte) dell'aggregato.	intero
percentuale di capacità utilizzata	Percentuale di spazio su disco attualmente in uso.	intero
volumeConteggio	Il numero di volumi totali.	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	Nome del cluster ONTAP di destinazione.	corda

Nome	Descrizione	Tipo
clusterUUID	Identificatore univoco universale a 128 bit del cluster ONTAP di destinazione.	corda
clusterSerialNumber	Numero di serie del cluster ONTAP di destinazione.	corda

snapMirrorEndpoint

L'oggetto snapMirrorEndpoint contiene informazioni sui sistemi di archiviazione SnapMirror remoti che comunicano con il cluster di archiviazione 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 per l'oggetto nel cluster locale.	intero
gestioneIP	Indirizzo IP di gestione del cluster dell'endpoint.	corda
Nome cluster	Nome del cluster ONTAP . Questo valore viene automaticamente popolato con il valore di "clusterName" dall'oggetto snapMirrorClusterIdentity.	corda
nome utente	Nome utente di gestione per il sistema ONTAP .	corda
indirizzi IP	Elenco degli indirizzi IP di archiviazione intercluster per tutti i nodi del cluster. È possibile ottenere questi indirizzi IP con il metodo ListSnapMirrorNetworkInterfaces.	matrice di stringhe
è Connesso	Lo stato di connettività del collegamento di controllo al cluster ONTAP .	booleano

snapMirrorJobScheduleCronInfo

L'oggetto snapMirrorJobScheduleCronInfo contiene informazioni sulla pianificazione di un cron job sul sistema ONTAP .

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
snapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
NomePianificazioneLavoro	Il nome della pianificazione del lavoro.	corda
jobScheduleDescription	Un riepilogo del programma, generato automaticamente e leggibile.	corda

snapMirrorLunInfo

L'oggetto snapMirrorLunInfo contiene informazioni sull'oggetto ONTAP LUN.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
snapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
creazioneTimestamp	Ora di creazione del LUN.	Stringa di data ISO 8601
lunName	Il nome del LUN.	corda
sentiero	Il percorso del LUN.	corda
misurare	La dimensione del LUN in byte.	intero
dimensioneUsato	Numero di byte utilizzati dalla LUN.	intero

Nome	Descrizione	Tipo
stato	Lo stato di accesso corrente della LUN. Valori possibili: • in linea • non in linea • errore_estero_lun • nvfail • errore_spazio	corda
volume	Nome del volume che contiene il LUN.	corda
server virtuale	Il Vserver che contiene il LUN.	corda

snapMirrorNetworkInterface

L'oggetto snapMirrorNetworkInterface contiene informazioni sulle interfacce logiche intercluster (LIF).

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
Stato amministrativo	Se l'interfaccia logica (LIF) è abilitata o disabilitata a livello amministrativo. Valori possibili: • su • giù	corda
snapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
NomeInterfaccia	Il nome LIF.	corda
indirizzo di rete	L'indirizzo IP del LIF.	corda
maschera di rete	La maschera di rete del LIF.	corda

Nome	Descrizione	Tipo
ruolointerfaccia	Il ruolo del LIF. Valori possibili: • indefinito • grappolo • dati • gestione_nodi • intercluster • gestione_cluster	corda
stato operativo	Lo stato operativo del LIF (se ha 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	corda
vserverName	Il nome del Vserver.	corda

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 .	corda
modello	Il modello del nodo ONTAP .	corda
numero di serie	Il numero di serie del nodo ONTAP .	corda
versione del prodotto	La versione del prodotto ONTAP .	corda

Nome	Descrizione	Tipo
isNodeHealthy	Lo stato di salute di un nodo nel cluster ONTAP . Valori possibili: • VERO • falso	corda
isNodeEligible	Se il nodo è idoneo o meno a partecipare a un cluster ONTAP . Valori possibili: • VERO • falso	corda

snapMirrorPolicy

L'oggetto snapMirrorPolicy contiene informazioni su una policy SnapMirror archiviata su un sistema ONTAP .

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
snapMirrorEndpointID	L'ID del sistema ONTAP di destinazione.	intero
NomePolitica	Il nome univoco assegnato alla policy.	corda
tipo di politica	Il tipo di politica. Valori possibili: • specchio asincrono • specchio_vault	corda
commento	Una descrizione leggibile associata alla policy SnapMirror .	corda

Nome	Descrizione	Tipo
trasferimentoPriorità	La priorità con cui viene eseguito un trasferimento SnapMirror . Valori possibili: • normale: la priorità predefinita. Questi trasferimenti vengono programmati prima della maggior parte dei trasferimenti a bassa priorità. • basso: questi trasferimenti hanno la priorità più bassa e vengono programmati dopo la maggior parte dei normali trasferimenti prioritari.	corda
policyRules	Un elenco di oggetti che descrivono le regole della policy.	snapMirrorPolicyRule vettore
totalKeepCount	Il conteggio totale della conservazione per tutte le regole nella policy.	intero
totalRules	Numero totale di regole nella policy.	intero
vserverName	Nome del Vserver per la policy SnapMirror .	corda

snapMirrorPolicyRule

L'oggetto snapMirrorPolicyRule contiene informazioni sulle regole in un criterio SnapMirror .

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
snapMirrorLabel	Etichetta della copia snapshot, utilizzata per la selezione della copia snapshot nelle relazioni di protezione dati estese.	corda

Nome	Descrizione	Tipo
keepCount	Specifica il numero massimo di copie snapshot conservate sul volume di destinazione 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	Identificatore univoco per ciascun oggetto snapMirrorRelationship in un array, come verrebbe restituito in ListSnapMirrorRelationships. Questo UUID viene creato e restituito dal sistema ONTAP .	corda
sorgenteVolume	Un oggetto che descrive il volume sorgente.	snapMirrorVolumeInfo
destinazioneVolume	Un oggetto che descrive il volume di destinazione.	snapMirrorVolumeInfo
tasso di trasferimento massimo corrente	La velocità di trasferimento massima attuale tra i volumi di origine e di destinazione, in kilobyte al secondo.	intero

Nome	Descrizione	Tipo
è sano	Se la relazione è sana o meno. Valori possibili: • vero: la relazione è sana. • falso: la relazione non è sana. Ciò può essere causato dal fallimento o dall'interruzione di un aggiornamento manuale o programmato, oppure dal ritardo dell'ultimo aggiornamento programmato.	booleano
tempo di ritardo	Quantità di tempo in secondi per cui i dati sul volume di destinazione sono in ritardo rispetto ai dati sul volume di origine.	intero
lastTransferDuration	Tempo in secondi impiegato per completare l'ultimo trasferimento.	intero
ultimoErroreTrasferimento	Un messaggio che descrive la causa dell'ultimo errore di trasferimento.	corda
lastTransferSize	Numero totale di byte trasferiti durante l'ultimo trasferimento.	intero
lastTransferEndTimestamp	Timestamp della fine dell'ultimo trasferimento.	Stringa di data ISO 8601
ultimo tipo di trasferimento	Il tipo di trasferimento precedente nella relazione.	corda
maxTransferRate	Specifica la velocità massima di trasferimento 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

Nome	Descrizione	Tipo
Stato specchio	Lo stato speculare della relazione SnapMirror . Valori possibili: • 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 SnapMirror . • interrotto: il volume di destinazione è di lettura-scrittura e sono presenti snapshot.	corda
più recenteSnapshot	Nome della copia Snapshot più recente sul volume di destinazione.	corda
NomePolitica	Specifica il nome del criterio ONTAP SnapMirror per la relazione. È possibile recuperare un elenco delle policy disponibili con ListSnapMirrorPolicies. I valori di esempio sono "MirrorLatest" e "MirrorAndVault".	corda
tipo di politica	Tipo di policy ONTAP SnapMirror per la relazione. Vedere ListSnapMirrorPolicies. Esempi sono: "async_mirror" o "mirror_vault".	corda
relazioneProgresso	Numero totale di byte elaborati finora per l'attività corrente della relazione, come restituito in relationship-status. Questa impostazione viene effettuata solo quando il membro "relationshipStatus" indica che è in corso un'attività.	intero

Nome	Descrizione	Tipo
stato di relazione	Lo stato della relazione SnapMirror . Valori possibili: • oziare • trasferimento • controllo • quiescente • inattivo • in coda • preparazione • finalizzazione • abortire • rottura	corda
tipo di relazione	Il tipo di relazione SnapMirror . Nei cluster di archiviazione che eseguono il software Element, questo valore è sempre "extended_data_protection".	corda
Nome programma	Nome della pianificazione cron preesistente sul sistema ONTAP utilizzata per aggiornare la relazione SnapMirror . È possibile recuperare un elenco delle pianificazioni disponibili con ListSnapMirrorSchedules.	corda
motivo malsano	Il motivo per cui la relazione non è sana.	corda

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	Descrizione	Tipo
nome	Il nome del volume.	corda
tipo	Il tipo di volume. Valori possibili: • rw: volume di lettura-scrittura • ls: Volume di condivisione del carico • dp: Volume di protezione dei dati	corda
server virtuale	Il nome del Vserver proprietario di questo volume.	corda
NomeAggr	Il nome dell'aggregato contenente.	corda
stato	Lo stato del volume. Valori possibili: • in linea • limitato • non in linea • misto	corda
misurare	Dimensione totale del file system (in byte) del volume.	corda
availSize	La dimensione (in byte) dello spazio disponibile nel volume.	corda

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 su un cluster di archiviazione che esegue il software Element. • ontap: il volume risiede su un cluster ONTAP remoto.	corda
ID volume	L'ID del volume. Valido solo se "type" è solidfire.	intero
server virtuale	Il nome del Vserver proprietario di questo volume. Valido solo se "type" è ontap.	corda
nome	Il nome del volume.	corda

snapMirrorVserver

L'oggetto snapMirrorVserver contiene informazioni sulle macchine virtuali di archiviazione (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.	corda
Tipo di server virtuale	Il tipo di Vserver. Valori possibili: • dati • amministratore • sistema • nodo	corda

Nome	Descrizione	Tipo
sottotipo vserver	Il sottotipo del Vserver. Valori possibili: • predefinito • dp_destinazione • dati • sincronizzazione_sorgente • destinazione_sincronizzazione	corda
volumeradice	Il volume radice del Vserver.	corda
rootVolumeAggregate	L'aggregato su cui verrà creato il volume radice.	corda
vserverAggregateInfo	Un array di oggetti snapMirrorVserverAggregateInfo.	Oggetto JSON
adminState	Lo stato amministrativo dettagliato del Vserver. Valori possibili: • corsa • fermato • di partenza • fermandosi • inizializzazione • eliminazione	corda
Stato operativo	Lo stato operativo di base del Vserver. Valori possibili: • corsa • fermato	corda

snapMirrorVserverAggregateInfo

L'oggetto snapMirrorVserverAggregateInfo contiene informazioni sulle macchine virtuali di archiviazione dati disponibili (chiamate anche Vserver) nel cluster ONTAP di destinazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
NomeAggr	Nome dell'aggregato assegnato a un Vserver.	corda
aggrAvailSize	Dimensione disponibile dell'aggregato assegnato.	intero

istantanea

L'oggetto snapshot contiene informazioni su uno snapshot creato per un volume. Puoi usare il `ListSnapshots` Metodo API per recuperare un elenco di informazioni 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 di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
somma di controllo	Una piccola rappresentazione in forma di stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in seguito per confrontare altri snapshot e rilevare errori nei dati.	corda
createTime	Ora in formato UTC+0 in cui è stato creato lo snapshot.	Stringa di data ISO 8601
enableReplication	Identifica se lo snapshot è abilitato per la replica remota.	booleano

Nome	Descrizione	Tipo
motivo di scadenza	Indica come viene impostata la scadenza dello snapshot. Valori possibili: • API: il tempo di scadenza viene impostato tramite l'API. • Nessuno: non è impostata alcuna scadenza. • Test: il tempo di scadenza è impostato per il test. • fifo: la scadenza avviene secondo il principio first-in-first-out.	corda
tempo di scadenza	Ora in cui questo snapshot scadrà e verrà eliminato dal cluster.	Stringa di data ISO 8601
ID gruppo	ID del gruppo se lo snapshot è membro di uno snapshot di gruppo.	intero
groupsnapshotUUID	Contiene informazioni su ogni snapshot del gruppo. Ciascuno di questi membri avrà un parametro UUID per l'UUID dello snapshot.	corda
instanceCreateTime	Ora in cui è stato creato lo snapshot sul cluster locale.	Stringa di data ISO 8601
instanceSnapshotUUID	ID univoco universale dello snapshot sul cluster locale. Questo ID non viene replicato in altri cluster.	corda
nome	Nome univoco assegnato allo snapshot. Se non viene specificato alcun nome, il nome è il timestamp in formato UTC+0 del momento in cui è stato creato lo snapshot.	corda
Stati remoti	Un array contenente l'identificatore universale e lo stato di replica di ogni snapshot remoto sul cluster di destinazione, così come visualizzato dal cluster di origine.	remoteClusterSnapshotStatus vetto re

Nome	Descrizione	Tipo
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare i criteri di conservazione degli snapshot sugli endpoint SnapMirror . Se non impostato, questo valore è nullo.	corda
ID istantanea	ID univoco di uno snapshot esistente.	corda
snapshotUUID	L'ID univoco universale di uno snapshot esistente. Quando lo snapshot viene replicato tra i cluster, questo ID viene replicato insieme ad esso e viene utilizzato per identificare lo snapshot tra i cluster.	corda
stato	Stato attuale 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 per l'uso e non è ancora scrivibile. • RemoteSyncing: questo snapshot viene replicato da un cluster remoto. • Fatto: la preparazione o la replica di questo snapshot sono state completate e ora è utilizzabile. • Attivo: questo snapshot è il ramo attivo. • Clonazione: questo snapshot è coinvolto in un'operazione CopyVolume.	corda
dimensione totale	La dimensione totale in byte dello snapshot.	intero
virtualVolumeID	ID del volume virtuale associato a questo snapshot.	UUID
ID volume	ID del volume da cui è stato creato lo snapshot.	intero

Nome	Descrizione	Tipo
NomeVolume	Nome del volume al momento della creazione dello snapshot.	corda

Trova maggiori informazioni

[ListSnapshots](#)

snmpTrapRecipient

L'oggetto snmpTrapRecipient contiene informazioni su un host configurato per ricevere trap SNMP generate dal cluster di archiviazione. Puoi usare il `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
ospite	L'indirizzo IP o il nome host dell'host di destinazione.	corda
porta	Numero di porta UDP sull'host a cui deve essere inviata la trap. L'intervallo valido è compreso tra 1 e 65535. 0 (zero) non è un numero di porta valido. La porta predefinita è 162.	intero
comunità	Stringa di comunità SNMP.	corda

contenitore di stoccaggio

L'oggetto storageContainer contiene gli attributi di un contenitore di archiviazione di volumi virtuali. È possibile recuperare queste informazioni per ogni contenitore di archiviazione nel cluster utilizzando `ListStorageContainers` Metodo API.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
ID account	ID dell'account del sistema di archiviazione associato al contenitore di archiviazione.	intero

Nome	Descrizione	Tipo
iniziatoreSegreto	Il segreto di autenticazione CHAP per l'iniziatore associato al contenitore di archiviazione.	corda
nome	Il nome del contenitore di stoccaggio.	corda
protocolloEndpointType	Tipo di endpoint del protocollo del contenitore di archiviazione. SCSI è l'unico valore valido.	corda
stato	Lo stato del contenitore di stoccaggio. Valori possibili: • Attivo: il contenitore di stoccaggio è in uso. • Bloccato: il contenitore di stoccaggio è bloccato.	corda
storageContainerID	ID univoco del contenitore di archiviazione.	UUID
targetSecret	Il segreto di autenticazione CHAP per la destinazione associata al contenitore di archiviazione.	corda
volumi virtuali	Un elenco di ID dei volumi virtuali associati al contenitore di archiviazione.	matrice UUID

Trova maggiori informazioni

[ListStorageContainers](#)

sincronizzazioneJob

L'oggetto syncJob contiene informazioni sui processi di clonazione, replica remota o sincronizzazione delle sezioni 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
blocchi al secondo	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 ramo	Restituito solo per i processi di sincronizzazione della replica remota. Valori possibili: • istantanea • volume	corda
byte al secondo	Numero di byte che il clone elabora al secondo. Presente solo se il membro del tipo è impostato su clone o slice.	galleggiante
cloneID	Identificatore dell'operazione di clonazione in corso. Presente solo se il membro del tipo è impostato su clone.	intero
byte correnti	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	Identificatore del servizio che ospita la replica primaria per il volume. Presente solo se il membro del tipo è impostato su remoto.	intero
dstVolumeID	ID del volume di destinazione. Presente solo se il membro del tipo è impostato su clone o remoto.	intero
tempo trascorso	Tempo trascorso, in secondi, dall'inizio del processo di sincronizzazione.	float o intero a seconda del tipo di operazione di sincronizzazione
groupCloneID	ID dell'operazione di clonazione del gruppo in corso.	intero

Nome	Descrizione	Tipo
ID nodo	Specifica il nodo su cui avviene la clonazione. Presente solo se il membro del tipo è impostato su clone.	intero
percentuale completata	Percentuale di completamento del processo di sincronizzazione.	float o intero a seconda del tipo di operazione di sincronizzazione
tempo rimanente	Tempo stimato, in secondi, per completare l'operazione.	galleggiante
sliceID	ID dell'unità slice in fase di sincronizzazione.	intero
palcoscenico	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 segnalato per questa fase del processo di replicazione. • dati: la replicazione è in corso e consiste nel trasferire la maggior parte dei dati al cluster remoto. • intero: indica la compatibilità con le versioni precedenti della slice per i processi di sincronizzazione delle slice.	corda
ID istantanea	ID dello snapshot da cui è stato creato il clone. Presente solo se il membro del tipo è impostato su clone.	intero
IDServizioSorgente	ID del servizio di origine.	intero
IDVolumesorgente	ID del volume di origine.	intero
byte totali	Numero totale di byte del clone. Presente solo se il membro del tipo è impostato su clone o slice.	intero

Nome	Descrizione	Tipo
tipo	Il tipo di operazione di sincronizzazione. Valori possibili: • clone • fetta • bloccare • remoto	corda

Trova maggiori informazioni

[ListSyncJobs](#)

attività (volumi virtuali)

L'oggetto attività contiene informazioni su un'attività di volume virtuale attualmente in esecuzione o terminata nel sistema. Puoi usare il `ListVirtualVolumeTasks` metodo per recuperare queste informazioni per tutte le attività del volume virtuale.

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	ID univoco del volume virtuale in fase di clonazione (per le attività di clonazione).	UUID
metadati genitori	Un oggetto contenente metadati dell'elemento padre per attività che clonano o creano snapshot di un volume virtuale.	Oggetto JSON
parentTotalSize	Spazio totale disponibile (in byte) sul padre per attività di clonazione o snapshot.	intero
parentUsedSize	Spazio utilizzato dall'elemento padre (in byte) per attività di clonazione o snapshot.	intero

Nome	Descrizione	Tipo
operazione	Il tipo di operazione che l'attività sta eseguendo. Valori possibili: • sconosciuto: l'operazione dell'attività è sconosciuta. • preparare: l'attività sta preparando un volume virtuale. • snapshot: l'attività consiste nel creare uno snapshot di un volume virtuale. • rollback: l'attività esegue il rollback di un volume virtuale in uno snapshot. • clone: l'attività consiste nel creare un clone del volume virtuale. • fastClone: l'attività consiste nel creare un clone veloce di un volume virtuale. • copyDiff: l'attività consiste nel copiare blocchi diversi in un volume virtuale.	corda
stato	Lo stato attuale dell'attività del volume virtuale. Valori possibili: • Errore: l'attività non è riuscita e ha restituito un errore. • In coda: l'attività è in attesa di essere eseguita. • In esecuzione: l'attività è attualmente in esecuzione. • Successo: l'attività è stata completata correttamente.	corda
virtualVolumeHostID	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 maggiori informazioni

[ListVirtualVolumeTasks](#)

usmUser

È possibile utilizzare l'oggetto SNMP `usmUser` con `SetSnmplnfo` Metodo API per configurare SNMP sul cluster di archiviazione.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	Tipo di accesso SNMP per questo utente. Valori possibili: • <code>rouser</code>: accesso di sola lettura. • <code>rwuser</code>: accesso in lettura-scrittura. Tutti gli oggetti MIB del software Element sono di sola lettura.	corda
nome	Il nome dell'utente.	corda
password	La password dell'utente.	corda
frase segreta	La passphrase dell'utente.	corda
secLevel	Il tipo di credenziali richieste per questo utente. Valori possibili: • <code>noauth</code>: non è richiesta alcuna password o passphrase. • <code>auth</code>: è richiesta una password per l'accesso dell'utente. • <code>priv</code>: Per l'accesso dell'utente sono necessarie una password e una passphrase.	corda

Trova maggiori informazioni

[ImpostaSnmplnfo](#)

rete virtuale

L'oggetto `virtualNetwork` contiene informazioni su una specifica rete virtuale. Puoi usare il `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
blocchi di indirizzi	L'intervallo di blocchi di indirizzi attualmente assegnati alla rete virtuale. Membri: • disponibile: stringa binaria composta da "1" e "0". "1" indica che l'indirizzo IP è disponibile, mentre "0" indica che l'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. • dimensione: la dimensione di questo blocco di indirizzi. • inizio: il primo indirizzo IP nel blocco.	Matrice di oggetti JSON
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
nome	Il nome assegnato alla rete virtuale.	corda
maschera di rete	L'indirizzo IP della netmask per la rete virtuale.	corda
svip	L'indirizzo IP di archiviazione per la rete virtuale.	corda
porta d'accesso	Il gateway utilizzato per la rete virtuale.	corda
ID di rete virtuale	Identificatore univoco per una rete virtuale.	intero
virtualNetworkTag	Identificatore del tag VLAN.	intero

Trova maggiori informazioni

[ElencoRetiVirtuali](#)

volume virtuale

L'oggetto `virtualVolume` contiene informazioni di configurazione su un volume virtuale, nonché informazioni sugli snapshot del volume virtuale. Non include informazioni sul tempo di esecuzione o sull'utilizzo. Puoi usare il `ListVirtualVolumes` metodo per recuperare queste informazioni per un cluster.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
<code>legature</code>	Un elenco di ID di binding per questo volume virtuale.	matrice UUID
<code>bambini</code>	Un elenco di UUID di volumi virtuali che sono figli di questo volume virtuale.	matrice UUID
<code>discendenti</code>	Quando si passa <code>recursive: true</code> al metodo <code>ListVirtualVolumes</code> , viene visualizzato un elenco di UUID di volumi virtuali che sono discendenti di questo volume virtuale.	matrice UUID
<code>metadati</code>	Coppie chiave-valore dei metadati del volume virtuale, come tipo di volume virtuale, tipo di sistema operativo guest e così via.	Oggetto JSON
<code>parentVirtualVolumeID</code>	ID del volume virtuale padre. Se l'ID è composto da soli zeri, si tratta di un volume virtuale indipendente senza alcun collegamento a un elemento padre.	UUID
<code>ID istantanea</code>	ID dello snapshot del volume sottostante. Questo valore è "0" se il volume virtuale non rappresenta uno snapshot.	intero
Informazioni sull'istantanea	L'oggetto snapshot per lo snapshot associato (null se non identico).	istantanea

Nome	Descrizione	Tipo
stato	Stato attuale del volume virtuale. Valori possibili: • clonazione: il volume virtuale viene elaborato in risposta a un'operazione di clonazione 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.	corda
contenitore di stoccaggio	Un oggetto che descrive il contenitore di archiviazione proprietario di questo volume virtuale.	contenitore di stoccaggio
virtualVolumeID	ID univoco del volume virtuale.	UUID
virtualVolumeType	Il tipo di volume virtuale.	corda
ID volume	L'ID del volume sottostante.	intero
Informazioni sul volume	Quando si passa details: true al metodo ListVirtualVolumes, questo membro è un oggetto che descrive il volume.	volume

Trova maggiori informazioni

- [ListVirtualVolumes](#)
- [istantanea](#)
- [contenitore di stoccaggio](#)
- [volume](#)

volume

L'oggetto volume contiene informazioni di configurazione sui volumi accoppiati o non accoppiati. Non include informazioni sull'esecuzione o sull'utilizzo e non contiene informazioni sui volumi virtuali.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
accesso	Tipo di accesso consentito per il volume. Valori possibili: • <code>readOnly</code>: Sono consentite solo le operazioni di lettura. • <code>readWrite</code>: Sono consentite letture e scritture. • <code>locked</code>: Non sono consentite letture o scritture. • <code>replicationTarget</code>: Designato come volume di destinazione in una coppia di volumi replicati.	corda
ID account	L'accountID dell'account contenente il volume.	intero
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
dimensione del blocco	La dimensione dei blocchi sul volume.	intero
createTime	Ora in formato UTC+0 in cui è stato creato il volume.	Stringa ISO 8601
schema di protezione attuale	Lo schema di protezione utilizzato per questo volume. Se un volume viene convertito da uno schema di protezione a un altro, questo membro riflette lo schema di protezione in cui il volume viene convertito.	corda
deleteTime	Ora formattata UTC+0 in cui il volume è stato eliminato.	Stringa ISO 8601
enable512e	Se impostato su <code>true</code> , il volume fornisce l'emulazione del settore da 512 byte.	booleano
enableSnapMirrorReplication	Se il volume può essere utilizzato o meno per la replica con endpoint <code>SnapMirror</code> .	booleano

Nome	Descrizione	Tipo
fifoSize	Specifica il numero massimo di snapshot del volume da mantenere contemporaneamente se si utilizza la modalità di conservazione degli snapshot First-In-First-Out (FIFO).	intero
iqn	Nome qualificato iSCSI del volume.	corda
ultimoAccesso	L'ultima volta che si è verificato un accesso (incluso I/O) al volume (formattato come UTC+0). Se l'orario dell'ultimo accesso non è noto, questo valore è nullo.	Stringa ISO 8601
lastAccessTimeIO	L'ultima volta che si è verificato un I/O sul volume (formattato come UTC+0). Se l'orario dell'ultimo accesso non è noto, questo valore è nullo.	Stringa ISO 8601
minFifoSize	Specifica il numero minimo di slot snapshot First-In-First-Out (FIFO) riservati simultaneamente dal volume se si utilizza la modalità di conservazione snapshot First-In-First-Out (FIFO).	intero
nome	Il nome del volume fornito al momento della creazione.	corda
precedenteSchema di protezione	Se un volume viene convertito da uno schema di protezione a un altro, questo membro riflette lo schema di protezione da cui il volume viene convertito. Questo membro non cambia finché non viene avviata una conversione. Se un volume non è mai stato convertito, questo membro è nullo.	corda
Tempo di purificazione	Ora in formato UTC+0 in cui il volume è stato eliminato dal sistema.	Stringa ISO 8601
qualità	Impostazioni della qualità del servizio per questo volume.	Qualità del servizio

Nome	Descrizione	Tipo
qosPolicyID	ID della policy QoS associata al volume. Il valore è nullo se il volume non è associato a una policy.	intero
scsiEUIDeviceID	Identificatore univoco globale del dispositivo SCSI per il volume nel formato a 16 byte basato su EUI-64.	corda
scsiNAADeviceID	Identificatore univoco globale del dispositivo SCSI per il volume nel formato NAA IEEE Registered Extended.	corda
sliceCount	Il numero di sezioni sul volume. Questo valore è sempre "1".	intero
stato	Lo stato attuale del volume. Valori possibili: • init: un volume che è in fase di inizializzazione e non è pronto per le connessioni. • attivo: un volume attivo pronto per le connessioni. • eliminato: un volume che è stato contrassegnato per l'eliminazione, ma non ancora ripulito.	corda
dimensione totale	Il totale dei byte della 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 a cui appartiene un volume. Questo valore è un elenco vuoto se un volume non appartiene ad alcun gruppo di accesso al volume.	array di interi
volumeConsistencyGroupUUID	ID univoco universale del gruppo di coerenza del volume di cui il volume è membro.	UUID

Nome	Descrizione	Tipo
ID volume	VolumeID univoco per il volume.	intero
coppie di volumi	Informazioni su un volume accoppiato. Visibile solo se un volume è associato. Questo valore è un elenco vuoto se il volume non è associato.	volumePair vettore
volumeUUID	L'ID univoco universale del volume.	UUID

Trova maggiori informazioni

- [ListActiveVolumes](#)
- [ElencoVolumiEliminati](#)
- [ElencoVolumi](#)
- [ListVolumesForAccount](#)
- [Qualità del servizio](#)

volumeAccessGroup

L'oggetto `volumeAccessGroup` contiene informazioni su uno specifico gruppo di accesso al 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 di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON
volumi eliminati	Matrice di volumi eliminati dal gruppo di accesso al volume e non ancora eliminati dal sistema.	array di interi
ID iniziatore	Un elenco di ID degli iniziatori mappati al gruppo di accesso al volume.	array di interi
iniziatori	Matrice di iniziatori IQN/WWPN univoci mappati al gruppo di accesso al volume.	matrice di stringhe

Nome	Descrizione	Tipo
nome	Nome del gruppo di accesso al volume.	corda
volumeAccessGroupID	Identificatore univoco VolumeAccessGroupID per il gruppo di accesso al volume.	intero
volumi	Un elenco di VolumeID appartenenti al gruppo di accesso al volume.	array di interi

Trova maggiori informazioni

[ListVolumeAccessGroups](#)

volumePair

L'oggetto volumePair contiene informazioni su un volume abbinato a un altro volume su un cluster diverso. Se il volume non è associato, questo oggetto è vuoto. Puoi usare il `ListActivePairedVolumes` E `ListActiveVolumes` Metodi API per restituire informazioni sui volumi accoppiati.

Membri dell'oggetto

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Tipo
clusterPairID	Il cluster su cui è accoppiato il volume.	intero

Nome	Descrizione	Tipo
replica remota	Dettagli sulla replicazione del volume. Membri: • modalità: (stringa) Una tra "Async", "Sync" o "SnapshotsOnly". • pauseLimit: (intero) Solo per uso interno. • remoteServiceID: (intero) ID del servizio slice remoto. • resumeDetails: (stringa) Riservato per uso futuro. • snapshotReplication (oggetto JSON) ◦ stato: (stringa) Lo stato della replica dello snapshot in corso, se ne è in corso una. ◦ stateDetails: (stringa) Riservato per uso futuro. • stato: (stringa) Lo stato della replica del volume. • stateDetails: (stringa) Riservato per uso futuro.	Oggetto JSON
remoteSliceID	ID della slice definita dal cluster sul cluster remoto.	intero
remoteVolumeID	ID del volume sul cluster remoto a cui è associato il volume locale.	intero
NomeVolumeRemoto	Il nome del volume remoto.	corda
volumePairUUID	Un identificatore univoco universale, definito dal cluster, per questa coppia in un formato canonico.	corda

Trova maggiori 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:

- [Ottieni statistiche sul volume](#)
- [ListVolumeStatsByAccount](#)
- [ListVolumeStatsByVolume](#)
- [ListVolumeStatsByVolumeAccessGroup](#)

Questo oggetto contiene i seguenti membri:

Nome	Descrizione	Calcolo	Tipo
ID account	ID dell'account del proprietario del volume.	N / A	intero
IOPS effettivi	Gli IOPS effettivi correnti sul volume negli ultimi 500 millisecondi.	Punto nel tempo	intero
ritardo asincrono	Periodo di tempo trascorso dall'ultima sincronizzazione del volume con il cluster remoto. Se il volume non è abbinato, questo è nullo. Nota: un volume di destinazione in uno stato di replicazione attivo ha sempre un asyncDelay pari a 0 (zero). I volumi di destinazione sono consapevoli del sistema durante la replica e presuppongono che asyncDelay sia sempre accurato.	N / A	Stringa di durata ISO 8601 o null
dimensione media dell'IOP	Dimensione media in byte delle recenti operazioni di I/O sul volume negli ultimi 500 millisecondi.	Punto nel tempo	intero
burstIOPSCredit	Numero totale di crediti IOP disponibili per l'utente. Quando i volumi non raggiungono il massimo IOPS configurato, vengono accumulati dei crediti.	N / A	intero
clientQueueDepth	Numero di operazioni di lettura e scrittura in sospeso sul volume.	N / A	intero
desiredMetadataHosts	I servizi di metadati (slice) verso cui viene eseguita la migrazione se i metadati del volume vengono migrati tra servizi di metadati. Un valore "null" indica che il volume non è in fase di migrazione.	N / A	Oggetto JSON

Nome	Descrizione	Calcolo	Tipo
latenzaUsec	Tempo medio, in microsecondi, impiegato per completare le operazioni sul volume negli ultimi 500 millisecondi. Un valore "0" (zero) indica che non vi è alcun I/O sul volume.	Punto nel tempo	intero
metadatiHosts	I 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 inattivo.	N / A	Oggetto JSON
IOPS normalizzati	Numero medio di IOPS per l'intero cluster negli ultimi 500 millisecondi.	Punto nel tempo	intero
nonZeroBlocks	Numero totale di blocchi da 4 KiB contenenti dati dopo il completamento dell'ultima operazione di garbage collection.	N / A	intero
Leggi byte	Numero totale di byte cumulativi letti dal volume dalla sua creazione.	Monotonicamente crescente	intero
readBytesLastSample	Numero totale di byte letti dal volume durante l'ultimo periodo di campionamento.	Punto nel tempo	intero
readLatencyUsec	Tempo medio, in microsecondi, impiegato per completare le operazioni di lettura sul volume negli ultimi 500 millisecondi.	Punto nel tempo	intero
readLatencyUsecTotal	Tempo totale impiegato per eseguire operazioni di lettura dal volume.	Monotonicamente crescente	intero
readOps	Il numero totale di operazioni di lettura sul volume dalla sua creazione.	Monotonicamente crescente	intero
readOpsLastSample	Numero totale di operazioni di lettura durante l'ultimo periodo di campionamento.	Punto nel tempo	intero
samplePeriodMsec	La lunghezza del periodo di campionamento, in millisecondi.	N / A	intero

Nome	Descrizione	Calcolo	Tipo
slicelopsStats	Statistiche di utilizzo I/O per un volume. Disponibile a partire da Element 12.8. Valori possibili per slicelopsStats: • largeStatistics: statistiche I/O per il volume misurate su un periodo di tempo più lungo, in genere le ultime 24 ore. • smallStatistics: statistiche I/O per il volume misurate in un periodo di tempo più breve, in genere l'ultima ora. Valori possibili per largeStatistics e smallStatistics: • averageReadlops: IOPS di lettura medi per il volume. • averageTotallops: IOPS totali medi (lettura + scrittura) per il volume. • averageWritelops: IOPS di scrittura medi per il volume. • nCampioni: numero di campioni inclusi nel calcolo statistico. • peakReadlops: il massimo IOPS di lettura osservato in un intervallo statistico. • peakTotallops: IOPS totali massimi osservati in un intervallo statistico. • peakWritelops: il massimo IOPS di scrittura osservato in un intervallo statistico. • sliceID: ID volume o ID slice	Punto nel tempo	Oggetto JSON
acceleratore	Un valore mobile compreso tra 0 e 1 che rappresenta la misura in cui il sistema sta limitando i client al di sotto del loro maxIOPS a causa della replica dei dati, degli errori temporanei e degli snapshot acquisiti.	N / A	galleggiante
marca temporale	L'ora corrente nel formato UTC+0.	N / A	Stringa di data ISO 8601
Letture non allineate	Il totale cumulativo delle operazioni di lettura non allineate su un volume dalla creazione del volume.	Monotonicamente crescente	intero
non allineatoScrive	Il totale cumulativo delle operazioni di scrittura non allineate su un volume dalla creazione del volume.	Monotonicamente crescente	intero
volumeAccessGroups	Elenco degli ID dei gruppi di accesso al volume a cui appartiene un volume.	N / A	array di interi

Nome	Descrizione	Calcolo	Tipo
ID volume	L'ID del volume.	N / A	intero
volumeDimensione	Capacità totale fornita in byte.	N / A	intero
volumeUtilizzo	Un valore in virgola mobile che descrive il livello di utilizzo delle capacità di input/output del volume da parte del client rispetto all'impostazione QoS maxIOPS per quel volume. Valori possibili: • 0: Il client non sta utilizzando il volume. • Da 0,01 a 0,99: il client non utilizza appieno le capacità 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 QoS burstIOPS è impostata su un valore superiore a maxIOPS. Ad esempio, se maxIOPS è impostato su 1000 e burstIOPS è impostato su 2000, volumeUtilization il valore sarebbe 2,00 se il client utilizzasse completamente il volume.	N / A	galleggiante
scriviBytes	Il totale cumulativo dei byte scritti nel volume dalla sua creazione.	Monotonicamente crescente	intero
writeBytesLastSample	Numero totale di byte scritti sul volume durante l'ultimo periodo di campionamento.	Monotonicamente crescente	intero
writeLatencyUsec	Tempo medio, in microsecondi, impiegato per completare le operazioni di scrittura su un volume negli ultimi 500 millisecondi.	Punto nel tempo	intero
writeLatencyUsecTotal	Tempo totale impiegato per eseguire operazioni di scrittura sul volume.	Monotonicamente crescente	intero
writeOps	Il totale cumulativo delle operazioni di scrittura sul volume dalla sua creazione.	Monotonicamente crescente	intero
writeOpsLastSample	Numero totale di operazioni di scrittura durante l'ultimo periodo di campionamento.	Punto nel tempo	intero
zeroBlocks	Numero totale di blocchi vuoti da 4 KiB senza dati dopo il completamento dell'ultimo ciclo di operazioni di garbage collection.	Punto nel tempo	intero

Metodi comuni

OttieniAPI

Puoi usare il `GetAPI` metodo per ottenere un elenco di tutti i metodi API e degli endpoint API supportati che possono essere utilizzati nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
<versione>	Un elenco di tutti i metodi API supportati per questa versione del software, dove <versione> è la versione corrente del software in esecuzione su questo sistema.	matrice di stringhe
versione corrente	La versione corrente del software del cluster di archiviazione.	corda
versioni supportate	Un elenco di tutti gli endpoint API supportati dal sistema.	matrice di stringhe

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetAPI",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "12.0": [
```

"AbortSnapMirrorRelationship",
"AddAccount",
"AddClusterAdmin",
"AddDrives",
"AddIdpClusterAdmin",
"AddInitiatorsToVolumeAccessGroup",
"AddKeyServerToProviderKmp",
"AddLdapClusterAdmin",
"AddNodes",
"AddVirtualNetwork",
"AddVolumesToVolumeAccessGroup",
"BreakSnapMirrorRelationship",
"BreakSnapMirrorVolume",
"CancelClone",
"CancelGroupClone",
"CheckPingOnVlan",
"CheckProposedCluster",
"CheckProposedNodeAdditions",
"ClearClusterFaults",
"CloneMultipleVolumes",
"CloneVolume",
"CompleteClusterPairing",
"CompleteVolumePairing",
"CopyVolume",
"CreateBackupTarget",
"CreateClusterInterfacePreference",
"CreateClusterSupportBundle",
"CreateGroupSnapshot",
"CreateIdpConfiguration",
"CreateInitiators",
"CreateKeyProviderKmp",
"CreateKeyServerKmp",
"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",
"ListQoS Policies",
```

```
"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"
    ]
}
}

```

Ottieni risultato asincrono

Puoi usare `GetAsyncResult` per recuperare il risultato delle chiamate di metodi asincroni. L'esecuzione di alcune chiamate di metodo richiede un po' di tempo e potrebbe non essere completata quando il sistema invia la risposta iniziale. Per ottenere lo stato o il risultato della chiamata al metodo, utilizzare `GetAsyncResult` per interrogare il valore `asyncHandle` restituito dal metodo.

`GetAsyncResult` restituisce lo stato generale dell'operazione (in corso, completata o errore) in modo standard, ma i dati effettivamente 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 i successivi tentativi di interrogare tale `asyncHandle` restituiscono un errore. È possibile mantenere attivo `asyncHandle` per query future impostando il parametro `keepResult` su `true`.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
asyncHandle	Un valore restituito dalla chiamata al metodo asincrono originale.	intero	Nessuno	Sì
Mantieni il risultato	Se è vero, GetAsyncResult non rimuove il risultato asincrono quando lo restituisce, consentendo future query a tale asyncHandle.	booleano	falso	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
stato	Stato della chiamata al metodo asincrono. Valori possibili: - in esecuzione: il metodo è ancora in esecuzione. - completo: il metodo è completo e il risultato o l'errore sono disponibili.	corda
risultato	Se il metodo asincrono è stato completato correttamente, questo è il risultato dell'operazione asincrona. Se l'operazione asincrona non riesce, questo membro non è presente.	corda
errore	Se lo stato è completo e il metodo asincrono non è riuscito, questo membro include i dettagli dell'errore. Se l'operazione asincrona è riuscita, questo membro non è presente.	corda
tipo di risultato	Tipo di operazione eseguita o eseguita dalla chiamata al metodo asincrono.	corda

Nome	Descrizione	Tipo
dettagli	Se lo stato è in esecuzione, questo membro include informazioni rilevanti per l'operazione corrente del metodo. Se il metodo asincrono non è in esecuzione, questo membro non è presente.	Oggetto JSON
createTime	Ora in cui è stato chiamato il metodo asincrono, nel formato UTC+0.	Stringa di data ISO 8601
ultimoAggiornamento	Ora dell'ultimo aggiornamento dello stato del metodo asincrono, nel formato UTC+0.	Stringa di data ISO 8601

Nota: il valore restituito da `GetAsyncResult` è essenzialmente una versione annidata della risposta JSON standard con un campo di stato aggiuntivo.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetAsyncResult",
  "params": {
    "asyncHandle" : 389
  },
  "id" : 1
}
```

Esempio di risposta: errore di metodo

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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`, allora "response.error"

corrisponderebbe a un errore con il metodo GetAsyncResult stesso (ad esempio la query di un asyncHandle inesistente).

Esempio di risposta: errore di attività asincrona

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

“response.result.error” corrisponderebbe a un risultato di errore dalla chiamata al metodo originale.

Esempio di risposta: successo dell'attività asincrona

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

“response.result.result” è il valore restituito per la chiamata al metodo originale se la chiamata è stata completata correttamente.

Nuovo dalla versione

9,6

Ottieni statistiche complete

L'ingegneria NetApp utilizza il `GetCompleteStats` Metodo API per testare nuove funzionalità. I dati restituiti da `GetCompleteStats` non è documentato, cambia frequentemente e non se ne garantisce l'accuratezza. Non dovresti usare `GetCompleteStats` per la raccolta di dati sulle prestazioni o qualsiasi altra integrazione di gestione con un cluster di storage che esegue il software Element.

Utilizzare i seguenti metodi API supportati per recuperare informazioni statistiche:

- [Ottieni statistiche sul volume](#)
- [Ottieni statistiche cluster](#)
- [Ottieni statistiche nodo](#)
- [Ottieni statistiche di guida](#)

Nuovo dalla versione

9,6

Ottieni limiti

Puoi usare il `GetLimits` metodo per ottenere i valori limite impostati dall'API. Questi valori potrebbero cambiare tra le versioni 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` Il metodo 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 di ritorno

Questo metodo restituisce un oggetto JSON con coppie nome-valore contenenti i limiti API.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetLimits",
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": 10000000000,
    "volumesPerAccountCountMax": 2000,
    "volumesPerGroupSnapshotMax": 32,
    "volumesPerVolumeAccessGroupCountMax": 2000,
    "witnessNodesPerClusterCountMax": 4
  }
}

```

Nuovo dalla versione

9,6

Ottieni origine

Puoi usare il `GetOrigin` metodo per ottenere il certificato di origine per il luogo in cui è stato creato il nodo.

Parametri



Questo metodo restituisce "null" se non è presente alcuna certificazione di origine.

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo restituisce le informazioni sulla certificazione di origine del fornitore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetOrigin",
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "integrator": "SolidFire",
  "<signature>": {
    "pubkey": [public key info],
    "version": 1,
    "data": [signature info]
  },
  "contract-id": "none",
  "location": "Boulder, CO",
  "organization": "Engineering",
  "type": "element-x"
}
]
```

Nuovo dalla versione

9,6

Ottieni statistiche grezze

L'ingegneria NetApp utilizza il `GetRawStats` Metodo API per testare nuove funzionalità. I dati restituiti da `GetRawStats` non è documentato, cambia frequentemente e non se ne garantisce l'accuratezza. Non dovresti usare `GetRawStats` per la raccolta di dati sulle prestazioni o qualsiasi altra integrazione di gestione con un cluster di storage che esegue il software Element.

Utilizzare i seguenti metodi API supportati per recuperare informazioni statistiche:

- [Ottieni statistiche sul volume](#)
- [Ottieni statistiche cluster](#)
- [Ottieni statistiche nodo](#)
- [Ottieni statistiche di guida](#)

Nuovo dalla versione

9,6

ElencoRisultatiAsincroni

Puoi usare `ListAsyncResults` per elencare i risultati di tutti i metodi asincroni attualmente in esecuzione e completati sul sistema. Interrogazione dei risultati asincroni con `ListAsyncResults` non causa la scadenza degli `asyncHandles` completati; puoi usare `GetAsyncResult` per interrogare uno qualsiasi degli `asyncHandle` restituiti da `ListAsyncResults`.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
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 coinvolgono il sistema nell'aggiunta di un'unità al cluster. • BulkVolume: operazioni di copia tra volumi, ad esempio backup o ripristini. • Clonazione: operazioni di clonazione del volume. • DriveRemoval: operazioni che coinvolgono il sistema che copia i dati da un'unità in preparazione alla sua rimozione dal cluster. • RtfiPendingNode: operazioni che coinvolgono il sistema che installa software compatibile su un nodo prima di aggiungerlo al cluster.	matrice di stringhe	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
asyncHandles	Un array di risultati di metodi asincroni serializzati.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListAsyncResults",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      },
      ...
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Ottieni risultato asincrono](#)

Metodi API dell'account

Aggiungi account

Puoi usare `AddAccount` per aggiungere un nuovo account al sistema. È possibile utilizzare questo metodo anche per creare nuovi volumi nel nuovo account man mano che l'account viene creato. Le impostazioni del protocollo 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	Necessario
<code>attributes</code>	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
<code>enableChap</code>	Specifica se le credenziali dell'account CHAP possono essere utilizzate da un iniziatore per accedere ai volumi.	booleano	VERO	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
initiatorSecret	Il segreto CHAP da utilizzare per l'iniziatore. Questo segreto deve essere lungo dai 12 ai 16 caratteri e deve essere impenetrabile. Il segreto CHAP dell'iniziatore deve essere univoco e non può essere uguale al segreto CHAP di destinazione. Se non specificato, viene creato un segreto casuale.	corda	Nessuno	NO
targetSecret	Il segreto CHAP da utilizzare per la destinazione (autenticazione CHAP reciproca). Questo segreto deve essere lungo dai 12 ai 16 caratteri e deve essere impenetrabile. Il segreto CHAP di destinazione deve essere univoco e non può essere uguale al segreto CHAP di avvio. Se non specificato, viene creato un segreto casuale.	corda	Nessuno	NO
username	Il nome utente univoco per questo account. (Deve contenere da 1 a 64 caratteri).	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

account	Un oggetto contenente informazioni sull'account appena creato.	account
ID account	ID dell'oggetto account appena creato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "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
  }
}
```

Nuovo dalla versione

9,6

OttieniAccountPerID

Puoi usare `GetAccountByID` per ottenere dettagli su un account specifico, in base al suo `accountID`.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID account	ID dell'account per il quale si desidera ottenere informazioni.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
account	Dettagli dell'account.	account

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetAccountByID",
  "params": {
    "accountID" : 3
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "account": {
    "attributes": {},
    "username": "account3",
    "targetSecret": "targetsecret",
    "volumes": [],
    "enableChap": true,
    "status": "active",
    "accountID": 3,
    "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
    "initiatorSecret": "initiatorsecret"
  }
}
```

Nuovo dalla versione

9,6

OttieniAccountPerNome

Puoi usare `GetAccountByName` per ottenere dettagli su un account specifico, in base al suo nome utente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome utente	Nome utente per l'account.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
account	Dettagli dell'account.	account

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetAccountByName",
  "params": {
    "username" : "jimmyd"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "account": {
    "attributes": {},
    "username": "jimmyd",
    "targetSecret": "targetsecret",
    "volumes": [],
    "enableChap": true,
    "status": "active",
    "accountID": 1,
    "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
    "initiatorSecret": "initiatorsecret"
  }
}
```

Nuovo dalla versione

9,6

Ottieni efficienza dell'account

Puoi usare `GetAccountEfficiency` per ottenere statistiche di efficienza su un account di volume. Questo metodo restituisce informazioni sull'efficienza solo per l'account fornito come parametro.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID account	Specifica l'account del volume per il quale vengono restituite le statistiche sull'efficienza.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
compressione	Quantità di spazio risparmiata dalla compressione dei dati per tutti i volumi nell'account. Espresso come rapporto in cui il valore "1" indica che i dati sono stati memorizzati senza compressione.	galleggiante
deduplicazione	Quantità di spazio risparmiata evitando di duplicare i dati per tutti i volumi dell'account. Espresso come rapporto.	galleggiante
volumi mancanti	I volumi che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati dal fatto che il ciclo di Garbage Collection (GC) è stato eseguito meno di un'ora prima, da una perdita temporanea della connettività di rete o da servizi riavviati dopo il ciclo GC.	array di interi

Nome	Descrizione	Tipo
thinProvisioning	Rapporto tra lo spazio utilizzato e la quantità di spazio allocato per l'archiviazione dei dati. Espresso come rapporto.	galleggiante
marca temporale	L'ultima volta che i dati sull'efficienza sono stati raccolti dopo la Garbage Collection (GC), nel formato UTC+0.	Stringa di data ISO 8601

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetAccountEfficiency",
  "params": {
    "accountID": 3
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "compression": 2.020468042933262,
    "deduplication": 2.042488619119879,
    "missingVolumes": [],
    "thinProvisioning": 1.010087163391013,
    "timestamp": "2014-03-10T14:06:02Z"
  }
}
```

Nuovo dalla versione

9,6

ElencoAccount

Puoi usare `ListAccounts` per ottenere l'elenco completo degli account tenant di

archiviazione, con supporto di paging opzionale. Gli account degli elementi consentono l'accesso ai volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
includeStorageContainers	Per impostazione predefinita, i contenitori di archiviazione dei volumi virtuali sono inclusi nella risposta. Per escludere i contenitori di archiviazione, impostare su false.	booleano	VERO	NO
IDAccountInizio	AccountID iniziale da restituire. Se non esiste alcun account con questo accountID, come inizio dell'elenco viene utilizzato l'account successivo in ordine di accountID. Per scorrere l'elenco, passare l'accountID dell'ultimo account nella risposta precedente + 1.	intero	Nessuno	NO
limite	Numero massimo di oggetti account da restituire.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
conti	L'elenco degli account.	accountvettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListAccounts",
  "params": {
    "startAccountID" : 0,
    "limit" : 1000
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Modifica Account

Puoi usare il `ModifyAccount` metodo per modificare un account esistente.

Quando si blocca un account, tutte le connessioni esistenti da quell'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 riconessioni successive. Per cancellare gli attributi di un account, specificare {} per il parametro `attributes`.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID account	AccountID per l'account da modificare.	intero	Nessuno	Sì
attributi	Elenco di 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
iniziatoreSegreto	Il segreto CHAP da utilizzare per l'iniziatore. Questo segreto deve essere lungo dai 12 ai 16 caratteri e deve essere impenetrabile. Il segreto CHAP dell'iniziatore deve essere univoco e non può essere uguale al segreto CHAP di destinazione.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
stato	Stato dell'account. Valori possibili: • attivo: l'account è attivo e le connessioni sono consentite. • bloccato: l'account è bloccato e le connessioni sono rifiutate.	corda	Nessuno	NO
targetSecret	Il segreto CHAP da utilizzare per la destinazione (autenticazione CHAP reciproca). Questo segreto deve essere lungo dai 12 ai 16 caratteri e deve essere impenetrabile. Il segreto CHAP di destinazione deve essere univoco e non può essere uguale al segreto CHAP di avvio.	corda	Nessuno	NO
nome utente	Utilizzato per modificare il nome utente associato all'account. (Deve contenere da 1 a 64 caratteri).	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
account	Un oggetto contenente informazioni sull'account modificato.	account

Richiedi esempio

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 al seguente esempio:

```
{
  "account": {
    "storageContainerID": "abcdef01-1234-5678-90ab-cdef01234567",
    "username": "user1",
    "accountID": 1,
    "volumes": [
    ],
    "enableChap": true,
    "initiatorSecret": "txz123456q890",
    "attributes": {
    },
    "status": "active",
    "targetSecret": "rxel23b567890"
  }
}
```

Nuovo dalla versione

9,6

RimuoviAccount

Puoi usare il `RemoveAccount` metodo per rimuovere un account esistente. È necessario eliminare e ripulire tutti i volumi associati all'account utilizzando `DeleteVolume` prima di poter rimuovere l'account. Se i volumi sull'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	Necessario
ID account	L'ID dell'account da rimuovere.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

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 al seguente esempio:

```
{
  "id" : 1,
  "result" : { }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Elimina volume](#)

Metodi API dell'amministratore

AggiungiClusterAdmin

Puoi usare il `AddClusterAdmin` metodo per aggiungere un nuovo account

amministratore del cluster. Un amministratore del cluster può gestire il cluster tramite l'API e gli strumenti di gestione. Gli amministratori del cluster sono completamente separati e non correlati agli account tenant standard.

Ogni amministratore del cluster può essere limitato a un sottoinsieme dell'API. Dovresti utilizzare più account di amministrazione del cluster per utenti e applicazioni diversi. Come buona pratica, è consigliabile concedere a ciascun amministratore del cluster le autorizzazioni minime necessarie; ciò riduce il potenziale impatto della compromissione delle credenziali.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accesso	Controlla quali metodi può utilizzare l'amministratore del cluster.	matrice di stringhe	Nessuno	Sì
accettareEula	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 fallisce.	booleano	Nessuno	Sì
attributi	Elenco di coppie nome/valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
password	Password utilizzata per autenticare l'amministratore di questo cluster.	corda	Nessuno	Sì
nome utente	Nome utente univoco per questo amministratore del cluster. Deve avere una lunghezza compresa tra 1 e 1024 caratteri.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ID amministratore cluster	ClusterAdminID per l'amministratore del cluster appena creato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result" : {
    "clusterAdminID": 2
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Controllo degli accessi](#)

OttieniCurrentClusterAdmin

Puoi usare il `GetCurrentClusterAdmin` metodo per restituire informazioni per l'amministratore primario del cluster corrente. L'amministratore del cluster primario è stato creato al momento della creazione del cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ClusterAdmin	Informazioni sull'amministratore del cluster.	ClusterAdmin

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetCurrentClusterAdmin",
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "clusterAdmin": {
      "access": [
        "administrator"
      ],
      "attributes": null,
      "authMethod": "Cluster"
      "clusterAdminID": 1,
      "username": "admin"
    }
  }
}
```

Nuovo dalla versione

10,0

OttieniLoginBanner

Puoi usare il `GetLoginBanner` metodo per ottenere il banner dei Termini di utilizzo attualmente attivo che gli utenti vedono quando accedono all'interfaccia web di Element.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
bandiera	Il testo attuale del banner Termini di utilizzo. Questo valore può contenere testo anche quando il banner è disattivato.	corda
abilitato	Lo stato del banner Termini di utilizzo. Valori possibili: • vero: il banner Termini di utilizzo viene visualizzato al momento dell'accesso all'interfaccia web. • false: il banner dei Termini di utilizzo non viene visualizzato al momento dell'accesso all'interfaccia web.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 3411,
  "method": "GetLoginBanner",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 3411,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": false
    }
  }
}
```

Nuovo dalla versione

10,0

ListClusterAdmins

Puoi usare il `ListClusterAdmins` metodo per restituire l'elenco di tutti gli amministratori del cluster.

Possono esserci più account di amministratore del cluster con diversi livelli di autorizzazione. Nel sistema può esserci un solo amministratore del cluster primario. L'amministratore primario 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 sul cluster.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
mostraNascosto	Mostra gli utenti amministratori del cluster nascosti, come l'amministratore SNMP.	booleano	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
amministratori del cluster	Informazioni su tutti gli amministratori di cluster e LDAP esistenti per un cluster.	ClusterAdmin vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListClusterAdmins",
  "params": {},
  "showHidden": true
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ModificaClusterAdmin

Puoi usare il `ModifyClusterAdmin` metodo per modificare le impostazioni per un amministratore di cluster, un amministratore di cluster LDAP o un amministratore di cluster di provider di identità (IdP) 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	Necessario
accesso	Controlla quali metodi può utilizzare questo amministratore del cluster.	matrice di stringhe	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
ID amministratore cluster	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 l'amministratore di questo cluster. Questo parametro non si applica a un amministratore di cluster LDAP o IdP.	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyClusterAdmin",
  "params": {
    "clusterAdminID" : 2,
    "password"      : "7925Brc429a"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1
  "result" : { }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Controllo degli accessi](#)

RimuoviClusterAdmin

Puoi usare il `RemoveClusterAdmin` metodo per rimuovere un amministratore di cluster, un amministratore di cluster LDAP o un amministratore di cluster di un provider di identità (IdP) di terze parti. Non è possibile rimuovere l'account Cluster Admin "admin".

Parametro

Quando viene rimosso un amministratore del cluster IdP che ha sessioni autenticate associate a un IdP di un provider di identità di terze parti, tali sessioni verranno disconnesse o potrebbero subire una perdita di diritti di accesso nella sessione corrente. La perdita dei diritti di accesso dipenderà dal fatto che l'amministratore del cluster IdP rimosso corrisponda a uno dei numerosi amministratori del cluster IdP degli attributi SAML di un determinato utente. Il set rimanente di amministratori del cluster IdP corrispondenti determina un set ridotto di diritti di accesso aggregati. Gli altri tipi di utenti amministratori del cluster vengono disconnessi quando vengono rimossi i rispettivi amministratori del cluster.

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID amministratore cluster	ClusterAdminID per l'amministratore del cluster da rimuovere.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveClusterAdmin",
  "params": {
    "clusterAdminID" : 2
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1
  "result" : { }
}
```

Nuovo dalla versione

9,6

ImpostaLoginBanner

Puoi usare il `SetLoginBanner` Metodo per configurare il banner dei Termini di utilizzo che gli utenti vedono quando accedono all'interfaccia web di Element.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
bandiera	Il testo desiderato del banner dei Termini di utilizzo. La lunghezza massima consentita è di 4.096 caratteri.	corda	Nessuno	NO
abilitato	Lo stato del banner Termini di utilizzo. Valori possibili: • <code>true</code>: Il banner dei Termini di utilizzo viene visualizzato al momento dell'accesso all'interfaccia web. • <code>false</code>: Il banner dei Termini di utilizzo non viene visualizzato al momento dell'accesso all'interfaccia web.	booleano	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
bandiera	Il testo attuale del banner Termini di utilizzo. Questo valore può contenere testo anche quando il banner è disattivato.	corda

Nome	Descrizione	Tipo
abilitato	Lo stato del banner Termini di utilizzo. Valori possibili: • vero: il banner Termini di utilizzo viene visualizzato al momento dell'accesso all'interfaccia web. • false: il banner dei Termini di utilizzo non viene visualizzato al momento dell'accesso all'interfaccia web.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 3920,
  "method": "SetLoginBanner",
  "params": {
    "banner": "Welcome to NetApp!",
    "enabled": true
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 3920,
  "result": {
    "loginBanner": {
      "banner": "Welcome to NetApp!",
      "enabled": true
    }
  }
}
```

Nuovo dalla versione

10,0

Metodi API del cluster

Aggiungi nodi

Puoi usare il `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" nel cluster. I cluster di archiviazione che eseguono il software Element creano automaticamente un'immagine di un nodo nella versione presente nel 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 è lo stesso dell'aggiunta di nodi di archiviazione Element iSCSI a un cluster. I nodi Fibre Channel sono registrati nel sistema con un `NodeID`. Quando diventano accessibili, vengono messi nello stato "nodo in sospeso". Il `ListAllNodes` Il metodo restituirà 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 necessita di un numero sufficiente di indirizzi IP di archiviazione virtuale per allocare un IP virtuale al nuovo nodo. Se non sono disponibili indirizzi IP virtuali per il nuovo nodo, il `AddNode` l'operazione fallisce. Utilizzare il `ModifyVirtualNetwork` metodo per aggiungere più indirizzi IP di archiviazione alla tua rete virtuale.

Una volta aggiunto un nodo, tutte le unità sul nodo vengono rese disponibili e puoi aggiungerle utilizzando `AddDrives` metodo per aumentare la capacità di archiviazione del cluster.



Dopo aver aggiunto un nuovo nodo, potrebbero essere necessari alcuni secondi prima che questo si avvii e registri le sue unità come disponibili.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
installazione automatica	Se è vero, verrà eseguito un ripristino dell'immagine di fabbrica (RTFI) sul nodo al momento dell'aggiunta. Il comportamento predefinito è eseguire RTFI. Se il <code>cEnableAutoInstall</code> Se la costante del cluster è falsa, ha la priorità su questo parametro. Se è in corso un aggiornamento, il processo RTFI non verrà eseguito indipendentemente dal valore di questo parametro.	booleano	Nessuno	NO
nodi in sospeso	NodeID in sospeso per i nodi da aggiungere. È possibile elencare tutti i nodi in sospeso utilizzando il metodo <code>ListPendingNodes</code> .	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
installazione automatica	Se i nodi aggiunti vengono restituiti o meno all'immagine di fabbrica.	booleano

nodi	Un array di oggetti che mappano il precedente "pendingNodeID" al "nodeID". Quando si aggiunge un nodo in sospeso che esegue una versione software incompatibile, questa matrice include un valore asyncHandle che è possibile utilizzare con il metodo GetAsyncResult per interrogare lo stato del processo di creazione automatica delle immagini.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "AddNodes",
  "params": {
    "autoInstall" : true,
    "pendingNodes" : [1]
  },
  "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Aggiungi unità](#)
- [Ottieni risultato asincrono](#)
- [Elenca tutti i nodi](#)
- [Modificare la rete virtuale](#)

ClearClusterFaults

Puoi usare il `ClearClusterFaults` metodo per cancellare le informazioni sui guasti attuali e su quelli rilevati in precedenza. È possibile eliminare sia i guasti risolti che quelli non risolti.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tipi di errore	Determina i tipi di guasti da eliminare. Valori possibili: • attuale: Difetti attualmente rilevati e non ancora risolti. • risolti: guasti precedentement e rilevati e risolti. • tutti: sia guasti attuali che risolti. Lo stato di errore può essere determinato dal campo "resolved" dell'oggetto errore.	corda	risolto	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ClearClusterFaults",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

CreaPreferenzaInterfacciaCluster

IL `CreateClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di archiviazione che eseguono il software Element di creare e archiviare informazioni arbitrarie sul cluster di archiviazione. Questo metodo è per uso interno.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome della preferenza dell'interfaccia del cluster.	corda	Nessuno	Sì
valore	Valore della preferenza dell'interfaccia del cluster.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
    "method": "CreateClusterInterfacePreference",
    "params": {
        "name": "prefname",
        "value": "testvalue"
    },
    "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
    "id": 1,
    "result": {}
}
```

Nuovo dalla versione

11,0

DeleteClusterInterfacePreference

IL `DeleteClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di archiviazione 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	Necessario
nome	Nome della preferenza dell'interfaccia del cluster da eliminare.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteClusterInterfacePreference",
  "params": {
    "name": "prefname"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

11,0

DisabilitaFunzionalità

Puoi usare il `DisableFeature` metodo per disabilitare il `VolumeLoadBalanceOnActualIOPS` caratteristica. `VolumeLoadBalanceOnActualIOPS` è disabilitato per impostazione predefinita.

Se si tenta di disattivare un'altra funzionalità, ad esempio VVols, viene visualizzato il seguente messaggio di errore:



```
{"error":{"code":500,"message":"VolumeLoadBalanceOnActualIOPS is
the only feature that can be
disabled","name":"xAPINotPermitted"},"id":null}
```

Parametro

Questo metodo ha il seguente parametro di input.

Nome	Descrizione	Tipo	Valore predefinito	Necessario
caratteristica	Disattivare una funzionalità del cluster. Valore possibile: VolumeLoadBalanceOnActualIOPS: Disabilita il bilanciamento delle sezioni sugli IOPS effettivi anziché sugli IOPS minimi.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableFeature",
  "params": {
    "feature" : "VolumeLoadBalanceOnActualIOPS"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

12,8

Abilita funzionalità

Puoi usare il `EnableFeature` metodo per abilitare le funzionalità del cluster, come VVols, che sono disabilite per impostazione predefinita.

Parametro

Questo metodo ha il seguente parametro di input.



Per i sistemi che eseguono Element Software 11.x, l'abilitazione dei volumi virtuali prima o dopo l'impostazione del monitoraggio del dominio di protezione fa sì che la funzionalità dei domini di protezione del cluster funzioni solo a livello di nodo.

Nome	Descrizione	Tipo	Valore predefinito	Necessario
caratteristica	Abilita una funzionalità cluster. Valori possibili: • <code>fips</code>: Abilita la crittografia certificata FIPS 140-2 per le comunicazioni HTTPS. • <code>FipsDrives</code>: Abilita il supporto unità FIPS 140-2 per il cluster di archiviazione. • <code>SnapMirror</code>: Abilita la funzionalità del cluster di replica SnapMirror . • <code>VolumeLoadBalanceOnActualIOPS</code>: Abilita il bilanciamento delle sezioni sugli IOPS effettivi anziché sugli IOPS minimi. Disponibile a partire da Element 12.8. • <code>vvols</code>: Abilita la funzionalità cluster VVols del software Element.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableFeature",
  "params": {
    "feature" : "vvols"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Ottieni capacità cluster

Puoi usare il `GetClusterCapacity` per restituire misurazioni di capacità di alto livello per un intero cluster di storage. Questo metodo restituisce campi che è possibile utilizzare per calcolare i tassi di efficienza mostrati nell'interfaccia utente Web di Element. È possibile utilizzare i calcoli dell'efficienza negli script per restituire i tassi di efficienza per thin provisioning, deduplicazione, compressione ed efficienza complessiva.

Calcoli di efficienza

Utilizzare le seguenti equazioni per calcolare il thin provisioning, la deduplicazione e la compressione. Queste equazioni si applicano all'elemento 8.2 e successivi.

- $\text{thinProvisioningFactor} = (\text{nonZeroBlocks} + \text{zeroBlocks}) / \text{nonZeroBlocks}$
- $\text{deDuplicationFactor} = (\text{nonZeroBlocks} + \text{snapshotNonZeroBlocks}) / \text{uniqueBlocks}$
- $\text{compressionFactor} = (\text{uniqueBlocks} * 4096) / (\text{uniqueBlocksUsedSpace} * 0,93)$

Calcolo del tasso di efficienza complessiva

Utilizzare la seguente equazione per calcolare l'efficienza complessiva del cluster utilizzando i risultati dei calcoli di thin provisioning, deduplicazione e efficienza di compressione.

- $\text{efficiencyFactor} = \text{thinProvisioningFactor} * \text{deDuplicationFactor} * \text{compressionFactor}$

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
capacità del cluster	Misurazioni della capacità del cluster di storage.	capacità del cluster

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterCapacity",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    }
  }
}
```

Nuovo dalla versione

9,6

Ottieni soglia completa del cluster

Puoi usare il `GetClusterFullThreshold` metodo per visualizzare le fasi impostate per i livelli di riempimento del cluster. Questo metodo restituisce tutte le metriche di pienezza per il cluster.



Quando un cluster raggiunge la fase di errore di riempimento del cluster di blocchi, gli IOPS massimi su tutti i volumi vengono ridotti linearmente agli IOPS minimi del volume quando il cluster si avvicina alla fase critica. Ciò aiuta a impedire che il cluster raggiunga la fase critica di riempimento del cluster di blocchi.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
bloccoPienezza	Livello corrente calcolato di riempimento dei blocchi 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 dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato Avviso 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). • stage4Critical: il sistema non è in grado di fornire una protezione ridondante dei dati in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato Errore nell'interfaccia utente dell'elemento. • stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture sono sospese. Corrisponde allo stato Critico nell'interfaccia utente dell'elemento.	corda
pienezza	Riflette il livello più alto di pienezza tra "blockFullness" e "metadatiFullness".	corda

Nome	Descrizione	Tipo
maxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio dei metadati può essere sovradimensionato rispetto alla quantità di spazio disponibile. Ad esempio, se ci fosse abbastanza spazio per i metadati per archiviare 100 TiB di volumi e questo numero fosse impostato su 5, potrebbero essere creati volumi per un valore di 500 TiB.	intero

Nome	Descrizione	Tipo
MetadataFullness	Livello attuale calcolato di completezza 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 dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato Avviso 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). • stage4Critical: il sistema non è in grado di fornire una protezione ridondante dei dati in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato Errore nell'interfaccia utente dell'elemento. • stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture sono sospese. Corrisponde allo stato Critico nell'interfaccia utente dell'elemento.	corda
sliceReserveUsedThresholdPct	Condizione di errore. Se l'utilizzo della slice riservata è maggiore di questo valore, viene attivato un avviso di sistema.	intero

Nome	Descrizione	Tipo
stage2AwareThreshold	Condizione di consapevolezza. Valore impostato per il livello di soglia del cluster di fase 2.	intero
stage2BlockThresholdBytes	Numero di byte utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di fase 2.	intero
stage2MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di pienezza di fase 2.	
stage3BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 3.	intero
stage3BlockThresholdPercent	Il valore percentuale impostato per la fase 3. Raggiunto questo livello di riempimento, nel registro degli avvisi viene visualizzato un avviso.	intero
stage3LowThreshold	Condizione di errore. Soglia alla quale viene creato un avviso di sistema a causa della scarsa capacità di un cluster.	intero
stage3MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di pienezza di fase 3.	intero
stage3MetadataThresholdPercent	Valore percentuale impostato per la fase 3 di completezza dei metadati. Raggiunto questo valore percentuale, verrà pubblicato un avviso nel registro degli avvisi.	intero
stage4BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 4.	intero

Nome	Descrizione	Tipo
stage4CriticalThreshold	Condizione di errore. Soglia alla quale viene creato un avviso di sistema per segnalare una capacità criticamente bassa su un cluster.	intero
stage4MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di pienezza di fase 4.	intero
stage5BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 5.	intero
stage5MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di pienezza di fase 5.	intero
sommaTotaleClusterBytes	La capacità fisica del cluster, misurata in byte.	intero
somma totale dei metadati del cluster byte	Quantità totale di spazio che può essere utilizzata per archiviare i metadati.	intero
sommaByteClusterUsati	Numero di byte di archiviazione utilizzati nel cluster.	intero
sommaMetadatiUtilizzatiClusterBytes	Quantità di spazio utilizzata sulle unità di volume per archiviare i metadati.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "GetClusterFullThreshold",
  "params" : {},
  "id" : 1
}
```


Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Modificasoglia completa del cluster](#)

OttieniClusterHardwareInfo

Puoi usare il `GetClusterHardwareInfo` Metodo per recuperare lo stato hardware e le informazioni per tutti i nodi Fibre Channel, nodi iSCSI e unità nel cluster. In genere, ciò include produttori, fornitori, versioni e altre informazioni di identificazione dell'hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tipo	Includere nella risposta solo uno dei seguenti tipi di informazioni hardware. Valori possibili: • unità: Elenca solo le informazioni sull'unità nella risposta. • nodi: elenca solo le informazioni sui nodi nella risposta. • tutto: include nella risposta sia le informazioni sull'unità che quelle sul nodo. Se questo parametro viene omissso, si presume che il tipo sia all.	corda	Tutto	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
clusterHardwareInfo	Informazioni hardware per tutti i nodi e le unità nel cluster. Ogni oggetto in questo output è etichettato con il nodeID del nodo specificato.	Informazioni hardware

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterHardwareInfo",
  "params": {
    "type": "all"
  },
  "id": 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniClusterHardwareInfo](#)

Ottieni informazioni sul cluster

Puoi usare il `GetClusterInfo` metodo per restituire informazioni di configurazione sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
clusterInfo	Informazioni sul cluster.	clusterInfo

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": null,
  "result": {
    "clusterInfo": {
      "attributes": {},
      "defaultProtectionScheme": "doubleHelix",
      "enabledProtectionSchemes": [
        "doubleHelix"
      ],
      "encryptionAtRestState": "disabled",
      "ensemble": [
        "10.10.10.32",
        "10.10.10.33",
        "10.10.10.34",
        "10.10.10.35",
        "10.10.10.36"
      ],
      "mvip": "10.10.11.225",
      "mvipInterface": "Bond1G",
      "mvipNodeID": 1,
      "mvipVlanTag": "0",
      "name": "ClusterName",
      "repCount": 2,
      "softwareEncryptionAtRestState": "disabled",
      "supportedProtectionSchemes": [
        "doubleHelix"
      ],
      "svip": "10.10.10.111",
      "svipInterface": "Bond10G",
      "svipNodeID": 1,
      "svipVlanTag": "0",
      "uniqueID": "ahf7",
      "uuid": "bcfd04b6-9151-4b3a-a6fa-bca22dd145cd",
      "volumeLoadBalanceOnActualIopsState": "enabled"
    }
  }
}
```

Nuovo dalla versione

9,6

OttieniClusterInterfacePreference

IL `GetClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di archiviazione che eseguono il software Element di ottenere informazioni su una preferenza di interfaccia del cluster esistente. Questo metodo è per uso interno.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome della preferenza dell'interfaccia del cluster.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
preferenza	Nome e valore della preferenza dell'interfaccia del cluster richiesta.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterInterfacePreference",
  "params": {
    "name": "prefname"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "preference": {
      "name": "prefname",
      "value": "testvalue"
    }
  }
}
```

Nuovo dalla versione

11,0

OttieniClusterMasterNodeID

Puoi usare il `GetClusterMasterNodeID` metodo per recuperare l'ID del nodo che esegue attività di amministrazione a livello di cluster e contiene l'indirizzo IP virtuale di archiviazione (SVIP) e l'indirizzo IP virtuale di gestione (MVIP).

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ID nodo	ID del nodo master.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterMasterNodeID",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1
  "result": {
    "nodeID": 1
  }
}
```

Nuovo dalla versione

9,6

Ottieni statistiche cluster

Puoi usare il `GetClusterStats` metodo per recuperare misurazioni di attività di alto livello per il cluster. I valori restituiti sono cumulativi a partire dalla creazione del cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
clusterStats	Informazioni sull'attività del cluster.	clusterStats

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterStats",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
    }
  }
}

```

Nuovo dalla versione

9,6

Ottieni informazioni sulla versione del cluster

Puoi usare il `GetClusterVersionInfo` metodo per recuperare informazioni sulla versione del software Element in esecuzione su ciascun nodo del cluster. Questo metodo restituisce anche informazioni sui nodi che sono attualmente in fase di aggiornamento del software.

Membri dell'oggetto informazioni sulla versione del cluster

Questo metodo ha i seguenti membri oggetto:

Nome	Descrizione	Tipo
ID nodo	ID del nodo.	intero
nodeInternalRevision	Versione software interna del nodo.	corda
nodeVersion	Versione software del nodo.	corda

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
clusterAPIVersion	La versione API corrente sul cluster.	corda
clusterVersion	Versione del software Element attualmente in esecuzione sul cluster.	corda
clusterVersionInfo	Elenco dei nodi nel cluster con informazioni sulla versione per ciascun nodo.	Matrice di oggetti JSON
pendingClusterVersion	Se presente, questa è la versione a cui il software del cluster è attualmente in fase di aggiornamento o ripristino.	corda

Nome	Descrizione	Tipo
softwareVersionInfo	Lo stato di un aggiornamento. Membri dell'oggetto: • versione corrente: La versione corrente del software su un nodo. • nodeID: ID del nodo che viene aggiornato da <code>currentVersion</code> a <code>pendingVersion</code>. Questo campo è 0 (zero) se non è in corso alcun aggiornamento. • packageName: Nome del pacchetto software che si sta installando. • pendingVersion: la versione del software che si sta installando. • startTime: data e ora di avvio dell'installazione, nel formato UTC+0.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterVersionInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": ""
    }
  }
}

```

Nuovo dalla versione

9,6

OttieniStatoFunzionalità

Puoi usare il `GetFeatureStatus` metodo per recuperare lo stato di una funzionalità del cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
caratteristica	Lo stato di una funzionalità del cluster. Se non viene fornito alcun valore, il sistema restituisce lo stato di tutte le funzionalità. Valori possibili: • <code>Vvols</code>: Recupera lo stato della funzionalità del cluster VVols. • <code>SnapMirror</code>: Recupera lo stato della funzionalità del cluster di replica SnapMirror . • <code>Fips</code>: Recupera lo stato della crittografia FIPS 140-2 per la funzionalità di comunicazione HTTPS. • <code>FipsDrives</code>: Recupera lo stato della funzionalità di crittografia dell'unità FIPS 140-2. • <code>VolumeLoadBalanceOnActualIOPS</code>: Recupera lo stato del bilanciamento delle sezioni in base agli IOPS effettivi anziché alla funzionalità Min IOPS. Disponibile a partire da Element 12.8.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
caratteristiche	Una matrice di oggetti feature che indicano il nome della feature e il suo stato. Membri dell'oggetto: • feature: (stringa) Il nome della feature. • abilitato: (booleano) Indica se la funzionalità è abilitata o meno.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetFeatureStatus",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id": 1,
  "result": {
    "features": [
      {
        "enabled": true,
        "feature": "Vvols"
      },
      {
        "enabled": true,
        "feature": "SnapMirror"
      },
      {
        "enabled": true,
        "feature": "Fips"
      },
      {
        "enabled": true,
        "feature": "FipsDrives"
      },
      {
        "enabled": true,
        "feature": "VolumeLoadBalanceOnActualIOPS"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Ottieni informazioni sulla sessione di accesso

Puoi usare il `GetLoginSessionInfo` metodo per restituire il periodo di tempo in cui una sessione di autenticazione di accesso è valida sia per le shell di accesso che per l'interfaccia utente terminale.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
loginSessionInfo	Un oggetto contenente il periodo di scadenza dell'autenticazione. Possibili oggetti restituiti: tempo scaduto: Tempo, in minuti, dopo il quale la sessione scadrà e 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 immesso il timeout.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetLoginSessionInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result" : {
    "loginSessionInfo" : {
      "timeout" : "30:00"
    }
  }
}
```

Nuovo dalla versione

9,6

Ottieni informazioni hardware del nodo

Puoi usare il `GetNodeHardwareInfo` metodo per restituire tutte le informazioni hardware e lo stato del nodo specificato. In genere, ciò include produttori, fornitori, versioni e altre informazioni di identificazione dell'hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID nodo	ID del nodo per il quale vengono richieste informazioni hardware. Se viene specificato un nodo Fibre Channel, vengono restituite informazioni su un nodo Fibre Channel.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodeHardwareInfo	Informazioni hardware per il nodeID specificato. Ogni oggetto in questo output è etichettato con il nodeID del nodo specificato.	Informazioni hardware

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeHardwareInfo",
  "params": {
    "nodeID": 1
  },
  "id" : 1
}
```


Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[GetNodeHardwareInfo \(output per i nodi Fibre Channel\)](#)

[GetNodeHardwareInfo \(output per iSCSI\)](#)

Ottieni statistiche nodo

Puoi usare il `GetNodeStats` metodo per recuperare le misurazioni dell'attività di alto livello per un singolo nodo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID nodo	Specifica l'ID del nodo per il quale verranno restituite le statistiche.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodeStats	Informazioni sull'attività del nodo.	nodeStats

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeStats",
  "params": {
    "nodeID": 5
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "nodeStats": {
      "cBytesIn": 1579657943924,
      "cBytesOut": 1683056745816,
      "count": 119529,
      "cpu": 0,
      "cpuTotal": 56289,
      "mBytesIn": 475476878,
      "mBytesOut": 269270423,
      "networkUtilizationCluster": 0,
      "networkUtilizationStorage": 0,
      "nodeHeat": {
        "primaryTotalHeat": 0.00098,
        "recentPrimaryTotalHeat": 0.00099,
        "recentTotalHeat": 0.00099,
        "totalHeat": 0.00098
      },
      "readLatencyUSecTotal": 10125300382,
      "readOps": 15640075,
      "sBytesIn": 1579657943924,
      "sBytesOut": 1683056745816,
      "ssLoadHistogram": {
        "Bucket0": 4873,
        "Bucket1To19": 6301620,
        "Bucket20To39": 396452,
        "Bucket40To59": 142,
        "Bucket60To79": 0,
        "Bucket80To100": 0
      },
      "timestamp": "2024-03-04T20:13:22.105428Z",
      "usedMemory": 106335510528,
      "writeLatencyUSecTotal": 7314512535,
      "writeOps": 59154830
    }
  }
}
```

Nuovo dalla versione

9,6

ListActiveNodes

Puoi usare il `ListActiveNodes` metodo per restituire l'elenco dei nodi attualmente attivi presenti nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodi	Elenco dei nodi attivi nel cluster.	nodo vetto

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListActiveNodes",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[ListActiveNodes](#)

Elenca tutti i nodi

Puoi usare il `ListAllNodes` metodo per elencare i nodi attivi e in sospeso nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
nodi	Elenco di oggetti che descrivono i nodi attivi nel cluster.	nodo
pendingActiveNodes	Elenco di oggetti che descrivono i nodi attivi in sospeso per il cluster.	pendingActiveNode vettore
nodi in sospeso	Elenco di oggetti che descrivono i nodi in sospeso per il cluster.	nodo in sospeso vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListAllNodes",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": []
  }
}

```

Nuovo dalla versione

9,6

ListClusterFaults

Puoi usare il `ListClusterFaults` metodo per elencare le informazioni su eventuali errori rilevati sul cluster. Con questo metodo è possibile elencare sia i guasti attuali sia quelli risolti. Il sistema memorizza nella cache gli errori ogni 30 secondi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
migliori pratiche	Includere guasti causati da una configurazione di sistema non ottimale. Valori possibili: • VERO • falso	booleano	Nessuno	NO
tipi di errore	Determina i tipi di errori restituiti. Valori possibili: • corrente: elenca i guasti attivi e non risolti. • risolto: elenca i guasti precedentemente rilevati e risolti. • tutti: elenca sia i guasti attuali che quelli risolti. È possibile visualizzare lo stato dell'errore nel membro "resolved" dell'oggetto errore.	corda	Tutto	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
difetti	Un oggetto che descrive gli errori del cluster richiesti.	colpa

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListClusterFaults",
  "params": {
    "faultTypes": "current",
    "bestPractices": true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id": 1,
  "result": {
    "faults": [
      {
        "blocksUpgrade": false,
        "clusterFaultID": 3,
        "code": "driveAvailable",
        "data": null,
        "date": "2024-04-03T22:22:56.660275Z",
        "details": "Node ID 1 has 6 available drive(s).",
        "driveID": 0,
        "driveIDs": [],
        "externalSource": "",
        "networkInterface": "",
        "nodeHardwareFaultID": 0,
        "nodeID": 1,
        "resolved": true,
        "resolvedDate": "2024-04-03T22:24:54.598693Z",
        "serviceID": 0,
        "severity": "warning",
        "type": "drive"
      },
      {
        "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"
      }
    ]
  }
}

```


Nuovo dalla versione

9,6

ListClusterInterfacePreferences

IL `ListClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di archiviazione che eseguono il software Element di elencare le preferenze dell'interfaccia del cluster esistente memorizzate nel sistema. Questo metodo è per uso interno.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
preferenze	Un elenco di oggetti dell'interfaccia del cluster attualmente archiviati nel cluster di archiviazione, ciascuno contenente il nome e il valore della preferenza.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListClusterInterfacePreferences",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id": 1,
  "result": {
    "preferences": [
      {
        "name": "prefname",
        "value": "testvalue"
      }
    ]
  }
}

```

Nuovo dalla versione

11,0

ElencoEventi

Puoi usare il `ListEvents` metodo per elencare gli eventi rilevati sul cluster, ordinati dal più vecchio al più recente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID unità	Specifica che verranno restituiti solo gli eventi con questo ID unità.	intero	0	NO
endEventID	Identifica la fine di un intervallo di ID evento da restituire.	intero	(illimitato)	NO
endPublishTime	Specifica che verranno restituiti solo gli eventi pubblicati prima di questo orario.	corda	0	NO
endReportTime	Specifica che verranno restituiti solo gli eventi segnalati prima di questo orario.	corda	0	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tipoevento	Specifica il tipo di eventi da restituire. Vedere evento per possibili tipi di eventi.	corda	0	NO
maxEventi	Specifica il numero massimo di eventi da restituire.	intero	(illimitato)	NO
ID nodo	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.			
ID evento di avvio	Identifica l'inizio di una serie di eventi da restituire.	intero	0	NO
inizioPubblicazione Ora	Specifica che verranno restituiti solo gli eventi pubblicati dopo questo orario.	corda	0	NO
startReportTime	Specifica che verranno restituiti solo gli eventi segnalati dopo questo orario.	corda	0	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
eventi	Elenco degli eventi.	evento vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListEvents",
  "params": {
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
]
}
}

```

Nuovo dalla versione

9,6

ListNodeStats

Puoi usare il `ListNodeStats` Metodo per visualizzare le misurazioni dell'attività di alto livello per tutti i nodi di archiviazione in un cluster di archiviazione.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodeStats	Informazioni sull'attività del nodo di archiviazione.	nodeStats

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{  
  "method": "ListNodeStats",  
  "params": {},  
  "id" : 1  
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id": 1,
  "result": {
    "nodeStats": {
      "nodes": [
        {
          "cBytesIn": 223022159806,
          "cBytesOut": 206324217921,
          "count": 17274,
          "cpu": 0,
          "cpuTotal": 9796,
          "mBytesIn": 608219007,
          "mBytesOut": 3487659798,
          "networkUtilizationCluster": 0,
          "networkUtilizationStorage": 0,
          "nodeHeat": {
            "primaryTotalHeat": 0.00028,
            "recentPrimaryTotalHeat": 0.0,
            "recentTotalHeat": 0.00097,
            "totalHeat": 0.00138
          },
          "nodeID": 1,
          "readLatencyUSecTotal": 8964,
          "readOps": 29544,
          "sBytesIn": 223022159806,
          "sBytesOut": 206324217921,
          "ssLoadHistogram": {
            "Bucket0": 5083,
            "Bucket1To19": 5637426,
            "Bucket20To39": 19389,
            "Bucket40To59": 156,
            "Bucket60To79": 0,
            "Bucket80To100": 0
          },
          "timestamp": "2024-02-27T18:21:26.183659Z",
          "usedMemory": 104828780544,
          "writeLatencyUSecTotal": 271773335,
          "writeOps": 23898
        }
      ]
    }
  }
}

```

Nuovo dalla versione

9,6

ElencoISCSISessioni

Puoi usare il `ListISCSISessions` metodo per elencare le informazioni di connessione iSCSI per i volumi nel cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Informazioni su ciascuna sessione iSCSI.	sessione

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListISCSISessions",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "id": 1,
  "result": {
    "sessions": [
      {
        "accountID": 1,
        "accountName": "account1",
        "authentication": {
          "authMethod": "CHAP",
          "chapAlgorithm": "SHA3_256",
          "chapUsername": "iqn.1994-05.com."redhat:1cf11f3eed3",
          "direction": "two-way"
        },
        "createTime": "2022-10-03T22:02:49.121723Z",
        "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
      }
      ...
    ]
  }
}

```

Nuovo dalla versione

9,6

ElencoServizi

Puoi usare il `ListServices` Metodo per elencare le informazioni sui servizi per nodi, unità, software corrente e altri servizi in esecuzione sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
servizi	Servizi in esecuzione su unità e nodi.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListServices",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
"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"
        }
    }
]
}

```

Nuovo dalla versione

9,6

Elenco nodi in sospeso

Puoi usare il `ListPendingNodes` metodo per elencare i nodi di archiviazione in sospeso nel sistema. I nodi in sospeso sono nodi di archiviazione in esecuzione e configurati per unirsi al cluster di archiviazione, ma che non sono ancora stati aggiunti tramite il metodo API `AddNodes`.

Indirizzi di gestione IPv4 e IPv6

Notare che `ListPendingNodes` non elenca i nodi in sospeso che hanno tipi di indirizzo diversi 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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodi in sospenso	Elenco dei nodi in sospenso nel cluster.	nodo in sospenso vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListPendingNodes",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Aggiungi nodi](#)

Elenco nodi attivi in sospeso

Puoi usare il `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 riportati all'immagine di fabbrica.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
pendingActiveNodes	Elenco di oggetti che contengono informazioni dettagliate su tutti i nodi PendingActive nel sistema.	pendingActiveNode vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListPendingActiveNodes",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Modificasoglia completa del cluster

Puoi usare il `ModifyClusterFullThreshold` Metodo per modificare il livello al quale il sistema genera un evento quando il cluster di storage si avvicina a una determinata capacità di utilizzo. È possibile utilizzare l'impostazione della soglia per indicare la quantità accettabile di spazio di archiviazione a blocchi utilizzato prima che il sistema generi un avviso.

Ad esempio, se si desidera essere avvisati quando il sistema raggiunge il 3% di utilizzo dello storage a blocchi al di sotto del livello "Errore", immettere il valore "3" per il parametro `stage3BlockThresholdPercent`. Se viene raggiunto questo livello, il sistema invia un avviso al registro eventi nella Cluster Management Console.

Parametri

Questo metodo ha i seguenti parametri di input:



È necessario selezionare almeno un parametro.

Nome	Descrizione	Tipo	Valore predefinito	Necessario
maxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio dei metadati può essere sovradimensionato rispetto alla quantità di spazio disponibile. Ad esempio, se ci fosse abbastanza spazio per i metadati per archiviare 100 TiB di volumi e questo numero fosse impostato su 5, potrebbero essere creati volumi per un valore di 500 TiB.	intero	5	NO
stage2AwareThreshold	Numero di nodi di capacità rimanenti nel cluster prima che il sistema attivi una notifica di capacità.	intero	Nessuno	NO
stage3BlockThresholdPercent	Percentuale di utilizzo dello storage a blocchi al di sotto della soglia "Errore" che fa sì che il sistema attivi un avviso di "Avviso" del cluster.	intero	Nessuno	NO
stage3MetadataThresholdPercent	Percentuale di utilizzo dello spazio di archiviazione dei metadati al di sotto della soglia "Errore" che fa sì che il sistema attivi un avviso "Avviso" del cluster.	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

bloccoPienezza	Livello corrente calcolato di riempimento dei blocchi 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 dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato Avviso 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). • stage4Critical: il sistema non è in grado di fornire una protezione ridondante dei dati in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato Errore nell'interfaccia utente dell'elemento. • stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture sono sospese. Corrisponde allo stato Critico nell'interfaccia utente dell'elemento.	corda
pienezza	Riflette il livello più alto di pienezza tra "blockFullness" e "metadatiFullness".	corda

maxMetadataOverProvisionFactor	Un valore rappresentativo del numero di volte in cui lo spazio dei metadati può essere sovradimensionato rispetto alla quantità di spazio disponibile. Ad esempio, se ci fosse abbastanza spazio per i metadati per archiviare 100 TiB di volumi e questo numero fosse impostato su 5, potrebbero essere creati volumi per un valore di 500 TiB.	intero

MetadataFullness	Livello attuale calcolato di completezza 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 dati ridondante da due guasti non simultanei dei nodi. Corrisponde allo stato Avviso 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). • stage4Critical: il sistema non è in grado di fornire una protezione ridondante dei dati in caso di guasto di un singolo nodo. Non è possibile creare nuovi volumi o cloni. Corrisponde allo stato Errore nell'interfaccia utente dell'elemento. • stage5CompletelyConsumed: Completamente consumato. Il cluster è di sola lettura e le connessioni iSCSI vengono mantenute, ma tutte le scritture sono sospese. Corrisponde allo stato Critico nell'interfaccia utente dell'elemento.	corda
sliceReserveUsedThresholdPct	Condizione di errore. Viene attivato un avviso di sistema se l'utilizzo della slice riservata è maggiore del valore sliceReserveUsedThresholdPct restituito.	intero

stage2AwareThreshold	Condizione di consapevolezza. Valore impostato per il livello di soglia del cluster "Fase 2".	intero
stage2BlockThresholdBytes	Numero di byte utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di pienezza di fase 2.	intero
stage2MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di pienezza di fase 2.	
stage3BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 3.	intero
stage3BlockThresholdPercent	Il valore percentuale impostato per la fase 3. Raggiunto questo livello di riempimento, nel registro degli avvisi viene visualizzato un avviso.	intero
stage3LowThreshold	Condizione di errore. Soglia alla quale viene creato un avviso di sistema a causa della scarsa capacità di un cluster.	intero
stage3MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza del quale si verificherà una condizione di pienezza di fase 3.	
stage4BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 4.	intero
stage4CriticalThreshold	Condizione di errore. Soglia alla quale viene creato un avviso di sistema per segnalare una capacità criticamente bassa su un cluster.	intero

stage4MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di pienezza di fase 4.	
stage5BlockThresholdBytes	Numero di byte di archiviazione utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di riempimento di fase 5.	intero
stage5MetadataThresholdBytes	Numero di byte di metadati utilizzati dal cluster in corrispondenza dei quali si verificherà una condizione di pienezza di fase 5.	
sommaTotaleClusterBytes	La capacità fisica del cluster, misurata in byte.	intero
somma totale dei metadati del cluster byte	Quantità totale di spazio che può essere utilizzata per archiviare i metadati.	intero
sommaByteClusterUsati	Numero di byte di archiviazione utilizzati nel cluster.	intero
sommaMetadatiUtilizzatiClusterBytes	Quantità di spazio utilizzata sulle unità di volume per archiviare i metadati.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "ModifyClusterFullThreshold",
  "params" : {
    "stage3BlockThresholdPercent" : 3
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
  }
}

```

Nuovo dalla versione

9,6

ModificaPreferenzaInterfacciaCluster

IL `ModifyClusterInterfacePreference` Il metodo consente ai sistemi integrati con cluster di archiviazione che eseguono il software Element di modificare una preferenza di interfaccia del cluster esistente. Questo metodo è per uso interno.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome della preferenza dell'interfaccia del cluster da modificare.	corda	Nessuno	Sì

valore	Il nuovo valore della preferenza dell'interfaccia del cluster.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyClusterInterfacePreference",
  "params": {
    "name": "testname",
    "value": "newvalue"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

11,0

Rimuovi nodi

Puoi usare `RemoveNodes` per rimuovere uno o più nodi che non dovrebbero più partecipare al cluster.

Prima di rimuovere un nodo, è necessario rimuovere tutte le unità contenute nel nodo utilizzando `RemoveDrives` metodo. Non è possibile rimuovere un nodo finché il `RemoveDrives` il processo è stato completato e tutti i dati sono stati migrati dal nodo. Dopo aver rimosso un nodo, questo viene registrato come nodo in sospeso. È possibile aggiungere nuovamente il nodo o chiuderlo (chiudendo il nodo lo si rimuove dall'elenco dei nodi in sospeso).

Rimozione del nodo master del cluster

Se usi `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, effettuare 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 solo il nodo master del cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>ignoraEnsembleToleranceChange</code>	Ignora le modifiche alla tolleranza ai guasti dei nodi dell'ensemble quando si rimuovono i nodi. Se il cluster di storage utilizza schemi di protezione dei dati che tollerano più guasti dei nodi e la rimozione dei nodi ridurrebbe la tolleranza ai guasti dei nodi dell'insieme, la rimozione del nodo normalmente fallisce con un errore. È possibile impostare questo parametro su <code>true</code> per disabilitare il controllo della tolleranza dell'ensemble in modo che la rimozione del nodo vada a buon fine.	booleano	falso	NO
<code>nodi</code>	Elenco dei <code>NodeID</code> per i nodi da rimuovere.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveNodes",
  "params": {
    "nodes" : [3,4,5]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1
  "result" : {},
}
```

Nuovo dalla versione

9,6

SetLoginSessionInfo

Puoi usare il `SetLoginSessionInfo` metodo per impostare il periodo di tempo per cui è valida un'autenticazione di accesso per una sessione. Una volta trascorso il periodo di accesso senza attività sul sistema, l'autenticazione scade. Per continuare ad accedere al cluster una volta trascorso il periodo di accesso, sono necessarie nuove credenziali di accesso.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tempo scaduto	Periodo di scadenza dell'autenticazione del cluster. Formattato in HH:mm:ss. Ad esempio: 01:30:00, 00:90:00 e 00:00:5400 possono essere tutti utilizzati per ottenere un periodo di timeout di 90 minuti. Il valore minimo di timeout è 1 minuto. Se non viene specificato alcun valore o è impostato su zero, la sessione di accesso non ha alcun valore di timeout.	corda	30 minuti	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetLoginSessionInfo",
  "params": {
    "timeout" : "01:30:00"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Fermare

Puoi usare il `Shutdown` metodo per riavviare o arrestare i nodi in un cluster. Utilizzando questo metodo è possibile 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	Necessario
nodi	Elenco dei NodeID per i nodi da riavviare o arrestare.	array di interi	Nessuno	Sì
opzione	Azioni da intraprendere per il cluster. Valori possibili: • restart: riavvia il cluster. • halt: esegue uno spegnimento completo.	corda	ricomincia	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "Shutdown",
  "params": {
    "nodes": [
      2,
      3,
      4
    ],
    "option": "halt"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "failed": [],
    "successful": [
      6
    ]
  }
}
```

Nuovo dalla versione

9,6

Metodi API per la creazione di cluster

CheckProposedCluster

Puoi usare il `CheckProposedCluster` Metodo per testare un set di nodi di archiviazione prima di creare un cluster di archiviazione con essi, per identificare possibili errori o guasti che potrebbero verificarsi dal tentativo, come capacità di nodi misti non bilanciate o tipi di nodi non supportati per cluster di archiviazione a due nodi.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nodi	Un elenco di indirizzi IP di archiviazione del set iniziale di nodi di archiviazione che costituiscono il cluster di archiviazione.	matrice di stringhe	Nessuno	Sì
forza	Impostare su true per l'esecuzione su tutti i nodi di archiviazione nel cluster di archiviazione.	booleano	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
proposedClusterValid	Indica se i nodi di archiviazione proposti costituiranno un cluster di archiviazione valido. Valori possibili: • VERO • falso	booleano
proposedClusterErrors	Errori che si verificherebbero se un cluster di archiviazione venisse creato utilizzando i nodi di archiviazione proposti.	matrice di stringhe

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
    "proposedClusterValid": true,
    "proposedClusterErrors": [ ]
  }
}
```

Nuovo dalla versione

11,0

Crea cluster

Puoi usare il `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 anche 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 per il cluster ed eseguito il [OttieniBootstrapConfig](#) Per ottenere gli indirizzi IP per il resto dei 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	Necessario
accettareEula	Indicare l'accettazione del Contratto di licenza con l'utente finale durante la creazione di questo cluster. Per accettare l'EULA, impostare questo parametro su true.	booleano	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
enableSoftwareEncryptionAtRest	Abilitare questo parametro per utilizzare la crittografia basata su software a riposo. Il valore predefinito è falso su tutti i cluster. Una volta abilitata la crittografia software a riposo, non è possibile disattivarla sul cluster.	booleano	VERO	NO
mvip	Indirizzo IP mobile (virtuale) per il cluster sulla rete di gestione.	corda	Nessuno	Sì
nodi	Indirizzi CIP/SIP del set iniziale di nodi che compongono il cluster. L'IP di questo nodo deve essere presente nell'elenco.	matrice di stringhe	Nessuno	Sì
numeroordine	Numero alfanumerico dell'ordine di vendita. Richiesto sulle piattaforme basate su software.	corda	Nessuno	No (piattaforme basate su hardware) Sì (piattaforme basate su software)

Nome	Descrizione	Tipo	Valore predefinito	Necessario
password	Password iniziale per l'account amministratore del cluster.	corda	Nessuno	Sì
numero di serie	Numero di serie alfanumerico a nove cifre. Potrebbe essere necessario su piattaforme basate su software.	corda	Nessuno	No (piattaforme basate su hardware) Sì (piattaforme basate su software)
svip	Indirizzo IP mobile (virtuale) per il cluster sulla rete di archiviazione (iSCSI).	corda	Nessuno	Sì
nome utente	Nome utente per l'amministratore del cluster.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- ["OttieniBootstrapConfig"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

OttieniBootstrapConfig

Puoi usare il `GetBootstrapConfig` metodo per ottenere informazioni su cluster e nodi dal file di configurazione bootstrap. Utilizzare questo metodo API su un singolo nodo prima che venga unito 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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Nome cluster	Nome del cluster.	corda
mvip	Indirizzo MVIP del cluster. Vuoto se il nodo non fa parte di un cluster.	corda
NomeNodo	Nome del nodo.	corda
nodi	Elenco di informazioni su ciascun nodo in attesa attiva di unirsi al cluster. Valori possibili: • chassisType: (stringa) Piattaforma hardware del nodo. • cip: (stringa) 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: (stringa) Nome host del nodo. • mip: (stringa) Indirizzo IP di gestione IPv4 del nodo. • mipV6: (stringa) Indirizzo IP di gestione IPv6 del nodo. • nodeType: (stringa) Nome del modello del nodo. • versione: (stringa) Versione del software attualmente installato sul nodo.	Matrice di oggetti JSON
svip	Indirizzo SVIP del cluster. Null se il nodo non fa parte di un cluster.	corda

Nome	Descrizione	Tipo
versione	Versione del software Element attualmente installata sul nodo chiamato da questo metodo API.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetBootstrapConfig",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
  }
}

```

Metodi API Drive

Aggiungi unità

Puoi usare il `AddDrives` Metodo per aggiungere una o più unità disponibili al cluster, consentendo alle unità di ospitare una parte dei dati per il cluster.

Quando si aggiunge un nodo di archiviazione 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 il [ListDrives](#) metodo per visualizzare le unità disponibili per essere aggiunte. Quando si aggiunge un'unità, il sistema determina automaticamente il tipo di unità da utilizzare.

Il metodo è asincrono e restituisce un risultato non appena vengono avviati i processi di ribilanciamento delle unità nel cluster. Tuttavia, potrebbe essere necessario più tempo per ribilanciare i dati nel cluster utilizzando le unità appena aggiunte; il ribilanciamento continua anche dopo il completamento della chiamata al metodo `AddDrives`. Puoi usare il [Ottieni risultato asincrono](#) metodo per interrogare l'`asyncHandle` restituito dal metodo. Dopo che il metodo `AddDrives` ritorna, puoi usare [ListSyncJobs](#) metodo per vedere l'avanzamento del ribilanciamento dei dati con le nuove unità.



Quando si aggiungono più unità, è più efficiente aggiungerle con un'unica chiamata al metodo `AddDrives` anziché con più metodi individuali, ciascuno con una singola unità. Ciò riduce la quantità di bilanciamento dei dati che deve essere eseguito per stabilizzare il carico di archiviazione sul cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
unità	Informazioni su ciascuna unità da aggiungere al cluster. Valori possibili: • driveID: ID dell'unità da aggiungere (intero). • tipo: tipo di unità da aggiungere (stringa). I valori validi sono "slice", "block" o "volume". Se omissso, il sistema assegna il tipo corretto.	Matrice di oggetti JSON	Nessuno	Sì (il tipo è facoltativo)

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListDrives](#)
- [ListSyncJobs](#)

Ottieni informazioni sull'hardware dell'unità

Puoi usare il `GetDriveHardwareInfo` metodo per ottenere tutte le informazioni

hardware per l'unità specificata. In genere, ciò include produttori, fornitori, versioni e altre informazioni di identificazione dell'hardware associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID unità	ID dell'unità per la richiesta.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
risultato	Restituite informazioni hardware per il driveID specificato.	Informazioni hardware

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetDriveHardwareInfo",
  "params": {
    "driveID": 5
  },
  "id" : 100
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[ListDrives](#)

Ottieni statistiche di guida

Puoi usare il `GetDriveStats` metodo per ottenere misurazioni di attività di alto livello per una singola unità. I valori sono cumulativi a partire dall'aggiunta dell'unità al cluster. Alcuni valori sono specifici delle unità a blocchi. Quando si esegue questo metodo, vengono restituiti dati statistici per i tipi di unità a blocchi o a metadati.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID unità	ID dell'unità per la richiesta.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
Statistiche di guida	Informazioni sull'attività dell'unità per il driveID specificato.	Statistiche di guida

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetDriveStats",
  "params": {
    "driveID": 3
  },
  "id" : 1
}
```

Esempio di risposta (blocco unità)

Questo metodo restituisce una risposta simile al seguente esempio per un'unità 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 metadati del volume)

Questo metodo restituisce una risposta simile al seguente esempio per un'unità metadati del 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
    }
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[ListDrives](#)

ListDrives

Puoi usare il `ListDrives` metodo per elencare le unità presenti nei nodi attivi del cluster. Questo metodo restituisce le unità aggiunte come metadati di volume o unità a blocchi, nonché le unità non aggiunte e disponibili.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
unità	Elenco delle unità nel cluster.	guidare vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListDrives",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

ListDriveStats

Puoi usare il `ListDriveStats` metodo per elencare le misurazioni dell'attività di alto livello per più unità nel cluster. Per impostazione predefinita, questo metodo restituisce statistiche per tutte le unità nel cluster e queste misurazioni sono cumulative a partire dall'aggiunta dell'unità al cluster. Alcuni valori restituiti da questo metodo sono specifici delle unità a blocchi, mentre altri sono specifici delle unità a metadati.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
unità	Elenco degli ID unità (driveID) per i quali restituire le statistiche dell'unità. Se si omette questo parametro, vengono restituite le misurazioni per tutte le unità.	array di interi	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Statistiche di guida	Elenco delle informazioni sull'attività dell'unità per ciascuna unità.	Statistiche di guida vettore
errori	Questo elenco contiene il driveID e il messaggio di errore associato. È sempre presente e vuoto se non ci sono errori.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 1,
  "method": "ListDriveStats",
  "params": {
    "drives": [22,23]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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"
        }
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Ottieni statistiche di guida](#)

Rimuovi unità

Puoi usare il `RemoveDrives` metodo per rimuovere in modo proattivo le unità che fanno

parte del cluster. È possibile utilizzare questo metodo quando si riduce la capacità del cluster o ci si prepara a sostituire unità prossime alla fine del loro ciclo di vita.

`RemoveDrives` crea una terza copia dei dati del blocco sugli altri nodi del 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 hanno servizi in esecuzione o dati attivi.

`RemoveDrives` è un metodo asincrono. A seconda della capacità totale delle unità rimosse, potrebbero essere necessari diversi minuti per migrare tutti i dati.

Quando si rimuovono più unità, utilizzare una singola `RemoveDrives` chiamata di metodo anziché più metodi individuali con una singola unità ciascuno. Ciò riduce la quantità di bilanciamento dei dati che deve essere eseguito per stabilizzare in modo uniforme il carico di archiviazione sul cluster.

È anche possibile rimuovere le unità con stato "fallito" utilizzando `RemoveDrives`. Quando si rimuove un'unità con stato "fallito", l'unità non torna allo stato "disponibile" o "attivo". L'unità non è disponibile per l'uso nel cluster.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
unità	Elenco di driveID da rimuovere dal cluster.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveDrives",
  "params": {
    "drives" : [3, 4, 5]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListDrives](#)

SecureEraseDrives

Puoi usare il `SecureEraseDrives` metodo per rimuovere eventuali dati residui dalle unità che hanno lo stato "disponibile". È possibile utilizzare questo metodo quando si sostituisce un'unità che sta per esaurirsi e che conteneva dati sensibili. Questo metodo utilizza un comando Security Erase Unit per scrivere un modello predeterminato sull'unità e reimposta la chiave di crittografia sull'unità. Il completamento di questo metodo asincrono potrebbe richiedere diversi minuti.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
unità	Elenco degli ID delle unità da cancellare in modo sicuro.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SecureEraseDrives",
  "params": {
    "drives" : [3, 4, 5]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1
  "result" : {
    "asyncHandle" : 1
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListDrives](#)

Metodi API Fibre Channel

GetVolumeAccessGroupLunAssignments

Puoi usare il `GetVolumeAccessGroupLunAssignments` metodo per recuperare i dettagli sui mapping LUN di un gruppo di accesso al volume specificato.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroupID	Un ID univoco del gruppo di accesso al volume utilizzato per restituire informazioni.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroupLunAssignments	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVolumeAccessGroupLunAssignments",
  "params": {
    "volumeAccessGroupID": 5
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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}
      ]
    }
  }
}

```

Nuovo dalla versione

9,6

ListFibreChannelPortInfo

Puoi usare il `ListFibreChannelPortInfo` metodo per elencare le informazioni sulle porte Fibre Channel.

Questo metodo API è pensato per essere utilizzato su nodi individuali; per accedere ai singoli nodi Fibre Channel sono richiesti un ID utente e una password. Tuttavia, questo metodo può essere utilizzato sul cluster se il parametro `force` è impostato su `true`. Se utilizzato sul cluster, vengono elencate tutte le interfacce Fibre Channel.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare su <code>true</code> per eseguirlo su tutti i nodi del cluster.	booleano	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo

FibreChannelPorts	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	FibreChannelPort vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListFibreChannelPortInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
]
}

```

```
}  
}  
}  
}
```

Nuovo dalla versione

9,6

ListFibreChannelSessions

Puoi usare il `ListFibreChannelSessions` metodo per elencare le informazioni sulle sessioni Fibre Channel su un cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Un elenco di oggetti che descrivono le sessioni Fibre Channel attive sul cluster.	sessione vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{  
  "method": "ListFibreChannelSessions",  
  "params": {},  
  "id" : 1  
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListNodeFibreChannelPortInfo

Puoi usare il `ListNodeFibreChannelPortInfo` metodo per elencare le informazioni sulle porte Fibre Channel su un nodo.

Questo metodo API è pensato per essere utilizzato su nodi individuali; per accedere ai singoli nodi Fibre Channel sono richiesti un ID utente e una password. Se utilizzato sul cluster, vengono elencate tutte le interfacce Fibre Channel.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
FibreChannelPorts	Un elenco di tutte le porte Fibre Channel fisiche o una porta per un singolo nodo.	FibreChannelPort vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListNodeFibreChannelPortInfo",
  "params": {
    "nodeID": 5,
    "force": true
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
]
}
}

```

Nuovo dalla versione

9,6

ModifyVolumeAccessGroupLunAssignments

Puoi usare il `ModifyVolumeAccessGroupLunAssignments` metodo per definire assegnazioni LUN personalizzate per volumi specifici.

Questo metodo modifica solo i valori LUN impostati sul parametro lunAssignments nel gruppo di accesso al volume. Tutte le altre assegnazioni LUN rimangono invariate.

I valori di assegnazione 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 gruppi di accesso al volume diversi.



I valori LUN validi sono compresi tra 0 e 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 se si verifica un'eccezione.

ATTENZIONE:

Se si modifica l'assegnazione di un LUN per un volume con I/O attivo, l'I/O potrebbe essere interrotto. Prima di modificare le assegnazioni LUN del volume, è necessario modificare la configurazione del server.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroupID	ID univoco del gruppo di accesso al volume per il quale verranno modificate le assegnazioni LUN.	intero	Nessuno	Sì
lunAssignments	Gli ID del volume con i nuovi valori LUN assegnati.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroupLunAssignments	Un oggetto contenente i dettagli delle assegnazioni LUN del gruppo di accesso al volume modificato.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroupLunAssignments": {
      "deletedLunAssignments": [],
      "lunAssignments": [
        {
          "lun": 0,
          "volumeID": 832
        },
        {
          "lun": 1,
          "volumeID": 834
        }
      ],
      "volumeAccessGroupID": 218
    }
  }
}
```

Nuovo dalla versione

9,6

Metodi API dell'iniziatore

Creainiziatori

Puoi usare `CreateInitiators` per creare più nuovi IQN di iniziatore o nomi di porte mondiali (WWPN) e, facoltativamente, assegnare loro alias e attributi. Quando usi `CreateInitiators` per creare nuovi iniziatori, è anche possibile aggiungerli ai gruppi di accesso al volume.

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 alcun completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
iniziatori	Un elenco di oggetti contenente le caratteristiche di ciascun nuovo iniziatore. Oggetti: • alias: (Facoltativo) Il nome descrittivo da assegnare a questo iniziatore. (corda) • attributes: (Facoltativo) Un set di attributi JSON da assegnare a questo iniziatore. (oggetto JSON) • chapUsername: (Facoltativo) Il nome utente CHAP univoco per questo iniziatore. Se non specificato durante la creazione e <code>requireChap</code> è <code>true</code>, il valore predefinito è il nome dell'iniziatore (IQN). (corda) • initiatorSecret: (Facoltativo) Il segreto CHAP utilizzato per autenticare l'iniziatore. Se non specificato durante la creazione e <code>requireChap</code> è <code>true</code>, il valore predefinito è un segreto generato casualmente. (corda)	Matrice di oggetti JSON	Nessuno	Sì
624	name:			

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
iniziatori	Elenco di oggetti che descrivono gli iniziatori appena creati.	iniziatorevettore

Errore

Questo metodo può restituire il seguente errore:

Nome	Descrizione
xInitiatorExists	Restituito se il nome dell'iniziatore scelto esiste già.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

identificatori di rete virtuale associati a questo iniziatore. Se si definiscono una o più reti virtuali, questo iniziatore potrà accedere solo a tali reti virtuali. Se non si definisce alcuna rete virtuale, questo iniziatore può

```
{
  "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": []
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Iniziatori di elenchi](#)

Eliminalniziatori

Puoi usare `DeleteInitiators` per eliminare uno o più iniziatori dal sistema (e da tutti i 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 alcun iniziatore (non è possibile alcun completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
iniziatori	Un array di ID di iniziatori da eliminare.	array di interi	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Errore

Questo metodo può restituire il seguente errore:

Nome	Descrizione
xInitiatorDoesNotExist	Restituito se il nome dell'iniziatore scelto non esiste.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 5101,
  "method": "DeleteInitiators",
  "params": {
    "initiators": [
      145,
      147
    ]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 5101,
  "result": {}
}
```

Nuovo dalla versione

9,6

Iniziatori di elenchi

Puoi usare il `ListInitiators` metodo per ottenere l'elenco degli IQN iniziatori o dei nomi delle porte mondiali (WWPN).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
iniziatori	Un elenco di ID iniziatori da recuperare. È possibile fornire questo parametro o il parametro startInitiatorID, ma non entrambi.	array di interi	Nessuno	NO
IDIniziatore di avvio	ID dell'iniziatore da cui iniziare l'elenco. È possibile fornire questo parametro o il parametro degli iniziatori, ma non entrambi.	intero	0	NO
limite	Numero massimo di oggetti iniziatori da restituire.	intero	(illimitato)	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
iniziatori	Elenco delle informazioni sull'iniziatore.	iniziatore vettore

Eccezioni

Questo metodo può avere la seguente eccezione:

Nome	Descrizione
xParametro non valido	Generato se si includono sia i parametri startInitiatorID che initiator nella stessa chiamata al metodo.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListInitiators",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "initiators": [
      {
        "alias": "",
        "attributes": {},
        "initiatorID": 2,
        "initiatorName": "iqn.1993-08.org.debian:01:c84ffd71216",
        "volumeAccessGroups": [
          1
        ]
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Modificainiziatori

Puoi usare il `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 prima con il [Eliminalniziatori](#) metodo e crearne uno nuovo con il [Crealniziatori](#) metodo.

Se `ModifyInitiators` non riesce a modificare uno degli iniziatori forniti nel parametro, il metodo restituisce un errore e non modifica alcun iniziatore (non è possibile alcun completamento parziale).

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario

iniziatori	Un elenco di oggetti contenente le caratteristiche di ciascun iniziatore da modificare. Possibili oggetti: • alias: (Facoltativo) Un nuovo nome descrittivo da assegnare all'iniziatore. (corda) • 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. (corda) • forceDuringUpgrade: Completa la modifica dell'iniziatore durante un aggiornamento. • initiatorID: (Obbligatorio) L'ID dell'iniziatore da modificare. (numero intero) • initiatorSecret: (Facoltativo) Un nuovo segreto CHAP utilizzato per autenticare l'iniziatore. (corda) • requireChap: (Facoltativo) Vero se CHAP è richiesto per	Matrice di oggetti JSON	Nessuno	Sì

Valore di ritorno questo iniziatore.
Questo metodo ha il seguente valore di ritorno:
(booleano)

Nome	Descrizione	Tipo
iniziatori	Elenco di oggetti che descrivono gli iniziatori appena modificati.	iniziatore vettore

Richiedi esempio la destinazione (quando si utilizza l'autenticazione CHAP al seguente esempio:

```
{
  "id": 6683,
  "method": "ModifyInitiators",
  "params": {
    "initiators": [
      {
        "initiatorID": 2,
        "alias": "alias1",
        "volumeAccessGroupID": null
      },
      {
        "initiatorID": 3,
        "alias": "alias2",
        "volumeAccessGroupID": 1
      }
    ]
  }
}
```

le reti.

Esempio di risposta • volumeAccessGroupID:
Questo metodo restituisce una risposta simile al seguente esempio:
(facoltativo) ID
del gruppo di
accesso al
volume a cui
deve essere
aggiunto
l'iniziatore. Se
l'iniziatore si
trovava in
precedenza in
un gruppo di
accesso al
volume diverso,
viene rimosso
dal vecchio
gruppo di
accesso al
volume. Se

```
{
  "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
        ]
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [CreaIniziatori](#)
- [EliminaIniziatori](#)

Metodi API LDAP

AggiungiLdapClusterAdmin

Puoi usare il `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 di amministrazione del cluster LDAP sono completamente separati e non correlati agli account tenant standard.

Parametri

È possibile utilizzare questo metodo anche per aggiungere un gruppo LDAP definito in Active Directory®. Il livello di accesso concesso al gruppo viene trasmesso ai singoli utenti del gruppo LDAP.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accesso	Controlla quali metodi può utilizzare questo amministratore del cluster.	matrice di stringhe	Nessuno	Sì
accettareEula	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 fallisce.	booleano	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
nome utente	Nome utente distinto per il nuovo amministratore del cluster LDAP.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Controllo degli accessi](#)

Abilita autenticazione LDAP

Puoi usare il `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 archiviazione utilizzando le proprie credenziali LDAP.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tipo di autorizzazione	Identifica quale metodo di autenticazione utente utilizzare. Valori possibili: • DirectBind • SearchAndBind	corda	Cerca e associa	NO
groupSearchBaseDN	Il DN di base dell'albero da cui iniziare la ricerca del sottoalbero del gruppo.	corda	Nessuno	NO
groupSearchType	Controlla il filtro di ricerca del gruppo predefinito utilizzato. Valori possibili: • NoGroups: nessun supporto di gruppo. • ActiveDirectory: appartenenza annidata a tutti i gruppi di Active Directory di un utente. • MemberDN: gruppi di stile MemberDN (livello singolo).	corda	Directory attiva	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
serverURIs	Un elenco separato da virgole di URI del server LDAP o LDAPS. È possibile aggiungere una porta personalizzata alla fine di un URI LDAP o LDAPS utilizzando due punti seguiti dal numero di 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.	matrice di stringhe	Nessuno	Sì
userSearchBaseDN	Il DN di base dell'albero da cui iniziare la ricerca del sottoalbero. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind.	corda	Nessuno	NO
searchBindDN	Un DN completamente qualificato 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 obbligatorio quando si utilizza un authType di SearchAndBind.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
cercaBindPassword	Password per l'account searchBindDN utilizzato per la ricerca. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind.	corda	Nessuno	Sì
filtroricercautente	Filtro di ricerca LDAP da utilizzare quando si interroga il server LDAP. La stringa dovrebbe contenere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente che esegue l'autenticazione. Ad esempio, (&(objectClass=person)(sAMAccountName=%USERNAME%)) utilizzerà il campo sAMAccountName in Active Directory per far corrispondere il nome utente immesso durante l'accesso al cluster. Questo parametro è obbligatorio quando si utilizza un authType di SearchAndBind.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ModelloDNutente	Un modello di stringa utilizzato per definire un modello per la costruzione di un nome distinto (DN) utente completo. La stringa dovrebbe contenere il testo segnaposto "%USERNAME%" che viene sostituito con il nome utente dell'utente che esegue l'autenticazione. Questo parametro è obbligatorio quando si utilizza un authType di DirectBind.	corda	Nessuno	Sì
groupSearchCustom Filter	Da utilizzare con il tipo di ricerca CustomFilter, un filtro LDAP da utilizzare per restituire i DN dei gruppi di un utente. La stringa può contenere il testo segnaposto %USERNAME% e %USERDN% da sostituire con il nome utente e il nome utente completo, se necessario.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
  }
}
```

Nuovo dalla versione

9,6

Disabilita l'autenticazione LDAP

Puoi usare il `DisableLdapAuthentication` metodo per disabilitare l'autenticazione LDAP e rimuovere tutte le impostazioni di configurazione LDAP. Questo metodo non rimuove alcun account amministratore del cluster configurato per utenti o gruppi. Dopo aver disabilitato l'autenticazione LDAP, gli amministratori del cluster configurati per utilizzare l'autenticazione LDAP non potranno più accedere al cluster.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableLdapAuthentication",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

OttieniLdapConfiguration

Puoi usare il `GetLdapConfiguration` metodo per ottenere la configurazione LDAP attualmente attiva sul cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno.

Nome	Descrizione	Tipo
Configurazione ldap	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 disabilitata, tutte le impostazioni restituite sono vuote, ad eccezione di "authType" e "groupSearchType", che sono impostate rispettivamente su "SearchAndBind" e "ActiveDirectory".	Configurazione ldap

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetLdapConfiguration",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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%))"
    }
  }
}
```

Nuovo dalla versione

9,6

TestLdapAuthentication

Puoi usare il `TestLdapAuthentication` metodo per convalidare le impostazioni di autenticazione LDAP attualmente abilitate. Se la configurazione è corretta, la chiamata API restituisce l'appartenenza al gruppo dell'utente testato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome utente	Il nome utente da testare.	corda	Nessuno	Sì
password	La password per il nome utente da testare.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Configurazione ldap	Un oggetto ldapConfiguration da testare. Se si fornisce questo parametro, il sistema verifica la configurazione fornita anche se l'autenticazione LDAP è attualmente disabilitata.	Configurazione ldap	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
gruppi	Elenco dei gruppi LDAP che includono l'utente testato come membro.	vettore
nomeutente	Nome distinto LDAP completo dell'utente testato.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestLdapAuthentication",
  "params": { "username": "admin1",
              "password": "admin1PASS"
            },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

Metodi API di autenticazione a più fattori

AddIdpClusterAdmin

Puoi usare il `AddIdpClusterAdmin` metodo per aggiungere un utente amministratore del cluster autenticato da un Identity Provider (IdP) di terze parti. Gli account di amministrazione del cluster IdP vengono configurati in base alle informazioni sui valori degli attributi SAML fornite nell'asserzione SAML dell'IdP associata all'utente. Se un utente si autentica correttamente con l'IdP e ha istruzioni di attributi SAML all'interno dell'asserzione SAML che corrispondono a più account di amministrazione del cluster IdP, l'utente avrà il livello di accesso combinato di quegli account di amministrazione del cluster IdP corrispondenti.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accesso	Controlla quali metodi può utilizzare questo amministratore del cluster IdP.	matrice di stringhe	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accettareEula	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 fallisce.	booleano	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
nome utente	Un mapping attributo-valore SAML a un amministratore del cluster IdP (ad esempio, email=test@ example.com). Ciò può essere definito utilizzando un soggetto SAML specifico utilizzando NameID o come voce nell'istruzione dell'attributo SAML, come ad esempio eduPersonAffiliation.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ID amministratore cluster	Identificatore univoco per l'amministratore del cluster appena creato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "AddIdpClusterAdmin",
  "params": {
    "username": "email=test@example.com",
    "acceptEula": true,
    "access": ["administrator"]
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result": {
    "clusterAdminID": 13
  }
}
```

Nuovo dalla versione

12,0

Crea configurazione Idp

Puoi usare il `CreateIdpConfiguration` Metodo per creare una potenziale relazione di trust per l'autenticazione utilizzando un Identity Provider (IdP) di terze parti per il cluster. Per la comunicazione 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	Necessario
idpMetadata	Metadati IdP da memorizzare.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome idp	Nome utilizzato per identificare un provider IdP per l'accesso singolo SAML 2.0.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
idpConfigInfo	Informazioni sulla configurazione dell'Identity Provider (IdP) di terze parti.	"idpConfigInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MIID...SlBHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nuovo dalla versione

12,0

DeleteAuthSession

Puoi usare il `DeleteAuthSession` metodo per eliminare una singola sessione di autenticazione utente. Se l'utente chiamante non è presente nel `ClusterAdmins/Administrator AccessGroup`, è possibile eliminare solo la sessione di autenticazione appartenente all'utente chiamante.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID sessione	Identificatore univoco per la sessione di autenticazione da eliminare.	UUID	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessione	Informazioni sulla sessione per l'autorizzazione all'eliminazione.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteAuthSession",
  "params": {
    "sessionID": "a862a8bb-2c5b-4774-a592-2148e2304713"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

12,0

DeleteAuthSessionsByClusterAdmin

Puoi usare il `DeleteAuthSessionsByClusterAdmin` metodo per eliminare tutte le sessioni di autenticazione associate allo specificato `ClusterAdminID`. Se il `ClusterAdminID` specificato è mappato a un gruppo di utenti, tutte le sessioni di autenticazione per tutti i membri di quel gruppo verranno eliminate. Per visualizzare un elenco di sessioni per una possibile eliminazione, utilizzare il metodo `ListAuthSessionsByClusterAdmin` con `ClusterAdminID` parametro.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID amministratore cluster	Identificatore univoco per l'amministratore del cluster.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione eliminate.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteAuthSessionsByClusterAdmin",
  "params": {
    "clusterAdminID": 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}
```

Nuovo dalla versione

12,0

EliminaAuthSessionsByUsername

Puoi usare il `DeleteAuthSessionsByUsername` metodo per eliminare tutte le sessioni di autenticazione per un dato utente. Un chiamante che non fa parte di `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 potrebbero essere eliminate, utilizzare `ListAuthSessionsByUsername` con gli stessi parametri. Per visualizzare un elenco di sessioni per una possibile eliminazione, utilizzare `ListAuthSessionsByUsername` metodo con lo stesso parametro.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Metodo di autenticazione	Metodo di autenticazione delle sessioni utente da eliminare. Solo un chiamante nel ClusterAdmins/Administrator AccessGroup può fornire questo parametro. I valori possibili sono: • authMethod=Cluster specifica il nome utente ClusterAdmin. • authMethod=Ldap specifica il DN LDAP dell'utente. • authMethod=Idp specifica l'UUID IdP o il NameID dell'utente. Se l'IdP non è configurato per restituire nessuna delle due opzioni, viene specificato un UUID casuale emesso al momento della creazione della sessione.	Metodo di autenticazione	Nessuno	NO
nome utente	Identificatore univoco per l'utente.	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione eliminate.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteAuthSessionsByUsername",
  "params": {
    "authMethod": "Cluster",
    "username": "admin"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}
```

Nuovo dalla versione

12,0

Elimina configurazione Idp

Puoi usare il `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 fornitore di servizi SAML dal cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
idpConfigurationID	UUID per la configurazione dell'IdP di terze parti.	UUID	Nessuno	NO
Nome idp	Nome utilizzato per identificare e recuperare un provider IdP per l'accesso singolo SAML 2.0.	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "idpName": "https://provider.name.url.com"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result": {}
}
```

Nuovo dalla versione

12,0

Disabilita l'autenticazione Idp

Puoi usare il `DisableIdpAuthentication` metodo per disabilitare il supporto per l'autenticazione tramite IdP di terze parti per il cluster. Una volta disabilitati, gli utenti autenticati da IdP di terze parti non saranno più in grado di accedere al cluster e tutte le sessioni autenticate attive verranno invalidate/disconnesse. Gli amministratori LDAP e del cluster possono accedere al cluster tramite le interfacce utente supportate.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableIdpAuthentication",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result": {}
}
```

Nuovo dalla versione

12,0

Abilita autenticazione Idp

Puoi usare il `EnableIdpAuthentication` metodo per abilitare il supporto per l'autenticazione tramite IdP di terze parti per il cluster. Una volta abilitata l'autenticazione IdP, gli amministratori LDAP e del cluster non saranno più in grado di accedere al cluster tramite le interfacce utente supportate e tutte le sessioni autenticate attive verranno 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	Necessario
idpConfigurationID	UUID per la configurazione dell'IdP di terze parti. Se esiste una sola configurazione IdP, l'impostazione predefinita è abilitare tale configurazione. Se si dispone di un solo IdpConfiguration, non è necessario fornire il parametro idpConfigurationID.	UUID	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableIdpAuthentication",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result": {}
}
```

Nuovo dalla versione

12,0

Ottieni stato di autenticazione Idp

Puoi usare il `GetIdpAuthenticationState` metodo per restituire informazioni sullo stato dell'autenticazione tramite IdP di terze parti.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
abilitato	Indica se è abilitata l'autenticazione IdP di terze parti.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetIdpAuthenticationState"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result": {"enabled": true}
}
```

Nuovo dalla versione

12,0

ListActiveAuthSessions

Puoi usare il `ListActiveAuthSessions` metodo per elencare tutte le sessioni autenticate attive. Solo gli utenti con diritti di accesso amministrativi possono chiamare questo metodo.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Informazioni sulla sessione per le sessioni di autenticazione.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListActiveAuthSessions"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}
```

Nuovo dalla versione

12,0

ListIdpConfigurations

Puoi usare il `ListIdpConfigurations` metodo per elencare le configurazioni per IdP di terze parti. Facoltativamente, puoi fornire il `enabledOnly` flag per recuperare la configurazione IdP attualmente abilitata o un UUID dei metadati IdP o un nome IdP per interrogare le informazioni per una configurazione IdP specifica.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>abilitatoSolo</code>	Filtra il risultato per restituire la configurazione IdP attualmente abilitata.	booleano	Nessuno	NO
<code>idpConfigurationID</code>	UUID per la configurazione dell'IdP di terze parti.	UUID	Nessuno	NO
<code>Nome idp</code>	Recupera le informazioni di configurazione dell'IdP per un nome IdP specifico.	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>idpConfigInfos</code>	Informazioni sulle configurazioni degli IdP di terze parti.	"idpConfigInfo" vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListIdpConfigurations",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nuovo dalla versione

12,0

Aggiorna configurazione Idp

Puoi usare il `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	Necessario
generateNewCertificate	Se specificato come vero, viene generata una nuova chiave SAML e un nuovo certificato che sostituiscono la coppia esistente. Nota: la sostituzione del certificato esistente interromperà la fiducia stabilita tra il cluster e l'IdP finché i metadati del Service Provider del cluster non verranno ricaricati nell'IdP. Se non specificato o impostato su false, il certificato e la chiave SAML rimangono invariati.	booleano	Nessuno	NO
idpConfigurationID	UUID per la configurazione dell'IdP di terze parti.	UUID	Nessuno	NO
idpMetadata	Metadati IdP per i dettagli di configurazione e integrazione per l'accesso singolo SAML 2.0.	corda	Nessuno	NO
Nome idp	Nome utilizzato per identificare e recuperare un provider IdP per l'accesso singolo SAML 2.0.	corda	Nessuno	NO
nuovoIdpName	Se specificato, questo nome sostituisce il vecchio nome IdP.	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
idpConfigInfo	Informazioni sulla configurazione dell'IdP di terze parti.	"idpConfigInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "UpdateIdpConfiguration",
  "params": {
    "idpConfigurationID": "f983c602-12f9-4c67-b214-bf505185cfed",
    "generateNewCertificate": true
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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://priver.name.url.com",
      "serviceProviderCertificate": "-----BEGIN CERTIFICATE-----\n
MI...BHi\n
-----END CERTIFICATE-----\n",
      "spMetadataUrl": "https://10.193.100.100/auth/ui/saml2"
    }
  }
}
```

Nuovo dalla versione

12,0

Metodi API di autenticazione della sessione

ListAuthSessionsByClusterAdmin

Puoi usare il `ListAuthSessionsByClusterAdmin` metodo per elencare tutte le sessioni di autenticazione associate allo specificato `ClusterAdminID`. Se specificato `ClusterAdminID` se si associa 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	Necessario
ID amministratore cluster	Identificatore univoco per l'amministratore del cluster.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessions	Elenco delle informazioni sulla sessione per le sessioni di autenticazione.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListAuthSessionsByClusterAdmin",
  "clusterAdminID": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}
```

Nuovo dalla versione

12,0

ListAuthSessionsByUsername

Puoi usare il `ListAuthSessionsByUsername` metodo per elencare tutte le sessioni di autenticazione per l'utente specificato. Un chiamante che non dispone dei privilegi `AccessGroup ClusterAdmins/Amministratore` può elencare solo le proprie sessioni. Un chiamante con privilegi `ClusterAdmins/Amministratore` può elencare le sessioni appartenenti a qualsiasi utente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Metodo di autenticazione	Metodo di autenticazione delle sessioni utente da elencare. Solo un chiamante nel <code>ClusterAdmins/Administratore</code> <code>AccessGroup</code> può fornire questo parametro. I valori possibili sono: • authMethod=Cluster specifica il nome utente <code>ClusterAdmin</code>. • authMethod=Ldap specifica il DN LDAP dell'utente. • authMethod=Idp specifica l'UUID IdP o il NameID dell'utente. Se l'IdP non è configurato per restituire nessuna delle due opzioni, viene specificato un UUID casuale emesso al momento della creazione della sessione.	Metodo di autenticazione	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome utente	Identificatore univoco per l'utente.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sessioni	Elenco delle informazioni sulla sessione per le sessioni di autenticazione.	"authSessionInfo"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListAuthSessionsByUsername",
  "authMethod": "Cluster",
  "username": "admin"
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}
```

Nuovo dalla versione

12,0

Metodi API del nodo

CheckPingOnVlan

Puoi usare il `CheckPingOnVlan` Metodo per testare la connettività di rete su una VLAN temporanea durante l'esecuzione della convalida di rete pre-distribuzione.

`CheckPingOnVlan` crea un'interfaccia VLAN temporanea, invia pacchetti ICMP a tutti i nodi nel cluster di archiviazione utilizzando l'interfaccia VLAN e quindi rimuove l'interfaccia.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tentativi	Specifica il numero di volte in cui il sistema deve ripetere il ping di prova.	intero	5	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ospiti	Specifica un elenco separato da virgole di indirizzi o nomi host di dispositivi da sottoporre a ping.	corda	I nodi nel cluster	NO
interfaccia	L'interfaccia (base) esistente da cui devono essere inviati i ping. Valori possibili: • Bond10G: invia ping dall'interfaccia Bond10G. • Bond1G: invia ping dall'interfaccia Bond1G.	corda	Nessuno	Sì
dimensione del pacchetto	Specifica il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore all'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
proibire la frammentazione	Abilita il flag DF (Do not Fragment) per i pacchetti ICMP.	booleano	falso	NO
sourceAddressV4	L'indirizzo IPv4 di origine da utilizzare nei pacchetti ping ICMP.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
sourceAddressV6	L'indirizzo IPv6 di origine da utilizzare nei pacchetti ping ICMP.	corda	Nessuno	Sì
timeout totaleSec	Specifica il tempo in secondi che il ping deve attendere per una risposta del sistema prima di emettere il successivo tentativo di ping o di terminare il processo.	intero	5	NO
virtualNetworkTag	ID VLAN da utilizzare durante l'invio dei pacchetti ping.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Elenco di tutti gli IP con cui il nodo è riuscito a comunicare e statistiche di risposta al ping.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
    "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
    }
  }
}
```

Nuovo dalla versione

11,1

CheckProposedNodeAdditions

Puoi usare il `CheckProposedNodeAdditions` Metodo per testare un set di nodi di archiviazione per verificare se è possibile aggiungerli a un cluster di archiviazione senza

errori o violazioni delle best practice.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nodi	Un elenco di indirizzi IP di archiviazione dei nodi di archiviazione pronti per essere aggiunti a un cluster di archiviazione.	matrice di stringhe	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
proposedClusterValid	Indica se i nodi di archiviazione proposti costituiranno un cluster di archiviazione valido. Valori possibili: • VERO • falso	booleano

proposedClusterErrors	Errori che si verificherebbero se un cluster di archiviazione venisse creato utilizzando i nodi di archiviazione proposti. Possibili codici di errore: • <code>nodesNoCapacity</code>: I nodi non avevano alcuna capacità utilizzabile. • <code>nodesTooLarge</code>: I nodi costituiscono una porzione troppo grande della capacità del cluster per lo schema di protezione attiva. • <code>nodesConnectFailed</code>: Impossibile connettersi ai nodi per interrogare la configurazione hardware. • <code>nodesQueryFailed</code>: Impossibile interrogare i nodi per la configurazione hardware. • <code>nodesClusterMember</code>: Gli indirizzi IP per i nodi sono già in uso nel cluster. • <code>nonFipsNodeCapable</code>: Impossibile aggiungere un nodo non compatibile con FIPS al cluster di archiviazione mentre è abilitata la funzionalità di crittografia dell'unità FIPS 140-2. • <code>nonFipsDrivesCapable</code>: Impossibile aggiungere un nodo con unità non compatibili con FIPS al cluster mentre è abilitata la funzionalità di crittografia delle unità FIPS 140-2.	matrice di stringhe

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
    "proposedClusterValid": true,
    "proposedClusterErrors": [ ]
  }
}
```

Nuovo dalla versione

11,0

Crea Cluster Support Bundle

Puoi usare il `CreateClusterSupportBundle` sul nodo di gestione per raccogliere i bundle di supporto da tutti i nodi di un cluster. I singoli pacchetti di supporto dei nodi sono compressi come file tar.gz. Il bundle di supporto del cluster è un file tar contenente i bundle di supporto del nodo. È possibile eseguire questo metodo solo su un nodo di gestione; non funziona se eseguito su un nodo di archiviazione.

Parametri



È necessario chiamare questo metodo sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
consentilncompleto	Consente allo script di continuare l'esecuzione se non è possibile raccogliere i bundle da uno o più nodi.	booleano	Nessuno	NO
Nome del bundle	Nome univoco per ogni pacchetto di supporto creato. Se non viene fornito alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo	corda	Nessuno	NO
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.	corda	Nessuno	Sì
nodi	Gli indirizzi IP dei nodi da cui raccogliere i bundle. Utilizzare nodes o mvip, ma non entrambi, per specificare i nodi da cui raccogliere i bundle. Questo parametro è obbligatorio se mvip non è specificato.	matrice di stringhe	Nessuno	Sì
password	La password di amministratore del cluster. Nota: questa password è visibile come testo una volta inserita.	corda	Nessuno	Sì
nome utente	Nome utente dell'amministratore del cluster.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateClusterSupportBundle",
  "params": {
    "bundlename": "clusterbundle",
    "mvip": "132.119.120.100"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

Crea pacchetto di supporto

Puoi usare `CreateSupportBundle` per creare un file di bundle di supporto nella directory del nodo. Dopo la creazione, il bundle viene memorizzato sul 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	Necessario
Nome del bundle	Nome univoco per il pacchetto di supporto. Se non viene specificato alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.	corda	Nessuno	NO
extraArgs	Utilizzare '--compress gz' per creare il pacchetto di supporto come file tar.gz.	corda	Nessuno	NO
timeoutSec	Numero di secondi di esecuzione dello script del pacchetto di supporto.	intero	1500	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

dettagli	I dettagli del pacchetto di supporto. Valori possibili: • bundleName: il nome specificato nel metodo <code>CreateSupportBundleAPI</code>. Se non è stato specificato alcun nome, verrà utilizzato "supportbundle". • extraArgs: gli argomenti passati con questo metodo. • file: un elenco dei file del pacchetto di supporto creati dal sistema. • output: l'output della riga di comando dallo script che ha creato il bundle di supporto. • timeoutSec: numero di secondi di esecuzione dello script del bundle di supporto prima di arrestarsi. • url: URL del pacchetto di supporto creato.	Oggetto JSON
durata	Ora utilizzata per creare il pacchetto di supporto nel formato: HH:MM:SS.ssssss.	corda
risultato	Il successo o il fallimento dell'operazione del pacchetto di supporto.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateSupportBundle",
  "params": {
    "extraArgs": "--compress gz"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

Elimina tutti i pacchetti di supporto

Puoi usare il `DeleteAllSupportBundles` metodo per eliminare tutti i pacchetti di supporto generati con `CreateSupportBundle` Metodo API.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteAllSupportBundles",
  "params": {}
},
"id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Disabilita modalità manutenzione

Puoi usare il `DisableMaintenanceMode` metodo per far uscire un nodo di archiviazione dalla modalità di manutenzione. È consigliabile disattivare la modalità di manutenzione solo dopo aver completato la manutenzione e quando il nodo è online.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nodi	Elenco degli ID dei nodi di archiviazione da rimuovere dalla modalità di manutenzione.	array di interi	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

asyncHandle	È possibile utilizzare il metodo GetAsyncResult per recuperare questo asyncHandle e determinare quando la transizione alla modalità di manutenzione è completa.	intero
modalità corrente	Lo stato attuale della modalità di manutenzione del nodo. Valori possibili: • Disabilitato: non è stata richiesta alcuna manutenzione. • FailedToRecover: il nodo non è riuscito a riprendersi dalla modalità di manutenzione. • Imprevisto: il nodo è stato trovato offline, ma era in modalità Disabilitato. • RecoveringFromMaintenance: il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: vengono intraprese azioni per preparare un nodo all'esecuzione della manutenzione. • ReadyForMaintenance: il nodo è pronto per essere sottoposto a manutenzione.	MaintenanceMode (stringa)

modalità richiesta	Lo stato di modalità di manutenzione richiesto del nodo. Valori possibili: • Disabilitato: non è stata richiesta alcuna manutenzione. • FailedToRecover: il nodo non è riuscito a riprendersi dalla modalità di manutenzione. • Imprevisto: il nodo è stato trovato offline, ma era in modalità Disabilitato. • RecoveringFromMaintenance: il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: vengono intraprese azioni per preparare un nodo all'esecuzione della manutenzione. • ReadyForMaintenance: il nodo è pronto per essere sottoposto a manutenzione.	MaintenanceMode (stringa)

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableMaintenanceMode",
  "params": {
    "nodes": [6]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {
      "requestedMode": "Disabled",
      "asyncHandle": 1,
      "currentMode": "Enabled"
    }
}
```

Nuovo dalla versione

12,2

Trova maggiori informazioni

["Concetti sulla modalità di manutenzione dello storage NetApp HCI"](#)

DisabilitaSsh

Puoi usare il `DisableSsh` metodo per disabilitare il servizio SSH per un singolo nodo di archiviazione. Questo metodo non influisce sulla durata del timeout del servizio SSH a livello di cluster.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
abilitato	Lo stato del servizio SSH per questo nodo.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableSsh",
  "params": {
    },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {"enabled": false}
}
```

Abilita modalità di manutenzione

Puoi usare il `EnableMaintenanceMode` metodo per preparare un nodo di archiviazione per la manutenzione. Gli scenari di manutenzione includono qualsiasi attività che richieda lo spegnimento o il riavvio del nodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza con errori non risolti	Forza l'attivazione della modalità di manutenzione per questo nodo anche in presenza di errori del cluster bloccanti.	booleano	Falso	NO
nodi	Elenco degli ID nodo da mettere in modalità manutenzione. È supportato un solo nodo alla volta.	array di interi	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Limite di scambio primario al minuto	Numero di slice primarie da scambiare al minuto. Se non specificato, tutte le sezioni primarie verranno scambiate contemporaneamente.	intero	Nessuno	NO
tempo scaduto	Specifica per quanto tempo la modalità di manutenzione deve rimanere abilitata prima di essere disattivata automaticamente. Formattato come stringa di tempo (ad esempio, HH:mm:ss). Se non specificato, la modalità di manutenzione rimarrà abilitata finché non verrà disabilitata esplicitamente.	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	È possibile utilizzare il metodo GetAsyncResult per recuperare questo asyncHandle e determinare quando la transizione alla modalità di manutenzione è completa.	intero

modalità corrente	Lo stato attuale della modalità di manutenzione del nodo. Valori possibili: • Disabilitato: non è stata richiesta alcuna manutenzione. • FailedToRecover: il nodo non è riuscito a riprendersi dalla modalità di manutenzione. • RecoveringFromMaintenance: il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: vengono intraprese azioni per preparare un nodo all'esecuzione della manutenzione. • ReadyForMaintenance: il nodo è pronto per essere sottoposto a manutenzione.	MaintenanceMode (stringa)
modalità richiesta	Lo stato di modalità di manutenzione richiesto del nodo. Valori possibili: • Disabilitato: non è stata richiesta alcuna manutenzione. • FailedToRecover: il nodo non è riuscito a riprendersi dalla modalità di manutenzione. • RecoveringFromMaintenance: il nodo è in fase di ripristino dalla modalità di manutenzione. • PreparingForMaintenance: vengono intraprese azioni per preparare un nodo all'esecuzione della manutenzione. • ReadyForMaintenance: il nodo è pronto per essere sottoposto a manutenzione.	MaintenanceMode (stringa)

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:


```
{
  "method": "EnableMaintenanceMode",
  "params": {
    "forceWithUnresolvedFaults": False,
    "nodes": [6],
    "perMinutePrimarySwapLimit" : 40,
    "timeout" : "01:00:05"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "requestedMode": "ReadyForMaintenance",
    "asyncHandle": 1,
    "currentMode": "Disabled"
  }
}
```

Nuovo dalla versione

12,2

Trova maggiori informazioni

["Concetti sulla modalità di manutenzione dello storage NetApp HCI"](#)

AbilitaSsh

Puoi usare il `EnableSsh` metodo per abilitare 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 parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
abilitato	Lo stato del servizio SSH per questo nodo.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableSsh",
  "params": {
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {"enabled": true}
}
```

OttieniClusterConfig

Puoi usare il `GetClusterConfig` Metodo API per restituire informazioni sulla configurazione del cluster utilizzata dal nodo per comunicare con il proprio cluster.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
grappolo	Informazioni sulla configurazione del cluster che il nodo utilizza per comunicare con il cluster.	grappolo

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterConfig",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

9,6

Ottieni stato cluster

Puoi usare il `GetClusterState` Metodo API per indicare se un nodo fa parte di un cluster oppure no.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
grappolo	Nome del cluster.	corda
stato	• Disponibile: il nodo non è stato configurato con un nome cluster. • In sospeso: il nodo è in sospeso per un cluster denominato specifico e può essere aggiunto. • Attivo: il nodo è un membro attivo di un cluster e non può essere aggiunto a un altro cluster.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterState",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" :
    "cluster" : "Cluster101"
    "state" : "Active"
}
```

Nuovo dalla versione

9,6

OttieniConfig

Puoi usare il `GetConfig` Metodo API per ottenere tutte le informazioni di configurazione per un nodo. Questo metodo API include le stesse informazioni disponibili in entrambi i `GetClusterConfig` E `GetNetworkConfig` Metodi API.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
configurazione	I dettagli di configurazione del cluster. Questo oggetto contiene: • grappolo: Informazioni sul cluster che identificano il modo in cui il nodo di archiviazione comunica con il cluster di archiviazione 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

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetConfig",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [OttieniClusterConfig](#)
- [OttieniConfigurazione di rete](#)
- [OttieniConfig](#)

GetDriveConfig

Puoi usare il `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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
driveConfig	Informazioni sulle unità collegate al nodo.	guidare

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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'unità di un solo nodo di archiviazione.

```

{
  "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
    }
  }
}

```

OttieniConfigurazioneHardware

Puoi usare il `GetHardwareConfig` metodo per ottenere le informazioni sulla configurazione hardware di un nodo. Questi dati di configurazione sono destinati all'uso interno. Per ottenere un inventario più utile dei componenti hardware del sistema live, utilizzare `GetHardwareInfo` metodo invece.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
configurazione hardware	Elenco delle informazioni hardware e delle impostazioni correnti.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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
    }
  }
}

```

Nuovo dalla versione

9,6

Ottieni informazioni sull'hardware

Puoi usare il `GetHardwareInfo` metodo per ottenere informazioni hardware in tempo reale e lo stato di un singolo nodo. Le informazioni sull'hardware in genere includono produttori, fornitori, versioni, unità e altre informazioni identificative associate.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare questo parametro "force" su true per eseguirlo su tutti i nodi del cluster.	booleano	falso	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
Informazioni hardware	Informazioni hardware per il nodo.	Informazioni hardware

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetHardwareInfo",
  "params": {
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    },
    ...
]
}
}
}

```

Nuovo dalla versione

9,6

OttieniIpmiConfig

Puoi usare il `GetIpmiConfig` metodo per recuperare informazioni sui sensori hardware dai sensori presenti nel nodo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo
tipo di telaio	Utilizzato per visualizzare informazioni per ciascun tipo di chassis del nodo. Valori possibili: - all: restituisce informazioni sui sensori per ogni tipo di telaio. {tipo di telaio}: restituisce informazioni sul sensore per un tipo di telaio specificato.	corda

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Nome del sensore	Nome del sensore trovato.	corda
ID sensore univoco	Identificatore univoco del sensore.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetIpmiConfig",
  "params": {
    "chassisType": "all"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
    ],
}

```

Nuovo dalla versione

9,6

OttieniIpmiInfo

Puoi usare il `GetIpmiInfo` Metodo per visualizzare un report dettagliato dei sensori (oggetti) per le ventole dei nodi, le temperature di aspirazione e di scarico e gli

alimentatori monitorati dal sistema.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
sensori	Informazioni dettagliate da ciascun sensore all'interno di un nodo.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetIpmiInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

A causa della lunghezza della risposta restituita per questo metodo API, alcune parti della risposta sono state intenzionalmente eliminate da questo documento. Sono incluse le parti delle informazioni hardware che il sistema monitora per garantire che il nodo funzioni con prestazioni 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"
  },

```

EACH NODE

```

{THIS ENTIRE SECTION IS REPEATED FOR THE INLET TEMPERATURE OF

```

```

    "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"
  },

```

NODE

```

{THIS ENTIRE SECTION IS REPEATED FOR EACH POWER SUPPLY ON EACH

```

```

    "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"
    },
    .
    .
    .
}
]
}
}
}
}

```

Nuovo dalla versione

9,6

Ottieni Configurazione di rete

Puoi usare il `GetNetworkConfig` metodo per visualizzare le informazioni sulla configurazione di rete per un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
rete	Tipi di connessione di rete e impostazioni correnti per ciascuna interfaccia di rete del nodo.	rete (tutte le interfacce)

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNetworkConfig",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniConfigurazione di rete](#)

OttieniInterfaccia di Rete

Puoi usare il `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	Necessario
interfaccia	Nome dell'interfaccia su cui ottenere informazioni per ciascun nodo. Valori possibili: • Bond1G • Bond10G	corda	Nessuno	NO
forza	Impostare questo parametro su true per eseguirlo su tutti i nodi del cluster.	booleano	falso	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
nodi	Una matrice di oggetti che descrivono l'interfaccia per ciascun nodo di archiviazione nel cluster di archiviazione. Ogni oggetto all'interno dell'array contiene i seguenti elementi: • nodeID: (intero) ID del nodo di archiviazione nel cluster di archiviazione a cui si applicano le informazioni sull'interfaccia. • risultato: (interfaccia di rete) Informazioni sulla configurazione dell'interfaccia per questo nodo di archiviazione.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNetworkInterface",
  "params": {
    "interface": "Bond1G",
    "force": true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
        }
      }
    }
  ]
}

```

Nuovo dalla versione

9,6

GetNodeActiveTlsCiphers

Puoi usare il `GetNodeActiveTlsCiphers` 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 di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Cifrari obbligatori	Elenco delle suite di cifratura TLS obbligatorie per il nodo. Si tratta di cifrari sempre attivi sul nodo.	corda
Cifrari supplementari	Elenco delle suite di cifratura TLS supplementari per il nodo.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeActiveTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    ]
  }
}
```

Ottieni report sui drive dei nodi Fips

Puoi usare il `GetNodeFipsDrivesReport` metodo per verificare lo stato della capacità di crittografia dell'unità FIPS 140-2 di un singolo nodo nel cluster di archiviazione. È

necessario eseguire questo metodo su un singolo nodo di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
fipsDrives	Un oggetto JSON contenente lo stato del supporto delle funzionalità FIPS 140-2 per questo nodo. Valori possibili: • Nessuno: il nodo non è compatibile con FIPS. • Parziale: il nodo supporta FIPS, ma non tutte le unità nel nodo sono unità FIPS. • Pronto: il nodo è compatibile con FIPS e tutte le unità nel nodo sono unità FIPS (oppure non sono presenti unità).	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "fipsDrives": "None"
  }
}
```

Nuovo dalla versione

11,5

Ottieni certificato SSL nodo

Puoi usare il `GetNodeSSLCertificate` metodo per recuperare il certificato SSL attualmente attivo sul nodo di gestione.

Parametri



È necessario chiamare questo metodo sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
certificato	Il testo completo del certificato codificato in PEM.	corda
dettagli	Le informazioni decodificate del certificato.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "GetNodeSSLCertificate",
  "params" : {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
```

```

"certificate": "-----BEGIN CERTIFICATE-----
\nMIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSIb3DQEBBQUAMIGDMQswCQYD\nVUzELMAkGA1UECBMCTlYxFTATBgNVBACUFDZlZ2FzLCBCYWJ5ITEhMB8G\nBIYXBWZ5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\nN0YXlzaW4udmVnYXNwHhcNMTcwMzA4MjI1MDI2WhcN\nUEBhMCVVMxCzAJBgNVBAGTAk5WMRUwEwYD\nVnYXNzdGF5c2luLnZl\nnZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f\nnLKQNWEEWMR\nn6akedKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH\nP4\nt6P/Si0aYr4ovx15wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nGZQF3iOsIcBHtLKE5186JVT6j5dg6yjUGQO352ylc9HXHcn6lb/jyl0DmVNU\nmoyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K6lS\nn7dg9cyXu4afXcgKy14JiNBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzx+AC\nDgQWBBRvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrnDJyTsdnEbaGBiasBhjCBgzELMAkG\nZWhcywgQmFieSExITaf\nnBgNVBAoTGFdoYXQgSGFwcGVucyBpbWZlZ2FzZGgkAzBsiFZjjf/MwDAYDVR0T\nnBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s71mQPECwVLfiE/ndtIbnpe\no5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRoIFpX6N\nWvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nERv51g1gua6AE3tBrl0v8q1G4zMJboo3YEwMFwxLkxAFXR\nr4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n10QoQDWNDoTeRBsz80nwiouA==\nn-----END CERTIFICATE-----\n",
    "details": {
        "issuer":
"/C=US/ST=NV/L=Denver/O=NetApp/emailAddress=test@netapptest.org",
        "modulus":
"F14FB6F1F9CB290356116311E9A91E0CAB9E852A52EFDA1D2C68A0235F2A94257F01463964B8EAB138C1BD325546FE38CA809380DAF1DFA53B1473F8B7A3FF4A2D1A62BE28BF1979C03A44337432CB924F07B25E94E07A003EDF9A24F078FDB41D162966F63E533ECB6041429AB829199405DE239221C047B4B284E75F3A2554FA8F9760EB28D41903B7E76CA573D1D71DC9FA95BFE3CA5D0399535467471A430026212DC99A8CB1FB38FF61AE162AAFB64AA4C05FB6D7D05DF01C77D79D99479CCF1F113E4DFFD03E2BA952EDD83D7325EEE1A7D77202B2D78262341BEA6C18E1809B44EFAC80CBAAD31EED313378E376471BF58F2688DCF117E002ABE8AD6B",
        "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

Puoi usare il `GetNodeSupportedTlsCiphers` 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 di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Cifrari obbligatori	Elenco delle suite di cifratura TLS obbligatorie per il nodo. Si tratta di cifrari sempre attivi sul nodo.	corda
defaultSupplementalCiphers	Elenco delle suite di cifratura TLS supplementari predefinite per il nodo. I cifrari supplementari vengono ripristinati in questo elenco quando si esegue il metodo API <code>ResetNodeSupplementalTlsCiphers</code> .	corda
Cifrari supplementari supportati	Elenco delle suite di cifratura TLS supplementari disponibili che è possibile configurare con il metodo API <code>SetNodeSupplementalTlsCiphers</code> .	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeSupportedTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
    ]
  }
}

```

Ottieni informazioni sulla patch

Puoi usare il `GetPatchInfo` metodo per ottenere informazioni sulle patch software Element installate su un nodo di archiviazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
force	Forza l'esecuzione del metodo su tutti i nodi nel cluster di archiviazione. Questa operazione è necessaria 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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
patch	Oggetto contenente informazioni sulle patch installate su questo nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetPatchInfo",
  "params": {
    "force": false,
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
        ]
      }
    }
  }
}
```

Nuovo dalla versione

12,3

Ottieni operazione in sospeso

Puoi usare il `GetPendingOperation` metodo per rilevare un'operazione su un nodo attualmente in corso. Questo metodo può essere utilizzato anche per segnalare il completamento di un'operazione.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
in attesa di	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.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetPendingOperation",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "pendingOperation" : {
      "pending" : "true",
      "operation" : "TestDrivesInternal",
    }
  }
}
```

Nuovo dalla versione

9,6

OttieniSshInfo

Puoi usare il `GetSshInfo` metodo per interrogare lo stato del servizio SSH su un singolo nodo.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
risultato	Lo stato del servizio SSH per questo nodo.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "GetSshInfo",
  "params" : {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "enabled": false
  }
}
```

ListDriveHardware

Puoi usare il `ListDriveHardware` metodo per elencare tutte le unità connesse a un nodo. Se utilizzato su nodi individuali, questo metodo restituisce informazioni sull'hardware dell'unità. Se utilizzato sul nodo master del cluster MVIP, questo metodo restituisce informazioni per tutte le unità su tutti i nodi.

Parametri



La riga "securitySupported": true della risposta del metodo non implica che le unità siano in grado di crittografare; implica solo che è possibile interrogare lo 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 funzionalità di sicurezza su queste unità non riusciranno.

Questo metodo ha il seguente parametro:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare su true per eseguire questo metodo su tutti i nodi.	booleano	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
driveHardware	Restituite informazioni sull'hardware dell'unità per il nodo.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListDriveHardware",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Abilita crittografia a riposo](#)

ListNetworkInterfaces

Puoi usare il `ListNetworkInterfaces` metodo per elencare le informazioni su ciascuna interfaccia di rete su un nodo. Questo metodo API è pensato per essere utilizzato su singoli nodi; per accedere ai singoli nodi è richiesta l'autenticazione tramite ID utente e password. Tuttavia, è possibile utilizzare questo metodo sul cluster se al parametro `force` viene assegnato il valore `true` nella chiamata al metodo. Quando il parametro viene utilizzato sul cluster, vengono elencate tutte le interfacce.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
force	Valori possibili: • <code>true</code>: vengono restituite informazioni su tutte le interfacce di rete nel cluster. • <code>false</code>: non viene restituita alcuna informazione.	booleano	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
interfacce	Un elenco di informazioni di configurazione per ciascuna interfaccia di rete del nodo di archiviazione (o dell'intero cluster di archiviazione, se <code>force = true</code>).	interfaccia di rete <code>vettore</code>

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListNetworkInterfaces",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
            }
          ]
        }
      }
    ]
  }
}
```


Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
networkInterfaceStats	Un elenco di informazioni statistiche di rete, come il numero di pacchetti eliminati e vari tipi di errori di rete, per ciascuna interfaccia di rete di un nodo di archiviazione.	networkInterfaceStats vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListNetworkInterfaceStats",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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
    }
  ]
}

```

Nuovo dalla versione

12,3

ListTests

Puoi usare il `ListTests` metodo per elencare i test disponibili per l'esecuzione su un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
test	Elenco dei test che possono essere eseguiti sul nodo.	matrice di stringhe

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListTests",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "tests": [
      "TestConnectEnsemble",
      "TestConnectMvip",
      "TestConnectSvip",
      "TestDrives",
      "TestHardwareConfig",
      "TestLocateCluster",
      "TestPing",
      "TestLocalConnectivity",
      "TestRemoteConnectivity",
      "TestNetworkConfig"
    ]
  }
}
```

Nuovo dalla versione

9,6

ElencoUtilità

Puoi usare il `ListUtilities` metodo per elencare le operazioni che possono essere eseguite su un nodo.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
utilità	Elenco delle utilità attualmente disponibili per l'esecuzione sul nodo.	matrice di stringhe

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListUtilities",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "utilities": [
      "ResetDrives",
      "ResetNode",
      "RestartNetworking",
      "RestartServices",
      "CreateSupportBundle",
      "DeleteAllSupportBundles",
      "CreateClusterSupportBundle"
    ]
  }
}
```

Nuovo dalla versione

9,6

RemoveNodeSSLCertificate

Puoi usare il RemoveNodeSSLCertificate metodo per rimuovere il certificato SSL

dell'utente e la chiave privata per il nodo di gestione. Dopo aver rimosso 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 sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "RemoveNodeSSLCertificate",
  "params" : {},
  "id" : 3
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 3,
  "result" : {}
}
```

ResetDrives

Puoi usare il `ResetDrives` metodo per inizializzare in modo proattivo le unità e rimuovere tutti i dati attualmente presenti su un'unità. L'unità può quindi essere riutilizzata in un nodo esistente o utilizzata in un nodo aggiornato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
unità	Elenco dei nomi dei dispositivi (non driveID) da reimpostare.	corda	Nessuno	Sì
forza	Impostare su true per reimpostare l'unità.	booleano	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Dettagli delle unità che vengono ripristinate.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ResetDrives",
  "params": {
    "drives" : "slot3",
    "force" : true
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

Reimposta nodo

Puoi usare il `ResetNode` metodo per ripristinare un nodo alle impostazioni di fabbrica. Quando si chiama questo metodo, tutti i dati, i pacchetti (aggiornamenti software, ecc.), le configurazioni e i file di registro vengono eliminati dal nodo. Tuttavia, durante questa operazione le impostazioni di rete del nodo vengono mantenute. I nodi che partecipano a un cluster non possono essere ripristinati alle impostazioni di fabbrica.

Parametri

L'API `ResetNode` può essere utilizzata solo sui nodi che si trovano nello stato "Disponibile". Non può essere utilizzato su nodi che sono "Attivi" in un cluster o in stato "In sospeso".

ATTENZIONE:

Questo metodo cancella tutti i dati dei clienti presenti sul nodo.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
costruire	Utilizzato per specificare l'URL di un'immagine software Element remota su cui verrà reimpostato il nodo.	URL	Nessuno	NO
forza	Impostare su true per reimpostare il nodo.	booleano	Nessuno	Sì
opzioni	Utilizzato per immettere le specifiche per l'esecuzione delle operazioni di reset. Se necessario, i dettagli saranno forniti dal supporto NetApp .	Oggetto JSON	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ResetNode",
  "params": {
    "build" : "file:///sf/rtfi/image/filesystem.squashfs",
    "force" : true
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
}
}
}

```


Nuovo dalla versione

9,6

ResetNodeSupplementalTlsCiphers

Puoi usare il `ResetNodeSupplementalTlsCiphers` metodo per ripristinare l'elenco predefinito dei cifrari TLS supplementari. È possibile utilizzare questo comando sui nodi di gestione.

Parametro



È necessario chiamare questo metodo sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ResetNodeSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Riavviare la rete

Puoi usare il `RestartNetworking` metodo per riavviare i servizi di rete su un nodo.

ATTENZIONE:

Questo metodo riavvia tutti i servizi di rete su un nodo, causando una perdita temporanea della connettività di rete.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare su true per riavviare i servizi di rete su un nodo.	booleano	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RestartNetworking",
  "params": {
    "force" : true
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{ "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Riavvia i servizi

Puoi usare il `RestartServices` metodo per riavviare i servizi su un nodo.

Parametri

ATTENZIONE:

Questo metodo provoca l'interruzione temporanea dei servizi del nodo.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare su true per riavviare i servizi su un nodo.	booleano	Nessuno	Sì
servizio	Nome del servizio da riavviare.	corda	Nessuno	NO
azione	Azione da eseguire sul servizio (avvio, arresto, riavvio).	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
dettagli	L'output della procedura di riavvio del servizio, inclusi gli errori (se presenti).	Oggetto JSON
durata	Tempo, in secondi, impiegato per riavviare i servizi sul nodo.	corda
risultato	Risultati della ripartenza.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RestartServices",
  "params": {
    "force" : true
    "action" : restart,
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "details": "solidfire stop/waiting\nsolidfire start/running, process 7284\n",
    "duration": "00:00:02.541594",
    "result": "Passed"
  }
}
```

Nuovo dalla versione

9,6

ImpostaClusterConfig

Puoi usare il `SetClusterConfig` metodo per impostare la configurazione che un nodo utilizza 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	Necessario
grappolo	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 in questo parametro.	grappolo	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
grappolo	Informazioni di configurazione utilizzate dal nodo per comunicare con il cluster.	grappolo

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetClusterConfig",
  "params": {
    "cluster": {
      "name": "myhost",
      "mipi": "Bond10G"
    },
    "id" : 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
    }
  }
}

```

Nuovo dalla versione

9,6

ImpostaConfig

Puoi usare il `SetConfig` metodo per impostare le informazioni di rete e cluster per il nodo. Questo metodo include le stesse impostazioni in un singolo metodo API che sono disponibili utilizzando entrambi `SetClusterConfig` E `SetNetworkConfig` metodi. Con questo metodo è necessario includere solo i campi che si desidera modificare.

Parametro

ATTENZIONE:

La modifica della modalità di legame 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	Necessario
grappolo	Informazioni sul cluster che identificano il modo in cui il nodo di archiviazione comunica con il cluster di archiviazione a cui è associato.	grappolo	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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
configurazione	La nuova e attuale configurazione del nodo. Questo oggetto contiene: • grappolo: Informazioni sul cluster che identificano il modo in cui il nodo di archiviazione comunica con il cluster di archiviazione 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

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetConfig",
  "params": {
    "cluster": {
      "name": "MyHostname"
    },
    "network": {
      "Bond10G": {
        "bond-mode": "ALB"
      }
    }
  }
}
```

Esempio di risposta

La risposta di questo metodo è la stessa del metodo GetConfig. Quando si utilizza SetConfig, vengono visualizzati tutti i campi per la visualizzazione dell'oggetto e i valori aggiornati.

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [ImpostaClusterConfig](#)
- [ImpostaConfigurazione di Rete](#)
- [OttieniConfig](#)

ImpostaConfigurazione di Rete

Puoi usare il SetNetworkConfig metodo per impostare la configurazione di rete per un nodo. Per visualizzare le impostazioni di rete correnti per un nodo, eseguire il comando GetNetworkConfig Metodo API.

Parametro

ATTENZIONE:

La modifica della modalità di legame 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	Necessario
rete	Un oggetto contenente le impostazioni di rete dei nodi da modificare. È sufficiente aggiungere come attributi in questo parametro i campi che si desidera modificare in questo metodo.	rete (tutte le interfacce)	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
rete	La nuova e attuale configurazione di rete per il nodo.	rete (tutte le interfacce)

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 della risposta del metodo `GetNetworkConfig`. Il metodo visualizza tutti i membri per ciascun oggetto e include i nuovi valori per tutti i membri modificati.

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [OttieniConfigurazione di rete](#)
- [OttieniConfigurazione di rete](#)

SetNodeSSLCertificate

Puoi usare il `SetNodeSSLCertificate` metodo per impostare un certificato SSL utente e una chiave privata per il nodo di gestione.



Dopo aver utilizzato l'API, è necessario riavviare il nodo di gestione.

Parametri



È necessario chiamare questo metodo sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
certificato	Versione di testo codificata PEM del certificato. 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 sui sistemi operativi e sui browser più comuni. Se l'estensione non è presente, l'API rifiuterà il certificato come non valido.	corda	Nessuno	Sì
chiave privata	Versione testuale codificata PEM della chiave privata.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "SetNodeSSLCertificate",
  "params" : {
    "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIEowIBAAKCAQEA8U+28fnLKQNWEMMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovx15wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrpgGZQF3iOSIcBhtLKE5186JVT6j5dg\n6yJUGQO352ylc9HXXcn6lb
/jy10DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
lS7dg9cyXu4afXcgKy14JiNBvqbBjhGJtE\n76yAy6rTHu0xM3jjdkcb9Y8miNzx+ACq+itaw
IDAQABAoIBAHI1j1IZr6/sltqVW\n00qVC/49dyNu+KWVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw9208D2OZvbuOx
k7Put2p6se\nfgNzSjf2SI5DIX3UME5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuH11esIyXXa2hqkU+1+iF2iGRMTiXac4C8d11NU\nWGIR
```

```
"certificate": "-----BEGIN CERTIFICATE-----\n\nmIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqGSib3DQEBBQUAMIGDMQswCQYD\n\nVUuzELMAkGA1UECBMCTlYxFTATBgNVBAcUDFZlZ2FzLCBCYWJ5ITEhMB8G\n\nBIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBfH53\n\nN0YXlzaW4udmVnYXMwHhcNMTCwMzA4MjI1MDI2WhcN\n\nUEBhMCVVMxCzAJBgNVBAGTAk5WMRUwEwYD\n\ndoYXQgSGFwcGVucyBpbWZldhcywgcwQmFieSEExITafBgNVBAoTGF\n\nVnYXNzdGF5c2luLnZl\n\nnLKQNWEWMMR\n\nP4\n\nGZQF3iOsICbHTLKE5186JVT6j5dg6yjUGQO352ylc9HXHCn6lb/jyl0DmVNU\n\nmoyx+zj/Ya4WKq+2SqTAX7bXOF3wHHfXnZlHnm8fet5N/9A+K6lS\n\nNBvqbBjhgtE76yAy6rTHu0xm3jjdkcb9Y8minzx+F+AC\n\nDgQWBBrvvBRPno5S34zGRhrnDJyTsdnEbTCB\n\nDJyTsdnEbaGBiasbhjCBgzELMAkG\n\nZWdhcywgQmFieSEExITaf\n\nVR0T\n\no5geQHCHnNlu5RV9j8ayHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\n\nWvB6zgiAcMRIKqu3DmJ7y3CFGk9dHolQ+WYnoO/eIMy0cot26JB15H\n\nERv5lg1gua6AE3tBrllov8qlG4zMJboo3YEwMFwxLkxAFXR\n\nr4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n\n10QoQDWNDOTeRBsz80nwioUA==\n\n-----END CERTIFICATE-----\n"},
```

```
"id" : 2
```

```
}
```

```
{
  "id" : 2,
  "result" : {}
}
```

SetNodeSupplementalTlsCiphers

Puoi usare il `SetNodeSupplementalTlsCiphers` metodo per specificare l'elenco dei cifrari TLS supplementari. È possibile utilizzare questo comando sui nodi di gestione.

Parametro



È necessario chiamare questo metodo sul nodo di gestione. Per esempio:

```
https://<management node IP>:442/json-rpc/10.0
```

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Cifrari supplementari	I nomi delle suite di cifratura supplementari utilizzano lo schema di denominazione OpenSSL. L'uso dei nomi delle suite di cifratura non distingue tra maiuscole e minuscole.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Cifrari obbligatori	Elenco delle suite di cifratura TLS obbligatorie per il nodo. Si tratta di cifrari sempre attivi sul nodo.	corda
Cifrari supplementari	Elenco delle suite di cifratura TLS supplementari per il nodo.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "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"
    ]
  }
}
```

Fermare

Puoi usare il `Shutdown` metodo per riavviare o arrestare i nodi in un cluster. Utilizzando questo metodo è possibile 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	Necessario
nodi	Elenco dei NodeID per i nodi da riavviare o arrestare.	array di interi	Nessuno	Sì
opzione	Azioni da intraprendere per il cluster. Valori possibili: • restart: riavvia il cluster. • halt: esegue uno spegnimento completo.	corda	ricomincia	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "Shutdown",
  "params": {
    "nodes": [
      2,
      3,
      4
    ],
    "option": "halt"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "failed": [],
    "successful": [
      6
    ]
  }
}
```

Nuovo dalla versione

9,6

TestConnectEnsemble

Puoi usare il `TestConnectEnsemble` metodo per verificare la connettività con un insieme di database specificato. Per impostazione predefinita, utilizza l'ensemble per il cluster a cui è associato il nodo. In alternativa, è possibile fornire un insieme diverso per testare la connettività.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
insieme	Un elenco separato da virgole di indirizzi IP di cluster di nodi ensemble per i test di connettività.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Oggetti restituiti: • <code>nodes</code>: (oggetto) Un elenco di ciascun nodo dell'ensemble nel test e i risultati dei test. • <code>duration</code>: (stringa) Tempo necessario per eseguire il test. • <code>result</code>: (stringa) I risultati dell'intero test.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestConnectEnsemble",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
  }
}
```

Nuovo dalla versione

9,6

TestConnectMvip

Puoi usare il `TestConnectMvip` metodo per testare la connessione di gestione al cluster di archiviazione. Il test esegue il ping dell'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	Necessario
mvip	È possibile passare questo valore per testare la connessione di gestione di un MVIP diverso. Non è necessario utilizzare questo valore quando si testa la connessione al cluster di destinazione.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test (oggetto JSON): • <code>connected</code>: Indica se il test è riuscito a connettersi al MVIP (booleano) • <code>mvip</code>: Il MVIP testato su (stringa) • <code>pingBytes</code>: Dettagli dei test ping con 56 byte e 1500 byte (oggetto) ◦ 56: Risultati del test ping da 56 byte (oggetto JSON): ▪ <code>individualResponseTimes</code>: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ <code>individualStatus</code>: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ <code>responseTime</code>: Tempo medio di risposta al ping (stringa) ▪ <code>successful</code>: Indica se il test ping ha avuto esito positivo (booleano) ◦ 1500: Risultati del test ping da 1500 byte (oggetto JSON): ▪ <code>individualResponseTimes</code>: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ <code>individualStatus</code>: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ <code>responseTime</code>: Tempo medio di risposta al ping (stringa)	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio. Se il test
non ha avuto esito

```
{
  "method": "TestConnectMvip",
  "params": {
    "mvip" : "172.27.62.50"
  },
  "id":1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
}
}

```

Nuovo dalla versione

9,6

TestConnectSvip

Puoi usare il `TestConnectSvip` metodo per testare la connessione di archiviazione al cluster di archiviazione. Il test esegue il ping dell'SVIP tramite pacchetti ICMP e, se ha esito positivo, si connette come iniziatore iSCSI.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
svip	È possibile passare questo valore per testare la connessione di gestione di un SVIP diverso. Non è necessario utilizzare questo valore quando si testa la connessione al cluster di destinazione.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Informazioni sull'operazione di test (oggetto JSON): • <code>connected</code>: Indica se il test è riuscito a connettersi allo SVIP (booleano) • <code>svip</code>: Il test SVIP è stato eseguito su (stringa) • <code>pingBytes</code>: Dettagli dei test ping con 56 byte e 9000 byte (oggetto) ◦ 56: Risultati del test ping da 56 byte (oggetto JSON): ▪ <code>individualResponseTimes</code>: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ <code>individualStatus</code>: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ <code>responseTime</code>: Tempo medio di risposta al ping (stringa) ▪ <code>successful</code>: Indica se il test ping ha avuto esito positivo (booleano) ◦ 9000: Risultati del test ping da 9000 byte (oggetto JSON): ▪ <code>individualResponseTimes</code>: Elenco dei tempi di risposta da ciascun nodo dell'ensemble (array di stringhe) ▪ <code>individualStatus</code>: Elenco dello stato del ping da ciascun nodo dell'ensemble (array booleano) ▪ <code>responseTime</code>: Tempo medio di risposta al ping (stringa)	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio. Indica se il test ping ha avuto successo o no.

```
{
  "method": "TestConnectSvip",
  "params": {
    "svip" : "172.27.62.50"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
}
}

```

Nuovo dalla versione

9,6

Test Drive

Puoi usare il `TestDrives` metodo per eseguire una convalida hardware su tutte le unità sul nodo. Questo metodo rileva i guasti hardware sulle unità e li segnala nei risultati dei test di convalida.

Parametri

Puoi usare solo il `TestDrives` metodo sui nodi che non sono "attivi" in un cluster.



Questo test dura circa 10 minuti.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
forza	Impostare su true per testare le unità sul nodo.	booleano	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
minuti	Specifica il numero di minuti per l'esecuzione del test.	intero	10	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Informazioni sul successo o sul fallimento dell'operazione di test.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestDrives",
  "params": {
    "force": true,
    "minutes" : 10
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una tabella contenente i risultati dei test per ciascuna unità nel nodo.

Nuovo dalla versione

9,6

TestHardwareConfig

Puoi usare il `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 tutte le unità.

Parametri



Questi test non sono pensati per rilevare guasti hardware.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
pulito	Avvia il test di configurazione hardware con una cache pulita. Valori possibili: • true: elimina il file dei risultati dei test memorizzati nella cache e riesegue i test. • false: recupera i risultati dei test memorizzati nella cache.	booleano	falso	NO
forza	Per ripristinare correttamente il nodo, è necessario includere il parametro force in questo metodo.	booleano	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Dettagli sulla configurazione hardware.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestHardwareConfig",
  "params": {
    "force": true
  },
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[TestHardwareConfig](#)

TestLocateCluster

Puoi usare il `TestLocateCluster` metodo per convalidare che il nodo possa 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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Informazioni sul successo o sul fallimento dell'operazione di test.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestLocateCluster",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
  }
}

```

Nuovo dalla versione

9,6

TestLocalConnectivity

Puoi usare il `TestLocalConnectivity` metodo per effettuare il ping dell'IP del cluster (CIP) di ciascun nodo in un cluster attivo.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Tempi di risposta ping individuali per ciascun nodo nel cluster locale attivo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestLocalConnectivity",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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"
}
}

```

Nuovo dalla versione

9,6

TestNetworkConfig

Puoi usare il `TestNetworkConfig` metodo per verificare che le impostazioni di rete configurate corrispondano alle impostazioni di rete utilizzate sul sistema.

Parametri

Quando si configura un nodo con il metodo `SetNetworkConfig`, nell'interfaccia utente o nell'interfaccia utente terminale, la configurazione viene convalidata e memorizzata. Il test API `TestNetworkConfig` utilizza la configurazione memorizzata per la logica di post-validazione. Ad esempio, in caso di interruzione di corrente o di guasto della rete, è possibile utilizzare questo metodo API per garantire che un nodo funzioni con la configurazione di rete più recente. Ciò convalida che non ci sono errori nella configurazione e che la configurazione corrente è in uso.

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 i seguenti esempi di risposta.

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Contiene tutti gli errori rilevati durante la convalida delle impostazioni di rete attualmente memorizzate con la configurazione di rete in esecuzione.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 dell'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"
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Imposta Configurazione di Rete](#)

TestPing

Puoi usare il `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	Necessario
tentativi	Specifica il numero di volte in cui il sistema deve ripetere il ping di prova.	intero	5	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ospiti	Specifica un elenco separato da virgole di indirizzi o nomi host di dispositivi da sottoporre a ping. Se non viene specificato alcun host, il metodo esegue il ping degli host nel cluster di archiviazione.	corda	Nessuno	NO
interfaccia	L'interfaccia (base) esistente da cui devono essere inviati i ping. Valori possibili: • Bond10G: Invia ping dall'interfaccia Bond10G. • Bond1G: Invia ping dall'interfaccia Bond1G.	corda	Nessuno	NO
dimensione del pacchetto	Specifica il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore all'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
proibire la frammentazione	Abilita il flag DF (Do not Fragment) per i pacchetti ICMP.	booleano	falso	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
sourceAddressV4	L'indirizzo IPv4 di origine da utilizzare nei pacchetti ping ICMP.	corda	Nessuno	NO
sourceAddressV6	L'indirizzo IPv6 di origine da utilizzare nei pacchetti ping ICMP.	corda	Nessuno	NO
timeout totaleSec	Specifica il tempo in secondi che il ping deve attendere per una risposta del sistema prima di emettere il successivo tentativo di ping o di terminare il processo.	intero	5	NO
virtualNetworkTag	ID VLAN da utilizzare durante l'invio dei pacchetti ping.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Elenco di tutti gli IP con cui il nodo è riuscito a comunicare e statistiche di risposta al ping.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestPing",
  "params": {
    "interface": "Bond1G",
    "hosts": "192.168.0.1"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
  }
}

```

Nuovo dalla versione

5,0

TestRemoteConnectivity

Puoi usare `TestRemoteConnectivity` metodo per effettuare il ping di ciascun nodo del cluster remoto e verificare la connessione al database dell'ensemble remoto. Per

ottenere risultati utili con questo metodo, i cluster devono essere accoppiati. Se la connessione al database remoto fallisce, la risposta del sistema elenca le eccezioni.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
dettagli	Tempi di risposta ping individuali per ciascun nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestRemoteConnectivity",
  "params": {
    "force": "true"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
}
}

```

Nuovo dalla versione

9,6

Metodi API di replicazione

Ordine delle operazioni di accoppiamento dei cluster

Prima di poter utilizzare la replica remota, è necessario stabilire una connessione tra una coppia di cluster di archiviazione che eseguono il software Element.

Utilizzare il seguente set di metodi API per stabilire una connessione al cluster:

- [StartClusterPairing](#):

Questo metodo API crea e restituisce una chiave di associazione utilizzata per stabilire una coppia di cluster. La chiave è codificata e contiene informazioni utilizzate per stabilire comunicazioni tra cluster. Un singolo cluster può essere abbinato ad altri quattro cluster. Tuttavia, per ogni associazione di cluster deve essere generata una nuova chiave. Il [StartClusterPairing](#) Il metodo genera una nuova chiave ogni volta che viene chiamato. Utilizzare ogni chiave univoca con il [CompleteClusterPairing](#) metodo per associare ogni cluster aggiuntivo.



Per motivi di sicurezza, la chiave di associazione non deve essere inviata ad altri utenti via e-mail. La chiave contiene un nome utente e una password.

- [CompleteClusterPairing](#):

Questo metodo utilizza la chiave di associazione creata con [StartClusterPairing](#) Metodo API per creare una coppia di cluster. Emettere il [CompleteClusterPairing](#) Metodo API con il parametro clusterPairingKey alla destinazione. Il cluster di origine è il cluster che ha creato la chiave.

Trova maggiori informazioni

- [StartClusterPairing](#)
- [CompleteClusterPairing](#)

Ordine di accoppiamento dei volumi delle operazioni

Prima di poter associare i volumi, è necessario creare una coppia di cluster tra due cluster corrispondenti.

Utilizzare il seguente set di metodi API per stabilire una connessione al cluster:

- [StartVolumePairing](#):

Questo metodo API crea e restituisce una chiave di associazione del volume utilizzata per creare una coppia di volumi. La chiave contiene informazioni utilizzate per stabilire comunicazioni tra volumi.

- [CompleteVolumePairing](#):

Questo metodo utilizza la chiave di associazione creata con [StartVolumePairing](#) Metodo API per creare una coppia di volumi. Emettere 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 il [Modifica coppia di volumi](#) Metodo API per stabilire la direzione della replicazione dei dati del volume identificando quale volume è la destinazione. I dati vengono replicati dal volume di origine al volume di destinazione.

Trova maggiori informazioni

- [StartVolumePairing](#)
- [CompleteVolumePairing](#)
- [Modifica coppia di volumi](#)

Modalità di replica supportate per cluster accoppiati

Nei cluster accoppiati sono supportate le seguenti modalità di replicazione:

- 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 del sistema viene inviata all'host e i dati vengono inviati al volume di destinazione della replica.

- Replica dei dati solo tramite snapshot: solo gli snapshot del volume vengono replicati sul cluster di destinazione.

CompleteClusterPairing

IL CompleteClusterPairing Il metodo è il secondo passaggio nel processo di associazione dei cluster. Utilizzare questo metodo con la chiave codificata ricevuta dal StartClusterPairing metodo per completare il processo di associazione dei cluster.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
clusterPairingKey	Una stringa di caratteri restituita da StartClusterPairing Metodo API.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
clusterPairID	Identificatore univoco per la coppia di cluster.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CompleteClusterPairing",
  "params": {
    "clusterPairingKey" :
    "7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d37343536366139353364326
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "clusterPairID" : 1
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[StartClusterPairing](#)

CompleteVolumePairing

Puoi usare `CompleteVolumePairing` per completare l'abbinamento dei due volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	L'ID del volume che completerà la coppia di volumi.	intero	Nessuno	Sì
volumePairingKey	La chiave restituita dal StartVolumePairing Metodo API.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CompleteVolumePairing",
  "params": {
    "volumeID" : 12,
    "volumePairingKey" :
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223
a2231636561313336322d346338662d343631612d626537322d37343536366139353364326
6222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a22313
9322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755
2222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c227270634
36f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5
f53465f706169725f50597a796647704c7246564432444a42227d"
    },
    "id" : 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[StartVolumePairing](#)

ListClusterPairs

Puoi usare il `ListClusterPairs` metodo per elencare tutti i cluster associati al cluster corrente. Questo metodo restituisce informazioni sulle coppie di cluster attive e in sospeso, come statistiche sulla coppia corrente, nonché sulla connettività e sulla latenza (in millisecondi) della coppia di cluster.

Parametro

Questo metodo non ha parametri di input:

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
clusterPairs	Informazioni su ciascun cluster accoppiato.	clusterPair vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListClusterPairs",
  "params": {
    },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "id": 1,
  "result": {
    "clusterPairs": [
      {
        "clusterName": "cluster2",
        "clusterPairID": 3,
        "clusterPairUUID": "9866fbef-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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListActivePairedVolumes

Puoi usare il `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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumi	Informazioni sul volume per i volumi accoppiati.	volumePair vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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": "306f746f000000018f47acc01000000000",
"scsiNAADeviceID": "6f47acc1000000000306f746f000000018",
"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"
    }
]
}
}
}
}

```

Nuovo dalla versione

9,6

Modifica coppia di volumi

Puoi usare il `ModifyVolumePair` metodo per mettere in pausa o riavviare la replica tra una coppia di volumi. Questo metodo viene impostato sul volume sorgente (il volume con accesso in lettura/scrittura).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	Numero identificativo del volume da modificare.	intero	Nessuno	Sì
in pausaManuale	La replica remota può essere sospesa o riavviata sul volume di origine (lettura/scrittura). Valori possibili: • vero: sospendi la replica del volume. • false: riavvia la replica del volume. Se non viene specificato alcun valore, non verrà eseguita alcuna modifica nella replica.	booleano	Nessuno	NO

modalità	Modalità di replica del volume. Valori possibili: • Asincrono: le scritture vengono riconosciute quando vengono completate localmente. Il cluster non attende che le scritture vengano replicate sul cluster di destinazione. • Sincronizzazione: la sorgente riconosce la scrittura quando i dati vengono archiviati localmente e sul cluster remoto. • SnapshotsOnly: vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.	corda	Nessuno	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyVolumePair",
  "params": {
    "pausedManual": false,
    "volumeID": 5,
    "mode": "sync"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

RimuoviClusterPair

Puoi usare il `RemoveClusterPair` metodo per chiudere le connessioni aperte tra due cluster accoppiati.

Parametro



Prima di rimuovere una coppia di cluster, è necessario rimuovere tutte le coppie di volumi dai cluster con il metodo API `RemoveVolumePair`.

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
clusterPairID	Identificatore univoco utilizzato per associare due cluster.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveClusterPair",
  "params": {
    "clusterPairID": 1
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

RemoveVolumePair

Puoi usare il `RemoveVolumePair` metodo per rimuovere l'associazione remota tra due volumi. Utilizzare questo metodo sia sui volumi di origine che su quelli di destinazione abbinati. Quando si rimuovono le informazioni di associazione del volume, i dati non vengono più replicati da o verso il volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	ID del volume su cui arrestare il processo di replica.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveVolumePair",
  "params": {
    "volumeID": 5
  }
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
  }
}
```

Nuovo dalla versione

9,6

StartClusterPairing

Puoi usare il `StartClusterPairing` Metodo per creare una chiave codificata da un cluster che viene utilizzata per l'associazione con un altro cluster. La chiave creata da questo metodo API viene utilizzata in `CompleteClusterPairing` metodo per stabilire un accoppiamento di cluster. È possibile associare un cluster a un massimo di altri quattro cluster.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
clusterPairingKey	Una stringa di caratteri utilizzata da CompleteClusterPairing Metodo API.	corda

Nome	Descrizione	Tipo
clusterPairID	Identificatore univoco per la coppia di cluster.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "StartClusterPairing",
  "params": {
    },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "clusterPairID": 1,
    "clusterPairingKey":
"7b22636c7573746572506169724944223a312c22636c75737465725061697255554944223a2231636561313336322d346338662d343631612d626537322d373435363661393533643266222c22636c7573746572556e697175654944223a2278736d36222c226d766970223a223139322e3136382e3133392e313232222c226e616d65223a224175746f54657374322d6330755222c2270617373776f7264223a22695e59686f20492d64774d7d4c67614b222c22727063436f6e6e656374696f6e4944223a3931333134323634392c22757365726e616d65223a225f5f53465f706169725f50597a796647704c7246564432444a42227d"
    }
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[CompleteClusterPairing](#)

StartVolumePairing

Puoi usare il StartVolumePairing Metodo per creare una chiave codificata da un

volume che viene utilizzato per l'associazione con un altro volume. La chiave che questo metodo crea viene utilizzata nel `CompleteVolumePairing` metodo per stabilire un accoppiamento di volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
modalità	Modalità del volume su cui avviare il processo di associazione. La modalità può essere impostata solo se il volume è quello della sorgente. Valori possibili: • Async: Le scritture vengono riconosciute quando vengono completate localmente. Il cluster non attende che le scritture vengano replicate sul cluster di destinazione. (Predefinito se non è specificato alcun parametro di modalità.) • Sync: La sorgente riconosce la scrittura quando i dati vengono archiviati localmente e sul cluster remoto. • SnapshotsOnly: Vengono replicati solo gli snapshot creati sul cluster di origine. Le scritture attive dal volume di origine non vengono replicate.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	ID del volume su cui avviare il processo di associazione.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumePairingKey	Una stringa di caratteri utilizzata da CompleteVolumePairing Metodo API.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "StartVolumePairing",
  "params": {
    "mode": "Async",
    "volumeID" : 14
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "volumePairingKey" :
    "7b226d766970223a223139322e3136382e3133392e313232222c22766f6c756d654944223
    a312c22766f6c756d654e616d65223a2254657374222c22766f6c756d65506169725555494
    4223a2236393632346663622d323032652d343332352d613536392d6563396336353563376
    23561227d"
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[CompleteVolumePairing](#)

Metodi API di sicurezza

AggiungiKeyServerAuthProviderKmip

Puoi usare il `AddKeyServerToAuthProviderKmip` metodo per assegnare un server di chiavi KMIP (Key Management Interoperability Protocol) al fornitore di chiavi specificato. Durante l'assegnazione, il server viene contattato per verificarne la funzionalità. Se il server delle chiavi specificato è già assegnato al fornitore delle chiavi specificato, non viene intrapresa alcuna azione e non viene restituito alcun errore. È possibile rimuovere l'assegnazione utilizzando `RemoveKeyServerFromAuthProviderKmip` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	ID del fornitore delle chiavi a cui assegnare il server delle chiavi.	intero	Nessuno	Sì
ID del server chiave	L'ID del server delle chiavi da assegnare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valore di ritorno. L'assegnazione è considerata riuscita finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "AddKeyServerToProviderK mip",
  "params": {
    "keyProviderID": 1,
    "keyServerID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

CreateKeyProviderK mip

Puoi usare il `CreateKeyProviderK mip` metodo per creare un fornitore di chiavi KMIP (Key Management Interoperability Protocol) con il nome specificato. Un fornitore di chiavi definisce un meccanismo e una posizione per recuperare le chiavi di autenticazione. Quando si crea un nuovo fornitore di chiavi KMIP, non gli viene assegnato alcun server di chiavi KMIP. Per creare un server di chiavi KMIP, utilizzare `CreateKeyServerK mip` metodo. Per assegnarlo a un fornitore, vedere `AddKeyServerToProviderK mip` .

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome del fornitore di chiavi	Nome da associare al fornitore di chiavi KMIP creato. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProvider	Un oggetto contenente dettagli sul fornitore di chiavi appena creato.	"Fornitore di chiaviKmp"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateKeyProviderKmp",
  "params": {
    "keyProviderName": "ProviderName",
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "kmipKeyProvider": {
      "keyProviderName": "ProviderName",
      "keyProviderIsActive": true,
      "kmipCapabilities": "SSL",
      "keyServerIDs": [
        15
      ],
      "keyProviderID": 1
    }
  }
}
```

Nuovo dalla versione

11,7

CreateKeyServerKmip

Puoi usare il `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 poter utilizzare questo metodo. Per le configurazioni di server chiave in cluster, è necessario fornire i nomi host o gli indirizzi IP di tutti i nodi del server nel parametro `kmipKeyServerHostnames`. Puoi usare il `TestKeyServerKmip` metodo per testare un server di chiavi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipCaCertificate	Il certificato della chiave pubblica della CA radice del server delle chiavi esterno. Verrà utilizzato per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server chiave in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati radice di tutte le CA.	corda	Nessuno	Sì
kmipClientCertificate	Un certificato PKCS#10 X.509 codificato Base64 in formato PEM utilizzato dal client Solidfire KMIP.	corda	Nessuno	Sì
kmipKeyServerHost names	Matrice dei nomi host o degli indirizzi IP associati a questo server di chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server chiave sono in una configurazione cluster.	matrice di stringhe	Nessuno	Sì
kmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipKeyServerPort	Il numero di porta associato a questo server di chiavi KMIP (in genere 5696).	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServer	Un oggetto contenente dettagli sul server delle chiavi appena creato.	"KeyServerKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "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
    }
  }
}
```

Nuovo dalla versione

11,7

Crea coppia di chiavi pubbliche e private

Puoi usare il `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 archiviazione 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	Necessario
Nome comune	Il campo Nome comune del nome distinto X.509 (CN).	corda	Nessuno	NO
Paese	Il campo Paese del nome distinto X.509 ©.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
indirizzo e-mail	Il campo Indirizzo e-mail del nome distinto X.509 (MAIL).	corda	Nessuno	NO
località	Il campo Nome località del nome distinto X.509 (L).	corda	Nessuno	NO
organizzazione	Il campo Nome organizzazione del nome distinto X.509 (O).	corda	Nessuno	NO
unità organizzativa	Il campo Nome unità organizzativa (OU) del nome distinto X.509.	corda	Nessuno	NO
stato	Il campo Stato o Nome della provincia del nome distinto X.509 (ST o SP o S).	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno. Se non si verificano errori, la creazione della chiave è considerata riuscita.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreatePublicPrivateKeyPair",
  "params": {
    "commonName": "Name",
    "country": "US",
    "emailAddress" : "email@domain.com"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

DeleteKeyProviderKmip

Puoi usare il `DeleteKeyProviderKmip` metodo per eliminare il fornitore di chiavi KMIP (Key Management Interoperability Protocol) inattivo specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	L'ID del fornitore della chiave da eliminare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno. L'operazione di eliminazione è considerata riuscita finché non si verificano errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteKeyProviderKmip",
  "params": {
    "keyProviderID": "1"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

DeleteKeyServerKmip

Puoi usare il `DeleteKeyServerKmip` metodo per eliminare un server di chiavi KMIP (Key Management Interoperability Protocol) esistente. È possibile eliminare un server di chiavi a meno che non sia l'ultimo assegnato al suo provider e che il provider fornisca chiavi attualmente in uso.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP da eliminare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno. L'operazione di eliminazione è considerata riuscita se non si verificano errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteKeyServerKmip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

Disabilita la crittografia a riposo

Puoi usare il `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 disabilitata. Puoi usare il `GetClusterInfo` metodo per interrogare il sistema per vedere quando il processo è stato completato.



- Non è possibile utilizzare questo metodo per disattivare la crittografia software a riposo. Per disabilitare la crittografia software a riposo, è necessario ["creare un nuovo cluster"](#) con la crittografia software a riposo disabilitata.
- Per visualizzare lo stato corrente della crittografia a riposo, della crittografia software a riposo o di entrambe sul cluster, utilizzare ["metodo per ottenere informazioni sul cluster"](#). Puoi usare il `GetSoftwareEncryptionAtRestInfo` ["metodo per ottenere informazioni che il cluster utilizza per crittografare i dati a riposo"](#).

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- ["Ottieni informazioni sul cluster"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Abilita crittografia a riposo

Puoi usare il `EnableEncryptionAtRest` metodo per abilitare la crittografia Advanced Encryption Standard (AES) a 256 bit a riposo sul cluster, in modo che il cluster possa gestire la chiave di crittografia utilizzata per le unità su ciascun nodo. Questa funzione non è abilitata per impostazione predefinita.



- Per visualizzare lo stato corrente della crittografia a riposo e/o della crittografia software a riposo sul cluster, utilizzare ["metodo per ottenere informazioni sul cluster"](#). Puoi usare il `GetSoftwareEncryptionAtRestInfo` ["metodo per ottenere informazioni che il cluster utilizza per crittografare i dati a riposo"](#).
- Questo metodo non abilita la crittografia software a riposo. Questo può essere fatto solo utilizzando il ["metodo di creazione del cluster"](#) con `enableSoftwareEncryptionAtRest` impostato su `true`.

Quando si abilita la crittografia a riposo, il cluster gestisce automaticamente le chiavi di crittografia internamente per le unità su ciascun nodo del cluster.

Se viene specificato un `keyProviderID`, la password viene generata e recuperata in base al tipo di fornitore di chiavi. In genere, questa operazione viene eseguita utilizzando un server di chiavi KMIP (Key Management Interoperability Protocol) nel caso di un fornitore di chiavi KMIP. Dopo questa operazione, il provider specificato viene considerato attivo e non può essere eliminato finché la crittografia a riposo non viene disabilitata utilizzando `DisableEncryptionAtRest` metodo.



Se si dispone di un tipo di nodo con un numero di modello che termina con "-NE", il `EnableEncryptionAtRest` la chiamata al metodo fallirà con una risposta del tipo "Crittografia non consentita". Il cluster ha rilevato un nodo non crittografabile".



È opportuno abilitare o disabilitare la crittografia solo quando il cluster è in esecuzione e in buono stato. Puoi abilitare o disabilitare la crittografia a tua discrezione e tutte le volte che ne hai bisogno.



Questo processo è asincrono e restituisce una risposta prima che la crittografia venga abilitata. Puoi usare il `GetClusterInfo` metodo per interrogare il sistema per vedere quando il processo è stato completato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	L'ID di un fornitore di chiavi KMIP da utilizzare.	intero	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableEncryptionAtRest",
  "params": {},
  "id": 1
}
```

Esempi di risposta

Questo metodo restituisce una risposta simile al seguente esempio dal metodo `EnableEncryptionAtRest`. Non ci sono risultati da segnalare.

```
{
  "id": 1,
  "result": {}
}
```

Quando la crittografia a riposo è abilitata su un cluster, `GetClusterInfo` restituisce un risultato che descrive lo stato della crittografia a riposo (`"encryptionAtRestState"`) come `"abilitato"`. Dopo che la crittografia a riposo è completamente abilitata, lo stato restituito cambia in `"abilitato"`.

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- ["SecureEraseDrives"](#)
- ["Ottieni informazioni sul cluster"](#)
- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Ottieni richiesta di firma del certificato del client

Puoi usare il `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 fiducia per l'interazione con servizi esterni.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
clientCertificateSignRequest	Una richiesta di firma del certificato client PKCS#10 X.509 codificato in formato PEM Base64.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClientCertificateSignRequest",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "clientCertificateSignRequest":
    "MIIBYjCCATMCAQAwgYkxCzAJBgNVBAYTA1VTMRMwEQYDVQQIEwpDYWxpZm9ybm..."
  }
}
```

Nuovo dalla versione

11,7

GetKeyProviderKmp

Puoi usare il `GetKeyProviderKmp` metodo per recuperare informazioni sul fornitore di chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID fornitore di chiavi	ID dell'oggetto fornitore di chiavi KMIP da restituire.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProvider	Un oggetto contenente dettagli sul fornitore della chiave richiesto.	"Fornitore di chiaviKnip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetKeyProviderKnip",
  "params": {
    "keyProviderID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id": 1,
  "result":
  {
    "kmipKeyProvider": {
      "keyProviderID": 15,
      "kmipCapabilities": "SSL",
      "keyProviderIsActive": true,
      "keyServerIDs": [
        1
      ],
      "keyProviderName": "ProviderName"
    }
  }
}

```

Nuovo dalla versione

11,7

GetKeyServerKmp

Puoi usare il `GetKeyServerKmp` metodo per restituire informazioni sul server delle chiavi KMIP (Key Management Interoperability Protocol) specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP su cui restituire informazioni.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
<code>kmipKeyServer</code>	Un oggetto contenente dettagli sul server delle chiavi richiesto.	"KeyServerKmp"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetKeyServerKnip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    }
  }
}
```

Nuovo dalla versione

11,7

Ottieni informazioni sulla crittografia software a riposo

Puoi usare il `GetSoftwareEncryptionAtRestInfo` Metodo per ottenere informazioni sulla crittografia software a riposo che il cluster utilizza per crittografare i dati a riposo.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Parametro	Descrizione	Tipo	Opzionale
masterKeyInfo	Informazioni sulla chiave master di crittografia a riposo del software corrente.	EncryptionKeyInfo	VERO
rekeyMasterKeyAsyncResultID	ID del risultato asincrono dell'operazione di reimpostazione delle chiavi corrente o più recente (se presente), se non è stata ancora eliminata. GetAsyncResult l'output includerà un newKey campo che contiene informazioni sulla nuova chiave principale e un keyToDecommission campo che contiene informazioni sulla vecchia chiave.	intero	VERO
stato	Stato attuale della crittografia software a riposo. I valori possibili sono disabled O enabled .	corda	Falso
versione	Numero di versione che viene incrementato ogni volta che viene abilitata la crittografia software a riposo.	intero	Falso

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{  
  "method": "getsoftwareencryptionatrestinfo"  
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "masterKeyInfo": {
      "keyCreatedTime": "2021-09-20T23:15:56Z",
      "keyID": "4d80a629-a11b-40ab-8b30-d66dd5647cfd",
      "keyManagementType": "internal"
    },
    "state": "enabled",
    "version": 1
  }
}
```

Nuovo dalla versione

12,3

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

ListKeyProvidersKmip

Puoi usare il `ListKeyProvidersKmip` metodo per recuperare un elenco di tutti i fornitori 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	Necessario
keyProviderIsActive	I filtri hanno restituito oggetti server chiave KMIP in base al loro stato attivo. Valori possibili: • true: restituisce solo i provider di chiavi KMIP attivi (che forniscono chiavi attualmente in uso). • false: restituisce solo i provider di chiavi KMIP inattivi (che non forniscono chiavi e possono essere eliminati). Se omissso, i provider di chiavi KMIP restituiti non vengono filtrati in base al fatto che siano attivi.	booleano	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipKeyProviderHasServerAssigned	I filtri hanno restituito i provider di chiavi KMIP in base al fatto che abbiano o meno un server di chiavi KMIP assegnato. Valori possibili: • true: restituisce solo i provider di chiavi KMIP a cui è assegnato un server di chiavi KMIP. • false: restituisce solo i provider di chiavi KMIP a cui non è assegnato un server di chiavi KMIP. Se omissso, 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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyProviders	Un elenco dei fornitori di chiavi KMIP che sono stati creati.	"Fornitore di chiaviKmp"vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListKeyProvidersKmip",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
  {
    "kmipKeyProviders": [
      {
        "keyProviderID": 15,
        "kmipCapabilities": "SSL",
        "keyProviderIsActive": true,
        "keyServerIDs": [
          1
        ],
        "keyProviderName": "KeyProvider1"
      }
    ]
  }
}
```

Nuovo dalla versione

11,7

ListKeyServersKmip

Puoi usare il `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	Necessario
ID fornitore di chiavi	Se specificato, il metodo restituisce solo i server delle chiavi KMIP assegnati al provider delle chiavi KMIP specificato. Se omissso, i server delle chiavi KMIP restituiti non verranno filtrati in base al fatto che siano assegnati o meno al fornitore di chiavi KMIP specificato.	intero	Nessuno	NO
kmipAssignedProvidersActive	I filtri hanno restituito oggetti server chiave KMIP in base al loro stato attivo. Valori possibili: • true: restituisce solo i server delle chiavi KMIP attivi (che forniscono le chiavi attualmente in uso). • false: restituisce solo i server delle chiavi KMIP inattivi (che non forniscono chiavi e possono essere eliminati). Se omissso, i server delle chiavi KMIP restituiti non vengono filtrati in base al fatto che siano attivi o meno.	booleano	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
kmipHasProviderAs signed	I filtri hanno restituito i server delle chiavi KMIP in base all'assegnazione o meno di un fornitore di chiavi KMIP. Valori possibili: • true: restituisce solo i server di chiavi KMIP a cui è assegnato un provider di chiavi KMIP. • false: restituisce solo i server di chiavi KMIP a cui non è assegnato un provider di chiavi KMIP. Se omissso, 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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServers	L'elenco completo dei server chiave KMIP che sono stati creati.	"KeyServerKmp" vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListKeyServersKmip",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "kmipKeyServers": [
    {
      "kmipKeyServerName": "keyserverName",
      "kmipClientCertificate": "dKkkirWmnWXbj9T/UWZYB2oK0z5...",
      "keyServerID": 15,
      "kmipAssignedProviderIsActive": true,
      "kmipKeyServerPort": 5696,
      "kmipCaCertificate": "MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/E...",
      "kmipKeyServerHostnames": [
        "server1.hostname.com", "server2.hostname.com"
      ],
      "keyProviderID": 1
    }
  ]
}
```

Nuovo dalla versione

11,7

ModifyKeyServerKmip

Puoi usare il `ModifyKeyServerKmip` metodo per modificare un server di chiavi KMIP (Key Management Interoperability Protocol) esistente con gli attributi specificati. Sebbene l'unico parametro obbligatorio sia `keyServerID`, una richiesta contenente solo `keyServerID` non eseguirà alcuna azione e non restituirà alcun errore. Tutti gli altri parametri specificati sostituiranno i valori esistenti per il server delle chiavi con il `keyServerID` specificato. Durante l'operazione viene contattato il server delle chiavi per verificarne il funzionamento. È possibile specificare più nomi host o indirizzi IP con il parametro `kmipKeyServerHostnames`, ma solo se i server chiave sono in una configurazione in cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server chiavi KMIP da modificare.	intero	Nessuno	Sì
kmipCaCertificate	Il certificato della chiave pubblica della CA radice del server delle chiavi esterno. Verrà utilizzato per verificare il certificato presentato dal server delle chiavi esterno nella comunicazione TLS. Per i cluster di server chiave in cui i singoli server utilizzano CA diverse, fornire una stringa concatenata contenente i certificati radice di tutte le CA.	corda	Nessuno	NO
kmipClientCertificate	Un certificato PKCS#10 X.509 codificato Base64 in formato PEM utilizzato dal client Solidfire KMIP.	corda	Nessuno	NO
kmipKeyServerHost names	Matrice dei nomi host o degli indirizzi IP associati a questo server di chiavi KMIP. È necessario fornire più nomi host o indirizzi IP solo se i server chiave sono in una configurazione cluster.	matrice di stringhe	Nessuno	NO

kmipKeyServerName	Il nome del server delle chiavi KMIP. Questo nome viene utilizzato solo a scopo di visualizzazione e non deve essere univoco.	corda	Nessuno	NO
kmipKeyServerPort	Il numero di porta associato a questo server di chiavi KMIP (in genere 5696).	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
kmipKeyServer	Un oggetto contenente dettagli sul server delle chiavi appena modificato.	"KeyServerKmip"

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:


```
{
  "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
    }
  }
}
```

Nuovo dalla versione

11,7

RekeySoftwareEncryptionAtRestMasterKey

Puoi usare il `RekeySoftwareEncryptionAtRestMasterKey` Metodo per ricodificare la chiave master di crittografia software a riposo utilizzata per crittografare le DEK (chiavi di crittografia dei dati). Durante la creazione del cluster, la crittografia software a riposo viene configurata per utilizzare Internal Key Management (IKM). Questo metodo di reimpostazione delle chiavi 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` Se il parametro non è specificato, l'operazione di reimpostazione delle chiavi viene eseguita utilizzando la configurazione di gestione delle chiavi esistente. Se il `keyManagementType` è specificato e il fornitore della chiave è esterno, il `keyProviderID` deve essere utilizzato anche il parametro.

Parametro	Descrizione	Tipo	Opzionale
Tipo di gestione delle chiavi	Tipo di gestione delle chiavi utilizzato per gestire la chiave principale. I valori possibili sono: <code>Internal</code> : Reimpostare la chiave utilizzando la gestione delle chiavi interne. <code>External</code> : Reimpostare la chiave utilizzando la gestione delle chiavi esterne. Se questo parametro non viene specificato, l'operazione di reimpostazione delle chiavi viene eseguita utilizzando la configurazione di gestione delle chiavi esistente.	corda	VERO
ID fornitore di chiavi	L'ID del fornitore della chiave da utilizzare. Questo è un valore univoco restituito come parte di uno dei <code>CreateKeyProvider</code> metodi. L'ID è richiesto solo quando <code>keyManagementType</code> È <code>External</code> e non è altrimenti valido.	intero	VERO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Parametro	Descrizione	Tipo	Opzionale
asyncHandle	Determinare lo stato dell'operazione di reimpostazione delle chiavi utilizzando questo asyncHandle valore con GetAsyncResult . GetAsyncResult l'output includerà un newKey campo che contiene informazioni sulla nuova chiave principale e un keyToDecommission campo che contiene informazioni sulla vecchia chiave.	intero	Falso

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "rekeysoftwareencryptionatrestmasterkey",
  "params": {
    "keyManagementType": "external",
    "keyProviderID": "<ID number>"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "asyncHandle": 1
}
```

Nuovo dalla versione

12,3

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

RemoveKeyServerFromProviderKmip

Puoi usare il `RemoveKeyServerFromProviderKmip` metodo per annullare l'assegnazione del server delle chiavi KMIP (Key Management Interoperability Protocol) specificato al provider a cui era assegnato. È possibile annullare l'assegnazione di un server di chiavi al suo provider, a meno che non sia l'ultimo e il suo provider sia attivo (che fornisce chiavi attualmente in uso). Se il server delle chiavi specificato non è assegnato a un provider, non viene intrapresa alcuna azione e non viene restituito alcun errore.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID del server chiave	ID del server delle chiavi KMIP da annullare l'assegnazione.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno. La rimozione è considerata riuscita finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveKeyServerFromProviderKmip",
  "params": {
    "keyServerID": 1
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

SignSshKeys

Dopo che SSH è abilitato sul cluster utilizzando "[Metodo EnableSSH](#)", puoi usare il `SignSshKeys` metodo per ottenere l'accesso a una shell su un nodo.

A partire dall'elemento 12.5, `sfreadonly` è un nuovo account di sistema che consente la risoluzione dei problemi di base su un nodo. Questa API consente l'accesso SSH utilizzando `sfreadonly` account di sistema su tutti i nodi del cluster.



Salvo diversa indicazione da parte del supporto NetApp, qualsiasi modifica al sistema non è supportata, invalidando il contratto di supporto e potendo causare instabilità o inaccessibilità dei dati.

Dopo aver utilizzato il metodo, è necessario copiare il portachiavi dalla risposta, salvarlo sul sistema che avvierà la connessione SSH, quindi eseguire il seguente comando:

```
ssh -i <identity_file> sfreadonly@<node_ip>
```

``identity_file`` è un file da cui viene letta l'identità (chiave privata) per l'autenticazione con chiave pubblica e ``node_ip`` è l'indirizzo IP del nodo. Per maggiori informazioni su ``identity_file``, vedere la pagina man di SSH.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
durata	Numero intero da 1 a 24 che indica il numero di ore per cui la chiave firmata è valida. Se la durata non è specificata, viene utilizzato il valore predefinito.	intero	1	NO
chiave pubblica	Se specificato, questo parametro restituirà solo signed_public_key anziché creare un portachiavi completo per l'utente.  Chiavi pubbliche che inviate tramite la barra degli URL in un browser con + vengono interpretati come segni spaziati e di interruzione.	corda	Nulla	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
sfadmin	Consente l'accesso all'account shell sfadmin quando si effettua la chiamata API con accesso al cluster supportAdmin o quando il nodo non si trova in un cluster.	booleano	Falso	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
stato_keygen	Contiene l'identità nella chiave firmata, i principali consentiti e le date di inizio e fine valide per la chiave.	corda
chiave privata	Un valore di chiave SSH privata viene restituito solo se l'API sta generando un portachiavi completo per l'utente finale.  Il valore è codificato in Base64; è necessario decodificare il valore quando viene scritto in un file per garantire che venga letto come una chiave privata valida.	corda

Nome	Descrizione	Tipo
chiave pubblica	Un valore di chiave SSH pubblica viene restituito solo se l'API sta generando un portachiavi completo per l'utente finale.  Quando si passa un parametro <code>public_key</code> al metodo API, solo il <code>signed_public_key</code> il valore viene restituito nella risposta.	corda
chiave pubblica firmata	La chiave pubblica SSH risultante dalla firma della chiave pubblica, indipendentemente dal fatto che sia stata fornita dall'utente o generata tramite API.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SignSshKeys",
  "params": {
    "duration": 2,
    "publicKey":<string>
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "id": null,
  "result": {
    "signedKeys": {
      "keygen_status": <keygen_status>,
      "signed_public_key": <signed_public_key>
    }
  }
}

```

In questo esempio, viene firmata e restituita una chiave pubblica valida per la durata (1-24 ore).

Nuovo dalla versione

12,5

TestKeyProviderKmip

Puoi usare il `TestKeyProviderKmip` metodo per verificare se il fornitore 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	Necessario
ID fornitore di chiavi	L'ID del fornitore della chiave da testare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno. Il test è considerato riuscito finché non viene restituito alcun errore.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestKeyProviderKmp",
  "params": {
    "keyProviderID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

TestKeyServerKmp

Puoi usare il `TestKeyServerKmp` 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	Necessario
ID del server chiave	ID del server delle chiavi KMIP da testare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno. Il test è considerato riuscito se non vengono restituiti errori.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestKeyServerKnip",
  "params": {
    "keyServerID": 15
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result":
    {}
}
```

Nuovo dalla versione

11,7

Metodi API SnapMirror

AbortSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `AbortSnapMirrorRelationship` Metodo per interrompere i trasferimenti SnapMirror avviati ma non ancora completati.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeInfo	Nessuno	Sì
Punto di controllo chiaro	Determina se cancellare o meno il checkpoint di riavvio. Valori possibili: • VERO • falso	booleano	falso	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror interrotta.	snapMirrorRelationship

Nuovo 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 diventa indipendente e di lettura-scrittura e può quindi divergere dall'origine. Puoi ristabilire la relazione con il `ResyncSnapMirrorRelationship` Metodo API. Questo metodo richiede che il cluster ONTAP sia disponibile.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeInfo	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror interrotta.	snapMirrorRelationship

Nuovo dalla versione

10,1

Trova maggiori informazioni

[BreakSnapMirrorVolume](#)

BreakSnapMirrorVolume

L'interfaccia utente web Element utilizza `BreakSnapMirrorVolume` metodo per interrompere la relazione SnapMirror tra un contenitore sorgente ONTAP e un volume di destinazione Element. L'interruzione di un volume Element SnapMirror è utile se un sistema ONTAP diventa non disponibile durante la replica dei dati su un volume Element. Questa funzionalità consente a un amministratore di storage di assumere il controllo di un volume Element SnapMirror , interromperne 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	Necessario
ID volume	Il volume su cui eseguire l'operazione di interruzione. La modalità di accesso al volume deve essere snapMirrorTarget.	intero	Nessuno	Sì
ID istantanea	Ripristina il volume allo snapshot identificato da questo ID. Il comportamento predefinito è quello di tornare allo snapshot più recente.	intero	Nessuno	NO
conserva	Conserva tutti gli snapshot più recenti di quello identificato da snapshotID. Valori possibili: • true: conserva gli snapshot più recenti di snapshotID. • false: non conservare gli snapshot più recenti di snapshotID. Se il valore è falso, tutti gli snapshot più recenti di snapshotID verranno eliminati.	booleano	falso	NO
accesso	Modalità di accesso al volume risultante. Valori possibili: • leggiScrivi • sola lettura • bloccato	corda	leggiScrivi	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Nuovo dalla versione

10,0

Trova maggiori informazioni

[BreakSnapMirrorRelationship](#)

CreaSnapMirrorEndpoint

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	Necessario
gestionelP	Indirizzo IP di gestione dell'endpoint remoto SnapMirror .	corda	Nessuno	Sì
nome utente	Nome utente di gestione per il sistema ONTAP .	corda	Nessuno	Sì
password	La password di gestione per il sistema ONTAP .	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorEndpoint	L'endpoint SnapMirror appena creato.	snapMirrorEndpoint

Nuovo dalla versione

10,0

CreateSnapMirrorEndpointUnmanaged

Il sistema di archiviazione software Element utilizza

CreateSnapMirrorEndpointUnmanaged metodo per consentire agli endpoint SnapMirror remoti e non gestiti di comunicare con un cluster di archiviazione Element. Gli endpoint non gestiti non possono essere amministrati tramite le API Element SnapMirror . Devono essere gestiti tramite software di gestione ONTAP o API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome cluster	Il nome dell'endpoint.	corda	Nessuno	Sì
indirizzi IP	Elenco di indirizzi IP per un cluster di sistemi di archiviazione ONTAP che devono comunicare con questo cluster di archiviazione Element.	matrice di stringhe	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorEndpoint	L'endpoint SnapMirror appena creato.	snapMirrorEndpoint

Nuovo dalla versione

10,3

Crea relazioneSnapMirror

L'interfaccia utente web Element utilizza CreateSnapMirrorRelationship Metodo per creare una relazione di protezione dati estesa SnapMirror tra un endpoint di origine e uno di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
sorgenteVolume	Il volume sorgente nella relazione.	snapMirrorVolumeIn fo	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione.	snapMirrorVolumeIn fo	Nessuno	Sì
tipo di relazione	Il tipo di relazione. Nei sistemi di archiviazione che eseguono il software Element, questo valore è sempre "extended_data_protection".	corda	Nessuno	NO
NomePolitica	Specifica il nome del criterio ONTAP SnapMirror per la relazione. Se non specificato, il nome predefinito del criterio è MirrorLatest.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Nome programma	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.	corda	Nessuno	NO
maxTransferRate	Specifica la velocità massima di trasferimento 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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Informazioni sulla relazione SnapMirror appena creata.	snapMirrorRelationship

Nuovo dalla versione

10,1

CreaSnapMirrorVolume

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	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
server virtuale	Il nome del Vserver.	corda	Nessuno	Sì
nome	Nome del volume ONTAP di destinazione.	corda	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 specificato alcun tipo, il tipo predefinito è dp.	corda	Nessuno	NO
aggregato	L'aggregato ONTAP contenente il volume in cui crearlo. È possibile utilizzare ListSnapMirrorAggregates per ottenere informazioni sugli aggregati ONTAP disponibili.	corda	Nessuno	Sì
misurare	La dimensione del volume in byte.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorVolume	Informazioni su un volume SnapMirror .	snapMirrorVolume

Nuovo dalla versione

10,1

DeleteSnapMirrorEndpoints

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	Necessario
snapMirrorEndpointIds	Un array di ID di endpoint SnapMirror da eliminare.	array di interi	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Nuovo dalla versione

10,0

EliminaSnapMirrorRelazioni

L'interfaccia utente web Element utilizza `DeleteSnapMirrorRelationships` metodo per rimuovere una o più relazioni SnapMirror tra un endpoint di origine e uno di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
destinazioneVolumi	Il volume o i volumi di destinazione nella relazione SnapMirror .	snapMirrorVolumeIn fo vettore	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Se l'azione di eliminazione è riuscita, questo oggetto contiene un messaggio di successo. Se l'azione non riesce, viene visualizzato un messaggio di errore.	Oggetto JSON

Nuovo 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	Necessario
snapMirrorEndpointID	Se specificato, il sistema elenca le informazioni sulla versione dell'endpoint con lo snapMirrorEndpointID specificato. Se non specificato, il sistema elenca le informazioni sulla versione di tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ontapVersionInfo	Informazioni sulla versione software dell'endpoint ONTAP .	ontapVersionInfo vettore

Nuovo dalla versione

10,1

OttieniSnapMirrorClusterIdentity

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	Necessario
snapMirrorEndpointID	Se specificato, il sistema elenca l'identità del cluster dell'endpoint con lo snapMirrorEndpointID specificato. Se non specificato, il sistema elenca l'identità del cluster di tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorClusterIdentity	Un elenco delle identità del cluster degli endpoint SnapMirror .	snapMirrorClusterIdentity vettore

Nuovo dalla versione

10,1

InizializzaSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza

`InitializeSnapMirrorRelationship` Metodo per inizializzare il volume di destinazione in una relazione SnapMirror eseguendo un trasferimento di base iniziale tra cluster.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	L'ID del sistema ONTAP remoto.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeInfo	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
maxTransferRate	Specifica la velocità massima di trasferimento 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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Informazioni sulla relazione SnapMirror inizializzata.	snapMirrorRelationship

Nuovo dalla versione

10,1

ListSnapMirrorAggregates

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorAggregates` metodo per elencare tutti gli aggregati SnapMirror disponibili sul sistema ONTAP remoto. Un aggregato descrive un insieme di risorse di archiviazione fisica.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorAggregates	Elenco degli aggregati disponibili sul sistema di stoccaggio ONTAP .	snapMirrorAggregate vettore

Nuovo dalla versione

10,1

ListSnapMirrorEndpoints

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorEndpoints` metodo per elencare tutti gli endpoint SnapMirror con cui comunica il cluster di archiviazione Element.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointIDs	Restituisce solo gli oggetti associati a questi ID. Se non vengono forniti ID o l'array è vuoto, il metodo restituisce tutti gli ID degli endpoint SnapMirror .	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorEndpoints	Un elenco degli endpoint SnapMirror esistenti.	snapMirrorEndpoint vettore

Nuovo dalla versione

10,0

ListSnapMirrorLuns

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorLuns` metodo per elencare le informazioni LUN per la relazione SnapMirror dal cluster ONTAP remoto.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	Elenca solo le informazioni LUN associate all'ID endpoint specificato.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeIn fo	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
snapMirrorLunInfos	Un elenco di oggetti contenenti informazioni sui LUN SnapMirror .	snapMirrorLunInfo vettore

Nuovo 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	Necessario
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
ruolointerfaccia	Elenca solo l'interfaccia di rete che svolge il ruolo specificato.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorNetworkInterfaces	Elenco delle interfacce di rete SnapMirror disponibili sul sistema di archiviazione ONTAP remoto.	snapMirrorNetworkInterface vettore

Nuovo dalla versione

10,1

ListSnapMirrorNodes

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	Necessario
snapMirrorEndpointID	Se specificato, il sistema elenca i nodi dell'endpoint con lo snapMirrorEndpointID specificato. Se non specificato, il sistema elenca i nodi di tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorNodes	Un elenco dei nodi sul cluster ONTAP .	snapMirrorNode vettore

Nuovo dalla versione

10,1

ListSnapMirrorPolicies

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorPolicies` metodo per elencare tutte le policy SnapMirror su un sistema ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	Elenca 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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorPolicies	Elenco delle policy SnapMirror sul sistema di archiviazione ONTAP .	snapMirrorPolicy vettore

Nuovo dalla versione

10,1

ListSnapMirrorSchedules

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorSchedules` metodo per ottenere un elenco di pianificazioni disponibili su un cluster ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	Se specificato, il sistema elenca le pianificazioni dell'endpoint con l'ID endpoint SnapMirror specificato. Se non specificato, il sistema elenca le pianificazioni di tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorSchedules	Un elenco delle pianificazioni SnapMirror sul cluster ONTAP remoto.	snapMirrorJobScheduleCronInfo vettore

Nuovo 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 archiviazione Element.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	Elenca solo le relazioni associate all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca le relazioni da tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO
destinazioneVolume	Elenca le relazioni associate al volume di destinazione specificato.	snapMirrorVolumeInfo	Nessuno	NO
sorgenteVolume	Elenca le relazioni associate al volume sorgente specificato.	snapMirrorVolumeInfo	Nessuno	NO
server virtuale	Elenca le relazioni sul Vserver specificato.	corda	Nessuno	NO
ID relazione	Elenca le relazioni associate all'ID relazione specificato.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationships	Un elenco di oggetti contenenti informazioni sulle relazioni SnapMirror .	snapMirrorRelationship vettore

Nuovo 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	Necessario
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".	corda	Nessuno	NO
nome	Elenca solo i volumi ONTAP con il nome specificato.	corda	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	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorVolumes	Elenco dei volumi SnapMirror disponibili sul sistema di archiviazione ONTAP .	snapMirrorVolume vettore

Nuovo dalla versione

10,1

ListSnapMirrorVservers

L'interfaccia utente Web del software Element utilizza `ListSnapMirrorVservers` metodo per elencare tutti i Vserver SnapMirror disponibili su un sistema ONTAP remoto.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	Elenca solo i Vserver associati all'ID endpoint specificato. Se non viene fornito alcun ID endpoint, il sistema elenca i Vserver da tutti gli endpoint SnapMirror noti.	intero	Nessuno	NO
Tipo di server virtuale	Elenca solo i Vserver del tipo specificato. Valori possibili: • amministratore • dati • nodo • sistema	corda	Nessuno	NO
vserverName	Elenca solo i Vserver con il nome specificato.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorVservers	Elenco dei Vserver SnapMirror disponibili sul sistema di archiviazione ONTAP .	snapMirrorVservervettore

Nuovo dalla versione

10,1

ModificaSnapMirrorEndpoint

L'interfaccia utente Web del software Element utilizza `ModifySnapMirrorEndpoint` Metodo per modificare il nome e gli attributi di gestione per un endpoint SnapMirror .

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
SnapMirrorEndpointID	L'endpoint SnapMirror da modificare.	intero	Nessuno	Sì
gestioneIP	Il nuovo indirizzo IP di gestione per il sistema ONTAP .	corda	Nessuno	NO
nome utente	Il nuovo nome utente di gestione per il sistema ONTAP .	corda	Nessuno	NO
password	La nuova password di gestione per il sistema ONTAP .	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorEndpoint	Informazioni sull'endpoint SnapMirror modificato.	snapMirrorEndpoint

Nuovo dalla versione

10,0

ModifySnapMirrorEndpoint (non gestito)

Il software Element utilizza questa versione del `ModifySnapMirrorEndpoint` Metodo per modificare gli attributi del nome del cluster di archiviazione o dell'indirizzo IP per un endpoint SnapMirror non gestito. Gli endpoint non gestiti non possono essere amministrati tramite le API Element SnapMirror . Devono essere gestiti tramite software di gestione ONTAP o API.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
SnapMirrorEndpointID	L'endpoint SnapMirror da modificare.	intero	Nessuno	Sì
Nome cluster	Il nuovo nome dell'endpoint.	corda	Nessuno	NO
indirizzi IP	Il nuovo elenco di indirizzi IP per un cluster di sistemi di archiviazione ONTAP che dovrebbero comunicare con questo cluster di archiviazione Element.	matrice di stringhe	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorEndpoint	Informazioni sull'endpoint SnapMirror modificato.	snapMirrorEndpoint

Nuovo dalla versione

10,3

Modificare la relazione SnapMirror

Puoi usare `ModifySnapMirrorRelationship` per modificare gli intervalli in cui si verifica uno snapshot pianificato. Utilizzando questo metodo è anche possibile eliminare o mettere in pausa una pianificazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	Sì
maxTransferRate	Specifica la velocità massima di trasferimento 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
NomePolitica	Specifica il nome del criterio ONTAP SnapMirror per la relazione.	corda	Nessuno	NO
Nome programma	Nome della pianificazione cron preesistente sul sistema ONTAP utilizzata per aggiornare la relazione SnapMirror .	corda	Nessuno	NO

snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente gli attributi di relazione SnapMirror modificati.	snapMirrorRelationship

Nuovo dalla versione

10,1

Aggiorna relazione SnapMirror

L'interfaccia utente Web del software Element utilizza

UpdateSnapMirrorRelationship Metodo per rendere il volume di destinazione in una relazione SnapMirror uno specchio aggiornato del volume di origine.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
maxTransferRate	Specifica la velocità massima di trasferimento 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 di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror aggiornata.	snapMirrorRelationship

Nuovo dalla versione

10,1

QuiesceSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza `QuiesceSnapMirrorRelationship` metodo per disabilitare i futuri trasferimenti di dati per una relazione SnapMirror . Se è in corso un trasferimento, lo stato della relazione diventa "quiescent" fino al completamento del trasferimento. Se il trasferimento in corso viene interrotto, non verrà riavviato. È possibile riattivare 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	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror inattiva.	snapMirrorRelationship

Nuovo dalla versione

10,1

ResumeSnapMirrorRelationship

L'interfaccia utente Web del software Element utilizza

`ResumeSnapMirrorRelationship` metodo per abilitare trasferimenti futuri per una relazione SnapMirror inattiva.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror ripristinata.	snapMirrorRelationship

Nuovo 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 uno di destinazione. Quando si risincronizza una relazione, il sistema rimuove gli snapshot sul volume di destinazione che sono 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	Necessario
snapMirrorEndpointID	ID endpoint del sistema di archiviazione ONTAP remoto che comunica con il cluster di archiviazione Element.	intero	Nessuno	Sì
destinazioneVolume	Il volume di destinazione nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
maxTransferRate	Specifica la velocità massima di trasferimento 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
sorgenteVolume	Il volume sorgente nella relazione SnapMirror .	snapMirrorVolumeinfo	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
snapMirrorRelationship	Un oggetto contenente informazioni sulla relazione SnapMirror risincronizzata.	snapMirrorRelationship

Nuovo dalla versione

10,1

Metodi API di configurazione del sistema

DisabilitaBmcColdReset

Puoi usare il `DisableBmcColdReset` metodo per disabilitare l'attività in background che reimposta periodicamente il Baseboard Management Controller (BMC) per tutti i nodi del cluster.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
cBmcResetDurationMinutes	Restituisce il tempo tra gli intervalli di reset. L'intervallo dovrebbe essere sempre 0 dopo il completamento del comando.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableBmcColdReset",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "cBmcResetDurationMinutes": 0
  }
}
```

Nuovo dalla versione

12,0

DisabilitaClusterSsh

Puoi usare il `DisableClusterSsh` metodo per disabilitare il servizio SSH per l'intero cluster di archiviazione. Quando si aggiungono nodi al cluster di archiviazione, i nuovi nodi ereditano questa impostazione a livello di cluster.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
risultato	Un oggetto JSON contenente lo stato del servizio SSH per il cluster di archiviazione, il tempo rimanente prima che SSH venga disabilitato e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableClusterSsh",
  "params": {
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      } ]
    }
  }
}
```

Nuovo dalla versione

10,3

Disabilita Snmp

Puoi usare il `DisableSnmp` metodo per disabilitare SNMP sui nodi del cluster.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DisableSnmp",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "result" : {},
  "id" : 1
}
```

Nuovo dalla versione

9,6

AbilitaBmcColdReset

Puoi usare il `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	Necessario
tempo scaduto	Tempo tra le operazioni di reset BMC , in minuti.	intero	20160 minuti	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
cBmcResetDurationMinutes	Restituisce il tempo tra gli intervalli di reset. L'intervallo dovrebbe essere sempre 0 dopo il completamento del comando.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableBmcColdReset",
  "params": {
    "timeout": 36000
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "cBmcResetDurationMinutes": 36000
  }
}
```

Nuovo dalla versione

12,0

AbilitaClusterSsh

Puoi usare il `EnableClusterSsh` metodo per abilitare il servizio SSH su tutti i nodi nel cluster di archiviazione.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
durata	Periodo di tempo per cui il servizio SSH rimarrà abilitato.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Un oggetto JSON contenente lo stato del servizio SSH per il cluster di archiviazione, il tempo rimanente prima che SSH venga disabilitato e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableClusterSsh",
  "params": {
    "duration" : "02:00:00.00"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      } ]
    }
  }
}

```

Nuovo dalla versione

10,3

AbilitaSnmpp

Puoi usare il `EnableSnmpp` metodo per abilitare SNMP sui nodi del cluster. Quando si abilita SNMP, l'azione si applica a tutti i nodi del cluster e i valori passati sostituiscono tutti i valori impostati in qualsiasi chiamata precedente a `EnableSnmpp`.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snmpV3Enabled	Se impostato su true, SNMP v3 è abilitato su ciascun nodo del cluster. Se impostato su false, SNMP v2 è abilitato.	booleano	falso	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "EnableSnmp",
  "params": {
    "snmpV3Enabled" : "true"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

OttieniBinAssignmentProperties

Puoi usare il `GetBinAssignmentProperties` metodo per recuperare le proprietà di assegnazione dei bin nel database.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
proprietà	Descrive in dettaglio le proprietà di tutte le assegnazioni di bin correnti nel database.	matrice binAssignmentProperties

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetBinAssignmentProperties",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": []  
    }  
}  
}
```

Nuovo dalla versione

12,0

OttieniClusterSshInfo

Puoi usare il `GetClusterSshInfo` metodo per interrogare lo stato del servizio SSH per l'intero cluster di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
risultato	Un oggetto JSON contenente lo stato del servizio SSH per il cluster di archiviazione, il tempo rimanente prima che SSH venga disabilitato e lo stato del servizio SSH per ciascun nodo.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{  
  "method": "GetClusterSshInfo",  
  "params": {},  
  "id" : 1  
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      } ]
    }
  }
```

Nuovo dalla versione

10,3

OttieniStrutturaCluster

Puoi usare il `GetClusterStructure` metodo per eseguire il backup delle informazioni di configurazione del cluster di archiviazione corrente. Se la configurazione del cluster di archiviazione 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 parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Un oggetto JSON contenente le informazioni di configurazione correnti del cluster di archiviazione.	clusterStructure

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetClusterStructure",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result" : <clusterStructure object containing configuration
information>
}
```

Nuovo dalla versione

10,3

OttieniFipsReport

Puoi usare il `GetFipsReport` metodo per verificare lo stato di supporto della funzionalità di crittografia FIPS 140-2 di tutti i nodi nel cluster di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Un oggetto JSON contenente lo stato del supporto delle funzionalità FIPS 140-2 per ogni nodo e informazioni di errore per ogni nodo che non ha risposto alla query.	fipsReport

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetFipsReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
        }
      }
    ]
  }
}

```

Nuovo dalla versione

10,3

OttieniLldpConfig

Puoi usare il `GetLldpConfig` metodo per ottenere la configurazione del Link Layer Discovery Protocol (LLDP) per ciascun nodo di un cluster di storage.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
lldpConfig	Informazioni sulla configurazione LLDP del cluster di archiviazione.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetLldpConfig",
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": null,
  "result": {
    "lldpConfig": {
      "enableLldp": true,
      "enableMed": false,
      "enableOtherProtocols": true
    }
  }
}
```

OttieniLldpInfo

Puoi usare il `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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
lldpInfo	Informazioni sulle impostazioni LLDP dello chassis, dell'interfaccia e del vicino per ciascun nodo di un cluster di storage.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetLldpInfo",
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

11,0

Trova maggiori informazioni

[OttieniLldpInfo](#)

Ottieni report sui drive dei nodi Fips

Puoi usare il `GetNodeFipsDrivesReport` metodo per verificare lo stato della capacità di crittografia dell'unità FIPS 140-2 di un singolo nodo nel cluster di archiviazione. È necessario eseguire questo metodo su un singolo nodo di archiviazione.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
fipsDrives	Un oggetto JSON contenente lo stato del supporto delle funzionalità FIPS 140-2 per questo nodo. Valori possibili: • Nessuno: il nodo non è compatibile con FIPS. • Parziale: il nodo supporta FIPS, ma non tutte le unità nel nodo sono unità FIPS. • Pronto: il nodo è compatibile con FIPS e tutte le unità nel nodo sono unità FIPS (oppure non sono presenti unità).	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNodeFipsDrivesReport",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "fipsDrives": "None"
  }
}
```

Nuovo dalla versione

11,5

Ottieni informazioni Ntp

Puoi usare il `GetNtpInfo` metodo per ottenere le informazioni di configurazione correnti del protocollo NTP (Network Time Protocol).

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
server	Elenco dei server NTP.	matrice di stringhe
client di trasmissione	Indica se i nodi del cluster sono in ascolto dei messaggi NTP trasmessi. Valori possibili: • VERO • falso	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNtpInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "broadcastclient" : false,
    "servers" : [ "us.pool.ntp.org" ]
  }
}
```

Nuovo dalla versione

9,6

Ottieni informazioni Nvram

Puoi usare il `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	Necessario
forza	Per eseguire correttamente questo metodo su tutti i nodi del cluster, è necessario includere il parametro <code>force</code> .	booleano	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>nvramInfo</code>	Serie di eventi ed errori rilevati sulla scheda NVRAM .	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetNvramInfo",
  "params": {
    "force": true
  },
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Ottieni informazioni Nvram](#)

OttieniProtectionDomainLayout

Puoi usare il `GetProtectionDomainLayout` Metodo per restituire tutte le informazioni sul dominio di protezione per un cluster, incluso in quale chassis e in quale dominio di protezione personalizzato si trova ciascun nodo.

Parametro

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
protezioneDomainLayout	Elenco dei nodi, ciascuno con i relativi domini di protezione.	Elenco JSON di "nodeProtectionDomains" oggetti.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetProtectionDomainLayout",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  ]
}

```

```
]
}
}
```

Nuovo dalla versione

12,0

OttieniHost di registrazione remoti

Puoi usare il `GetRemoteLoggingHosts` metodo per ottenere l'elenco corrente dei server di registro.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
host remoti	Elenco di informazioni su indirizzi IP e porte relative agli host configurati per ricevere informazioni di registrazione inoltrate.	Server di registrazione vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 3386609,
  "method": "GetRemoteLoggingHosts",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 3386609,
  "result": {
    "remoteHosts": [
      {
        "host": "172.16.1.20",
        "port": 10514
      },
      {
        "host": "172.16.1.25"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Imposta host di registrazione remoti](#)

OttieniSnmptACL

Puoi usare il `GetSnmptACL` metodo per ottenere le autorizzazioni di accesso SNMP correnti sui nodi del cluster.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
reti	Elenco delle reti e tipo di accesso che hanno ai server SNMP in esecuzione sui nodi del cluster. Questo valore è presente se SNMP v3 è disabilitato.	rete vettore

Nome	Descrizione	Tipo
Utenti usm	Elenco degli utenti e tipo di accesso di cui dispongono ai server SNMP in esecuzione sui nodi del cluster. Questo valore è presente se SNMP v3 è abilitato.	usmUser vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetSnmPACL",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "usmUsers" : [
      {
        "name": "jdoe",
        "access": "rouser",
        "secLevel": "priv",
        "password": "mypassword",
        "passphrase": "mypassphrase",
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

OttieniSnmPInfo

Puoi usare il `GetSnmPInfo` metodo per ottenere le informazioni di configurazione correnti del protocollo SNMP (Simple Network Management Protocol).

Parametri



GetSnmpInfo è obsoleto per le versioni di Element successive alla versione 8.0. IL [OttieniSnmpState](#) E [SetSnmpACL](#) sostituiscono il metodo GetSnmpInfo.

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

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 disabilitato.	rete
abilitato	Indica se i nodi nel cluster sono configurati per SNMP. Valori possibili: • VERO • falso	booleano
snmpV3Enabled	Se il nodo nel cluster è configurato per SNMP v3. Valori possibili: • VERO • falso	booleano
Utenti usm	Se SNMP v3 è abilitato, il cluster restituisce un elenco di parametri di accesso utente per SNMP. Questo viene restituito al posto del parametro networks.	usmUser

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetSnmpInfo",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "enabled" : true,
    "networks" : [
      {
        "access" : "rosys",
        "cidr" : 0,
        "community" : "public",
        "network" : "localhost"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [OttieniSnmpState](#)
- [SetSnmpACL](#)

OttieniSnmpState

Puoi usare il `GetSnmpState` metodo per ottenere lo stato corrente della funzionalità SNMP.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
abilitato	Valori possibili: • VERO • falso Il valore predefinito è falso. Restituisce true se i nodi nel cluster sono configurati per SNMP.	booleano
snmpV3Enabled	Valori possibili: • VERO • falso Il valore predefinito è falso. Restituisce true se i nodi nel cluster sono configurati per SNMP v3.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetSnmpState",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "enabled": true,
    "snmpV3Enabled": false
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[SetSnmpACL](#)

OttieniSnmpTrapInfo

Puoi usare il `GetSnmpTrapInfo` metodo per ottenere le informazioni di configurazione attuali della trap SNMP.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
trapRecipients	Elenco degli host che devono ricevere le trap generate dal cluster.	snmpTrapRecipient vettore
clusterFaultTrapsEnabled	Il valore true indica che è configurato un <code>solidFireClusterFaultNotification</code> per essere inviato all'elenco dei destinatari delle trap quando viene registrato un errore del cluster.	booleano
clusterFaultResolvedTrapsEnabled	Il valore true indica che è configurato un <code>solidFireClusterFaultResolvedNotification</code> per essere inviato all'elenco dei destinatari della trap quando viene risolto un errore del cluster.	booleano
clusterEventTrapsEnabled	Il valore true indica che un <code>solidFireClusterEventNotification</code> è configurato per essere inviato all'elenco dei destinatari trap quando viene registrato un evento cluster.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetSnmpTrapInfo"
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

Ottieni certificato SSL

Puoi usare il `GetSSLCertificate` metodo per recuperare il certificato SSL attualmente attivo sui nodi di archiviazione del cluster.


```

DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAGTAk5WMRUwEwYDVQHFAXW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbjBWZWdhcy4uLjEtMCsGCSqG
SIb3DQEJARYe\nd2hhdGhhcHBlnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjjf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s7lmQPECwVLfiE/ndtIbnpe\nmQq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\nniebEgAaE5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nnDEwvdl+DwKxnS1cx1v
ERv51g1gua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAjJDg
10QoQDWNDoTerBs80nwiouA==\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"
    }
}
}

```

Nuovo dalla versione

10,0

ListProtectionDomainLevels

Puoi usare il `ListProtectionDomainLevels` metodo per elencare i livelli di tolleranza e resilienza del cluster di archiviazione. I livelli di tolleranza indicano la capacità del cluster di continuare a leggere e scrivere dati in caso di guasto, mentre i livelli di resilienza indicano la capacità del cluster di storage di ripristinarsi automaticamente in seguito a uno o più guasti.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
protectionDomainLevels	Un elenco dei diversi livelli di dominio di protezione, ognuno dei quali fornisce informazioni sulla tolleranza e la resilienza del cluster di archiviazione.	protezioneDomainLevel

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListProtectionDomainLevels",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    }
}
]
}
}

```

Nuovo dalla versione

11,0

RimuoviCertificatoSSL

Puoi usare il `RemoveSSLCertificate` metodo per rimuovere il certificato SSL dell'utente e la chiave privata per i nodi di archiviazione nel cluster. Dopo aver rimosso il certificato e la chiave privata, i nodi di archiviazione vengono configurati per utilizzare il certificato e la chiave privata predefiniti.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "RemoveSSLCertificate",
  "params" : {},
  "id" : 3
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 3,
  "result" : {}
}
```

Nuovo dalla versione

10,0

ReimpostaConfigurazioneRete

Puoi usare il `ResetNetworkConfig` metodo per aiutare a 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 di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ResetNetworkConfig",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo non restituisce una risposta.

Nuovo dalla versione

11,0

ResetSupplementalTlsCiphers

Puoi usare il `ResetSupplementalTlsCiphers` metodo per ripristinare l'elenco predefinito dei cifrari TLS supplementari. È possibile utilizzare questo metodo sull'intero cluster.

Parametro

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ResetSupplementalTlsCiphers",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

11,3

ImpostaStrutturaCluster

Puoi usare il `SetClusterStructure` metodo per ripristinare le informazioni di configurazione del cluster di archiviazione 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	Un oggetto JSON contenente le informazioni di configurazione correnti del cluster di archiviazione.	clusterStructure

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
risultato	Gestione dei risultati asincroni.	<code>asyncHandle</code>

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetClusterStructure",
  "params": <insert clusterStructure object here>,
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result" : {
    "asyncHandle": 1
  }
}
```

Nuovo dalla versione

10,3

ImpostaLldpConfig

Puoi usare il `SetLldpConfig` metodo per configurare le impostazioni del Link Layer Discovery Protocol (LLDP) per un cluster di archiviazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
abilitaAltriProtocolli	Abilita l'uso automatico di altri protocolli di rilevamento: CDP, FDP, EDP e SONMP.	booleano	VERO	NO
enableMed	Abilita Media Endpoint Discovery (LLDP-MED).	booleano	falso	NO
abilitaLldp	Abilita o disabilita LLDP.	booleano	VERO	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
lldpConfig	Informazioni sulla configurazione LLDP corrente del cluster di archiviazione, comprese le impostazioni modificate di recente.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 3920,
  "method": "SetLldpConfig",
  "params": {
    "lldpConfig": {
      "enableMed": true
    }
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 3920,
  "result": {
    "lldpConfig": {
      "enableLldp": true,
      "enableMed": true,
      "enableOtherProtocols": true
    }
  }
}
```

ImpostaNtpInfo

Puoi usare il `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 broadcast NTP trasmette periodicamente informazioni orarie sulla rete, è possibile configurare facoltativamente i nodi come client broadcast.

Parametri



Assicurati di utilizzare server NTP interni alla tua rete, anziché quelli predefiniti di installazione.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
server	Elenco dei server NTP da aggiungere a ciascun nodo della configurazione NTP.	matrice di stringhe	Nessuno	Sì
client di trasmissione	Abilita ogni nodo del cluster come client broadcast.	booleano	falso	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

ImpostaProtezioneDominioLayout

Puoi usare il `SetProtectionDomainLayout` metodo per assegnare nodi a domini di protezione personalizzati.

È necessario fornire informazioni per tutti i nodi attivi nel cluster e non è possibile fornire informazioni per i nodi inattivi. Tutti i nodi in un dato chassis devono essere assegnati allo stesso dominio di protezione personalizzato. È necessario fornire lo stesso `protectionDomainType` per tutti i nodi. I `protectionDomainType` che non sono personalizzati, come `node` 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 archiviazione contenenti chassis condivisi
- Cluster di storage a due nodi

Il metodo restituisce un errore se utilizzato su cluster di archiviazione con queste configurazioni.

Parametro

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>protezioneDomainLayout</code>	Informazioni sul dominio di protezione per ciascun nodo.	Elenco JSON di <code>"nodeProtectionDomains"</code> oggetti.	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>protezioneDomainLayout</code>	Elenco dei nodi, ciascuno con i relativi domini di protezione.	Elenco JSON di <code>"nodeProtectionDomains"</code> oggetti.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```

{
  "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 al seguente esempio:

```
{
  "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"
        }
      ]
    }
  ]
}

```

Nuovo dalla versione

12,0

Imposta host di registrazione remoti

Puoi usare il `SetRemoteLoggingHosts` Metodo per configurare la registrazione remota dai nodi nel cluster di archiviazione a uno o più server di registrazione centralizzati. La registrazione remota viene eseguita tramite TCP utilizzando la porta predefinita 514. Questa API non si aggiunge agli host di registrazione esistenti. Piuttosto, sostituisce ciò che esiste attualmente con nuovi valori specificati da questo metodo API. Puoi usare `GetRemoteLoggingHosts` per determinare quali sono gli host di registrazione correnti e quindi utilizzare `SetRemoteLoggingHosts` per impostare l'elenco desiderato di host di registrazione attuali e nuovi.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
host remoti	Elenco degli host destinatari dei messaggi di log.	Server di registrazione <code>vetto</code>	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniHost di registrazione remoti](#)

SetSnmppACL

Puoi usare il `SetSnmppACL` 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 `SetSnmppACL` . Si noti inoltre che i valori impostati con questa interfaccia sostituiscono tutti i valori di rete o `usmUsers` impostati con `SetSnmppInfo` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
reti	Elenco delle reti e tipo di accesso che hanno ai server SNMP in esecuzione sui nodi del cluster. Per i possibili valori di rete, vedere l'oggetto di rete SNMP. Questo parametro è obbligatorio se SNMP v3 è disabilitato.	rete	Nessuno	NO
Utenti usm	Elenco degli utenti e tipo di accesso di cui dispongono ai server SNMP in esecuzione sui nodi del cluster. Questo parametro è obbligatorio se SNMP v3 è abilitato.	usmUser	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[ImpostaSnmpInfo](#)

ImpostaSnmpInfo

Puoi usare il `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 le versioni Element 6.0 e successive. Utilizzare il [AbilitaSnmp](#) e [SetSnmpACL](#) metodi invece.

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
reti	Elenco delle reti e tipo di accesso che hanno ai server SNMP in esecuzione sui nodi del cluster. Vedi SNMPrete oggetto per valori possibili. Questo parametro è obbligatorio solo per SNMP v2.	rete vettore	Nessuno	NO
abilitato	Se impostato su true, SNMP è abilitato su ciascun nodo del cluster.	booleano	falso	NO
snmpV3Enabled	Se impostato su true, SNMP v3 è abilitato su ciascun nodo del cluster.	booleano	falso	NO
Utenti usm	Se SNMP v3 è abilitato, questo valore deve essere passato al posto del parametro networks. Questo parametro è obbligatorio solo per SNMP v3.	usmUser	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Esempio di richiesta con SNMP v3 abilitato

Le richieste per questo metodo sono simili al seguente esempio:


```
{
  "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 abilitato

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id" : 1
  "result" :{
  }
}
```

Nuovo dalla versione

9,6

ImpostaSnmptTrapInfo

Puoi usare il `SetSnmptTrapInfo` metodo per abilitare e disabilitare la generazione di notifiche SNMP del cluster (trap) e per specificare il set di host che ricevono le notifiche. I valori che passi con ciascuno `SetSnmptTrapInfo` la chiamata al metodo sostituisce tutti i valori impostati in qualsiasi chiamata precedente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo
trapRecipients	Elenco degli host che devono ricevere le trap generate dal cluster di archiviazione. Se è abilitato uno qualsiasi dei tipi di trappola, è richiesto almeno un oggetto. Questo parametro è obbligatorio solo se uno qualsiasi dei parametri booleani è impostato su true. (Nessun valore predefinito. (Non richiesto.)	snmpTrapRecipient vettore
clusterFaultTrapsEnabled	Se impostato su true, una notifica di errore del cluster corrispondente viene inviata all'elenco configurato dei destinatari delle trap quando viene registrato un errore del cluster. (Valore predefinito: falso. (Non richiesto.)	booleano

Nome	Descrizione	Tipo
clusterFaultResolvedTrapsEnabled	Se impostato su true, una notifica di risoluzione dell'errore del cluster corrispondente viene inviata all'elenco configurato dei destinatari delle trap quando un errore del cluster viene risolto. (Valore predefinito: falso. (Non richiesto.)	booleano
clusterEventTrapsEnabled	Se impostato su true, una notifica di evento del cluster corrispondente viene inviata all'elenco configurato dei destinatari trap quando viene registrato un evento del cluster. (Valore predefinito: falso. (Non richiesto.)	booleano

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetSnmptTrapInfo",
  "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 al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

SetSSLCertificate

Puoi usare il `SetSSLCertificate` metodo per impostare un certificato SSL utente e una chiave privata per i nodi di archiviazione nel cluster.



Dopo aver utilizzato l'API, è necessario riavviare il nodo di gestione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
certificato	La versione testuale codificata PEM del certificato. Nota: quando si imposta un certificato di nodo o cluster, il certificato deve includere l'estensione <code>extendedKeyUsage</code> per <code>serverAuth</code> . Questa estensione consente di utilizzare il certificato senza errori sui sistemi operativi e sui browser più comuni. Se l'estensione non è presente, l'API rifiuterà il certificato come non valido.	corda	Nessuno	Sì
chiave privata	Versione testuale codificata PEM della chiave privata.	corda	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method" : "SetSSLCertificate",
  "params" : {
    "privateKey": "-----BEGIN RSA PRIVATE KEY-----
\nMIIIEowIBAAKCAQEA8U+28fnLKQNWEMMR6akeDKuehSpS79odLGigI18qlCV/AUY5\nZLjqsT
jBvTJVRv44yoCTgNrx36U7FHP4t6P/Si0aYr4ovx15wDpEM3Qyy5JPB7Je\nlOB6AD7fmiTweP
20HRYpZvY+Uz7LYEFCmrpgGZQF3iOSIcBhtLKE5186JVT6j5dg\n6yYjUGQO352ylc9HXHcn6lb
/jy10DmVNUZ0caQwAmIS3Jmoyx+zj/Ya4WKq+2SqTA\nX7bX0F3wHHfXnZlHnM8fET5N/9A+K6
1S7dg9cyXu4afXcgKy14JiNBvqbBjhGJtE\n76yAy6rThu0xM3jjdkcb9Y8miNzx+ACq+itaw
IDAQABAoIBAHIj1Izr6/sltqVW\n00qVC/49dyNu+KwVSq92ti9rFe7hBPueh9gklh78hP9Qli
tLkir3YK4GFsTFUMux\n7z1NRCxA/4LrmLSkAjW2kRXDfVl2bwZq0ua9NefGw9208D2OZvbuOx
k7Put2p6se\nfngNzSjf2SI5DIX3UMe5dDN5FByu52CJ9mI4U16ngbWln2wc4nsxJg0aAEkzB7w
nq\nt+Am5/Vu1LI6rGiG6oHEW0oGSuH11esIyXXa2hQkU+1+iF2iGRMTiXac4C8d11NU\nnWGIR
CXFJAmsAQ+hQm7pmtsKdEqumj/PIoGXf0BoFVEWaIjIMEgnfuLZp8IelJQXn\nnSFJbk2ECgYEA
+d5ooU4thZXylWHUZqomaxyzOruA1T53UeH69HiFTrLjvfwuaiqj\nn1HzPlhms6hxexwzldzAp
gog/NOM+2bAc0rn0dqvtV4doejt1DZKRqrNCf/cuN2QX\nnjaCJC1CWau3sEHCckLOhWeY4HaPS
oWq0GKLmKkKDChB4nWUYg3gSWQkCgYEA9zuN\nnHW8GPS+yjixeKXmkKO0x/vvxzR+J5HH5znaI
Hss48THyhZxpLr+v30Hy2h0yAlBS\nnny5Ja6wsomb0mVe4NxVtVawg2E9vVvTa1UC+TNmFBBuL
RPfjcnjDerrSuQ5lYY+M\nnC9MJtXGfhp//G0bzwsRzZxOBsUJb15tpaZIs9MCgYAJricpkKjM
0xlZ1jdVXsos\nnPilnbho4qLngrzuUuxKXEPEnzBxUOqCpwQgdzZLYYw788TCVVIVXLEYem2s0
7dDA\nnDTo+WrzQNkvC6IgqtXH1RgqegIoG1VbgQsbsYmDhdaQ+os4+A0eQXw3vgAhJ/qNJ\nnjQ
4Ttw3ylt7FYkRH26ACWQKBgQC74Zmf4JuRLAo5WSZFxpcmMvtnlvdutqUH4kXA\nnzPssy6t+QE
La1fFbAXkZ5PglITK752aiaX6KQNG6qRsA3VS1J6drD9/2AofOQU17\nn+jOkGzmmoXf49Zj3iS
akwg0ZbQNGXNxEsCAUr0BYAobPp9/fB4PbtUs99fvtocFr\nnjS562QKBgCb+JMDP5q7jpUuspj
0obd/ZS+MsomE+gFAMBJ71KFQ7KuoNezNFO+ZE\nn3rnr8AqAm4VMzqRahs2PWNe2H14J4hKu96
qNpNHbsW1NjXdAL9P7oqQIrhGLVdhX\nnInDxVtGXMdMoet4BKnfte1rXFKHgGqXJoczq4JWzGS
IHNgvkrH60\nn-----END RSA PRIVATE KEY-----\n",
    "certificate": "-----BEGIN CERTIFICATE-----
\nMIIIEdzCCA1+gAwIBAgIJAMwbIhWY43/zMA0GCSqSISIb3DQEBBQUAMIGDMQswCQYD\nnVQQGEw
JVUzELMAkGA1UECBMCTlYxFTATBgNVBAcUZFZlZ2FzLCBCYWJ5ITEhMB8G\nnA1UEChMYV2hhdcC
BIYXBwZW5zIGluIFZlZ2FzLi4uMS0wKwYJKoZIhvcNAQkBFh53\nnaGF0aGFwcGVuc0B2ZWdhc3
N0YXlzaW4udmVnYXMwHhcNMjcwMzA2MjI1MDI2WhcN\nnmjcwMzA2MjI1MDI2WjCBGzELMAkGA1
UEBhMCVVMxZAJBgNVBAgTAk5WMRUwEwYD\nnVQQHFAxWZWdhcywgQmFieSExITAFBgNVBAoTGF
doYXQgSGFwcGVucyBpbWZwZWh\ncy4uLjEtMCsGCSqSISIb3DQEJARYed2hhcGhhcHBlbnNadm
VnYXNzdGF5c2luLnZl\nnZ2FzMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA8U+28f
nLKQNWEMMR\nn6akeDKuehSpS79odLGigI18qlCV/AUY5ZLjqsTjBvTJVRv44yoCTgNrx36U7FH
P4\nt6P/Si0aYr4ovx15wDpEM3Qyy5JPB7JelOB6AD7fmiTweP20HRYpZvY+Uz7LYEFC\nnmrgp
GZQF3iOSIcBhtLKE5186JVT6j5dg6yYjUGQO352ylc9HXHcn6lb/jy10DmVNU\nnZ0caQwAmIS3J
moyx+zj/Ya4WKq+2SqTAX7bX0F3wHHfXnZlHnM8fET5N/9A+K61S\nn7dg9cyXu4afXcgKy14Ji
```

```

NBvqbBjhgJtE76yAy6rTHu0xM3jjdkcb9Y8miNzxF+AC\nq+itawIDAQABo4HrMIHoMB0GA1Ud
DgQWBBrvvBRPno5S34zGRhrnDJyTsdnEbTCB\nuAYDVR0jBIGwMIGtgBRvvBRPno5S34zGRhrn
DJyTsdnEbaGBiaSBhjCBgzELMAkG\nA1UEBhMCVVMxCzAJBgNVBAgTAk5WMRUwEwYDVQHFAXW
ZWdhcywgQmFieSExITAf\nBgNVBAoTGFdoYXQgSGFwcGVucyBpbWZhdhcy4uLjEtMCSGCSqG
S1b3DQEJARYe\nd2hhdGhhcHBlbnNAdmVnYXNzdGF5c2luLnZlZ2FzggkAzBsiFZjJf/MwDAYD
VR0T\nBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOCAQEAhVND5s7lmQPECwVLfiE/ndtIbnpe\nMq
o5geQHCHnNlu5RV9j8aYHp9kW2qCDJ5vueZtZ2L1tC4D7Jyfs3714rRolFpX6N\niebEgAae5e
WvB6zgiAcMRIKqu3DmJ7y3CFGk9dH0lQ+WYnoO/eIMy0coT26JB15H\nDEwvdl+DwknS1cx1v
ERv51glgua6AE3tBrlov8q1G4zMJboo3YEwMFwxLkxAFXR\nHgMoPDym099kvc84B1k7HkDGHp
r4tLfVelDJy2zCWIQ5ddbVpyPW2xuE4p4BGx2B\n7ASOjG+DzUxzwaUI6Jzvs3Xq5Jx8ZAJJDg
l0QoQDWNDoTeRBsz80nwioA==\n-----END CERTIFICATE-----\n"
    },
    "id" : 2
}

```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "id" : 2,
  "result" : {}
}

```

Nuovo dalla versione

10,0

SnmpSendTestTraps

‘SnmpSendTestTraps’ consente di testare la funzionalità SNMP per un cluster. Questo metodo indica al cluster di inviare trap SNMP di prova al gestore SNMP attualmente configurato.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
stato	Stato del test.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SnmpSendTestTraps",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "status": "complete"
  }
}
```

Nuovo dalla versione

9,6

Disponibilità dell'indirizzo di prova

Puoi usare il `TestAddressAvailability` Metodo per verificare se un determinato indirizzo IP è in uso su un'interfaccia all'interno del cluster di archiviazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
interfaccia	L'interfaccia di rete di destinazione (ad esempio eth0, Bond10G, ecc.).	corda	Nessuno	Sì
indirizzo	L'indirizzo IP da ricercare sull'interfaccia di destinazione.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
virtualNetworkTag	ID VLAN di destinazione.	intero	Nessuno	NO
tempo scaduto	Timeout in secondi per testare l'indirizzo di destinazione.	intero	5	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
indirizzo	L'indirizzo IP è stato testato.	corda
disponibile	Vero se l'indirizzo IP richiesto è in uso, falso in caso contrario.	booleano

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "TestAddressAvailability",
  "params": {
    "interface": "Bond10G",
    "address": "10.0.0.1",
    "virtualNetworkTag": 1234
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "address": "10.0.0.1",
    "available": true
  }
}
```


Metodi API di rete multitenant

Convenzioni di denominazione delle reti virtuali

I sistemi di archiviazione NetApp Element utilizzano numeri in aumento continuo come identificatori univoci per tutti gli oggetti nel sistema.

Quando si crea un nuovo volume, il nuovo volumeID è 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 Element ha un VirtualNetworkID pari a 1. Questo ID non è la stessa cosa di un numero di tag VLAN.

È possibile utilizzare VirtualNetworkID e VirtualNetworkTag (tag VLAN) in modo intercambiabile, ove indicato nei metodi API.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

AggiungiVirtualNetwork

Puoi usare il `AddVirtualNetwork` metodo per aggiungere una nuova rete virtuale a una configurazione cluster.

Quando si aggiunge una rete virtuale, viene creata un'interfaccia per ciascun nodo e ogni interfaccia richiede un indirizzo IP di rete virtuale. Il numero di indirizzi IP specificato come parametro per questo metodo API deve essere uguale o maggiore del numero di nodi nel cluster. Il sistema fornisce in blocco gli 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 [Modificare la rete virtuale](#) metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
blocchi di indirizzi	Intervallo univoco di indirizzi IP da includere nella rete virtuale. Membri richiesti per l'oggetto: • inizio: l'inizio dell'intervallo di indirizzi IP. (corda) • dimensione: numero di indirizzi IP da includere nel blocco. (numero intero)	Matrice di oggetti JSON	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
porta d'accesso	L'indirizzo IP di un gateway della rete virtuale. Questo parametro è valido solo se il parametro namespace è impostato su true.	corda	Nessuno	NO
nome	Un nome definito dall'utente per la nuova rete virtuale.	corda	Nessuno	Sì
spazio dei nomi	Se impostato su true, abilita la funzionalità VLAN di archiviazione instradabile creando e configurando uno spazio dei nomi e la rete virtuale in esso contenuta.	booleano	Nessuno	NO
maschera di rete	Maschera di rete univoca per la rete virtuale in fase di creazione.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
svip	Indirizzo IP di archiviazione univoco per la rete virtuale in fase di creazione.	corda	Nessuno	Sì
virtualNetworkTag	Un tag di rete virtuale (VLAN) univoco. I valori supportati sono da 1 a 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 falso.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
ID di rete virtuale	ID della rete virtuale della nuova rete virtuale.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
    "virtualNetworkID": 5
  }
}
```

Nuovo dalla versione

9,6

Modificare la rete virtuale

Puoi usare il `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 possibile utilizzarlo anche per abilitare o disabilitare gli spazi dei nomi, nonché per aggiungere o rimuovere un gateway se gli spazi dei nomi sono abilitati sulla rete virtuale.



Questo metodo richiede come parametro il `virtualNetworkID` o il `virtualNetworkTag`, ma non entrambi.

ATTENZIONE:

L'abilitazione o la disabilitazione della funzionalità VLAN di archiviazione instradabile per una rete virtuale esistente modificando il parametro `namespace` interrompe tutto il traffico gestito dalla rete virtuale. È consigliabile modificare il parametro `namespace` durante una finestra di manutenzione programmata.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID di rete virtuale	Identificatore univoco della rete virtuale da modificare. Questo è l'ID della rete virtuale assegnato dal cluster.	intero	Nessuno	NO

virtualNetworkTag	Il tag di rete che identifica la rete virtuale da modificare.	intero	Nessuno	NO
blocchi di indirizzi	Il nuovo blocco di indirizzi da impostare per questa rete virtuale. Ciò potrebbe includere nuovi blocchi di indirizzi da aggiungere all'oggetto esistente oppure omettere blocchi di indirizzi non utilizzati che devono essere rimossi. In alternativa, è possibile estendere o ridurre le dimensioni dei blocchi di indirizzi esistenti. È possibile aumentare solo la dimensione dei blocchi di indirizzi iniziali per un oggetto Rete virtuale; non è possibile diminuirla. Membri richiesti per questo oggetto: • inizio: l'inizio dell'intervallo di indirizzi IP. (corda) • dimensione: numero di indirizzi IP da includere nel blocco. (numero intero)	Oggetto JSON	Nessuno	NO

porta d'accesso	L'indirizzo IP di un gateway della rete virtuale. Questo parametro è valido solo se il parametro namespace è impostato su true.	corda	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
nome	Il nuovo nome per la rete virtuale.	corda	Nessuno	NO
spazio dei nomi	Se impostato su true, abilita la funzionalità VLAN di archiviazione instradabile ricreando la rete virtuale e configurando uno spazio dei nomi che la contenga. Se impostato su falso, disabilita la funzionalità VRF per la rete virtuale. La modifica di questo valore interrompe il traffico che attraversa questa rete virtuale.	booleano	Nessuno	NO
maschera di rete	Nuova maschera di rete per questa rete virtuale.	corda	Nessuno	NO
svip	L'indirizzo IP virtuale di archiviazione per questa rete virtuale. L'SVIP per una rete virtuale non può essere modificato. È necessario creare una nuova rete virtuale per utilizzare un indirizzo SVIP diverso.	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": 1,
  "result": {
  }
}
```

Nuovo dalla versione

9,6

ElencoRetiVirtuali

Puoi usare il `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. Per questo metodo non sono richiesti parametri. 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	Necessario
ID di rete virtuale	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
ID di rete virtuali	ID di rete da includere nell'elenco.	array di interi	Nessuno	NO
virtualNetworkTags	Tag di rete da includere nell'elenco.	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
reti virtuali	Oggetto contenente indirizzi IP di reti virtuali.	rete virtuale

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:


```
{
  "method": "ListVirtualNetworks",
  "params": {
    "virtualNetworkIDs": [5,6]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  },
  {
  }
]
}

```

Nuovo dalla versione

9,6

RimuoviVirtualNetwork

Puoi usare il `RemoveVirtualNetwork` metodo per rimuovere una rete virtuale aggiunta in precedenza.



Questo metodo richiede come parametro il `virtualNetworkID` o il `virtualNetworkTag`, ma non entrambi.



Non è possibile rimuovere una rete virtuale se ad essa sono associati degli iniziatori. Per prima cosa, dissociare gli iniziatori, quindi rimuovere la rete virtuale.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID di rete virtuale	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 di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveVirtualNetwork",
  "params": {
    "virtualNetworkID": 5
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Metodi API del volume

AnnulaClona

Puoi usare il `CancelClone` metodo per interrompere un processo di clonazione o copia di un volume in corso. Quando si annulla un'operazione di clonazione di gruppo, il

sistema completa e rimuove l'asynchHandle associato all'operazione.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
cloneID	Il cloneID per il processo di clonazione in corso.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CancelClone",
  "params": {
    "cloneID" : 5,
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

AnnullaGruppoClona

Puoi usare il `CancelGroupClone` metodo per interrompere un processo di clonazione in corso su un gruppo di volumi. Quando si annulla un'operazione di clonazione di gruppo, il sistema completa e rimuove l'asynchHandle associato all'operazione.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
groupCloneID	Il cloneID per il processo di clonazione in corso.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CancelGroupClone",
  "params": {
    "cloneID" : 5,
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {}
}
```

Nuovo dalla versione

9,6

Clona più volumi

Puoi usare il `CloneMultipleVolumes` metodo per creare un clone di un gruppo di volumi specificati. È possibile assegnare un set coerente di caratteristiche a un gruppo di più volumi quando vengono clonati insieme.

Prima di utilizzare il parametro `groupSnapshotID` per clonare i volumi in uno snapshot di gruppo, è necessario innanzitutto creare lo snapshot di gruppo utilizzando [Crea istantanea di gruppo](#) 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	Necessario
accesso	Nuovo metodo di accesso predefinito per i nuovi volumi se non sovrascritto dalle informazioni passate nell'array del volume.	corda	Nessuno	NO
enableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con endpoint SnapMirror . Valori possibili: • VERO • falso	booleano	falso	NO
ID istantanea gruppo	ID dello snapshot del gruppo da utilizzare come base per il clone.	intero	Nessuno	NO
nuovoIDAccount	Nuovo ID account per i volumi se non sovrascritto dalle informazioni passate nella matrice dei volumi.	intero	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumi	Raccolta di membri specificati per i nuovi volumi. Membri: • volumeID: (obbligatorio) • accesso: (facoltativo) può essere readOnly, readWrite, locked o replicationTarget. • attributi: (facoltativo) elenco di coppie nome-valore in formato oggetto JSON. • nome: (facoltativo) Nuovo nome per il clone. • newAccountID: (facoltativo) ID account per i nuovi volumi. • newSize: (facoltativo) Dimensione totale del volume, in byte. La dimensione è arrotondata al megabyte più vicino. Se non vengono specificati membri facoltativi, i valori vengono ereditati dai volumi di origine.	Matrice di oggetti JSON	Nessuno	Sì (volumeID)

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore restituito da una chiamata di metodo asincrona.	intero
groupCloneID	ID univoco del nuovo clone del gruppo.	intero
membri	Elenco di volumeID per le coppie di volumi di origine e destinazione.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:


```

{
  "id": 1,
  "result": {
    "asyncHandle": 12,
    "groupCloneID": 4,
    "members": [
      {
        "srcVolumeID": 5,
        "volumeID": 29
      },
      {
        "srcVolumeID": 18,
        "volumeID": 30
      },
      {
        "srcVolumeID": 20,
        "volumeID": 31
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

CloneVolume

Puoi usare il `CloneVolume` metodo per creare una copia di un volume. Questo metodo è asincrono e potrebbe richiedere una quantità di tempo variabile per essere completato.

Il processo di clonazione inizia immediatamente quando si effettua il `CloneVolume` richiesta ed è rappresentativo dello stato del volume quando viene emesso il metodo API. Puoi usare il [Ottieni risultato asincrono](#) metodo per determinare quando il processo di clonazione è completo e il nuovo volume è disponibile per le connessioni. Puoi usare [ListSyncJobs](#) per vedere i progressi nella 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 [ModificaVolume](#) .



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	Necessario
accesso	Accesso consentito per il nuovo volume. Se non viene specificato alcun valore, il valore di accesso non cambia. Valori possibili: • <code>readOnly</code>: (Facoltativo) Sono consentite solo le operazioni di lettura. • <code>readWrite</code>: (Facoltativo) Sono consentite letture e scritture. • <code>locked</code>: (Facoltativo) Non sono consentite letture o scritture. Se non specificato, viene utilizzato il valore di accesso del volume da clonare. • <code>replicationTarget</code>: (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.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
enable512e	Specifica se il nuovo volume deve utilizzare l'emulazione del settore a 512 byte. Se non specificato, viene utilizzata l'impostazione del volume da clonare.	booleano	Impostazione del volume originale	NO
enableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con endpoint SnapMirror . Valori possibili: • VERO • falso	booleano	falso	NO
nome	Nome del nuovo volume clonato; deve essere lungo da 1 a 64 caratteri.	corda	Nessuno	Sì
nuovoIDAccount	AccountID per il proprietario del nuovo volume. Se non specificato, viene utilizzato l'accountID del proprietario del volume da clonare.	intero	AccountID del proprietario del volume originale	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nuovaDimensione	Nuova dimensione del volume, in byte. Potrebbe essere maggiore o minore della dimensione del volume da clonare. Se non specificato, la dimensione del volume non viene modificata. La dimensione è arrotondata al MB più vicino.	intero	Nessuno	NO
ID istantanea	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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero
cloneID	Il cloneID per il volume appena clonato.	intero
curva	I valori della curva QoS applicati al clone.	Oggetto JSON
volume	Un oggetto contenente informazioni sul volume appena clonato.	volume
ID volume	VolumeID per il volume appena clonato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CloneVolume",
  "params": {
    "volumeID" : 5,
    "name" : "mysqldata-snapshot1",
    "access" : "readOnly"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
}
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListSyncJobs](#)
- [ModificaVolume](#)

CopiaVolume

Puoi usare il `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, quali IQN, impostazioni QoS, dimensioni, account e 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 preferibile che i client smontino il volume di destinazione prima che l'operazione abbia inizio. Se il volume di destinazione viene modificato durante l'operazione, le modifiche andranno perse. Questa operazione può richiedere un tempo variabile per essere completata. Puoi usare il [Ottieni risultato asincrono](#) metodo per determinare quando il processo è terminato, [eListSyncJobs](#) per vedere l'avanzamento della copia.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
dstVolumeID	VolumeID del volume da sovrascrivere.	intero	Nessuno	Sì
ID volume	VolumeID del volume da cui leggere.	intero	Nessuno	Sì
ID istantanea	ID dello snapshot utilizzato come origine del clone. Se non viene fornito alcun ID, viene utilizzato il volume attivo corrente.	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	Valore handle utilizzato per ottenere il risultato dell'operazione.	intero
cloneID	CloneID per il volume appena clonato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CopyVolume",
  "params": {
    "volumeID" : 3,
    "dstVolumeID" : 2
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "asyncHandle": 9,
    "cloneID": 5
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListSyncJobs](#)

Crea politica QoS

Puoi usare il `CreateQoSPolicy` metodo per creare un oggetto `QoSPolicy` che è possibile applicare in seguito a un volume al momento della creazione o della modifica. Una policy QoS ha un ID univoco, un nome e impostazioni QoS.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome della policy QoS, ad esempio oro, platino o argento.	corda	Nessuno	Sì
qualità	Le impostazioni QoS rappresentate da questa policy.	Qualità del servizio	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
Politica QOS	L'oggetto <code>QoSPolicy</code> appena creato.	Politica QoSP

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 68,
  "method": "CreateQoSPolicy",
  "params": {
    "name": "bronze",
    "qos": {
      "minIOPS": 50,
      "maxIOPS": 15000,
      "burstIOPS": 15000
    }
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": []
    }
  }
}

```

Nuovo dalla versione

10,0

Crea volume

Puoi usare il `CreateVolume` metodo per creare un nuovo volume vuoto sul cluster. Non appena il volume viene creato, è disponibile per la connessione tramite iSCSI.

I volumi creati senza valori QoS specificati utilizzano i valori predefiniti. È possibile visualizzare i valori predefiniti per un volume utilizzando `GetDefaultQoS` metodo.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
access	Modalità di accesso al volume. Se questo parametro è incluso, l'unico valore supportato è snapMirrorTarget.	corda	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: associa il volume alla policy QoS specificata nel parametro QoSPolicyID. • false: Non associare il volume alla policy QoS specificata nel parametro QoSPolicyID. Se impostato su false, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi una policy QoS nel parametro QoSPolicy.	booleano	VERO	NO
attributes	Elenco di 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

Nome	Descrizione	Tipo	Valore predefinito	Necessario
dontMoveforIopsRebalance	Impedisce lo spostamento di un volume durante il bilanciamento del carico con IOPS effettivi. Questa impostazione è disponibile a partire da Element 12.8 ed è efficace solo quando "VolumeLoadBalanceOnActualIOPS" è abilitato. Valori possibili: • <code>true</code>: Il volume non bilancia il carico in base agli IOPS effettivi. • <code>false</code>: Il volume bilancia il carico in base agli IOPS effettivi. Nota: il bilanciamento per l'alta disponibilità (guasto del nodo) ha la precedenza su VolumeLoadBalanceOnActualIOPS e dontMoveforIopsRebalance.	booleano	falso	NO
enable512e	Abilita l'emulazione del settore da 512 byte. Valori possibili: • <code>true</code>: Il volume fornisce l'emulazione del settore da 512 byte. • <code>false</code>: L'emulazione 512e non è abilitata.	booleano	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
enableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con 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 snapshot disponibili su un volume. Utilizzare questa opzione per limitare il consumo di snapshot FIFO degli slot snapshot disponibili. Se omissso, il valore predefinito è 24.	intero	24	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
minFifoSize	Specifica il numero minimo di slot snapshot First-In-First-Out (FIFO) riservati dal volume. Ciò garantisce che se si utilizzano sia snapshot FIFO che snapshot non FIFO su un volume, gli snapshot non FIFO non consumino involontariamente troppi slot FIFO. Garantisce inoltre che almeno questo numero di snapshot FIFO siano sempre disponibili. Poiché gli snapshot FIFO e non FIFO condividono lo stesso pool, minFifoSize riduce della stessa quantità il numero totale di possibili snapshot non FIFO. Se omissso, il valore predefinito è 0.	intero	0	NO
name	Nome del gruppo di accesso al volume (può essere specificato dall'utente). Non è obbligatorio che sia unico, ma è consigliato. Deve essere lungo da 1 a 64 caratteri.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
qos	Impostazioni iniziali della qualità del servizio per questo volume. Se non ne viene specificato alcuno, vengono utilizzati i valori predefiniti. 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 è mutuamente esclusivo con il qos parametro.	intero	Nessuno	NO
totalSize	Dimensione totale del volume, in byte. La dimensione è arrotondata al megabyte più vicino.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
volume	Oggetto contenente informazioni sul volume appena creato.	volume
ID volume	VolumeID per il volume appena creato.	intero

Nome	Descrizione	Tipo
curva	La curva è un insieme di coppie chiave-valore. Le chiavi sono le dimensioni I/O in byte. I valori rappresentano il costo di esecuzione di un IOP a una dimensione I/O specifica. La curva è calcolata in relazione a un'operazione da 4096 byte impostata a 100 IOPS.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateVolume",
  "params": {
    "name": "testit",
    "accountID": 22,
    "dontMoveForIopsRebalance": true,
    "totalSize": 1000000000000,
    "enable512e": false,
    "attributes": {},
    "qos": {
      "minIOPS": 500,
      "maxIOPS": 27000,
      "burstIOPS": 27000,
      "burstTime": 60
    }
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "curve": {
      "1048576": 15000,
      "131072": 1950,
      "16384": 270,
```



```

        "262144": 3900,
        "32768": 500,
        "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
    },
    "volume": {
        "access": "readWrite",
        "accountID": 22,
        "attributes": {},
        "blockSize": 4096,
        "createTime": "2024-04-02T13:03:02Z",
        "currentProtectionScheme": "doubleHelix",
        "deleteTime": "",
        "dontMoveForIopsRebalance": true,
        "enable512e": false,
        "enableSnapMirrorReplication": false,
        "fifoSize": 24,
        "iqn": "iqn.2010-01.com.solidfire:mysqldata.677",
        "lastAccessTime": null,
        "lastAccessTimeIO": null,
        "minFifoSize": 0,
        "name": "testit",
        "previousProtectionScheme": null,
        "purgeTime": "",
        "qos": {
            "burstIOPS": 27000,
            "burstTime": 60,
            "curve": {
                "1048576": 15000,
                "131072": 1950,
                "16384": 270,
                "262144": 3900,
                "32768": 500,
                "4096": 100,
                "524288": 7600,
                "65536": 1000,
                "8192": 160
            },
            "maxIOPS": 27000,
            "minIOPS": 500
        },
        "qosPolicyID": null,
        "scsiEUIDeviceID": "3365657500000140f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000003365657500000140",
    },

```

```

        "sliceCount": 0,
        "status": "active",
        "totalSize": 1000000716800,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeConsistencyGroupUUID": "8ed68e57-13ee-47df-8381-
29b125142718",
        "volumeID": 320,
        "volumePairs": [],
        "volumeUUID": "e0e2c938-4ecd-4de9-albe-f6b17c93ce5d"
    },
    "volumeID": 320
}
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniQoS predefinito](#)

Crea destinazione di backup

Puoi usare `CreateBackupTarget` per creare e memorizzare le informazioni sulla destinazione del backup in modo da non doverle reinserire ogni volta che viene creato un backup.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome per la destinazione del backup.	corda	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	Sì (ma può essere vuoto)

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
backupTargetID	Identificatore univoco assegnato alla nuova destinazione di backup.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateBackupTarget",
  "params": {
    "name": "mytargetbackup"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "backupTargetID": 1
  }
}
```

Nuovo dalla versione

9,6

Elimina QoSPolicy

Puoi usare il `DeleteQoSPolicy` metodo per eliminare una policy QoS dal sistema. Le impostazioni QoS per tutti i volumi creati o modificati con questa policy non saranno interessate.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
qosPolicyID	ID del criterio QoS da eliminare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 663,
  "method": "DeleteQoSPolicy",
  "params": {
    "qosPolicyID": 4
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 663,
  "result": {}
}
```

Nuovo dalla versione

9,6

Elimina volume

Puoi usare il `DeleteVolume` metodo per contrassegnare un volume attivo per l'eliminazione. Se contrassegnato, il volume viene eliminato definitivamente una volta trascorso l'intervallo di pulizia.

Dopo aver effettuato una richiesta di eliminazione di un volume, tutte le connessioni iSCSI attive al volume vengono immediatamente terminate e non sono consentite ulteriori connessioni finché il volume si trova in questo stato. Un volume contrassegnato non viene restituito nelle richieste di individuazione della destinazione.

Gli snapshot di un volume contrassegnato per l'eliminazione non saranno interessati. Gli snapshot vengono conservati finché il volume non viene eliminato dal sistema. Se un volume è contrassegnato per l'eliminazione ed è in corso un'operazione di lettura o scrittura di un volume in blocco, l'operazione di lettura o scrittura di un volume in blocco viene interrotta.

Se il volume eliminato è associato a un volume, la replica tra i volumi associati viene sospesa e nessun dato viene trasferito da o verso di esso mentre è in stato di eliminazione. Il volume remoto a cui era associato il volume eliminato entra nello stato `PausedMisconfigured` e i dati non vengono più inviati ad esso o dal volume

eliminato. Finché il volume eliminato non viene eliminato, è possibile ripristinarlo e riprendere il trasferimento dei dati. Se il volume eliminato viene eliminato dal sistema, il volume a cui era associato entra nello stato `StoppedMisconfigured` e lo stato di associazione del volume viene rimosso. Il volume eliminato diventa definitivamente non disponibile.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	ID del volume da eliminare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
volume	Oggetto contenente informazioni sul volume eliminato.	volume
ID volume	VolumeID del volume eliminato.	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 di esecuzione di un IOP a una dimensione I/O specifica. La curva è calcolata in relazione a un'operazione da 4096 byte impostata a 100 IOPS.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteVolume",
  "params": {
    "volumeID" : 5
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": "6a796179000000005f47acc0100000000",
      "scsiNAADeviceID": "6f47acc10000000006a796179000000005",
      "sliceCount": 1,
      "status": "deleted",
      "totalSize": 1000341504,
      "virtualVolumeID": null,
      "volumeAccessGroups": [
```

```

    1
  ],
  "volumeID": 5,
  "volumePairs": []
}
}
}

```

Nuovo dalla versione

9,6

EliminaVolumi

Puoi usare il `DeleteVolumes` metodo per contrassegnare più volumi attivi (fino a 500) per l'eliminazione. Se contrassegnato, il volume viene eliminato definitivamente una volta trascorso l'intervallo di pulizia.

Dopo aver effettuato una richiesta di eliminazione dei volumi, tutte le connessioni iSCSI attive ai volumi vengono immediatamente terminate e non sono consentite ulteriori connessioni finché i volumi si trovano in questo stato. Un volume contrassegnato non viene restituito nelle richieste di individuazione della destinazione.

Gli snapshot di un volume contrassegnato per l'eliminazione non saranno interessati. Gli snapshot vengono conservati finché il volume non viene eliminato dal sistema. Se un volume è contrassegnato per l'eliminazione ed è in corso un'operazione di lettura o scrittura di un volume in blocco, l'operazione di lettura o scrittura di un volume in blocco viene interrotta.

Se i volumi eliminati sono associati a un volume, la replica tra i volumi associati viene sospesa e nessun dato viene trasferito a essi o da essi mentre sono in stato di eliminazione. I volumi remoti a cui erano associati i volumi eliminati entrano nello stato `PausedMisconfigured` e i dati non vengono più inviati a essi o dai volumi eliminati. Finché i volumi eliminati non vengono eliminati, è possibile ripristinarli e riprendere il trasferimento dei dati. Se i volumi eliminati vengono eliminati dal sistema, i volumi a cui erano associati entrano nello stato `StoppedMisconfigured` e lo stato di associazione del volume viene rimosso. I volumi eliminati diventano definitivamente non disponibili.

Parametri

Questo metodo ha i seguenti parametri di input.



È obbligatorio almeno uno dei seguenti parametri e devi utilizzarne solo uno (sono tutti reciprocamente esclusivi).

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeID	Elenco degli ID dei volumi da eliminare dal sistema.	array di interi	Nessuno	Vedi Nota.

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroup IDs	Un elenco di ID di 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 di interi	Nessuno	Vedi Nota.
ID account	Un elenco di ID account. Tutti i volumi di questi account vengono eliminati dal sistema.	array di interi	Nessuno	Vedi Nota.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
volumi	Informazioni sul volume appena eliminato.	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 di esecuzione di un IOP a una dimensione I/O specifica. La curva è calcolata in relazione a un'operazione da 4096 byte impostata a 100 IOPS.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteVolumes",
  "params": {
    "accountIDs" : [1, 2, 3]
  },
  "id" : 1
}
```


Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": "707a7372000000001f47acc0100000000",
      "scsiNAADeviceID": "6f47acc1000000000707a737200000001",
      "status": "active",
      "totalSize": 10000003072,
      "virtualVolumeID": 5,
      "volumeAccessGroups": [],
      "volumePairs": [],
      "volumeID": 1
    } ]
  }
}
```

Nuovo dalla versione

9,6

Ottieni destinazione di backup

Puoi usare il `GetBackupTarget` Metodo per restituire informazioni su una destinazione di backup specifica che hai creato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
attributi	Elenco di 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.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
backupTarget	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 1,
  "method": "GetBackupTarget",
  "params": {
    "backupTargetID": 1
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "backupTarget": {
      "attributes" : {
        "size" : 100
      },
      "backupTargetID" : 1,
      "name" : "mytargetbackup"
    }
  }
}
```

Nuovo dalla versione

9,6

Ottieni statistiche sul volume

Puoi usare il `GetVolumeStats` metodo per ottenere misurazioni di attività di alto livello per un singolo volume. I valori sono cumulativi a partire dalla creazione del volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	Specifica il volume per il quale vengono raccolte le statistiche.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeStats	Informazioni sull'attività volumetrica.	volumeStats

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVolumeStats",
  "params": {
    "volumeID": 32
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "volumeStats": [
      {
        "accountID": 1,
        "actualIOPS": 4,
        "asyncDelay": null,
        "averageIOPSize": 5970,
        "burstIOPSCredit": 0,
        "clientQueueDepth": 0,
        "desiredMetadataHosts": null,
        "latencyUSec": 474,
        "metadataHosts": {
          "deadSecondaries": [],
          "liveSecondaries": [
            13
          ],
          "primary": 25
        },
        "nonZeroBlocks": 34931222,
        "normalizedIOPS": 4,
        "readBytes": 1282491003392,
        "readBytesLastSample": 0,
        "readLatencyUSec": 0,
        "readLatencyUSecTotal": 4581669750,
        "readOps": 15592933,
        "readOpsLastSample": 0,
        "samplePeriodMSec": 500,
        "sliceIopsStats": {
          "largeStatistics": {
            "averageReadIops": 17,
            "averageTotalIops": 43,
```

```

        "averageWriteIops": 26,
        "nSamples": 24,
        "peakReadIops": 19,
        "peakTotalIops": 47,
        "peakWriteIops": 30,
        "sliceID": 1
    },
    "smallStatistics": {
        "averageReadIops": 17,
        "averageTotalIops": 42,
        "averageWriteIops": 25,
        "nSamples": 120,
        "peakReadIops": 173,
        "peakTotalIops": 249,
        "peakWriteIops": 77,
        "sliceID": 1
    }
},
"throttle": 0,
"timestamp": "2025-02-03T21:18:38.880100Z",
"unalignedReads": 167319,
"unalignedWrites": 90836,
"volumeAccessGroups": [
    1
],
"volumeID": 1,
"volumeSize": 2147483648000,
"volumeUtilization": 0.00026666666666666667,
"writeBytes": 1385173585408,
"writeBytesLastSample": 12288,
"writeLatencyUsec": 474,
"writeLatencyUsecTotal": 11233350905,
"writeOps": 157060458,
"writeOpsLastSample": 2,
"zeroBlocks": 489356778
}
}
}

```

Nuovo dalla versione

9,6

OttieniQoS predefinito

Puoi usare il `GetDefaultQoS` metodo per ottenere i valori predefiniti della qualità del

servizio (QoS) per un volume appena creato.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
Qualità del servizio	I valori QoS predefiniti.	Qualità del servizio

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetDefaultQoS",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  }
}
```

Nuovo dalla versione

9,6

Ottieni la politica QoSPolicy

Puoi usare il `GetQoSPolicy` metodo per ottenere dettagli su una specifica policy QoS dal sistema.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
qosPolicyID	L'ID della policy da recuperare.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
Politica QOS	Dettagli della policy QoS richiesta.	Politica QoSP

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetQoSPolicy",
  "params": {
    "qosPolicyID": 2
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      ]
    }
  }
}
```


Nuovo dalla versione

10,0

OttieniConteggioVolume

Puoi usare il `GetVolumeCount` metodo per ottenere il numero di volumi attualmente presenti nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
contare	Numero di volumi attualmente presenti nel sistema.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVolumeCount",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "count": 7
  }
}
```

Nuovo dalla versione

9,6

OttieniEfficienzaVolume

Puoi usare il `GetVolumeEfficiency` metodo per ottenere informazioni su un volume. Per calcolare la capacità viene utilizzato solo il volume fornito come parametro in questo metodo API.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	Specifica il volume per cui viene calcolata la capacità.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
compressione	Quantità di spazio risparmiata comprimendo i dati su un singolo volume. Espresso come rapporto, dove 1 indica che i dati sono stati memorizzati senza essere compressi.	galleggiante
deduplicazione	Quantità di spazio risparmiata su un singolo volume evitando di duplicare i dati. Espresso come rapporto.	galleggiante
volumi mancanti	I volumi che non è stato possibile interrogare per i dati di efficienza. I volumi mancanti possono essere causati da Garbage Collection (GC) eseguito da meno di un'ora, da una temporanea perdita di rete o da servizi riavviati dopo il ciclo GC.	array di interi
thinProvisioning	Rapporto tra lo spazio utilizzato e la quantità di spazio allocato per l'archiviazione dei dati. Espresso come rapporto.	galleggiante

marca temporale	L'ultima volta che sono stati raccolti dati sull'efficienza dopo GC.	Stringa di dati ISO 8601

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVolumeEfficiency",
  "params": {
    "volumeID": 606
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "compression": 2.001591240821456,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1.009861932938856,
    "timestamp": "2014-03-10T16:06:33Z"
  }
}
```

Nuovo dalla versione

9,6

ListActiveVolumes

Puoi usare il `ListActiveVolumes` metodo per ottenere l'elenco dei volumi attivi attualmente presenti nel sistema. L'elenco dei volumi è ordinato in base all'ID del volume e può essere restituito in più parti (pagine).

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
includeVirtualVolumes	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 da restituire. Se non esiste alcun volume con questo VolumeID, come inizio dell'elenco viene utilizzato il volume successivo in base all'ordine di VolumeID. Per scorrere l'elenco, passare il VolumeID dell'ultimo volume nella risposta precedente + 1.	intero	0	NO
limite	Numero massimo di oggetti di informazioni sul volume da restituire. 0 (zero) restituisce tutti i volumi (illimitati).	intero	(illimitato)	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi attivi.	volume vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListActiveVolumes",
  "params": {
    "startVolumeID" : 0,
    "limit" : 1000
  },
  "id" : 1
}
```

Esempio di risposta

Data la lunghezza di questo esempio di risposta, esso è documentato in un argomento supplementare.

Nuovo dalla versione

9,6

ListBackupTargets

Puoi usare il `ListBackupTargets` metodo per ottenere informazioni su tutte le destinazioni di backup create.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
backupTargets	Oggetti restituiti per ogni destinazione di backup. Oggetti inclusi: • attributi: elenco di coppie nome-valore nel formato oggetto JSON. (oggetto JSON) • backupTargetID: identificatore univoco assegnato alla destinazione del backup. (numero intero) • nome: Nome della destinazione del backup. (corda)	Oggetto JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListBackupTargets",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "backupTargets": [
      {
        "attributes" : {},
        "backupTargetID" : 1,
        "name" : "mytargetbackup"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

ListBulkVolumeJobs

Puoi usare il `ListBulkVolumeJobs` Metodo per ottenere informazioni su ogni operazione di lettura o scrittura di volumi di grandi dimensioni che si verifica nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
bulkVolumeJobs	Una serie di informazioni per ogni lavoro di grandi dimensioni.	bulkVolumeJob vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListBulkVolumeJobs",
  "params": {
    },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": "eafffb0526d4fb47107061f09bfc9a806",
        "percentComplete": 8,
        "remainingTime": 506,
        "script": "bv_internal.py",
        "snapshotID": 509,
        "srcVolumeID": 3,
        "status": "running",
        "type": "read"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ElencoVolumiEliminati

Puoi usare il `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	Necessario
includeVirtualVolumes	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	VERO	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi eliminati.	volume vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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": "306f746f000000017f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000017",
        "sliceCount": 1,
        "status": "deleted",
        "totalSize": 1396703232,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 23,
        "volumePairs": []
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListQoSPolicies

Puoi usare il `ListQoSPolicies` metodo per elencare le impostazioni di tutte le policy QoS sul sistema.

Parametri

Questo metodo non ha parametri di input.

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
qosPolicies	Un elenco di dettagli su ciascuna policy QoS.	Politica QoS vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 231,
  "method": "ListQoSPolicies",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    ]
}
]
}
}

```

Nuovo dalla versione

10,0

ListSyncJobs

Puoi usare il `ListSyncJobs` metodo per ottenere informazioni sui processi di sincronizzazione in esecuzione su un cluster di archiviazione Element. Questo metodo restituisce informazioni sui processi di sincronizzazione slice, clone, block e remote.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>syncJobs</code>	Elenco di oggetti che descrivono i processi di sincronizzazione attualmente in esecuzione nel sistema.	sincronizzazioneJob vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListSyncJobs",
  "params": { },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
]
}

```

Nuovo dalla versione

9,6

ElencoVolumeQoSHistogrammi

Puoi usare il `ListVolumeQoSHistograms` metodo per generare un istogramma dell'utilizzo della qualità del servizio (QoS) per un volume 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	Necessario
volumeID	Un elenco facoltativo di ID volume che specifica per quali volumi devono essere generati istogrammi QoS.	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
qosHistograms	Un elenco di oggetti che descrivono l'utilizzo del volume per uno o più volumi.	Matrice di oggetti JSON

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeQoSHistograms",
  "params": {
    "volumeIDs": [1]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
}
]
}
}

```

ElencoVolumi

Puoi usare il `ListVolumes` metodo per ottenere un elenco dei volumi presenti 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	Necessario
conti	Vengono restituiti solo i volumi di proprietà degli account specificati qui. Mutuamente esclusivi con il parametro volumeIDs.	array di interi	Nessuno	NO
includeVirtualVolumes	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	VERO	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
è accoppiato	Restituisce i volumi accoppiati o non accoppiati. Valori possibili: • true: restituisce tutti i volumi accoppiati. • false: restituisce tutti i volumi non accoppiati.	booleano	Nessuno	NO
limite	Consente di impostare il numero massimo di risultati di volume restituiti. Mutuamente esclusivi con il parametro volumeIDs.	intero	10000	NO
startVolumeID	Vengono restituiti solo i volumi con un ID maggiore o uguale a questo valore. Mutuamente esclusivi con il parametro volumeIDs.	intero	Nessuno	NO
volumeID	Un elenco di ID volume. Se si specifica questo parametro, gli altri parametri operano solo su questo set di volumi. Mutuamente esclusivi con i parametri accounts, startVolumeID e limit.	array di interi	NO	NO
NomeVolume	Vengono restituite solo le informazioni sull'oggetto volume che corrispondono al nome del volume.	corda	NO	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeStatus	Vengono restituiti solo i volumi con uno stato uguale al valore dello stato. Valori possibili: • creazione • creazione di istantanee • attivo • cancellato	corda	NO	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumi	Elenco dei volumi.	volume vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumes",
  "params": {
    "volumeIDs": [1],
    "volumeStatus": "active",
    "isPaired": "false"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": "6a796179000000001f47acc0100000000",
        "scsiNAADeviceID": "6f47acc10000000006a79617900000001",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 5000658944,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 1,
        "volumePairs": []
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListVolumeStats

Puoi usare il `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 `volumeIDs`). I valori di misurazione sono cumulativi a partire dalla creazione del volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>includeVirtualVolumes</code>	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su <code>false</code> .	booleano	VERO	NO
<code>volumeID</code>	Un elenco di volumi da cui recuperare informazioni sulle attività.	array di interi	NO	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>volumeStats</code>	Elenco delle informazioni sull'attività di volume.	volumeStats vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeStats",
  "params": {
    "volumeIDs": [1]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  }
]
}
}

```

Nuovo dalla versione

9,6

ListVolumesForAccount

Puoi usare il `ListVolumesForAccount` Metodo per elencare i volumi attivi e (in attesa) eliminati per un account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>includeVirtualVolumes</code>	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	VERO	NO
ID account	Vengono restituiti tutti i volumi di proprietà di questo accountID.	intero	NO	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo

volumi	Elenco delle informazioni sul volume.	volume vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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": "306f746f000000019f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000019",
        "sliceCount": 1,
        "status": "active",
        "totalSize": 1000341504,
        "virtualVolumeID": null,
        "volumeAccessGroups": [],
        "volumeID": 25,
        "volumePairs": []
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListVolumeStatsByAccount

Puoi usare il `ListVolumeStatsByAccount` metodo per elencare le misurazioni dell'attività di volume di alto livello per ogni account. I valori vengono sommati da tutti i volumi posseduti dall'account.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>includeVirtualVolumes</code>	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su <code>false</code> .	booleano	VERO	NO
<code>conti</code>	Un elenco di ID account per i quali restituire le statistiche del volume. Se omesso, vengono restituite le statistiche per tutti gli account.	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>volumeStats</code>	Elenco delle informazioni sull'attività del volume per ciascun account. Nota: il membro <code>volumeID</code> è 0 per ciascuna voce, poiché i valori rappresentano la somma di tutti i volumi posseduti dall'account.	<code>volumeStats</code> vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeStatsByAccount",
  "params": {"accounts": [3]},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

ListVolumeStatsByVirtualVolume

Puoi usare il `ListVolumeStatsByVirtualVolume` Metodo per elencare le statistiche

del volume per tutti i volumi nel 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	Necessario
virtualVolumeIds	Un elenco di uno o più ID di volumi virtuali per i quali recuperare informazioni. Se si specifica questo parametro, il metodo restituisce informazioni solo su questi volumi virtuali.	Array di stringhe UUID	NO	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeStats	Un elenco di oggetti contenenti informazioni sulle attività per ciascun volume virtuale nel sistema.	volumeStats vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeStatsByVirtualVolume",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    }
  ]
}

```

Nuovo dalla versione

9,6

ListVolumeStatsByVolume

Puoi usare il `ListVolumeStatsByVolume` metodo per elencare le misurazioni dell'attività di alto livello per ogni volume, per volume. I valori sono cumulativi a partire dalla creazione del volume.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>includeVirtualVolumes</code>	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su <code>false</code> .	booleano	VERO	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>volumeStats</code>	Elenco delle informazioni sull'attività di volume.	volumeStats vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeStatsByVolume",
  "params": {},
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
```

```

"id": 1,
"result": {
  "volumeStats": [
    {
      "accountID": 1,
      "actualIOPS": 4,
      "asyncDelay": null,
      "averageIOPSize": 5970,
      "burstIOPSCredit": 0,
      "clientQueueDepth": 0,
      "desiredMetadataHosts": null,
      "latencyUSec": 474,
      "metadataHosts": {
        "deadSecondaries": [],
        "liveSecondaries": [
          13
        ],
        "primary": 25
      },
      "nonZeroBlocks": 34931222,
      "normalizedIOPS": 4,
      "readBytes": 1282491003392,
      "readBytesLastSample": 0,
      "readLatencyUSec": 0,
      "readLatencyUSecTotal": 4581669750,
      "readOps": 15592933,
      "readOpsLastSample": 0,
      "samplePeriodMSec": 500,
      "sliceIopsStats": {
        "largeStatistics": {
          "averageReadIops": 17,
          "averageTotalIops": 43,
          "averageWriteIops": 26,
          "nSamples": 24,
          "peakReadIops": 19,
          "peakTotalIops": 47,
          "peakWriteIops": 30,
          "sliceID": 1
        },
        "smallStatistics": {
          "averageReadIops": 17,
          "averageTotalIops": 42,
          "averageWriteIops": 25,
          "nSamples": 120,
          "peakReadIops": 173,
          "peakTotalIops": 249,

```

```

        "peakWriteIops": 77,
        "sliceID": 1
    }
},
"throttle": 0,
"timestamp": "2025-02-03T21:18:38.880100Z",
"unalignedReads": 167319,
"unalignedWrites": 90836,
"volumeAccessGroups": [
    1
],
"volumeID": 1,
"volumeSize": 2147483648000,
"volumeUtilization": 0.00026666666666666667,
"writeBytes": 1385173585408,
"writeBytesLastSample": 12288,
"writeLatencyUsec": 474,
"writeLatencyUsecTotal": 11233350905,
"writeOps": 157060458,
"writeOpsLastSample": 2,
"zeroBlocks": 489356778
}
]
}
}

```

Nuovo dalla versione

9,6

ListVolumeStatsByVolumeAccessGroup

Puoi usare il `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	Necessario
includeVirtualVolumes	Per impostazione predefinita, i volumi virtuali sono inclusi nella risposta. Per escludere i volumi virtuali, impostare su false.	booleano	VERO	NO
volumeAccessGroups	Un array di VolumeAccessGroupID per i quali viene restituita l'attività del volume. Se omissso, vengono restituite le statistiche per tutti i gruppi di accesso al volume.	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeStats	Elenco delle informazioni sull'attività del volume per tutti i volumi nel gruppo di accesso al 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

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVolumeStatsByVolumeAccessGroup",
  "params": {"volumeAccessGroups": [1]},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

Modifica destinazione backup

Puoi usare il `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	Necessario
backupTargetID	ID target univoco per il target da modificare.	intero	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
nome	Nuovo nome per la destinazione del backup.	corda	Nessuno	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyBackupTarget",
  "params": {
    "backupTargetID" : 1,
    "name": "yourtargetS3"
    "attributes" : {
      "size" : 500,
    }
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Modifica politica QoS

Puoi usare il `ModifyQoSPolicy` metodo per modificare una policy QoS esistente sul sistema.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
qosPolicyID	L'ID della policy da modificare.	intero	Nessuno	Sì
nome	Se fornito, il nome della policy QoS (ad esempio oro, platino, argento) viene modificato in questo valore.	corda	Nessuno	NO
qualità	Se fornite, le impostazioni QoS per questo criterio vengono modificate in base a queste impostazioni. È possibile fornire valori QoS parziali e modificare solo alcune delle impostazioni QoS.	Oggetto QoS	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
Politica QOS	Dettagli della nuova politica QoS modificata.	Politica QoSP

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 1950,
  "method": "ModifyQoSPolicy",
  "params": {
    "qosPolicyID": 2,
    "qos": {
      "minIOPS": 51,
      "maxIOPS": 15002,
      "burstIOPS": 15002
    }
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      ]
    }
  }
}

```

Nuovo dalla versione

10,0

ModificaVolume

Puoi usare il `ModifyVolume` metodo per modificare le impostazioni su un volume esistente. È possibile apportare modifiche a un volume alla volta e le modifiche verranno applicate immediatamente.

Se non si specificano i valori QoS quando si modifica un volume, questi rimangono invariati rispetto a prima della modifica. È possibile recuperare i valori QoS predefiniti per un volume appena creato eseguendo il comando `GetDefaultQoS` metodo.

Quando è necessario aumentare le dimensioni di un volume replicato, procedere nel seguente ordine per evitare errori di replica:

1. Aumentare le dimensioni del volume con l'accesso replicationTarget.
2. Aumentare le dimensioni della sorgente o del volume con accesso readWrite.

Assicurarsi che i volumi di destinazione e di origine abbiano le stesse dimensioni.



Se si modifica lo stato di accesso in bloccato o replicationTarget, tutte le connessioni iSCSI esistenti vengono terminate.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	VolumeID del volume da modificare.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accesso	Accesso consentito per il volume. Valori possibili: • readOnly: Sono consentite solo le operazioni di lettura. • readWrite: Sono consentite letture e 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 SnapMirror .	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID account	L'accountID a cui viene riassegnato il volume. Se non viene specificato alcun nome, verrà utilizzato il nome dell'account precedente.	intero	Nessuno	NO
associare alla politica QoS	Associare il volume al criterio QoS specificato. Valori possibili: • <code>true</code>: associa il volume alla policy QoS specificata nel parametro <code>QoSPolicyID</code>. • <code>false</code>: Non associare il volume alla policy QoS specificata nel parametro <code>QoSPolicyID</code>. Se impostato su <code>false</code>, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi una policy QoS nel parametro <code>QoSPolicy</code>.	booleano	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
createTime	Una stringa di data ISO 8601 da impostare come data di creazione del nuovo volume. Obbligatorio se setCreateTime è impostato su true.	Stringa ISO 8601	Nessuno	NO
dontMoveforIopsRebalance	Impedisce lo spostamento di un volume durante il bilanciamento del carico con IOPS effettivi. Questa impostazione è disponibile a partire da Element 12.8 ed è efficace solo quando "VolumeLoadBalanceOnActualIOPS" è abilitato. Valori possibili: • true: Il volume non bilancia il carico in base agli IOPS effettivi. • false: Il volume bilancia il carico in base agli IOPS effettivi. Nota: il bilanciamento per l'alta disponibilità (guasto del nodo) ha la precedenza su VolumeLoadBalanceOnActualIOPS e dontMoveforIopsRebalance.	booleano	falso	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
enableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con 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 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 conteggio attuale degli snapshot FIFO.	intero	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
minFifoSize	Specifica il numero di slot snapshot riservati solo per snapshot First-In-First-Out (FIFO). Poiché gli snapshot FIFO e non FIFO condividono lo stesso pool, il parametro minFifoSize riduce della stessa quantità il numero totale di possibili snapshot non FIFO. Si noti che non è possibile modificare questo valore in modo che entri in conflitto con il conteggio attuale degli 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 sulla sorgente prima di scriverli sulla destinazione. • sync: Non attende la conferma della trasmissione dei dati dalla sorgente per iniziare a scrivere i dati sulla destinazione.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
qualità	Le nuove impostazioni di qualità del servizio per questo volume. Se non specificato, le impostazioni QoS non vengono modificate. Valori possibili: • minIOPS • maxIOPS • burstIOPS	Qualità del servizio	Nessuno	NO
qosPolicyID	ID del criterio le cui impostazioni QoS devono essere applicate ai volumi specificati. Questo parametro è mutuamente esclusivo con il parametro qos.	intero	Nessuno	NO
impostaCreateTime	Impostare su true per modificare la data registrata della creazione del volume.	booleano	Nessuno	NO
dimensione totale	La nuova dimensione del volume in byte. 1000000000 equivale a 1 GB. La dimensione è arrotondata al megabyte più vicino. Questo parametro può essere utilizzato solo per aumentare le dimensioni di un volume.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volume	Oggetto contenente informazioni sul volume appena modificato.	volume

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyVolume",
  "params": {
    "volumeID": 319,
    "access": "readWrite",
    "dontMoveForIopsRebalance": false
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "volume": {
      "access": "readWrite",
      "accountID": 22,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2024-04-01T19:39:40Z",
      "currentProtectionScheme": "doubleHelix",
      "deleteTime": "",
      "dontMoveForIopsRebalance": false,
      "enable512e": false,
      "enableSnapMirrorReplication": false,
      "fifoSize": 24,
      "iqn": "iqn.2010-01.com.solidfire:3eeu.suite40.319",
      "lastAccessTime": "2024-04-02T12:41:34Z",
      "lastAccessTimeIO": "2024-04-01T20:41:19Z",
      "minFifoSize": 0,
      "name": "suite40",
      "previousProtectionScheme": null,
      "purgeTime": ""
    }
  }
}
```

```

    "qos": {
      "burstIOPS": 27000,
      "burstTime": 60,
      "curve": {
        "1048576": 15000,
        "131072": 1950,
        "16384": 270,
        "262144": 3900,
        "32768": 500, "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
      },
      "maxIOPS": 27000,
      "minIOPS": 500
    },
    "qosPolicyID": null,
    "scsiEUIDeviceID": "336565750000013ff47acc0100000000",
    "scsiNAADeviceID": "6f47acc100000000336565750000013f",
    "sliceCount": 1,
    "status": "active",
    "totalSize": 1000000716800,
    "virtualVolumeID": null,
    "volumeAccessGroups": [
      22
    ],
    "volumeConsistencyGroupUUID": "3003109e-6e75-444c-8cee-470d641a09c3",
    "volumeID": 319,
    "volumePairs": [],
    "volumeUUID": "78203136-b0eb-454b-9f67-2c867ec7d7bb"
  }
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniQoS predefinito](#)

Modifica Volumi

Puoi usare il `ModifyVolumes` metodo per configurare fino a 500 volumi esistenti contemporaneamente. I cambiamenti avvengono immediatamente. Se `ModifyVolumes`

non riesce a modificare nessuno dei volumi specificati, nessuno dei volumi specificati viene modificato.

Se non si specificano 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 il comando `GetDefaultQoS` metodo.

Quando è necessario aumentare le dimensioni dei volumi da replicare, procedere nel seguente ordine per evitare errori di replica:

1. Aumentare le dimensioni del volume con l'accesso `replicationTarget`.
2. Aumentare le dimensioni della sorgente o del volume con accesso `readWrite`.

Assicurarsi che i volumi di destinazione e di origine abbiano le stesse dimensioni.



Se si modifica lo stato di accesso in bloccato o `replicationTarget`, tutte le connessioni iSCSI esistenti vengono terminate.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
accesso	Accesso consentito ai volumi. Valori possibili: • readOnly: Sono consentite solo le operazioni di lettura. • readWrite: Sono consentite letture e 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.	corda	Nessuno	NO
ID account	L'accountID a cui vengono riassegnati i volumi. Se non viene specificato alcun nome, verrà utilizzato il nome dell'account precedente.	intero	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
associare alla politica QoS	Associare il volume al criterio QoS specificato. Valori possibili: • <code>true</code>: associa il volume alla policy QoS specificata nel parametro <code>QoSPolicyID</code>. • <code>false</code>: Non associare il volume alla policy QoS specificata nel parametro <code>QoSPolicyID</code>. Se impostato su <code>false</code>, qualsiasi associazione di policy esistente viene rimossa, indipendentemente dal fatto che si specifichi una policy QoS nel parametro <code>QoSPolicy</code>.	booleano	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
<code>createTime</code>	Una stringa di data ISO 8601 da impostare come data di creazione del nuovo volume. Obbligatorio se <code>setCreateTime</code> è impostato su <code>true</code> .	Stringa ISO 8601	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
dontMoveforIopsRebalance	Impedisce lo spostamento di un volume durante il bilanciamento del carico con IOPS effettivi. Questa impostazione è disponibile a partire da Element 12.8 ed è efficace solo quando "VolumeLoadBalanceOnActualIOPS" è abilitato. Valori possibili: • <code>true</code>: Il volume non bilancia il carico in base agli IOPS effettivi. • <code>false</code>: Il volume bilancia il carico in base agli IOPS effettivi. Nota: il bilanciamento per l'alta disponibilità (guasto del nodo) ha la precedenza su VolumeLoadBalanceOnActualIOPS E dontMoveforIopsRebalance .	booleano	falso	NO
enableSnapMirrorReplication	Determina se il volume può essere utilizzato per la replica con endpoint SnapMirror . Valori possibili: • <code>true</code> • <code>false</code>	booleano	falso	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
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 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 conteggio attuale degli snapshot FIFO.	intero	Nessuno	NO
minFifoSize	Specifica il numero di slot snapshot riservati solo per snapshot First-In-First-Out (FIFO). Poiché gli snapshot FIFO e non FIFO condividono lo stesso pool, il parametro minFifoSize riduce della stessa quantità il numero totale di possibili snapshot non FIFO. Si noti che non è possibile modificare questo valore in modo che entri in conflitto con il conteggio attuale degli snapshot non FIFO.	intero	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
modalità	Modalità di replica del volume. Valori possibili: • asynch: Attende che il sistema riconosca che i dati sono memorizzati sulla sorgente prima di scriverli sulla destinazione. • sync: Non attende la conferma della trasmissione dei dati dalla sorgente per iniziare a scrivere i dati sulla destinazione.	corda	Nessuno	NO
qualità	Le nuove impostazioni della qualità del servizio per i volumi. Se non specificato, le impostazioni QoS non vengono modificate. Valori possibili: • minIOPS • maxIOPS • burstIOPS	Qualità del servizio	Nessuno	NO
qosPolicyID	ID del criterio le cui impostazioni QoS devono essere applicate ai volumi specificati. Questo parametro è mutuamente esclusivo con il parametro qos.	intero	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
impostaCreateTime	Impostare su true per modificare la data registrata della creazione del volume.	booleano	Nessuno	NO
dimensione totale	La nuova dimensione dei volumi in byte. 10000000000 equivale a 1 GB. La dimensione è arrotondata al megabyte più vicino. Questo parametro può essere utilizzato solo per aumentare le dimensioni di un volume.	intero	Nessuno	NO
volumeID	Un elenco di volumeID per i volumi da modificare.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volume	Un array di oggetti contenente informazioni su ogni volume appena modificato.	volume vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyVolumes",
  "params": {
    "volumeIDs": [319,22],
    "access": "readWrite",
    "dontMoveForIopsRebalance": false
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "volumes":
    {
      "access": "readWrite",
      "accountID": 22,
      "attributes": {},
      "blockSize": 4096,
      "createTime": "2024-04-01T19:39:40Z",
      "currentProtectionScheme": "doubleHelix",
      "deleteTime": "",
      "dontMoveForIopsRebalance": false,
      "enable512e": false,
      "enableSnapMirrorReplication": false,
      "fifoSize": 24,
      "iqn": "iqn.2010-01.com.solidfire:3eeu.suite40.319",
      "lastAccessTime": "2024-04-02T12:41:34Z",
      "lastAccessTimeIO": "2024-04-01T20:41:19Z",
      "minFifoSize": 0,
      "name": "suite40",
      "previousProtectionScheme": null,
      "purgeTime": "",
      "qos": {
        "burstIOPS": 27000,
        "burstTime": 60,
        "curve": {
          "1048576": 15000,
          "131072": 1950,
          "16384": 270,
          "262144": 3900,

```

```

        "32768": 500,
        "4096": 100,
        "524288": 7600,
        "65536": 1000,
        "8192": 160
    },
    "maxIOPS": 27000,
    "minIOPS": 500
},
"qosPolicyID": null,
"scsiEUIDeviceID": "336565750000013ff47acc0100000000",
"scsiNAADeviceID": "6f47acc100000000336565750000013f",
"sliceCount": 1,
"status": "active",
"totalSize": 1000000716800,
"virtualVolumeID": null,
"volumeAccessGroups": [
22
],
"volumeConsistencyGroupUUID": "3003109e-6e75-444c-8cee-
470d641a09c3",
"volumeID": 319,
"volumePairs": [],
"
}
}
}

```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[OttieniQoS predefinito](#)

PurgeDeletedVolume

Puoi usare il `PurgeDeletedVolume` metodo per eliminare immediatamente e definitivamente un volume che è stato eliminato. È necessario eliminare un volume utilizzando `DeleteVolume` prima che possa essere eliminato.

I volumi vengono eliminati automaticamente dopo un certo periodo di tempo, pertanto in genere non è necessario utilizzare questo metodo.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	VolumeID del volume da eliminare.	intero	NO	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "PurgeDeletedVolume",
  "params": {
    "volumeID" : 5
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[Elimina volume](#)

Elimina i volumi eliminati

Puoi usare il `PurgeDeletedVolumes` Metodo per eliminare immediatamente e definitivamente i volumi eliminati; è possibile utilizzare questo metodo per eliminare fino a 500 volumi contemporaneamente.

È necessario eliminare i volumi utilizzando `DeleteVolumes` prima che possano essere eliminati. I volumi vengono eliminati automaticamente dopo un certo periodo di tempo, pertanto in genere non è necessario utilizzare questo metodo.



Se si eliminano contemporaneamente un gran numero di volumi o se ai volumi eliminati sono associati molti snapshot, il metodo potrebbe non funzionare e restituire l'errore "xDBCConnectionLoss". In tal caso, riprovare la chiamata al metodo con un numero inferiore di volumi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeID	Un elenco di volumi ID da eliminare dal sistema.	array di interi	NO	NO
ID account	Un elenco di ID account. Tutti i volumi di tutti gli account specificati vengono eliminati dal sistema.	array di interi	NO	NO
volumeAccessGroup IDs	Un elenco di volumeAccessGroup ID. Tutti i volumi di tutti i gruppi di accesso ai volumi specificati vengono eliminati dal sistema.	array di interi	NO	NO

Nota: è possibile specificare solo uno dei parametri sopra indicati per ogni chiamata al metodo. Specificarne più di uno, o nessuno, genera un errore.

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "PurgeDeletedVolumes",
  "params": {
    "accountIDs" : [1, 2, 3]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[EliminaVolumi](#)

RimuoviBackupTarget

Puoi usare il `RemoveBackupTarget` metodo per rimuovere le destinazioni di backup.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
backupTargetID	ID target univoco del target da rimuovere.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveBackupTarget",
  "params": {
    "backupTargetID" : 1
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

RipristinaVolumeEliminato

Puoi usare il `RestoreDeletedVolume` metodo per contrassegnare nuovamente un volume eliminato 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	Necessario
ID volume	VolumeID del volume eliminato da ripristinare.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RestoreDeletedVolume",
  "params": {
    "volumeID" : 5
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Imposta QoS predefinito

Puoi usare il `setDefaultQoS` Metodo per configurare i valori predefiniti di qualità del servizio (QoS) (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	Necessario
minIOPS	Numero minimo di IOPS sostenuti forniti dal cluster a un volume.	intero	Nessuno	NO
IOPS massimi	Numero massimo di IOPS sostenuti forniti dal cluster a un volume.	intero	Nessuno	NO
burstIOPS	Numero massimo di IOPS consentito in uno scenario di burst breve.	intero	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
minIOPS	Numero minimo di IOPS sostenuti forniti dal cluster a un volume.	intero

Nome	Descrizione	Tipo
IOPS massimi	Numero massimo di IOPS sostenuti forniti dal cluster a un volume.	intero
burstIOPS	Numero massimo di IOPS consentito in uno scenario di burst breve.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "SetDefaultQoS",
  "params": {
    "burstIOPS":8000,
    "maxIOPS":1000,
    "minIOPS":200
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id":1,
  "result": {
    "burstIOPS":8000,
    "maxIOPS":1000,
    "minIOPS":200
  }
}
```

Nuovo dalla versione

9,6

StartBulkVolumeRead

Puoi usare il `StartBulkVolumeRead` metodo per avviare una sessione di lettura di massa su un volume specificato.

Su un volume possono essere eseguiti contemporaneamente solo due processi di volume di massa. Quando si inizializza la sessione, i dati vengono letti da un volume di archiviazione SolidFire per essere archiviati su una fonte di backup esterna. L'accesso ai dati esterni avviene tramite un server web in esecuzione su un nodo di archiviazione Element. Le informazioni sull'interazione con il server per l'accesso ai dati esterni vengono trasmesse tramite uno script in esecuzione sul sistema di archiviazione.

All'inizio di un'operazione di lettura di un volume in blocco, viene creato uno snapshot del volume, che viene eliminato al termine della lettura. È anche 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 il livello di riempimento del cluster è pari a 2 o 3. Gli snapshot non vengono creati quando il livello di riempimento del cluster è pari a 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
formato	Il formato dei dati del volume. Può essere: • uncompressed: Ogni byte del volume viene restituito senza alcuna compressione. • native: Vengono restituiti dati opachi, più piccoli e più efficienti da archiviare e scrivere in una successiva scrittura di volume di massa.	corda	Nessuno	Sì
ID volume	L'ID del volume da leggere.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID istantanea	ID di uno snapshot creato in precedenza, utilizzato per letture di volumi in blocco. Se non viene immesso alcun ID, viene creato uno snapshot dell'immagine del volume attivo corrente.	intero	Nessuno	NO
sceneggiatura	Il nome di uno script eseguibile. Se non viene specificato alcun nome di script, la chiave e l'URL sono necessari per accedere ai nodi di archiviazione Element. Lo script viene eseguito sul nodo primario e la chiave e l'URL vengono restituiti allo script in modo che sia possibile contattare il server Web locale.	corda	Nessuno	NO
Parametri di script	Parametri JSON da passare allo script.	Oggetto JSON	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON. " Saperne di più ".	Oggetto JSON	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	ID del processo asincrono da verificare per verificarne il completamento.	intero

chiave	Chiave opaca che identifica in modo univoco la sessione.	corda
URL	URL per accedere al server web del nodo.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "StartBulkVolumeRead",
  "params": {
    "volumeID" : 5,
    "format" : "native",
    "snapshotID" : 2
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "asyncHandle" : 1,
    "key" : "11eed8f086539205beeaadd981aad130",
    "url" : "https://127.0.0.1:44000/"
  }
}
```

Nuovo dalla versione

9,6

StartBulkVolumeWrite

Puoi usare il `StartBulkVolumeWrite` metodo per avviare una sessione di scrittura di volumi di grandi dimensioni su un volume specificato.

Su un volume possono essere eseguiti contemporaneamente solo due processi di volume di massa. Quando si inizializza la sessione, i dati vengono scritti su un volume di archiviazione Element da una fonte di backup esterna. L'accesso ai dati esterni avviene tramite un server web in esecuzione su un nodo di archiviazione

Element. Le informazioni sull'interazione con il server per l'accesso ai dati esterni vengono trasmesse tramite uno script in esecuzione sul sistema di archiviazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
formato	Il formato dei dati del volume. Può essere: • uncompressed: Ogni byte del volume viene restituito senza alcuna compressione. • native: Vengono restituiti dati opachi, più piccoli e più efficienti da archiviare e scrivere in una successiva scrittura di volume di massa.	corda	Nessuno	Sì
ID volume	ID del volume su cui scrivere.	intero	Nessuno	Sì
sceneggiatura	Il nome di uno script eseguibile. Se non viene specificato alcun nome di script, la chiave e l'URL sono necessari per accedere ai nodi di archiviazione Element. Lo script viene eseguito sul nodo primario e la chiave e l'URL vengono restituiti allo script in modo che sia possibile contattare il server Web locale.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
Parametri di script	Parametri JSON da passare allo script.	Oggetto JSON	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON. " Saperne di più ".	Oggetto JSON	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
asyncHandle	ID del processo asincrono da verificare per verificarne il completamento.	intero
chiave	Chiave opaca che identifica in modo univoco la sessione.	corda
URL	URL per accedere al server web del nodo.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "StartBulkVolumeWrite",
  "params": {
    "volumeID" : 5,
    "format"   : "native",
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result" : {
    "asyncHandle" : 1,
    "key" : "11eed8f086539205beeaadd981aad130",
    "url" : "https://127.0.0.1:44000/"
  }
}
```

Nuovo dalla versione

9,6

AggiornaStatoVolumeMassuale

Puoi usare il `UpdateBulkVolumeStatus` metodo per aggiornare lo stato di un lavoro di volume di massa avviato con `StartBulkVolumeRead` O `StartBulkVolumeWrite` metodi.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
chiave	La chiave assegnata durante l'inizializzazione di un StartBulkVolumeRead O StartBulkVolumeWrite sessione.	corda	Nessuno	Sì
stato	Il sistema imposta lo stato del lavoro di volume in blocco specificato. Valori possibili: • in esecuzione: lavori ancora attivi. • completo: Lavori svolti. • falliti: lavori che non sono riusciti.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
percentuale completata	Percentuale di avanzamento del lavoro di grandi volumi completato.	corda	Nessuno	NO
messaggio	Restituisce lo stato del lavoro di volume in blocco una volta completato.	corda	Nessuno	NO
attributi	Attributi JSON; aggiorna il contenuto del lavoro di volume in blocco.	Oggetto JSON	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
stato	Stato della sessione richiesta. Stato restituito: • preparazione • attivo • Fatto • fallito	corda
attributi	Restituisce gli attributi specificati nella chiamata al metodo. I valori vengono restituiti indipendentemente dal fatto che siano stati modificati o meno.	corda
URL	URL per accedere al server web del nodo; fornito solo se la sessione è ancora attiva.	corda

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "UpdateBulkVolumeStatus",
  "params": {
    "key": "0b2f532123225febda2625f55dcb0448",
    "status": "running"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result": {
    "status" : "running",
    "url" : "https://10.10.23.47:8443/"
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [StartBulkVolumeRead](#)
- [StartBulkVolumeWrite](#)

Metodi API del gruppo di accesso al volume

AggiungiIniziatoriAlGruppoAccessoVolume

Puoi usare il `AddInitiatorsToVolumeAccessGroup` metodo per aggiungere iniziatori a un gruppo di accesso al volume specificato.

Il formato accettato di un IQN di avvio 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 un trattino (`-`). Vedere il seguente esempio:

```
iqn.2010-01.com.solidfire:17oi.solidfire-0.1
```

Il formato accettato di un WWPN dell'iniziatore Fibre Channel 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	Necessario
iniziatori	Elenco di ID o 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 iniziatori, il metodo restituisce un errore se uno qualsiasi degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è deprecato; è consigliabile utilizzare gli ID degli iniziatori ogniqualvolta possibile.	array di interi o array di stringhe (obsoleto)		Sì
volumeAccessGroup ID	ID del gruppo di accesso al volume a cui aggiungere l'iniziatore.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	volumeAccessGroup

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 13171,
  "method": "AddInitiatorsToVolumeAccessGroup",
  "params": {
    "initiators": [116,117],
    "volumeAccessGroupID": 96
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      ]
    }
  }
}
```

Nuovo dalla versione

9,6

AggiungiVolumiAlGruppoAccessoVolumi

Puoi usare il `AddVolumesToVolumeAccessGroup` metodo per aggiungere volumi a un gruppo di accesso al volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumi	Elenco di volumiID da aggiungere al gruppo di accesso al volume.	array di interi	Nessuno	Sì
volumeAccessGroupID	VolumeAccessGroupID del gruppo di accesso al volume a cui vengono aggiunti i volumi.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	volumeAccessGroup

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "AddVolumesToVolumeAccessGroup",
  "params": {
    "volumeAccessGroupID": 96,
    "volumes": [1,2]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
      ]
    }
  }
}
```

Nuovo dalla versione

9,6

Crea gruppo di accesso al volume

Puoi usare `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 immettere iniziatori e volumi.

Qualsiasi IQN iniziatore aggiunto al gruppo di accesso al volume è in grado di accedere a qualsiasi volume nel 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 al volume, tenere presente quanto segue:

- Un gruppo di accesso al volume può contenere fino a 64 IQN iniziatori.
- Un iniziatore può appartenere solo a un gruppo di accesso al volume.

- Un gruppo di accesso al volume può contenere fino a 2000 volumi.
- Ogni 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	Necessario
iniziatori	Elenco di ID o 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 iniziatori, il metodo restituisce un errore se uno qualsiasi degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è deprecato; è consigliabile utilizzare gli ID degli iniziatori ogniqualvolta possibile.	array di interi o array di stringhe (obsoleto)		NO
nome	Nome del gruppo di accesso al volume. Non è obbligatorio che sia unico, ma è consigliato. Deve essere lungo da 1 a 64 caratteri.	corda	Nessuno	Sì
volumi	Elenco di volumiID da includere nel gruppo di accesso al volume.	array di interi		NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	{}	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena creato.	volumeAccessGroup
volumeAccessGroupID	ID del gruppo di accesso al volume appena creato.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "id": null,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [],
      "initiatorIDs": [
        95
      ],
      "initiators": [
        "iqn.1993-08.org.debian: 01: a31b1d799d5c"
      ],
      "name": "myaccessgroup",
      "volumeAccessGroupID": 96,
      "volumes": [
        327
      ]
    },
    "volumeAccessGroupID": 96
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [Ottieni risultato asincrono](#)
- [ListSyncJobs](#)
- [ModificaVolume](#)

DeleteVolumeAccessGroup

Puoi usare DeleteVolumeAccessGroup per eliminare un gruppo di accesso al volume.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroupID	ID del gruppo di accesso al volume da eliminare.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
deleteOrphanInitiators	Specifica se eliminare o meno gli oggetti iniziatori. Valori possibili: • true: elimina gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. • false: non eliminare gli oggetti iniziatori 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 ID o tag di rete virtuale. Valori possibili: • vero: il gruppo di accesso al volume verrà eliminato. • falso: predefinito. Non eliminare il gruppo di accesso al volume se ha un ID o un tag di rete virtuale.	booleano	falso	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteVolumeAccessGroup",
  "params": {
    "force": true,
    "volumeAccessGroupID" : 3
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id" : 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

ListVolumeAccessGroups

Puoi usare il `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	Necessario
limite	Numero massimo di oggetti volumeAccessGroup da restituire. Mutuamente esclusivi con il parametro volumeAccessGroups.	intero	Illimitato	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
startVolumeAccessGroupID	ID del gruppo di accesso al volume da cui iniziare l'elenco. Mutuamente esclusivi con il parametro volumeAccessGroups.	intero	0	NO
volumeAccessGroups	Elenco dei valori volumeAccessGroupID da recuperare. Mutuamente esclusivi con i parametri startVolumeAccessGroupID e limit.	array di interi		NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroups	Un elenco di oggetti che descrivono ciascun gruppo di accesso al volume.	volumeAccessGroup vettore
volumeAccessGroupsNotFound	Elenco dei gruppi di accesso al volume non trovati dal sistema. Presente se è stato utilizzato il parametro volumeAccessGroups e il sistema non è riuscito a trovare uno o più gruppi di accesso al volume specificati.	array di interi

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:


```
{
  "method": "ListVolumeAccessGroups",
  "params": {
    "startVolumeAccessGroupID": 3,
    "limit"      : 1
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "volumeAccessGroups": [
      {
        "attributes": {},
        "deletedVolumes": [],
        "initiatorIDs": [],
        "initiators": [],
        "name": "example1",
        "volumeAccessGroupID": 3,
        "volumes": []
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

RimuoviVolumiDaVolumeAccessGroup

Puoi usare il `RemoveVolumesFromVolumeAccessGroup` metodo per rimuovere volumi da un gruppo di accesso al volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroupID	VolumeAccessGroupID da cui rimuovere i volumi.	intero	Nessuno	Sì
volumi	VolumeID dei volumi da rimuovere dal gruppo di accesso al volume.	array di interi	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	volumeAccessGroup

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RemoveVolumesFromVolumeAccessGroup",
  "params": {
    "volumeAccessGroupID": 96,
    "volumes": [1,2]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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": []
    }
  }
}

```

Nuovo dalla versione

9,6

RemoveInitiatorsFromVolumeAccessGroup

Puoi usare il `RemoveInitiatorsFromVolumeAccessGroup` metodo per rimuovere gli iniziatori da un gruppo di accesso al volume specificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroupID	ID del gruppo di accesso al volume da cui vengono rimossi gli iniziatori.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
iniziatori	Elenco di ID o 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 iniziatori, il metodo restituisce un errore se uno qualsiasi degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è deprecato; è consigliabile utilizzare gli ID degli iniziatori ogniqualvolta possibile.	array di interi (consigliato) o array di stringhe (obsoleto)	Nessuno	NO
deleteOrphanInitiators	Specifica se eliminare o meno gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. Valori possibili: • true: elimina gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. • false: non eliminare gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. Questa è l'impostazione predefinita.	booleano	falso	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	volumeAccessGroup

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 13171,
  "method": "RemoveInitiatorsFromVolumeAccessGroup",
  "params": {
    "initiators": [114,115],
    "volumeAccessGroupID": 96
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 13171,
  "result": {
    "volumeAccessGroup": {
      "attributes": {},
      "deletedVolumes": [
        327
      ],
      "initiatorIDs": [],
      "initiators": [],
      "name": "test",
      "volumeAccessGroupID": 96,
      "volumes": [
        346
      ]
    }
  }
}
```

Nuovo dalla versione

9,6

ModificaVolumeAccessGroup

Puoi usare il `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 i volumi o gli iniziatori, l'elenco corrente di iniziatori e volumi non verrà modificato.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroup ID	ID del gruppo di accesso al volume da modificare.	intero	Nessuno	Sì
nome	Il nuovo nome per questo gruppo di accesso al volume.	corda	Nessuno	NO
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO

iniziatori	Elenco di ID o 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 iniziatori, il metodo restituisce un errore se uno qualsiasi degli iniziatori non esiste già. Il passaggio dei nomi degli iniziatori è deprecato; è consigliabile utilizzare gli ID degli iniziatori ogniqualvolta possibile.	array di interi (consigliato) o array di stringhe (obsoleto)	Nessuno	NO
deleteOrphanInitiators	Specifica se eliminare o meno gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. Valori possibili: • true: elimina gli oggetti iniziatori dopo che sono stati rimossi da un gruppo di accesso al volume. • false: non eliminare gli oggetti iniziatori 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 volume da modificare.	array di interi	Nessuno	volumeAccessGroup

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
volumeAccessGroup	Un oggetto contenente informazioni sul gruppo di accesso al volume appena modificato.	volumeAccessGroup

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifyVolumeAccessGroup",
  "params": {
    "volumeAccessGroupID": 96,
    "name": "accessgrouptest",
    "initiators": [115,114],
    "volumes": [
      346
    ],
    "attributes": {}
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```
{
  "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
      ]
    }
  }
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

- [AggiungiIniziatoriAlGruppoAccessoVolume](#)
- [AggiungiVolumiAlGruppoAccessoVolumi](#)
- [RemoveInitiatorsFromVolumeAccessGroup](#)
- [RimuoviVolumiDaVolumeAccessGroup](#)

GetVolumeAccessGroupEfficiency

Puoi usare il `GetVolumeAccessGroupEfficiency` metodo per ottenere informazioni sull'efficienza di un gruppo di accesso al volume. Per calcolare la capacità viene utilizzato solo il gruppo di accesso al volume fornito come parametro in questo metodo API.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
volumeAccessGroup ID	Specifica il gruppo di accesso al volume per il quale viene calcolata la capacità.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
compressione	Quantità di spazio risparmiata dalla compressione dei dati per tutti i volumi nel gruppo di accesso al volume. Espresso come rapporto in cui il valore 1 indica che i dati sono stati archiviati senza compressione.	galleggiante
deduplicazione	Quantità di spazio risparmiata evitando di duplicare i dati per tutti i volumi nel gruppo di accesso al volume. Espresso come rapporto.	galleggiante
thinProvisioning	Rapporto tra lo spazio utilizzato e la quantità di spazio allocato per l'archiviazione dei dati. Espresso come rapporto.	galleggiante
marca temporale	L'ultima volta che i dati sull'efficienza sono stati raccolti dopo la garbage collection.	Stringa di dati ISO 8601
volumi mancanti	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 temporanea perdita di rete o dal riavvio dei servizi dopo il ciclo di garbage collection.	array di interi

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVolumeAccessGroupEfficiency",
  "params": {
    "volumeAccessGroupID": 1
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "compression": 2.006012925331075,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1.009861932938856,
    "timestamp": "2014-03-10T17:05:27Z"
  }
}
```

Nuovo dalla versione

9,6

Metodi API per snapshot del volume

Panoramica delle istantanee

Uno snapshot del volume è una copia di un volume effettuata in un dato momento. È possibile utilizzare gli snapshot per riportare un volume allo stato in cui si trovava al momento della creazione dello snapshot.

È possibile raggruppare gli snapshot dei volumi in modo che i volumi correlati possano essere sottoposti a backup o rollback in modo coerente. Uno snapshot di gruppo cattura un'immagine in un dato momento di tutti i file di suddivisione del volume. È quindi possibile utilizzare l'immagine per riportare un gruppo di volumi a uno stato temporale specifico e garantire che tutti i dati siano coerenti in tutti i volumi del gruppo.

È possibile pianificare l'esecuzione autonoma degli snapshot del volume a intervalli definiti. È possibile definire gli intervalli in base all'ora, ai giorni della settimana o ai giorni del mese. È anche possibile utilizzare snapshot pianificati per garantire che gli snapshot vengano sottoposti a backup su un archivio remoto a scopo di archiviazione.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Documentazione per le versioni precedenti dei prodotti NetApp SolidFire ed Element"](#)

Crea istantanea di gruppo

Puoi usare `CreateGroupSnapshot` per creare una copia puntuale di un gruppo di volumi.

È possibile utilizzare questo snapshot in un secondo momento come backup o rollback per garantire che i dati sul gruppo di volumi siano coerenti per il momento in cui è stato creato lo snapshot.

PIENEZZA_CLUSTER



È possibile creare snapshot se il cluster è al livello 1, 2 o 3. Non è possibile creare snapshot quando il cluster è pieno al livello 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>attributes</code>	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
<code>enableRemoteReplication</code>	Specifica se lo snapshot verrà replicato o meno su un archivio remoto. Valori possibili: • <code>true</code>: Lo snapshot verrà replicato nell'archivio remoto. • <code>false</code>: Lo snapshot non verrà replicato nell'archivio remoto.	booleano	falso	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ensureSerialCreation	Specifica che lo snapshot non deve essere creato se è in corso una precedente replica dello snapshot. I valori possibili sono: • <code>true</code>: Ciò garantisce che venga replicato solo uno snapshot alla volta. La creazione di un nuovo snapshot non riuscirà se è ancora in corso una replica di uno snapshot precedente. • <code>false</code>: Predefinito. La creazione di questo snapshot è consentita se è ancora in corso un'altra replica dello snapshot.	booleano	false	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
expirationTime	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con retention. Se nessuno dei due expirationTime, O retention sono specificati, lo snapshot non scadrà. Il formato dell'ora è una stringa di data ISO 8601 per la scadenza basata sul tempo, altrimenti non scadrà. Un valore di null fa sì che l'istantanea venga conservata in modo permanente. Un valore di fifo fa sì che lo snapshot venga conservato secondo il principio First-In-First-Out (FIFO), rispetto agli altri snapshot FIFO presenti nel volume. L'API non funzionerà se non è disponibile spazio FIFO.	Stringa di data ISO 8601	Nessuno	NO
name	Il nome dello snapshot del gruppo. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stato acquisito lo snapshot del gruppo. La lunghezza massima consentita per il nome è di 255 caratteri.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
retention	Questo parametro è lo stesso del expirationTime parametro, eccetto che il formato dell'ora è HH:mm:ss. Se nessuno dei due expirationTime né retention sono specificati, lo snapshot non scadrà.	corda	Nessuno	NO
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror .	corda	Nessuno	NO
volumes	ID univoco dell'immagine del volume da cui copiare.	matrice volumeID	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

membri	Elenco di checksum, volumeID e snapshotID per ciascun membro del gruppo. Valori validi: - checksum: una piccola rappresentazione in forma di stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in seguito per confrontare altri snapshot e rilevare errori nei dati. (corda) - snapshotID: ID univoco di uno snapshot da cui viene creato il nuovo snapshot. Lo snapshotID deve provenire da uno snapshot sul volume specificato. (numero intero) - volumeID: ID del volume di origine per lo snapshot. (numero intero)	Matrice di oggetti JSON
ID istantanea gruppo	ID univoco del nuovo snapshot del gruppo.	ID groupSnapshot
groupSnapshot	Oggetto contenente informazioni sullo snapshot del gruppo appena creato.	groupSnapshot

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateGroupSnapshot",
  "params": {
    "volumes": [1,2]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  }
]
}
}

```

Nuovo dalla versione

9,6

Crea programma

Puoi usare `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 su un volume o un 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 intervallo di tempo non divisibile per 5 minuti, lo snapshot verrà eseguito nel successivo intervallo di tempo divisibile per 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 il cluster è al livello 1, 2 o 3. Non è possibile creare snapshot quando il cluster è pieno al livello 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
attributes	Utilizzare la stringa “frequency” per indicare la frequenza dello snapshot. Valori possibili: • Days of Week • Days of Month • Time Interval	Oggetto JSON	Nessuno	NO
hasError	Aiuto necessario con la descrizione	booleano	false	NO
hours	Numero di ore tra snapshot ricorrenti o ora in ora GMT in cui verrà eseguito lo snapshot in modalità Giorni della settimana o Giorni del mese. I valori validi sono compresi tra 0 e 23.	intero	Nessuno	NO
lastRunStatus	Il risultato o lo stato dell’ultima creazione pianificata dello snapshot.	corda	Nessuno	NO
name	Il nome dell’istantanea. Se non viene immesso alcun nome, vengono utilizzate la data e l’ora in cui è stato acquisito lo snapshot del gruppo. La lunghezza massima consentita per il nome è di 244 caratteri.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
minutes	Numero di minuti tra snapshot ricorrenti o minuto in ora GMT in cui verrà eseguito lo snapshot in modalità Giorni della settimana o Giorni del mese. I valori validi sono compresi tra 5 e 59.	intero	Nessuno	NO
paused	Indica se la pianificazione deve essere sospesa 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 la prossima volta che lo scheduler è attivo. Se impostato su true, lo snapshot pianificato viene eseguito la volta successiva che lo scheduler è attivo e viene reimpostato su false. I valori validi sono: • true • false	booleano	false	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
scheduleName	Nome univoco per la pianificazione. La lunghezza massima consentita per il nome della pianificazione è di 244 caratteri.	corda	Nessuno	Sì
scheduleType	Indica il tipo di pianificazione da creare. Il valore valido è snapshot.	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
scheduleInfo	Il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume da cui è stato creato lo snapshot. Valori validi: • volumeID: ID del volume da includere nello snapshot. (numero intero) • volumes: Elenco degli ID volume da includere nello snapshot del gruppo. (array di interi) • name: Nome dello snapshot da utilizzare. (corda) • enableRemoteReplication: Indica se lo snapshot deve essere incluso nella replica remota. (booleano) • retention: La quantità di tempo per cui lo snapshot verrà conservato in HH:mm:ss. Se vuoto, lo snapshot viene conservato per sempre. (corda) • fifo: Lo snapshot viene conservato secondo il principio First-In-First-Out (FIFO). (corda)	Oggetto JSON	Nessuno	Sì
1068	ensureSerial			

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror.	corda	Nessuno	NO
startingDate	Ora dopo la quale verrà eseguita la programmazione. Se non impostato, la pianificazione inizia immediatamente. Formattato in base all'ora UTC.	Stringa di data ISO 8601	Nessuno	NO
toBeDeleted	Specifica che questa pianificazione degli snapshot deve essere eliminata al termine della creazione dello snapshot.	booleano	false	NO
monthdays	I giorni del mese in cui verrà scattata una foto. I valori validi sono compresi tra 1 e 31.	array di interi	Nessuno	Sì (se si pianifica per giorni del mese)

Nome	Descrizione	Tipo	Valore predefinito	Necessario
weekdays	Giorno della settimana in cui verrà creato lo snapshot. Valori richiesti (se utilizzati): • Day: dalle 0 alle 6 (da domenica a sabato) • Offset: per ogni possibile settimana del mese, da 1 a 6 (se maggiore di 1, la corrispondenza avviene solo nell'N-esimo giorno 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 intrapresa alcuna azione. Offset:1 (predefinito) significa che lo snapshot viene creato per questo giorno della settimana, indipendentemente da dove cade nel mese)	Matrice di oggetti JSON	Nessuno	Sì (se si pianifica per giorni della settimana)

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
IDprogramma	ID della pianificazione creata.	intero
programma	Un oggetto contenente informazioni sulla pianificazione appena creata.	programma

Esempio di richiesta 1

La seguente pianificazione di esempio ha i seguenti parametri:

- Non sono specificati orari o minuti di inizio, in modo che la programmazione inizi il più vicino possibile alla mezzanotte (00:00:00Z).
- Non è ricorrente (verrà eseguito solo una volta).
- Si svolge una volta la prima domenica o il primo mercoledì successivo al 1° giugno 2015, UTC 19:17:15Z (a seconda di quale giorno si verifica per primo).
- Include un solo volume (volumeID = 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 di cui sopra restituisce una risposta simile al seguente esempio:

```

{
  "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
  }
}

```

Esempio di richiesta 2

La seguente pianificazione di esempio ha i seguenti parametri:

- È ricorrente (verrà eseguito a ogni intervallo programmato del mese all'ora specificata).

- Si svolge il 1°, il 10, il 15 e il 30 di ogni mese successivo alla data di inizio.
- Si svolge alle 12:15 di ogni giorno in cui è previsto.
- Include un solo volume (volumeID = 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 di cui sopra restituisce una risposta simile al seguente esempio:

```

{
  "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
  }
}

```

Richiesta esempio 3

La seguente pianificazione di esempio ha i seguenti parametri:

- Inizierà entro 5 minuti dall'intervallo programmato del 2 aprile 2015.
- È ricorrente (verrà eseguito a ogni intervallo programmato del mese all'ora specificata).
- Si svolge il secondo, il terzo e il quarto giorno di ogni mese successivo alla data di inizio.
- La corsa si svolge alle 14:45 di ogni giorno in cui è prevista.
- Comprende 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 di cui sopra restituisce una risposta simile al seguente esempio:

```

{
  "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
  }
}

```

Nuovo dalla versione

9,6

Crea istantanea

Puoi usare `CreateSnapshot` per creare una copia di un volume in un dato momento. È possibile creare uno snapshot da qualsiasi volume o da uno snapshot esistente.

Se non si fornisce uno SnapshotID con questo metodo API, viene creato uno snapshot dal ramo attivo del volume. Se il volume da cui viene creato lo snapshot viene replicato su un cluster remoto, lo snapshot può essere replicato anche sulla stessa destinazione. Utilizzare il parametro enableRemoteReplication per abilitare la replica degli snapshot.



È possibile creare snapshot se il cluster è al livello 1, 2 o 3. Non è possibile creare snapshot quando il cluster è pieno al livello 4 o 5.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
attributes	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
enableRemoteReplication	Specifica se lo snapshot verrà replicato o meno su un archivio remoto. Valori possibili: • true: Lo snapshot verrà replicato nell'archivio remoto. • false: Lo snapshot non verrà replicato nell'archivio remoto.	booleano	falso	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ensureSerialCreation	Specifica che lo snapshot non deve essere creato se è in corso una precedente replica dello snapshot. I valori possibili sono: • <code>true</code>: Ciò garantisce che venga replicato solo uno snapshot alla volta. La creazione di un nuovo snapshot non riuscirà se è ancora in corso una replica di uno snapshot precedente. • <code>false</code>: Predefinito. La creazione di questo snapshot è consentita se è ancora in corso un'altra replica dello snapshot.	booleano	false	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
tempo di scadenza	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con <code>retention</code>. Se non vengono specificati né <code>expirationTime</code> né <code>retention</code>, lo snapshot non scadrà. Il formato dell'ora è una stringa di data ISO 8601 per la scadenza basata sul tempo, altrimenti non scadrà. Un valore di <code>null</code> fa sì che l'istantanea venga conservata in modo permanente. Un valore di <code>fifo</code> fa sì che lo snapshot venga conservato secondo il principio First-In-First-Out, rispetto agli altri snapshot FIFO presenti nel volume. L'API non funzionerà se non è disponibile spazio FIFO.	corda	Nessuno	NO
name	Il nome dell'istantanea. Se non viene inserito alcun nome, vengono utilizzate la data e l'ora in cui è stato acquisito lo snapshot. La lunghezza massima consentita per il nome è di 255 caratteri.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
retention	Questo parametro è lo stesso del expirationTime parametro, eccetto che il formato dell'ora è HH:mm:ss. Se nessuno dei due expirationTime né retention sono specificati, lo snapshot non scadrà.	corda	Nessuno	NO
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror .	corda	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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
somma di controllo	Una stringa che rappresenta le cifre corrette nello snapshot memorizzato. Questo checksum può essere utilizzato in seguito per confrontare altri snapshot e rilevare errori nei dati.	corda

ID istantanea	ID univoco del nuovo snapshot.	ID istantanea
istantanea	Un oggetto contenente informazioni sullo snapshot appena creato.	istantanea

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateSnapshot",
  "params": {
    "volumeID": 1
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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` Viene chiamata l'API e lo snapshot non viene creato. Questo è un comportamento previsto. Riprova il `CreateSnapshot` Chiamata API.

Nuovo dalla versione

9,6

EliminaSnapshot di Gruppo

Puoi usare `DeleteGroupSnapshot` per eliminare uno snapshot di gruppo.

È possibile utilizzare il parametro `saveMembers` per conservare tutti gli snapshot creati per i volumi nel gruppo, ma l'associazione al gruppo verrà rimossa.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID istantanea gruppo	ID univoco dello snapshot del gruppo.	intero	Nessuno	Sì
salvaMembri	Specifica cosa eliminare quando si elimina uno snapshot di gruppo. Valori validi: • vero: gli snapshot vengono conservati, ma l'associazione al gruppo viene rimossa. • false: il gruppo e gli snapshot vengono eliminati.	booleano	falso	NO

Valore di ritorno

Questo metodo non ha valore di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteGroupSnapshot",
  "params": {
    "groupSnapshotID": 10,
    "saveMembers" : true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

EliminaSnapshot

Puoi usare il `DeleteSnapshot` metodo per eliminare uno snapshot.

Non è possibile eliminare uno snapshot che è attualmente lo snapshot 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	Necessario
ID istantanea	ID dello snapshot da eliminare.	intero	Nessuno	Sì
overrideSnapMirror Hold	Sostituisce il blocco applicato agli snapshot durante la replica. È possibile utilizzare questo parametro per eliminare gli snapshot SnapMirror obsoleti dopo che la relazione SnapMirror associata è stata eliminata.	booleano	falso	NO

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteSnapshot",
  "params": {
    "snapshotID": 8,
    "overrideSnapMirrorHold": true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Trova maggiori informazioni

[RollbackToSnapshot](#)

Ottieni pianificazione

Puoi usare `GetSchedule` per ottenere informazioni su uno snapshot pianificato.

È possibile visualizzare informazioni su una pianificazione specifica se nel sistema sono presenti molte pianificazioni snapshot. Con questo metodo è possibile recuperare informazioni anche su più di una pianificazione specificando ID aggiuntivi nel parametro `scheduleID`.

Parametro

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
IDprogramma	ID univoco della pianificazione o delle più pianificazioni da visualizzare.	intero	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
programma	Una serie di attributi di pianificazione.	programmavettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetSchedule",
  "params": {
    "scheduleID" : 2
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": []
    }
  }
}
```

Nuovo dalla versione

9,6

ListGroupSnapshots

Puoi usare `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	Necessario
ID istantanea gruppo	Recupera informazioni per un ID snapshot di gruppo individuale.	intero	Nessuno	NO
volumi	Un array di ID volume univoci da interrogare. Se non si specifica questo parametro, verranno inclusi tutti gli snapshot di gruppo sul cluster.	matrice volumeID	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
istantanee di gruppo	Un elenco di oggetti contenente informazioni su ogni snapshot di gruppo.	groupSnapshot vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListGroupSnapshots",
  "params": {
    "volumes": [
      31,
      49
    ]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
}
]

```

```
}
```

Nuovo dalla versione

9,6

ListSchedules

Puoi usare `ListSchedules` per ottenere informazioni su tutti gli snapshot pianificati che sono stati creati.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
orari	Un elenco delle pianificazioni attualmente presenti nel cluster.	programmavettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListSchedules",
  "params": {},
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": []  
    }  
]  
}  
}
```

Nuovo dalla versione

9,6

ListSnapshots

Puoi usare `ListSnapshots` per restituire gli attributi di ogni snapshot acquisito 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	Necessario
ID volume	Recupera gli snapshot per un volume. Se volumeID non viene fornito, vengono restituiti tutti gli snapshot per tutti i volumi.	intero	Nessuno	NO
ID istantanea	Recupera informazioni per un singolo ID snapshot.	intero	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
istantanee	Informazioni su ogni snapshot per ogni volume. Se volumeID non viene fornito, vengono restituiti tutti gli snapshot per tutti i volumi. Gli snapshot che si trovano in un gruppo vengono restituiti con un ID gruppo.	istantanee vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListSnapshots",
  "params": {
    "volumeID": "1"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ModificaSnapshotGruppo

Puoi usare `ModifyGroupSnapshot` per modificare gli attributi di un gruppo di snapshot. È possibile utilizzare questo metodo anche per consentire la replica remota degli snapshot creati sul volume di lettura/scrittura (di origine) su un sistema di archiviazione di destinazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario

enableReplication	Utilizzare per abilitare la replica dello snapshot creato su un cluster remoto. Valori possibili: • <code>true</code>: Lo snapshot verrà replicato nell'archivio remoto. • <code>false</code>: Lo snapshot non verrà replicato nell'archivio remoto.	booleano	falso	NO
tempo di scadenza	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con ritenzione. Se non vengono specificati né <code>expirationTime</code> né <code>retention</code> sullo snapshot originale, lo snapshot non scadrà. Il formato dell'ora è una stringa di data ISO 8601 per la scadenza basata sul tempo, altrimenti non scadrà. Un valore di <code>null</code> fa sì che l'istantanea venga conservata in modo permanente. Un valore <code>fifo</code> fa sì che lo snapshot venga conservato secondo il principio First-In-First-Out (FIFO), rispetto agli altri snapshot FIFO presenti nel volume. L'API non funzionerà se non è disponibile spazio FIFO.	Stringa di data ISO 8601	Nessuno	NO

nome	Il nome dello snapshot del gruppo. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stato acquisito lo snapshot del gruppo. La lunghezza massima consentita per il nome è di 255 caratteri.	corda	Nessuno	NO
ID istantanea gruppo	L'ID del gruppo di snapshot.	corda	Nessuno	Sì
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
groupSnapshot	Oggetto contenente informazioni sullo snapshot del gruppo appena modificato.	groupSnapshot

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 695,
  "method": "ModifyGroupSnapshot",
  "params": {
    "groupSnapshotID": 3,
    "enableRemoteReplication": true,
    "expirationTime": "2016-04-08T22:46:25Z"
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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"
    }
  }
}

```

Nuovo dalla versione

9,6

Modifica pianificazione

Puoi usare `ModifySchedule` per modificare gli intervalli in cui si verifica uno snapshot pianificato. Utilizzando questo metodo è anche possibile eliminare o mettere in pausa una pianificazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
attributi	Utilizzare per modificare la frequenza di occorrenza dello snapshot. Valori possibili: • Days of Week • Days of Month • Time Interval	Oggetto JSON	Nessuno	NO
ore	Numero di ore tra gli snapshot oppure ora in cui verrà eseguito lo snapshot in modalità Giorni della settimana o Giorni del mese. I valori validi sono compresi tra 0 e 24.	corda	Nessuno	NO
nome	Il nome dell'istantanea. Se non viene immesso alcun nome, vengono utilizzate la data e l'ora in cui è stato acquisito lo snapshot del gruppo. La lunghezza massima consentita per il nome è di 244 caratteri.	corda	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
minuti	Numero di minuti tra gli snapshot o minuto in cui verrà eseguito lo snapshot in modalità Giorni della settimana o Giorni del mese. I valori validi sono compresi tra 0 e 59.	intero	Nessuno	NO
ultimoStatoEsecuzione	Il risultato o lo stato dell'ultima creazione pianificata dello snapshot.	corda	Nessuno	NO
in pausa	Indica se la pianificazione deve essere sospesa 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

Nome	Descrizione	Tipo	Valore predefinito	Necessario
runNextInterval	Utilizzare per scegliere se eseguire o meno lo snapshot la prossima volta che lo scheduler è attivo. Valori validi: • true • false Se impostato su true, lo snapshot pianificato viene eseguito la volta successiva che lo scheduler è attivo, per poi tornare a false.	booleano	falso	NO
IDprogramma	ID univoco della pianificazione.	intero	Nessuno	Sì
Nome programma	Nome univoco per la pianificazione. La lunghezza massima consentita per il nome della pianificazione è di 244 caratteri.	corda	Nessuno	NO
tipo di programma	Indica il tipo di pianificazione da creare. L'unico valore supportato è snapshot .	corda	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
scheduleInfo	Il nome univoco assegnato alla pianificazione, il periodo di conservazione per lo snapshot creato e l'ID del volume da cui è stato creato lo snapshot. Valori validi: • enableRemote Replication: Indica se lo snapshot deve essere incluso nella replica remota. (booleano) • ensureSerial Creation: specifica se è consentita la creazione di un nuovo snapshot se è in corso una replica di snapshot precedente. (booleano) • name: Nome dello snapshot da utilizzare. (corda) • retention: La quantità di tempo per cui viene conservato lo snapshot. A seconda dell'ora, viene visualizzato in uno dei seguenti formati: ◦ fifo: Lo snapshot viene conservato secondo il principio FIFO (First-In-First-Out). Se vuoto, lo	"programma"	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror.	corda	Nessuno	NO
da eliminare	Indica se la pianificazione è contrassegnata per l'eliminazione. Valori validi: • <code>true</code> • <code>false</code>	booleano	Nessuno	NO
data di inizio	Indica la data in cui è iniziata o inizierà la prima volta la programmazione.	Stringa di data ISO 8601	Nessuno	NO
giorni del mese	I giorni del mese in cui verrà scattata una foto. I valori validi sono compresi tra 1 e 31.	array di interi	Nessuno	Sì
giorni feriali	Giorno della settimana in cui verrà creato lo snapshot. Il giorno della settimana inizia con domenica con il valore 0 e uno scostamento di 1.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
programma	Un oggetto contenente gli attributi della pianificazione modificata.	programma

Richiedi esempio

```
{
  "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
        }
      ]
    }
  }
}

```

Nuovo dalla versione

9,6

ModificaSnapshot

Puoi usare `ModifySnapshot` per modificare gli attributi attualmente assegnati a uno snapshot. È possibile utilizzare questo metodo anche per consentire la replica remota degli snapshot creati sul volume di lettura/scrittura (di origine) su un cluster di archiviazione di destinazione che esegue il software Element.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
enableReplication	Utilizzare per abilitare la replica dello snapshot creato su un cluster di archiviazione remoto. Valori possibili: • <code>true</code>: Lo snapshot verrà replicato nell'archivio remoto. • <code>false</code>: Lo snapshot non verrà replicato nell'archivio remoto.	booleano	falso	NO

tempo di scadenza	Specificare il tempo dopo il quale è possibile rimuovere lo snapshot. Non può essere utilizzato con ritenzione. Se non vengono specificati né expirationTime né retention sullo snapshot originale, lo snapshot non scadrà. Il formato dell'ora è una stringa di data ISO 8601 per la scadenza basata sul tempo, altrimenti non scadrà. Un valore null fa sì che lo snapshot venga conservato in modo permanente. Un valore fifo fa sì che lo snapshot venga conservato secondo il principio First-In-First-Out (FIFO), rispetto agli altri snapshot FIFO presenti nel volume. L'API non funzionerà se non è disponibile spazio FIFO.	Stringa di data ISO 8601	Nessuno	NO
nome	Il nome dell'istantanea. Se non viene inserito alcun nome, vengono utilizzate la data e l'ora in cui è stato acquisito lo snapshot. La lunghezza massima consentita per il nome è di 255 caratteri.	corda	Nessuno	NO

snapMirrorLabel	Etichetta utilizzata dal software SnapMirror per specificare la politica di conservazione degli snapshot su un endpoint SnapMirror .	corda	Nessuno	NO
ID istantanea	Identificatore dello snapshot.	corda	Nessuno	Sì

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
istantanea	Un oggetto contenente informazioni sullo snapshot appena modificato.	istantanea

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ModifySnapshot",
  "params": {
    "snapshotID": 3114,
    "enableRemoteReplication": "true",
    "name" : "Chicago"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
    }
  }
}
```

Nuovo dalla versione

9,6

RollbackToGroupSnapshot

Puoi usare `RollbackToGroupSnapshot` per ripristinare tutti i singoli volumi in un gruppo di snapshot allo snapshot individuale di ciascun 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 il cluster è pieno nella fase 1, 2 o 3. Gli snapshot non vengono creati quando il livello di riempimento del cluster è pari a 4 o 5.
- Il rollback dei volumi in uno snapshot di gruppo potrebbe non riuscire quando è in corso la sincronizzazione delle sezioni. Riprova `RollbackToGroupSnapshot` al termine della sincronizzazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
groupSnapshotID	ID univoco dello snapshot del gruppo.	intero	Nessuno	Sì
attributes	Elenco di coppie nome-valore nel formato oggetto JSON.	Oggetto JSON	Nessuno	NO
name	Nome per lo snapshot di gruppo dello stato corrente del volume che viene creato se <code>saveCurrentState</code> è impostato su vero. Se non si specifica un nome, il nome degli snapshot (gruppo e volume individuale) verrà impostato su un timestamp dell'ora in cui si è verificato il rollback.	corda	Nessuno	NO
saveCurrentState	Specifica se salvare o meno l'immagine del volume attivo precedente. Valori validi: • <code>true</code>: Viene mantenuta l'immagine del volume attivo precedente. • <code>false</code>: L'immagine del volume attivo precedente viene eliminata.	booleano	falso	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo

membri	Un array contenente i volumiID e gli snapshotID dei membri dello snapshot di gruppo. Valori: • checksum: una piccola rappresentazione in forma di stringa dei dati nello snapshot memorizzato. Questo checksum può essere utilizzato in seguito per confrontare altri snapshot e rilevare errori nei dati. (corda) • snapshotID: ID univoco di uno snapshot da cui viene creato il nuovo snapshot. Lo snapshotID deve essere uno snapshot sul volume specificato. (numero intero) • volumeID: ID del volume di origine per lo snapshot. (numero intero)	Matrice di oggetti JSON
ID istantanea gruppo	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 del gruppo che RollbackToGroupSnapshot appena tornato a.	groupSnapshot

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 438,
  "method": "RollbackToGroupSnapshot",
  "params": {
    "groupSnapshotID": 1,
    "name": "grpsnap1",
    "saveCurrentState": true
  }
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

RollbackToSnapshot

Puoi usare il `RollbackToSnapshot` metodo per creare uno snapshot esistente dell'immagine del volume attivo. Questo metodo crea un nuovo snapshot da uno snapshot esistente.

Il nuovo snapshot diventa attivo e quello esistente viene conservato finché non viene eliminato manualmente. Lo snapshot precedentemente attivo viene eliminato a meno che non si imposti il parametro `saveCurrentState` su `true`.

PIENEZZA_CLUSTER



- È possibile creare snapshot se il cluster è al livello 1, 2 o 3. Non è possibile creare snapshot quando il cluster è pieno al livello 4 o 5.
- Il rollback di un volume a uno snapshot potrebbe non riuscire quando è in corso la sincronizzazione delle sezioni. Riprova `RollbackToSnapshot` al termine della sincronizzazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
ID volume	VolumeID per il volume.	intero	Nessuno	Sì
attributi	Elenco di coppie nome-valore nel formato oggetto JSON.	Attributi JSON	Nessuno	NO
nome	Nome per l'istantanea. Se non viene specificato alcun nome, viene utilizzato il nome dello snapshot di cui si sta eseguendo il rollback, aggiungendo "-copy" alla fine del nome.	corda	Nessuno	NO
ID istantanea	ID di uno snapshot creato in precedenza sul volume specificato.	intero	Nessuno	Sì

Nome	Descrizione	Tipo	Valore predefinito	Necessario
salvaStatoAttuale	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 di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
somma di controllo	Una piccola rappresentazione in forma di stringa dei dati nello snapshot memorizzato.	corda
ID istantanea	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
istantanea	Se saveCurrentState è stato impostato su false, questo valore è nullo. Se saveCurrentState è impostato su true, viene visualizzato un oggetto contenente informazioni sullo snapshot appena creato.	istantanea

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "RollbackToSnapshot",
  "params": {
    "volumeID": 1,
    "snapshotID": 3114,
    "saveCurrentState": true
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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
  }
}
```

Nuovo dalla versione

9,6

Metodi API del volume virtuale

Crea contenitore di archiviazione

Puoi usare il `CreateStorageContainer` metodo per creare un contenitore di archiviazione Virtual Volume (VVol). È possibile utilizzare contenitori di archiviazione per la creazione di report e l'allocazione delle risorse. Per utilizzare la funzionalità Volumi virtuali è necessario creare almeno un contenitore di archiviazione.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
nome	Nome del contenitore di stoccaggio. Segue le restrizioni sulla denominazione degli account del software Element.	corda	Nessuno	Sì
ID account	Account contenitore non di archiviazione che diventerà un contenitore di archiviazione.	intero	Nessuno	NO
iniziatoreSegreto	Il segreto per l'autenticazione CHAP per l'iniziatore.	corda	Nessuno	NO
targetSecret	Il segreto per l'autenticazione CHAP per la destinazione.	corda	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
contenitore di stoccaggio	Oggetto contenente informazioni sul contenitore di archiviazione appena creato.	contenitore di stoccaggio

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "CreateStorageContainer",
  "params": {
    "name" : "example"
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

9,6

Elimina contenitori di archiviazione

Puoi usare il `DeleteStorageContainers` Metodo per rimuovere contemporaneamente dal sistema fino a 2000 contenitori di archiviazione Virtual Volume (VVol). I contenitori di archiviazione rimossi non devono contenere VVol.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
storageContainerIDs	Un elenco di ID dei contenitori di archiviazione da eliminare. È possibile specificare fino a 2000 ID nell'elenco.	matrice UUID	Nessuno	Sì

Valori di ritorno

Questo metodo non ha valori di ritorno.

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "DeleteStorageContainers",
  "params": {
    "storageContainerIDs" : ["a9ec1138-e386-4a44-90d7-b9acbbc05176"]
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {}
}
```

Nuovo dalla versione

9,6

Ottieni efficienza del contenitore di archiviazione

Puoi usare il `GetStorageContainerEfficiency` metodo per recuperare informazioni sull'efficienza di un contenitore di archiviazione di volumi virtuali.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
storageContainerID	ID del contenitore di archiviazione per il quale recuperare informazioni sull'efficienza.	intero	Nessuno	Sì

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
compressione	Quantità di spazio risparmiata dalla compressione dei dati per tutti i volumi virtuali nel contenitore di archiviazione. Espresso come rapporto in cui il valore 1 indica che i dati sono stati memorizzati senza compressione.	galleggiante
deduplicazione	Quantità di spazio risparmiata evitando di duplicare i dati per tutti i volumi virtuali nel contenitore di archiviazione. Espresso come rapporto.	galleggiante
volumi mancanti	I volumi virtuali su cui non è stato possibile interrogare i dati di efficienza. I volumi mancanti possono essere causati dal fatto che il ciclo di Garbage Collection (GC) è stato eseguito meno di un'ora prima, da una perdita temporanea della connettività di rete o da servizi riavviati dopo il ciclo GC.	array di interi
thinProvisioning	Rapporto tra lo spazio utilizzato e la quantità di spazio allocato per l'archiviazione dei dati. Espresso come rapporto.	galleggiante
marca temporale	L'ultima volta che sono stati raccolti dati sull'efficienza dopo GC.	Stringa di dati ISO 8601

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetStorageContainerEfficiency",
  "params": {
    "storageContainerID" : "6c95e24f-9f0b-4793-affb-5a4bc6c3d7e1"
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "compression": 1,
    "deduplication": 1,
    "missingVolumes": [],
    "thinProvisioning": 1,
    "timestamp": "2016-04-12T15:39:49Z"
  }
}
```

Nuovo dalla versione

9,6

OttieniConteggioVolumeVirtuale

Puoi usare il `GetVirtualVolumeCount` metodo per recuperare il numero di volumi virtuali attualmente presenti nel sistema.

Parametri

Questo metodo non ha parametri di input.

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
contare	Numero di volumi virtuali attualmente presenti nel sistema.	intero

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "GetVirtualVolumeCount",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "id": 1,
  "result": {
    "count": 5
  }
}
```

Nuovo dalla versione

9,6

ListProtocolEndpoints

Puoi usare il `ListProtocolEndpoints` metodo per recuperare informazioni su tutti gli endpoint del protocollo nel cluster. Gli endpoint del protocollo regolano l'accesso ai contenitori di archiviazione dei volumi virtuali associati.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
protocolEndpointIDs	Un elenco di ID endpoint del protocollo per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti gli endpoint del protocollo.	array UUID protocolEndpointID	Nessuno	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
protocolEndpoints	Elenco di oggetti contenenti informazioni su ciascun endpoint del protocollo nel sistema.	protocolEndpoint vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "id": 1,
  "method": "ListProtocolEndpoints",
  "params": {}
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListStorageContainers

Puoi usare il `ListStorageContainers` Metodo per recuperare informazioni su tutti i contenitori di archiviazione di volumi virtuali noti al sistema.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>storageContainerIDs</code>	Un elenco di ID di contenitori di archiviazione per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti i contenitori di archiviazione nel sistema.	matrice UUID	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
contenitori di stoccaggio	Elenco di oggetti contenenti informazioni su tutti i contenitori di archiviazione nel sistema.	contenitore di stoccaggio vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListStorageContainers",
  "params": {
    "storageContainerIDs": ["efda8307-b916-4424-979e-658a3f16894d"]
  },
  "id" : 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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": []
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListVirtualVolumeBindings

Puoi usare il `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	Necessario
virtualVolumeBindingIDs	Un elenco di ID di associazione di volumi virtuali per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti i binding dei volumi virtuali.	array di interi	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
legature	Un elenco di oggetti che descrivono tutti i volumi virtuali nel cluster associati agli endpoint del protocollo.	legame

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVirtualVolumeBindings",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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"
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

ListVirtualVolumeHosts

Puoi usare il `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	Necessario
<code>virtualVolumeHostIDs</code>	Un elenco di ID host di volumi virtuali per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutti gli host del volume virtuale.	array UUID <code>virtualVolumeHostID</code>	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>ospiti</code>	Un elenco di oggetti che descrivono gli host dei volumi virtuali nel cluster.	ospite vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVirtualVolumeHosts",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```
{
  "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": "564dela4-9a99-da0f-8b7c-3a41dfd64bf1",
        "visibleProtocolEndpointIDs": [
          "5dd53da0-b9b7-43f9-9b7e-b41c2558e92b"
        ]
      }
    ]
  }
}
```

Nuovo dalla versione

9,6

ListVirtualVolumes

Puoi usare il `ListVirtualVolumes` metodo per elencare i volumi virtuali attualmente presenti nel sistema. È possibile utilizzare questo metodo per elencare tutti i volumi virtuali oppure solo un sottoinsieme.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
dettagli	Il livello di dettaglio nella risposta. Valori possibili: • vero: includi maggiori dettagli su ciascun VVol nella risposta. • false: includi il livello standard di dettaglio su ciascun VVol nella risposta.	booleano	Falso	NO
limite	Numero massimo di volumi virtuali da elencare.	intero	10000	NO
ricorsivo	Specifica se includere o meno nella risposta informazioni sui figli di ciascun VVol. Valori possibili: • vero: includi informazioni sui figli di ciascun VVol nella risposta. • false: non includere informazioni sui figli di ciascun VVol nella risposta.	booleano	Falso	NO
startVirtualVolumeID	ID del volume virtuale da cui iniziare l'elenco nella risposta.	Tipo UUID	Nessuno	NO

Nome	Descrizione	Tipo	Valore predefinito	Necessario
virtualVolumeIDs	Un elenco di ID di volumi virtuali per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni solo su questi volumi virtuali.	array UUID virtualVolumeID	Nessuno	NO

Valori di ritorno

Questo metodo ha i seguenti valori di ritorno:

Nome	Descrizione	Tipo
nextVirtualVolumeID	ID del volume virtuale successivo nell'elenco.	UUID
volumi virtuali	Un elenco di oggetti che descrivono i volumi virtuali attualmente presenti nel sistema.	volume virtuale vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVirtualVolumes",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:

```

{
  "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
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ListVirtualVolumeTasks

Puoi usare il `ListVirtualVolumeTasks` metodo per ottenere un elenco di attività del volume virtuale nel sistema.

Parametri

Questo metodo ha il seguente parametro di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario
<code>virtualVolumeTaskIDs</code>	Un elenco di ID attività di volume virtuale per i quali recuperare informazioni. Se si omette questo parametro, il metodo restituisce informazioni su tutte le attività del volume virtuale.	matrice UUID	Nessuno	NO

Valore di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
<code>compiti</code>	Un elenco di oggetti che descrivono le attività del volume virtuale nel cluster.	compito vettore

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "method": "ListVirtualVolumeTasks",
  "params": {
  },
  "id": 1
}
```

Esempio di risposta

Questo metodo restituisce una risposta simile al seguente esempio:


```

{
  "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"
      }
    ]
  }
}

```

Nuovo dalla versione

9,6

ModificaContentore di archiviazione

Puoi usare il `ModifyStorageContainer` metodo per apportare modifiche a un contenitore di archiviazione di volumi virtuali esistente.

Parametri

Questo metodo ha i seguenti parametri di input:

Nome	Descrizione	Tipo	Valore predefinito	Necessario

storageContainerID	ID univoco del contenitore di archiviazione del volume virtuale da modificare.	UUID	Nessuno	Sì
iniziatoreSegreto	Il nuovo segreto per l'autenticazione CHAP per l'iniziatore.	corda	Nessuno	NO
targetSecret	Il nuovo segreto per l'autenticazione CHAP per la destinazione.	corda	Nessuno	NO

Valori di ritorno

Questo metodo ha il seguente valore di ritorno:

Nome	Descrizione	Tipo
contenitore di stoccaggio	Informazioni sul contenitore di archiviazione appena creato.	contenitore di stoccaggio

Richiedi esempio

Le richieste per questo metodo sono simili al seguente esempio:

```
{
  "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 al seguente esempio:

```
{
  "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"
    }
  }
}
```

Nuovo dalla versione

9,6

Controllo degli accessi

I metodi API Element disponibili variano in base al tipo di accesso impostato.



Sono disponibili tipi di accesso tramite l'API che non sono disponibili nell'interfaccia utente di Element.

conti

Per il tipo di accesso agli account sono disponibili i seguenti metodi:

Aggiungi account
OttieniAccountPerID
Modifica Account
OttieniAccountPerNome
ElencoAccount
Ottieni efficienza dell'account
RimuoviAccount

amministratore

Tutti i metodi sono disponibili per il tipo di accesso amministratore.

ClusterAdmin

Per il tipo di accesso amministratore del cluster sono disponibili i seguenti metodi:

AggiungiClusterAdmin
ListBackupTargets
AggiungiIniziatoriAlGruppoAccessoVolume
ListBulkVolumeJobs
AggiungiLdapClusterAdmin
ListClusterAdmins
AggiungiVirtualNetwork
ListClusterPairs
AggiungiVirtualNetwork
ListNodeFibreChannelPortInfo
Aggiungi volume a gruppo di accesso al volume
ListBackupTargets
Clona più volumi
ListDriveHardware
CompleteClusterPairing
ListFibreChannelSessions
CompleteVolumePairing
ListFibreChannelPortInfo
Crea destinazione di backup

ListGroupSnapshots
Crea programma
ListActivePairedVolumes
Crea istantanea
Modifica destinazione backup
Crea pacchetto di supporto
ModificaClusterAdmin
Crea Cluster Support Bundle
ModificaSnapshotGruppo
Crea istantanea di gruppo
Modificasogliacompleta del cluster
Crea gruppo di accesso al volume
ModificaVolumeAccessGroup
Elimina tutti i pacchetti di supporto
ModifyVolumeAccessGroupLunAssignments
EliminaSnapshot
Modifica coppia di volumi
EliminaSnapshot di Gruppo
Modificare la rete virtuale
DeleteVolumeAccessGroup
RimuoviClusterAdmin
Disabilita la crittografia a riposo

RemoveVolumePair
Disabilita l'autenticazione LDAP
RimuoviVirtualNetwork
Disabilita Snmp
RimuoviVolumiDaVolumeAccessGroup
Abilita crittografia a riposo
RemoveInitiatorsFromVolumeAccessGroup
Abilita autenticazione LDAP
RollbackToSnapshot
AbilitaSnmp
RollbackToGroupSnapshot
Ottieni destinazione di backup
SetLoginSessionInfo
Ottieni soglia completa del cluster
ImpostaNtpInfo
OttieniClusterMasterNodeID
SetSnmpACL
OttieniConfigurazioneHardware
ImpostaSnmpInfo
OttieniLdapConfiguration
ImpostaSnmpTrapInfo
Ottieni informazioni sulla sessione di accesso

Imposta host di registrazione remoti
Ottieni informazioni Ntp
Fermare
Ottieni informazioni Nvram
StartBulkVolumeRead
Ottieni statistiche grezze
StartBulkVolumeWrite
OttieniSnmpACL
StartClusterPairing
GetVolumeAccessGroupEfficiency
StartVolumePairing
GetVolumeAccessLunAssignments
TestLdapAuthentication
OttieniVirtualNetwork

unità

Per il tipo di accesso alle unità sono disponibili i seguenti metodi:

ListDrives
Rimuovi unità
Aggiungi unità
SecureEraseDrives

nodì

Per il tipo di accesso ai nodi sono disponibili i seguenti metodi:

Aggiungi nodi
Elenco nodi in sospeso
ListActiveNodes
Rimuovi nodi

Leggere

Per il tipo di accesso in lettura sono disponibili i seguenti metodi:

OttieniAccountPerID
ListCloneJobs
OttieniAccountPerNome
ElencoVolumiEliminati
Ottieni risultato asincrono
ListDriveHardware
Ottieni capacità cluster
ListDrives
OttieniQoS predefinito
ElencoEventi
Ottieni statistiche di guida
ElencoISCSISessioni
Ottieni l'aggiornamento del software
Elenco nodi in sospeso
Ottieni statistiche sul volume
ListSyncJobs

ElencoAccount
ListVolumeAccessGroups
ListActiveNodes
ListVolumeStatsByAccount
ListActiveNodes
ListVolumeStatsByVolume
ListActiveVolumes
ListVolumeStatsByVolumeAccessGroup
Elenca tutti i nodi
ListVolumesForAccount
ListBackupTargets

segnalazione

Per il tipo di accesso alla segnalazione sono disponibili i seguenti metodi:

ClearClusterFaults
OttieniEfficienzaVolume
Ottieni efficienza dell'account
Ottieni statistiche sul volume
Ottieni capacità cluster
ListCloneJobs
OttieniClusterHardwareInfo
ListClusterFaults
Ottieni informazioni sul cluster

ListClusterPairs
OttieniClusterMasterNodeID
ListDriveHardware
Ottieni statistiche cluster
ElencoEventi
Ottieni informazioni sull'hardware dell'unità
ElencoISCSISessioni
Ottieni statistiche di guida
ListSchedules
OttieniConfigurazione di rete
ElencoServizi
Ottieni informazioni hardware del nodo
ListSyncJobs
Ottieni statistiche nodo
ElencoRetiVirtuali
OttieniSnmpInfo
ListVolumeStatsByAccount
OttieniSnmpTrapInfo
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:

Crea volume
Elimina volume
Modifica destinazione backup
CloneVolume
DeleteVolumePairing
ModificaVolumi
Clona più volumi
Ottieni destinazione di backup
Modifica coppia di volumi
Crea destinazione di backup
OttieniQoS predefinito
PurgeDeletedVolume
Crea istantanea
ListActiveVolumes
RimuoviBackupTarget
Crea istantanea di gruppo
ListBackupTarget
RemoveVolumePair
CompleteVolumePairing

ListGroupSnapshots
RipristinaVolumeEliminato
Clona più volumi
ListVolumesForAccount
RollbackToGroupSnapshot
EliminaSnapshot di Gruppo
ElencoVolumiEliminati
RollbackToSnapshot
EliminaSnapshot
ListGroupSnapshots
StartBulkVolumeRead
StartBulkVolumeWrite
StartVolumePairing
AggiornaStatoVolumeMassuale

scrivere

Per il tipo di accesso in scrittura sono disponibili i seguenti metodi:

Aggiungi unità
Rimuovi nodi
Aggiungi nodi
RimuoviAccount
Aggiungi account
RimuoviVolumiDaVolumeAccessGroup

AggiungiVolumeAGruppoAccessoVolume
RemoveInitiatorsFromVolumeAccessGroup
AggiungiIniziatoriAlGruppoAccessoVolume
DeleteVolumeAccessGroup
Crea gruppo di accesso al volume
Elimina volume
ModificaVolumeAccessGroup
RipristinaVolumeEliminato
Modifica Account
PurgeDeletedVolume
Crea volume
ModificaVolume
CloneVolume
Ottieni risultato asincrono
Rimuovi unità

Informazioni correlate

["Scopri i tipi di accesso disponibili nell'interfaccia utente di Element"](#)

Esempi di risposta

OttieniConfig

IL `GetConfig` restituisce una risposta simile al seguente esempio. 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
}
}
}
}
}

```

OttieniClusterHardwareInfo

Il `GetClusterHardwareInfo` restituisce una risposta simile al seguente esempio.

```
{
  "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-e3a7-3c47608cfac",
          "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
  }
}

```



```

    "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},
  {...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",
    "modelName": "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": "660000000",
    "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
  }
}

```

```
}  
}
```

OttieniLldpInfo

IL `GetLldpInfo` restituisce una risposta simile al seguente esempio.

```
{  
  "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"
        }
    ]
}

```



```

        "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` metodo per iSCSI restituisce una risposta simile al seguente esempio.

```

{
    "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 i nodi Fibre Channel)

IL `GetNodeHardwareInfo` Il metodo per i nodi Fibre Channel restituisce una risposta simile al seguente esempio.

```

{
  "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": "330000000",
"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": "330000000",
"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": "330000000",
"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": "330000000",
"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
},
"fibresChannelPorts": [
  {
    "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": "330000000",
  "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": "330000000",
  "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": "330000000",
  "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": "660000000",
    "description": "SATA controller",
    "physid": "1f.2",
    "product": "C600/X79 series chipset 6-Port SATA AHCI Controller",
    "vendor": "Intel Corporation",
    "version": "05",
    "width": "32"
  }
},
"system": {
  "fcv-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"
}
}

```

Ottieni informazioni Nvram

IL `GetNvramInfo` restituisce una risposta simile al seguente esempio.


```

{
  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"
}
}

```

ListActiveNodes

IL `ListActiveNodes` restituisce una risposta simile al seguente esempio.

```

{
    "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` restituisce una risposta simile al seguente esempio.

```

{
  "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": "306f746f000000001f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f00000001",
        "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": "306f746f000000006f47acc0100000000",
    "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": "306f746f000000007f47acc01000000000",
    "scsiNAADeviceID": "6f47acc1000000000306f746f000000007",
    "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": "306f746f000000008f47acc01000000000",
    "scsiNAADeviceID": "6f47acc1000000000306f746f000000008",
    "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": "306f746f000000010f47acc0100000000",
    "scsiNAADeviceID": "6f47acc100000000306f746f000000010",
    "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": "306f746f000000011f47acc01000000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000011",
        "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": "306f746f000000012f47acc0100000000",
        "scsiNAADeviceID": "6f47acc1000000000306f746f000000012",
        "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": "306f746f000000018f47acc01000000000",
"scsiNAADeviceID": "6f47acc1000000000306f746f000000018",
"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 restituisce una risposta simile al seguente esempio.

```

{
  "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 vCenter Server

NetApp Element Plug-in per vCenter Server fornisce un plug-in all'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, vedere ["Documentazione del plug-in NetApp Element per vCenter Server"](#) .

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)

Archiviazione del monitor con SolidFire Active IQ

"SolidFire Active IQ" è uno strumento basato sul Web che fornisce visualizzazioni storiche costantemente aggiornate dei dati dell'intero cluster. È possibile impostare avvisi per eventi, soglie o metriche specifici. SolidFire Active IQ consente di monitorare le prestazioni e la capacità del sistema, nonché di rimanere informati sullo stato di salute del cluster.

Puoi trovare le seguenti informazioni sul tuo sistema in SolidFire Active IQ:

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

Per saperne di più su SolidFire Active IQ, vedere ["Documentazione di SolidFire Active IQ"](#) .

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- [Sito di supporto NetApp](#) > [Strumenti 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 utilità 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 VMware vCenter ed evitare di definire le stesse risorse di archiviazione e di elaborazione o istanze vCenter in più nodi di gestione.

Per i cluster che eseguono il software Element versione 11.3 o successiva, è possibile lavorare con il nodo di gestione utilizzando una delle due interfacce:

- Con l'interfaccia utente del nodo di gestione([https://\[mNode IP\]:442](https://[mNode IP]:442)), è possibile apportare modifiche alle impostazioni di rete e cluster, eseguire test di sistema o utilizzare utilità di sistema.
- Con l'interfaccia utente API REST integrata([https://\[mNode IP\]/mnode](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.

Installa o ripristina un nodo di gestione:

- ["Installa un nodo di gestione"](#)
- ["Configurare un controller di interfaccia di rete \(NIC\) di archiviazione"](#)
- ["Recupera un nodo di gestione"](#)

Accedi al nodo di gestione:

- ["Accedi al nodo di gestione \(interfaccia utente o API REST\)"](#)

Cambia il certificato SSL predefinito:

- ["Modificare il certificato SSL predefinito del nodo di gestione"](#)

Eseguire attività con l'interfaccia utente del nodo di gestione:

- ["Panoramica dell'interfaccia utente del nodo di gestione"](#)

Eseguire attività con le API REST del nodo di gestione:

- ["Panoramica dell'interfaccia utente dell'API REST del nodo di gestione"](#)

Disattiva o abilita la funzionalità SSH remota oppure avvia una sessione di tunnel di supporto remoto con il supporto NetApp per aiutarti a risolvere i seguenti problemi:

- ["Accesso ai nodi di archiviazione tramite SSH per la risoluzione dei problemi di base"](#)
 - ["Abilita le connessioni remote al supporto NetApp"](#)
 - ["Gestire la funzionalità SSH sul nodo di gestione"](#)

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Installa o ripristina un nodo di gestione

Installa un nodo di gestione

È possibile installare manualmente il nodo di gestione per il cluster che esegue il software NetApp Element utilizzando l'immagine appropriata per la configurazione.

Questa procedura manuale è destinata agli amministratori di storage all-flash SolidFire che non utilizzano NetApp Deployment Engine per l'installazione del nodo di gestione.

Prima di iniziare

- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- La tua installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.



Se è necessario il supporto IPv6, è possibile utilizzare il nodo di gestione 11.1.

- Hai l'autorizzazione per scaricare il software dal sito di supporto NetApp .
- 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.

Informazioni su questo compito

Il nodo di gestione Element 12.2 è un aggiornamento facoltativo. Non è necessario per le distribuzioni esistenti.

Prima di seguire questa procedura, dovresti avere una comprensione di ["Volumi persistenti"](#) e se vuoi usarli o meno. I volumi persistenti sono facoltativi ma consigliati per il ripristino dei dati di configurazione del nodo di gestione in caso di perdita di una macchina virtuale (VM).

Passaggio 1: scaricare ISO o OVA e distribuire la VM

Scaricare l'ISO o l'OVA appropriato dal sito di supporto NetApp e installare la VM.

Passi

1. Scarica l'OVA o l'ISO per la tua installazione da "[Element Software](#)" pagina sul sito di supporto NetApp .
 - a. Selezionare **Scarica l'ultima versione** e accettare l'EULA.
 - b. Seleziona l'immagine del nodo di gestione che desideri scaricare.
2. Se hai scaricato l'OVA, segui questi passaggi:
 - a. Distribuisci l'OVA.
 - b. Se il cluster di archiviazione 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 archiviazione (ad esempio, eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di archiviazione.
3. Se hai scaricato l'ISO, segui questi passaggi:
 - a. Crea una nuova VM a 64 bit dal tuo hypervisor con la seguente configurazione:
 - Sei CPU virtuali
 - 24 GB di RAM
 - Tipo di adattatore di archiviazione 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 dell'adattatore di archiviazione selezionando **Personalizza hardware > Hardware virtuale**. Se necessario, modificare LSI Logic SAS in **LSI Logic Parallel**.

- Disco virtuale da 400 GB, thin provisioning
- Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
- (Facoltativo) Un'interfaccia di rete virtuale con accesso alla rete di gestione del cluster di storage. Se il cluster di archiviazione 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 archiviazione (eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di archiviazione.



Non accendere la VM prima del passaggio che indica di farlo più avanti in questa procedura.

- b. Collegare l'ISO alla VM e avviare l'immagine di installazione .iso.



L'installazione di un nodo di gestione tramite l'immagine potrebbe comportare un ritardo di 30 secondi prima che venga visualizzata la schermata iniziale.

4. Una volta completata l'installazione, accendere la macchina virtuale per il nodo di gestione.

Passaggio 2: creare l'amministratore del nodo di gestione e configurare la rete

Una volta completata l'installazione della VM, creare l'utente amministratore del nodo di gestione e configurare la rete del nodo di gestione.

Passi

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente amministratore del nodo di gestione.



Per spostarsi tra le opzioni del menu, premere i tasti freccia Su o Giù. Per spostarsi tra i pulsanti, premere Tab. Per passare dai pulsanti ai campi, premere Tab. Per navigare 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 IP con un'unità di trasmissione massima (MTU) inferiore a 1500 byte, è necessario eseguire i seguenti passaggi:
 - a. Posizionare temporaneamente il nodo di gestione su una rete vSphere senza DHCP, ad esempio iSCSI.
 - b. Riavviare la VM o riavviare la rete della VM.
 - c. Utilizzando l'interfaccia utente terminale (TUI), configurare l'IP corretto sulla rete di gestione con un MTU maggiore o uguale a 1500 byte.
 - d. Riassegnare la rete VM corretta alla VM.



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 del nodo di gestione (eth0).



Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di archiviazione, consultare le istruzioni per la configurazione di un'altra scheda di rete: ["Configurare un controller di interfaccia di rete \(NIC\) di archiviazione"](#).

Passaggio 3: configurare la sincronizzazione dell'ora

Prima di configurare il nodo di gestione, sincronizzare l'ora tra il nodo di gestione e il cluster di archiviazione.

Passi

1. Verificare che l'ora sia sincronizzata tra il nodo di gestione e il cluster di archiviazione tramite NTP:



A partire dall'elemento 12.3.1, i sotto-passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1, procedere a [sottofase \(f\)](#) per completare la configurazione della sincronizzazione dell'ora.

1. Accedi al nodo di gestione tramite SSH o la console fornita dal tuo hypervisor.
2. Fermare NTPD:

```
sudo service ntpd stop
```

3. Modifica il file di configurazione NTP `/etc/ntp.conf`:
 - a. Commenta i server predefiniti(`server 0.gentoo.pool.ntp.org`) aggiungendo un `#` davanti a ciascuno.
 - b. Aggiungere una nuova riga per ogni server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati sul cluster di archiviazione che si utilizzerà in un [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. Una volta completato, salvare il file di configurazione.

4. Forza una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

5. Riavviare NTPD.

```
sudo service ntpd start
```

6. Disabilitare la sincronizzazione oraria con l'host tramite l'hypervisor (di seguito è riportato un esempio VMware):



Se si distribuisce 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. Disattiva la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

b. Visualizza e conferma lo stato attuale del servizio:

```
vmware-toolbox-cmd timesync status
```

c. In vSphere, verificare che Synchronize guest time with host la casella non è selezionata nelle opzioni della VM.



Non abilitare questa opzione se in futuro apporti modifiche alla VM.



Non modificare l'NTP dopo aver completato la configurazione della sincronizzazione dell'ora perché influisce sull'NTP quando si esegue il [comando di configurazione](#) sul nodo di gestione.

Passaggio 4: impostare il nodo di gestione

Configurare il nodo di gestione utilizzando `setup-mnode` comando.

Passi

1. Configurare ed eseguire il comando di configurazione del nodo di gestione:



Ti verrà 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 raggiungere una rete pubblica.

```
sudo /sf/packages/mnode/setup-mnode --mnode_admin_user [username]
--storage_mvip [mvip] --storage_username [username] --telemetry_active
[true]
```

- a. Sostituisci il valore tra parentesi quadre [] (incluse le parentesi) per ciascuno dei seguenti parametri obbligatori:



La forma abbreviata del nome del comando è tra parentesi () e può essere sostituita al nome completo.

- **--mnode_admin_user (-mu) [nome utente]:** 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 archiviazione che esegue il software Element. Configurare il nodo di gestione con lo stesso cluster di archiviazione utilizzato durante [Configurazione dei server NTP](#).
 - **--storage_username (-su) [nome utente]:** il nome utente dell'amministratore del cluster di archiviazione per il cluster specificato da `--storage_mvip` parametro.
 - **--telemetry_active (-t) [true]:** Mantieni il valore true che abilita la raccolta dati per l'analisi da parte di Active IQ.
- b. (Facoltativo): aggiungere i parametri dell'endpoint Active IQ al comando:
 - **--remote_host (-rh) [AIQ_endpoint]:** l'endpoint in cui i dati di telemetria Active IQ vengono inviati per essere elaborati. Se il parametro non è incluso, viene utilizzato l'endpoint predefinito.
 - c. (Consigliato): aggiungere i seguenti parametri del volume persistente. Non modificare o eliminare l'account e i volumi creati per la funzionalità dei volumi persistenti, altrimenti si verificherà una perdita di capacità di gestione.
 - **--use_persistent_volumes (-pv) [true/false, default: false]:** Abilita o disabilita i volumi persistenti. Immettere il valore true per abilitare la funzionalità dei volumi persistenti.
 - **--persistent_volumes_account (-pva) [nome_account]:** Se `--use_persistent_volumes` è impostato su true, utilizzare questo parametro e immettere il nome dell'account di archiviazione 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 per i volumi persistenti separato dal resto dell'ambiente.

- **--persistent_volumes_mvip (-pvm) [mvip]**: immettere l'indirizzo IP virtuale di gestione (MVIP) del cluster di archiviazione che esegue il software Element che verrà utilizzato con i volumi persistenti. Questa operazione è necessaria solo se il nodo di gestione gestisce più cluster di archiviazione. Se non vengono gestiti più cluster, verrà utilizzato il cluster MVIP predefinito.

d. Configurare un server proxy:

- **--use_proxy (-up) [true/false, default: false]**: Abilita o disabilita l'uso 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. Questo è necessario se si desidera utilizzare un proxy. Se lo specifichi, ti verrà chiesto di inserire `--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) [porta, predefinita: 0]**: La porta proxy. Se lo specifichi, ti verrà chiesto di inserire il nome host o l'IP del proxy(`--proxy_hostname_or_ip`).
- **--proxy_ssh_port (-ps) [porta, predefinita: 443]**: La porta del proxy SSH. Per impostazione predefinita, la porta è 443.

e. (Facoltativo) Utilizzare la guida sui 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. Esegui il `setup-mnode` comando.

Passaggio 5: configurare le risorse del controller

Individua l'ID di installazione e aggiungi una risorsa del controller vCenter.

Passi

1. Individuare l'ID di installazione:

- Da un browser, accedi all'interfaccia utente dell'API REST del nodo di gestione:
- Accedere all'MVIP di archiviazione ed effettuare l'accesso. Questa azione determina l'accettazione del certificato per il passaggio successivo.
- Aprire l'interfaccia utente dell'API REST del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- Seleziona **Autorizza** e completa quanto segue:
 - Immettere il nome utente e la password del cluster.
 - Inserisci l'ID cliente come `mnode-client`.
 - Selezionare **Autorizza** per iniziare una sessione.
- Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.
- Seleziona **Provalo**.
- Selezionare **Esegui**.

- h. Dal corpo della risposta del codice 200, copiare e salvare il `id` per l'installazione da utilizzare in una fase successiva.

L'installazione presenta una configurazione di risorse di base creata durante l'installazione o l'aggiornamento.

2. Aggiungere una risorsa del controller vCenter per NetApp Hybrid Cloud Control alle risorse note del nodo di gestione:
 - a. Accedi all'interfaccia utente dell'API del servizio `mnode` sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode` :

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

- b. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client` .
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudi la finestra.
- c. Selezionare **POST /assets/{asset_id}/controllers** per aggiungere una sotto-risorsa del controller.



È necessario creare un nuovo ruolo NetApp HCC in vCenter per aggiungere una sotto-risorsa del controller. Questo nuovo ruolo NetApp HCC limiterà la visualizzazione dei servizi del nodo di gestione alle sole risorse NetApp. Vedere ["Creare un ruolo NetApp HCC in vCenter"](#) .

- d. Seleziona **Provalo**.
- e. Inserisci l'ID della risorsa di base padre che hai copiato negli appunti nel campo **asset_id**.
- f. Inserisci i valori del payload richiesti con il tipo `vCenter` e credenziali `vCenter`.
- g. Selezionare **Esegui**.

Trova maggiori informazioni

- ["Volumi persistenti"](#)
- ["Aggiungere una risorsa controller al nodo di gestione"](#)
- ["Configurare una scheda di rete di archiviazione"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Creare un ruolo NetApp HCC in vCenter

È necessario creare un ruolo NetApp HCC in vCenter per aggiungere manualmente le risorse vCenter (controller) al nodo di gestione dopo l'installazione o per modificare i controller esistenti.

Questo ruolo NetApp HCC limita la visualizzazione dei servizi del nodo di gestione alle sole risorse NetApp.

Informazioni su questo compito

- Questa procedura descrive i passaggi disponibili nella versione 6.7 di vSphere. L'interfaccia utente di vSphere potrebbe differire leggermente da quella descritta, a seconda della versione di vSphere installata. Per ulteriore assistenza, consultare la documentazione di VMware vCenter.
- A "[creare un nuovo ruolo NetApp HCC](#)", per prima cosa devi configurare un nuovo account utente in vCenter, creare un ruolo NetApp HCC e quindi assegnare le autorizzazioni utente.
- Per le configurazioni host NetApp ESXi, è necessario aggiornare l'account utente creato da NDE al nuovo ruolo NetApp HCC:
 - Utilizzo "[questa opzione](#)" se l'host NetApp ESXi non esiste all'interno di un cluster host vCenter
 - Utilizzo "[questa opzione](#)" se l'host NetApp ESXi esiste all'interno di un cluster host vCenter
- Puoi "[configurare una risorsa controller](#)" che esiste già sul nodo di gestione.
- Utilizzare il nuovo ruolo NetApp HCC per "[aggiungere una risorsa](#)" al nodo di gestione.

Crea un nuovo ruolo NetApp HCC

Configurare un nuovo account utente in vCenter, creare un ruolo NetApp HCC e quindi assegnare le autorizzazioni all'utente.

Configurare un nuovo account utente in vCenter

Per configurare un nuovo account utente in vCenter, procedere come segue.

Passi

1. Accedi a vSphere Web Client come `administrator@vsphere.local` o equivalente.
2. Dal menu, seleziona **Amministrazione**.
3. Nella sezione **Single Sign On**, seleziona **Utenti e Gruppi**.
4. Nell'elenco **Dominio**, seleziona `vsphere.local` o il tuo dominio LDAP.
5. Selezionare **Aggiungi utente**.
6. Compila il modulo **Aggiungi utente**.

Crea un nuovo ruolo NetApp HCC in vCenter

Per creare un nuovo ruolo NetApp HCC in vCenter, procedere come segue.

Passi

1. Selezionare **Modifica ruolo** e assegnare le autorizzazioni richieste.
2. Nel riquadro di navigazione a sinistra, seleziona **Globale**.
3. Selezionare **Diagnostica e Licenze**.
4. Nel riquadro di navigazione a sinistra, seleziona **Host**.
5. Selezionare **Manutenzione, Alimentazione, Configurazione partizione di archiviazione e Firmware**.
6. Salva come `NetApp Role`.

Assegnare le autorizzazioni utente a vCenter

Per assegnare le autorizzazioni utente al nuovo ruolo NetApp HCC in vCenter, procedere come segue.

Passi

1. Dal menu, seleziona **Host e Cluster**.
2. Nel riquadro di navigazione a sinistra, seleziona una delle seguenti opzioni:
 - Il vCenter di livello superiore.
 - Il vCenter desiderato se ci si trova in modalità collegata.



- A partire da NetApp Element Plug-in per vCenter Server 5.0, da utilizzare ["Modalità collegata vCenter"](#), è possibile registrare Element Plug-in da un nodo di gestione separato per ciascun vCenter Server che gestisce i cluster di storage NetApp SolidFire (consigliato).
- Utilizzo del plug-in NetApp Element per vCenter Server 4.10 e versioni precedenti per gestire le risorse del cluster da altri vCenter Server utilizzando ["Modalità collegata vCenter"](#) è limitato solo ai cluster di archiviazione locali.

3. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP
- b. Utilizza la ricerca per trovare il nuovo utente che hai creato in [Configurare un nuovo account utente in vCenter](#).
- c. Selezionare `NetApp Role`.



NON selezionare **Propaga ai figli**.

Add Permission | satyabra-vcenter01.mgmt.ict.openengla... X

User: vsphere.local

Q netapp

Role: NetApp Role

☐ Propagate to children

CANCEL OK

Assegnare le autorizzazioni utente al datacenter

Per assegnare le autorizzazioni utente al data center in vCenter, procedere come segue.

Passi

1. Nel riquadro a sinistra, seleziona **Datacenter**.
2. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
3. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.
- b. Utilizza la ricerca per trovare il nuovo utente HCC che hai creato in [Configurare un nuovo account utente in vCenter](#).
- c. Selezionare `ReadOnly role`.



NON selezionare **Propaga ai figli**.

Assegnare autorizzazioni utente ai datastore NetApp HCI

Per assegnare le autorizzazioni utente ai datastore NetApp HCI in vCenter, procedere come segue.

Passi

1. Nel riquadro a sinistra, seleziona **Datacenter**.
2. Crea una nuova cartella di archiviazione. Fare clic con il tasto destro del mouse su **Datacenter** e selezionare **Crea cartella di archiviazione**.
3. Trasferire tutti i datastore NetApp HCI dal cluster di storage e quelli locali al nodo di elaborazione nella nuova cartella di storage.
4. Selezionare la nuova cartella di archiviazione.
5. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
6. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.
- b. Utilizza la ricerca per trovare il nuovo utente HCC che hai creato in [Configurare un nuovo account utente in vCenter](#).
- c. Selezionare `Administrator role`
- d. Seleziona **Propaga ai figli**.

Assegnare autorizzazioni utente a un cluster host NetApp

Per assegnare le autorizzazioni utente a un cluster host NetApp in vCenter, procedere come segue.

Passi

1. Nel riquadro di navigazione a sinistra, seleziona il cluster host NetApp.
2. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.

3. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.
- b. Utilizza la ricerca per trovare il nuovo utente HCC che hai creato in [Configurare un nuovo account utente in vCenter](#).
- c. Selezionare `NetApp Role O Administrator`.
- d. Seleziona **Propaga ai figli**.

Configurazioni host NetApp ESXi

Per le configurazioni host NetApp ESXi, è necessario aggiornare l'account utente creato da NDE al nuovo ruolo NetApp HCC.

L'host NetApp ESXi non esiste in un cluster host vCenter

Se l'host NetApp ESXi non esiste all'interno di un cluster host vCenter, è possibile utilizzare la seguente procedura per assegnare il ruolo NetApp HCC e le autorizzazioni utente in vCenter.

Passi

1. Dal menu, seleziona **Host e Cluster**.
2. Nel riquadro di navigazione a sinistra, seleziona l'host NetApp ESXi.
3. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.
 - b. Utilizza la ricerca per trovare il nuovo utente che hai creato in [Configurare un nuovo account utente in vCenter](#).
 - c. Selezionare `NetApp Role O Administrator`.
5. Seleziona **Propaga ai figli**.

L'host NetApp ESXi esiste in un cluster host vCenter

Se un host NetApp ESXi è presente all'interno di un cluster host vCenter con host ESXi di altri fornitori, è possibile utilizzare la seguente procedura per assegnare il ruolo NetApp HCC e le autorizzazioni utente in vCenter.

1. Dal menu, seleziona **Host e Cluster**.
2. Nel riquadro di navigazione a sinistra, espandere il cluster host desiderato.
3. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
4. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.

- b. Utilizza la ricerca per trovare il nuovo utente che hai creato in [Configurare un nuovo account utente in vCenter](#) .
- c. Selezionare NetApp Role .



NON selezionare **Propaga ai figli**.

5. Nel riquadro di navigazione a sinistra, seleziona un host NetApp ESXi.
6. Nel riquadro di navigazione a destra, seleziona **Autorizzazioni**.
7. Selezionare l'icona **+** per aggiungere il nuovo utente.

Aggiungere i seguenti dettagli nella finestra **Aggiungi autorizzazione**:

- a. Selezionare `vsphere.local` o il tuo dominio LDAP.
 - b. Utilizza la ricerca per trovare il nuovo utente che hai creato in [Configurare un nuovo account utente in vCenter](#) .
 - c. Selezionare NetApp Role `O Administrator` .
 - d. Seleziona **Propaga ai figli**.
8. Ripetere la procedura per gli host NetApp ESXi rimanenti nel cluster host.

La risorsa del controller esiste già sul nodo di gestione

Se una risorsa controller esiste già sul nodo di gestione, eseguire i passaggi seguenti per configurare il controller utilizzando `PUT /assets /{asset_id} /controllers /{controller_id}` .

Passi

1. Accedi all'interfaccia utente dell'API del servizio mnode sul nodo di gestione:

<https://<ManagementNodeIP>/mnode>

2. Selezionare **Autorizza** e immettere le credenziali per accedere alle chiamate API.
3. Selezionare `GET /assets` per ottenere l'ID genitore.
4. Selezionare `PUT /assets /{asset_id} /controllers /{controller_id}` .
 - a. Inserire nel corpo della richiesta le credenziali create durante la configurazione dell'account.

Aggiungi una risorsa al nodo di gestione

Se è necessario aggiungere manualmente una nuova risorsa dopo l'installazione, utilizzare il nuovo account utente HCC creato in [Configurare un nuovo account utente in vCenter](#) . Per maggiori informazioni, vedere ["Aggiungere una risorsa controller al nodo di gestione"](#).

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Configurare un controller di interfaccia di rete (NIC) di archiviazione

Se si utilizza una scheda di rete aggiuntiva per l'archiviazione, è possibile accedere tramite SSH al nodo di gestione oppure utilizzare la console vCenter ed eseguire un comando curl per configurare un'interfaccia di rete con o senza tag.

Prima di iniziare

- Conosci il tuo indirizzo IP eth0.
- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai distribuito un nodo di gestione 11.3 o versione successiva.

Opzioni di configurazione

Scegli l'opzione più adatta al tuo ambiente:

- [Configurare un controller di interfaccia di rete \(NIC\) di archiviazione per un'interfaccia di rete senza tag](#)
- [Configurare un controller di interfaccia di rete \(NIC\) di archiviazione per un'interfaccia di rete con tag](#)

Configurare un controller di interfaccia di rete (NIC) di archiviazione per un'interfaccia di rete senza tag

Passi

1. Aprire una console SSH o vCenter.
2. Sostituisci i valori nel seguente modello di comando ed esegui il comando:



I valori sono rappresentati da \$ per ciascuno dei parametri richiesti per la nuova interfaccia di rete di archiviazione. IL `cluster` L'oggetto nel modello seguente è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` O `-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 controller di interfaccia di rete (NIC) di archiviazione per un'interfaccia di rete con tag

Passi

1. Aprire una console SSH o vCenter.
2. Sostituisci i valori nel seguente modello di comando ed esegui il comando:



I valori sono rappresentati da \$ per ciascuno dei parametri richiesti per la nuova interfaccia di rete di archiviazione. IL `cluster` L'oggetto nel modello seguente è obbligatorio e può essere utilizzato per la ridenominazione del nome host del nodo di gestione. `--insecure` O `-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"
}
```

Trova maggiori informazioni

- ["Aggiungere una risorsa controller al nodo di gestione"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Recupera 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 distribuire un nuovo OVA ed eseguire uno script di ridistribuzione per estrarre i dati di configurazione da un nodo di gestione installato in precedenza che esegue la versione 11.3 e successive.

Cosa ti servirà

- Il tuo precedente nodo di gestione eseguiva il software NetApp Element versione 11.3 o successiva con ["Volumi persistenti"](#) funzionalità attivata.
- Si conoscono i valori MVIP e SVIP del cluster contenente i volumi persistenti.
- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- La tua installazione utilizza IPv4. Il nodo di gestione 11.3 non supporta IPv6.
- Hai l'autorizzazione per scaricare il software dal sito di supporto NetApp .
- 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

Passi

1. [Scarica ISO o OVA e distribuisce la VM](#)
2. [Configurare la rete](#)
3. [Configurare la sincronizzazione dell'ora](#)
4. [Configurare il nodo di gestione](#)

Scarica ISO o OVA e distribuisce la VM

1. Scarica l'OVA o l'ISO per la tua installazione da ["Software Element"](#) pagina sul sito di supporto NetApp .
 - a. Selezionare **Scarica l'ultima versione** e accettare l'EULA.
 - b. Seleziona l'immagine del nodo di gestione che desideri scaricare.
2. Se hai scaricato l'OVA, segui questi passaggi:
 - a. Distribuisce l'OVA.
 - b. Se il cluster di archiviazione 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 archiviazione (ad esempio, eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di archiviazione.
3. Se hai scaricato l'ISO, segui questi passaggi:
 - a. Crea una nuova macchina virtuale a 64 bit dal tuo hypervisor con la seguente configurazione:
 - Sei CPU virtuali
 - 24 GB di RAM
 - Disco virtuale da 400 GB, thin provisioning
 - Un'interfaccia di rete virtuale con accesso a Internet e accesso allo storage MVIP.
 - (Facoltativo per l'archiviazione all-flash SolidFire) Un'interfaccia di rete virtuale con accesso alla rete di gestione del cluster di archiviazione. Se il cluster di archiviazione 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 archiviazione (eth1) o assicurarsi che la rete di gestione possa instradare verso la rete di archiviazione.



Non accendere la macchina virtuale prima del passaggio che indica di farlo più avanti in questa procedura.

b. Collegare l'ISO alla macchina virtuale e avviare l'immagine di installazione .iso.



L'installazione di un nodo di gestione tramite l'immagine potrebbe comportare un ritardo di 30 secondi prima che venga visualizzata la schermata iniziale.

4. Una volta completata l'installazione, accendere la macchina virtuale per il nodo di gestione.

Configurare la rete

1. Utilizzando l'interfaccia utente del terminale (TUI), creare un utente amministratore del nodo di gestione.



Per spostarsi tra le opzioni del menu, premere i tasti freccia Su o Giù. Per spostarsi tra i pulsanti, premere Tab. Per passare dai pulsanti ai campi, premere Tab. Per navigare tra i campi, premere i tasti freccia Su o Giù.

2. Configurare la rete del nodo di gestione (eth0).



Se è necessaria una scheda di rete aggiuntiva per isolare il traffico di archiviazione, consultare le istruzioni per la configurazione di un'altra scheda di rete: "[Configurare un controller di interfaccia di rete \(NIC\) di archiviazione](#)".

Configurare la sincronizzazione dell'ora

1. Verificare che l'ora sia sincronizzata tra il nodo di gestione e il cluster di archiviazione tramite NTP:



A partire dall'elemento 12.3.1, i sotto-passaggi da (a) a (e) vengono eseguiti automaticamente. Per il nodo di gestione 12.3.1 o successivo, procedere [asottofase \(f\)](#) per completare la configurazione della sincronizzazione dell'ora.

1. Accedi al nodo di gestione tramite SSH o la console fornita dal tuo hypervisor.

2. Fermare NTPD:

```
sudo service ntpd stop
```

3. Modifica il file di configurazione NTP /etc/ntp.conf :

- Commenta i server predefiniti(`server 0.gentoo.pool.ntp.org`) aggiungendo un # davanti a ciascuno.
- Aggiungere una nuova riga per ogni server di riferimento orario predefinito che si desidera aggiungere. I server di riferimento orario predefiniti devono essere gli stessi server NTP utilizzati sul cluster di archiviazione che si utilizzerà in un "[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. Una volta completato, salvare il file di configurazione.

4. Forza una sincronizzazione NTP con il server appena aggiunto.

```
sudo ntpd -gq
```

5. Riavviare NTPD.

```
sudo service ntpd start
```

6. Disabilitare la sincronizzazione oraria con l'host tramite l'hypervisor (di seguito è riportato un esempio VMware):



Se si distribuisce 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. Disattiva la sincronizzazione periodica dell'ora:

```
vmware-toolbox-cmd timesync disable
```

b. Visualizza e conferma lo stato attuale del servizio:

```
vmware-toolbox-cmd timesync status
```

c. In vSphere, verificare che Synchronize guest time with host la casella non è selezionata nelle opzioni della VM.



Non abilitare questa opzione se in futuro apporti modifiche alla VM.



Non modificare l'NTP dopo aver completato la configurazione della sincronizzazione dell'ora perché influisce sull'NTP quando si esegue il [comando di ridistribuzione](#) sul nodo di gestione.

Configurare il nodo di gestione

1. Creare una directory di destinazione temporanea per il contenuto del bundle dei servizi di gestione:

```
mkdir -p /sf/etc/mnode/mnode-archive
```

2. Scaricare il bundle dei servizi di gestione (versione 2.15.28 o successiva) precedentemente installato sul nodo di gestione esistente e salvarlo nel `/sf/etc/mnode/ elenco`.
3. Estrarre il bundle scaricato utilizzando il seguente comando, sostituendo il valore tra parentesi quadre [] (incluse le parentesi) con il nome del file del bundle:

```
tar -C /sf/etc/mnode -xvf /sf/etc/mnode/[management services bundle file]
```

4. Estrarre il file risultante nel `/sf/etc/mnode-archive elenco`:

```
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. Sostituisci il valore tra parentesi quadre [] (incluse le parentesi) per ciascuno dei seguenti parametri obbligatori:
 - **[indirizzo IP mvip]**: indirizzo IP virtuale di gestione del cluster di storage. Configurare il nodo di gestione con lo stesso cluster di archiviazione utilizzato durante ["Configurazione dei server NTP"](#).
 - **[nome account volume persistente]**: nome dell'account associato a tutti i volumi persistenti in questo cluster di archiviazione.

1. Configurare ed eseguire il comando redeploy 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 precedente:



Ti verrà 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 raggiungere una rete pubblica.

```
sudo /sf/packages/mnode/redeploy-mnode --mnode_admin_user [username]
```

- a. Sostituire il valore tra parentesi quadre [] (incluse le parentesi) con 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.



Puoi aggiungere il nome utente o lasciare che sia lo script a chiederti le informazioni.

- b. Esegui il `redeploy-mnode` comando. Al termine della ridistribuzione, lo script visualizza un messaggio di successo.
- c. Se si accede alle interfacce Web di Element (ad esempio il nodo di gestione o NetApp Hybrid Cloud Control) utilizzando il nome di dominio completo (FQDN) del sistema, "[riconfigurare l'autenticazione per il nodo di gestione](#)".



Capacità SSH che fornisce "[Accesso alla sessione del tunnel di supporto remoto \(RST\) del supporto NetApp](#)" è disabilitato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 e versioni successive. Se in precedenza hai abilitato la funzionalità SSH sul nodo di gestione, potrebbe essere necessario "[disabilitare nuovamente SSH](#)" sul nodo di gestione recuperato.

Trova maggiori informazioni

- "[Volumi persistenti](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"
- "[Documentazione del software SolidFire ed Element](#)"

Accedi al nodo di gestione

A partire dalla versione 11.3 del software NetApp Element, 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 dei test e delle utilità del sistema operativo.

Per i cluster che eseguono il software Element versione 11.3 o successiva, è possibile utilizzare una delle due interfacce:

- Utilizzando l'interfaccia utente del nodo di gestione([https:// \[mNode IP\]:442](https://[mNode IP]:442)), è possibile apportare modifiche alle impostazioni di rete e cluster, eseguire test di sistema o utilizzare utilità di sistema.
- Utilizzando l'interfaccia utente API REST integrata([https://\[mNode IP\]/mnode](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.

Accedi all'interfaccia utente per nodo di gestione

Dall'interfaccia utente per nodo è possibile accedere alle impostazioni di rete e cluster e utilizzare test e utilità di sistema.

Passi

1. Accedi 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
```

Management

Network Settings - Management

Method :

Link Speed :

IPv4 Address :

IPv4 Subnet Mask :

IPv4 Gateway Address :

IPv6 Address :

IPv6 Gateway Address :

MTU :

DNS Servers :

Search Domains :

Status :

Routes

Add

- Quando richiesto, immettere il nome utente e la password del nodo di gestione.

Accedi all'interfaccia utente dell'API REST del nodo di gestione

Dall'interfaccia utente dell'API REST è possibile accedere a un menu di API correlate ai servizi che controllano i servizi di gestione sul nodo di gestione.

Passi

- Per accedere all'interfaccia utente dell'API REST per i servizi di gestione, immettere l'indirizzo IP del nodo di gestione seguito da /mnode :

```
https://[IP address]/mnode
```

MANAGEMENT SERVICES API ^{4.0}

[Base URL: /mnode]
https://10.117.1.100/mnode/swagger/json

The configuration REST service for MANAGEMENT SERVICES

NetApp - Website

NetApp Commercial Software License

Authorize 

logs Log service

GET /logs Get logs from the MNODE service(s)

assets Asset service

POST /assets Add a new asset

GET /assets Get all assets

GET /assets/compute-nodes Get all compute nodes

GET /assets/compute-nodes/{compute_node_id} Get a specific compute node by ID

GET /assets/controllers Get all controllers

GET /assets/controllers/{controller_id} Get a specific controller by ID

GET /assets/storage-clusters Get all storage clusters

GET /assets/storage-clusters/{storage_cluster_id} Get a specific storage cluster by ID

PUT /assets/{asset_id} Modify an asset with a specific ID

DELETE /assets/{asset_id} Delete an asset with a specific ID

GET /assets/{asset_id} Get an asset by it's ID

POST /assets/{asset_id}/compute-nodes Add a compute asset

GET /assets/{asset_id}/compute-nodes Get compute assets

PUT /assets/{asset_id}/compute-nodes/{compute_id} Update a specific compute node asset

DELETE /assets/{asset_id}/compute-nodes/{compute_id} Delete a specific compute node asset

2. Selezionare **Autorizza** o qualsiasi icona a forma di lucchetto e immettere le credenziali di amministratore del cluster per ottenere i permessi per utilizzare le API.

Trova maggiori informazioni

- ["Abilita il monitoraggio Active IQ e NetApp"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Modificare il certificato SSL predefinito del nodo di gestione

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

Quando si configura un nodo di gestione, viene creato un certificato Secure Sockets Layer (SSL) autofirmato univoco e una chiave privata che vengono utilizzati per tutte le comunicazioni HTTPS tramite l'interfaccia utente dell'elemento, l'interfaccia utente per nodo o le API. Il software Element supporta sia i certificati

autofirmati sia i certificati emessi e verificati da un'autorità di certificazione (CA) attendibile.

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

- **GetNodeSSLCertificate**

Puoi usare il "[Metodo GetNodeSSLCertificate](#)" per recuperare informazioni sul certificato SSL attualmente installato, compresi tutti i dettagli del certificato.

- **SetNodeSSLCertificate**

Puoi usare il "[Metodo SetNodeSSLCertificate](#)" per impostare i certificati SSL del cluster e per nodo sul certificato e sulla chiave privata forniti. Il sistema convalida il certificato e la chiave privata per impedire che venga applicato un certificato non valido.

- **RemoveNodeSSLCertificate**

Questo "[Metodo RemoveNodeSSLCertificate](#)" rimuove il certificato SSL e la chiave privata attualmente installati. Il cluster genera quindi un nuovo certificato autofirmato e una chiave privata.

Trova maggiori informazioni

- "[Cambia il certificato SSL predefinito del software Element](#)"
- "[Quali sono i requisiti per l'impostazione di certificati SSL personalizzati in Element Software?](#)"
- "[Documentazione del software SolidFire ed Element](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"

Lavorare con 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 cluster, eseguire test di sistema o utilizzare utilità di sistema.

Attività che puoi eseguire con l'interfaccia utente del nodo di gestione:

- "[Configurare il monitoraggio degli avvisi](#)"
- "[Modificare e testare le impostazioni di rete, cluster e sistema del nodo di gestione](#)"
- "[Eseguire le utilità di sistema dal nodo di gestione](#)"

Trova maggiori informazioni

- "[Accedi al nodo di gestione](#)"
- "[Plug-in NetApp Element per vCenter Server](#)"
- "[Documentazione del 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 l'archiviazione all-flash SolidFire . L'esecuzione degli strumenti per questi cluster genera il seguente errore 405, previsto data la 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 testare le impostazioni di rete, cluster e sistema del nodo di gestione

È possibile modificare e testare le impostazioni di rete, cluster e sistema del nodo di gestione.

- [Aggiorna le impostazioni di rete del nodo di gestione](#)
- [Aggiorna le impostazioni del cluster del nodo di gestione](#)
- [Testare le impostazioni del nodo di gestione](#)

Aggiorna le impostazioni di rete del nodo di gestione

Nella scheda 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. Visualizza o inserisci le seguenti informazioni:
 - a. **Metodo**: Scegli uno dei seguenti metodi per configurare l'interfaccia:
 - `loopback`: Utilizzare per definire l'interfaccia di loopback IPv4.
 - `manual`: Utilizzare per definire le interfacce per le quali non viene effettuata alcuna configurazione predefinita.
 - `dhcp`: Utilizzare per ottenere un indirizzo IP tramite DHCP.
 - `static`: Utilizzare per definire interfacce Ethernet con indirizzi IPv4 assegnati staticamente.
 - b. **Velocità di collegamento**: la velocità negoziata dalla NIC virtuale.
 - c. **Indirizzo IPv4**: l'indirizzo IPv4 per la rete eth0.
 - d. **Maschera di sottorete IPv4**: suddivide gli indirizzi della rete IPv4.
 - e. **Indirizzo gateway IPv4**: indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.
 - f. **Indirizzo IPv6**: l'indirizzo IPv6 per la rete eth0.
 - g. **Indirizzo gateway IPv6**: indirizzo di rete del router per inviare pacchetti fuori dalla rete locale.



Le opzioni IPv6 non sono supportate per le versioni 11.3 o successive del nodo di gestione.

- h. **MTU**: dimensione massima del pacchetto che un protocollo di rete può trasmettere. Deve essere maggiore o uguale a 1500. Se si aggiunge una seconda scheda di rete di archiviazione, il valore dovrebbe essere 9000.
- i. **Server DNS**: interfaccia di rete utilizzata per la comunicazione del cluster.
- j. **Cerca domini**: cerca altri indirizzi MAC disponibili nel sistema.
- k. **Stato**: Valori possibili:
 - UpAndRunning
 - Down
 - Up
- l. **Percorsi**: percorsi statici verso host o reti specifici tramite l'interfaccia associata per la quale i percorsi sono configurati.

Aggiorna le impostazioni del cluster del nodo di gestione

Nella scheda Impostazioni cluster dell'interfaccia utente per nodo del nodo di gestione, è possibile modificare i campi dell'interfaccia cluster quando un nodo si trova negli stati Disponibile, In sospeso, In sospeso attivo e Attivo.

1. Aprire l'interfaccia utente del nodo di gestione per nodo.
2. Selezionare la scheda **Impostazioni cluster**.
3. Visualizza o inserisci le seguenti informazioni:
 - **Ruolo**: ruolo del nodo di gestione nel cluster. Valore possibile: Management .
 - **Versione**: versione del software Element in esecuzione sul cluster.
 - **Interfaccia predefinita**: interfaccia di rete predefinita utilizzata per la comunicazione del nodo di gestione con il cluster che esegue il software Element.

Testare le impostazioni del nodo di gestione

Dopo aver modificato le impostazioni di gestione e di rete per il nodo di gestione e aver confermato le modifiche, è possibile eseguire dei 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. Completa una delle seguenti operazioni:
 - a. Per verificare che le impostazioni di rete configurate siano valide per il sistema, selezionare **Test configurazione di rete**.
 - b. Per testare la connettività di rete a tutti i nodi del cluster su interfacce 1G e 10G utilizzando pacchetti ICMP, selezionare **Test Ping**.
4. Visualizza o inserisci quanto segue:
 - **Host**: specificare un elenco separato da virgole di indirizzi o nomi host di dispositivi da sottoporre a ping.
 - **Tentativi**: specifica il numero di volte in cui il sistema deve ripetere il ping di prova. Predefinito: 5.
 - **Dimensione pacchetto**: specifica il numero di byte da inviare nel pacchetto ICMP inviato a ciascun IP. Il numero di byte deve essere inferiore all'MTU massimo specificato nella configurazione di rete.

- **Timeout mSec:** specifica il numero di millisecondi da attendere per ogni singola risposta ping. Predefinito: 500 ms.
- **Timeout totale sec:** specifica il tempo in secondi che il ping deve attendere per una risposta del sistema prima di emettere il successivo tentativo di ping o di terminare il processo. Predefinito: 5.
- **Proibisci frammentazione:** abilita il flag DF (non frammentare) per i pacchetti ICMP.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Eseguire le utilità di sistema dal nodo di gestione

È possibile utilizzare l'interfaccia utente per nodo del nodo di gestione per creare o eliminare bundle di supporto cluster, reimpostare le impostazioni di configurazione del nodo o riavviare la rete.

Passi

1. Aprire l'interfaccia utente del nodo di gestione per nodo utilizzando le credenziali di amministratore del nodo di gestione.
2. Selezionare **Utilità di sistema**.
3. Selezionare il pulsante relativo all'utilità che si desidera eseguire:
 - a. **Controllo alimentazione:** riavvia, spegne e riaccende il nodo o lo spegne. Specificare una delle seguenti opzioni.



Questa operazione provoca una perdita temporanea della connettività di rete.

- **Azione:** Le opzioni includono `Restart` e `Halt` (spegnimento).
 - **Ritardo di riattivazione:** qualsiasi tempo aggiuntivo prima che il nodo torni online.
- b. **Crea bundle di supporto cluster:** crea il bundle di supporto cluster per assistere il supporto NetApp nelle valutazioni diagnostiche di uno o più nodi in un cluster. Specificare le seguenti opzioni:
 - **Nome pacchetto:** Nome univoco per ogni pacchetto di supporto creato. Se non viene specificato alcun nome, come nome del file vengono utilizzati "supportbundle" e il nome del nodo.
 - **Mvip:** MVIP del cluster. I bundle vengono raccolti da tutti i nodi del cluster. Questo parametro è obbligatorio se il parametro Nodi non è specificato.
 - **Nodi:** gli indirizzi IP dei nodi da cui raccogliere i bundle. Utilizzare `Nodes` o `Mvip`, ma non entrambi, per specificare i nodi da cui raccogliere i bundle. Questo parametro è obbligatorio se `Mvip` non è specificato.
 - **Nome utente:** Nome utente dell'amministratore del cluster.
 - **Password:** la password dell'amministratore del cluster.
 - **Consenti incompleto:** consente allo script di continuare l'esecuzione se non è possibile raccogliere i bundle da uno o più nodi.
 - **Argomenti aggiuntivi:** questo parametro viene fornito al `sf_make_support_bundle` sceneggiatura. Questo parametro deve essere utilizzato solo su richiesta del supporto NetApp.
 - c. **Elimina tutti i pacchetti di supporto:** elimina tutti i pacchetti di supporto correnti sul nodo di gestione.

d. **Reimposta nodo:** reimposta il nodo di gestione su una nuova immagine di installazione. In questo modo vengono ripristinate tutte le impostazioni predefinite, ad eccezione della configurazione di rete. Specificare le seguenti opzioni:

- **Build:** URL di un'immagine software Element remota su cui verrà ripristinato il nodo.
- **Opzioni:** Specifiche per l'esecuzione delle operazioni di reset. Se necessario, i dettagli saranno forniti dal supporto NetApp .



Questa operazione provoca una perdita temporanea della connettività di rete.

e. **Riavvia rete:** riavvia tutti i servizi di rete sul nodo di gestione.



Questa operazione provoca una perdita temporanea della connettività di rete.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Lavorare con l'API REST del nodo di gestione

Panoramica dell'interfaccia utente dell'API REST del nodo di gestione

Utilizzando l'interfaccia utente API REST 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 puoi eseguire con le API REST:

Autorizzazione

- ["Ottieni 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 risorse di cluster di archiviazione"](#)

Gestione delle risorse

- ["Visualizza o modifica le risorse del controller esistenti"](#)
- ["Creare e gestire risorse di cluster di archiviazione"](#)
- ["Utilizzare l'API REST per raccogliere i log di sistema di Element"](#)

- "Verificare le versioni del sistema operativo e dei servizi del nodo di gestione"
- "Ottenere i log dai servizi di gestione"

Trova maggiori informazioni

- "Accedi al nodo di gestione"
- "Plug-in NetApp Element per vCenter Server"
- "Documentazione del software SolidFire ed Element"

Ottieni l'autorizzazione per utilizzare le API REST

È necessario autorizzare prima di poter utilizzare le API per i servizi di gestione nell'interfaccia utente dell'API REST. Per farlo è necessario ottenere un token di accesso.

Per ottenere un token, è necessario fornire le credenziali di amministratore del cluster e un ID client. Ogni gettone dura circa dieci minuti. Dopo la scadenza di un token, è possibile autorizzare nuovamente un nuovo token di accesso.

La funzionalità di autorizzazione viene configurata per te durante l'installazione e la distribuzione del nodo di gestione. Il servizio token si basa sul cluster di archiviazione definito durante la configurazione.

Prima di iniziare

- La versione del cluster deve eseguire il software NetApp Element 11.3 o versione successiva.
- Avresti dovuto distribuire un nodo di gestione che esegue la 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`
```

Passaggi dell'interfaccia utente dell'API REST

1. Accedi all'interfaccia utente dell'API REST per il servizio immettendo l'indirizzo IP del nodo di gestione seguito dal nome del servizio, ad esempio `/mnode/`:

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

2. Selezionare **Autorizza**.



In alternativa, puoi selezionare l'icona del lucchetto accanto a qualsiasi API di servizio.

3. Completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Non immettere un valore per il segreto client.

d. Selezionare **Autorizza** per iniziare una sessione.

4. Chiudere la finestra di dialogo **Autorizzazioni disponibili**.



Se si tenta di eseguire un comando dopo la scadenza del token, un `401 Error: UNAUTHORIZED` appare il messaggio. Se vedi questo messaggio, autorizza di nuovo.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Abilita il monitoraggio Active IQ e NetApp

È possibile abilitare il monitoraggio dell'archiviazione Active IQ se non lo si è già fatto durante l'installazione o l'aggiornamento. Potrebbe essere necessario utilizzare questa procedura se non è stato configurato SolidFire Active IQ durante l'installazione di un sistema di archiviazione all-flash SolidFire .

Il servizio di raccolta Active IQ inoltra i dati di configurazione e le metriche delle prestazioni del cluster basate sul software Element a SolidFire Active IQ per la creazione di report storici e il monitoraggio delle prestazioni quasi in tempo reale. Il servizio di monitoraggio NetApp consente l'inoltro degli 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 Element 11.3 o versioni successive per funzionare correttamente. Per verificare di essere in grado di utilizzare tutte le funzioni di Active IQ , NetApp consiglia quanto segue:
 - Il cluster di archiviazione esegue il software NetApp Element 11.3 o versione successiva.
 - Hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.
- Hai accesso a Internet. Il servizio di raccolta Active IQ non può essere utilizzato da siti oscuri privi di connettività esterna.

Passi

1. Ottieni l'ID risorsa di base per l'installazione:

a. Aprire l'interfaccia utente dell'API REST del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

b. Seleziona **Autorizza** e completa quanto segue:

- i. Immettere il nome utente e la password del cluster.
- ii. Inserisci l'ID cliente come `mnode-client` .
- iii. Selezionare **Autorizza** per iniziare una sessione.
- iv. Chiudi la finestra.

c. Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.

- d. Seleziona **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 presenta una configurazione di risorse di base creata durante l'installazione o l'aggiornamento.

2. Attiva la telemetria:

- a. Accedi all'interfaccia utente dell'API del servizio mnode sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode` :

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

- b. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:

- i. Immettere il nome utente e la password del cluster.
- ii. Inserisci l'ID cliente come `mnode-client` .
- iii. Selezionare **Autorizza** per iniziare una sessione.
- iv. Chiudi la finestra.

- c. Configura la risorsa di base:

- i. Selezionare **PUT /assets/{asset_id}**.
- ii. Seleziona **Provalo**.
- iii. Inserire quanto segue nel payload JSON:

```
{
  "telemetry_active": true
  "config": {}
}
```

iv. Inserire l'ID base del passaggio precedente in **asset_ID**.

v. Selezionare **Esegui**.

Il servizio Active IQ viene riavviato automaticamente ogni volta che vengono modificate le risorse. La modifica delle risorse comporta un breve ritardo prima che le impostazioni vengano applicate.

3. Se non lo hai già fatto, aggiungi una risorsa del controller vCenter per NetApp Hybrid Cloud Control alle risorse note del nodo di gestione:



Per i servizi di monitoraggio NetApp è necessaria una risorsa controller.

- a. Selezionare **POST /assets/{asset_id}/controllers** per aggiungere una sotto-risorsa del controller.
- b. Seleziona **Provalo**.
- c. Inserisci l'ID della risorsa di base padre che hai copiato negli appunti nel campo **asset_id**.
- d. Inserire i valori di carico utile richiesti con `type` COME `vCenter` e credenziali vCenter.

```
{
  "username": "string",
  "password": "string",
  "ip": "string",
  "type": "vCenter",
  "host_name": "string",
  "config": {}
}
```



``ip`` è l'indirizzo IP di vCenter.

e. Selezionare **Esegui**.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Configurare NetApp Hybrid Cloud Control per più vCenter

È possibile configurare NetApp Hybrid Cloud Control per gestire le risorse da due o più vCenter che non utilizzano la modalità collegata.

Dovresti utilizzare questo processo dopo l'installazione iniziale quando devi aggiungere risorse per un'installazione ridimensionata di recente o quando nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente alla tua installazione.

Cosa ti servirà

- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Passi

1. ["Aggiungere nuovi vCenter come risorse del controller"](#) alla configurazione del nodo di gestione.
2. Aggiorna l'API del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```



In alternativa, puoi attendere 2 minuti affinché l'inventario venga aggiornato nell'interfaccia utente NetApp Hybrid Cloud Control.

- a. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client`.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudi la finestra.
 - b. Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.
 - c. Seleziona **Provalo**.
 - d. Selezionare **Esegui**.
 - e. Dalla risposta, copia l'ID della risorsa di installazione ("`id`").
 - f. Dall'interfaccia utente dell'API REST, seleziona **GET /installations/{id}**.
 - g. Seleziona **Provalo**.
 - h. Imposta l'aggiornamento su `True`.
 - i. Incolla l'ID della risorsa di installazione nel campo `id`.
 - j. Selezionare **Esegui**.
3. Aggiorna il browser NetApp Hybrid Cloud Control per visualizzare le modifiche.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del 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 dell'API REST.

Potrebbe essere necessario aggiungere una risorsa se di recente hai ridimensionato l'installazione e le nuove risorse non sono state aggiunte automaticamente alla configurazione. Utilizza queste API per aggiungere risorse aggiunte di recente alla tua installazione.

Cosa ti servirà

- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

- Hai creato un nuovo ruolo NetApp HCC in vCenter per limitare la visualizzazione dei servizi del nodo di gestione alle sole risorse NetApp. Vedere ["Creare un ruolo NetApp HCC in vCenter"](#)

Passi

1. Ottieni l'ID risorsa di base per l'installazione:

a. Aprire l'interfaccia utente dell'API REST del servizio di inventario sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

b. Seleziona **Autorizza** e completa quanto segue:

- i. Immettere il nome utente e la password del cluster.
- ii. Inserisci l'ID cliente come `mnode-client`.
- iii. Selezionare **Autorizza** per iniziare una sessione.
- iv. Chiudi la finestra.

c. Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.

d. Seleziona **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 presenta una configurazione di risorse di base creata durante l'installazione o l'aggiornamento.

g. Dall'interfaccia utente dell'API REST, seleziona **GET /installations/{id}**.

h. Seleziona **Provalo**.

i. Incolla l'ID della risorsa di installazione nel campo `id`.

j. Selezionare **Esegui**.

k. Dalla risposta, copia e salva l'ID del controller del cluster(`"controllerId"`) per utilizzarlo in una fase successiva.

2. Per aggiungere una sotto-risorsa 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. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client`.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudi la finestra.
- c. Selezionare **POST /assets/{asset_id}/controllers**.
- d. Seleziona **Provalo**.
- e. Immettere l'ID della risorsa di base padre nel campo **asset_id**.
- f. Aggiungere i valori richiesti al payload.
- g. Selezionare **Esegui**.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Creare e gestire risorse di cluster di archiviazione

È possibile aggiungere nuove risorse del cluster di archiviazione al nodo di gestione, modificare le credenziali archiviate per le risorse del cluster di archiviazione note ed eliminare le risorse del cluster di archiviazione dal nodo di gestione utilizzando l'API REST.

Cosa ti servirà

- Assicurati che la versione del cluster di storage esegua il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Opzioni di gestione delle risorse del cluster di archiviazione

Scegli una delle seguenti opzioni:

- [Recupera l'ID di installazione e l'ID cluster di una risorsa cluster di archiviazione](#)
- [Aggiungi una nuova risorsa cluster di archiviazione](#)
- [Modifica le credenziali archiviate per una risorsa del cluster di archiviazione](#)
- [Elimina una risorsa del cluster di archiviazione](#)

Recupera l'ID di installazione e l'ID cluster di una risorsa cluster di archiviazione

È possibile utilizzare l'API REST per ottenere l'ID di installazione e l'ID del cluster di archiviazione. Per aggiungere una nuova risorsa del cluster di archiviazione è necessario l'ID di installazione, mentre per modificare o eliminare una risorsa specifica del cluster di archiviazione è necessario l'ID del cluster.

Passi

1. Accedi all'interfaccia utente dell'API REST per il servizio di inventario immettendo l'indirizzo IP del nodo di gestione seguito da `/inventory/1/`:

```
https://<ManagementNodeIP>/inventory/1/
```

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Selezionare **GET /installations**.
4. Seleziona **Provalo**.
5. Selezionare **Esegui**.

L'API restituisce un elenco di tutte le installazioni note.

6. Dal corpo della risposta del codice 200, salvare il valore nel `id` campo, che puoi trovare nell'elenco delle installazioni. Questo è l'ID di installazione. Per 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. Accedi all'interfaccia utente dell'API REST per il servizio di archiviazione immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

8. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:

- a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
9. Selezionare **GET /clusters**.
 10. Seleziona **Provalo**.
 11. Inserisci l'ID di installazione salvato in precedenza nel `installationId` parametro.
 12. Selezionare **Esegui**.

L'API restituisce un elenco di tutti i cluster di archiviazione noti in questa installazione.

13. Dal corpo della risposta del codice 200, trova il cluster di archiviazione corretto e salva il valore nel `cluster storageId` campo. Questo è l'ID del cluster di archiviazione.

Aggiungi una nuova risorsa cluster di archiviazione

È possibile utilizzare l'API REST per aggiungere una o più nuove risorse del cluster di archiviazione all'inventario del nodo di gestione. Quando si aggiunge una nuova risorsa del cluster di archiviazione, questa viene automaticamente registrata nel nodo di gestione.

Cosa ti servirà

- Hai copiato il [ID cluster di archiviazione e ID di installazione](#) per tutti i cluster di archiviazione che desideri aggiungere.
- Se si aggiunge più di un nodo di archiviazione, è necessario aver letto e compreso le limitazioni del "[Cluster autorevole](#)" e supporto di più cluster di storage.



Tutti gli utenti definiti sul cluster autorevole vengono definiti come utenti su tutti gli altri cluster collegati all'istanza NetApp Hybrid Cloud Control.

Passi

1. Accedi all'interfaccia utente dell'API REST per il servizio di archiviazione immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Selezionare **POST /clusters**.
4. Seleziona **Provalo**.
5. Immettere le informazioni del nuovo cluster di archiviazione nei seguenti parametri nel campo **Corpo della richiesta**:

```
{
  "installationId": "a1b2c34d-e56f-1a2b-c123-1ab2cd345d6e",
  "mvip": "10.0.0.1",
  "password": "admin",
  "userId": "admin"
}
```

Parametro	Tipo	Descrizione
installationId	corda	L'installazione in cui aggiungere il nuovo cluster di archiviazione. Inserisci in questo parametro l'ID di installazione salvato in precedenza.
mvip	corda	Indirizzo IP virtuale di gestione IPv4 (MVIP) del cluster di storage.
password	corda	Password utilizzata per comunicare con il cluster di archiviazione.
userId	corda	ID utente utilizzato per comunicare con il cluster di archiviazione (l'utente deve disporre di privilegi di amministratore).

6. Selezionare **Esegui**.

L'API restituisce un oggetto contenente informazioni sulla risorsa del cluster di archiviazione appena aggiunta, ad esempio nome, versione e indirizzo IP.

Modifica le credenziali archiviate per una risorsa del cluster di archiviazione

È possibile modificare le credenziali archiviate che il nodo di gestione utilizza per accedere a un cluster di archiviazione. L'utente scelto deve avere accesso come amministratore del cluster.



Assicurati di aver seguito i passaggi in [Recupera l'ID di installazione e l'ID cluster di una risorsa cluster di archiviazione](#) prima di continuare.

Passi

1. Accedi all'interfaccia utente dell'API REST per il servizio di archiviazione immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.

- b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Selezionare **PUT /clusters/{storageId}**.
 4. Seleziona **Provalo**.
 5. Incolla l'ID del cluster di archiviazione copiato in precedenza nel `storageId` parametro.
 6. Modificare uno o entrambi i seguenti parametri nel campo **Corpo della richiesta**:

```
{
  "password": "adminadmin",
  "userId": "admin"
}
```

Parametro	Tipo	Descrizione
password	corda	Password utilizzata per comunicare con il cluster di archiviazione.
userId	corda	ID utente utilizzato per comunicare con il cluster di archiviazione (l'utente deve disporre di privilegi di amministratore).

7. Selezionare **Esegui**.

Elimina una risorsa del cluster di archiviazione

È possibile eliminare una risorsa del cluster di archiviazione se il cluster di archiviazione non è più in servizio. Quando si rimuove una risorsa del cluster di archiviazione, la sua registrazione dal nodo di gestione viene automaticamente annullata.



Assicurati di aver seguito i passaggi in [Recupera l'ID di installazione e l'ID cluster di una risorsa cluster di archiviazione](#) prima di continuare.

Passi

1. Accedi all'interfaccia utente dell'API REST per il servizio di archiviazione immettendo l'indirizzo IP del nodo di gestione seguito da `/storage/1/`:

```
https://<ManagementNodeIP>/storage/1/
```

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.

- c. Selezionare **Autorizza** per iniziare una sessione.
- d. Chiudi la finestra.
3. Selezionare **ELIMINA** /clusters/{storageId}.
4. Seleziona **Provalo**.
5. Inserisci l'ID del cluster di archiviazione copiato in precedenza nel `storageId` parametro.
6. Selezionare **Esegui**.

In caso di successo, l'API restituisce una risposta vuota.

Trova maggiori informazioni

- ["Cluster autorevole"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Visualizza o modifica le risorse del 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 VMware vCenter registrate sul nodo di gestione per l'installazione di NetApp SolidFire .

Prima di iniziare

- Assicurati che la versione del tuo cluster esegua il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Accedi all'API REST dei servizi di gestione

Passi

1. Accedi all'interfaccia utente dell'API REST per i servizi di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/vcenter/1/` :

```
https://<ManagementNodeIP>/vcenter/1/
```

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client` .
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.

Visualizza le informazioni memorizzate sui controller esistenti

È possibile elencare i controller vCenter esistenti registrati nel nodo di gestione e visualizzare le informazioni archiviate su di essi utilizzando l'API REST.

Passi

1. Selezionare **GET /compute/controllers**.
2. Seleziona **Provalo**.
3. Selezionare **Esegui**.

L'API restituisce un elenco di tutti i controller vCenter noti, 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 conoscere lo stato di connessione di un particolare controller, copiare l'ID del controller da `id` campo di quel controller negli appunti e vedere [Visualizza lo stato di un controller esistente](#).

Visualizza lo stato di un controller esistente

È possibile visualizzare lo stato di tutti i controller vCenter esistenti registrati nel nodo di gestione. L'API restituisce uno stato che indica se NetApp Hybrid Cloud Control può connettersi al controller vCenter, nonché il motivo di tale stato.

Passi

1. Selezionare **GET /compute/controllers/{controller_id}/status**.
2. Seleziona **Provalo**.
3. Inserisci l'ID del controller copiato in precedenza nel `controller_id` parametro.
4. Selezionare **Esegui**.

L'API restituisce lo stato di questo specifico controller vCenter, insieme al motivo di tale stato.

Modifica le proprietà memorizzate di un controller

È possibile modificare il nome utente o la password memorizzati per uno qualsiasi dei controller vCenter esistenti registrati con il nodo di gestione. Non è possibile modificare l'indirizzo IP memorizzato di un controller vCenter esistente.

Passi

1. Selezionare **PUT /compute/controllers/{controller_id}**.
2. Immettere l'ID del controller di un controller vCenter nel `controller_id` parametro.
3. Seleziona **Provalo**.
4. Modificare uno dei seguenti parametri nel campo **Corpo della richiesta**:

Parametro	Tipo	Descrizione
<code>userId</code>	corda	Modificare l'ID utente utilizzato per comunicare con il controller vCenter (l'utente deve disporre di privilegi di amministratore).
<code>password</code>	corda	Modificare la password utilizzata per comunicare con il controller vCenter.

5. Selezionare **Esegui**.

L'API restituisce informazioni aggiornate sul controller.

Trova maggiori informazioni

- ["Aggiungere una risorsa controller al nodo di gestione"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del 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 raggiungere una rete pubblica.

Un server proxy viene utilizzato per i collettori di telemetria e le connessioni tunnel inverse. È possibile abilitare e configurare un server proxy tramite l'interfaccia utente dell'API REST se non è stato già configurato un server proxy durante l'installazione o l'aggiornamento. È anche possibile modificare le impostazioni del server proxy esistente o disabilitare un server proxy.

Il comando per configurare un server proxy aggiorna 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 utilità software Element installate sul nodo di gestione, incluso il tunnel di supporto inverso per il supporto NetApp .

Prima di iniziare

- Dovresti conoscere le informazioni sull'host e sulle credenziali del server proxy che stai configurando.
- Assicurati che la versione del tuo cluster esegua il software NetApp Element 11.3 o versione successiva.
- Assicurarsi di aver distribuito un nodo di gestione che esegue la 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.

Passi

1. Accedi all'interfaccia utente dell'API REST sul nodo di gestione immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode` :

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

2. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client` .
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Selezionare **METTI /impostazioni**.
4. Seleziona **Provalo**.
5. Per abilitare un server proxy, è necessario impostare `use_proxy` al vero. Immettere l'IP o il nome host e le destinazioni della porta proxy.

Il nome utente proxy, la password proxy e la porta SSH sono facoltativi 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**.



A seconda dell'ambiente, potrebbe essere necessario riavviare il nodo di gestione.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Verificare le versioni del sistema operativo e dei servizi del nodo di gestione

È possibile verificare i numeri di versione del sistema operativo del nodo di gestione, del bundle dei servizi di gestione e dei singoli servizi in esecuzione sul nodo di gestione utilizzando l'API REST nel nodo di gestione.

Cosa ti servirà

- Il tuo cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Opzioni

- [Comandi API](#)
- [Passaggi dell'interfaccia utente dell'API REST](#)

Comandi API

- Ottieni informazioni sulla versione del sistema operativo del nodo di gestione, del bundle dei 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"
```

- Ottieni 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 del ricciolo.

Passaggi dell'interfaccia utente dell'API REST

1. Accedi all'interfaccia utente dell'API REST per il servizio immettendo l'indirizzo IP del nodo di gestione seguito da `/mnode/` :

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

2. Eseguire una delle seguenti operazioni:

- Ottieni informazioni sulla versione del sistema operativo del nodo di gestione, del bundle dei servizi di gestione e del servizio API del nodo di gestione (`mnode-api`) in esecuzione sul nodo di gestione:
 - i. Selezionare **OTTIENI /informazioni**.
 - ii. Seleziona **Provalo**.
 - iii. Selezionare **Esegui**.

La versione del pacchetto di servizi di gestione(`"mnode_bundle_version"`), versione del sistema operativo del nodo di gestione(`"os_version"`) e versione API del nodo di gestione(`"version"`) sono indicati nel corpo della risposta.

- Ottieni informazioni sulla versione dei singoli servizi in esecuzione sul nodo di gestione:
 - i. Selezionare **OTTIENI /servizi**.
 - ii. Seleziona **Provalo**.
 - iii. Selezionare lo stato come **In esecuzione**.
 - iv. Selezionare **Esegui**.

I servizi in esecuzione sul nodo di gestione sono indicati nel corpo della risposta.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Ottenere i 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 oppure specificare servizi specifici e utilizzare parametri di query per definire meglio i risultati restituiti.

Cosa ti servirà

- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

Passi

1. Aprire l'interfaccia utente dell'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. Seleziona **Autorizza** o qualsiasi icona a forma di lucchetto e completa quanto segue:

- Immettere il nome utente e la password del cluster.
- Se il valore non è già compilato, immettere l'ID client come mnode-client.
- Selezionare **Autorizza** per iniziare una sessione.
- Chiudi la finestra.

3. Selezionare **GET /logs**.

4. Seleziona **Provalo**.

5. Specificare i seguenti parametri:

- **Lines**: Inserisci il numero di righe che desideri vengano restituite dal registro. Questo parametro è un numero intero il cui valore predefinito è 1000.



Per evitare di richiedere l'intera cronologia del contenuto del registro, impostando Lines su 0.

- **since**: Aggiunge un timestamp ISO-8601 per il punto di partenza dei registri di servizio.



Utilizzare un ragionevole **since** parametro quando si raccolgono log di intervalli di tempo più ampi.

- **service-name**: Inserisci un nome di servizio.



Utilizzare il **GET /services** comando per elencare i servizi sul nodo di gestione.

- **stopped**: Impostato su **true** per recuperare i log dai servizi interrotti.

6. Selezionare **Esegui**.

7. Dal corpo della risposta, seleziona **Scarica** per salvare l'output del registro.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Gestisci le connessioni di supporto

Accesso ai nodi di archiviazione tramite SSH per la risoluzione dei problemi di base

A partire da Element 12.5, è possibile utilizzare l'account di sistema sfreadonly sui nodi di archiviazione per la risoluzione dei problemi di base. È anche possibile abilitare e aprire l'accesso al tunnel di supporto remoto per il supporto NetApp per la risoluzione avanzata dei problemi.

L'account di sistema sfreadonly consente l'accesso per eseguire comandi di base per la risoluzione dei problemi di rete e del sistema Linux, inclusi ping .



Salvo diversa indicazione da parte del supporto NetApp , qualsiasi modifica apportata a questo sistema non è supportata, invalidando il contratto di supporto e potrebbe causare instabilità o inaccessibilità dei dati.

Prima di iniziare

- **Autorizzazioni di scrittura:** verifica di disporre delle autorizzazioni di scrittura per la directory di lavoro corrente.
- **(Facoltativo) Genera la tua coppia di chiavi:** Esegui `ssh-keygen` dalla distribuzione Windows 10, MacOS o Linux. Si tratta di un'azione una tantum per creare una coppia di chiavi utente e può essere riutilizzata per future sessioni di risoluzione dei problemi. Potresti voler utilizzare certificati associati agli account dei dipendenti, che funzionerebbero anche in questo modello.
- **Abilita la funzionalità SSH sul nodo di gestione:** per abilitare la funzionalità di accesso remoto sulla modalità di gestione, vedere ["questo argomento"](#) . Per i servizi di gestione 2.18 e versioni successive, la funzionalità di accesso remoto è disabilitata per impostazione predefinita sul nodo di gestione.
- **Abilita la funzionalità SSH sul cluster di archiviazione:** per abilitare la funzionalità di accesso remoto sui nodi del cluster di archiviazione, vedere ["questo argomento"](#) .
- **Configurazione del firewall:** se il nodo di gestione si trova dietro un server proxy, nel file `sshd.config` sono richieste le seguenti porte TCP:

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

Opzioni di risoluzione dei problemi

- [Risolvere i problemi di un nodo del cluster](#)
- [Risolvi i problemi di un nodo del cluster con il supporto NetApp](#)
- [Risolvi i problemi di un nodo che non fa parte del cluster](#)

Risolvere i problemi di un nodo del cluster

È possibile eseguire la risoluzione dei problemi di base utilizzando l'account di sistema sfreadonly:

Passi

1. Accedi tramite SSH al nodo di gestione utilizzando le credenziali di accesso all'account selezionate durante l'installazione della VM del nodo di gestione.
2. Sul nodo di gestione, vai a `/sf/bin`.
3. Trova lo script appropriato per il tuo sistema:
 - SignSshKeys.ps1
 - SignSshKeys.py
 - SignSshKeys.sh



SignSshKeys.ps1 dipende da PowerShell 7 o versione successiva e SignSshKeys.py dipende da Python 3.6.0 o versione successiva e ["modulo richieste"](#).

IL SignSshKeys sceneggiatori `user`, `user.pub`, E `user-cert.pub` file nella directory di lavoro corrente, che vengono poi utilizzati dal `ssh` comando. Tuttavia, quando un file di chiave pubblica viene fornito allo script, solo un `<public_key>` file (con `<public_key>` sostituito con il prefisso del file della chiave pubblica passato nello script) viene scritto nella directory.

4. Eseguire lo script sul nodo di gestione per generare il portachiavi SSH. Lo script abilita l'accesso SSH utilizzando l'account di sistema sfreadonly su tutti i nodi del cluster.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--publickey [public key path]
```

- a. Sostituisci il valore tra parentesi quadre [] (incluse le parentesi) per ciascuno dei seguenti parametri:



È possibile utilizzare il parametro in forma abbreviata o completa.

- **--ip | -i [indirizzo IP]**: indirizzo IP del nodo di destinazione su cui eseguire l'API.
 - **--user | -u [nome utente]**: Utente del cluster utilizzato per eseguire la chiamata API.
 - **(Facoltativo) --duration | -d [ore]**: durata della validità di una chiave firmata espressa come numero intero in ore. L'impostazione predefinita è 24 ore.
 - **(Facoltativo) --publickey | -k [percorso chiave pubblica]**: il percorso di una chiave pubblica, se l'utente sceglie di fornirne una.
- b. Confronta il tuo input con il seguente comando di esempio. In questo esempio, 10.116.139.195 è l'IP del nodo di archiviazione, `admin` è il nome utente del cluster e la durata di validità della chiave è di due ore:

```
sh /sf/bin/SignSshKeys.sh --ip 10.116.139.195 --user admin --duration
2
```

c. Esegui il comando.

5. SSH agli IP dei nodi:

```
ssh -i user sfreadonly@[node_ip]
```

Sarai in grado di eseguire comandi di base per la risoluzione dei problemi di rete e del sistema Linux, come `ping` e altri comandi di sola lettura.

6. (Facoltativo) Disabilita **"funzionalità di accesso remoto"** di nuovo dopo aver completato la risoluzione dei problemi.



Se non lo si disabilita, SSH rimane abilitato sul nodo di gestione. La configurazione abilitata per SSH persiste sul nodo di gestione attraverso aggiornamenti e upgrade finché non viene disabilitata manualmente.

Risolvi i problemi di un nodo del cluster con il supporto NetApp

Il supporto NetApp può eseguire una risoluzione avanzata dei problemi con un account di sistema che consente a un tecnico di eseguire una diagnostica Element più approfondita.

Passi

1. Accedi tramite SSH al nodo di gestione utilizzando le credenziali di accesso all'account selezionate durante l'installazione della VM del nodo di gestione.
2. Esegui il primo comando con il numero di porta inviato dal supporto NetApp per aprire il tunnel di supporto:

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

Il supporto NetApp accederà al tuo nodo di gestione tramite il tunnel di supporto.

3. Sul nodo di gestione, vai a `/sf/bin`.
4. Trova lo script appropriato per il tuo sistema:
 - `SignSshKeys.ps1`
 - `SignSshKeys.py`
 - `SignSshKeys.sh`



`SignSshKeys.ps1` dipende da PowerShell 7 o versione successiva e `SignSshKeys.py` dipende da Python 3.6.0 o versione successiva e **"modulo richieste"**.

IL `SignSshKeys` sceneggiatori `user`, `user.pub`, E `user-cert.pub` file nella directory di lavoro corrente, che vengono poi utilizzati dal `ssh` comando. Tuttavia, quando un file di chiave pubblica viene fornito allo script, solo un `<public_key>` file (con `<public_key>` sostituito con il prefisso del file della chiave pubblica passato nello script) viene scritto nella directory.

5. Esegui lo script per generare il portachiavi SSH con `--sfadmin` bandiera. Lo script abilita SSH su tutti i nodi.

```
SignSshKeys --ip [ip address] --user [username] --duration [hours]
--sfadmin
```

Per SSH come `--sfadmin` a un nodo in cluster, è necessario generare il portachiavi SSH utilizzando un `--user` con `supportAdmin` accesso al cluster.

Per configurare `supportAdmin` Per accedere agli account degli amministratori del cluster, è possibile utilizzare l'interfaccia utente Element o le API:



- "Configurare l'accesso "supportAdmin" utilizzando l'interfaccia utente Element"
- Configurare `supportAdmin` accesso tramite API e aggiunta "supportAdmin" come il "access" digita la richiesta API:
 - "Configurare l'accesso "supportAdmin" per un nuovo account"
 - "Configurare l'accesso "supportAdmin" per un account esistente"

Per ottenere il `clusterAdminID` , puoi usare il "ListClusterAdmins" API.

Per aggiungere `supportAdmin` per accedere, è necessario disporre dei privilegi di amministratore del cluster o di amministratore.

- a. Sostituisci il valore tra parentesi quadre [] (incluse le parentesi) per ciascuno dei seguenti parametri:



È possibile utilizzare il parametro in forma abbreviata o completa.

- `--ip` | `-i` [indirizzo IP]: indirizzo IP del nodo di destinazione su cui eseguire l'API.
- `--user` | `-u` [nome utente]: Utente del cluster utilizzato per eseguire la chiamata API.
- (Facoltativo) `--duration` | `-d` [ore]: durata della validità di una chiave firmata espressa come numero intero in ore. L'impostazione predefinita è 24 ore.

- b. Confronta il tuo input con il seguente comando di esempio. In questo esempio, `192.168.0.1` è l'IP del nodo di archiviazione, `admin` è il nome utente del cluster, la durata della validità della chiave è di due ore e `--sfadmin` consente l'accesso al nodo di supporto NetApp per la risoluzione dei problemi:

```
sh /sf/bin/SignSshKeys.sh --ip 192.168.0.1 --user admin --duration 2
--sfadmin
```

- c. Esegui il comando.

6. SSH agli IP dei nodi:

```
ssh -i user sfadmin@[node_ip]
```

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

```
rst --killall
```

8. (Facoltativo) Disabilita ["funzionalità di accesso remoto"](#) di nuovo dopo aver completato la risoluzione dei problemi.



Se non lo si disabilita, SSH rimane abilitato sul nodo di gestione. La configurazione abilitata per SSH persiste sul nodo di gestione attraverso aggiornamenti e upgrade finché non viene disabilitata manualmente.

Risolvi i problemi di un nodo che non fa parte del cluster

È possibile eseguire la risoluzione dei problemi di base di un nodo che non è ancora stato aggiunto a un cluster. A questo scopo è possibile utilizzare l'account di sistema sfreadonly con o senza l'aiuto del supporto NetApp . Se hai configurato un nodo di gestione, puoi utilizzarlo per SSH ed eseguire lo script fornito per questa attività.

1. Da un computer Windows, Linux o Mac su cui è installato un client SSH, eseguire lo script appropriato per il sistema fornito dal supporto NetApp .
2. SSH all'IP del nodo:

```
ssh -i user sfreadonly@[node_ip]
```

3. (Facoltativo) Disabilita ["funzionalità di accesso remoto"](#) di nuovo dopo aver completato la risoluzione dei problemi.



Se non lo si disabilita, SSH rimane abilitato sul nodo di gestione. La configurazione abilitata per SSH persiste sul nodo di gestione attraverso aggiornamenti e upgrade finché non viene disabilitata manualmente.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione NetApp HCI"](#)

Avvia una sessione di supporto NetApp remota

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

È possibile aprire una porta TCP per una connessione tunnel inversa SSH con il supporto NetApp . 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 disabilitata per impostazione predefinita sul nodo di gestione. Per abilitare 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 richieste le seguenti porte TCP:

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

Passi

- Accedi al tuo nodo di gestione e apri una sessione terminale.
- Al prompt, 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) Disabilita ["funzionalità di accesso remoto"](#) Ancora.



Se non lo si disabilita, SSH rimane abilitato sul nodo di gestione. La configurazione abilitata per SSH persiste sul nodo di gestione attraverso aggiornamenti e upgrade finché non viene disabilitata manualmente.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del 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. Capacità SSH che fornisce ["Accesso alla sessione del tunnel di supporto remoto \(RST\) del supporto NetApp"](#) è disabilitato 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 abilitare e disabilitare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di controllo NetApp Hybrid Cloud.

Cosa ti servirà

- *** Autorizzazioni NetApp Hybrid Cloud Control***: hai le autorizzazioni di amministratore.
- **Autorizzazioni di amministratore del cluster**: disponi delle autorizzazioni di amministratore sul cluster di archiviazione.
- **Software Element**: il cluster esegue il software NetApp Element 11.3 o versione successiva.
- **Nodo di gestione**: hai distribuito un nodo di gestione che esegue la versione 11.3 o successiva.

- **Aggiornamenti sui servizi di gestione:**

- Per utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud, è necessario aggiornare "[pacchetto di servizi di gestione](#)" alla versione 2.20.69 o successiva.
- Per utilizzare l'interfaccia utente dell'API REST, è necessario aggiornare il proprio "[pacchetto di servizi di gestione](#)" alla versione 2.17.

Opzioni

- [Disabilitare o abilitare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di controllo NetApp Hybrid Cloud](#)

Dopo aver effettuato l'accesso, puoi eseguire una qualsiasi delle seguenti attività: "[autenticare](#)" :

- [Disabilitare o abilitare la funzionalità SSH sul nodo di gestione tramite API](#)
- [Determinare lo stato della capacità SSH sul nodo di gestione utilizzando le API](#)

Disabilitare o abilitare la funzionalità SSH sul nodo di gestione utilizzando l'interfaccia utente di controllo NetApp Hybrid Cloud

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Capacità SSH che fornisce "[Accesso alla sessione del tunnel di supporto remoto \(RST\) del supporto NetApp](#)" è disabilitato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disabilitazione di SSH non termina né disconnette le sessioni client SSH esistenti al nodo di gestione. Se si disabilita SSH e si sceglie di riabilitarlo in un secondo momento, è possibile farlo tramite l'interfaccia utente di controllo NetApp Hybrid Cloud.



Per abilitare o disabilitare l'accesso al supporto tramite SSH per un cluster di archiviazione, è necessario utilizzare "[Pagina delle impostazioni del cluster dell'interfaccia utente dell'elemento](#)".

Passi

1. Dalla Dashboard, seleziona il menu delle opzioni in alto a destra e seleziona **Configura**.
2. Nella schermata **Supporto accesso per nodo di gestione**, attiva l'interruttore per abilitare SSH del nodo di gestione.
3. Dopo aver completato la risoluzione dei problemi, nella schermata **Supporto accesso per nodo di gestione**, attiva l'interruttore per disabilitare SSH del nodo di gestione.

Disabilitare o abilitare la funzionalità SSH sul nodo di gestione tramite API

È possibile disattivare o riattivare la funzionalità SSH sul nodo di gestione. Capacità SSH che fornisce "[Accesso alla sessione del tunnel di supporto remoto \(RST\) del supporto NetApp](#)" è disabilitato per impostazione predefinita sui nodi di gestione che eseguono i servizi di gestione 2.18 o versioni successive. La disabilitazione di SSH non termina né disconnette le sessioni client SSH esistenti al nodo di gestione. Se disabiliti SSH e decidi di riabilitarlo in un secondo momento, puoi farlo utilizzando la stessa API.

comando API

Per i servizi di gestione 2.18 o successivi:

```
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 del ricciolo.

Passaggi dell'interfaccia utente dell'API REST

1. Accedi all'interfaccia utente dell'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. Seleziona **Autorizza** e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Dall'interfaccia utente dell'API REST, selezionare **PUT /settings/ssh**.
 - a. Seleziona **Provalo**.
 - b. Imposta il parametro **abilitato** su `false` per disabilitare SSH o `true` per riattivare la funzionalità SSH precedentemente disabilitata.
 - c. Selezionare **Esegui**.

Determinare lo stato della capacità SSH sul nodo di gestione utilizzando le API

È possibile determinare se la funzionalità SSH è abilitata o meno sul nodo di gestione utilizzando un'API del servizio del nodo di gestione. SSH è disabilitato per impostazione predefinita sui nodi di gestione che eseguono servizi di gestione versione 2.18 o successiva.

comando API

Per i servizi di gestione 2.18 o successivi:

```
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 del ricciolo..

Passaggi dell'interfaccia utente dell'API REST

1. Accedi all'interfaccia utente dell'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. Seleziona **Autorizza** e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client`.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Dall'interfaccia utente dell'API REST, seleziona **GET /settings/ssh**.
 - a. Seleziona **Provalo**.
 - b. Selezionare **Esegui**.

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Aggiorna il tuo sistema di archiviazione all-flash NetApp SolidFire

Panoramica della sequenza di aggiornamento

È possibile mantenere aggiornato il sistema di archiviazione SolidFire Element dopo l'implementazione aggiornando in sequenza tutti i componenti di archiviazione NetApp .

Questi componenti includono servizi di gestione, NetApp Hybrid Cloud Control, software Element, nodo di gestione e (a seconda dell'installazione) Element Plug-in per vCenter Server.

- A partire da novembre 2023, non sarà più possibile avviare l'aggiornamento di un componente tramite NetApp Hybrid Cloud Control o REST API, poiché i certificati delle chiavi di firma (privati e pubblici) sono scaduti il 5 novembre 2023. Puoi aggirare questo problema ["esecuzione di un aggiornamento sul posto del nodo di gestione"](#) alla versione 12.8 prima di utilizzare NetApp Hybrid Cloud Control o REST API per aggiornare i servizi di gestione, il software Element e il firmware di storage.

Se si sta distribuendo un nuovo nodo di gestione con la versione 12.8, è possibile utilizzare NetApp Hybrid Cloud Control o REST API per eseguire gli aggiornamenti dei componenti nell'ordine elencato in [sequenza di aggiornamento del sistema](#) .



- I seguenti nodi non sono supportati. Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x:
 - A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
 - A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608 e nodi FC FC0025 e SF-FCN-01.
- A partire da Element 12.5, NetApp HealthTools non è più supportato per gli aggiornamenti software di Element. Se stai utilizzando Element 11.0 o 11.1, devi prima ["aggiorna a Element 12.3 utilizzando HealthTools"](#) e poi eseguire l'aggiornamento a Element 12.5 o versione successiva utilizzando NetApp Hybrid Cloud Control.

IL [sequenza di aggiornamento del sistema](#) Il contenuto descrive le attività necessarie per completare un aggiornamento del sistema di archiviazione all-flash SolidFire . Idealmente, queste procedure vengono eseguite come parte di una sequenza di aggiornamento più ampia e non in modo isolato. Se è necessario un aggiornamento o un upgrade basato sui componenti, consultare i prerequisiti della procedura per garantire che vengano affrontate ulteriori complessità.

IL ["Sequenza di aggiornamento di vSphere"](#) incluso il contenuto Element Plug-in per vCenter Server descrive i passaggi aggiuntivi pre e post aggiornamento necessari per reinstallare Element Plug-in per vCenter Server.

Prima di iniziare

- Stai eseguendo il nodo di gestione 11.3 o versione successiva. Le versioni più recenti del nodo di gestione hanno un'architettura modulare che fornisce servizi individuali.



Per verificare la versione, accedi al tuo nodo di gestione e visualizza il numero di versione dell'elemento nel banner di accesso. Se non hai 11.3, vedi ["Aggiorna il tuo nodo di gestione"](#) .

- Hai aggiornato i tuoi servizi di gestione almeno alla versione 2.1.326.

Gli aggiornamenti tramite NetApp Hybrid Cloud Control non sono disponibili nelle versioni precedenti del pacchetto di servizi.

- Hai verificato che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di archiviazione e i nodi. Ogni nodo deve essere configurato con un nameserver DNS nell'interfaccia utente Web per nodo(`https://[IP address]:442`) senza errori di cluster irrisolti correlati allo sfasamento temporale.
- Hai programmato tempo sufficiente per il tuo **"Software Element"** E **"firmware di archiviazione"** aggiornamenti. Quando si esegue l'aggiornamento al software Element 12.5 o versione successiva, il tempo necessario per l'aggiornamento varia a seconda della versione del software Element e degli aggiornamenti del firmware.

Sequenza di aggiornamento del sistema

È possibile utilizzare la seguente sequenza per aggiornare il sistema di archiviazione all-flash NetApp SolidFire per Element 12.5 o versioni successive.

Passi

1. **"Eseguire controlli sullo stato di integrità dell'archiviazione Element prima di aggiornare l'archiviazione"**.
2. **"(Facoltativo) Aggiorna il tuo nodo di gestione"**.



Non è più necessario aggiornare il sistema operativo del nodo di gestione per aggiornare il software Element sul cluster di archiviazione. Se il nodo di gestione è versione 11.3 o successiva, è sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti di Element utilizzando NetApp Hybrid Cloud Control. Seguire la procedura di aggiornamento del nodo di gestione per il proprio scenario se è necessario aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio per correggere problemi di sicurezza.

3. **"Aggiorna i servizi di gestione da Hybrid Cloud Control"**.



- Il bundle dei servizi di gestione 2.27 include Element Plug-in per vCenter Server 5.5, compatibile solo con il nodo di gestione 12.8. Quando si esegue l'aggiornamento ai servizi di gestione 2.27, è necessario modificare la sequenza di aggiornamento e aggiornare il bundle dei servizi di gestione *dopo* l'aggiornamento a Element 12.8 per garantire la compatibilità tra il nodo di gestione e i servizi di gestione.

- Se si esegue l'aggiornamento ai servizi di gestione dalla versione 2.21.61 alla versione 2.26.40, è necessario aggiornare il bundle dei servizi di gestione *prima* di eseguire l'aggiornamento a Element 12.8.



Se si aggiornano i servizi di gestione alla versione 2.16 o successiva e si esegue un nodo di gestione dalla versione 11.3 alla 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione.

4. **"Aggiorna il software Element e il firmware di archiviazione"**.
5. **"(Facoltativo) Aggiorna solo il firmware dell'archiviazione Element"**.



È possibile eseguire questa attività quando diventa disponibile un nuovo aggiornamento del firmware di archiviazione al di fuori di una versione principale.

6. ["Aggiorna il tuo Element Plug-in per vCenter Server"](#).

Trova maggiori informazioni

- ["Plug-in NetApp Element per vCenter Server"](#)
- ["Documentazione del software SolidFire ed Element"](#)

Procedure di aggiornamento del sistema

Eseguire controlli di integrità dell'archiviazione Element prima di aggiornare l'archiviazione

È necessario eseguire controlli di integrità prima di aggiornare Element Storage per garantire che tutti i nodi di archiviazione nel cluster siano pronti per il successivo aggiornamento di Element Storage.

Cosa ti servirà

- **Servizi di gestione:** Hai effettuato l'aggiornamento all'ultimo pacchetto di servizi di gestione (2.10.27 o successivo).



Prima di aggiornare il software Element, è necessario effettuare l'aggiornamento al pacchetto di servizi di gestione più recente.

- **Nodo di gestione:** Stai eseguendo il nodo di gestione 11.3 o versione successiva.
- **Software Element:** la versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- **Contratto di licenza con l'utente finale (EULA):** a partire dalla versione 2.20.69 dei servizi di gestione, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API NetApp Hybrid Cloud Control per eseguire i controlli di integrità dello storage Element:
 - a. Aprire l'indirizzo IP del nodo di gestione in un browser web:

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

- b. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
- d. Viene visualizzato l'EULA. Scorri verso il basso, seleziona **Accetto per gli aggiornamenti attuali e futuri** e seleziona **Salva**.

Opzioni di controllo sanitario

È possibile eseguire controlli di integrità utilizzando l'interfaccia utente NetApp Hybrid Cloud Control o l'API di NetApp Hybrid Cloud Control:

- [Utilizzare NetApp Hybrid Cloud Control per eseguire controlli sullo stato di integrità dello storage Element prima di aggiornarlo](#)(Metodo preferito)

Puoi anche scoprire di più sui controlli di integrità dell'archiviazione eseguiti dal servizio:

- [Controlli di integrità dell'archiviazione effettuati dal servizio](#)

Utilizzare NetApp Hybrid Cloud Control per eseguire controlli sullo stato di integrità dello storage Element prima di aggiornarlo

Utilizzando NetApp Hybrid Cloud Control, è possibile verificare che un cluster di storage sia pronto per essere aggiornato.

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
4. Nella pagina **Aggiornamenti**, seleziona la scheda **Archiviazione**.
5.  Seleziona il controllo sanitario per il cluster di cui si desidera verificare la disponibilità all'aggiornamento.
6. Nella pagina **Controllo integrità storage**, seleziona **Esegui controllo integrità**.
7. In caso di problemi, procedere come segue:
 - a. Andare all'articolo specifico della Knowledge Base elencato per ciascun problema oppure eseguire la soluzione specificata.
 - b. Se viene specificata una KB, completare la procedura descritta nell'articolo della KB pertinente.
 - c. Dopo aver risolto i problemi del cluster, seleziona **Riesegui controllo integrità**.

Una volta completato il controllo dello stato senza errori, il cluster di archiviazione è pronto per l'aggiornamento. Vedi aggiornamento del nodo di archiviazione "[istruzioni](#)" per procedere.

Utilizzare l'API per eseguire controlli sullo stato di integrità dell'archiviazione Element prima di aggiornare l'archiviazione

È possibile utilizzare l'API REST per verificare che un cluster di archiviazione sia pronto per essere aggiornato. Il controllo dello stato di salute verifica che non vi siano ostacoli all'aggiornamento, come nodi in sospenso, problemi di spazio su disco ed errori del cluster.

Passi

1. Individuare l'ID del cluster di archiviazione:
 - a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

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

- b. Seleziona **Autorizza** e completa quanto segue:

- i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client` se il valore non è già compilato.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente dell'API REST, seleziona `GET /assets`.
 - d. Seleziona **Provalo**.
 - e. Selezionare **Esegui**.
 - f. Dalla risposta, copia il "id" dal "storage" sezione del cluster di cui si intende verificare la disponibilità all'aggiornamento.



Non usare il "parent" valore in questa sezione perché questo è l'ID del nodo di gestione, non l'ID del cluster di archiviazione.

```
"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 controlli di integrità sul cluster di archiviazione:

- a. Aprire l'interfaccia utente dell'API REST di archiviazione sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client` se il valore non è già compilato.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
- c. Selezionare **POST /health-checks**.
- d. Seleziona **Provalo**.
- e. Nel campo dei parametri, immettere l'ID del cluster di archiviazione ottenuto nel passaggio 1.


```
{
  "config": {},
  "storageId": "123a45b6-1a2b-12a3-1234-1a2b34c567d8"
}
```

- f. Selezionare **Esegui** per eseguire un controllo dello stato di integrità sul cluster di archiviazione specificato.

La risposta dovrebbe 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. Copia il `healthCheckId` questo fa parte della risposta.
3. Verificare i risultati dei controlli sanitari:
- a. Selezionare **GET /health-checks/{healthCheckId}**.
- b. Seleziona **Provalo**.
- c. Immettere l'ID del controllo sanitario nel campo del parametro.
- d. Selezionare **Esegui**.
- e. Scorrere fino alla fine del corpo della risposta.

Se tutti i controlli di integrità hanno esito positivo, il risultato sarà simile al seguente esempio:

```
"message": "All checks completed successfully.",
"percent": 100,
"timestamp": "2020-03-06T00:03:16.321621Z"
```

4. Se il message il ritorno indica che si sono verificati problemi riguardanti l'integrità del cluster, procedere come segue:
 - a. Seleziona **GET /health-checks/{healthCheckId}/log**
 - b. Seleziona **Provalo**.
 - c. Immettere l'ID del controllo sanitario nel campo del parametro.
 - d. Selezionare **Esegui**.
 - e. Esamina eventuali errori specifici e ottieni i link agli articoli della Knowledge Base associati.
 - f. Andare all'articolo specifico della Knowledge Base elencato per ciascun problema oppure eseguire la soluzione specificata.
 - g. Se viene specificata una KB, completare la procedura descritta nell'articolo della KB pertinente.
 - h. Dopo aver risolto i problemi del cluster, eseguire nuovamente **GET /health-checks /{healthCheckId}/log**.

Controlli di integrità dell'archiviazione effettuati dal servizio

I controlli sullo stato di integrità dell'archiviazione eseguono i seguenti controlli per cluster.

Controlla il nome	Nodo/Cluster	Descrizione
controlla_risultati_asincroni	Grappolo	Verifica che il numero di risultati asincroni nel database sia inferiore a una soglia.
controlla_errori_del_cluster	Grappolo	Verifica che non vi siano errori del cluster che bloccano l'aggiornamento (come definito nella sorgente dell'elemento).
controlla_velocità_di_caricamento	Nodo	Misura la velocità di caricamento tra il nodo di archiviazione e il nodo di gestione.
controllo_velocità_di_conneessione	Nodo	Verifica che i nodi siano connessi al nodo di gestione che fornisce i pacchetti di aggiornamento e stima la velocità di connessione.
controlla_nuclei	Nodo	Controlla i dump di crash del kernel e i file core sul nodo. Il controllo non riesce per eventuali arresti anomali verificatisi in un periodo di tempo recente (soglia 7 giorni).
controlla_spazio_disco_radice	Nodo	Verifica che il file system radice abbia spazio libero sufficiente per eseguire un aggiornamento.

Controlla il nome	Nodo/Cluster	Descrizione
check_var_log_disk_space	Nodo	Verifica che <code>/var/log</code> lo spazio libero soddisfa una certa soglia percentuale di spazio libero. In caso contrario, il controllo ruoterà ed eliminerà i registri più vecchi per rientrare nella soglia. Il controllo fallisce se non riesce a creare spazio libero sufficiente.
controlla_nodi_in_attesa	Grappolo	Verifica che non vi siano nodi in sospeso nel cluster.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiornare un nodo di gestione

È possibile aggiornare il nodo di gestione alla versione 12.5 o successiva dalla versione 12.3.x o successiva.

Per aggiornare il software Element sul cluster di storage non è più necessario aggiornare il sistema operativo del nodo di gestione. È sufficiente aggiornare i servizi di gestione alla versione più recente per eseguire gli aggiornamenti di Element utilizzando NetApp Hybrid Cloud Control. Seguire la procedura di aggiornamento del nodo di gestione per il proprio scenario se si desidera aggiornare il sistema operativo del nodo di gestione per altri motivi, ad esempio per correggere problemi di sicurezza.



Se hai bisogno di informazioni sull'aggiornamento dei nodi di gestione 12.2 o precedenti, consulta ["Documentazione sull'aggiornamento del nodo di gestione Element 12.3.x"](#).

Passaggio 1: aggiornare la versione hardware della VM su un nodo di gestione

Se si esegue un aggiornamento sul posto di un nodo di gestione esistente a Element 12.8, prima di eseguire l'aggiornamento è necessario assicurarsi che la versione hardware della VM sul nodo di gestione sia compatibile con ESXi 6.7 (versione hardware della VM 14) o successiva, a seconda dell'ambiente.

Passi

1. Accedi a vSphere Web Client come amministratore vCenter.
2. Dal menu vSphere Client, seleziona **VM e modelli**.
3. Fare clic con il pulsante destro del mouse sulla macchina virtuale (VM) e selezionare **Spegnimento > Arresta il sistema operativo guest**.

Attendere che la macchina virtuale sia spenta.
4. Fare clic con il pulsante destro del mouse sulla VM e selezionare **Compatibilità > Aggiorna compatibilità VM**.
5. Selezionare **Sì**.
6. Selezionare ESXi 6.7 o una versione successiva, a seconda della versione del proprio ambiente vSphere.

7. Selezionare **OK**.
8. Una volta completato l'aggiornamento, fare clic con il pulsante destro del mouse sulla VM e selezionare **Alimentazione > Accendi**.
9. Selezionare **vSphere Client Update** e verificare che la compatibilità della VM sia alla versione desiderata.

Passaggio 2: aggiornare un nodo di gestione a Element 12.5 o versione successiva

Scegli una delle seguenti opzioni di aggiornamento:

- [Aggiornare un nodo di gestione alla versione 12.5 o successiva dalla versione 12.3.x o successiva](#)
- [Riconfigurare l'autenticazione utilizzando l'API REST del nodo di gestione](#)

Seleziona questa opzione se hai aggiornato **sequenzialmente** (1) la versione dei servizi di gestione e (2) la versione di Element Storage e desideri **mantenere** il nodo di gestione esistente:



Se non si aggiornano in sequenza i servizi di gestione seguiti dall'archiviazione degli elementi, non sarà possibile riconfigurare la riautenticazione utilizzando questa procedura. Seguire invece la procedura di aggiornamento appropriata.

Aggiornare un nodo di gestione alla versione 12.5 o successiva dalla versione 12.3.x o successiva

È possibile eseguire un aggiornamento sul posto del nodo di gestione dalla versione 12.3.x o successiva alla versione 12.5 o successiva senza dover predisporre una nuova VM del nodo di gestione.



Il nodo di gestione Element 12.5 o successivo è un aggiornamento facoltativo. Non è necessario per le distribuzioni esistenti.

Prima di iniziare

- La RAM della VM del nodo di gestione è di 24 GB.
- Il nodo di gestione che intendi aggiornare è la versione 12.0 e utilizza la rete IPv4. La versione 12.5 o successiva del nodo di gestione non supporta IPv6.



Per verificare la versione del tuo nodo di gestione, accedi al tuo nodo di gestione e visualizza il numero di versione dell'elemento nel banner di accesso.

- Hai aggiornato il tuo pacchetto di servizi di gestione all'ultima versione utilizzando NetApp Hybrid Cloud Control. È possibile accedere a NetApp Hybrid Cloud Control dal seguente IP:
`https://<ManagementNodeIP>`
- Se si sta aggiornando il nodo di gestione alla versione 12.5 o successiva, per procedere è necessario disporre dei servizi di gestione 2.21.61 o successivi.
- Hai configurato un adattatore di rete aggiuntivo (se necessario) utilizzando le istruzioni per "[configurazione di una scheda di rete di archiviazione aggiuntiva](#)".



I volumi persistenti potrebbero richiedere una scheda di rete aggiuntiva se eth0 non può essere instradato verso SVIP. Configurare una nuova scheda di rete sulla rete di archiviazione iSCSI per consentire la configurazione di volumi persistenti.

- I nodi di archiviazione eseguono Element 12.3.x o versioni successive.

Passi

1. Accedere alla VM del nodo di gestione tramite SSH o accesso alla console.
2. Scarica il "nodo di gestione ISO" per il software Element dal sito di supporto NetApp alla VM 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 confrontando l'output con quanto disponibile sul sito di supporto NetApp 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 directory home 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 stai aggiornando, esegui il seguente comando per aggiornare la versione del sistema operativo del nodo di gestione. Dopo l'aggiornamento, lo script conserva tutti i file di configurazione necessari, come le impostazioni del proxy e del collettore Active IQ .

```
sudo /sf/rtfi/bin/sfrtfi_inplace  
file:///upgrade/casper/filesystem.squashfs sf_upgrade=1
```

Una volta completato il processo di aggiornamento, il nodo di gestione si riavvia con un nuovo sistema operativo.



Dopo aver eseguito il comando `sudo` descritto in questo passaggio, la sessione SSH viene terminata. Per un monitoraggio continuo è necessario l'accesso alla console. Se non è possibile accedere alla console durante l'aggiornamento, riprovare ad accedere tramite SSH e verificare la connettività dopo 15-30 minuti. Una volta effettuato l'accesso, puoi confermare la nuova versione del sistema operativo nel banner SSH che indica che l'aggiornamento è riuscito.

8. Sul nodo di gestione, eseguire il comando `redploy-mnode` script per conservare le impostazioni di configurazione dei servizi di gestione precedenti:



Lo script conserva la configurazione precedente dei servizi di gestione, inclusa la configurazione del servizio di raccolta Active IQ, dei controller (vCenter) o del proxy, a seconda delle impostazioni.

```
sudo /sf/packages/mnode/redploy-mnode -mu <mnode user>
```



Se in precedenza hai disabilitato la funzionalità SSH sul nodo di gestione, devi ["disabilitare nuovamente SSH"](#) sul nodo di gestione recuperato. Capacità SSH che fornisce ["Accesso alla sessione del tunnel di supporto remoto \(RST\) del supporto NetApp"](#) è abilitato sul nodo di gestione per impostazione predefinita.

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) i servizi di gestione e (2) l'archiviazione degli elementi. Se è stato seguito un ordine di aggiornamento diverso, consultare le procedure per gli aggiornamenti dei nodi di gestione in loco.

Prima di iniziare

- Hai aggiornato i tuoi servizi di gestione alla versione 2.20.69 o successiva.
- Il cluster di archiviazione esegue Element 12.3 o versione successiva.
- Hai aggiornato in sequenza i tuoi servizi di gestione, quindi hai aggiornato il tuo spazio di archiviazione Element. Non è possibile riconfigurare l'autenticazione utilizzando questa procedura a meno che non siano stati completati gli aggiornamenti nella sequenza descritta.

Passi

1. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

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

2. Seleziona **Autorizza** e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client` se il valore non è già compilato.
 - c. Selezionare **Autorizza** per iniziare una sessione.
3. Dall'interfaccia utente dell'API REST, selezionare **POST /services/reconfigure-auth**.
4. Seleziona **Provalo**.

5. Per il parametro **load_images**, seleziona `true`.

6. Selezionare **Esegui**.

Il corpo della risposta indica che la riconfigurazione è riuscita.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Servizi di gestione degli aggiornamenti

È possibile aggiornare i servizi di gestione all'ultima versione del bundle dopo aver installato il nodo di gestione 11.3 o versione successiva.

A partire dalla versione Element 11.3 del nodo di gestione, la progettazione del nodo di gestione è stata modificata in base a una nuova architettura modulare che fornisce servizi individuali. Questi servizi modulari forniscono funzionalità di gestione centralizzata ed estesa per un sistema di archiviazione 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.

Informazioni su questo compito

Il bundle dei servizi di gestione 2.27 include Element Plug-in per vCenter Server 5.5, compatibile solo con il nodo di gestione 12.8. Quando si esegue l'aggiornamento ai servizi di gestione 2.27, è necessario modificare la sequenza di aggiornamento e aggiornare il bundle dei servizi di gestione *dopo* l'aggiornamento a Element 12.8 per garantire la compatibilità tra il nodo di gestione e i servizi di gestione.

Se si esegue l'aggiornamento ai servizi di gestione dalla versione 2.21.61 alla versione 2.26.40, è necessario aggiornare il bundle dei servizi di gestione *prima* di eseguire l'aggiornamento a Element 12.8.



- I servizi di gestione 2.22.7 includono il plug-in Element 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 conformarsi alla direttiva VMware che rimuove il supporto per i plug-in locali. ["Saperne di più"](#).
- Per le note di rilascio più recenti sui servizi di gestione che descrivono i servizi principali, le nuove funzionalità, le correzioni di bug e le soluzioni alternative per ciascun pacchetto di servizi, vedere ["le note di rilascio dei servizi di gestione"](#)

Cosa ti servirà

A partire dalla versione 2.20.69 dei servizi di gestione, è necessario accettare e salvare il Contratto di licenza con l'utente finale (EULA) prima di utilizzare l'interfaccia utente o l'API 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. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.

3. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
4. Viene visualizzato l'EULA. Scorri verso il basso, seleziona **Accetto per gli aggiornamenti attuali e futuri** e seleziona **Salva**.

Opzioni di aggiornamento

È possibile aggiornare i servizi di gestione utilizzando l'interfaccia utente di controllo NetApp Hybrid Cloud o l'API REST del nodo di gestione:

- [Aggiorna i servizi di gestione utilizzando Hybrid Cloud Control](#)(Metodo consigliato)
- [Aggiorna i servizi di gestione utilizzando l'API del nodo di gestione](#)

Aggiorna i servizi di gestione utilizzando Hybrid Cloud Control

Puoi aggiornare i servizi di gestione NetApp utilizzando NetApp Hybrid Cloud Control.

I pacchetti di servizi di gestione forniscono funzionalità avanzate e correzioni all'installazione al di fuori delle versioni principali.

Prima di iniziare

- Stai eseguendo il nodo di gestione 11.3 o versione successiva.
- Se si stanno aggiornando i servizi di gestione alla versione 2.16 o successiva e si sta eseguendo un nodo di gestione dalla versione 11.3 alla 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
 - a. Spegnerne la VM del nodo di gestione.
 - b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB di RAM.
 - c. Accendere la VM del nodo di gestione.
- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai aggiornato i tuoi servizi di gestione 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 ogni versione del pacchetto di servizi, vedere ["Note sulla versione dei servizi di gestione"](#).

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
4. Nella pagina Aggiornamenti, seleziona la scheda **Servizi di gestione**.
5. Seguire le istruzioni sulla pagina per scaricare e salvare sul computer un pacchetto di aggiornamento dei servizi di gestione.
6. Seleziona **Sfoglia** per individuare il pacchetto salvato e caricarlo.

Dopo aver caricato il pacchetto, l'aggiornamento si avvia automaticamente.

Una volta avviato l'aggiornamento, potrai visualizzarne lo stato in questa pagina. Durante l'aggiornamento, potresti perdere la connessione con NetApp Hybrid Cloud Control e dover effettuare nuovamente l'accesso per visualizzare i risultati dell'aggiornamento.

Aggiorna i servizi di gestione utilizzando l'API del nodo di gestione

Gli utenti dovrebbero idealmente eseguire gli 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 sul nodo di gestione utilizzando l'API REST. È possibile eseguire ciascun comando dall'interfaccia utente dell'API REST per il nodo di gestione.

Prima di iniziare

- Hai distribuito un nodo di gestione software NetApp Element 11.3 o versione successiva.
- Se si stanno aggiornando i servizi di gestione alla versione 2.16 o successiva e si sta eseguendo un nodo di gestione dalla versione 11.3 alla 11.8, sarà necessario aumentare la RAM della VM del nodo di gestione prima di aggiornare i servizi di gestione:
 - a. Spegnerne la VM del nodo di gestione.
 - b. Modificare la RAM della VM del nodo di gestione da 12 GB a 24 GB di RAM.
 - c. Accendere la VM del nodo di gestione.
- La versione del cluster esegue il software NetApp Element 11.3 o versione successiva.
- Hai aggiornato i tuoi servizi di gestione 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 ogni versione del pacchetto di servizi, vedere ["Note sulla versione dei servizi di gestione"](#).

Passi

1. Aprire l'interfaccia utente dell'API REST sul nodo di gestione: <https://<ManagementNodeIP>/mnode>
2. Seleziona **Autorizza** e completa quanto segue:
 - a. Immettere il nome utente e la password del cluster.
 - b. Inserisci l'ID cliente come `mnode-client` se il valore non è già compilato.
 - c. Selezionare **Autorizza** per iniziare una sessione.
 - d. Chiudi la finestra.
3. Carica ed estrai il bundle di servizi sul nodo di gestione utilizzando questo comando: `PUT /services/upload`
4. Distribuire i servizi di gestione sul nodo di gestione: `PUT /services/deploy`
5. Monitora 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 maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiorna il software Element

Per aggiornare il software NetApp Element , è possibile utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud o l'API REST. Alcune operazioni vengono soppresse durante un aggiornamento del software Element, come l'aggiunta e la rimozione di nodi, l'aggiunta e la rimozione di unità e i comandi associati agli iniziatori, ai gruppi di accesso al volume e alle reti virtuali, tra gli altri.



Il bundle dei servizi di gestione 2.27 include Element Plug-in per vCenter Server 5.5, compatibile solo con il nodo di gestione 12.8. Quando si esegue l'aggiornamento ai servizi di gestione 2.27, è necessario modificare la sequenza di aggiornamento e aggiornare il bundle dei servizi di gestione *dopo* l'aggiornamento a Element 12.8 per garantire la compatibilità tra il nodo di gestione e i servizi di gestione.

Se si esegue l'aggiornamento ai servizi di gestione dalla versione 2.21.61 alla versione 2.26.40, è necessario aggiornare il bundle dei servizi di gestione *prima* di eseguire l'aggiornamento a Element 12.8.

Prima di iniziare

- **Privilegi di amministratore:** disponi delle autorizzazioni di amministratore del cluster di archiviazione per eseguire l'aggiornamento.
- **Percorso di aggiornamento valido:** hai controllato le informazioni sul percorso di aggiornamento per la versione di Element a cui stai effettuando l'aggiornamento e hai verificato che 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\[\"NetApp KB: matrice di aggiornamento per cluster di storage che eseguono NetApp Element Software\"\]](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[\)

A partire da Element 12.5, NetApp HealthTools non è più supportato per gli aggiornamenti software di Element. Se stai eseguendo Element 11.0 o 11.1, devi prima ["aggiorna a Element 12.3.x utilizzando HealthTools"](#) e poi eseguire l'aggiornamento a Element 12.5 o versione successiva utilizzando NetApp Hybrid Cloud Control.

- **Sincronizzazione dell'ora di sistema:** hai verificato che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di archiviazione e i nodi. Ogni nodo deve essere configurato con un nameserver DNS nell'interfaccia utente Web per nodo([https://\[IP_address\]:442](https://[IP_address]:442)) senza guasti di cluster irrisolti correlati allo sfasamento temporale.

- **Porte di sistema:** se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, è necessario assicurarsi che le porte necessarie siano aperte. Vedere ["Porte di rete"](#) per maggiori informazioni.
- **Nodo di gestione:** per l'interfaccia utente e l'API NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Stato del cluster:** hai verificato che il cluster è pronto per essere aggiornato. Vedere ["Eseguire controlli di integrità dell'archiviazione Element prima di aggiornare l'archiviazione"](#).
- **Controller di gestione della scheda base (BMC) aggiornato per i nodi di archiviazione H610S:** hai aggiornato la versione BMC per i tuoi nodi H610S. Vedi il ["note di rilascio e istruzioni di aggiornamento"](#).
- **Tempo di esecuzione dell'aggiornamento:** hai programmato tempo sufficiente per eseguire l'aggiornamento. Quando si esegue l'aggiornamento al software Element 12.5 o versione successiva, la durata del processo di aggiornamento varia a seconda della versione corrente del software Element e degli aggiornamenti del firmware.

Nodo di archiviazione	Versione attuale del software Element	Tempo approssimativo di installazione del software e del firmware per nodo ¹	Tempo approssimativo di sincronizzazione dei dati per nodo ²	Tempo di aggiornamento totale approssimativo per nodo
Tutti i nodi SolidFire e NetApp serie H con firmware aggiornato ³	12.x	15 minuti	da 10 a 15 minuti	da 20 a 30 minuti
H610S e H410S	12.x e 11.8	60 minuti	da 30 a 60 minuti	da 90 a 120 minuti
H610S	11.7 e precedenti	90 minuti	da 40 a 70 minuti	Da 130 a 160 minuti Devi anche "eseguire uno spegnimento completo del nodo e la disconnessione dell'alimentazione" per ogni nodo H610S.

¹Per una matrice completa del firmware e del driver firmware per il tuo hardware, vedi ["versioni del firmware di archiviazione supportate per i nodi di archiviazione SolidFire"](#).

²Se si combina un cluster con un carico IOPS di scrittura elevato con un tempo di aggiornamento del firmware più lungo, il tempo di sincronizzazione dei dati aumenterà.

³ I seguenti nodi non sono supportati. Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x:

- A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
- A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608 e nodi FC FC0025 e SF-FCN-01.

- **Contratto di licenza con l'utente finale (EULA):** a partire dalla versione 2.20.69 dei servizi di gestione, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API 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. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
c. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
d. Viene visualizzato l'EULA. Scorri verso il basso, seleziona **Accetto per gli aggiornamenti attuali e futuri** e seleziona **Salva**.

Opzioni di aggiornamento

Scegli una delle seguenti opzioni di aggiornamento del software Element:

- [Utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud per aggiornare lo storage Element](#)
- [Utilizzare l'API NetApp Hybrid Cloud Control per aggiornare lo storage Element](#)



Se si sta aggiornando un nodo della serie H610S a Element 12.5 o versione successiva e il nodo esegue una versione di Element precedente alla 11.8, sarà necessario eseguire i passaggi di aggiornamento aggiuntivi in questo ["Articolo della Knowledge Base"](#) per ogni nodo di archiviazione. Se si utilizza Element 11.8 o una versione successiva, non sono necessari ulteriori passaggi di aggiornamento.

Utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud per aggiornare lo storage Element

Utilizzando l'interfaccia utente di controllo di NetApp Hybrid Cloud, è possibile aggiornare un cluster di storage.



Per potenziali problemi durante l'aggiornamento dei cluster di storage utilizzando NetApp Hybrid Cloud Control e le relative soluzioni alternative, vedere questo ["Articolo della Knowledge Base"](#).

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
4. Nella pagina **Aggiornamenti**, seleziona **Archiviazione**.

Nella scheda **Archiviazione** sono elencati i cluster di archiviazione che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Aggiornamenti**.

5. Scegli tra le seguenti opzioni ed esegui la serie di passaggi applicabili al tuo cluster:

Opzione	Passi
Tutti i cluster che eseguono Element 11.8 e versioni successive	a. Seleziona Sfoggia per caricare il pacchetto di aggiornamento che hai scaricato. b. Attendi il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.  Il caricamento del file andrà perso se si esce dalla finestra del browser. Una volta caricato e convalidato correttamente il file, verrà visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere diversi minuti. Se in questa fase si esce dalla finestra del browser, il caricamento del file viene mantenuto. c. Seleziona Inizia aggiornamento.  Lo Stato dell'aggiornamento cambia durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, ad esempio sospendendo l'aggiornamento o se l'aggiornamento restituisce un errore. Vedere Modifiche allo stato dell'aggiornamento.  Mentre l'aggiornamento è in corso, puoi uscire dalla pagina e tornarci 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 è compressa. Per aggiornare la tabella è necessario espandere la riga del cluster oppure è possibile aggiornare la pagina. Una volta completato l'aggiornamento, sarà possibile scaricare i registri.

Opzione	Passi
Stai aggiornando un cluster H610S che esegue una versione Element precedente alla 11.8.	a. Selezionare la freccia a discesa accanto al cluster che si sta aggiornando e scegliere tra le versioni di aggiornamento disponibili. b. Seleziona Inizia aggiornamento. Una volta completato l'aggiornamento, l'interfaccia utente richiede di eseguire ulteriori passaggi di aggiornamento. c. Completare i passaggi aggiuntivi richiesti nel "Articolo della Knowledge Base" e conferma nell'interfaccia utente di aver completato la fase 2. Una volta completato l'aggiornamento, sarà possibile scaricare i registri. Per informazioni sulle varie modifiche dello stato di aggiornamento, vedere Modifiche allo stato dell'aggiornamento.

Modifiche allo stato dell'aggiornamento

Ecco i diversi stati mostrati nella colonna **Stato aggiornamento** nell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato all'ultima versione Element disponibile.
Versioni disponibili	Sono disponibili versioni più recenti del firmware Element e/o di archiviazione per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi sullo schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ciascun nodo nel cluster man mano che l'aggiornamento procede. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente vCenter Server.
Aggiornamento in pausa	Puoi scegliere di mettere in pausa l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Verrà visualizzato un messaggio nell'interfaccia utente che chiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di sospendere un aggiornamento, potrebbero essere necessarie fino a due ore affinché l'operazione di aggiornamento venga completamente sospesa. Per riprendere l'aggiornamento, seleziona Riprendi .

Stato di aggiornamento	Descrizione
In pausa	Hai messo in pausa l'aggiornamento. Selezionare Riprendi per riprendere il processo.
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, puoi tornare alla pagina e selezionare Riprendi . Quando si riprende l'aggiornamento, la barra di avanzamento torna indietro per alcuni minuti mentre il sistema esegue il controllo dello stato e verifica lo stato attuale dell'aggiornamento.
Completa con Follow-up	Solo per i nodi H610S che effettuano l'aggiornamento da una versione Element precedente alla 11.8. Una volta completata la fase 1 del processo di aggiornamento, questo stato richiede di eseguire ulteriori passaggi di aggiornamento (vedere " Articolo della Knowledge Base "). Dopo aver completato la fase 2 e confermato di averla completata, lo stato cambia in Aggiornato .

Utilizzare l'API NetApp Hybrid Cloud Control per aggiornare lo storage Element

È possibile utilizzare le API per aggiornare i nodi di archiviazione in un cluster alla versione più recente del software Element. Puoi utilizzare lo strumento di automazione che preferisci per eseguire le API. Il flusso di lavoro API qui documentato utilizza come esempio l'interfaccia utente dell'API REST disponibile sul nodo di gestione.

Passi

1. Scaricare il pacchetto di aggiornamento dell'archiviazione su un dispositivo accessibile al nodo di gestione.

Vai al software Element "[pagina dei download](#)" e scaricare l'immagine più recente del nodo di archiviazione.

2. Carica il pacchetto di aggiornamento dell'archiviazione sul nodo di gestione:

- a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client`.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente dell'API REST, seleziona **POST /packages**.
- d. Seleziona **Provalo**.
- e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.

- f. Selezionare **Esegui** per avviare il caricamento.
 - g. Dalla risposta, copia e salva l'ID del pacchetto("id") per utilizzarlo in una fase successiva.
3. Verificare lo stato del caricamento.
- a. Dall'interfaccia utente dell'API REST, seleziona **GET /packages/{id}/status**.
 - b. Seleziona **Provalo**.
 - c. Inserisci 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` una volta completato.

4. Individuare l'ID del cluster di archiviazione:

- a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client` .
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
 - c. Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.
 - d. Seleziona **Provalo**.
 - e. Selezionare **Esegui**.
 - f. Dalla risposta, copia l'ID della risorsa di installazione("id").
 - g. Dall'interfaccia utente dell'API REST, seleziona **GET /installations/{id}**.
 - h. Seleziona **Provalo**.
 - i. Incolla l'ID della risorsa di installazione nel campo **id**.
 - j. Selezionare **Esegui**.
 - k. Dalla risposta, copia e salva l'ID del cluster di archiviazione("id") del cluster che intendi aggiornare per utilizzarlo in un passaggio successivo.
5. Eseguire l'aggiornamento dello storage:
- a. Aprire l'interfaccia utente dell'API REST di archiviazione sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client` .

- iii. Selezionare **Autorizza** per iniziare una sessione.
- iv. Chiudere la finestra di autorizzazione.
- c. Selezionare **POST /aggiornamenti**.
- d. Seleziona **Provalo**.
- e. Immettere l'ID del pacchetto di aggiornamento nel campo dei parametri.
- f. Immettere l'ID del cluster di archiviazione 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 dovrebbe 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. Copia l'ID di aggiornamento("upgradeId") che fa parte della risposta.
6. Verificare l'avanzamento e i risultati dell'aggiornamento:
- a. Selezionare **GET /upgrades/{upgradeld}**.
 - b. Seleziona **Provalo**.
 - c. Inserisci l'ID di aggiornamento del passaggio precedente in **upgradeld**.
 - d. Selezionare **Esegui**.
 - e. Se durante l'aggiornamento si verificano problemi o si verificano requisiti particolari, procedere come segue:

Opzione	Passi
È necessario correggere i problemi di integrità del cluster dovuti a <code>failedHealthChecks</code> messaggio nel corpo della risposta.	i. Andare all'articolo specifico della Knowledge Base elencato per ciascun problema oppure eseguire la soluzione specificata. ii. Se viene specificata una KB, completare la procedura descritta nell'articolo della KB pertinente. iii. Dopo aver risolto i problemi del cluster, ripetere l'autenticazione se necessario e selezionare PUT /upgrades/{upgradeld}. iv. Seleziona Provalo. v. Inserisci l'ID di aggiornamento del passaggio precedente in upgradeld. vi. Entra <code>"action": "resume"</code> nel corpo della richiesta. <pre>{ "action": "resume" }</pre> vii. Selezionare Esegui.
È necessario sospendere l'aggiornamento perché la finestra di manutenzione sta per chiudersi o per un altro motivo.	i. Se necessario, ripetere l'autenticazione e selezionare PUT /upgrades/{upgradeld}. ii. Seleziona Provalo. iii. Inserisci l'ID di aggiornamento del passaggio precedente in upgradeld. iv. Entra <code>"action": "pause"</code> nel corpo della richiesta. <pre>{ "action": "pause" }</pre> v. Selezionare Esegui.

Opzione	Passi
Se si sta aggiornando un cluster H610S che esegue una versione Element precedente alla 11.8, viene visualizzato lo stato <code>finishedNeedsAck</code> nel corpo della risposta. È necessario eseguire ulteriori passaggi di aggiornamento per ciascun nodo di archiviazione H610S.	i. Completare i passaggi di aggiornamento aggiuntivi in questo "Articolo della Knowledge Base" per ogni nodo. ii. Se necessario, ripetere l'autenticazione e selezionare PUT /upgrades/{upgradeld}. iii. Seleziona Provalo. iv. Inserisci l'ID di aggiornamento del passaggio precedente in upgradeld. v. Entra <code>"action": "acknowledge"</code> nel corpo della richiesta. <pre>{ "action": "acknowledge" }</pre> vi. Selezionare Esegui.

- f. Eseguire l'API **GET /upgrades/{upgradeld}** più volte, secondo 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 terminato con successo quando `percent` il valore è 100 e il `state` indica `finished`.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

Se un'unità o un nodo si guasta durante un aggiornamento, l'interfaccia utente di Element mostrerà gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione degli errori 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, selezionare **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per ricevere assistenza nell'indagine sul guasto.

NetApp Hybrid Cloud Control ha un periodo di attesa preimpostato di tre ore, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro la finestra temporale di tre ore e l'aggiornamento riprende. In questo scenario non è necessario intraprendere alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento mostra **Errore** con un banner rosso. Dopo aver risolto il problema, puoi riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere interrotto temporaneamente per adottare misure correttive prima della scadenza delle tre ore. Il supporto utilizzerà l'API per annullare l'aggiornamento.



L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe comportare la rimozione non corretta delle unità dal nodo. Se le unità vengono rimosse in modo improprio, aggiungerle nuovamente durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe impiegare 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 ricevere assistenza.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiorna il firmware di archiviazione

A partire da Element 12.0 e dalla versione 2.14 dei servizi di gestione, è possibile eseguire aggiornamenti solo del firmware sui nodi di storage utilizzando l'interfaccia utente di controllo NetApp Hybrid Cloud e l'API REST. Questa procedura non aggiorna il software Element e consente di aggiornare il firmware di archiviazione al di fuori di una versione principale di Element.

Cosa ti servirà

- **Privilegi di amministratore:** disponi delle autorizzazioni di amministratore del cluster di archiviazione per eseguire l'aggiornamento.
- **Sincronizzazione dell'ora di sistema:** hai verificato che l'ora di sistema su tutti i nodi sia sincronizzata e che NTP sia configurato correttamente per il cluster di archiviazione e i nodi. Ogni nodo deve essere configurato con un nameserver DNS nell'interfaccia utente Web per nodo([https://\[IP address\]:442](https://[IP address]:442)) senza guasti di cluster irrisolti correlati allo sfasamento temporale.
- **Porte di sistema:** se si utilizza NetApp Hybrid Cloud Control per gli aggiornamenti, è necessario assicurarsi che le porte necessarie siano aperte. Vedere ["Porte di rete"](#) per maggiori informazioni.
- **Nodo di gestione:** per l'interfaccia utente e l'API NetApp Hybrid Cloud Control, il nodo di gestione nel tuo ambiente esegue la versione 11.3.
- **Servizi di gestione:** Hai aggiornato il tuo pacchetto di servizi di gestione all'ultima versione.



Per i nodi di archiviazione H610S che eseguono il software Element versione 12.0, è necessario applicare la D-patch SUST-909 prima di eseguire l'aggiornamento al bundle firmware di archiviazione 2.27. Contattare l'assistenza NetApp per ottenere la D-patch prima di effettuare l'aggiornamento. Vedere ["Note sulla versione 2.27 del pacchetto firmware di archiviazione"](#).



Prima di aggiornare il firmware sui nodi di archiviazione, è necessario eseguire l'aggiornamento al pacchetto di servizi di gestione più recente. Se stai aggiornando il software Element alla versione 12.2 o successiva, per procedere è necessario disporre dei servizi di gestione 2.14.60 o successivi.

- **Stato del cluster:** sono stati eseguiti controlli di integrità. Vedere ["Eseguire controlli di integrità dell'archiviazione Element prima di aggiornare l'archiviazione"](#).
- **Controller di gestione della scheda base (BMC) aggiornato per i nodi H610S:** hai aggiornato la versione BMC per i tuoi nodi H610S. Vedere ["note di rilascio e istruzioni di aggiornamento"](#).



Per una matrice completa del firmware e del driver firmware per l'hardware, vedere ["versioni del firmware di archiviazione supportate per i nodi di archiviazione SolidFire"](#).

- **Tempo di esecuzione dell'aggiornamento:** hai programmato tempo sufficiente per eseguire l'aggiornamento. Quando si esegue l'aggiornamento al software Element 12.5 o versione successiva, la durata del processo di aggiornamento varia a seconda della versione corrente del software Element e degli aggiornamenti del firmware.

Nodo di archiviazione	Versione attuale del software Element	Tempo approssimativo di installazione del software e del firmware per nodo ¹	Tempo approssimativo di sincronizzazione dei dati per nodo ²	Tempo di aggiornamento totale approssimativo per nodo
Tutti i nodi SolidFire e NetApp serie H con firmware aggiornato ³	12.x	15 minuti	da 10 a 15 minuti	da 20 a 30 minuti
H610S e H410S	12.x e 11.8	60 minuti	da 30 a 60 minuti	da 90 a 120 minuti
H610S	11.7 e precedenti	90 minuti	da 40 a 70 minuti	Da 130 a 160 minuti Devi anche "eseguire uno spegnimento completo del nodo e la disconnessione dell'alimentazione" per ogni nodo H610S.

¹Per una matrice completa del firmware e del driver firmware per il tuo hardware, vedi ["versioni del firmware di archiviazione supportate per i nodi di archiviazione SolidFire"](#).

²Se si combina un cluster con un carico IOPS di scrittura elevato con un tempo di aggiornamento del firmware più lungo, il tempo di sincronizzazione dei dati aumenterà.

³ I seguenti nodi non sono supportati. Se si tenta di aggiornare uno di questi nodi a una versione di Element non supportata, verrà visualizzato un errore che indica che il nodo non è supportato da Element 12.x:

- A partire dai nodi di archiviazione Element 12.8, SF4805, SF9605, SF19210 e SF38410.
- A partire dall'elemento 12.7, nodi di archiviazione SF2405 e SF9608 e nodi FC FC0025 e SF-FCN-01.

- **Contratto di licenza con l'utente finale (EULA):** a partire dalla versione 2.20.69 dei servizi di gestione, è necessario accettare e salvare l'EULA prima di utilizzare l'interfaccia utente o l'API NetApp Hybrid Cloud Control per aggiornare il firmware di storage:

- a. Aprire l'indirizzo IP del nodo di gestione in un browser web:

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

- b. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
- c. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
- d. Viene visualizzato l'EULA. Scorri verso il basso, seleziona **Accetto per gli aggiornamenti attuali e futuri** e seleziona **Salva**.

Opzioni di aggiornamento

Scegli una delle seguenti opzioni di aggiornamento del firmware di archiviazione:

- [Utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud per aggiornare il firmware di storage](#)
- [Utilizzare l'API NetApp Hybrid Cloud Control per aggiornare il firmware di storage](#)

Utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud per aggiornare il firmware di storage

È possibile utilizzare l'interfaccia utente di controllo NetApp Hybrid Cloud per aggiornare il firmware dei nodi di storage nel cluster.

Cosa ti servirà

- Se il nodo di gestione non è connesso a Internet, è necessario ["scaricare il pacchetto firmware di archiviazione"](#).



Per 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 archiviazione. Se si aggiorna un cluster di archiviazione Element a un firmware di archiviazione più recente della versione 2.76, i singoli nodi di archiviazione si riavvieranno durante l'aggiornamento solo se è stato scritto un nuovo firmware sul nodo.

Passi

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

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

2. Accedi a NetApp Hybrid Cloud Control fornendo le credenziali di amministratore del cluster di storage.
3. Selezionare **Aggiorna** nella parte in alto a destra dell'interfaccia.
4. Nella pagina **Aggiornamenti**, seleziona **Archiviazione**.



Nella scheda **Archiviazione** sono elencati i cluster di archiviazione che fanno parte dell'installazione. Se un cluster non è accessibile da NetApp Hybrid Cloud Control, non verrà visualizzato nella pagina **Aggiornamenti**. Se disponi di cluster che eseguono Element 12.0 o versioni successive, per questi cluster verrà elencata la versione corrente del bundle del firmware. Se i nodi di un singolo cluster hanno versioni firmware diverse o man mano che l'aggiornamento procede, nella colonna **Versione attuale del bundle firmware** verrà visualizzato **Multiplo**. È possibile selezionare **Multiplo** per passare 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 sui numeri di versione del bundle del firmware.

Se il cluster è aggiornato e/o non sono disponibili pacchetti di aggiornamento, le schede **Elemento** e **Solo firmware** non vengono visualizzate. Queste schede non vengono visualizzate nemmeno quando è in corso un aggiornamento. Se viene visualizzata la scheda **Elemento**, ma non la scheda **Solo firmware**, non sono disponibili pacchetti firmware.

5. Selezionare la freccia a discesa accanto al cluster che si sta aggiornando.
6. Seleziona **Sfoglia** per caricare il pacchetto di aggiornamento che hai scaricato.
7. Attendi il completamento del caricamento. Una barra di avanzamento mostra lo stato del caricamento.



Il caricamento del file andrà perso se si esce dalla finestra del browser.

Una volta caricato e convalidato correttamente il file, verrà visualizzato un messaggio sullo schermo. La convalida potrebbe richiedere diversi minuti. Se in questa fase si esce dalla finestra del browser, il caricamento del file viene mantenuto.

8. Selezionare **Solo firmware** e scegliere tra le versioni di aggiornamento disponibili.
9. Seleziona **Inizia aggiornamento**.



Lo **Stato dell'aggiornamento** cambia durante l'aggiornamento per riflettere lo stato del processo. Cambia anche in risposta alle azioni intraprese, ad esempio sospendendo l'aggiornamento o se l'aggiornamento restituisce un errore. Vedere [Modifiche allo stato dell'aggiornamento](#).



Mentre l'aggiornamento è in corso, puoi uscire dalla pagina e tornarci 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 è compressa. Per aggiornare la tabella è necessario espandere la riga del cluster oppure è possibile aggiornare la pagina.

Una volta completato l'aggiornamento, sarà possibile scaricare i registri.

Modifiche allo stato dell'aggiornamento

Ecco i diversi stati mostrati nella colonna **Stato aggiornamento** nell'interfaccia utente prima, durante e dopo il processo di aggiornamento:

Stato di aggiornamento	Descrizione
Aggiornato	Il cluster è stato aggiornato all'ultima versione disponibile di Element oppure il firmware è stato aggiornato all'ultima versione.

Stato di aggiornamento	Descrizione
Impossibile rilevare	Questo stato viene visualizzato quando l'API del servizio di archiviazione restituisce uno stato di aggiornamento che non è presente nell'elenco enumerato dei possibili stati di aggiornamento.
Versioni disponibili	Sono disponibili versioni più recenti del firmware Element e/o di archiviazione per l'aggiornamento.
In corso	L'aggiornamento è in corso. Una barra di avanzamento mostra lo stato dell'aggiornamento. I messaggi sullo schermo mostrano anche gli errori a livello di nodo e visualizzano l'ID di ciascun nodo nel cluster man mano che l'aggiornamento procede. È possibile monitorare lo stato di ciascun nodo utilizzando l'interfaccia utente Element o il plug-in NetApp Element per l'interfaccia utente vCenter Server.
Aggiornamento in pausa	Puoi scegliere di mettere in pausa l'aggiornamento. A seconda dello stato del processo di aggiornamento, l'operazione di pausa può avere esito positivo o negativo. Verrà visualizzato un messaggio nell'interfaccia utente che chiede di confermare l'operazione di pausa. Per garantire che il cluster si trovi in una posizione sicura prima di sospendere un aggiornamento, potrebbero essere necessarie fino a due ore affinché l'operazione di aggiornamento venga completamente sospesa. Per riprendere l'aggiornamento, seleziona Riprendi .
In pausa	Hai messo in pausa l'aggiornamento. Selezionare Riprendi per riprendere il processo.
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, puoi tornare alla pagina e selezionare Riprendi . Quando si riprende l'aggiornamento, la barra di avanzamento torna indietro per alcuni minuti mentre il sistema esegue il controllo dello stato e verifica lo stato attuale dell'aggiornamento.

Cosa succede se un aggiornamento non riesce utilizzando NetApp Hybrid Cloud Control

Se un'unità o un nodo si guasta durante un aggiornamento, l'interfaccia utente di Element mostrerà gli errori del cluster. Il processo di aggiornamento non passa al nodo successivo e attende la risoluzione degli errori 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, selezionare **Pausa** nell'interfaccia utente non funzionerà, perché l'aggiornamento attende che il cluster sia integro. Sarà necessario contattare il supporto NetApp per ricevere assistenza nell'indagine sul guasto.

NetApp Hybrid Cloud Control ha un periodo di attesa preimpostato di tre ore, durante il quale può verificarsi uno dei seguenti scenari:

- Gli errori del cluster vengono risolti entro la finestra temporale di tre ore e l'aggiornamento riprende. In questo scenario non è necessario intraprendere alcuna azione.
- Il problema persiste dopo tre ore e lo stato dell'aggiornamento mostra **Errore** con un banner rosso. Dopo aver risolto il problema, puoi riprendere l'aggiornamento selezionando **Riprendi**.
- Il supporto NetApp ha stabilito che l'aggiornamento deve essere interrotto temporaneamente per adottare misure correttive prima della scadenza delle tre ore. Il supporto utilizzerà l'API per annullare l'aggiornamento.



L'interruzione dell'aggiornamento del cluster durante l'aggiornamento di un nodo potrebbe comportare la rimozione non corretta delle unità dal nodo. Se le unità vengono rimosse in modo improprio, aggiungerle nuovamente durante un aggiornamento richiederà l'intervento manuale del supporto NetApp. Il nodo potrebbe impiegare 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 ricevere assistenza.

Utilizzare l'API NetApp Hybrid Cloud Control per aggiornare il firmware di storage

È possibile utilizzare le API per aggiornare i nodi di archiviazione in un cluster alla versione più recente del software Element. Puoi utilizzare lo strumento di automazione che preferisci per eseguire le API. Il flusso di lavoro API qui documentato utilizza come esempio l'interfaccia utente dell'API REST disponibile sul nodo di gestione.

Passi

1. Scaricare il pacchetto di aggiornamento del firmware di archiviazione su un dispositivo accessibile al nodo di gestione; andare al software Element ["pagina dei download"](#) e scaricare l'immagine del firmware di archiviazione più recente.
2. Caricare il pacchetto di aggiornamento del firmware di archiviazione sul nodo di gestione:
 - a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/package-repository/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client`.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
 - c. Dall'interfaccia utente dell'API REST, seleziona **POST /packages**.
 - d. Seleziona **Provalo**.
 - e. Selezionare **Sfoglia** e selezionare il pacchetto di aggiornamento.
 - f. Selezionare **Esegui** per avviare il caricamento.
 - g. Dalla risposta, copia e salva l'ID del pacchetto("`id`") per utilizzarlo in una fase successiva.
3. Verificare lo stato del caricamento.
 - a. Dall'interfaccia utente dell'API REST, seleziona **GET /packages/{id}/status**.
 - b. Seleziona **Provalo**.

- c. Inserisci l'ID del pacchetto firmware copiato nel passaggio precedente in **id**.
- d. Selezionare **Esegui** per avviare la richiesta di stato.

La risposta indica `state` **COME SUCCESS** una volta completato.

4. Individuare l'ID della risorsa di installazione:

- a. Aprire l'interfaccia utente dell'API REST del nodo di gestione sul nodo di gestione:

```
https://<ManagementNodeIP>/inventory/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
 - i. Immettere il nome utente e la password del cluster.
 - ii. Inserisci l'ID cliente come `mnode-client`.
 - iii. Selezionare **Autorizza** per iniziare una sessione.
 - iv. Chiudere la finestra di autorizzazione.
- c. Dall'interfaccia utente dell'API REST, seleziona **GET /installations**.
- d. Seleziona **Provalo**.
- e. Selezionare **Esegui**.
- f. Dalla risposta, copia 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 dell'API REST, seleziona **GET /installations/{id}**.
- h. Seleziona **Provalo**.
 - i. Incolla l'ID della risorsa di installazione nel campo **id**.
 - j. Selezionare **Esegui**.
- k. Dalla risposta, copia e salva l'ID del cluster di archiviazione(`"id"`) del cluster che intendi aggiornare per utilizzarlo in un passaggio successivo.

```

"storage": {
  "errors": [],
  "inventory": {
    "clusters": [
      {
        "clusterUuid": "a1bd1111-4f1e-46zz-ab6f-0a1111b1111x",
        "id": "a1bd1111-4f1e-46zz-ab6f-a1a1a111b012",

```

5. Eseguire l'aggiornamento del firmware di archiviazione:

- a. Aprire l'interfaccia utente dell'API REST di archiviazione sul nodo di gestione:

```
https://<ManagementNodeIP>/storage/1/
```

- b. Seleziona **Autorizza** e completa quanto segue:
- Immettere il nome utente e la password del cluster.
 - Inserisci l'ID cliente come `mnode-client`.
 - Selezionare **Autorizza** per iniziare una sessione.
 - Chiudi la finestra.
- c. Selezionare **POST /aggiornamenti**.
- d. Seleziona **Provalo**.
- e. Immettere l'ID del pacchetto di aggiornamento nel campo dei parametri.
- f. Immettere l'ID del cluster di archiviazione nel campo dei parametri.
- g. Selezionare **Esegui** per avviare l'aggiornamento.

La risposta dovrebbe 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. Copia l'ID di aggiornamento("upgradeId") che fa parte della risposta.
6. Verificare l'avanzamento e i risultati dell'aggiornamento:
- a. Selezionare **GET /upgrades/{upgradeld}**.
 - b. Seleziona **Provalo**.
 - c. Inserisci l'ID di aggiornamento del passaggio precedente in **upgradeld**.
 - d. Selezionare **Esegui**.
 - e. Se durante l'aggiornamento si verificano problemi o si verificano requisiti particolari, procedere come segue:

Opzione	Passi
È necessario correggere i problemi di integrità del cluster dovuti a <code>failedHealthChecks</code> messaggio nel corpo della risposta.	i. Andare all'articolo specifico della Knowledge Base elencato per ciascun problema oppure eseguire la soluzione specificata. ii. Se viene specificata una KB, completare la procedura descritta nell'articolo della KB pertinente. iii. Dopo aver risolto i problemi del cluster, ripetere l'autenticazione se necessario e selezionare PUT /upgrades/{upgradeld}. iv. Seleziona Provalo. v. Inserisci l'ID di aggiornamento del passaggio precedente in upgradeld. vi. Entra <code>"action": "resume"</code> nel corpo della richiesta. <pre>{ "action": "resume" }</pre> vii. Selezionare Esegui.
È necessario sospendere l'aggiornamento perché la finestra di manutenzione sta per chiudersi o per un altro motivo.	i. Se necessario, ripetere l'autenticazione e selezionare PUT /upgrades/{upgradeld}. ii. Seleziona Provalo. iii. Inserisci l'ID di aggiornamento del passaggio precedente in upgradeld. iv. Entra <code>"action": "pause"</code> nel corpo della richiesta. <pre>{ "action": "pause" }</pre> v. Selezionare Esegui.

f. Eseguire l'API **GET /upgrades/{upgradeld}** più volte, secondo 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 terminato con successo quando `percent` il valore è 100 e il `state` indica `finished`.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiorna 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 aver aggiornato per la prima volta il pacchetto dei 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'utilità di registrazione. È necessario modificare la registrazione del plug-in vCenter su ogni vCenter Server in cui è necessario utilizzare il plug-in.



Il bundle dei servizi di gestione 2.27 include Element Plug-in per vCenter Server 5.5, compatibile solo con il nodo di gestione 12.8. Quando si esegue l'aggiornamento ai servizi di gestione 2.27, è necessario modificare la sequenza di aggiornamento e aggiornare il bundle dei servizi di gestione *dopo* l'aggiornamento a Element 12.8 per garantire la compatibilità tra il nodo di gestione e i servizi di gestione.

Il bundle 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 a Management Services 2.22.7 o versione successiva per conformarsi alla direttiva VMware che rimuove il supporto per i plug-in locali. ["Saperne di più"](#).

Plug-in Element vCenter 5.0 o successivo

Questa procedura di aggiornamento copre i seguenti scenari di aggiornamento:

- Stai eseguendo l'aggiornamento a Element Plug-in per vCenter Server 5.5, 5.4, 5.3, 5.2, 5.1 o 5.0.
- Stai effettuando l'aggiornamento a vSphere Web Client HTML5 8.0 o 7.0.



Element Plug-in 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 vCenter a un plug-in remoto. È necessario aggiungere nuovamente i cluster al plug-in remoto. Questa è un'attività da eseguire una sola volta quando si esegue l'aggiornamento da un plug-in locale a uno remoto.

Plug-in Element vCenter 4.10 o precedente

Questa procedura di aggiornamento copre i seguenti scenari di aggiornamento:

- Stai effettuando l'aggiornamento a Element Plug-in per vCenter Server 4.10, 4.9, 4.8, 4.7, 4.6, 4.5 o 4.4.
- Stai effettuando l'aggiornamento a vSphere Web Client HTML5 7.0, 6.7 o 6.5.

- 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.

- Stai eseguendo l'aggiornamento a Flash vSphere Web Client 6.7.



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 di HTML5 vSphere Web Client e con altre build 6.7 U2 rilasciate prima dell'aggiornamento 2a (build 13643870). Per ulteriori informazioni sulle versioni vSphere supportate, consultare le note di rilascio per "[la tua versione del plug-in](#)".

Cosa ti servirà

- **Privilegi di amministratore:** disponi dei privilegi del ruolo 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:** la versione 4.x o 5.x del plug-in vCenter è registrata con un vCenter Server. Dall'utilità di registrazione(<https://<ManagementNodeIP>:9443>), selezionare **Stato registrazione**, compilare i campi necessari e selezionare **Verifica stato** per verificare che il plug-in vCenter sia già registrato e il numero di versione dell'installazione corrente.
- **Aggiornamenti dei servizi di gestione:** Hai aggiornato il tuo "[pacchetto di servizi di gestione](#)" alla versione più recente. Gli aggiornamenti al plug-in vCenter vengono distribuiti tramite aggiornamenti dei servizi di gestione rilasciati al di fuori delle principali release di prodotto per lo storage all-flash NetApp SolidFire.
- **Aggiornamenti del nodo di gestione:**

Plug-in Element vCenter 5.0 o successivo

Stai eseguendo un nodo di gestione che è stato "[aggiornato](#)" alla versione 12.3.x o successiva.

Plug-in Element vCenter 4.10 o precedente

Per il plug-in Element vCenter dalla versione 4.4 alla 4.10, si sta eseguendo un nodo di gestione che è stato "[aggiornato](#)" alla versione 11.3 o successiva. Il plug-in vCenter 4.4 o successivo richiede un nodo di gestione 11.3 o successivo con un'architettura modulare che fornisce servizi individuali. Il nodo di gestione deve essere acceso e il suo indirizzo IP o indirizzo DHCP deve essere configurato.

- **Aggiornamenti dello spazio di archiviazione degli elementi:**
 - 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 precedente, si dispone di un cluster che esegue il software NetApp Element 11.3 o successivo.
- **vSphere Web Client:** è necessario aver effettuato la disconnessione da vSphere Web Client prima di iniziare qualsiasi aggiornamento del plug-in. Se non effettui il logout, il client Web non riconoscerà gli

aggiornamenti apportati al plug-in durante questo processo.

Passi

1. Inserisci l'indirizzo IP del tuo nodo di gestione in un browser, inclusa la porta TCP per la registrazione:
<https://<ManagementNodeIP>:9443> L'interfaccia utente dell'utilità di registrazione si apre sulla pagina **Gestisci credenziali del servizio QoSSIOC** per il plug-in.

The screenshot shows the NetApp Element Plug-in for vCenter Server Management Node interface. The top header is dark blue with the NetApp logo and the text 'Element Plug-in for vCenter Server Management Node'. Below the header, there are two tabs: 'QoSSIOC Service Management' (selected) and 'vCenter Plug-in Registration'. The main content area is titled 'Manage QoSSIOC Service Credentials'. On the left, there is a sidebar with 'QoSSIOC Management' and two options: 'Manage Credentials' (selected) and 'Restart QoSSIOC Service'. The main form has three sections: 'Old Password' with a 'Current password' field and a note 'Current password is required'; 'New Password' with a 'New password' field and a note 'Must contain at least 8 characters with at least one lower-case and upper-case alphabet, a number and a special character like # \$ % & ' () - / . * ! @ ~ _'; and 'Confirm Password' with a 'Confirm New Password' field and a note 'New and confirm passwords must match'. At the bottom of the form is a 'SUBMIT CHANGES' button. At the very bottom of the page, there is a footer that says 'Contact NetApp Support at <http://mysupport.netapp.com>'.

2. Selezionare **Registrazione plug-in vCenter**.

Plug-in Element vCenter 5.0 o successivo

Viene visualizzata la pagina di registrazione del plug-in vCenter:

 **NetApp**

Element Plug-in for vCenter Server Management Node

GoSSIOC Service Management

vCenter Plug-in Registration

Manage vCenter Plug-in

Register Plug-in

Update Plug-in

Unregister Plug-in

Registration Status

vCenter Plug-in - Registration

Register version 5.0.0 of the NetApp Element Plug-in for vCenter Server with your vCenter server.
The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address

vCenter Server Address

Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name

vCenter Admin User Name

Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password

vCenter Admin Password

The password for the vCenter user name entered.

☐ Customize URL

Select to customize the Zip file URL.

Plug-in Zip URL

https://10.117.227.44:8333/vcp-ui/plugin.json

URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

Plug-in Element vCenter 4.10 o precedente

Viene visualizzata la pagina di registrazione del plug-in vCenter:

Manage vCenter Plug-in

- Register Plug-in
- Update Plug-in
- Unregister Plug-in
- Registration Status

vCenter Plug-in - Registration

Register version of the NetApp Element Plug-in for vCenter Server with your vCenter server.
The Plug-in will not be deployed until a fresh vCenter login after registration.

vCenter Address vCenter Server Address
Enter the IPV4, IPV6 or DNS name of the vCenter server to register plug-in on.

vCenter User Name vCenter Admin User Name
Ensure this user is a vCenter user that has administrative privileges for registration.

vCenter Password vCenter Admin Password
The password for the vCenter user name entered.

☐ **Customize URL**
Select to customize the Zip file URL.

Plug-in Zip URL https://10.117.227.12-9443/solidfire-plugin-4.6.0-bin.zip
URL of XML initialization file

REGISTER

Contact NetApp Support at <http://mysupport.netapp.com>

3. In **Gestisci plug-in vCenter**, seleziona **Aggiorna plug-in**.

4. Conferma o aggiorna le seguenti informazioni:

- a. L'indirizzo IPv4 o l'FQDN del servizio vCenter su cui registrerai il tuo plug-in.
- b. Nome utente dell'amministratore vCenter.



Le credenziali di nome utente e password immesse devono essere quelle di un utente con privilegi di amministratore vCenter.

- c. La password dell'amministratore di vCenter.
- d. (Per server interni/siti oscuri) A seconda della versione di Element Plug-in per vCenter, un URL personalizzato per il file JSON del plug-in o per il file ZIP del plug-in:

Plug-in Element vCenter 5.0 o successivo

Un URL personalizzato per il file JSON del plug-in.



Puoi selezionare **URL personalizzato** per personalizzare l'URL se stai utilizzando un server HTTP o HTTPS (sito oscuro) o se hai modificato il nome del file JSON o le impostazioni di rete. Per ulteriori passaggi di configurazione se si intende personalizzare un URL, consultare la documentazione di Element Plug-in per vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (dark site).

Plug-in Element vCenter 4.10 o precedente

Un URL personalizzato per il plug-in ZIP.



È possibile selezionare **URL personalizzato** per personalizzare l'URL se si utilizza un server HTTP o HTTPS (sito oscuro) o se sono stati modificati il nome del file ZIP o le impostazioni di rete. Per ulteriori passaggi di configurazione se si intende personalizzare un URL, consultare la documentazione di Element Plug-in per vCenter Server sulla modifica delle proprietà di vCenter per un server HTTP interno (dark site).

5. Selezionare **Aggiorna**.

Una volta completata la registrazione, nell'interfaccia utente dell'utilità di registrazione viene visualizzato un banner.

6. Accedi a vSphere Web Client come amministratore vCenter. Se hai già effettuato l'accesso a vSphere Web Client, devi prima disconnetterti, attendere due o tre minuti e quindi effettuare nuovamente l'accesso.



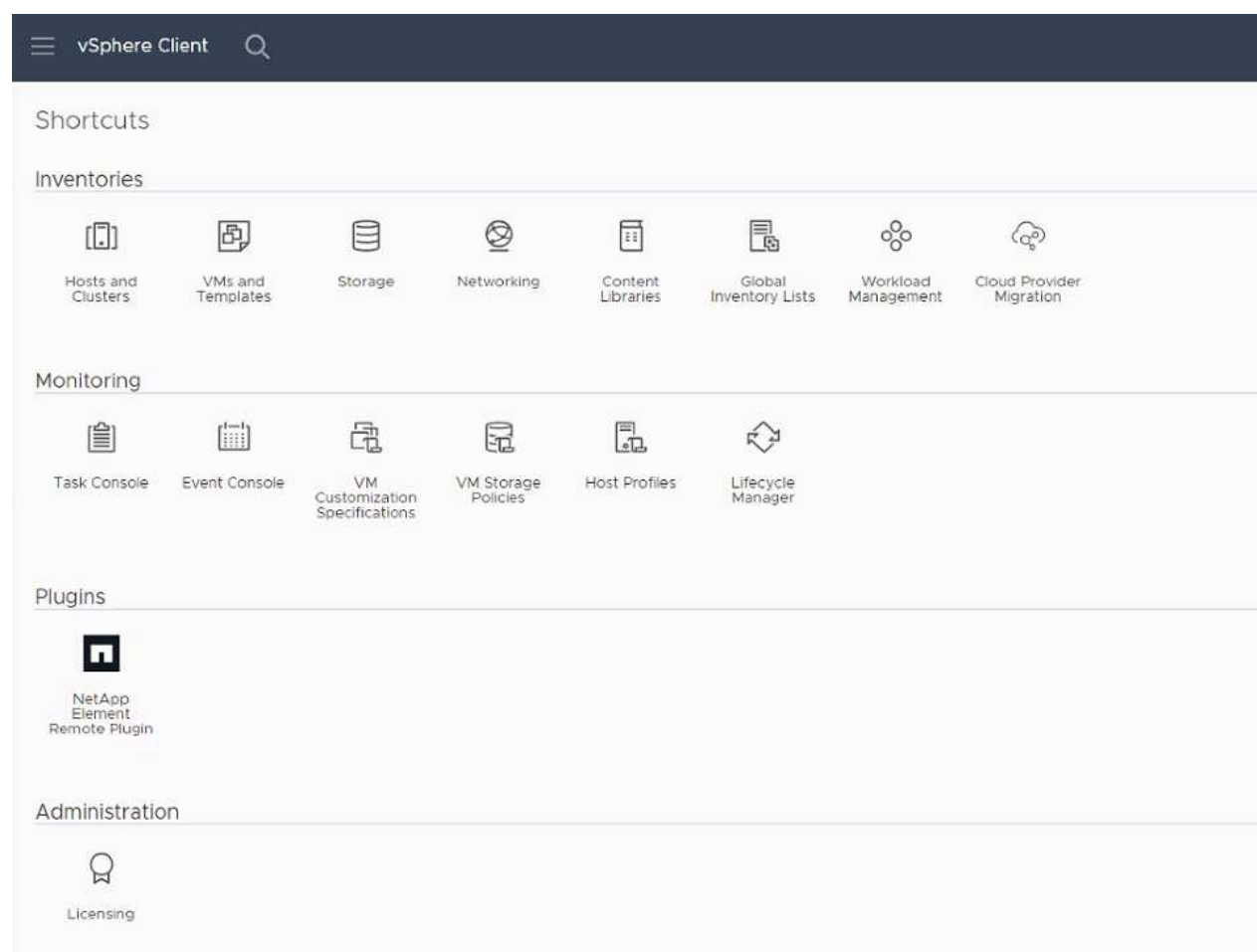
Questa azione crea un nuovo database e completa l'installazione in vSphere Web Client.

7. In vSphere Web Client, cercare le seguenti attività completate nel monitoraggio attività 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 **Collegamenti** di vSphere Web Client e nel pannello laterale.

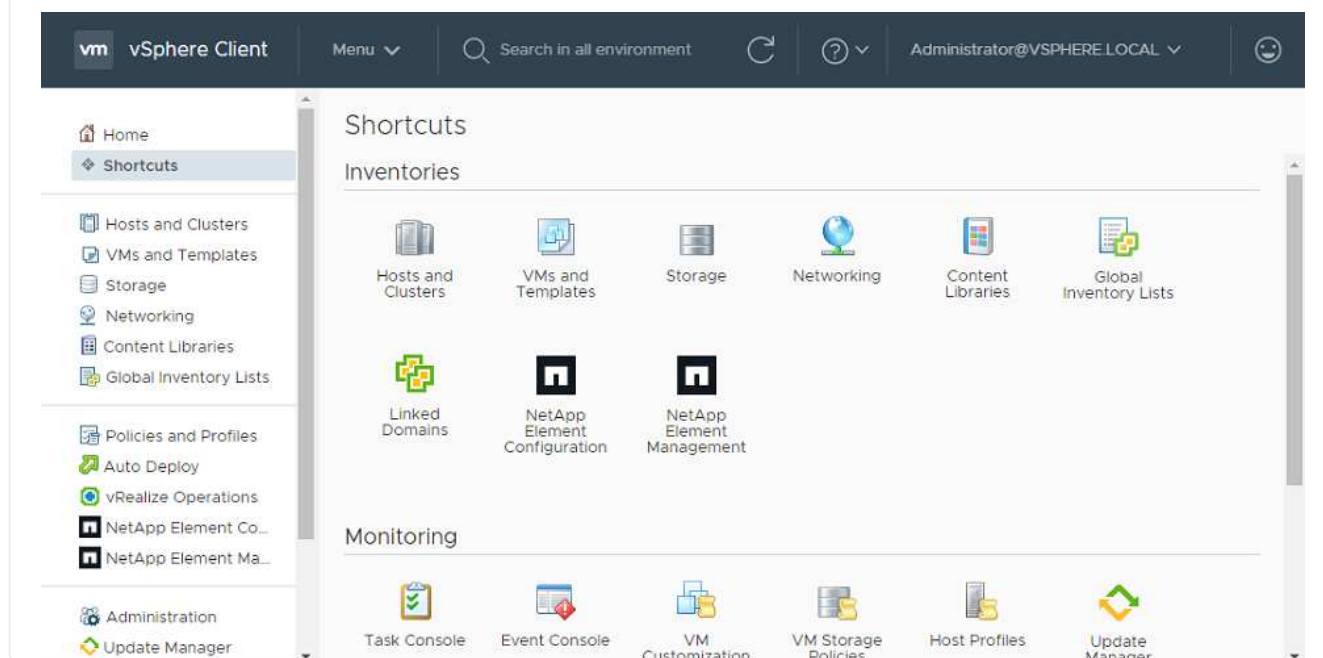
Plug-in Element vCenter 5.0 o successivo

Viene visualizzato il punto di estensione NetApp Element Remote Plugin:



Plug-in Element vCenter 4.10 o precedente

Vengono visualizzati i punti di estensione NetApp Element Configuration and Management:



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 l'aggiornamento a NetApp Element Plug-in per vCenter Server 4.8 o versione successiva con VMware vCenter Server 6.7U1, se i cluster di storage non sono elencati o viene visualizzato un errore del server nelle sezioni **Cluster** e **Impostazioni QoS** 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 **Informazioni** nel punto di estensione *Configurazione NetApp Element* del plug-in.

Dovresti vedere i seguenti dettagli sulla versione:

```
NetApp Element Plug-in Version: 5.5
NetApp Element Plug-in Build Number: 16
```



Il plug-in vCenter contiene contenuti della Guida in linea. Per assicurarti che la tua Guida contenga i contenuti più recenti, svuota la cache del browser dopo aver aggiornato il plug-in.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Aggiorna i tuoi componenti vSphere per un sistema di storage NetApp SolidFire con Element Plug-in per vCenter Server

Quando si aggiornano i componenti VMware vSphere, è necessario completare passaggi aggiuntivi. Questi passaggi sono necessari per i sistemi dotati di Element Plug-in per vCenter Server.

Passi

1. Per gli aggiornamenti vCSA, ["chiaro"](#) Impostazioni QoS nel plug-in (* Configurazione NetApp Element > Impostazioni QoS*). Il campo **Stato QoS** visualizza Not Configured dopo il completamento del processo.
2. Per gli aggiornamenti vCSA e Windows, ["annullare la registrazione"](#) il plug-in dal vCenter Server a cui è associato tramite l'utilità di registrazione.
3. ["Aggiorna vSphere, inclusi vCenter Server, ESXi, VM e altri componenti VMware"](#).



Dovresti eseguire l'aggiornamento a NetApp Element Plug-in per vCenter Server 5.0 o versione successiva per poter distribuire il plug-in con VMware vCenter 7.0 Update 3 senza dover applicare una soluzione alternativa.

Quando si esegue l'aggiornamento a VMware vCenter Server 7.0 Update 3, il plug-in Element per vCenter Server 4.x non riesce a distribuire. Per risolvere questo problema utilizzando Spring Framework 4, vedere ["questo articolo della Knowledge Base"](#).

4. ["Registro"](#) il plug-in Element per vCenter Server di nuovo con vCenter.
5. ["Aggiungi cluster"](#) utilizzando il plug-in.
6. ["Configurare le impostazioni QoSSIOC"](#) utilizzando il plug-in.
7. ["Abilita QoSSIOC"](#) per tutti i datastore controllati dal plug-in.

Trova maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Versioni precedenti della documentazione del software SolidFire e NetApp Element

La documentazione per le versioni precedenti è disponibile sul sito di supporto NetApp .

- ["Documentazione dell'elemento 12.2.1"](#)
- ["Documentazione dell'elemento 12.2"](#)
- ["Documentazione dell'elemento 12.0.1"](#)
- ["Documentazione dell'elemento 12.0"](#)
- ["Documentazione dell'elemento 11.8.2"](#)
- ["Documentazione dell'elemento 11.8.1"](#)
- ["Documentazione dell'elemento 11.8"](#)
- ["Documentazione dell'elemento 11.7"](#)
- ["Documentazione dell'elemento 11.5.1"](#)
- ["Documentazione dell'elemento 11.5"](#)
- ["Documentazione dell'elemento 11.3P1"](#)
- ["Documentazione dell'elemento 11.3.2"](#)
- ["Documentazione dell'elemento 11.1 e versioni precedenti"](#)

Per maggiori informazioni

- ["Documentazione del software SolidFire ed Element"](#)
- ["Plug-in NetApp Element per vCenter Server"](#)

Note legali

Le note legali forniscono accesso a dichiarazioni di copyright, marchi commerciali, brevetti e altro ancora.

Copyright

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

Marchi

NETAPP, il logo NETAPP e i marchi elencati nella pagina Marchi NetApp sono marchi di NetApp, Inc. Altri nomi di aziende e prodotti possono essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Politica sulla riservatezza

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

Open source

I file di avviso forniscono informazioni sui diritti d'autore e sulle licenze di terze parti utilizzati nel software NetApp .

- ["Avviso per il software Element 12.8"](#)
- ["Avviso per Element software 12.7"](#)
- ["Avviso per Ember OS 12.7"](#)
- ["Avviso per il nodo di gestione 12.7"](#)
- ["Avviso per il software Element 12.5"](#)
- ["Avviso per il nodo di gestione 12.5"](#)
- ["Avviso per Management Services 2.27.40 \(plug-in NetApp Element per VMware vCenter Server 5.5.16\)"](#)
- ["Avviso per Management Services 2.26.30 \(plug-in NetApp Element per VMware vCenter Server 5.4.1\)"](#)
- ["Avviso per Management Services 2.25.42 \(plug-in NetApp Element per VMware vCenter Server 5.3.9\)"](#)
- ["Avviso per Management Services 2.24.40 \(plug-in NetApp Element per VMware vCenter Server 5.2.12\)"](#)
- ["Avviso per Management Services 2.23.64 \(plug-in NetApp Element per VMware vCenter Server 5.1.12\)"](#)
- ["Avviso per Management Services 2.22.7 \(plug-in NetApp Element per VMware vCenter Server 5.0.37\)"](#)
- ["Avviso per Management Services 2.21.61 \(plug-in NetApp Element per VMware vCenter Server 4.10.12\)"](#)

- "Avviso per Management Services 2.20.69 (plug-in NetApp Element per vCenter Server 4.9.14)"
- "Avviso per Management Services 2.19.48 (plug-in NetApp Element per vCenter Server 4.8.34)"
- "Avviso per Management Services 2.18.91 (plug-in NetApp Element per vCenter Server 4.7.10)"
- "Avviso per Management Services 2.17.56 (plug-in NetApp Element per vCenter Server 4.6.32)"
- "Avviso per Management Services 2.17.52 (plug-in NetApp Element per vCenter Server 4.6.29)"
- "Avviso per Management Services 2.16 (plug-in NetApp Element per vCenter Server 4.6.29)"
- "Avviso per Management Services 2.14 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per Management Services 2.13 (plug-in NetApp Element per vCenter Server 4.5.42)"
- "Avviso per il pacchetto firmware di archiviazione 2.182.0"
- "Avviso per il pacchetto firmware di archiviazione 2.175.0"
- "Avviso per il pacchetto firmware di archiviazione 2.164.0"
- "Avviso per il pacchetto firmware di archiviazione 2.150"
- "Avviso per il pacchetto firmware di archiviazione 2.146"
- "Avviso per il pacchetto firmware di archiviazione 2.99.2"
- "Avviso per il pacchetto firmware di archiviazione 2.76"
- "Avviso per il pacchetto firmware di archiviazione 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 COMMERCIALIZZABILITÀ 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 CONSEGUENZIALE (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.